BANGLADESH CYBERSECURITY MAGAZINE

Indicator of Compromise (IoC) of FASTCash 2.0

BGD e-GOV CIRT

September, 2020

SECURING YOUR WORK PLACE FROM CYBER ATTACK AND GLOBAL BEST PRACTICES

Choosing, Implementing and Running a Security Information and Event Management (SIEM) Solution

BGD e-GOV CIRT

Name of Magazine	**Bangladesh Cybersecurity Magazine**
Chief Patron	Zunaid Ahmed Palak Hon'ble State Minister for ICT
Chief Advisor	N M Zeaul Alam Senior Secretary, ICT Division
Chief Editor	Tarique M Barkatullah Project Director
Magazine Mode	Monthly
Issue	September 2020
Published From	BGD e-GOV CIRT, Bangladesh Computer Council, ICT Division, Ministry of Posts, Telecommunications and Information Technology
Address	E-14/X, ICT Tower, Agargaon, Dhaka-1207, Bangladesh
Contact	info@cirt.gov.bd
Content Provider	BGD e-GOV CIRT Team
Content Finalized by	Tarique M Barkatullah, Project Director Tawhidur Rahman Pial, Team Lead
Content Designer	BGD e-GOV CIRT Team
Image Content	From Internet
Graphics Content	From Internet
Copyright	All rights reserved

Contents

BGD e-GOV CIRT

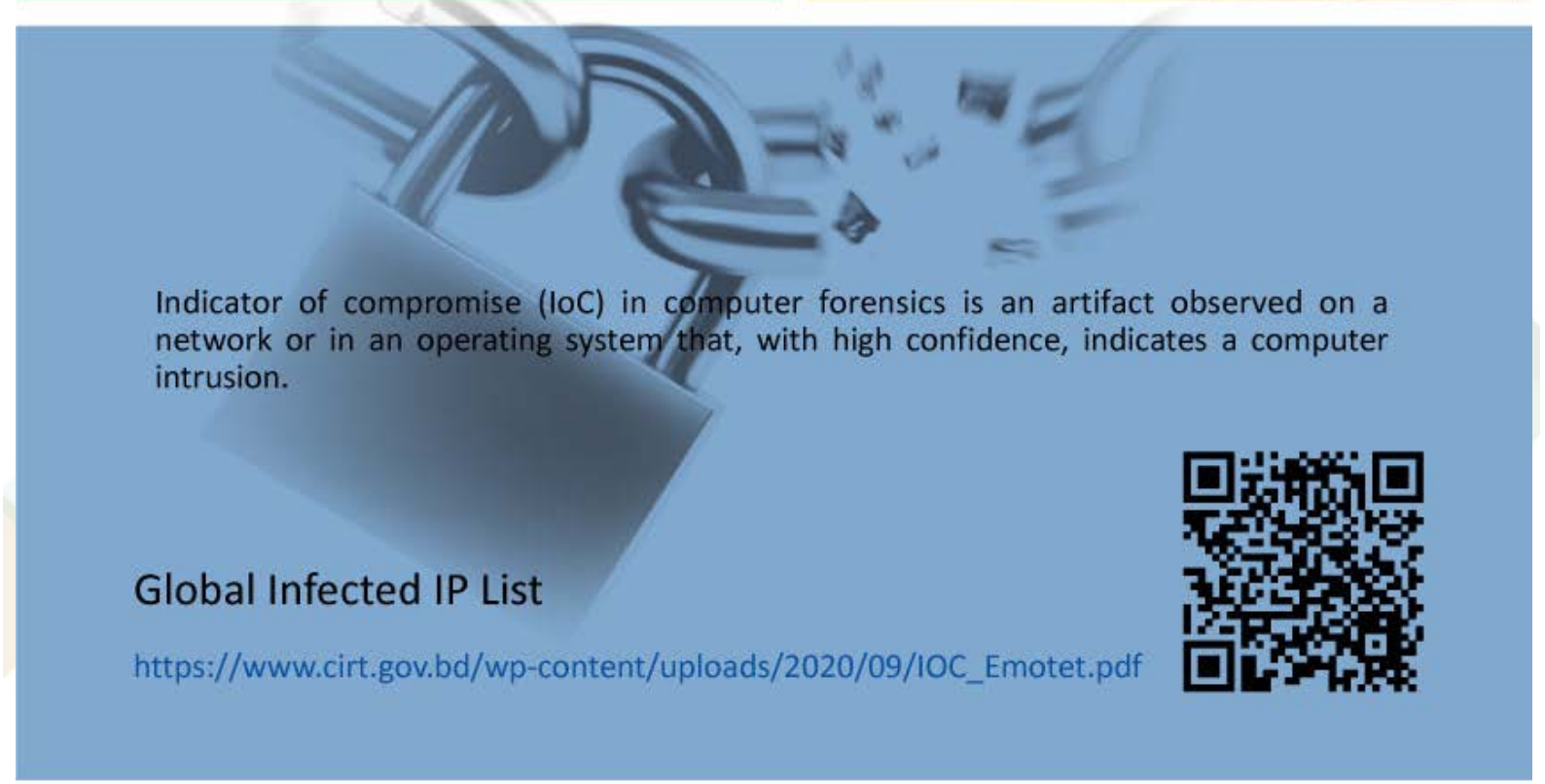
Bangladesh e-Government Computer Incident Response Team

National CIRT [N-CERT]

BGD e-GOV CIRT

Indicator of Compromise (IOC) of FastCash 2.0

BGD e-GOV CIRT in association with its global partners has obtained recent threat intelligence on Indicator of Compromise (IOC) of FastCash 2.0. The IOCs are provided below for necessary action by the relevant stakeholders.



Indicator of compromise (IoC) in computer forensics is an artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.

Global Infected IP List

https://www.cirt.gov.bd/wp-content/uploads/2020/09/IOC_Emotet.pdf

Indicator of compromise (IoC) in computer forensics is an artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.

Indicator type	Indicator
FileHash-SHA256	820ca1903a30516263d630c7c08f2b95f7b65dffceb21129c51c9e21cf9551c6
FileHash-SHA256	d928b1c1096e636463afbd19f40a6b325e159196b4497895748c31535ea503dc
FileHash-SHA256	16251b20e449d46e2b431c3aed229cd1f43f1ff18db67cc5a7fa7dd19673a9bc
FileHash-SHA256	f12db45c32bda3108adb8ae7363c342fdd5f10342945b115d830701f95c54fa9
FileHash-SHA256	0e3552c8232e007f421f241ea4188ea941f4d34eab311a5c2341488749d892c7
FileHash-SHA256	4a740227eeb82c20286d9c112ef95f0c1380d0e90ffb39fc75c8456db4f60756
FileHash-SHA256	2938200b7c0300c31aa458860b9f4f684f4f3f5893ab0f1d67c9d797168cad17
FileHash-SHA256	a1f06d69bd6379e310b10a364d689f21499953fa1118ec699a25072779de5d9b
FileHash-SHA256	d48b211533f37e082a907d4ee3b0364e5a363f1da14f74a81b187e1ce19945a8
FileHash-SHA256	f9d29b21bb93004cea6431e79f7aa24b9cc419289ca04c0353d9e3db3c587930
FileHash-MD5	4c26b2d0e5cd3bfe0a3d07c4b85909a4
FileHash-MD5	cf733e719e9677ebfbc84a3ab08dd0dc
FileHash-MD5	41fd85ff44107e4604db2f00e911a766
FileHash-MD5	5cfa1c2cb430bec721063e3e2d144feb
FileHash-MD5	52ec074d8cb8243976963674dd40ffe7
FileHash-MD5	f34b72471a205c4eee5221ab9a349c55
FileHash-MD5	01d397df2a1cf1d4c8e3615b7064856c
FileHash-MD5	b484b0dff093f358897486b58266d069
FileHash-MD5	4f67f3e4a7509af1b2b1c6180a03b3e4
FileHash-MD5	d1d779314250fab284fd348888c2f955
FileHash-SHA1	c1a9044f180dc7d0c87e256c4b9356463f2cb7c6
FileHash-SHA1	71f1bf658e0adb69240546df2bb95005e7e70f33
FileHash-SHA1	157cfb98caa48c2adb3475305c88986e777d9aa3
FileHash-SHA1	43a7858a0564c500e7f248762353f5b1ec3f3ef8
FileHash-SHA1	e8b58b9db83b4902a607559301f6985763d2647a
FileHash-SHA1	a0ebe36c61d4de405fe531ecf013720a3d56d5a1
FileHash-SHA1	810c7f2c3d045b7c755fb29646297a221cff163f
FileHash-SHA1	51b9d982abf1d866ed4e86e63dfee548c2f5a3fd
FileHash-SHA1	1c9a437ed876a0ce0e5374bd93acdfd9e9023f1f
FileHash-SHA1	a20ef335481c2b3a942df1879fca7762f2c69704
YARA	32fda75483f01579b78607113799a19382d72f4d
YARA	bbea5a6a1e6ad2446f2dc23414fbf0ca6dc834f6
YARA	b9d1e879e11d6ce46fa206879cb516d74e024b5e
YARA	ace0684fa59024586a396bfd428af8fc5521494e
FileHash-SHA256	9a776b895e93926e2a758c09e341accb9333edc1243d216a5e53f47c6043c852
FileHash-SHA256	c6930e298bba86c01d0fe2c8262c46b4fce97c6c5037a193904cfc634246fbec
FileHash-SHA256	129b8825eaf61dcc2321aad7b84632233fa4bbc7e24bdf123b507157353930f0
FileHash-SHA256	a917c1cc198cf36c0f2f6c24652e5c2e94e28d963b128d54f00144d216b2d118
FileHash-SHA256	32a4de070ca005d35a88503717157b0dc3f2e8da76ffd618fca6563aec9c81f8
FileHash-SHA256	f3ca8f15ca582dd486bd78fd57c2f4d7b958163542561606bebd250c827022de
FileHash-SHA256	8cad61422d032119219f465331308c5a61e21c9a3a431b88e1f8b25129b7e2a1
FileHash-SHA256	aca598e2c619424077ef8043cb4284729045d296ce95414c83ed70985c892c83
FileHash-SHA256	5cb7a352535b447609849e20aec18c84d8b58e377d9c6365eafb45cdb7ef949b
FileHash-SHA256	9ea5aa00e0a738b74066c61b1d35331170a9e0a84df1cc6cef58fd46a8ec5a2e
FileHash-SHA256	efd470cfa90b918e5d558e5c8c3821343af06eedfd484dfeb20c4605f9bdc30e
FileHash-MD5	3122b0130f5135b6f76fca99609d5cbe
FileHash-MD5	d45931632ed9e11476325189ccb6b530
FileHash-MD5	889e320cf66520485e1a0475107d7419
FileHash-MD5	c4141ee8e9594511f528862519480d36
FileHash-MD5	a2b1a45a242cee03fab0bedb2e460587

FileHash-MD5	97aaf130cfa251e5207ea74b2558293d
FileHash-MD5	acd15f4393e96fe5eb920727dc083aed
FileHash-MD5	34404a3fb9804977c6ab86cb991fb130
FileHash-MD5	40e698f961eb796728a57ddf81f52b9a
FileHash-MD5	bda82f0d9e2cb7996d2eefdd1e5b41c4
FileHash-MD5	dfd09e91b7f86a984f8687ed6033af9d
FileHash-SHA1	f5fc9d893ae99f97e43adcef49801782daced2d7
FileHash-SHA1	9ff715209d99d2e74e64f9db894c114a8d13229a
FileHash-SHA1	c92529097cad8996f3a3c8eb34b56273c29bdce5
FileHash-SHA1	b345e6fae155bfaf79c67b38cf488bb17d5be56d
FileHash-SHA1	2b22d9c673d031dfd07986906184e1d31908cea1
FileHash-SHA1	081d5bd155916f8a7236c1ea2148513c0c2c9a33
FileHash-SHA1	c7e7dd96fefca77bb1097aeeefef126d597126bd
FileHash-SHA1	50b4f9a8fa6803f0aabb6fd9374244af40c2ba4c
FileHash-SHA1	ce6bc34b887d60f6d416a05d5346504c54cff030

ব্যাংকে সাইবার আক্রমণের চেষ্টা প্রতিরোধ (দৈনিক বাংলাদেশ প্রতিদিন)

আর্টিকেল প্রকাশ – ৯ই সেপ্টেম্বর, ২০২০।

বাংলাদেশের ব্যাংকগুলোতে সাইবার আক্রমণের চেষ্টা প্রতিরোধ করা হয়েছে। সম্প্রতি বিগল বয়েজ নামে একটি সাইবার হ্যাকার গ্রুপ আক্রমণের চেষ্টা করে। পরে বাংলাদেশ ব্যাংক এ বিষয়ে সব প্রতিষ্ঠানকে সতর্ক করে চিঠি দেয়। এই আক্রমণের চেষ্টা বাংলাদেশ সরকারের কম্পিউটার ইনসিডেন্ড রেসপন্স টিম-সার্ট প্রতিরোধ করে দিয়েছে।

আমরা জনগণের পক্ষে বাংলাদেশ প্রতিদিন

প্রতিষ্ঠানটির প্রকল্প পরিচালক তারেক এম বরকতউল্লাহ গণমাধ্যমকে জানিয়েছেন, একটি হ্যাকার গ্রুপ জালিয়াতি করে অর্থ স্থানান্তর এবং এটিএম থেকে নগদ অর্থ সরানোর লক্ষ্যে বিশ্বজুড়ে ব্যাংকগুলোতে সাইবার হামলা চালাচ্ছে বলে সম্প্রতি সতর্ক করেছিল যুক্তরাষ্ট্র। 'বিগল বয়েজ' হ্যাকার গ্রুপ সাইবার হামলার যে চেষ্টা করেছিল, তা ব্যর্থ হয়েছে। দেশের তিনটি ইন্টারনেট সেবাদাতা প্রতিষ্ঠানের নেটওয়ার্কে হ্যাকার গ্রুপটির ম্যালওয়ারের অস্তিত্ব পাওয়া গিয়েছিল। হামলাকারীদের লক্ষ্য ছিল মূলত ব্যাংক। বাংলাদেশ ব্যাংকের নির্বাহী পরিচালক সিরাজুল ইসলাম বাংলাদেশ প্রতিদিনকে বলেন, সাইবার আক্রমণের বিষয়ে বাংলাদেশ ব্যাংকের নজরে কিছু পড়েনি। তবে কম্পিউটার কাউন্সিল থেকে আমাদের এ বিষয়ে সতর্ক থাকার জন্য বলা হয়েছিল। সে অনুযায়ী আমরা ব্যাংকগুলোকে সতর্ক করেছি।

'Danger is over': Bangladesh 'thwarts' cyber-heist bid by North Korean hackers (bdnwes24.com)

Published: 09 Sep 2020

Bangladesh has blocked a bid to steal money from banks through cyber-attacks by a North Korean group of hackers called the "BeagleBoyz", says the head of the government's Computer Incident Response Team or CIRT. "There is nothing to be afraid of now. The danger is over," said Tarique M Barkaullah, who directs the CIRT.

bdnews24.com Bangladesh's First Internet Newspaper

The US had recently alerted the banks around the world that the North Korean hackers were trying to steal money through transfers and cash withdrawals from ATMs.

Later, when the Bangladesh Bank warned about the risk of cyber-attacks, the banks limited online transactions in a move to ward off the threats.

Malware of "BeagleBoyz" had been found in three internet networks in Bangladesh, Barkatullah told bdnews24.com on Tuesday.

"The attackers mainly targeted the banks through the ISP networks. It has caused panic among the bankers," he said.

The hackers could not steal money from the banks because the bankers took "proper" cautionary steps under the supervision of Bangladesh Telecommunication Regulatory Commission, the CIRT director said.

সাইবার নিরাপত্তায় বিডিসার্ট (দৈনিক সমকাল)

আর্টিকেল প্রকাশ – ১৪ই সেপ্টেম্বর, ২০২০।

সমকাল টেকলাইফ

দেশের গুরুত্বপূর্ণ অবকাঠামোগুলোর সাইবার নিরাপত্তায় গবেষণা, সমস্যার তাৎক্ষণিক ব্যবস্থা গ্রহণ ও দিকনির্দেশনার মাধ্যমে সাইবার নিরাপত্তা বিধানে কাজ করে যাচ্ছে তথ্য ও যোগাযোগ প্রযুক্তি বিভাগ। সাইবার নিরাপত্তা নিশ্চিত করতে স্থাপন করা হয়েছে বিজিডি ই-গভর্নমেন্ট কম্পিউটার ইনসিডেন্স রেসপন্স টিম (সার্ট)।

বিশ্বের সঙ্গে তাল মিলিয়ে ডিজিটাল দেশ রূপান্তরের পথে এগিয়ে যাচ্ছে বাংলাদেশ। প্রতিটি সেক্টরই অনলাইন সেবার আওতায় আসছে। ডিজিটাইজেশনের পরিধি বাড়ার সঙ্গে সাইবার ক্রাইমের ঝুঁকিও বাড়ছে। সাইবার নিরাপত্তা যতই হুমকির সম্মুখীন হচ্ছে, ততই নিরাপত্তা জোরদার করতে উঠেপড়ে লেগেছে সংস্থাগুলো। বিশ্বজুড়ে অনন্য এক আলোচিত বিষয় এখন সাইবার ক্রাইম। সেই ক্রাইম সম্পর্কে সাইবার নিরাপত্তা গবেষকরা সবাইকে সতর্ক করার পরও কোনো কোনো ব্যক্তি ও প্রতিষ্ঠান নিজেকে রক্ষা করতে পারছেন না। সাম্প্রতিক বছরগুলোতে বিশ্বে অনেক প্রতিষ্ঠান সাইবার হামলার সম্মুখীন হয়েছে। গত মাসেই উত্তর কোরিয়ার একটি হ্যাকার গ্রুপের বাংলাদেশের ব্যাংকগুলোর ওপর নতুন করে সাইবার হামলার আশঙ্কায় সতর্কতা জারি করে কেন্দ্রীয় ব্যাংক। এর ফলে অনেক ব্যাংক অনলাইন ব্যাংকিং সেবা ও টাকা উত্তোলন সীমিত করেছিল। পূর্ব সতর্কতার ফলে এ যাত্রায় হামলার ঝুঁকি কমিয়ে আনা সম্ভব হয়েছে। শুধু আর্থিক প্রতিষ্ঠান নয়, জাতীয় তথ্যভাণ্ডার, আইনশৃঙ্খলা রক্ষাকারী বাহিনী, গুরুত্বপূর্ণ অবকাঠামোগুলোতে সাইবার নিরাপত্তা ত্রুটি দেখা দিলে গবেষণা, সমস্যার তাৎক্ষণিক ব্যবস্থা গ্রহণ ও দিকনির্দেশনার মাধ্যমে সাইবার নিরাপত্তা বিধানে নিরলসভাবে কাজ করে যাচ্ছে আইসিটি বিভাগ। এ বিভাগ থেকে সাইবার নিরাপত্তা বিধানের জন্য স্থাপন করা হয়েছে BGD e-GOV CIRT নামে কম্পিউটার ইনসিডেন্স রেসপন্স টিম।

সার্ট প্রজেক্ট পরিচালক (অপারেশন) তারেক এম বরকতউল্লাহ বলেন, বাংলাদেশ সরকারের অনলাইন সেবা ও কার্যক্রমের পরিধি অনেক বৃদ্ধি পেয়েছে। ডিজিটাল বাংলাদেশ পরিকল্পনার বাস্তবায়ন এবং জনগণের দোরগোড়ায় ডিজিটাল সেবা পৌঁছে দিতে কাজ করছে সরকার। বাংলাদেশ ব্যাংকে হ্যাকিং আক্রমণের পরই মূলত সাইবার সিকিউরিটির বিষয়টি তাৎপর্যপূর্ণ হয়ে ওঠে। আমরা গুরুত্বপূর্ণ অবকাঠামোর তথ্য নিরাপত্তার জন্য কাজ করছি। অভ্যন্তরীণ ও আন্তর্জাতিক সাহায্য সহযোগিতার ভিত্তিতে সাইবার নিরাপত্তার জন্য আমাদের অপারেশন টিম নিরলস কাজ করে যাচ্ছে। সার্টের যাত্রা সম্পর্কে তিনি বলেন, এক দিনে এ রকম সার্ট তৈরি করা সম্ভব নয়। ধীরে ধীরে কাজ ও অভিজ্ঞতা অর্জন করে এগোতে হয়েছে। আমাদের সবাই প্রশিক্ষণপ্রাপ্ত এবং আন্তর্জাতিকভাবে স্বীকৃত। আমাদের কাজের মানও আন্তর্জাতিকভাবে সন্তোষজনক, কিন্তু সার্টের সক্ষমতা ও পরিসর বাড়াতে আরও লোকবল প্রয়োজন। হ্যাকিংয়ের ঘটনা দিন দিন বৃদ্ধি পাচ্ছে, ফলে আমাদের আরও সক্ষমতা ও প্রতিরোধ শক্তি বাড়াতে হবে। বর্তমানে

আমরা শুধু ঢাকাভিত্তিক মনিটর করছি। আশা করছি, আগামী বছর নাগাদ জেলা পর্যায়ে সরকারি কার্যক্রম মনিটর শুরু করতে পারব। এটা করা গেলে তৃণমূল পর্যায়ের কার্যক্রমে কোনো ভাইরাস, আক্রমণ আছে কিনা, তা মনিটরিং ও প্রয়োজনীয় ব্যবস্থা গ্রহণে সহায়তা করতে পারব। এখনও সীমিত আকারে কেন্দ্রীয়ভাবে কাজ করছি। আগামীতে এর পরিসর ও লোকবল বাড়ানো হবে। ইতোমধ্যে বিভিন্ন সরকারি সংস্থার সাত শতাধিক সদস্যকে প্রশিক্ষণ দেওয়া হয়েছে। ক্রমান্বয়ে শিক্ষিত তরুণ এবং যারা সাইবার নিরাপত্তা সংশ্লিষ্ট রয়েছেন, তাদেরও প্রশিক্ষণ দেওয়া হবে।

