NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

August 2019, Edition 1.0

NETWORK INTELLIGENCE SECURITY ADVISORY

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

IN THIS EDITION:

Security Advisory Listing	Severity
LooCipher, a brand-new Ransomware is being distributed in the wild through a spam email campaign	Critical
Multiple spear-phishing campaigns from Sweed Threat Actor found targeting Government & Defense Organizations, as well as Banking & Financial Institutions on a global scale	Critical
Sodinokibi Ransomware is widely distributed via compromised web application server and spam email campaigns a on global scale	Critical
A new ransomware called eCh0raix, written in Go language found targeting Network Attached Storage (NAS) devices from vendors such as Synology, Lenovo Iomega (or LenovoEMC), and QNAP	Critical
Capital One Financial Corporation suffered a massive data breach incident caused due to misconfigured ModSecurity Web Application Firewall (WAF)	Critical

ALSO INSIDE

Security Patch Advisory

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

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

LooCipher, a brand-new Ransomware is being distributed in the wild through a spam email campaign

Severity: Critical

Date: July 10, 2019

IMPACT

LooCipher, a brand-new Ransomware is being This poses a serious risk of unauthorized access, data loss, financial loss, and can cause disruption in business operations in the wild through a spam email campaign.

EARLY WARNING

LooCipher Ransomware is more likely to adopt zero-day exploits for Microsoft vulnerabilities CVE-2019-1132, CVE-2019-0887, CVE-20191126, CVE-2019-1136, and CVE-2019-1037, in coming weeks. We strongly recommend our customers to immediately deploy security patches for the above-listed vulnerabilities.

INTRODUCTION

LooCipher, a brand-new Ransomware is being distributed in the wild through a spam email campaign. It uses high-level Windows API libraries such as Crypto++ for its encryption routine, which makes it difficult for Malware Analysis Sandboxes to reverse engineer the LooCipher Ransomware's binary code.

LooCipher Ransomware uses several encryption algorithms such as DES (Data Encryption Standard), AES (Advanced Encryption Standard), and ECC/ECDSA (Elliptic Curve Cryptography or Elliptic Curve Digital Signature Algorithm), for encrypting files on victim's computers. What encryption algorithm to prefer, is decided based on system information collected from the victim's computer.

LooCipher Ransomware starts its encryption routine by generating a 16byte data block with random characters chosen from a hard-coded string within the LooCipher Ransomware's code, by considering the current system time as the seed. The generated data block is then shuffled to create a 16-byte encryption key that LooCipher Ransomware uses to encrypt files on a victim's computer. The cryptographic algorithm used for creating a 16-byte encryption key would differ from system to system depending on what Windows version and system architecture being used on victim's computer.

LooCipher Ransomware excludes Windows System Directories such as "C:\Program Files", "C:\Program Files (x86)" and "C:\Windows", from its file encryption routine, to avoid any interruption during the file encryption process. LooCipher Ransomware encrypts all types of files, not limited to Database files, Web Application or Server files, Backup files, Virtual Disc files, and Virtual Machine files. Encrypted files are appended with .lcphr extension, and System Volume Shadow copies are immediately deleted to prevent the victim from restoring their Windows computer to the previous state

VULNERABILITY

Microsoft Windows Workstation and Server products are vulnerable to this attack

READ

- LooCipher: Can Encrypted Files Be Recovered From Hell?
- LooCipher: The New Infernal Ransomware

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Multiple spear-phishing campaigns from Sweed Threat Actor found targeting Government & Defense Organizations, as well as Banking & Financial Institutions on a global scale

Severity: Critical

Date: July 16, 2019

IMPACT

This poses a serious risk of unauthorized access, data breach, financial loss, and can impact the reputation of an organization

TARGETED CVE IDs

- CVE-2019-1132
- CVE-2019-0887
- CVE-2019-1130
- CVE-2019-1129
- CVE-2019-1037
- CVE-2019-1067
- CVE-2019-1113

INTRODUCTION

Multiple spear-phishing campaigns from Sweed Threat Actor found targeting Government & Defense Organizations, as well as Banking & Financial Institutions on a global scale. The attack involves the use of malicious macro-enabled Excel spreadsheet, obfuscated PowerShell Scripts, AutoIT-compiled scripts, and Agent Tesla Malware.

The attack is initiated via a spear-phishing email containing a macro-enabled Excel Spreadsheet (.xls), which is sent to the target victim as an email attachment. Once the victim opens this Excel Spreadsheet, the malicious macro will execute and initiate C2 request to download an obfuscated PowerShell script from the attacker's C&C server. Once PowerShell script is downloaded, the macro will trigger Windows Management Instrumentation (WMI) instance to execute PowerShell script on the victim's computer. This PowerShell script will execute a series of commands to check Public IP and other network related information on victim's computer, and then proceeds to download AutoIT-compiled scripts from attacker's C&C server.

