NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

April 2019, Edition 2.0

NETWORK INTELLIGENCE SECURITY ADVISORY

The major security news items of the month - major threats and breaches. The advisory also includes IOCs and remediation steps.

IN THIS EDITION:

Security Advisory Listing	Severity
LUCKY ELEPHANT: Credential Harvesting Campaign from Threat Actors found targeting Government, Defense and Telecommunication Organizations in South Asia	Critical
LockerGoga (.Locker) Ransomware found targeting ICS Industries across Europe, the Middle East and other parts of the world	Critical
A mass phishing campaign found distributing Emotet Banking Trojan, which further downloads TrickBot Banking Trojan and Ryuk Ransomware during thepost infection chain	Critical
A new phishing campaign pretending to be from DocuSign Company found distributing Hancitor Malware	High
A privilege escalation vulnerability (CVE-2019-0211) in Apache HTTP server can allow remote attacker to write and run scripts for gainingroot access on Unix systems	Critical

ALSO INSIDE

Data Breach Highlights

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

LUCKY ELEPHANT: Credential Harvesting Campaign from Threat Actors found targeting Government, Defense and Telecommunication Organizations in South Asia

Severity: Critical

Date: March 27, 2019

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with the latest security patches.
- Immediately apply Security Patches for Microsoft vulnerabilities CVE-2019-0808, CVE-2019-0797, CVE-2019-0784, CVE-2019-0667 & CVE-2019-0666, on Windows OS.
- Immediately apply Security Patches for Microsoft SMB vulnerabilities CVE-2019-0633 & CVE-2019-0630, on Windows OS.
- Ensure to Disable SMB version 1 (SMBv1) on Windows OS.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on a daily or weekly basis.
- Ensure web browsers are updated to the latest release.
- Ensure proper access control and email filtering are in place to protect Email Exchange Servers and Email Accounts.
- Ensure PowerShell feature is Disabled on non-administrative systems in the production environment.
- Ensure VBScript execution in Internet Explorer is Disable on connected Windows System.
- Ensure Macros are Disabled in Microsoft Office Product on connected Windows System.
- Ensure ActiveX Control is Disable in Office files.
- Ensure ActiveX Control is Disable in Internet Explorer.
- Kindly ensure Adobe Flash Player is updated to the latest release.
- Ensure internet facing devices, applications and services are using strong & complex passwords.
- Subscription to Anti-Phishing service is strongly recommended.
- Kindly Block mentioned IP/Domain on security devices.
- Kindly Block Hashes that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

IP ADDRESSES

- 103.243.173.253
- 128.127.105.13
- 179.43.169.20
- 77.244.211.55

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

LUCKY ELEPHANT: Credential Harvesting Campaign from Threat Actors found targeting Government, Defense and Telecommunication Organizations in South Asia

Severity: Critical

Date: March 27, 2019

DOMAINS

- afd-gov-bd.gq
- baf-mil-bd.tk
- checkbox.gq
- cyber-net-pk.cf
- fwo-com.tk
- g00gle-com.cf
- googlemail-com.gq
- live-com.gq
- live-com.ml
- live-service.cf
- login-live-com.cf
- login-yah00-com.tk
- login-yahoo-com.ga
- live-com-owa .gq
- account-update-com.tk
- account-updates-team.ga
- mail-ntc-net-pk.tk
- mail-paf-gov.cf
- outlook-livecom.cf
- outlook-live-com.cf
- outlook-live-com.ga
- outlooklive-com.ml
- outlook-live-com.tk
- outlookmail-com.tk
- paecgov-pk.cf
- account
- account-sign-in-security.ga
- mail-account-security-com.cf
- mail-accounts-verify-com.cf
- mail-intl-ja-mail-about.gq
- mail-nepalarmymil-np.gq
- mail-outlook-support-team.tk
- mail-sign-alert-notification.cf
- mail-updates-systems.ga
- mail-update-task.ga
- mail-update-team.ga
- mail-yahoo-com.tk
- mail-yahoo-task.tk
- micorsoft-outlook-update.ml
- mofa-gov-mm.ml
- mofagov-np.cf
- mofa-gov-np.cf
- mofa-gov-pk.tk
- molaw-gov-pk.cf
- outlook-com.cf
- paec-gov-pk.ga
- paec-gov-pk-taskmail.tk
- paecweb-gov.gq
- paecwebmail.gq
- paf-gov-pk.cf
- paf-gov-pk.ga
- paf-gov-pk.tk
- paknavy-pk.gq
- pmo-gov-pk.tk
- pnra-org.gq
- pof-gov-pk.tk
- rab-gov-bd.gq
- sco-gov-pk.tk
- sharepoint-google.ml
  slaf-gov-lk.ml
- super-net-pk.cf
- super-net-pk.tk
- test-updates.ga
- userscontent.com
  yahoo-com.ga
- yahoomail.cf
- yahoomail-com.cf
- yahoo-mail-com.ml