পুলিশ ক্লিয়ারেন্স সম্পর্কে প্রকল্পের সার্টিফাইং অথরিটি ম্যানেজার মীর মোহাম্মদ নাহিদুল হাসান বলেন, পুলিশ ক্লিয়ারেন্স নিয়ে অনেকেরই তিক্ত অভিজ্ঞতা রয়েছে। আগে কয়েকটি ধাপ পেরিয়ে যেখানে সেবাটি গ্রাহকের কাছে পৌঁছাতে প্রায় তিন সপ্তাহ লেগে যেত, তা এখন মাত্র তিন-চার দিনে দেওয়া সম্ভব হচ্ছে। আগামীতে আরও কম সময়ে সেবাটি দেওয়া যাবে।

সার্ট কী

কম্পিউটার ইনসিডেন্স রেসপন্স টিম (সার্ট) বাংলাদেশ সরকারের অধীনে কম্পিউটার সিকিউরিটি ইনসিডেন্টস, কার্যক্রম গ্রহণ, পর্যালোচনা, প্রতিক্রিয়া জানানোসহ আরও কিছু দায়িত্ব পালনকারী প্ল্যাটফর্ম। গুরুত্বপূর্ণ অবকাঠামোর তথ্য নিরাপত্তায় ত্রুটি দেখা দিলে গবেষণা, সমস্যার তাৎক্ষণিক ব্যবস্থা গ্রহণ ও দিকনির্দেশনা প্রদান করে। বাংলাদেশে সাইবার নিরাপত্তায় সরকারি বিভিন্ন ইউনিট, ক্রিটিক্যাল ইনফরমেশন ইনফ্রাস্ট্রাকচার, আর্থিক সংস্থা, আইন প্রয়োগকারী সংস্থা, অ্যাকাডেমিয়া ও সিভিল সোসাইটির সঙ্গে কাজ করছে। আন্তর্জাতিক সংগঠন এবং সাইবার নিরাপত্তা কমিউনিটির সঙ্গে একটি দৃঢ় সম্পর্ক বজায় রেখে আন্তর্জাতিক সাইবার ইস্যুতে বাংলাদেশ ফোকাল পয়েন্ট হিসেবে কাজ করে। বিশ্ব পরিমণ্ডলে পারস্পরিক সহযোগিতার মাধ্যমে সমস্যা সমাধানে কাজ করে থাকে।

সার্টের কী কাজ

সাইবার নিরাপত্তা বিধানের লক্ষ্যে সার্টের প্রাথমিক লক্ষ্য ও উদ্দেশ্য হলো ন্যাশনাল ডাটা সেন্টারের (এনডিসি) অবকাঠামো বজায় রাখা, এনডিসি স্থাপিত সেবাগুলোর নিরাপত্তা দুর্বলতা বা সাইবার ভালনারেবিলিটি খুঁজে বের এবং সতর্কবার্তা প্রদান করা। এ ছাড়া ন্যাশনাল ডাটা সেন্টারের নেটওয়ার্ক নিরাপত্তা সম্পর্কিত সন্দেহজনক কার্যকলাপ নিরীক্ষণ ও প্রয়োজনীয় ব্যবস্থা গ্রহণ, ন্যাশনাল ডাটা সেন্টারে স্থাপিত সেবা, পরিষেবাসমূহ যদি সাইবার নিরাপত্তাজনিত কারণে ক্ষতিগ্রস্ত বা বাধাগ্রস্ত হয়, তাহলে তা পুনরুদ্ধারে সহায়তা এবং নিয়ন্ত্রণ ব্যবস্থা গ্রহণ করে। অনুরোধের ভিত্তিতে এনডিসির বাইরে হোস্টিংকৃত সরকারের অন্য ওয়েবসাইটের নিরাপত্তা দুর্বলতাও খুঁজে সতর্কতামূলক ব্যবস্থা গ্রহণে পরামর্শ প্রদান করে এ টিম।

সাইবার হামলার সতর্কবার্তা

সার্ট বিশেষ সেন্সর ব্যবহার করে মনিটরিংয়ের মাধ্যমে গুরুত্বপূর্ণ নির্দিষ্ট ডাটা সেন্টারে কোনো অনাকাঙ্ক্ষিত কার্যক্রম লক্ষ্য করলে সতর্কতা ও পরবর্তী ব্যবস্থা গ্রহণ করে থাকে। যে সংকেত আমরা পাই, সে অনুযায়ী ব্যবস্থা গ্রহণ ও আন্তর্জাতিক সহযোগিতাও গ্রহণ করে। একাধিক ইউনিটের সমন্বয়ে কার্যক্রম পরিচালিত হয়। সার্ট টিম কোনো জটিল সমস্যার সমাধানে ব্যর্থ হলে আন্তর্জাতিক সহযোগিতা গ্রহণে সতর্কবার্তা প্রদান করে। সার্বিক সহযোগিতার ভিত্তি বিপদসংকেত পেলেই সাইবার নিরাপত্তা নিশ্চিতের ব্যবস্থা গ্রহণ করে।

সার্ট টিম

সাইবার সেন্সর, রিস্ক অ্যাসেসমেন্ট, আইটি অডিট, ইনসিডেন্ট হ্যান্ডলিং, ডিজিটাল ফরেনসিক ল্যাব, সাইবার জিম, অ্যাওয়ারনেস বিল্ডিং, সাইবার রেঞ্জ, সিআইআইএস এবং সাইবার থ্রেট ইন্টেলিজেন্স ইউনিট মিলে সার্ট টিম গঠিত। প্রতিটি বিভাগের কার্যক্রম নির্ধারিত থাকলেও একটি টিম হিসেবে পারস্পরিক কো-অর্ডিনেশনের মাধ্যমে পরিচালিত হয়। টিমের ৫২ জন প্রশিক্ষিত দক্ষ কর্মী নিরলসভাবে কাজ করে চলেছেন সাইবার নিরাপত্তা নিশ্চিতে।

সার্ট ল্যাবরেটরি ও সাইবার জিম

ডাটা পুনরুদ্ধার, ক্রাইম শনাক্তকরণ, কম্পিউটার নেটওয়ার্ক ট্রাফিক মনিটর ও বিশ্লেষণ করা হয় ল্যাবে। অপরাধের সংকেত, প্রমাণাদি সংগ্রহ, গবেষণা, তাৎক্ষণিক ব্যবস্থাসহ সাইবার নিরাপত্তাজনিত কার্যক্রম পরিচালিত হয় সুরক্ষিত গোপন ল্যাবে। কম্পিউটার ফরেনসিক, মোবাইল ফরেনসিক, ফরেনসিক সাপোর্ট সার্ভিস এবং ডিজিটাল ফরেনসিক প্রশিক্ষণ দেওয়া হয় এ ইউনিট থেকে। ক্রাইমের ধরন অনুযায়ী এককভাবে এবং প্রয়োজনে অন্য সংস্থার সঙ্গে সমন্বয় করে প্রশিক্ষণ ও কার্যক্রম পরিচালনা করা হয়।

আন্তর্জাতিক অঙ্গনে সার্ট

সাইবার নিরাপত্তা নিশ্চিত করা অত্যন্ত গুরুত্বপূর্ণ এবং জটিল কাজ হওয়ায় এককভাবে সব সমস্যা সমাধান সম্ভব হয় না। ভারত, নরওয়ে, পোল্যান্ডসহ বিশ্বের ২০টির অধিক সংস্থার সঙ্গে যুক্ত হয়ে পারস্পরিক সহযোগিতার ভিত্তিতে দেশে-বিদেশে সাইবার নিরাপত্তা নিয়ে কাজ করে সার্ট। আন্তর্জাতিক সংস্থা এবং সাইবার নিরাপত্তা কমিউনিটির সঙ্গে সমন্বয় ও সম্পর্ক বজায় রেখে আন্তর্জাতিক সাইবার ইস্যুতে বাংলাদেশ ফোকাল পয়েন্ট হিসেবে কাজ করে।

Cybersecurity monitoring and incident response teams are a must for every organisation and regulator

Dr Vilius Benetis, CEO of NRD Cyber Security.

Intro

Cyber-attacks are growing in scope and having harsher consequences: bigger money is stolen, information is encrypted and ransomed, business processes are stopped. Such cyber-attacks became more localized and adapted to specific technological vulnerabilities and human weaknesses. Cybercrime is evolving and will continue to grow, until we learn to deal with it, just as we do with physical crime. What methods and ways should be used to organize cybersecurity?

Cyberspace protection and responsibilities

First, we know that protection of all assets – physical and digital – is the responsibility of the owner and senior management of the organisation. Naturally, cybersecurity controls should be implemented for all IT systems. Cyber-attackers and cybercriminals are humans, or national governments - as have been observed in cybercrime in Bangladesh over recent years, incident response must be organized as well by humans using professional and internationally accepted methods of response, known as Computer Incident Response Team Services (CSIRT Services). The newest model from global association of incident response teams FIRST.org is presented below:

Specialized incident response centres and teams

Currently there are very few cybersecurity and globally recognised incident response teams professionally working in Bangladesh. For cybersecurity to work in the country, number of such teams over next 3 years should increase manyfold. Such teams typically are named CSIRT, Security Operation Center (SOC), Information Sharing and Analysis Center (ISAC), and similar.

Some of these teams will be created covering incident response and coordination needs in sectors, such as Banking, Insurance, Energy, Logistics, Aviation, Utilities. Some will be hosting consolidated resources of region – Dhaka City, Chittagong, etc. Most of them will be hosted inside organisations to handle cyber-attacks against own assets, and some – will be running as Managed Security Service Providers (MSSPs) – and will work as outsourced SOCs.

Bangladesh National CIRT along with BGD e-Gov CIRT are interested in such ecosystem of CSIRTs and SOCs to develop in the country, and for that reason over the last few years was organising seminars and events encouraging Banks, regulators, government organisations as well as private businesses to build CSIRTs and SOCs.

It is quite easy to build one by following these steps:

1. Assessment for Readiness;
2. Design;
3. Implementation;
4. Operations and Improvements.

First stage requires to clearly define mandate: authority and responsibilities of the CSIRT or SOC, build rapport with stakeholders, get commitment to approximate budget and roadmap.

Second and third stages are focused on designing and implementing mandate via services model, defining processes and procedures, working out organisational structure, skills, implementing technologies, tuning.

Such teams will require at least 1 year to become mature units. In this process experienced consultants could be involved if needed.

Each organization and sector are different and have their own needs and requirements for security. Hence, there is no 'one solution fits all' scenario in establishing CSIRT or SOC and factors, such as infrastructure, security team capacity, maturity and others should be considered in realising the true need. One way of understanding what size and composition team or centre the organization requires is to answer a series of questions. Below is an example of the different team composition variations we at NRD Cyber Security have developed based on most common practices we have seen in the field:

	Mini	Basic	Effective	Full Scale
Governance	• Mandate definition • FIRST.org membership • Roadmap & Strategy	• Mandate definition • FIRST.org membership • Roadmap & Strategy	• Mandate definition • FIRST.org membership • Roadmap & Strategy • Orgchart buildout	• Mandate definition • FIRST.org membership • Roadmap & Strategy • Orgchart buildout
People	• Featured CSIRT training • Limited remote support	• Relevant CSIRT training • Remote support • SOPs • Study mission tours	• Relevant CSIRT training • Remote support • SOPs • Study mission tours	• Relevant CSIRT training • On-site and remote support • SOPs • Study mission tours
Processes and services	• Incident handling service • Incident handling process	• Incident handling and outreach • Infrastructure support • Standard reporting	• Incident handling, outreach, digital forensics, vulnerability management • Process automation • Infrastructure support • Standard reporting	• Full scale CSIRT/SOC services • Process automation • Automated custom reporting • Maturity progress assessment • Infrastructure support
Measurements	• A few KPIs • No SLAs	• Basic KPIs • SLAs for processes	• KPIs system • SLAs for processes • SIM3 successful audit	• KPIs system • SLAs for services and automation • Annual reviews, SOC-CMM L3 C1.5
Technological Capability	• Incident registration and handling • PGP	• Incident registration and handling • Outreach and visualization portal • Internal support, PGP • Simple vulnerability assessment	• Incident detection and handling • Outreach and visualization portal • Internal support, PGP • Simple vulnerability assessment • Simple video wall • Simple threat intelligence • Simple digital forensics • Simple integration with ex. tooling • Situational awareness	• Incident detection and handling • Outreach and visualization portal • Internal support, PGP • Vulnerability assessment • Video wall • Threat intelligence • Digital Forensics • Integration with existing tooling • Situational awareness and EWS • Multi-site sensing at CII
Local resources	2-5 people	5-10 people	7-15 people	15-45 people
Duration	9 months	12 months	12-24 months	24-36 months

The signs of cybersecurity maturity

With the proliferation of advanced and high-risk cyber-attacks, sectoral cyber-incident response teams have begun to emerge around the world. Norwegians, South Koreans, Italians, Sri Lankans, French have set up dedicated CSIRTs for the Financial sector, and Poland has teams dedicated to both the Financial and Energy sectors. Egypt, Nigeria, Rwanda, Burundi, Uganda, India, Kenya, Kuwait and many other countries are currently developing their National Financial sector CSIRT services. The most common reasons for their creation are:

1) Willingness to accumulate, systematize and communicate sector-specific cybersecurity knowledge, information dissemination and

community in order to deal more effectively and quickly with specific cyber-attacks;

2) Willingness to adapt certain incident response processes and technologies, the development of resilience to sector-specific challenges, in particular the development of sectoral attacks;

3) Promoting good practices in sector-specific terminology and the application of common cybersecurity concepts such as responsible vulnerability detection, vulnerability management and common incident management exercises.

Most often, such sectoral cybersecurity centres are born in most sensitive and attacked sectors - the Financial sector, the Energy sector, the Health care system, the National Defence and certain Manufacturing sectors and Municipalities. The need often matures when it is understood that the processes, systems and protection of different sectors are unique. For example, security measures for hospital IT systems are different from online banking or ATMs. Cybersecurity works well when sectors are acting collectively: sharing information about cyber-attacks, best practices to protect their business processes and automation technologies.

Bangladesh National CIRT along with BGD e-Gov CIRT are interested in such ecosystem of CSIRTs and SOCs to develop in the country ..

Cyber Security support

For the past 5 years NRD Cyber Security has successfully been partnering with BCC to improve national cybersecurity capabilities in Bangladesh. NRD Cyber Security establishes cybersecurity capacity and enhances cyber resilience for nations and organizations. The company specializes in the establishment and modernization of cybersecurity teams and security operations centers as well as cyber threat intelligence and managed security services. Also, company's experts actively participate in international cybersecurity community, develop and improve methodologies for strengthening cyber resilience – FIRST.org CSIRT Services Framework, ITU CSIRT Establishment Framework, ENISA's Guidelines for CSIRT establishment.

Dr. Vilius Benetis is reachable on Linkedin or via NRD Bangladesh office to discuss CSIRT or SOC establishment concerns or sharing insights.

Securing your work place from cyber-attack and global best practices

Md. Sabbir Hossain, Risk Analyst
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

Recent cybercrime incidents have shown that even government networks are not safe from attack. In principle, these should be even better secured than normal company networks, but professional hackers have often managed to penetrate these systems in the past. The Bundestag was attacked in 2015. Companies are increasingly becoming the target of hackers against the backdrop of industrial espionage. The previous measures against these attacks are definitely not yet adequate and preventive. The aim of every company should be to act instead of react. In most cases, companies are rigorously surprised by attacks, if they even notice. Against this background, firewalls only help to protect one's own systems to a limited extent. Because, above all, complex infrastructures can only be protected with a great deal of security, a large number of measures and security-relevant technologies. The human factor also plays an important role. Most systems are connected to the Internet, where employees have to answer emails or open attachments.

Cyber-attacks are the de facto threat today. The increasing volume of data and the openness of the networks harbors dangers, because everyone uses smartphones, tablets, computers and other networked devices in everyday business. All of these devices are connected to the Internet and are therefore potential gateways for attackers to break into the entire company network. For the management level, the question arises: what threat scenarios are there, what damage can be expected to your own organization and how can companies protect themselves? With 220 million suspicious activities taking place on the networks every day, according to NATO, decision-makers often need even better information about the threat and the types of cyber-attacks.

At the moment, IT security has little perception in companies. The high degree of networking and the simultaneous exchange of company-critical data via the Internet offer cyber criminals greater potential than ever before. This is a big problem that companies have to adapt to today and in the future. Because, above all, data from the R&D, marketing, human resources and finance departments are in great demand. According to this, cyber criminals are particularly interested in customer and employee data, balance sheets or even access to bank accounts.

But what types of attacks do cyber criminals attempt to get into company systems? A list of the types of attacks is intended to give company decision-makers an overview of which attacks they should expect:

- Ransomware
- DDoS
- Phishing
- Botnet
- Insider Threat
- Malware
- APT etc.

These types of attack are defined by different attack vectors and type families with which cyber criminals attempt to break into company networks or infrastructures. These attack vectors are combinations of attack methods and techniques that a cybercriminal can use to gain access to IT systems.

These attack vectors include, for example, spam attempts that are sent by means of unwanted messages that are sent through targeted and untargeted via e-mail or other communication channels. In addition to unwanted advertising information, these messages primarily contain links to infected websites or attachments. Against this background, spam emails are also used for phishing attacks.

In addition to the common spam e-mails, cyber criminals try to locate weak points within the company's servers primarily with targeted attacks, because if systems are only equipped with inadequate firewalls, it is often easy for hackers.

Drive by exploit kits are also an important tool used by cyber criminals. With this attack vector, cyber criminals attempt to find security gaps on a computer by means of automated exploitation. Above all, users who are on a website are observed. Without further user interaction, the hacker tries to locate and exploit weak points in the web browser, in additional programs of the browser (plugins) or in the operating system of the user in order to implant malware unnoticed on the user's computer.

If your own company has been the victim of an attack, the specific extent of the damage depends to a large extent on the technical and organizational measures (TOMs) that have been taken to prevent the attack either preventively or detectively. Even if preventive measures could not prevent the attack, in the event of an attack detection measures and a quick response from the security organization can ensure that the damage is limited.

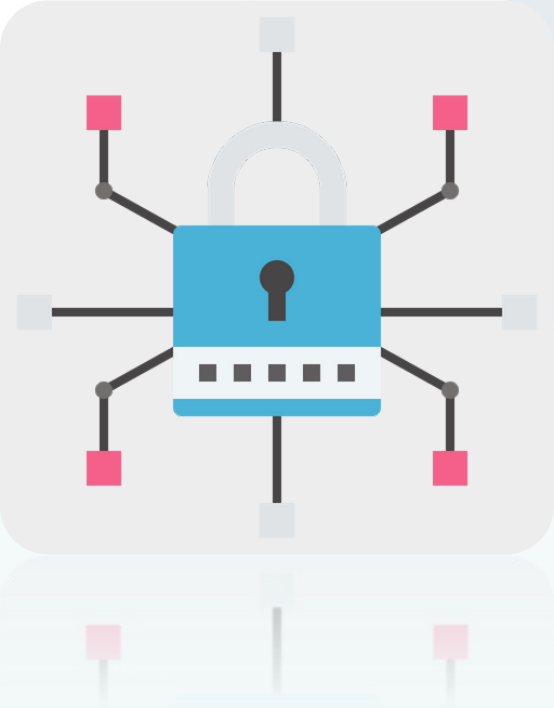
But what are the typical damages that companies can expect as a result of a cyber-attack?

In addition to the monetary aspects, in the form of compensation and damage to the company's image, industrial espionage is a major issue. Accordingly, this can be self-damage, in which the consequences of a cyber-attack mean the failure of production or services and thus high costs result from impairments or production interruptions.

In addition, damage to the company's image or reputation is a problem. In the event of an attack, companies often lose a good reputation with customers and may have to plan new budget for advertising campaigns in order to polish their image again.

As a rule, companies also have to pay compensation if they breached their legal or contractual obligations towards third parties as a result of an attack. These compensation payments can turn out to be very high, especially for systems and infrastructures that store a large amount of business-critical data.

The general best practices for companies include a large number of preventives, detective and reactive TOMs that know how to prevent infection from cyber-attacks or minimize the risk of attacks. These measures are particularly up-to-date given the number of targeted threat scenarios.



Preventive measures primarily serve to protect one's own systems and infrastructures from the attack vectors mentioned above. This includes protective measures for client systems that prohibit the execution of script files and guarantee protection on mail servers, through blocking or quarantine. In addition, various patch management applications that run on client systems can protect against drive-by attacks. The secure use of web servers also significantly reduces the attack surface.

In addition, preventive measures include sophisticated data security concepts and backups that still ensure the availability of the data in the event of an attack.

Raising employees' awareness plays another important role. Awareness can be created through training courses and campaigns and your own employees know how to take care of IT security and what to do in the event of a spam email or a social engineer attack.

In addition, secure administrator accounts, a precise definition of data types that may be stored on servers, and firewalls also serve to protect against infections.

In addition to preventive measures, detection measures (e.g. intrusion detection with automatic notification of the relevant people) may also be necessary in order to, in the event of an attack, evaluate log data that can determine the size of the attack and also identify ways in which these attacks are the company arrived.

Regular network monitoring can also check the interfaces between the server and the gateway and block possible attacks.

However, in the event of an attack that circumvented all preventive measures, the security organization should act quickly. These can be various technologies, the primary goal of which is to prevent damage, to guarantee the isolation of the infrastructures and systems and to ensure normal operation. It should be noted that a combination of preventive and reactive measures ensure that the attacked systems withstand. So no “either / or decision” - but only through this combination a high level of security arises within the company, which detects attacks and reacts quickly in the event of an attack in which preventive measures have been circumvented and tries to neutralize

attacks and also quickly generates a report / Can send log to your own security organization These technologies can be:

- Identity Access Management
- Antivirus
- Anti-malware and spyware
- Intrusion detection and prevention
- Next generation firewall
- Security information and event management
- Mobile device management
- Vulnerability Management
- Web application firewall
- DDoS protection
- Device control
- Data loss prevention
- Encryption
- Anti-spam
- Web filtering

Another measure against cyber-attacks can also be as a company to commission the hackers to attack their systems. The aim of the company's own hackers is to find the gaps in the systems before others can exploit them. Various service providers offer their resources in this context and support companies in closing the security gaps. For years, many companies lacked the awareness and competence to react appropriately to the threat from the Internet.