The AutoIT-compiled scripts are executed via Windows Management Instrumentation (WMI) instance, which deploys Agent Tesla malware onto the victim's computer. Once deployed, the Agent Tesla Malware will run as a legitimate Windows process to communicate to the attacker's C&C server. The Agent Tesla Malware uses SMTP port 587 for outbound C2 communication with C&C server and for data exfiltration. The Agent Tesla Malware also found using TCP Port 26 and 6388 for outbound C2 communication and data exfiltration.

VULNERABILITY

Microsoft Windows Workstation and Server Platforms are vulnerable to this attack

READ

SWEED: Exposing years of Agent Tesla campaigns

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Sodinokibi Ransomware is widely distributed via compromised web application server and spam email campaigns a on global scale

Severity: Critical

Date: July 24, 2019

IMPACT

This poses a serious risk of unauthorized access, data loss, financial loss, and can disrupt business operations.

AFFECTED PRODUCTS

- Microsoft Windows Workstation and Server products.
- Oracle WebLogic Server, versions 10.3.6.0, 12.1.3.0, and 12.2.1.3.0.

INTRODUCTION

Sodinokibi ransomware is widely distributed via compromised web application server and spam email campaign on a global scale. The attack involves exploitation of Oracle WebLogic vulnerabilities CVE2019-2725 & CVE-2019-2729 to compromise web server, and exploitation of Microsoft Windows vulnerability CVE-2018-8453, to run Sodinokibi ransomware with SYSTEM privilege & tamper with Windows Boot Configuration.

This attack is initially delivered via either malicious macro-enabled Word document or malicious website link received through spam email. Once opened or accessed, it will download Malware loader which will further download Sodinokibi ransomware as a final payload. Sodinokibi ransomware will trigger VSSAdmin commands through elevated Command Prompt instance, to delete shadow copies (system restore points) on Windows system, and then trigger BCDEdit commands to disable Windows Start-up recovery option and set BootStatusPolicy to ignore all Windows start-up failure messages. Sodinokibi ransomware is a severe threat to data stored on Windows-based system, as it runs with SYSTEM privilege via exploitation of Microsoft Windows vulnerability CVE-2018-8453.

TARGETED CVE IDs

- CVE-2019-1132
- CVE-2019-0887
- CVE-2019-1014
- CVE-2019-1017
- CVE-2019-0708
- CVE-2019-0892
- CVE-2019-0803
- CVE-2019-0859
- CVE-2019-0808
- CVE-2019-0797
- CVE-2019-0633
- CVE-2019-0630
- CVE-2018-8453
- CVE-2019-2725
- CVE-2019-2729

READ

Sodinokibi ransomware attacks with CVE-2018-8453

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

A new ransomware called eCh0raix, written in Go language found targeting Network Attached Storage (NAS) devices from vendors such as Synology, Lenovo Iomega (or LenovoEMC), and QNAP

Severity: Critical

Date: August 2, 2019

IMPACT

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

AFFECTED PRODUCTS

Network Attached Storage (NAS) devices from vendors such as Synology, Lenovo Iomega (or LenovoEMC), and QNAP, are vulnerable to this ransomware attack.

READ

Threat Actors Utilizing eCh0raix Ransomware Change NAS Targeting

INTRODUCTION

A new ransomware called eCh0raix, written in Go language found targeting Network Attached Storage (NAS) devices from vendors such as Synology, Lenovo Iomega (or LenovoEMC), and QNAP to infect and encrypt data of an organization. The eCh0raix ransomware targets NAS devices by taking advantage of weak credentials and exploiting known vulnerabilities. It uses SOCKS5 proxy to communicate with the C2 server hosted on TOR network. It downloads the ransom note, an RSA public key used to encrypt the encryption key employs for encrypting victim's files and provides real-time insight on the malware's activity to the attacker.

When executed on the NAS, it will perform language checks to see if the device is from certain CIS countries (Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Armenia, Moldova, Russia, Tajikistan, Uzbekistan, and Turkmenistan). If so, the ransomware will not encrypt any files. It will then search for and kill the following process on infected NAS devices using service stop %s or systemctl stop %s commands;

- apache2
- httpd
- nginx
- mysqld
- mysqd
- php-fpm

It will also automatically skip files from directory paths that include the following strings when searching for files to encrypt on compromised NAS devices

- /proc
- /boot/
- /sys/
- /run/
- /dev/
- /etc/
- /home/httpd
- /mnt/ext/opt
- .system/thumbnail
- .system/opt
- .config
- .qpkg

- It encrypts Microsoft Office documents and OpenOffice documents, PDFs, text files, archives, databases, photos, music, video, and image files using an AES in Cipher Feedback Mode (CFB) secret key created from an AES-256 key generated locally. This AES key is then encrypted with the downloaded or embedded public RSA key and stored in base64 format in the ransom note.

- It demands a ransom amount of 0.05-0.06 BTC ($500 ~ $700 USD) or more to return the files.

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Capital One Financial Corporation suffered a massive data breach incident caused due to misconfigured ModSecurity Web Application Firewall (WAF)

Severity: Critical

Date: August 5, 2019

IMPACT

This poses a serious risk of unauthorized access, data breach, financial loss, and can impact the reputation of the organization.