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

LockerGoga (.Locker) Ransomware found targeting ICS Industries across Europe, the Middle East and other parts of the world

Severity: Critical
Date: April 2, 2019

IMPACT

This poses a serious risk of unauthorized access, data loss, and causes disruption in business operation.

VULNERABILITY

All Microsoft Windows Workstation and Server are vulnerable.

TARGETED CVE IDs

- CVE-2019-0633
- CVE-2019-0630
- CVE-2019-0808
- CVE-2019-0797
- CVE-2019-0784
- CVE-2019-0667
- CVE-2019-0666

IMPORTANT

- Versions of Drupal 8 prior to 8.5.x are end-of-life and do not receive security coverage.

INTRODUCTION

On Tuesday 19th March 2019, Norsk Hydro (one of the largest aluminium producing company) got hit by a ransomware attack called LockerGoga. LockerGoga ransomware is on the radar since third week of January 2019 and it had also targeted Altran Technologies (a global innovation and engineering consulting firm) on Thursday 24th January 2019.

• LockerGoga ransomware caused massive disruption of aluminium production and business operations across Norsk Hydro's facilities. This LockerGoga ransomware attack cost them 300-350 million NOK (Norwegian krone) and it took almost two weeks to recover from this ransomware attack.

• LockerGoga ransomware is used in a targeted attack against ICS Industries in European countries, and it is being delivered via a spear-phishing email

Facts to know about this LockerGoga ransomware are:
■ The LockerGoga Ransomware is signed by Sectigo, Comodo Certificate Authority (acquired by Francisco Partners and known by its new brand name Sectigo) for code signing.
■ It is packed and highly obfuscated;
■ It has associated mutex activities;
■ It has Anti-Debug and Anti-VM protection, to evade detection. Functions such as GetLastError(), IsDebuggerPresent and OutputDebugStringA() are called as part of Anti-Debug and AntiVM protection, during LockerGoga Ransomware execution.
■ The LockerGoga Ransomware requires admin rights to run and deliver the intended attack.
■ It uses a combination of AES-256 and RSA encryption keys, to encrypt all the targeted files onto the victim's computer.
■ This LockerGoga Ransomware targets files with extensions such as .DOC, .DOT, .WBK, .DOCX, .DOTX, .DOCB, .XLM, .XLSX, .XLTX, .XLSB, .XLW, .PPT, .POT, .PPS, .PPTX, .POTX, .PPSX, .SLDX, and .PDF files.
■ It appends the file extension of encrypted file with .locker extension.

READ

- Ransomware Behind Norsk Hydro Attack Takes On Wiper-Like Capabilities

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A mass phishing campaign found distributing Emotet Banking Trojan, which further downloads TrickBot Banking Trojan and Ryuk Ransomware during the post infection chain

Severity: Critical

Date: April 02, 2019

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with the latest security patches.
- Strictly use least privilege accounts throughout the enterprise-wide network.
- Immediately apply Security Patches for Microsoft vulnerabilities CVE-2019-0808, CVE-2019-0797, CVE-2019-0784, CVE-2019-0667 & CVE-2019-0666, on Windows OS.
- Immediately apply Security Patches for Microsoft SMB vulnerabilities CVE-2019-0633 & CVE-2019-0630, on Windows OS.
- Ensure to Disable SMB version 1 (SMBv1) on Windows OS.
- Strictly restrict inbound communication on Ports 135, 139, 445, and 3389, from external networks (Internet).
- Kindly restrict access on Ports 135, 139, 445, and 3389, for servers in production and access should only be granted when needed.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on a daily or weekly basis.
- Ensure web browsers are updated to the latest release. 10. Ensure proper access control and email filtering are in place to protect Email Exchange Servers and Email Accounts.
- Ensure PowerShell and Remote Desktop features are Disabled on non-administrative systems in the production environment.
- Ensure VBScript execution in Internet Explorer is Disable on connected Windows System.
- Ensure Macros are Disabled in Microsoft Office Product on connected Windows System.
- Ensure ActiveX Control is Disable in Office files.
- Ensure ActiveX Control is Disable in Internet Explorer.
- Kindly ensure Adobe Flash Player is updated to the latest release.