A large number of IT decision-makers and CISOs do not yet know which strategy is the right one to counter cyberattacks or which measures and technologies are to be used against them. In order to advance the mindset and the IT security concept in the company, IT security and data protection should be practiced from the ground up and the risk of cyber-attacks should be minimized at every workplace and taken into account in the system design. Whenever new systems are built, think about security and data protection right from the start (security by design, privacy by design). Thus, infrastructures are given a certain security impact from the ground up. Against this background, external service providers in particular can support companies with their expertise and stand by as sparring partners.

Writer Bio: A security professional with over 9 years of experience in security consultation, security design, Framework Design, Policy Making, project development and execution, integration of various technologies, lawful interception system, OSINT, Digital Forensics, Cell interrogation & active tracking system, critical infrastructure security, tactical & intelligence solutions. He is currently employed in BGD e-GOV CIRT (Bangladesh National CERT) as well as pursuing his Masters Degree from University of Ottawa.

জিমেইল এ টু-স্টেপ ভেরিফিকেশন (2-Step Verification) চালু করবেন কিভাবে

Mohammad Ariful Islam, Information Security Specialist
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

ইমেইল ব্যবহার করে দ্রুততম সময়ের মধ্যে আমরা গুরত্বপূর্ণ তথ্য একে অপরের কাছে পৌছে দিতে পারি। শুধু তথ্যই নয়, ইমেইল একাউন্ট ব্যবহার করে আমরা বিভিন্ন সোস্যাল মিডিয়াতে (যেমনঃ ফেসবুক, টুইটার, লিংকডইন ইত্যাদি) একাউন্ট তৈরি ও ব্যবহার করি। পরবর্তীতে যদি কেউ সোস্যাল মিডিয়ার পাসওয়ার্ড ভুলে যায় তবে যে ইমেইল আইডি ব্যবহার করে একাউন্ট খোলা হয়েছিলো সেখানে পাসওয়ার্ড পরিবর্তন করার লিংক পাঠানো হয়। এই লিংকের মাধ্যমে নতুন পাসওয়ার্ড সেট করা যায়।

বিশ্বব্যাপী সাইবার আক্রমণ দিন দিন বেড়েই চলেছে। ডিজিটাল প্লাটফর্ম এ কাজের ক্ষেত্রে সাবধানতা অবলম্বন না করলে আমরাও সাইবার আক্রমণের শিকার হতে পারি। তাই ইমেইল একাউন্টে শুধু পাসওয়ার্ড ব্যবহার করেই নিরাপত্তা নিশ্চিত করা যাবে না। এর সাথে দ্বিতীয় স্তরের নিরাপত্তা হিসেবে ২-স্টেপ ভেরিফিকেশন চালু করতে হবে।

টু-স্টেপ ভেরিফিকেশন চালু করে ইমেইল একাউন্টে প্রবেশের জন্য পাসওয়ার্ডের দেয়ার পর দ্বিতীয় স্তরের নিরাপত্তার অংশ হিসেবে আপনার কাছে ভেরিফিকেশন কোড (verification code) পাঠানো হবে। এই কোড ব্যবহার করে আপনি সফলভাবে আপনার একাউন্টে লগইন করতে পারবেন। এই ভেরিফিকেশন কোড আপনার মোবাইলে পাঠানো হতে পারে অথবা আপনি যদি কোন অথেনটিকেটর অ্যাপ (Authenticator app) ব্যবহার করেন তাহলে সেই অ্যাপ থেকে কোড নিয়ে ব্যবহার করতে পারেন।

টু-স্টেপ ভেরিফিকেশন চালু করার জন্য বেশ কয়েকটি অপশন আছে। এর মধ্যে বহুল ব্যবহৃত হচ্ছে ভয়েস অথবা টেক্সট মেসেজ (Voice or text message) এর মাধ্যমে ২-স্টেপ ভেরিফিকেশন। এই অপশন চালু করলে আপনার মোবাইল নম্বরে ভেরিফিকেশন কোড পাঠানো হবে। এই ভেরিফিকেশন কোড ব্যবহার করে আপনি একাউন্টে লগইন করতে পারবেন।

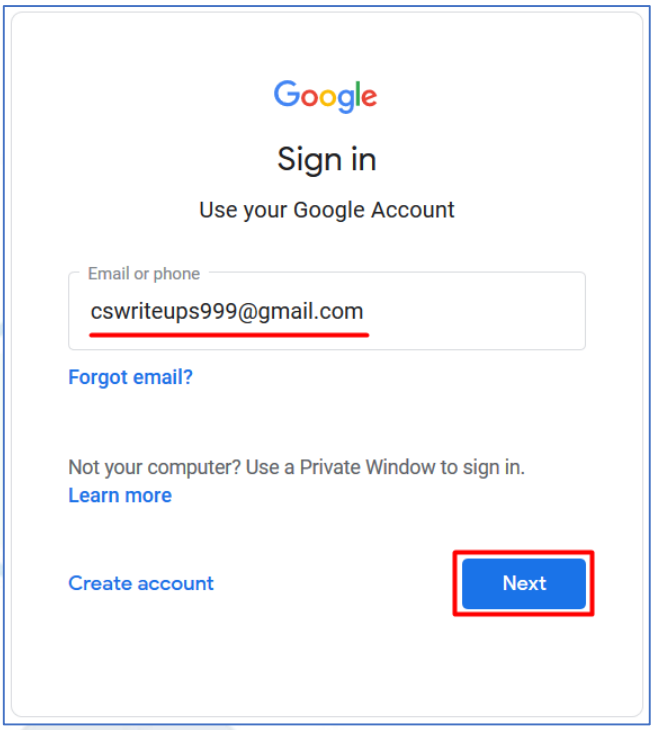
গুগলের জনপ্রিয় ইমেইল সেবা জিমেইল এ কিভাবে ভয়েস অথবা টেক্সট মেসেজ (Voice or text message) এর মাধ্যমে টু-স্টেপ ভেরিফিকেশন চালু করবেন সে বিষয়ে বিস্তারিত ধাপে ধাপে আলোচনা করা হলো।

ধাপ ১

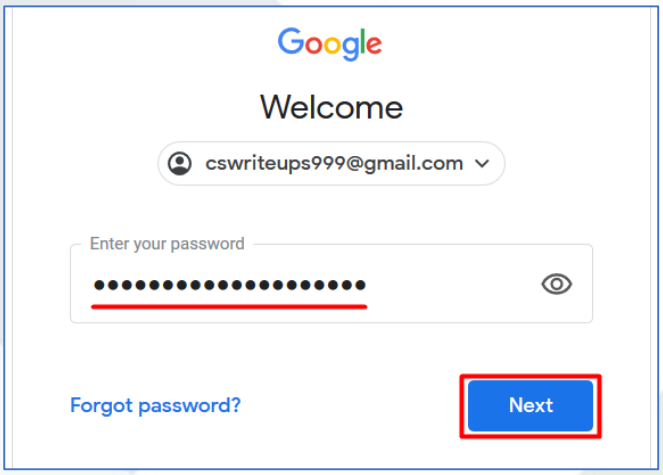
১.১ যে একাউন্টে টু-স্টেপ ভেরিফিকেশন চালু করবেন তাতে লগইন করুন। লগইন করতে নিম্নের লিংক ভিজিট করুন।

https://accounts.google.com

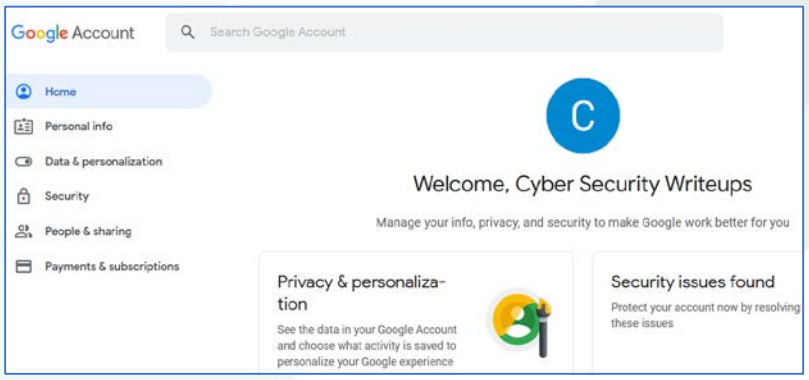
১.২ একাউন্টের নাম লিখে Next ক্লিক করুন।



এরপর পাসওয়ার্ড টাইপ করে Next ক্লিক করুন।



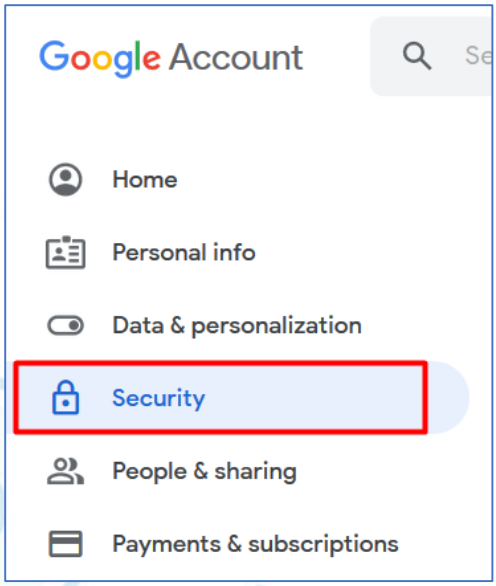
সফলভাবে লগইন হলে এই পেইজ দেখতে পাবেন। এখান থেকে আপনার একাউন্টের সুরক্ষা প্রদান, তথ্য পরিবর্তন এবং একাউন্ট সম্পর্কিত আরও অন্যান্য কাজ করতে পারবেন।

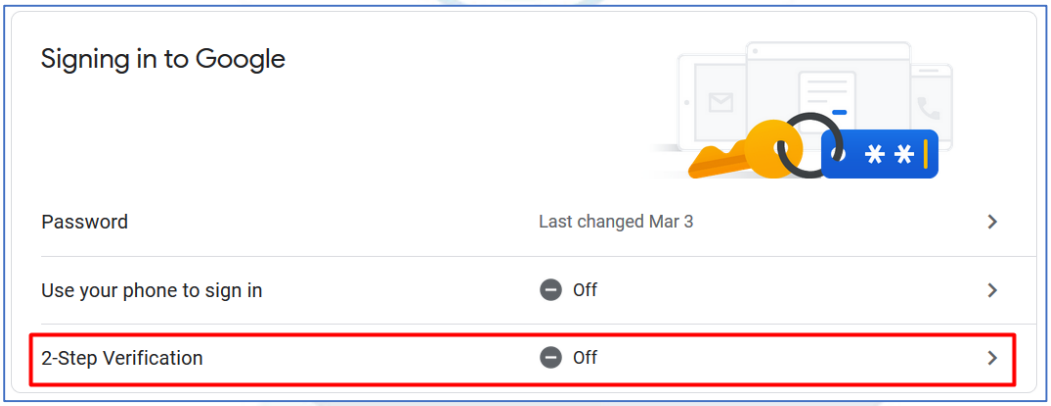


ধাপ ২

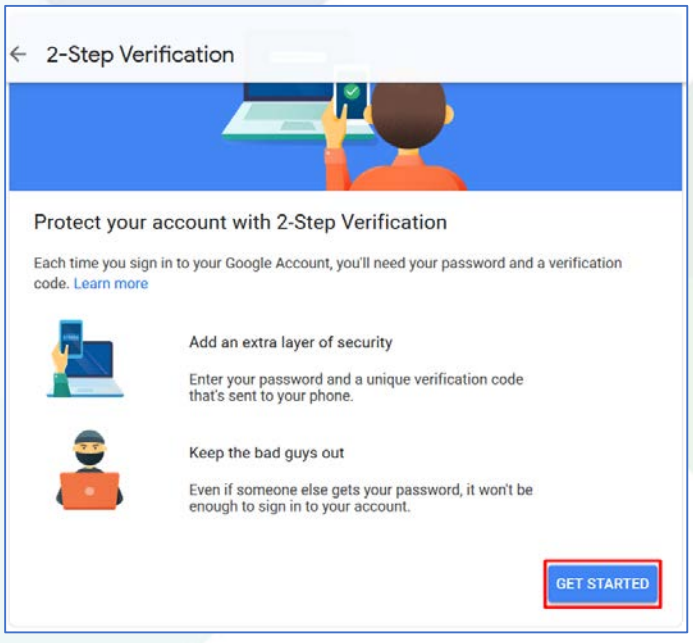
২.১ টু-স্টেপ ভেরিফিকেশন চালু করতে Security মেনুতে ক্লিক করুন।

১.২ এরপর 2-Step Verification এ ক্লিক করুন।





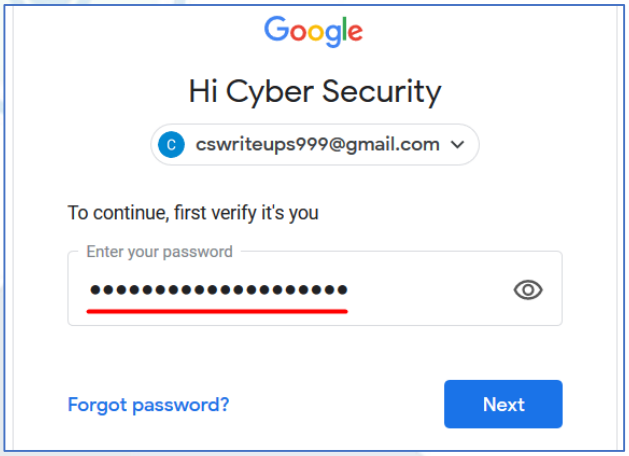
এই পেইজে টু-স্টেপ ভেরিফিকেশন সম্পর্কে জানতে পারবেন। GET STARTED এ ক্লিক করুন।



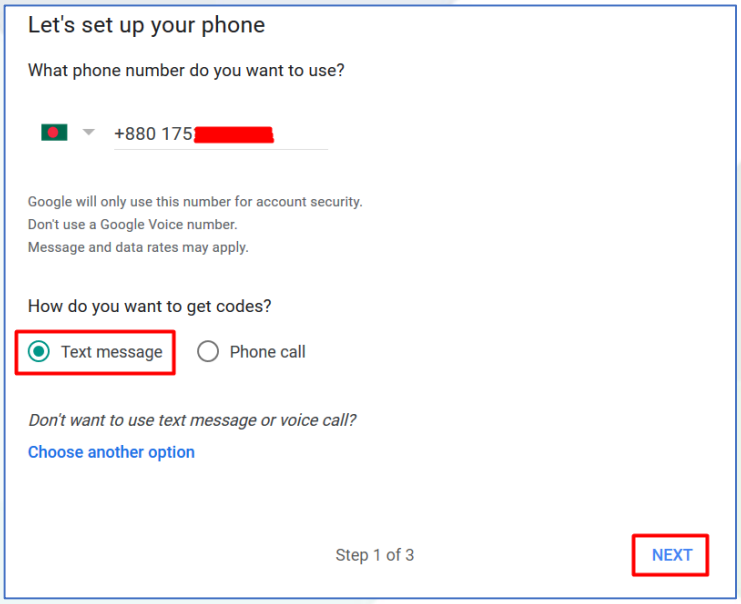
যেহেতু টু-স্টেপ ভেরিফিকেশন আপনার একাউন্টের অধিকতর নিরাপত্তা নিশ্চিত করে তাই এ পর্যায়ে পুনরায় ইমেইলের পাসওয়ার্ড দিতে হবে। একাউন্টের ব্যবহারকারী আসল কিনা তা পরীক্ষা করার জন্যই গুগল দ্বিতীয়বার পাসওয়ার্ড চায়।

অনেক ক্ষেত্রে ব্যবহারকারীরা তাদের কম্পিউটারে জিমেইল একাউন্ট ব্রাউজারে খুলে রাখে। সাইবার অপরাধীরা যাতে ব্যবহারকারীর একাউন্টের নিয়ন্ত্রণ (যেমনঃ পাসওয়ার্ড পরিবর্তন, টু-স্টেপ ভেরিফিকেশন চালু ইত্যাদি) নিতে না পারে তার জন্যই এই সুরক্ষা ব্যবস্থা।

পুনরায় ইমেইলের পাসওয়ার্ড লিখে Next এ ক্লিক করুন।

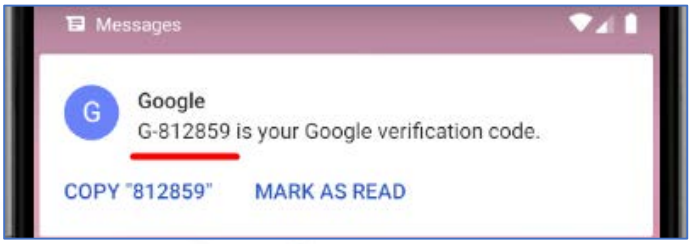


এখানে আমরা মোবাইল ফোনের ভয়েস অথবা টেক্সট মেসেজ (Voice or text message) এর মাধ্যমে এই টু-স্টেপ ভেরিফিকেশন চালু করবো। এখন যে মোবাইল নম্বরে আপনি ভেরিফিকেশন কোড পেতে চান সেই মোবাইল নম্বর লিখতে হবে।

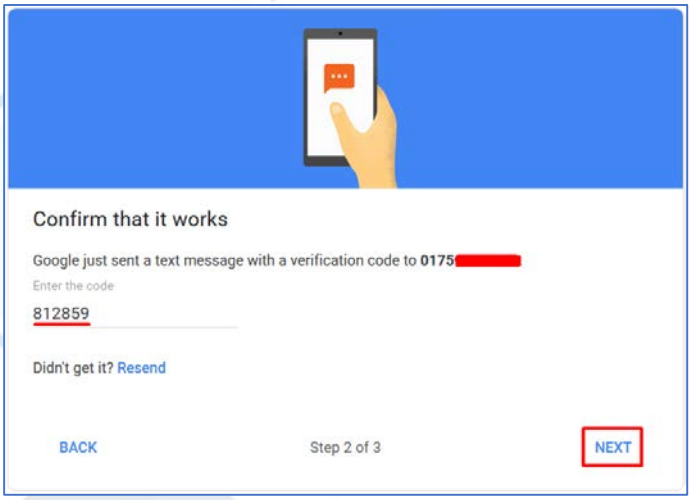


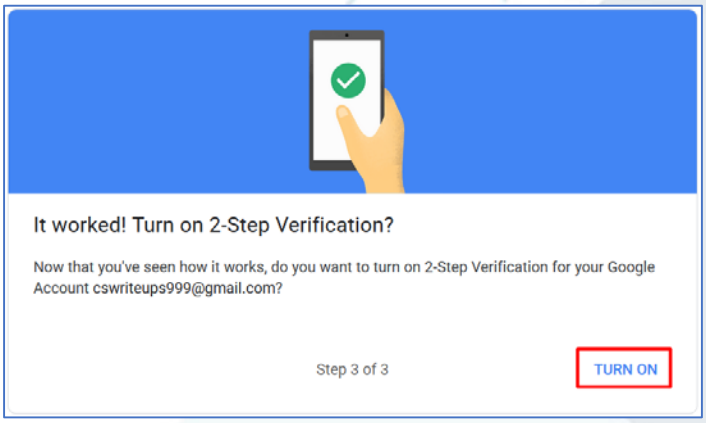
প্রথমে দেশ নির্বাচন করুন এবং মোবাইল নম্বর লিখুন। এরপর Text message নির্বাচন করে Next এ ক্লিক করুন।

গুগল থেকে আপনার মোবাইলে একটি ভেরিফিকেশন কোড এসএমএস (SMS) এর মাধ্যমে পাঠানো হবে।



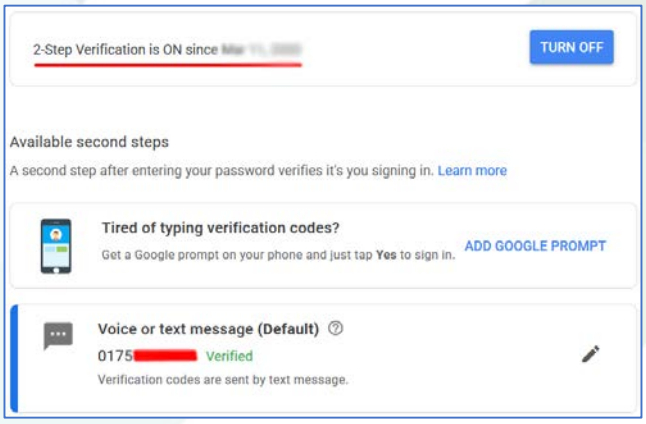
উক্ত ভেরিফিকেশন কোড লিখে Next এ ক্লিক করুন।





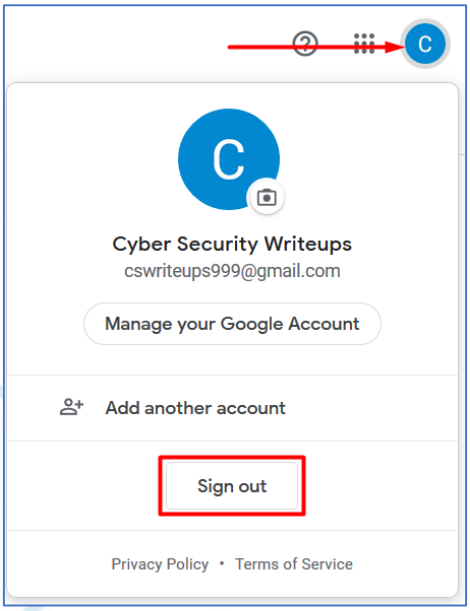
ভেরিফিকেশন কোড সঠিক হলে আপনি নিম্নোক্ত পেইজ দেখতে পাবেন যেখানে জানতে চাওয়া হবে আপনি টু-স্টেপ ভেরিফিকেশন চালু করতে চান কিনা? চালু করতে TURN ON এ ক্লিক