AFFECTED PRODUCTS

- Misconfigured ModSecurity WAF with elevated permissions is vulnerable.
- Microsoft Windows-based Cloud Instances are vulnerable.

READ

• Capital One Data Theft Impacts 106M People

INTRODUCTION

Capital One Financial Corporation (a company specialized in providing credit cards, auto loans, and banking services) headquartered in McLean, Virginia have suffered a massive data breach incident, where attacker had unauthorized access and downloaded nearly 30GB of credit card application data associated with Capital One Financial Corporation, between March 12, 2019, to July 17, 2019.

Capital One Financial Corporation got to hear about the data theft from a tip sent via email on July 17, 2019, claiming some of their leaked data is stored and available on software development platform called Github. Credit card application data of Capital One Financial Corporation was hosted on rented Amazon AWS cloud instance, which includes information such as customer names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. This data breach incident affected approximately 100 million applicants from the United States and 6 million applicants from Canada. Breached data also includes approximately 140,000 Social Security numbers and approximately 80,000 bank account numbers of applicants from the United States, and roughly 1 million Social Insurance Numbers (SINs) of applicants from Canada.

ROOT CAUSE

This incident was caused due to a misconfiguration in ModSecurity Web Application Firewall (WAF) which was used alongside Apache HTTP server and was hosted on Amazon AWS cloud instance. The misconfiguration such as more elevated permissions assigned then required in ModSecurity WAF, allowed the attacker to exploit Server Side Request Forgery (SSRF) flaw within the WAF by relaying requests to a key back-end metadata resource on the AWS instance which had current credentials temporarily available, and was stored by security service to allow access to any resources on the Amazon AWS cloud instance from ModSecurity WAF.

The investigation also reveals that the accused attacker was a former employee of Amazon AWS cloud service provider and was employed between May 2015 to September 2016. We strongly recommend our customers to take appropriate security measures to detect any misconfigured Security Device within their production line, by timely conducting configuration review for critical servers, network devices, and security devices.

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

22nd July 2019 – 28th July 2019 | TRAC-ID: NII19.07.0.5

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
July 25, 2019	Ubuntu Linux	USN-4076-1: Linux kernel vulnerabilities	▪ Ubuntu 16.04 LTS	Follow Update instructions
July 25, 2019	Ubuntu Linux	USN-4054-2: Firefox regressions	▪ Ubuntu 19.04 ▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Follow Update instructions
July 25, 2019	Ubuntu Linux	USN-4075-1: Exim vulnerability	▪ Ubuntu 19.04 ▪ Ubuntu 18.04 LTS ▪ Ubuntu 16.04 LTS	Follow Update instructions
July 25, 2019	Ubuntu Linux	USN-4074-1: VLC vulnerabilities	▪ Ubuntu 19.04 ▪ Ubuntu 18.04 LTS	Follow Update instructions

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

SUSE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
July 26, 2019	SUSE Linux	Security update for cronie	▪ SUSE Linux Enterprise Server 12-SP4 ▪ SUSE Linux Enterprise Desktop 12-SP4 ▪ SUSE CaaS Platform 3.0	Security Patch Update
July 25, 2019	SUSE Linux	Security update for rmt-server	▪ SUSE Linux Enterprise Module for Server Applications 15-SP1 ▪ SUSE Linux Enterprise Module for Public Cloud 15-SP1	Security Patch Update
July 25, 2019	SUSE Linux	Security update for libsolv, libzypp, zypper	▪ SUSE Linux Enterprise Server for SAP 12-SP3 ▪ SUSE Linux Enterprise Server 12-SP5 ▪ SUSE Linux Enterprise Server 12-SP4 ▪ SUSE Linux Enterprise Server 12-SP3-LTSS ▪ SUSE Linux Enterprise Desktop 12-SP5 ▪ SUSE Linux Enterprise Desktop 12-SP4 ▪ SUSE Enterprise Storage 5 ▪ SUSE CaaS Platform 3.0	Security Patch Update

F5 NETWORKS

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
July 24, 2019	F5 BIG-IP APM and LTM	K09940637: NTP vulnerability CVE-2019-11331	▪ F5 BIG-IP APM and LTM 15.0.0 ▪ F5 BIG-IP APM and LTM 14.0.0 - 14.1.0 ▪ F5 BIG-IP APM and LTM 13.1.0 - 13.1.1 ▪ F5 BIG-IP APM and LTM 12.1.0 - 12.1.4 ▪ F5 BIG-IP APM and LTM 11.5.2 - 11.6.4	Kindly update to fixed version
July 23, 2019	F5 BIG-IP APM and LTM	K10092301: BIND vulnerability CVE-2019-6471	▪ F5 BIG-IP APM and LTM 15.0.0 ▪ F5 BIG-IP APM and LTM 14.0.0 - 14.1.0 ▪ F5 BIG-IP APM and LTM 13.1.0 - 13.1.1 ▪ F5 BIG-IP APM and LTM 12.1.0 - 12.1.4 ▪ F5 BIG-IP APM and LTM 11.5.2 - 11.6.4	Kindly update to fixed version