IP ADDRESSES

- 192.161.54.60
- 69.164.196.21
- 107.150.40.234
- 162.211.64.20
- 217.12.210.54
- 89.18.27.34
- 193.183.98.154
- 51.255.167.0
- 91.121.155.13
- 87.98.175.85
- 185.97.7.7
- 191.98.77.181
- 187.207.136.122
- 201.183.239.117
- 187.240.45.54
- 47.44.54.70
- 89.223.90.138

DOMAINS

- efreedommaker.com
- retro11legendblue.com
- oussamatravel.com
- cashcow.ai
- shahdazma.com
- k2hdkojfkog3cd5g.onion
- kolejmontlari.com

A mass phishing campaign found distributing Emotet Banking Trojan, which further downloads TrickBot Banking Trojan and Ryuk Ransomware during the post infection chain

Severity: Critical

Date: April 02, 2019

PROTOCOLS USED FOR OUTBOUND C2

- 443 - Hypertext Transfer Protocol over TLS/SSL (HTTPS)
- 449 - AS Server Mapper
- 990 - FTP over TLS/SSL
- 8080 HTTP Alternate

AND, FOR LATERAL MOVEMENT

- 135 - Remote Procedure Call (RPC)
- 139 - NetBIOS
- 445 - Server Message Block (SMB)
- 3389 - Remote Desktop Protocol (RDP)

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A new phishing campaign pretending to be from DocuSign Company found distributing Hancitor Malware

Severity: High
Date: April 3, 2019

REMEDIATION

- Ensure Microsoft Windows Workstations and Servers are up-to-date with latest security patches.
- Strictly use least privilege accounts throughout the enterprise wide network.
- Immediately apply Security Patches for Microsoft vulnerabilities CVE-2019-0808, CVE-2019-0797, CVE-2019-0784, CVE-2019-0667 & CVE-2019-0666, on Windows OS.
- Immediately apply Security Patches for Microsoft SMB vulnerabilities CVE-2019-0633 & CVE-2019-0630, on Windows OS. 5. Ensure to Disable SMB version 1 (SMBv1) on Windows OS.
- Strictly restrict inbound communication on Ports 135, 139, 445, and 3389, from external networks (Internet).
- Kindly restrict access on Ports 135, 139, 445, and 3389, for servers in production and access should only be granted when needed.
- Ensure Antivirus Signature Database is up-to-date and Antivirus scan is run on daily or weekly basis.
- Ensure web browsers are updated to latest release.
- Ensure proper access control and email filtering are in place to protect Email Exchange Servers and Email Accounts.
- Ensure PowerShell and Remote Desktop features are Disabled on non-administrative systems in production environment.
- Ensure VBScript execution in Internet Explorer is Disable on connected Windows System. 13. Ensure Macros are Disabled in Microsoft Office Product on connected Windows System. 14. Ensure ActiveX Control is Disable in Office files.
- Ensure ActiveX Control is Disable in Internet Explorer.
- Kindly ensure Adobe Flash Player is updated to latest release.
- Ensure internet facing devices, applications and services are using strong & complex passwords.
- Kindly Block mentioned IP/Domain/Email on security devices.
- Kindly Block Hashes, that are not detected by your Antivirus Program or not known to your Antivirus Vendor.

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A new phishing campaign pretending to be from DocuSign Company found distributing Hancitor Malware

Severity: High
Date: April 3, 2019

IP ADDRESSES

- 124.156.244.77
- 176.104.107.5
- 213.159.203.175
- 212.95.103.44
- 198.105.244.228
- 47.254.75.177
- 193.183.98.66
- 91.217.137.37
- 192.71.245.208
- 178.17.170.179
- 82.196.9.45
- 151.80.222.79
- 68.183.70.217
- 217.144.135.7
- 158.69.160.164
- 207.148.83.241
- 5.189.170.196
- 217.144.132.148
- 94.247.43.254
- 188.165.200.156
- 159.89.249.249
- 150.249.149.222
- 208.67.222.222