আপনার একাউন্টে টু-স্টেপ ভেরিফিকেশন চালু আছে। এখন থেকে একাউন্টে পাসওয়ার্ড দিয়ে লগইন এর সময় আপনার মোবাইলে একটি ভেরিফিকেশন কোড পাঠানো হবে এবং ভেরিফিকেশন সফল হলেই কেবল আপনি একাউন্টে প্রবেশ করতে পারবেন।

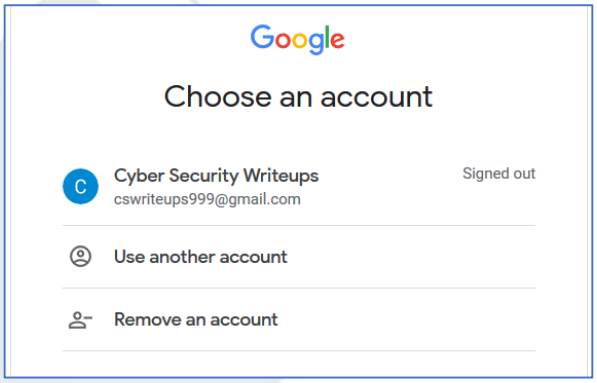


ধাপ ৩

একাউন্ট থেকে সাইন আউট (Sign out) করুন। সাইন আউট করতে প্রথমে নির্দেশিত আইকনে ক্লিক করুন এবং তারপর Sign out এ ক্লিক করুন।

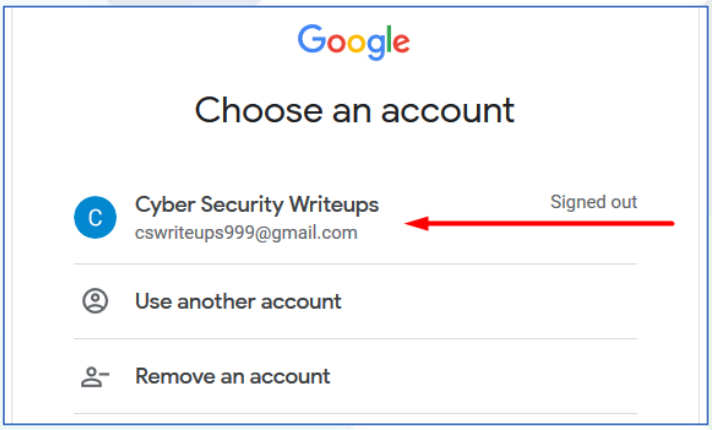


Sign out এ ক্লিক করলে নিচের পেইজটি দেখতে পাবেন।

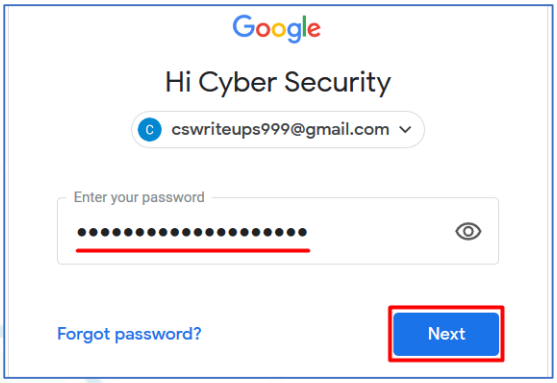


ধাপ ৪

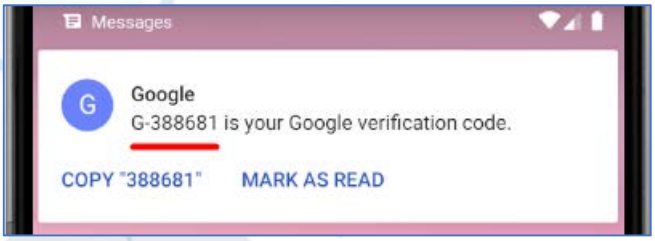
টু-স্টেপ ভেরিফিকেশন পরীক্ষা করার জন্য পুনরায় একাউন্টে লগইন করুন। লগইন করতে আপনার একাউন্টে ক্লিক করুন।



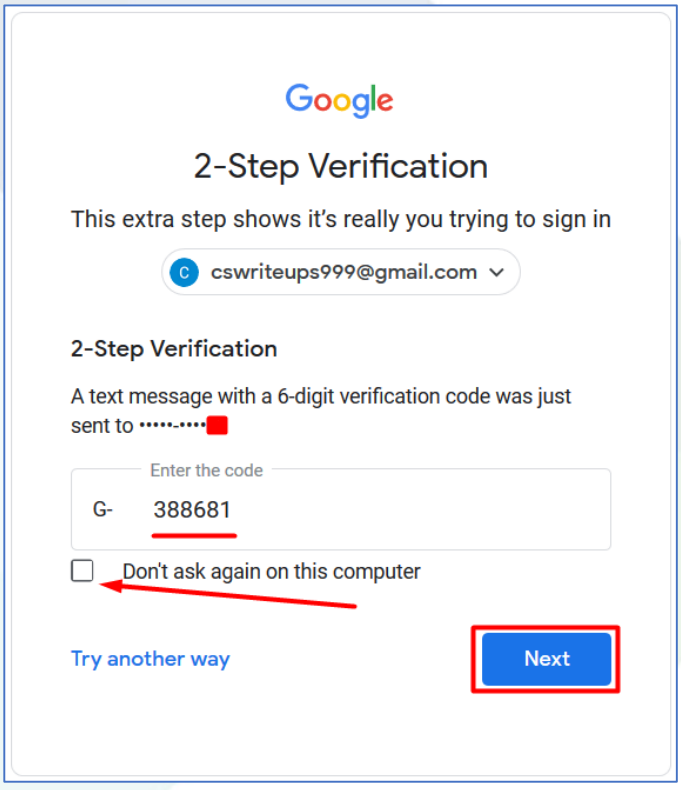
এরপর পাসওয়ার্ড টাইপ করে Next ক্লিক করুন।



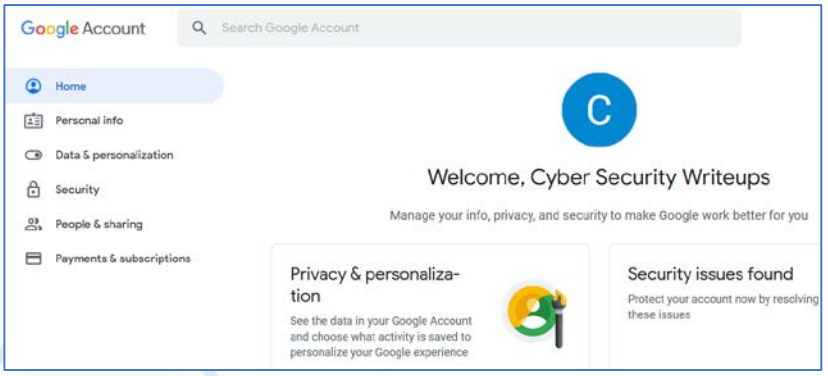
গুগল হতে আপনি আপনার মোবাইলে ভেরিফিকেশন কোড পাবেন।



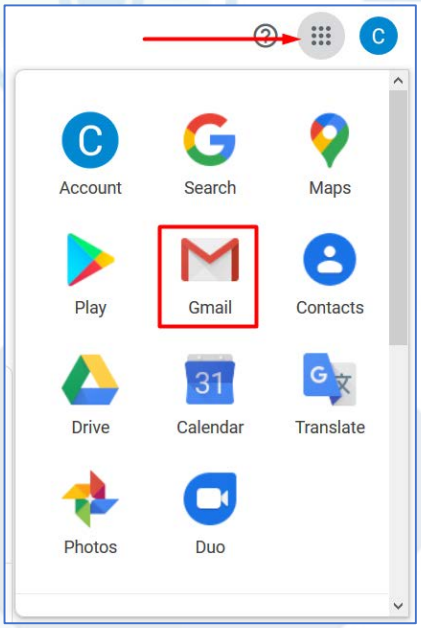
গুগল হতে আপনার মোবাইলে যে ভেরিফিকেশন কোড পাঠানো হয়েছে তা লিখে Next এ ক্লিক করুন। Don't ask again on this computer চেক বক্সে টিক চিহ্ন দেয়া থাকলে তা আনচেক (uncheck) করুন। যদি আপনি এই বক্সে টিক চিহ্ন সহ Next ক্লিক করেন তাহলে এই একাউন্টের জন্য এই কম্পিউটারে পরবর্তীতে টু-স্টেপ ভেরিফিকেশন চাইবে না। শুধু পাসওয়ার্ড দিলেই একাউন্টে লগইন করা যাবে।



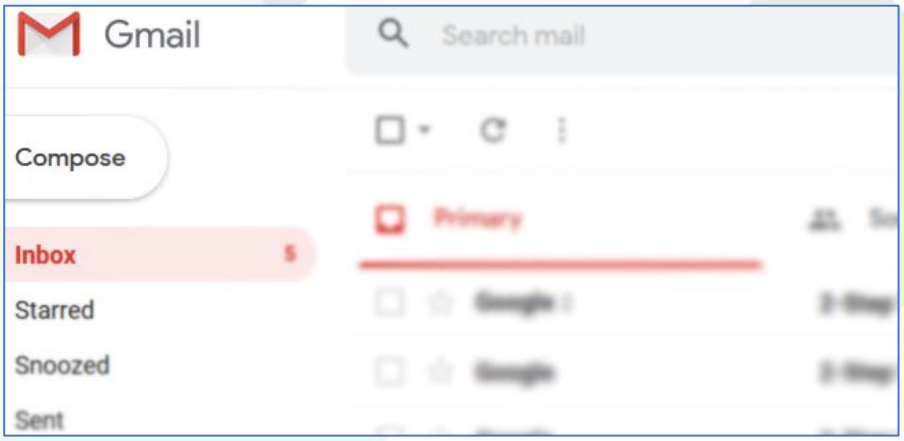
সফলভাবে লগইন হলে নিম্নোক্ত পেইজ দেখতে পাবেন।



জিমেইল এ প্রবেশ করতে নির্দেশিত আইকনে ক্লিক করে Gmail এ ক্লিক করুন।



জিমেইল এ প্রবেশ করলে আপনি আপনার ইমেইলসমূহ দেখতে পাবেন।



এছাড়াও আপনি নিচের লিংক ব্যবহার করে সরাসরি জিমেইল এ লগইন করতে পারবেন।

https://mail.google.com

সাইবার আক্রমণ হতে নিরাপদ থাকতে সতর্কতা স্বরুপ আপনার ইমেইল একাউন্টের পাসওয়ার্ড নিয়মিত বিরতিতে পরিবর্তন করুন এবং প্রতিবার ভিন্ন ভিন্ন পাসওয়ার্ড সেট করুন।

বিজিডি ই-গভ সার্ট

Simplifying PCI DSS (Payment Card Industry Data Security Standard)

Muhammad Moinul Hossain, IT Auditor
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

Foreword

The aim of this write-up is to assist organizations that store, process, communicate or otherwise handle credit or debit card data in understanding; how the PCI DSS applies to them; and what the requirements of the standard are. One of the myth about PCIDSS "PCI DSS is too hard". Understanding and implementing the 12 requirements of PCI DSS can seem daunting; especially for merchants without a large security or IT department. However, PCI DSS mostly calls for good, basic security. Even if there was no requirement for PCI DSS compliance, the best practices for security contained in the standard are steps that every business would want to take anyway to protect sensitive data and continuity of operations.

Here, basics of PCIDSS requirements and highlighting of few those requirements are now a days followed by most small, medium or large IT organization or business organizations.

Write-up objectives

- Highlighted few important requirements to understand the framework more easily.
- Typical payment card risks faced by organizations and basic knowledge to address few basic risk.
- Golden rules for protecting cardholder data.
- Scope and structure of the PCI DSS.
- The importance of segmenting the CDE (Cardholder Data Environment).
- The 12 high level requirements of PCI DSS.
- Interfacing with ISO/IEC 27001.

	Sub-requirement 1	Sub-requirement 2	Sub-requirement 3	Sub-requirement 4	Sub-requirement 5
Router & Firewall	Review of configuration rule(s) sets at least every six months	Always change ALL vendor-supplied defaults and remove or disable unnecessary default accounts	Follow Change Process	Maintain Network Diagram specially Cardholder Data Environment (CDE) and data flow across system	Establish Role & Responsibility Matrix
Do Not Use Vendor Supplied default Password	Change defaults/remove unnecessary default accounts	Develop configuration standards	Use strong cryptography	Maintain an inventory	
Protect stored cardholder data	Limit cardholder data storage and retention time	Do not store sensitive data after authorization	Mask PAN (Primary account number) when displayed. the first six and last four digits are the maximum number	Do not store the personal identification number (PIN)	Do not store the card verification code (three-digit or four-digit number printed on the front or back of a payment card used to verify, after authorization.
Encrypt transmission of cardholder data	Use Strong cryptography and security protocols:	Never send unprotected PANs by end-user	The use of WEP, SSL as a security control is prohibited	ASV (Approved Scanning Vendor) Quarterly (3)	

	Sub-requirement 1	Sub-requirement 2	Sub-requirement 3	Sub-requirement 4	Sub-requirement 5
across open, public networks	Only trusted keys and certificates are accepted	messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).			
Protect all systems against malware and regularly update anti-virus software or programs	Deploy anti-virus software on all systems (particularly personal computers and servers)	Ensure that anti-virus programs are capable of detecting, removing, and protecting	All anti-virus mechanisms Are kept current	Generate audit logs which are retained per PCI DSS Requirement 10	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users.
Develop and maintain secure systems and applications	Establish process to identify security vulnerabilities	Protect system and software from vulnerabilities	Critical Security Patches apply within 1 Month	Follow change control processes and procedures	Develop applications based on secure coding guidelines (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.)
Restrict access to cardholder data by business need to know	Level of privilege required (for example, user, administrator, etc.)	Access control system(s) that restricts access based on a user's	Level of privilege required (for example, user, administrator, etc.)	Restrict access to privileged user IDs to least privileges necessary to	

	Sub-requirement 1	Sub-requirement 2	Sub-requirement 3	Sub-requirement 4	Sub-requirement 5
	for accessing resources	need to know, and is set to "deny all" unless specifically allowed	for accessing resources	perform job responsibilities.	
Identify and authenticate access to system components	Remove/disable inactive user accounts within 90 days.	Immediately revoke access for any terminated users. Failed attempt (Lock user) =6	All users a unique ID. Passwords/phrases must meet the following: 1. Minimum length of at least seven (7) characters. 2. Contain both numeric and alphabetic characters	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Set the lockout duration to a minimum of 30 minutes. Change user passwords/passphrases at least once every 90 days.
Restrict physical access to cardholder data	Use appropriate facility entry controls to limit and monitor physical access	Video cameras or access control mechanisms (or both) to monitor sensitive areas	Classify media so the sensitivity of the data can be determined.	Maintain strict control over the storage and accessibility of media	CCTV data need to retain 3 month

	Sub-requirement 1	Sub-requirement 2	Sub-requirement 3	Sub-requirement 4	Sub-requirement 5
Track and Monitor all access to network resources and cardholder data	Protect audit trail files from unauthorized modifications	Promptly back up audit trail files to a centralized log server or media that is difficult to alter	Review at least daily: 1. All security events 2. Logs of all systems that store, process, or transmit CHD and/or SAD 3. Logs of all critical system	Retain audit trail history for at least one year, with a minimum of three months available for analysis	Follow up exceptions and anomalies identified during the review process
Regularly test security systems and processes	Perform quarterly internal vulnerability scans	Run internal and external network vulnerability scans at least quarterly	Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV)	Penetration testing at least annually and after any significant infrastructure or application upgrade	Wireless: 3 Month log check
Maintain a policy that addresses information security for all personnel	Establish, publish, maintain, and disseminate a security policy	Review the security policy at least annually	Implement a risk-assessment process at least annually	Service Provider activity monitoring Annually	Monitor and control all access to data

Data Center Security

Shariful Islam, Data Center (DC) Operations Manager
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

Introduction

Data center is used to store own or third party services and data within server and dedicated data storage facility. To ensure the Confidentiality, Integrity and Accessibility (C, I, A) of these services and data, securing one's data center is crucial.

Data Center

According to the New York Times, Data Center is a building, dedicated space within a building, or a group of buildings used to house computer systems and associated components, such as telecommunications and storage systems.

Since IT operations are crucial for business continuity, it generally includes redundant or backup components and infrastructure for power supply, data communication connections, environmental controls (e.g. air conditioning, fire suppression) and various security devices. A large data center is an industrial-scale operation using as much electricity as a small town.

Data Center Security

Data center security is the set of policies, precautions and practices adopted to avoid unauthorized access and manipulation of a data center's resources. The data center houses the enterprise applications and data, hence why providing a proper security system is critical. Denial of service (DoS), theft of confidential information, data alteration, and data loss are some of the common security problems afflicting data center environments.

According to the Cost of a Data Breach Survey, in which 49 U.S. companies in 14 different industry sectors participated, they noticed that:

- 39% of companies say negligence was the primary cause of data breaches
- Malicious or criminal attacks account for 37 percent of total breaches.
- The average cost of a breach is $5.5 million.

Security Challenges

Security controls for Data Centers are becoming a huge challenge due to increasing numbers of devices and equipment being added. These increased challenges can be handled by proper following ISMS standards stated in ISO 27001:2013 and other industry

standard. To help the data center professionals of Bangladesh to maintain proper Confidentiality, Integrity and Availability of data stored in their Data Center, Information and Communication Technology Division has published Data Center Guideline, 2020 with the help of BGD e-GOV CIRT.

Vulnerability and Attack

Data theft is always a concern among cyber security professionals. With the rise of cloud computing across cyber land scape, the quantity of stored data has increased in various data center. Following security concerns has been plagued data center operators and cyber security professionals in recent decade.

Threats

The following are examples of the most common threats to Data Centers:

- Breach of confidential information
- Denial of Service (DoS) Attack
- Unauthorized access and usage of computing resources
- Identity theft
- Data theft or alteration

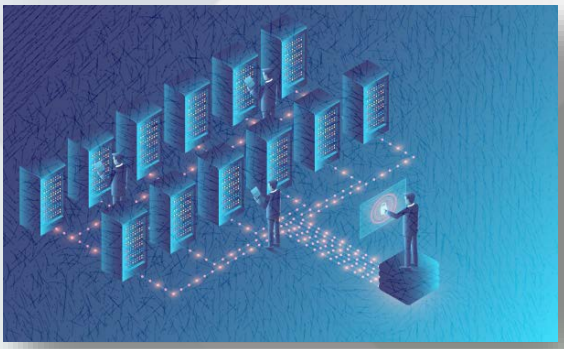
Vulnerabilities

The most common weaknesses in Data Centers are related to the following areas:

- The flaws in the implementation of things like software and protocols, wrong software design or incomplete testing, etc.
- Configuration flaws such as usage of default credentials, elements not properly configured, known vulnerabilities, out of date systems, etc.
- Ineffective security design
- Ineffective implementation of redundancy for critical systems
- Ineffective physical access control/lack of environmental controls, etc.

Based on the list of risks identified, each risk shall be mapped to security controls, that can be chosen from ISO 27001 (Annex A controls) or security controls from other local/international information security standards.

There are various types of the controls that can be implemented to mitigate identified risks, but this article will focus only on physical controls and virtual/network controls.



Common Attacks

In this section we are going to discuss some common data center attacks briefly.

- Scanning or Probing: One example of a probe- or scan-based attack is a port scan -

whereby "requests to a range of server port addresses on a host" are used, to find "an active port" and then cause harm via "a known vulnerability of that service." This reconnaissance activity often precedes an attack; its goal is to gain access by discovering information about a system or network.

- DoS (Denial of service): A denial-of-service attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. This type of attack generates a large volume of data to deliberately consume limited resources such as bandwidth, CPU cycles, and memory blocks.
- Distributed Denial of Service (DDoS): This kind of attack is a particular case of DoS where a large number of systems are compromised and used as source or traffic on a synchronized attack. In this kind of attack, the hacker does not use only one IP address but thousands of them.
- Unauthorized Access: When someone other than an account owner uses privileges associated to a compromised account to access to restricted resources using a valid account or a backdoor.
- Eavesdropping: Etymologically, Eavesdropping means secretly listen to a conversation. In the networking field, it is an unauthorized interception of information (usernames, passwords) that travels on the network. User logons are the most common signals sought.
- Viruses and Worms: These are malicious code that, when executed produce undesired results. Worms are self-replicating malware, whereas viruses, which also can replicate, need some kind of human action to cause damage.
- Internet Infrastructure Attacks: This kind of attack targets the critical components of the Internet infrastructure rather than individual systems or networks.
- Trust Exploitation: These attacks exploit the trust relationships that computer systems have to communicate.
- Session Hijacking also known as cookie hijacking: Consists of stealing a legitimate session established between a target and a trusted host. The attacker intercepts the session and makes the target believe it is communicating with the trusted host.
- Buffer Overflow Attacks: When a program allocates memory buffer space beyond what it had reserved, it results in memory corruption affecting the data stored in the memory areas that were overflowed.

- Layer 2 Attacks: This type of attack exploit the vulnerabilities of data link layer protocols and their implementations on layer 2 switching platforms.
- SQL injection: Also known as code injection, this is where input to a data-entry forms, due to incomplete data validation, allows entering harmful input that causes harmful instructions to be executed.

Data Center Security Standards

To maintain proper Confidentiality, Integrity and Availability of data stored in Data Center, Data Center Guideline, 2020 has stated following security standard as good practice.

1. ISO/IEC/BDS 27001: This standard describes the basic requirement concerning the ISMS in an organization (Organization or public authority). It emerged from the British standard BS 7799-2. Its objective is to specify the requirements for ISMS in a process approach. The standard primarily addresses organization's management and IT security managers, and secondarily implementation managers, technicians and administrators. The ISMS implementation can be audited by internal and external auditors.
2. ISO/IEC/BDS 27002: This is a guide to information security management. The standard emerged from the British BS 7799-1. Basically, this standard is to be applied where a need for information protection exists. The standard addresses IT security managers.
3. ISO/IEC/BDS 27006: This standard illustrates requirements for bodies providing audits and certifications of information security management systems.
4. The Payment Card Industry Data Security Standards (PCI DSS): PCI DSS facilitates the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect account data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). Data Centers should consider PCI DSS if its operations involve Banking and Financial systems and data.
5. ISO/IEC/BDS 27033: The objective of this standard is to focus on IT network security by specifying detailed guidelines aimed at different target groups within an organization. It includes security aspects in the handling, maintenance and operation of IT networks plus their external connections.
   - The standard comprises five parts:
   - Guidelines for network security

- Guidelines for the design and implementation of network security
- Securing communications between networks using Security Gateways
- Remote access
- Securing communications between networks using Virtual Private Networks (VPN)

6. ISO/IEC/BDS 27017: To ensured information security of data stored in cloud this security standard should be followed.

Security Controls and Risk Assessment

In ISO/IEC/BDS 27001 standard, there are 10 clauses and 14 controls. Physical and network security control and the role of risk assessment are stated below.

Physical security controls

The physical security of a Data Center is the set of protocols that prevent any kind of physical damage to the systems that store the organization's critical data. The selected security controls should be able to handle everything ranging from natural disasters to corporate espionage to terrorist attacks. Examples of physical security controls include the following:

- Secure Site selection by considering location factors like networking services, proximity to power grids, telecommunications infrastructure, transportation lines and emergency services, geological risks and climate, etc.
- Natural disaster risk-free locations or Disaster Recovery site
- Physical Access Control with anti-tailgating/anti-pass-back turnstile gate which permits only one person to pass through after authentication
- Single entry point into the facility
- Additional physical access restriction to private racks
- CCTV camera surveillance with video retention as per organization policy
- 24×7 on-site security guards, Network Operations Center (NOC) Services and technical team
- Regular maintenance of hardware in use
- Monitoring access control/activities
- Air conditioning and indirect cooling to control the temperature and humidity
- Monitoring of temperature and humidity
- Uninterruptible Power Supply (UPS)
- Smoke detectors to provide early warning of a fire at its incipient stage

- Fire protection systems, including fire extinguishers. Preferably the fire prevention shall be with zoned dry-pipe sprinkler
- Cabling Security including raised floor cabling, for security reasons and to avoid the addition of cooling systems above the racks

Network security controls

Virtual security or network security are measures put in place to prevent any unauthorized access that will affect the confidentiality, integrity or availability of data stored on servers or computing devices. Network security is quite difficult to handle as there are multiple ways to compromise the network of an organization. The biggest challenge of network security is that methods of hacking or network attacks evolve year after year. For example, a hacker may decide to use a malware, or malicious software, to bypass the various firewalls and gain access to the organization's critical information. Virtual attacks can be prevented by using the below techniques:

- Encryption for web applications, files and databases
- Audit Logs of all user activities and monitoring the same
- Best Practices for password security. Usage of strong passwords and secure usernames which are encrypted via 256-bit SSL, and not storing them in plain text, set up of scheduled expirations, prevention of password reuse
- Role Based Access Control
- AD (Active Directory)/LDAP (Lightweight Directory Access Protocol) integration
- Controls based on IP (Internet Protocol) addresses
- Encryption of the session ID cookies in order to identify each unique user
- Dual factor authentication
- Frequent third party VAPT (Vulnerability and Penetration Testing)
- Malware prevention through firewalls and other network devices

Risk assessment

According to ISO/IEC/BDS 27001, it is important to conduct a risk assessment and implement appropriate security controls in order to achieve compliance to ISO 27001, ensuring a secure Data Center. The IT infrastructure of any organization is mainly dependent on the hardware (like servers, storage, etc.) which is in the Data Center. This means that, whenever an organization implements ISO 27001 or other information security standards, the organization needs to consider the risk assessment for the Data

Center to fully protect the data. If you looking forward to do a third party risk assessment of your Data Center, BGD e-GOV CIRT is happy to help you out.

Conclusion

In modern world, data center has become an integral part for centralized storage of huge amount of data and information. Most services are nowadays cloud based and cloud based solutions are increasing every day. New type of services provided by data center operations like SaaS, PaaS and IaaS have increased dependency on data center hugely. This booming business and changed landscape has made cyber-attack on data center more frequent. So data center security should be every data center operator's top priority.

Fileless Malware: An Emerging Threat

Mukul Ahmed, Incident Handler (Cyber Sensor)
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

Introduction

Fileless malware attack is on the rise, and it's one of the foremost important digital infiltration threats to companies, according to Symantec's 2019 Internet Security Threat Report. The magnitude of this threat is usually seen within the Report's finding that malicious PowerShell scripts — one of the key components of fileless malware attacks — increased quite 1,000 percent in 2018 and accounted for 89 percent of fileless malware attacks [1]. As of carbon black recently interviewed over 400 security researchers who discussed non-malware attacks, AI (AI) and machine learning (ML), among other topics. supported this, 64 percent said that their companies are experiencing an increasing number of fileless malware attacks, 93 percent consider fileless malware attacks more threatening than traditional malware and 62 percent of fileless malware attacks target customer data.[2]

As of carbon black report, utmost common sorts of fileless attacks were:

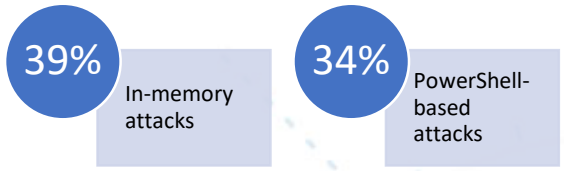


Figure 1.1: Statistics of Different type of Fileless Malware Attack. Image **Source:** VMware Carbon Black

In addition to going after customer data, fileless malware attacks mostly targeted corporate IP (53%), credentials (42%), and financial data (41%). Over half fileless malware attacks were designed for service disruption.[1]

Categorization of Fileless Attack

To demystify the term, the Microsoft Defender threat analysis team started categorising fileless attacks based on how they get onto a PC and where they're hosted. There are more than a dozen combinations of those 'entry points' and malware hosts getting used for fileless attacks -- a number of that are very sophisticated and are seldom used for targeted attacks, and a few of that have been commoditised and are showing up more often for common attacks like making an attempt to run a coin miner on the system. However, they constitute three broad groups.

Type one is really fileless, during which the attack is delivered on the network or from a device, the payload is handled in memory and nearly naught touches the disk at all. For instance, EternalBlue is a cyberattack exploit developed by the U.S. National Security Agency (NSA) and was leaked by the Shadow Brokers hacker group on April 14, 2017, one month when Microsoft released patches for the vulnerability. These are truly the most advanced attacks out there, but most of the attacks that get called fileless don't belong in this group.

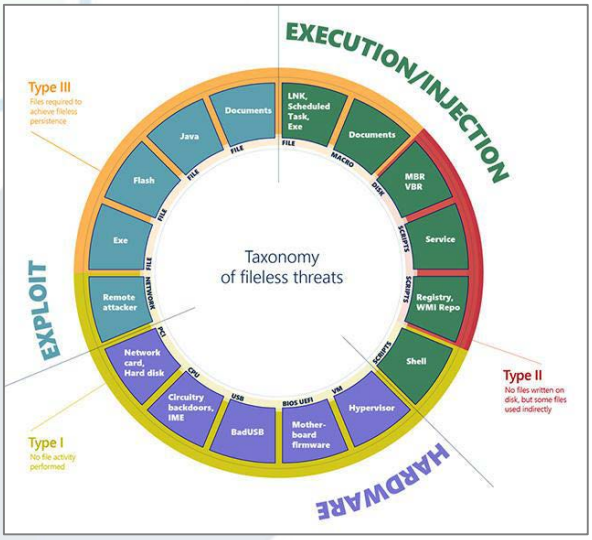


Figure 2.1: Categorization of Fileless Attack. Image Source: Microsoft

Type two attacks do use files, but indirectly, in order that they still count as fileless. Think of scripts getting used to launch attacks, whether it's JavaScript or PowerShell. We see a couple of that focus on the MBR and check out to render machines completely useless in order that they won't boot. But they mostly use the registry and WMI and various other mechanisms like PowerShell to leverage a

number of the tools that are already present on the system to sequence setup activities.

Type three clearly begin with a file whether it is a document file with a macro in it, or a Java file, or Flash file, and sometimes even EXE files that drop certain files, however then persistence is fileless. So as soon as the payload is dropped, the payload achieves persistence through both staying simply in memory or staying in the registry and running from there.

Many of these Type three attacks come from email, but the file attachments won't show up as obviously malicious if an antivirus scans the files. Generally, .EXE file isn't attached in email rather a document is attached with a macro which links to a different file then that file goes and downloads the payload. VBA code doesn't have a binary that antivirus software can scan, but it can load PowerShell scripts that download and run attacks.

What Is Fileless Malware

Fileless malware does not leverage traditional executable files like as file base malware does. It uses a way called living-off-the-land binaries — or "LoLBins". Living-off-the-land tactics mean that attackers use legitimate tools for malicious purposes. There are more than 100 Windows system tools that can be leveraged and abused as LOLBins such as PowerShell, Windows Management Instrumentation (WMI), .NET Framework, Microsoft Office Macros. It piggybacks on legitimate scripts by executing malicious activity while the legitimate programs still run. Moreover, it can remain undetected because it's memory-based, not file-based. Instead, the fileless malware is written on to the RAM and does its deed from the memory. It remains there, causing problem, until the computer is rebooted. Antivirus software often works with other sorts of malware because it detects the normal "footprints" of a signature. As fileless malware leaves no footprints therefore antivirus products can not detect.

How Fileless Malware Work

As mentioned, fileless malware is not hooked in to files being downloaded, installed and executed. It uses a far sneakier method of infecting a computer and executing, hiding within legitimate software packages, user tools and applications that already are installed on the pc. After analyzing such threats researchers have revealed numerous ways attackers use to infect victims. Some are traditional, others not so traditional.

The following are a few of the way been seen within the past exploited by attackers:

Phishing emails that include malicious downloads and links: With this method, the bulk of malware found is installed on the disk drive. However, fileless ransomware, codes are often remotely executed from memory or when a script is executed.

Legitimate applications: Compromised software packages installed like Word and JavaScript are often hijacked by attackers to execute malware.

Native application: Operating systems come with a number of preinstalled tools, like PowerShell and Windows Management Instrumentation (WMI), which can be exploited by attackers to run malicious code while piggybacking with legitimate code.

Lateral infection: By abusing PowerShell, certain fileless variants are seen moving laterally across networks, infecting other computers on an equivalent network.

Malicious websites masquerading as legitimate websites: An attacker will create a website to appear almost exactly like a legitimate business. When a user visits the website, in the background the website scans for vulnerabilities in plugins which might allow malicious code to be run within the browser's memory.

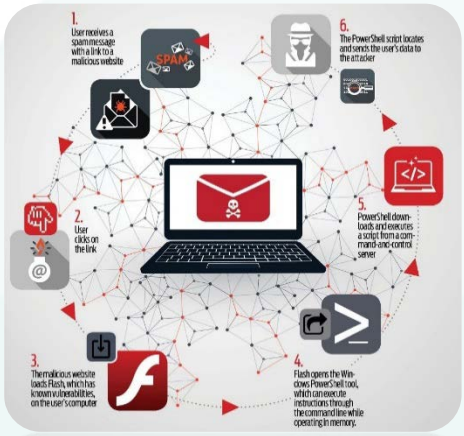


Figure 3.1: How Fileless Malware work. Image **Source:** CSO online

For Example, as can be seen from Figure 3.1 the steps of how fileless malware are targeting PowerShell as abuse LOLbins.[3]

Step 1: User receives a phishing email with a link to a malicious website.

Step 2: User clicks on the link.

Step 3: The malicious website loads Flash, which has known vulnerabilities on the user's computer.

Step 4: Flash opens the Windows PowerShell tool, which can execute instructions through the command line while operating in memory.

Step 5: PowerShell downloads and executes a script from a command and control server.

Step 6: The PowerShell scripts locates and sends the user's data to the attacker.

Fileless Malware Mitigation

As nothing is normally written to a computer's hard disk during an fileless malware attack, standard, signature-based antivirus programs are normally ineffective. So, what is the best way to mitigate against this attack if, on the surface they appear to be executing legitimate computer instructions. The simplest way to avoid the upload of this type of malware is to avoid clicking on the links that install the malicious code. Of course, this is not always possible, particularly when this malware is uploaded from legitimate-looking websites. Furthermore, hackers are often adept at redirecting their targets to illegitimate web

locations that are virtual copies of legal websites.

However, there are other, more practical measures that companies and consumers can go for avoid painful fileless malware attacks.

These include the following:

- Do patching operating systems as often as recommended by manufacturers.
- Deploying a process of "least privilege" and PowerShell logging.
- Instituting systematic network behavior analysis including the monitoring of computer process logging for unfamiliar activity.
- Disabling unnecessary macros in Windows programs such as Excel, PowerPoint, and Word.
- Computer service monitoring to identify any unusual service creation on regular basis.

As fileless malware attack is difficult to detect using standard antivirus packages and it is hard to remove even if it is located, multi-level security provides a robust method of defending against memory-resident

malware. This approach is increasingly deployed due to the expansion of corporate network perimeters as the growing use of mobile, IoT, and cloud technology make traditional antivirus protection ineffective. Multi-layer defense involves applying security measures across all of an enterprise's technology platforms. For instance, the smartphone layer would consist of the following security measures:

- Prevent modified operating systems from booting
- Kernel integrity monitoring
- Isolated execution of co-processors
- Drive encryption
- Secure storage

Similar defenses should be established across other layers of an organization's technology infrastructure to include:

- Firewall management
- Email protection
- Web gateways
- Micro data segmentation

In addition to going multi-layer, enterprises must also get predictive. Potential fileless malware attacks can be mitigated by monitoring suspicious network behavior. For instance, configuring IP numbers to extract those emanating from unusual or irregular geographical areas can flag those connections and potentially block access.

Artificial intelligence (AI) systems are probably the way that subsequent generation of antivirus programs will develop within the future. AI can recognize "normal" network behavior and determine if anomalies occur. Such solutions must be able to isolate individual endpoints in a network and stop any

infection from spreading throughout the system.

Fileless malware is not hooked in to files being downloaded, installed and executed. It uses a far sneakier method of infecting a computer and executing, hiding within legitimate software packages, user tools and applications that already are installed on the pc.

Conclusion

Since the start of 2017, fileless malware attacks have magnified in range and sophistication. According to the Ponemon Institute report, traditional antivirus solutions became ineffective with four out of five organizations disgruntled with their existing antivirus packages. On the other hand, Endpoint solutions are increasingly deployed as organizations turn their focus from network solutions to a multi-layered security approach. Moreover, traditional network security isn't solely ineffective, it's conjointly tough and expensive to manage. Despite the risks exhibit by fileless malware, steps to mitigate against the threat are comparatively simple and inexpensive. The education of home consumers and company employees is certainly one altogether the foremost effective ways in which of reducing the possibility of fileless malware infection, and campaigns that unfold the message of the danger from this type of malware ought to be increased.

References

1. https://us.norton.com/internetsecurity-malware-what-is-fileless-malware..html
2. https://www.carbonblack.com/definitions/what-is-fileless-malware/
3. https://www.csoonline.com/article/3227046/what-is-a-fileless-attack-how-hackers-invade-systems-without-installing-software.html
4. https://www.cybereason.com/blog/fileless-malware
5. https://www.intelligonetworks.com/blog/fileless-malware
6. https://www.techrepublic.com/article/what-is-fileless-malware-and-how-do-you-protect-against-it/
7. https://www.allot.com/resources/TB_FILELESS_MALWARE_THREAT_BULLETIN.pd_.pdf

Choosing, Implementing and Running a Security Information and Event Management (SIEM) Solution

Mohammad Farhad Hussain, Senior Technical Specialist (Infrastructure)
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

A SIEM (Security Information & Event Management) is a platform for managing security incidents. It allows the collection of system logs and machine data from across your IT environment to help identify unusual or suspicious activity — and then reports an alert in real time if it finds anything suspicious. You can think of a SIEM as a tool that provides a comprehensive view of an organization's IT security.

A SIEM essentially takes inputs from many different sources of information within an IT environment, and allows correlation of that information to determine whether a security incident has occurred. In its most basic form, it ingests log files from devices on a network, as well as threat intelligence data in the marketplace. A SIEM aggregates this endless stream of data to help make sense of what's happening within your environment.

While there is little doubt that SIEM solutions are critical for compliance, security monitoring or IT optimization, it is getting harder for buyers to find the right product for their needs, especially given the number of solutions available and the different options for implementation (i.e. software, hardware, cloud, outsourced, co-managed, etc.).

Choosing the wrong solution can be expensive, arduous to maintain, and difficult to staff for constant monitoring, which is why many SIEM installations end up as a shelf-ware only.

SIEM solutions, in reality, are optimized for different use-cases and one size never fits all. In fact, the evolution of SIEM and Log Management has seen a shift from using solutions for just collecting logs and meeting compliance regulations to being a core part of the network security infrastructure.

The good news is that with the number of potential solutions to choose from, if you do your homework, you will find a solution that meets your requirements. So how do you cut through all the vendor claims and hype and select the right solution for your environment and needs?

Define Your Requirements

First, you need to know your requirements. This might seem obvious, but cannot be

overstated. Particularly in complex areas such as IT security, buyers can make the mistake of eliminating the ideal solution accidentally because they had tunnel-vision for a preconceived solution instead of first articulating the preferred business outcomes. Look at your requirements in depth and figure out your needs before heading to procurement. Keeping your objective in mind, consider these areas when drawing up requirements:

Collection - What data sources do you need to log? Do you need real-time collection? Do you need to collect all data or a subset?

Storage - Do you need to archive everything? How long do you need to store data? How long do you need to keep data online?

Compliance - What compliance regulations do you need to meet? Do they require specific functionality, such as regular monitoring, alerting and the ability for automatic remediation? What sorts of reports will you are required to produce?

Analysis - How will you use your data once collected -- for legal forensics, detecting threats in real-time, isolating attacks or incidents or for compliance audits?

Reporting - What sort of reports do you need? Do you want the ability to customize reports? Personnel - Do you have the expertise on-staff to most effectively use the solution? Or will you need assistance in platform administration, data analysis, and ongoing tuning?

Other consideration - Do you need multi-user access? What level of access should they have?

Consider Implementation

Once you identify your requirements, educate yourself on the implementation options and features available.

Appliance vs. software-based solution: When deciding between an appliance and a software solution, consider the following:

Redundancy: To protect your valuable IT infrastructure, you will need to calculate a 1xN relationship of live appliances to back-ups. If your appliance breaks down and you don't have a spare, you have to ship the appliance and wait for a replacement. With software, if your device breaks down, you can simply install the software on existing capacity in your infrastructure, and be able to back-up and running in minutes versus potentially days.

Scalability: With an appliance solution, although it is a turnkey solution, your SIEM solution has a floor and a ceiling. You need at least one device to get started, and it has a maximum capacity before you have to add another appliance at a high price. With a software solution, you can scale incrementally -- one IT infrastructure device at a time.

Single sign-on: Integrate easily with Active Directory or LDAP; same username/password or smartcard authentication; very attractive.

Storage: What retention period is best for your logs? Is it Weeks or Months or Years? With appliances, it's dictated by the disk size provided. With software you decide or can use network based storage.

Scalability should be thought of as multi-dimensional, encompassing:

Collection: Collection is a multi-step process. Receiving an event is not the only part of the process. Events must be processed and data committed to storage and these activities consume system resources. It is advisable to look at how vendors define scalability for all three activities.

Storage: Scalability is evident in not just storage size but also how easy it is to move data between on¬line and off-line storage, retrieve and process records. And what

happens to archiving when the system gets temporarily overloaded? Do the events get cached or lost?

Analysis/reporting: This important aspect of scalability is often ignored. A system might process 10 million events per minute but if it takes 10 hours to run a query you are probably not getting a scalable or for that matter a viable solution.

Types of SIEM Solutions

If you're looking for the right SIEM implementation for your organization, you have a few options from which you can choose. Each, of course, comes with its own pros and cons.

In-House SIEM: With an in-house SIEM solution, an organization would purchase the software and hardware and then manage it themselves, on premise.

Pros: In-house SIEM gives you ultimate control over your system. You can customize it to meet your organization's specific security needs and fine tune or update the system whenever you'd like. You wouldn't leverage a third party for any of it — you just log in and make your changes in real time. Additionally, all of your data stays "in-house", which is a requirement for some businesses.

Cons: With a self-managed SIEM, you're totally responsible for it. That means integrating it into your existing systems, monitoring logs, customizing alerts, and training and/or employing special staff to handle it — not to mention paying for the large initial investment. You also have to maintain the infrastructure,

perform your own system patching, and manage the implementation in its entirety.

Cloud-based SIEM: With cloud-based SIEM, customers subscribe to SIEM as a service.

Pros: The subscription SIEM platform is constantly updated. There's typically little to no SIEM hardware to maintain, and licensing is typically purchased as a monthly subscription based on capacity, versus purchasing up front. Customers control how they implement the SIEM system at their organization. They don't have to rely on a third party to manage the implementation.

Cons: Customers still must retain the expertise to leverage the SIEM functionality effectively. Some people may not be comfortable with their data residing anywhere other than their own data center. Additionally, many customers may choose to use subscription SIEM for a certain set of its capabilities; consequently, they may not realize its full benefits or potential.

Managed SIEM: Choosing a managed SIEM can mean one of the few options. For example, an organization could implement a SIEM themselves, and hire an expert managed security firm to monitor it. They could also hire that firm to both install and monitor the implementation.

Pros: Managed SIEM comes with the benefits of advanced technology and highly skilled professionals, without the burden of hiring, training and retaining special personnel yourself. Compliance support and managed security assistance mean you can worry less about security and focus more on business.

Cons: Again, depending on a third party for data security can make some customers uneasy. If you pick the wrong company, you may open yourself up to more risks or unwanted hassles. It's important to thoroughly research your options and pick the right managed SIEM provider for you, one that you can truly partner with.