DOMAINS

- chaibuckz.com
- cognitionclassroom.com
- fastandup.co.in
- intecwi.org
- mcnconstruction.net
- propertiesfirst.com
- sewardsfollybarandgrill.net
- unlaca.info
- unlaca.net
- unlaca.org
- ivanajankovic.com
- etsofevenghen.com
- hincasupheck.ru
- seromratbo.ru
- dokucenter.optitime.de
- jointings.org
- kitcross.ca
- shawneklassen.com
- laxmigroup1986.com
- beetfeetlife.
- supp.rivier.at
- amp.sorna.at
- beetfeetlife.bit
- api.sorna.at
- 222.222.67.208.in-addr.arpa
- cdn.avaregio.at

EMAIL

- docusign@milaromanoff.com

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A privilege escalation vulnerability (CVE-2019-0211) in Apache HTTP server can allow remote attacker to write and run scripts for gaining root access on Unix systems

Severity: Critical

Date: April 03, 2019

IMPACT

This flaw poses a serious risk of unauthorized access, data loss, data breach, and it may impact the reputation of an organization.

- CVE-2019-0211
- CVE-2019-0217
- CVE-2019-0215
- CVE-2019-0197
- CVE-2019-0196
- CVE-2019-0220

REMEDIATION

1. Kindly upgrade Apache HTTP Server to version 2.4.39 or later.

2. Kindly apply available security patches on RedHat, SUSE, Ubuntu, and Debian.

INTRODUCTION

A privilege escalation vulnerability (CVE-2019-0211) in Apache HTTP server can allow a remote attacker to write and run scripts for gaining root access on Unix systems such as RedHat, CentOS, SUSE, Fedora, IBM AIX, Oracle Solaris, Ubuntu, and Debian.

■ In Apache HTTP Server, this vulnerability is due to MPM event, worker or prefork running as less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) can execute arbitrary code with the elevated privilege of the parent process (running as root) by manipulating the scoreboard.

■ This privilege escalation vulnerability (CVE-2019-0211) in Apache HTTP server, is more likely to be taken advantage by Threat Actors for permanently wiping out data stored on Unix-based systems such as RedHat, CentOS, SUSE, Fedora, IBM AIX, Oracle Solaris, Ubuntu, and Debian.

VULNERABILITY

- RedHat Enterprise Linux
- CentOS Linux
- SUSE Linux
- Fedora Linux
- IBM AIX
- Oracle Solaris
- Ubuntu Linux
- Debian Linux

READ

- Apache Bug Lets Normal Users Gain Root Access Via Scripts
- Apache HTTP Server 2.4 vulnerabilities
- CVE-2019-0211: Apache HTTP Server privilege escalation from modules' scripts
- Advisories from RedHat, SUSE, Ubuntu and Debian

NETWORK INTELLIGENCE
Global cybersecurity provider

NEWSLETTER

April 2019, Edition 2.0

DATA BREACH HIGHLIGHTS

Buca di Beppo, Planet Hollywood Restaurants Hit by Card Breach

April 01, 2019

- Earl Enterprises admitted that hackers have stolen payment card data from tens ofits restaurants over a period of 10 months.
- Crooks used a PoS malware to syphon payment card data from point-of-sale (PoS) systems at the affected locations. The malicious code was designed to capture card numbers, expiration dates and cardholder names.

AeroGrow Discloses Data Breach of Customers' Payment Card Information

April 09, 2019

- AeroGrow discovered that attackers injected a Magecart skimmer into the website's payment page, the malicious code remained undetected between October 29, 2018, and March 4, 2019.
- The Magecart skimmer was able to syphon card number, expiration date, and CVV/CCV code provided by customers during the payment process.

State-sponsored hackers target Amnesty International Hong Kong with sophisticated cyber-attack

April 25, 2019

- Amnesty International's Hong Kong office got hit with a cyber attack launched by China-linked hackers.
- Security breach report confirms that supporters' names, Hong Kong identity card numbers and personal contact information were accessed by the hackers, and no financial data was compromised.
- The organizations discovered the security breach on March 15, 2019, during a scheduled migration of the Hong Kong office IT infrastructure to its international network.

Data breach of unknown entity exposes private data of 80 million U.S. households

April 30, 2019

- The 24GB database which includes the number of people living in each household with their full names, their marital status, income bracket, age, and more., got breached from unprotected Microsoft cloud server.