Conduct an Evaluation

After you make your shortlist, be sure to conduct an evaluation. Without an evaluation you are dependent on the vendor to give you correct information. One of several things can happen during implementation if you don't know what you're getting:

- The solution is unable to scale to your requirements
- The add-ons kill you on budget
- Excessive false positives are generated

- The analysis engine is too complicated to tune and you fail to detect a real threat
- Once you gain experience with the product and tune it to meet evolving objectives, you find the architecture inflexible
- Deployment is a nightmare and professional services are not in the budget
- The features and functionality you really need are hard to use and the capabilities you were most impressed with you never actually need to use

Before your evaluation be sure to put together your cross-functional SIEM project team that will eventually be a part of the implementation process. Members may include stakeholders from your organizations' legal, operations, HR, compliance and security departments. They can help you define the goals, scope and use cases of the deployment.

Once you've gone through the evaluation process, you should have gotten a feel around the kind of support you should expect to get. Will you be struggling to make it work or helped through the deployment and management process? If you choose to use a SIEM-as-a-Service model, you will hopefully not have any issues. But if you choose to just purchase the software and run it yourself, there's more to consider regarding support and maintenance.

For instance, if you need a new report, will your vendor work with you to develop this? What if you need a custom correlation rule or if you have a new data source that the vendor does not support? Or, if you have a looming audit and need your vendor's guidance through the process? Ask the vendor these questions. A trusted provider will be willing to give you value-added services without breaking your budget -- this can often mean the difference between a good and a great project.

At the end of the day, if you understood your problems, requirements and drivers and did your due diligence, you should be on your way to a successful project with a product that is optimized for your business problem.

SIEM Pricing

On-premise SIEM implementations are priced by appliance, or by hardware and software. Prices vary wildly based on how capable your SIEM platform actually is, out of the box. Typical pricing for a modestly capable solution starts in the tens of thousands of dollars range, and scales up from there. SIEM pricing models are either based on the volume of your data/events per second or on the number of devices sending logs. Pricing model based on number of devices sending logs is better

because by choosing this model you do not need to worry about data limits and it allows you to scale for future needs in a predictable manner.

Cloud-based SIEM pricing is typically based on the amount of data the SIEM platform processes, and is presented as a monthly subscription on an annual contract. You might pay a threshold fee/rate for the capacity of log files being processed by the SIEM per day, or per second. You may also have a pricing variable based on how long you want the log data retained for audit purposes (typically driven by compliance requirements).

Managed SIEM, in either on-premise, or as a service configuration, will include in the price the availability of expert security operations staff members to assist in the setup, configuration, optimization and ongoing management of your SIEM implementation.

In-house SIEM gives you ultimate control over your system. You can customize it to meet your organization's specific security needs and fine tune or update the system whenever you'd like. You wouldn't leverage a third party for any of it — you just log in and make your changes in real time. Additionally, all of your data stays "in-house", which is a requirement for some businesses.

Total Cost of Ownership

Your organization could always choose to take SIEM implementation and management all in-house. However, there are quite a few things you should keep in mind while considering this option. The value of your SIEM depends on how efficiently you are able to use it, whether that means recognizing security threats, prioritizing events, or even creating meaningful reports. This also refers to your team's ability to constantly improve threat intelligence, and to keep up with the speed at which digital threats are expanding and evolving.

All-in, implementing and managing a SIEM yourself effectively can cost you anywhere in the six-figure range in its first year. This cost includes not only the actual technology and its

installation, but the staff you'd need to hire and train to maintain it (and the space you'd need to house all of the aforementioned elements). And of course, as mentioned above, your SIEM is only as strong as the professionals who implement and maintain it. A managed SIEM implementation can start in the four

figure range for the first year, and scale upwards depending on how large your environment is.

Human Resources and skill sets required to run a SIEM

Assuming the SIEM has been installed and configured properly (i.e., in accordance with the desired use cases), a few different skill sets are needed.

SIEM Admin: This person handles the RUN function and will maintain the product in operational state and monitor its up-time. Other duties include deploying updates from the vendor and optimizing system performance. This is usually a fraction of a full time equivalent (FTE).

SIEM Analyst: This person handles the WATCH function and uses Event Tracker for security monitoring. In the case of an incident, reviews activity reports and investigates alerts. Depending on the extent of the infrastructure being monitored, this can range from a fraction of an FTE to several FTEs. You need to plan for coverage on weekends and after hours. Incident response may require notification of other admin personnel.

SIEM Expert: This person handles the TUNE function and refines/customizes the SIEM rules/content and creates rules to support new use cases. This function requires the highest skill level, familiarity with the network and expertise with the SIEM product.

The main skills required for SIEM analysts and experts are as follows:

Network Defense: The defense is the foremost task of SIEM analysts and experts therefore, they should be skilled in network defending. It helps them in monitoring, detecting, and analyzing the network threats that often intrude the networks via the internet. Networks are the easy targets for cyber attackers as it is actively connected to the internet and can pick up vulnerabilities randomly. They monitor network traffic and respond to suspicious activities immediately.

Ethical Hacking: A SIEM analyst when proficient in ethical hacking can identify potential threats and expose vulnerabilities so that the organization remains protected from malicious attackers. It also includes knowledge of penetration testing where the analyst tests network, systems, web applications, etc. to detect vulnerabilities and report them.

Incident Response: The SIEM analyst has to

manage adverse effects of a breach to minimize the impact and also suggest modifications in the existing security controls for future prevention.

Computer Forensics: To prevent the cybercrime successfully, the SIEM analysts should be aware of computer forensics. Knowledge of digital forensics will help them in collecting, analyzing, and reporting the data. The analyst can also create or gather evidence of the breach to avoid further breaches.

Reverse Engineering: Reverse engineering skills allow SIEM analysts to comprehend the performance of a software program and patch a bug.

Additionally, SIEM analysts are expected to be proficient with various skills of the operating systems, application security and more. Successful SIEM analysts bring an analytical mind, have interpersonal skills, and are team-players.

Your investment in SIEM will be completely wasted if you don't have smart people operating the tool on an ongoing basis. As a final word, the best SIEM deployments that bring the most value to organizations are run by teams of skilled, passionate, well-trained and dedicated SIEM analysts and experts.

Contact us: info@cirt.gov.bd
Incident report: cirt@cirt.gov.bd
PGP Key: 87DD 5483

www.cirt.gov.bd

/bgdegovcirt
/bgdegovcirt
/bgdegovcirt

Cyber Threat Hunting: Malicious Web Shell (Backdoor) Detection

Mohammad Makchudul Alam, Incident Handler
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

Web Shells

Web shells are actually programs used by the attackers as backdoors to the web applications in some sort. According to US-CERT:

"A web shell is a script that can be uploaded to a web server to enable remote administration of the machine. Infected web servers can be either Internet-facing or internal to the network, where the web shell is used to pivot further to internal hosts."

The US-CERT Alert (TA15-314A) states that APTs and online criminal groups have consistently used web shells as an attack vector to obtain a foothold that can potentially gain them unauthorized access to the network of interest.

The most common web shells are in PHP and ASP but web shells can be written in any language, as long as the target web server supports the language it's written in. Now there are a plethora of ways in order to upload a web shell onto the web server of interest:

- 1.XSS (Cross Site Scripting)
- 2.SQLi(SQL Injection)
- 3.RFI (Remote File Inclusion) or LFI (Local File Inclusion)
- 4.Other, such as: Incorrect configurations on the web server etc.

Some web shells:

In this demonstration session I'm using the below basic shells which are used as backdoor to the web server and also useful to generate system commands and gather sensitive information about the web server, directories, users etc….

- Basic Web Shell (Shell.php)
- c99.php
- r57.php

Various web shells can downloaded from these links: https://r57.gen.tr/shell.php, http://www.phpshelldownload.com/, http://www.r57c99.com/

Hunting Tools:

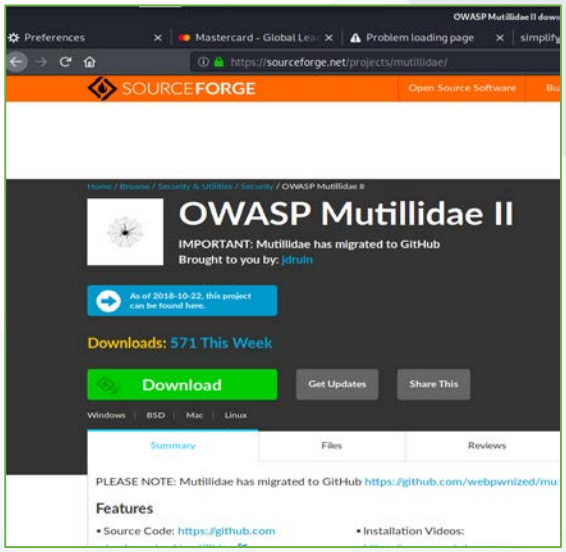
As there are tons of tools are available to detect web shells, I'm indicating just few of them, which are found handy to me at all:

1. **NeoPI**
   (https://github.com/Neohapsis/NeoPI)
   NeoPIis a Python script that uses a variety of statistical methods to detect obfuscated and encrypted content within text/script files.
2. **LOKI Simple IOC Scanner**
   (https://github.com/Neo23x0/Loki)
   LOKI is a free and simple IOC scanner. LOKI features some of the most effective rules borrowed from the rule sets of another tool called THOR APT Scanner.

3. **BackdoorMan**
   (https://github.com/cys3c/BackdoorMan) BackdoorManis a toolkit, written in Python, that helps you find malicious, hidden, and suspicious PHP scripts, including shells, in a chosen destination.
4. **Web Shell Detector**
   (http://www.shelldetector.com/)
   Web Shell Detector are scripts (PHP & Python) that will help you find and identify web shells (php, perl, asp, & aspx). Web Shell Detector has a "web shells" signature database that helps to identify "web shells" up to 99%.

In this hunting scenario I'll try to show web application threat or web shell detection by using Web Shell Detector and NeoPI tools.

Lab Arrangements



In this demonstration, we can use the following to prepare the LAB on VM:

- Used XAMPP Server (As Web Server) in Kali Linux
- Used OWASP Mutillidae (As Buggy Web Application Host)
- Shell Hunting Tool: Web Shell Hunter, NeoPI
- Server Address is http://127.0.0.1 (Local host)

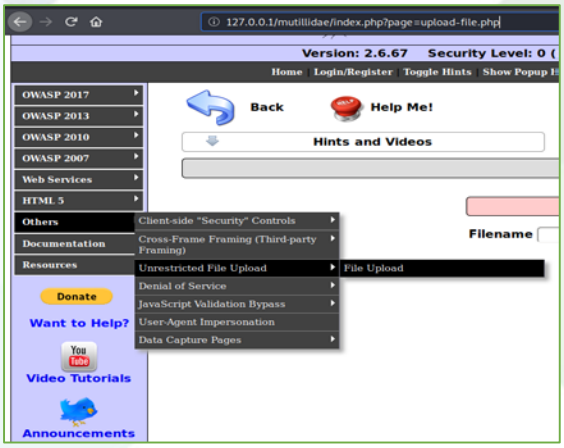
Install and Run Mutillidae:

To run the Buggy Web Application placing the mutillidae to the XAMPP folder (/opt/lampp/htdocs) the web application "Mutillidae" is accessible through web interface (OWASP Mutillidae is downloadable from: https://sourceforge.net/projects/mutillidae/)

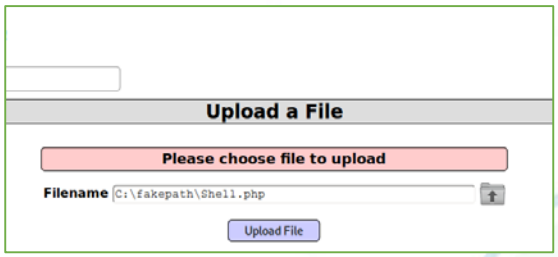
File/ Web Shell Upload to the Web Server:

1. Uploading Shell.php

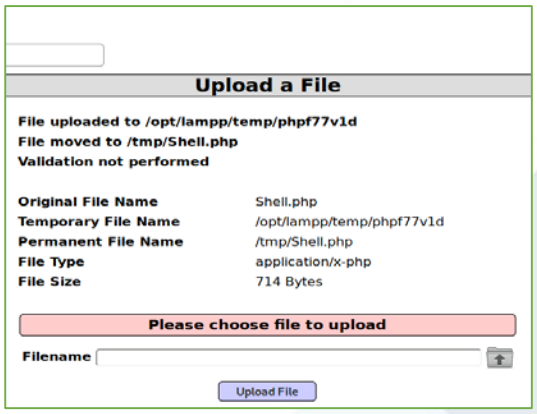
As we know there's many option to upload files or malicious shells to the web server through the web application, In that case as there is no restriction to upload any files to mutillidae we can use this option to upload malicious web shells to the application server, like as following:



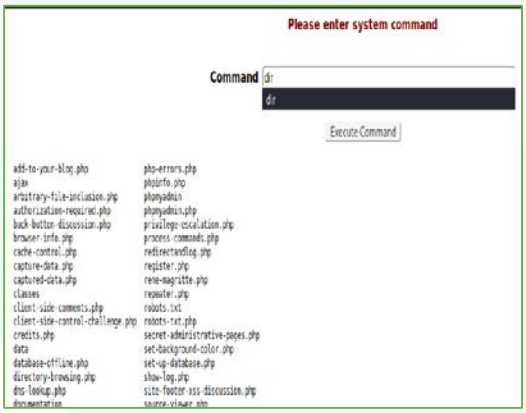
From the below figure we can see that Shell.php file is uploading to the web server without getting any restriction (*As this is the buggy web application*)



Now its appeared that **shell.php** file is uploaded to ***/opt/lamp/temp/phpf77vld*** and moved to ***/tmp*** location of the web server

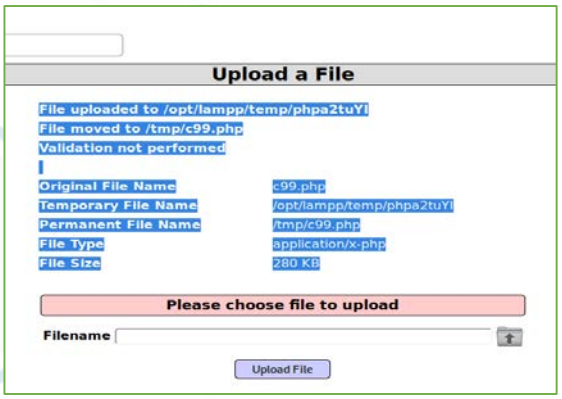


Now its appeared that accessing the **shell.php** (http://127.0.0.1/mutillidae/index.php?page=/tmp/Shell.php) actually providing a backdoor by which an attacker is able to run arbitrary commands to the web server:

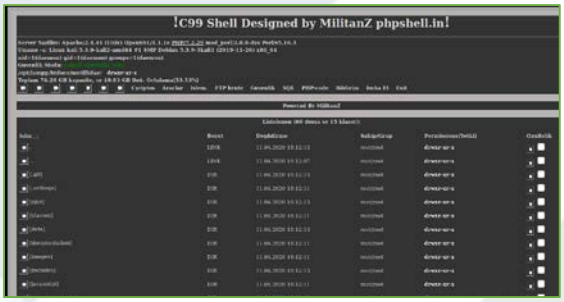


2. Uploading c99.php shell

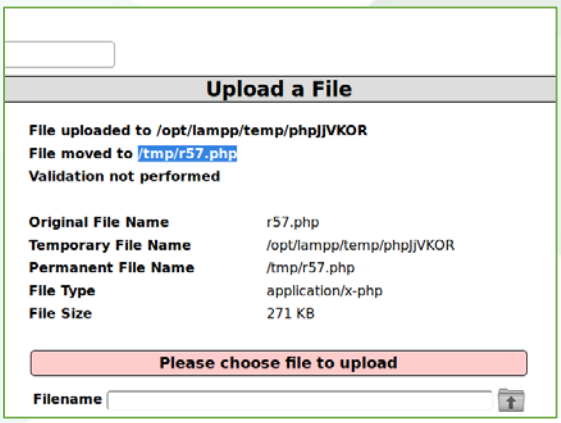
As previous Shell.php file in that case also found that c99.php is uploaded successfully and moved to /tmp location of the web server



Again found that c99.php (http://127.0.0.1/mutillidae/index.php?page=/tmp/c99.php) also providing a backdoor by which an attacker is able get extract sensitive information of the server:



3. Uploading r57.php shell



By accessing to r57.php through http://127.0.0.1/mutillidae/index.php?page=/tmp/r57.php

Similarly for the malicious r57.php file also found that this is acting as backdoor to the attacker and providing usable information and privileges to the attacker.

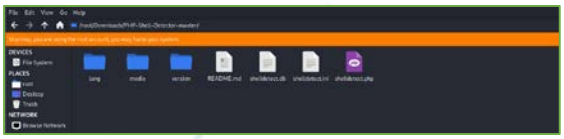
Trace The ENEMY! Detect Suspicious Web Shells!!

1. Hunting with Web Shell Detector (http://www.shelldetector.com/)

This tool is also downloadable from: https://github.com/emposha/PHP-Shell-Detector

By downloading and extracting all the files of "PHP-Shell-Detector-master" copy these to the "/opt/lampp/htdocs/" which is actually treated as the web server (and also contain the malicious r57.php, c99.php and Shell.php files) in this demonstration process.

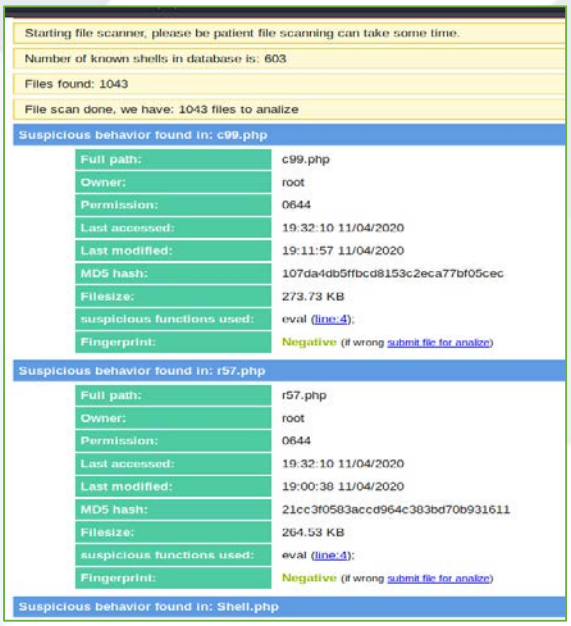
Mainly shelldetect.php file under the "PHP-Shell-Detector-master" will scan the web server directory to search the existence of malicious web shell or any other malicious files.



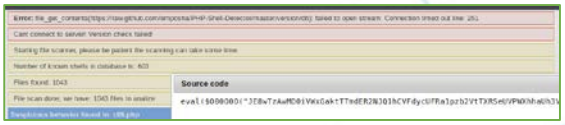
Now to execute shelldetect.php or the "PHP-Shell-Detector" tool we browse http://127.0.0.1/shelldetect.php which will start scanning automatically (Default Username: admin and Password: protect).

Finally this Web Shell Detector tool provide the scanning result by showing the detected malicious web shells/ backdoors lists.

In the following figure we can see that this tool detects our provided all the shells (c99.php, r57.php, Shell.php) and some other files which are treated risky due to their lines of suspicious codes.



This scanner also indicates the risky or suspicious line of codes by analyzing the source code of the malicious shells (Reference to the below image).

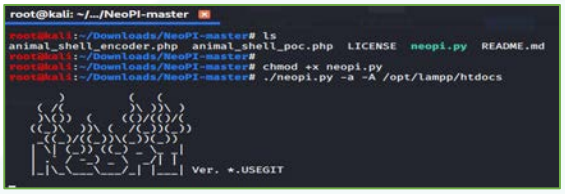


2. Hunting with NeoPI (https://github.com/Neohapsis/NeoPI)

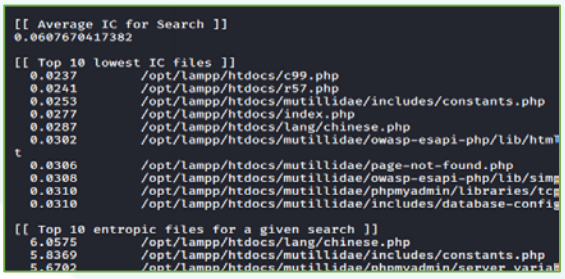
By downloading and extracting all the files of "NeoPI-master" from the github source this is needed to run the neopi.py script from the command shell.

As in the below figure showing that the command to execute the neopi.py script "./neopi.py –a –A /opt/lamp/htdocs" where

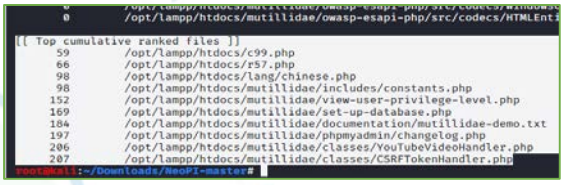
- -a : means all kind of files
- -A: means all kind of .ext files
- /opt/lampp/htdocs : Server Path needed to scan



This is noticeable that this scanner also provide the risky web shell list as scan result.



Also remarkable that, as Cumulative ranked files showing the most harmful files and we also found that c99.php and r57.php both shell files are presented as top ranked dangerous files/ web shells.



Quantum Computing and Geopolitics

Tawhidur Rahman, Senior Technical Specialist (Digital Security)
Strengthening of BGD e-GOV CIRT
Bangladesh Computer Council

Quantum computing is one of those topics that people find very interesting yet quite intimidating at the same time. When people hear — or read — that the core of quantum computing is quantum physics and quantum mechanics, they often get intimidated by the topic and steer away from it. I will not deny that some aspects of quantum computing are incredibly puzzling and hard to wrap your mind around.

The challenges of quantum mechanics

The fundamental properties of quantum mechanics have opened new opportunities for technology, but they can also pose some fundamental challenges. Elsa Kania, adjunct

senior fellow at the Center for a New American Security, argues that a sober view of these challenges can help temper some of the hype around quantum information technologies: "While references to 'the race for quantum computing' do abound, it is important to recognize that this is not just a race, but rather more of a marathon."

Operational challenges

To begin with, there are some scientific challenges that are unique to quantum technology. For example, the very nature of quantum mechanics makes it impossible to "clone" or duplicate qubits, which are the quantum equivalent of a classical computer bit. This makes many common programming techniques that rely on copying the value of a variable impossible to use with quantum technology. For similar reasons, it's impossible to read the same qubit twice. While this can be a great advantage for secure communications where you want to generate unforgeable cryptographic keys, it can create tremendous difficulties in computing as it complicates the techniques necessary to test or "debug" a program before running it.

Engineering challenges

Along with these scientific and operational challenges to quantum, there are also significant engineering problems. As one might assume, the complicated nature of quantum science means developing quantum technology is very difficult. While research and development are underway, most quantum systems exist only in a laboratory environment, with many challenges to be overcome before these systems can operate at scale.

One major hurdle includes reducing "noise." Noise is unwanted variations in data that interferes with computations and leads to errors. Noise is a problem for classical computers as well, but the sensitivity of qubits to external interference and their difficulty correcting errors that arise make it an especially difficult problem for quantum computers. Current attempts to overcome noise require laboratory settings that control for external vibrations and electromagnetic waves, and maintain very precise temperatures near absolute zero. Without solving the problem of noise, quantum systems can't reach their full potential.

Another challenge is increasing the number of qubits on a processor chip. Like a traditional computer's bit processor (i.e., 32-bit or 64-bit processor), quantum computers need qubit

processors with hundreds or even millions of qubits to complete complex computations accurately. Current quantum computers possess roughly 50 qubits. However, according to Dr. Jonathan Dowling of Louisiana State University, current efforts to develop quantum computers are seeing the number of quantum bits on a quantum computer's processor chips double every six months. "That is four times faster than Moore's Law for classical chips, but the nature of quantum computers—[through] superposition and entanglement—means that their processing speed grows exponentially with the number of qubits. So, the processing power of quantum computers obeys double exponential growth," Dowling noted. If this growth pattern continues, qubit processors could be capable of cracking one of the most widely used types of encryption, Rivest–Shamir–Adleman (RSA) encryption, and solving complex problems and simulations within the next decade.

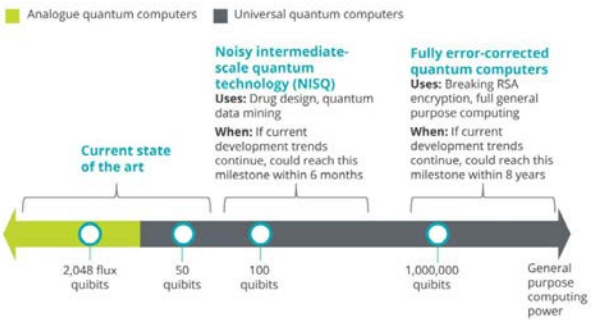
But just as with classical computers, the chip is not the only important component. New quantum computers and other such technologies also require ecosystems of supporting software, hardware, and algorithms, just as traditional computers, encryption, communications, and other technologies do. Developing these additional items will undoubtedly come with their own scientific and engineering challenges. It is important to note that quantum technologies are still in the early stages of development, which means that as these technologies mature, new problems requiring new solutions will likely come up.

Types of quantum computing systems

Not all quantum information technologies are the same. There are a few different approaches to creating qubits and using them to store, process, and output information. Those different approaches have varied strengths and limitations that make them suitable for different uses and influence their transition from the lab to the market (figure 2).

FIGURE 2

Quantum computers vary in how they can be used



Analogue quantum computers: Most associated with adiabatic quantum computers, quantum annealers, and direct quantum simulators, these types of quantum systems are some of the most developed systems to date. Because they are less capable of reducing noise, which impairs qubit quality, their functionality is currently limited to simpler and more specific use cases.

Noisy intermediate-scale quantum technology (NISQ): NISQ has been described as the next evolution in quantum computing.Although

NISQ is unlikely to completely replace analogue quantum computers, NISQ systems are more capable of tolerating noise, meaning they may require fewer qubits before being commercially viable. While improvements against noise are a design feature of NSIQ systems, noise will still impose limitations on these systems.

Fully error-corrected quantum computers: By using specially designed algorithms and additional qubits, these computers emulate a noiseless system.Because they require additional qubits to correct errors produced by noise, these systems are even more challenging to develop and may take longer to make commercially viable than analogue or NISQ systems. A fully error-corrected system would be able to solve a variety of complex problems and simulations.

Quantum's uses in national security

The possibilities afforded by advanced quantum information technologies may affect some of the most important national security tools and tasks, such as intelligence collection, solution optimization, encryption, stealth technology, computer processing, and communications. Indeed, the diversity of quantum applications across the national security domain warrants some immediate concern, both for how we can harness quantum systems and for how those quantum systems may undercut our security. But the pursuit of quantum systems necessitates advancing an ecosystem of quantum hardware, software, and algorithms, all of which have their own unique scientific, operational, and engineering challenges. So, while some concern is appropriate, too many scientific and technological challenges remain to expect radical change due to quantum technology in the near term. Still, government leaders should be aware of the emerging opportunities, challenges, and threats posed by quantum technology and begin taking steps to prepare for the coming change.

What can this mean for national security?

With uses ranging from code-breaking to code-making, and imaging to navigation, quantum information science has clear military and intelligence applications. Moreover, with developed countries such as the United States, China, Russia, Austria, Australia, Canada, the United Kingdom, and commercial companies around the globe investing in quantum research, these defense applications could have significant impact on relative national security.30 Government leaders, even those in nontechnical positions, should have a basic understanding of quantum systems and the emerging national security challenges so they can take steps to protect information and prepare their organizations, teams, and business practices for the quantum world. Here are some problem areas in national security matters where quantum science can be applied.

Loss of secrets

Information security is one of the most fundamental elements of national security. Whether it be military plans, advanced technology information, diplomatic cables, personal data, or company data, critical details related to state and business security are embedded in data being shared through public and private networks. If we can't protect this data, we can't expect any reasonable sense of national security. Cryptography is one way in which governments and private companies secure information.

The most immediately evident application of quantum computing is in national security. Quantum computers have the potential to disrupt current security protocols that protect global financial markets, render many of today's sophisticated encryption systems inoperable and upend secret government intelligence. International competition is of grave concern because one of these machines could in theory crack the encryption that protects sensitive information inside governments and businesses around the world. Quantum communications and cryptography would also offer a distinct tactical advantage to any actor that employs them on the battlefield.

Using quantum communications for the purposes of transmitting classified data is appealing to military planners across the world, as these transmissions are impossible to tap clandestinely thanks to the fundamental properties of matter. This poses an opportunity for a veritable "quantum leap" forward in military communication. Take a moment to imagine a global leak, an explosion of data unlike anything the planet has yet seen, where the innermost secrets of virtually every government, corporation, and entity on the planet become publicly available. Then combine this with the collapse of all trust on the internet. What would result is an undeniable destabilization of cyberspace and geopolitical stability.

How Real Is the Threat of Hijacked Machines?

Following the demands of the market for Omni channel presence, traditional business making is being digitally transformed. Big enterprises, medium and even micro businesses are embracing digital technology—such as cloud computing environments, IoT devices, mobility, microservices and DevOps—to deliver enhanced quality products and services at an increasing pace. Machines and machine identities are the core of this transformation.

Healthcare, water supply, electricity, oil and refinery, law enforcement, traffic management, airports and airplanes, all depend more and more on interconnected devices that need to authenticate themselves to ensure the proper functioning of highly critical infrastructure. Small or bigger scale incidents on critical infrastructure have significant physical and societal impact.

Machine authentication relies heavily on encryption algorithms. What could happen if an adversary could develop and use quantum computers to reverse engineer machine identities? The scenario of "Mortal Engines" will become a frightening reality. That actor would have the ability to wreak havoc. Hijacked machines could be turned against states, communities and cause deaths, not by physically killing people, but by, for example, contaminating the water supply. It could cause chaos in motorways and in air traffic control.

Geopolitical Implications of Quantum Computing

While at the microphysical level everything about quantum computing is very small, at the geopolitical level it's just the opposite: the implications are very large indeed. Quantum computing will bring seismic geopolitical implications, especially in the critical domains of information security and cyberwarfare.

When China launched in 2016 Micius, the world's first quantum communications enabled satellite, some remembered of the launch of the Soviet Union's Sputnik satellite in 1957, which caught the United States off guard and spurred a decades-long contest to regain and maintain global technological and military supremacy. This parallel was also pinned by Jian-Wei Pan, the lead researcher on the Micius project, who hailed the start of "a worldwide quantum space race."

Quantum computing is an emblematic battleground. Mastering such state-of-the-art technology is not a matter of prestige, it is a vital issue of determining the global status quo. Quantum computing is this century's moonshot—and now (as then), its outcome is about far more than national pride. It's nothing less than a matter of national security.

For militaries, the potential gains of quantum-enabled computing networks are clear. If the QUESS project is a success, China could gain an upper-hand in its space-based intelligence operations, including surveillance, reconnaissance, navigation, environmental monitoring, communications and attack assessment. If technology functions according to the laws of quantum theory, cyberattacks on satellites would become impossible, meaning that adversaries would not be able to interfere with military communications, for example by providing false coordinates or jamming signals. Strengthening these services would bolster China's geopolitical power-projection and increase its presence as a leading player in space technology. Quantum-enabled military communications could thus present China with an opportunity to reduce U.S. dominance in international affairs.

The U.S. National Academy of Sciences has published the report Quantum Computing: Progress and Prospects where in the findings it is mentioned that "Although the feasibility of a large-scale quantum computer is not yet certain…. Quantum computing research has

clear implications for national security. Even if the probability of creating a working quantum computer was low, given the interest and progress in this area, it seems likely this technology will be developed further by some nation-states. Thus, all nations must plan for a future of increased QC capability. The threat to current asymmetric cryptography is obvious and is driving efforts toward transitioning to post-quantum cryptography… But the national security implications transcend these issues. A larger, strategic question is about future economic and technological leadership….”

In 1919, Halford John Mackinder wrote in Democratic Ideals and Reality: A Study in the Politics of Reconstruction an influential theory for a route to world domination, writing:

"Who rules East Europe commands the Heartland:

Who rules the Heartland commands the World-Island:

Who rules the World-Island commands the World".

In the post WWII world, nuclear weapons determined the world balance and defined conventional warfare. QIS seems to be destined to redraw the rules of cyberwarfare. Whoever masters it, will cement their supremacy across almost every key technological domain. Given the dire consequences of falling behind, no country nor high-tech company can afford lagging in the quantum race, or even worse, ignoring it. Is quantum computing the new “World-Island”?

Reference:

1. https://diginomica.com/the-rise-of-the-digital-diplomat-in-a-turbulent-age
2. https://www.diplomacy.edu/resources/diplonews/issue365
3. https://www.iiss.org/publications/the-military-balance/the-military-balance-2019/quantum-computing-and-defence
4. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_264
5. https://www.weforum.org/agenda/2020/06/quantum-computers-security-challenges/
6. https://medium.com/digital-diplomacy/tagged/quantum-computing
7. https://medium.com/digital-diplomacy/us-to-invest-1b-in-ai-and-quantum-computing-b2b38408a292
8. https://www.tandfonline.com/doi/abs/10.1080/23340460.2016.1239388
9. https://thefinancialexpress.com.bd/views/from-digital-diplomacy-to-data-diplomacy-1579618123
10. http://www.ipsnews.net/2020/01/digital-diplomacy-data-diplomacy/
11. http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/ari98-2019-bjola-diplomacy-in-the-age-of-artificial-intelligence
12. https://www.semanticscholar.org/paper/Getting-digital-diplomacy-right%3A-what-quantum-can-Bjola/d231416a1432d116befe28f4732d1f6d99ba130f
13. https://www.venafi.com/blog/2020-predictions-geopolitical-implications-quantum-computers-hijacking-machines
14. https://www2.deloitte.com/us/en/insights/industry/public-sector/the-impact-of-quantum-technology-on-national-security.html

একটি স্ট্যান্ডার্ড প্যাচিং প্রসেস যেমন হওয়া উচিত

তামিম আহমেদ (CRISC, CISM,C|CISO)
কনসালটেন্ট, বিজিডি ই-গভ সার্ট

প্যাচ ম্যানেজমেন্ট হলো সফ্টওয়্যার আপডেট বিতরন করার প্রক্রিয়া। প্যাচগুলি সাধারণত সিস্টেমে ব্যবহৃত সফ্টওয়্যারের “ত্রুটি” / "দুর্বলতা" বা "বাগ" সংশোধন করতে সহায়তা করে। একটি স্ট্যান্ডার্ড প্যাচিং প্রসেস তৈরি করতে নিম্নলিখিত বিষয়গুলি বিবেচনা করা উচিত।

প্যাচটি কি কাজ করবে সেটি সম্পর্কে বিস্তারিত জানুন

১) প্রথমে প্যাচটির উদ্দেশ্য জেনে নিন, ভেন্ডর কর্তৃক প্রকাশিত প্যাচ নোট বিস্তারিত পড়ুন।

২) কোন সফ্টওয়্যার বা ফার্মওয়্যারের প্যাচটি ব্যবহারের সুযোগ রয়েছে সেটি সনাক্ত করুন।

৩) প্যাচ দ্বারা কোন বিষয়গুলোর সমাধান হবে তা তালিকাভুক্ত করুন।

৪) প্যাচ ডিপ্লয় করতে হলে কোন ধরনের ডিপেন্ডেন্সি বা নির্ভরশীলতা আছে কিনা তা সনাক্ত করুন।


Image source:
https://www.computerworld.com

প্যাচ ফাইল প্রস্তুত করণ

ক. যে প্যাচটি নিয়ে কাজ করবেন সেটি সঠিক সোর্স থেকে ডাউনলোড করা হয়েছে কিনা তা নিশ্চিত করতে হবে। ডাউনলোড এর পূর্বে ওয়েবসাইট এর টিএলএস / এসএসএল সার্টিফিকেটটি ভালো মতো যাচাই করে নিন। অনেক সময় ফিশিং এটাক স্পুফ ওয়েবসাইট অথবা ইমেইল এড্রেস ব্যবহার করে ব্যবহারকারীদের ম্যালিশিয়াস প্যাচ ডাউনলোডে উদ্বুদ্ধ করে থাকে। এছাড়াও নন-এনক্রিপ্টেড কোন চ্যানেলের মাধ্যমে যেমন এইচটিটিপি অথবা এফটিপি ওয়েবসার্ভার হতে প্যাচ ডাউনলোড করা উচিত নয়।

খ. ফাইলটি ডাউনলোডের পর checksum রান করে ভেন্ডর কর্তৃক সরবরাহকৃত হ্যাশ ভ্যালুর সাথে ডাউনলোডকৃত ফাইল এর হ্যাশ ভ্যালু মিলিয়ে নিন। যদি checksum ভ্যালু এক না হয় তাহলে ফাইলে ইন্ট্রিগ্রিটি সম্পর্কিত সমস্যা থাকতে পারে। সেক্ষেত্রে ভেন্ডর এর সাথে সরাসরি যোগাযোগ করুন।

গ. ডাউনলোড এবং সোর্স ভেরিফিকেশনের পর প্যাচ ফাইলগুলি সিস্টেম এর একটি কেন্দ্রীয় (Central) স্থানে ডাউনলোড করুন। উদাহরণস্বরূপ, আপনার সমস্ত উইন্ডোজ সফ্টওয়্যার (অপারেটিং সিস্টেম, ওয়েব ব্রাউজার এবং অন্যান্য অ্যাপ্লিকেশন সহ) ডাউনলোড করতে মাইক্রোসফ্টের

উইন্ডোজ সার্ভার আপডেট সার্ভিস (WSUS) ব্যবহার করতে পারেন।

প্যাচ আপডেট এর সঠিক সময় নির্ধারণ করুণ

প্যাচ আপডেটের জন্য সময় একটি অত্যন্ত গুরুত্বপূর্ণ বিষয়। প্যাচ ডিপ্লয়মেন্টের সময় এমনভাবে নির্ধারণ করতে হবে যেন সেসময় সার্ভিস ইমপ্যাক্ট সর্বনিম্ন থাকে। উদাহরণ স্বরূপ সিস্টেমে নেটওয়ার্ক ট্র্যাফিক যখন সবচেয়ে কম তখন ইউজার ইমপ্যাক্ট কম হবে।

ক. প্যাচিং রোলআউট ব্যর্থ হলে রোলব্যাকের জন্য সময় থাকতে হবে।

খ. প্যাচ আপডেট পরবর্তী সিস্টেম রিবুট এর প্রয়োজন হলে সেজন্যও অতিরিক্ত সময় হিসাব করে রাখতে হবে।

গ. যদি সিস্টেম একইসাথে ভিন্ন ভিন্ন টাইম জোনে কাজ করে সেক্ষেত্রে ব্যাচ ভিত্তিক প্যাচ ডিপ্লয়মেন্ট করতে হবে।

ব্যাকআপ এবং রোলব্যাক

আপনি যে সিস্টেমে পরিবর্তন করছেন তার রোলব্যাক পরিকল্পনা থাকা গুরুত্বপূর্ণ। প্যাচ প্রয়োগের পূর্বে ব্যাকআপ নেওয়া খুব জরুরি। কখনও কখনও টেস্ট এনভায়রনমেন্ট এ প্যাচ পরীক্ষা সফল হলেও পরেও প্রোডাকশন সিস্টেম এ ডিপ্লয় করার পর বাগ খুঁজে পাওয়া যায়। সেক্ষেত্রে সঠিক ব্যাকআপ-রিস্টোরেশন প্ল্যান এবং সিস্টেমের ব্যাকআপ থাকা জরুরী। রোলব্যাকের পূর্বে নিম্নবর্ণিত বিষয়গুলো বিবেচনা করা উচিত:

ক. প্রকৃত সমস্যাটি কি হয়েছিল

খ. ভেন্ডর বিষয়টি সম্পর্কে সচেতন থাকলে সমস্যা সমাধানে তাদের পরিকল্পনা কি

গ. রোলব্যাক ইমপ্যাক্ট খুব বেশি হলে কি পদক্ষেপ নাওয়া উচিত

টেস্টিং এবং নোটিফিকেশন পদ্ধতি

প্রোডাকশন সিস্টেমে সরাসরি প্যাচ ডিপ্লয়মেন্ট এর পূর্বে টেস্ট এনভায়রনমেন্টে প্যাচটি পরীক্ষা করা উচিত। যদি টেস্ট এনভায়রনমেন্ট না থাকে তবে একটি সিঙ্গেল সিস্টেম ইন্ট্যান্স এ পরীক্ষা করা যেতে পারে। টেস্ট সিস্টেমে প্যাচ ডিপ্লয়মেন্টের সকল সিস্টেম এবং এপ্লিকেশন সঠিক ভাবে কাজ করছে তা পরীক্ষা করতে হবে। টেস্ট ফলাফলের উপর ভিত্তি করে প্রোডকাশন এনভায়রনমেন্ট এ ডিপ্লয় করুন ।

প্যাচিং একটি নিয়মিত প্রক্রিয়া এবং বেশিরভাগ ব্যবহারকারীদের নিয়মিত প্যাচিং সম্পর্কে বিস্তারিত না জানলেও চলে। নিয়মিত প্যাচ এর বাইরে জরুরি প্যাচ ডিপ্লইয়ের ক্ষেত্রে কেবলমাত্র ব্যবহারকারীর কোনও ক্রিয়াকলাপ বা ইনপুট প্রদানের প্রয়োজন হয় (উদাহরণস্বরূপ: সিস্টেম রিবুট) তখন তা ব্যবহারকারীর নিকট নোটিফাই করা হয়। প্রতিষ্ঠানে প্যাচিং প্রক্রিয়া সম্পর্কিত

নির্দেশিকা থাকলে ব্যবহারকারীরা প্যাচিং পদ্ধতি ও তাঁর ইমপ্যাক্ট সম্বন্ধে জানতে পারবে।

প্যাচিং সম্পূর্ণ হয়েছে তা যাচাই করুন :

আপনি যেই প্যাচ নিয়ে কাজ করছেন তা যথাযত ভাবে ডিপ্লয় হয়েছে কিনা তা যাচাই করতে হবে। যদি ম্যানুয়ালি চেক করা সম্ভব না হয় সেক্ষেত্রে স্ক্যানিং টুলস ব্যবহার করে প্যাচ ব্যবহার করে সিস্টেম সম্পর্কিত দুর্বলতাগুলি সমাধান হয়েছে কিনা তা জানতে হবে অথবা সফ্টওয়্যারটির আপডেট সংস্করণ ইনষ্টল রয়েছে কিনা তা যাচাই করে দেখতে হবে। পরবর্তীতে প্যাচ কমপ্লায়েন্স রিপোর্ট প্রতিষ্ঠানের ম্যানেজমেন্ট বরাবর উপস্থাপন করা যেতে পারে।

Contact us: info@cirt.gov.bd
Incident report: cirt@cirt.gov.bd
PGP Key: 87DD 5483

www.cirt.gov.bd

/bgdegovcirt
/bgdegovcirt
/bgdegovcirt

BGD e-GOV CIRT has successfully participated on OIC-CERT Cybersecurity Drill – 2020 with 85% Score

The OIC-CERT Drill

An annual event for the OIC-CERT member teams with the objectives to:

- Test the communication capabilities of the members' point of contacts.
- Check the processes and procedures in managing contingencies.
- Test the technical competencies of participating teams.
- Simulate cross border cooperation in mitigating information security incidents.

The Arab Regional Cyber Drill

An annual event organized by ITU-ARCC to expose the participants from the national Computer Emergency Response Teams (CERTs) or incident response teams to various scenarios based on case studies and real-life situations, which provides them with an opportunity to test their skills and knowledge in responding to such attacks. The objective of Cyber Drill is to:

- Enhance the communication and incident response capabilities of the participating teams
- Ensure a continued collective effort in mitigating cyber threats among the Region's national Computer Incident Response Teams (CIRTs).

This year, Oman National CERT and ITU-ARCC unified the efforts and extended the value of Cyber Drill for cross regional benefits and joint the OIC-CERT and Arab Regional CERT in one cyber Drill event "The 8th Arab Regional & OIC-CERT Cyber Drill 2020" which held on 22nd September 2020.

Participants

This year 25 countries participated in the drill including, Egypt, Indonesia, Malaysia. Morocco, Bangladesh, Nigeria, Pakistan, Tunisia, Sudan, Sri Lanka, UAE, Uzbekistan, Somalia, Syria, Qatar, Kuwait, KSA, Tanzania, Benin, India, Hong Kong and Taiwan.

Figure: Team participating on Cyber Drill 2020

Theme of the 8th Arab Regional & OIC-CERT Cyber Drill 2020

The theme for 8th Arab Regional and OIC-CERT Cyber Security Drill 2020 was ***"Remote working and cyber threats"***.

Activities of BGD e-GOV CIRT

BGD e-GOV CIRT team has participated in the OIC-CERT Drill 2020. The team has successfully completed all the activities regarding the event and scored 85% with a very competitive response time.

Final Score Board:

Blockchain might be a big factor: Future Bangladesh

Md. Rayhanul Masud
Application Developer(e-Service)
BGD e-GOV CIRT
Bangladesh Computer Council

Towards ICT enabled future globe of the 21st century, Blockchain technology can be a blessing to curb different socio-economic problems. It is a buzzword everywhere visioning the propitious horizon of new opportunities and paradigms. In 2008, a pseudonymous researcher, Satoshi Nakamoto published the idea of his unique thinking. Almost 12 years have passed since then; with enormous research and implementation based on this philosophy. Developed countries around the world are reaping the fruits through various innovative solutions based on the power of this technology. And Bangladesh is not far behind the race to keep pace with. Both private and public sectors are trying to dovetail blockchain and their current solution making system interactions, more trustworthy and more fault-tolerant.

Bangladesh Computer Council (BCC) has exhibited some notable progression in this regard. To digitalize the pension system of the country's primary school teachers, the council has started a pilot project collaborated with IBM Blockchain[1].

Bangladesh National Digital Architecture (BNDA), a Team of BGD e-GOV CIRT (Computer Incident Response Team of

Bangladesh) has also introduced a solution powered by Ethereum Blockchain; that manages country's Food Grain Collection and Distribution system in a more transparent, organized and steadfast way. The Ministry of Food has taken initiatives to expedite Food Grain Collection and Distribution through the use of this solution which is going to start very soon this year[2].

Moreover, another blockchain powered solution generates certificates for the participants of various trainings offered by BKIICT (A special wing of BCC to develop skilled manpower); whereas these certificates are tamper-proof and can be verified by any entity throughout the country instantly[3]. It creates new prosperity for different organizations of the country to use this solution to get rid of document tampering and to ensure verifiability of the documents exchanged for different purposes.

The Government is very enthusiastic to leverage Blockchain Technology in the academic and professional arena. It arranged its first ever Blockchain Olympiad this year. 450 participants from 15 different institutions participated in the program. The Olympiad helped to create a bridge of knowledge sharing among the Blockchain enthusiasts throughout the country.

A good number of blockchain savvy groomed the participants to solve real life problems using blockchain. The successful accomplishment of the program selected top twelve teams to participate in the International Blockchain Olympiad, IBCOL 2020- jointly organised by City University of Hong Kong and Hong Kong Blockchain Society. Two of them bagged two of the six major awards for the country which is a remarkable success for the nation[4].

The aforementioned steps delineate the new horizon of Digital Bangladesh Vision through the proper use of technology. But the country still needs more technological infrastructure in the area of law regulation and enforcement. The news of people being deprived of their rights to get justice has become a very common phenomenon

nowadays. Very often, individuals from law enforcement forces get pressurized by powerful miscreants. Sometimes they get corrupted too reneging the promise to serve the purpose of the country

unconditionally.

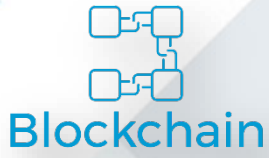
People sometimes have to return with a heavy heart when some unscrupulous officials deny to file the complaint. Some news also frustrate the mentality of the population as allegations get tampered during the process of crime investigation to gerrymander the will of legally convicted powers[5]. So, the scenario highly signifies the inevitable importance of resolution to these unwanted events. As blockchain technology offers distributed and immutable transparent data management solutions, it can be experimented to find a way regarding an easy way of filing complaints.

In our country, when people need to issue a complaint against any crime, they inform the police officials about their allegations. The officials prepare a document called First Information Report (FIR) [6] based on the received information. This process of filing a case can be done with the help of technology. People who want to file a complaint need to submit it through online which will be recorded in a blockchain ledger. The complaint will then be assigned to the related official by the system automatically. The assigned police official will prepare an E-FIR (Electronic First Information Record) and submit in the blockchain. The complainant will be notified about this assignment instantly and can verify the E-FIR issued by the official. If he/she finds any discrepancies in E-FIR, he/she will issue a dis-approval transaction in the blockchain mentioning the incongruous points. The complainant will issue an approval transaction for the opposite.

There is always a chance of deliberate case filing which might impede the genuine goal of the system. To redress the issue, Porichoy gateway[7] (Real-time E-KYC and Identity Management Platform of the country) might need to be integrated with the system to verify the true identity of the plaintiff. As all interactions are recorded with legal identities, legal actions can be taken if any deceptive behavior is found.

The system might have the provision to record various stages of the whole crime investigation process which will provide accountability and transparency of the probe. The complainant will be notified about the current progress of the investigation without any hassle. However, it will accelerate the overall workflow of the system to a great extent.

Our surroundings are inundated with volumes of problems and technology has always come there with a vision to ameliorate the pains and struggles. So, we have to embrace its power with celerity and robustness.



With the help of technology, Bangladesh will remove all hindrance and obstacles in the near future, where blockchain might be a big factor.

Links:

1. http://www.bcc.gov.bd/site/news/cc0c7efb-fa68-4682-8392-988476c4f4c0/IBM-Pilots-Blockchain-Solution-For-Primary-Teachers-Pensions-in-bd
2. https://businesspostbd.com/post/6972
3. http://bkiict.bcc.gov.bd/page/blockchain
4. https://thefinancialexpress.com.bd/sci-tech/bangladesh-wins-two-intl-blockchain-olympiad-awards-1594051080
5. https://www.thedailystar.net/country/manipulating-fir-ex-puthia-oc-undoubtedly-grave-offence-1834327
6. https://en.wikipedia.org/wiki/First_information_report
7. https://porichoy.gov.bd/

Implementation of National e-Service Bus for Digital Bangladesh

Tanimul Bari
Senior Technical Specialist (Software & e-Service)
BGD e-GOV CIRT
Bangladesh Computer Council

The concept of introducing National e-Service Bus and shared platforms/e-services to facilitate citizen service delivery utilizing emerging tools/technologies is a crucial part of Bangladesh National Digital Architecture (BNDA) and e-Government Interoperability Framework (e-GIF) project. This project has been envisioned to deliver a conceptual blueprint that defines the structure and operation of the Government of Bangladesh and a common integrated interoperability platform or service gateway for information exchange and introduce shared platforms/e-services to disseminate service and electronic information to citizens (G2C), businesses (G2B) and govt departments (G2G). It utilizes emerging tools/technologies (Blockchain, Big Data, Data Analytics, SOA etc) in a bid to embrace challenges of 4IR (Fourth Industrial

Revolution) and pave the way of digital innovation among govt agencies.

Objective

The objective is to assist GoB through BCC to design, develop, deploy and use National e-Servcie Bus and shared platforms/e-services, as part of the National Digital Architecture (NDA) and e-Government Interoperability Framework (e-GIF), to facilitate developing strategies, processes, plans, structures, technologies and systems across the Government, thereby developing an environment that enables the Government agencies to achieve its key objectives and outcomes through increased interoperability, better asset management, reduced risk and lower procurement costs.

National e-Service Bus

The Government has introduced National Enterprise Architecture (NEA) Bus (known as National e-Service Bus) under Bangladesh National Digital Architecture (BNDA) framework to ensure interoperability, availability and reusability of government online services, information and data. National e-Service Bus is a software driven middleware platform which is being developed keeping a provision to enable online services, sharing of information and data of ministries, departments and directorates to ensure interoperability and end user's easy access to it.

National e-service bus is a critical component in the interoperability architecture domain and key to ensuring seamless exchange of information and services for Government of Bangladesh. Considering the scope and span of e-service bus, due procedures and guidelines have been established around the governance to ensure robust and standardized controls are being followed by the NDA working team. The figure below is a conceptual representation of the e-Service Bus and its services connected to it.

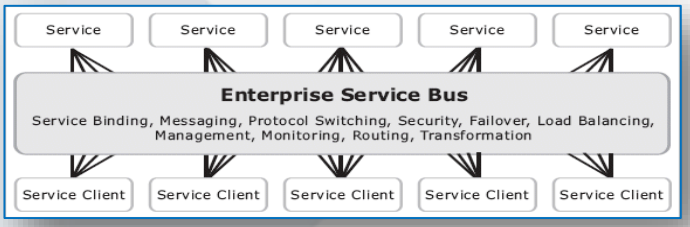


Figure 1: ESB Conceptual Diagram

It's a conduit for channeling and routing information requests to and fro from various government agencies. e-service bus is based on service oriented architecture paradigm. It works as an authentication mechanism for accessing data repositories such as the National Identity (NID), Birth & Death Registration system, Govt Employee Database etc and acts as a translator between different systems. The service definition and deployment lifecycle has been covered and due procedures including the roles and

responsibilities defined for the benefit of the SOA team working on NDA e-service bus.

Here we will illustrate process simplification using National e-Service Bus. In Bangladesh, citizen authenticity is determined by NID (National ID). There are many govt websites/portals and schemes (shown vertical in the picture below) that requires NID info for citizen authentication and verification purpose. Again, there are large application systems and e-services (shown horizontal in the picture below) that also requires NID. Again these application systems and e-services need to interact and exchange info/data with other govt websites/portals and schemes. This creates a very complex and zig-zag information flow path among the systems/services as shown in the picture below. Also, it creates demand to deploy smart network and huge load balancing facility on specific systems/services (e.g NID system) and it's owning agencies (e.g. Election Commission) that doesn't fall inside the agency's core responsibility.

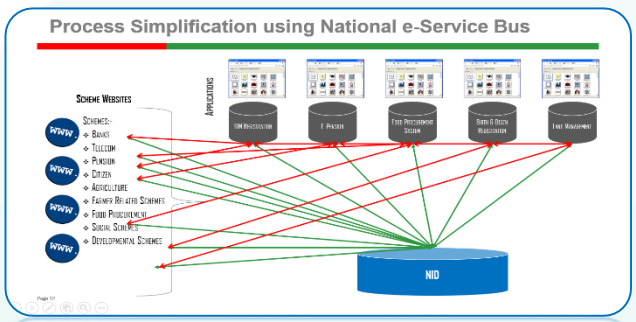


Figure 2: Scenario prior to e-Service Bus

This complex information flow can be simplified using the e-Service Bus concept. So the e-Service Bus will sit in the middle as a secure middleware platform (see the picture below) having capabilities like load balancing, traffic throttling, routing, transformation and so on. Govt application systems, Citizen services, Govt websites/portals and schemes will be connected with e-Service Bus to interact and exchange data/info with other systems (e.g NID). On the other hand, it shifts the smart networking and load balancing needs to BCC, owning agency of e-service bus, that is technically very much capable in this regard. It will also enable agencies (e.g Election Commission) to focus on their core functionalities.

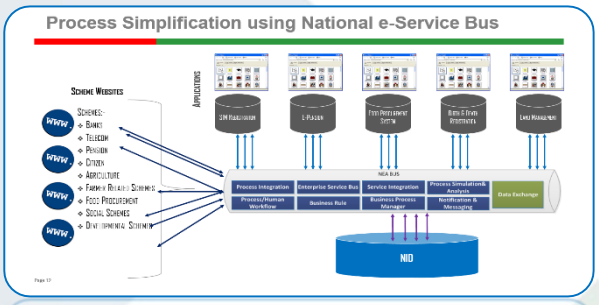


Figure 3: Simplified scenario after e-Servie Bus

This illustration assumes NID for simplicity, but the same concept can be applied for other heavily needed govt systems/services, such as, Birth & Death registration system, Govt Employee Database, Passport & Immigration system, National Data Center services etc.

Services and systems connected with National e-Service Bus

National e-Service Bus works in Producer-Consumer approach - some service will produce service to bus and some application/systems will consume service from bus. At present, 22-23 services are connected with e-service bus and exchanging data/info. For example, Citizen authentication service based on NID API, Birth & Death Registration system API, PayFixation System API, e-Primary System API etc are connected as service producer. Porichoy.gov.bd utilizes e-service bus for e-KYC and other verification/ authentication activities. There are other services that are connected as service consumers also.

Shared Services/Platforms:

At present Information Systems across the Government of Bangladesh are functioning on disparate component-run architectures, resulting in no smooth data exchange and interoperability between the information systems. This has also caused a fragmented hosting, networking and storage architecture, which is difficult and expensive to operate, creates unnecessary duplication of data and impedes effective information sharing and consolidation. The goal of the GoB is to meet the growing demands of the public, private sector organizations and citizens by providing integrated and interoperable e-services in a more secure, reliable and efficient manner through using ICTs. BCC has established BNDA framework to help GoB to meet it's goal and working to increase it's usage among govt agencies. BCC authority felt that the common/shared systems and platforms can easily be developed/procured in compliance with BNDA framework and connecting it with national e-service bus. In that case, it will create a unique reference to showcase/demonstrate benefit of shared platform/service and related activities. As a whole, it will definitely help BCC to achieve it's business and mission.

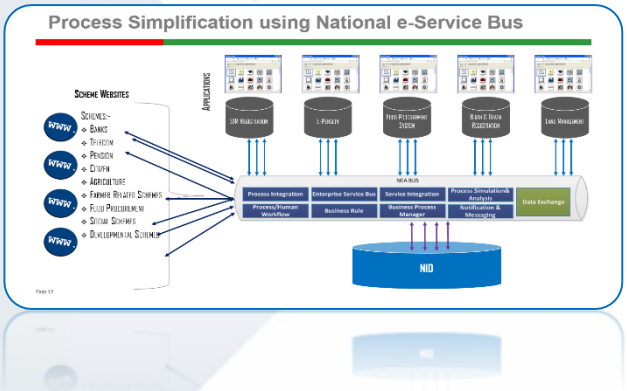


*Figure 4: Independent & dis*parate approach VS shared use of resources & standardized approach

It has been observed that organizations under the GOB are currently running (see left portion of above pic) with many difficulties, which prevent them from achieving the desired goal. The major difficulties are lack of integration and interoperability between the information systems, because each information system has been developed following different architecture and standards. There are also difficulties such as limited capacity, shortage of

resources, poor governance and management, lack of skilled manpower and proper planning. The overarching problem is to ensure interoperability between disparate data processing applications. It is anticipated that further improvements to operational efficiencies and streamlined IT projects can be achieved. First, cost containment, which is critical when dealing with other people's money – the taxpayers! Second security, which is becoming more and more important, especially as it relates to citizen privacy and third operational efficiency. Introduction of Shared platforms/services will not only save money, but will ensure right investments in right IT projects possible (see right portion of the pic above).

Shared services are typically used by multiple organizations for similar purpose. On the other hand, shared platforms will be typically used by other application system/services. In this case, shared platform exposes APIs via National e-service bus. Consumer application systems/services consumes exposed API from e-service bus.

BCC has established several shared platform and services as part of BNDA & e-GIF. Those are as follows-

- e-Recruitment System (erecruitment.bcc.gov.bd) -- shared e-service
- GeoDASH Platform (geodash.gov.bd) - shared Platform and e-service
- Blockchain Platform -- shared Platform
- Data Analytics Platform -- (analytics.bcc.gov.bd) shared Platform
- Project Tracking System (pts.bcc.gov.bd) -- shared e-service

Sample use-cases: how shared platform/e-service access e-service bus

We will describe 2 use-cases/illustrations –

i) BKIICT maintains an online Training Management System (TMS) to manage training related activities. The TMS system provides facility to generate certificate after successful completion of a course. This certificate contains various course related information e.g. certificate ID, certificate issuing date, certificate expiration date, course title and so on. Whenever a candidate applies for a job, he/she needs to present the training certificate to the employer/authority to prove his/her skillset in the specific field. But the employer/authority is unable to check the authenticity of the certificate immediately due to absence of proper online system. There can be some fraudulent practices in this case, such as, the certificate can be fake, or the certificate is manipulated by changing the original information. Here comes the necessity of Blockchain technology to eradicate/remove these problems.

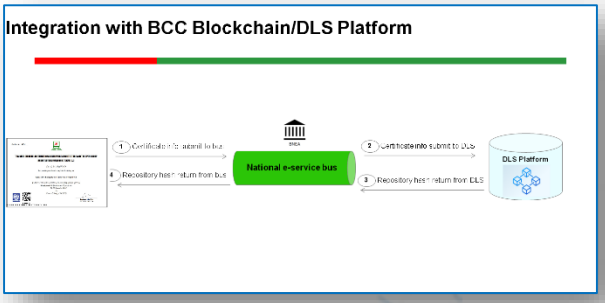


Figure 9: eRecrutiment System and Blockchain Platform

During certificate generation, identified critical info will be stored in BCC DLS platform, an important shared platform, via national e-service bus. So, TMS system will invoke registered API from e-service bus. e-service bus will forward the request to DLS platform. DLS platform will store the data and return unique pointer/hash for the stored data. The response goes back to TMS system via e-service bus. DLS platform returns a unique hash against each certificate. The unique hash will be embedded in the certificate via QR code. Employer organization will be able to identify whether any info in the certificate is manipulated or the certificate is a fake by scanning QR code (using companion app). In order to make the system working, BKIICT Training Management Systems embeds a unique identifier (via QR code) in each valid certificate when it is issued. The unique identifier is in fact the DLS repository hash of the certificate. It helps to identify manipulation attempts with certificate in a foolproof way!

ii) During development of eRecruitment Application as a shared e-service, It was decided to verify NID via e-service bus to verify authenticity of applicants as Bangladeshi citizen. In this case eRecruitment System will forward NID and Date of Birth to e-service bus. e-service bus will forward the request to NID system. NID database will return response to e-service bus that in turn returns it back to e-recruitment System. The whole message interchange takes pleace within seconds!

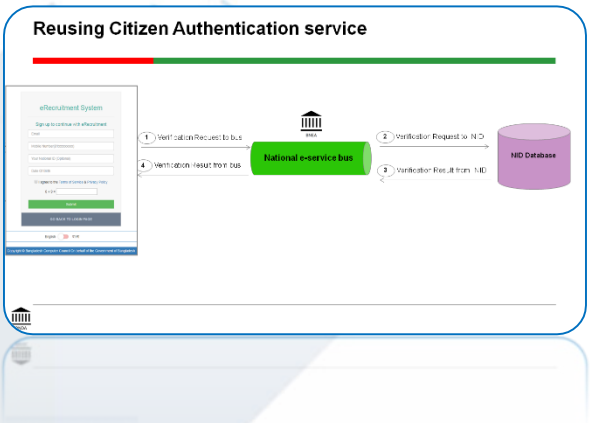


Figure 10: NID API access via e-Service Bus

Results achieved:

We will term the implementing National e-Service Bus as a successful one based on implementation achievements so far. Remarkable achievements and accomplishments are as follows

- The initiative was completed within budget and schedule. and it's working smoothly & flawlessly 24/7 hours
- As of now, 20+ e-services, citizen services and application systems are using National

e-Service Bus to provide/consume data and information. 4-5 Govt application systems and e-services are in pipeline to connect to national e-Service Bus.

- In EGDI (e-Governance Development Index) ranking, Bangladesh has improved 33 steps in last 4 years (115 at 2018 from 148 at 2014).
- To promote and boost usage of National e-Service Bus, it has been focused in BNDA guideline (1st version) by ICT Division. The guideline will enable ministries/agencies to on board regarding National e-Service Bus and shared platform/services.
- BCC has won PRESIDENT AWARD 2018 from The Open Group in 'Government Enterprise Architecture' category for establishing BNEA.
- BNDA & e-GIF has won WINNER award from ITU (International Telecommunication Union) in WSIS Prizes 2019 competition.

However, there is always scope for improvement. That's why BCC believes implementation of national e-Service Bus as an ongoing journey and continual improvement unless it's adopted by most Govt organizations.

BGD e-GOV CIRT Services

In the cyber security world, this has been denoted that security controls are three kinds; a) Detective, b) Corrective and c) Preventive.

BGD e-GOV CIRT introduces its services in two patterns in alignment with above security controls.

CIRT Services are,

1. Proactive Services
   - 1.1. Security assessments
   - 1.2. Configuration and maintenance services of security tools, applications and infrastructures
   - 1.3. Intrusion detection
   - 1.4. Security consulting
   - 1.5. Awareness building
   - 1.6. Cyber Sensor
2. Reactive Services
   - 2.1. Cyber security incident handling
     - 2.1.1. Vulnerability Assessment
     - 2.1.2. Penetration Test
     - 2.1.3. Incident Analysis
     - 2.1.4. Security Threat Notification
     - 2.1.5. Incident Coordination
   - 2.2. Digital Forensic Lab
     - 2.2.1. Evidence Detection
     - 2.2.2. Evidence Acquisition
     - 2.2.3. Evidence Analysis/Examination
     - 2.2.4. Documenting and Reporting

BGD e-GOV CIRT

ICT Tower, E-14/X, Agargaon
Dhaka, Bangladesh.

info@cirt.gov.bd

+8802 5500 7183

DIGITAL BANGLADESH
Skilled. Equipped. DigitalReady.

ICT DIVISION
FUTURE IS HERE

Bangladesh Computer Council