NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

March 2021, Edition 2.0

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
Threat Actor campaigns have struck some notable targets using less sophisticated yet dangerous ransomware like "HelloKitty" via phishing emails or as secondary infection through malware droppers	● Critical
TrickBot malware has been widely distributed via spam email campaigns for further spreading other malware families such as Ryuk, Conti, Emotet	● Critical
Remote Command Execution (RCE) vulnerability (CVE-2020-9020) in Iteris' Vantage Velocity field unit version 2.3.1, 2.4.2 and 3.0 were actively exploited in a malware attack and Hacking campaign	● Critical
Threat actor groups are using a new exfiltration technique to harvest sensitive information from e-commerce websites & hide the captured credit card data in JPG file format	● Critical

ALSO INSIDE

Security Patch Advisory

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

Threat Actor campaigns have struck some notable targets using less sophisticated yet dangerous ransomware like “HelloKitty” via phishing emails or as secondary infection through malware droppers

Severity: Critical

Date: March 19, 2021

URL'S

- 6x7dp6h3w6q3ugjv4yv5gycj3femb24kysgry5b44hhgfwc5ml5qrdad[.]onion
- x6gjpqs4jjvgpfvhghdz2dk7be34emyzluimticj5s5fexf4wa65ngad[.]onion

REMEDIATION

Block the threat indicators at their respective controls.
2. Ensure Microsoft Windows Workstations are updated with the latest security patches.
3. Ensure Microsoft Exchange Server and Microsoft IIS Server are updated with the latest security patches.
4. Do not click on links or download untrusted email attachments coming from unknown email addresses.
5. Inspect the sending email address in the header to ensure the address matches with the purported sender.
6. Ensure Domain Accounts follows the least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.
7. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through a VPN tunnel.
8. Enable User Account Control (UAC) to mitigate the impact of malware.
9. Keep all systems and software updated to the latest patched versions.
10. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through the Web Application Firewall (WAF).
11. Ensure to monitor suspicious activity or intrusion through the SIEM solution.
12. Ensure data backup is done periodically and ensure data backups are done via an out-of-band network onto the server with limited or no internet access.

READ

- HelloKitty: When Cyberpunk met cy-purr-crime
- HelloKitty Ransomware Lacks Stealth, But Still Strikes Home

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
78afe88dbfa9f7794037432db3975fa057eae3e4dc0f39bf19f2f04fa6e5c07c	Yes	Yes	No	No	No
fa722d0667418d68c4935e1461010a8f730f02fa1f595ee68bd0768fd5d1f8bb	Yes	Yes	Yes	Yes	Yes
c7d6719bbfb5baaadda498bf5ef49a3ada1d795b9ae4709074b0e3976968741e	Yes	Yes	Yes	Yes	Yes
9a7daafc56300bd94ceef23eac56a0735b63ec6b9a7a409fb5a9b63efe1aa0b0	Yes	Yes	Yes	Yes	Yes
38d9a71dc7b3c257e4bd0a536067ff91a500a49ece7036f9594b042dd0409339	Yes	Yes	Yes	No	Yes
501487b025f25ddf1ca32deb57a2b4db43ccf6635c1edc74b9cff54ce0e5bcfe	No	Yes	Yes	Yes	No

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

TrickBot malware has been widely distributed via spam email campaigns for further spreading other malware families such as Ryuk, Conti, Emotet

Severity: Critical

Date: March 18, 2021

IMPACT

TrickBot malware infection poses severe risk of credential disclosure, unauthorized access, host enumeration, remote execution of malicious code, plant further malware for persistent access to the network, data exfiltration and execute ransomware like disruptive attack, interruption in business services, cause financial loss, and impact reputation of an organization.

RECOMMENDATIONS

1. Ensure Microsoft Windows Servers and Workstations are updated with the latest security patches.
2. Ensure Microsoft Exchange Server and Microsoft IIS Server are updated with the latest security patches.
3. Enable User Account Control (UAC) to mitigate the impact of malware.
4. Ensure to use the least privileged account on a computer, while performing day to day business activities.
5. Limit unnecessary lateral communications between network hoses, segments, and devices.
6. Ensure Two-Factor authentication is enabled on all Business Email Accounts.
7. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.
8. It is strongly recommended to adopt and implement a zero-trust model across enterprise-wide cybersecurity operations and management
9. Ensure data backup is done periodically and ensure data backups are done via an out-of-band network onto the server with limited or no internet access.
10. Do not click on links or download untrusted email attachments coming from unknown email addresses.
11. Check devices to ensure that BIOS write protections are enabled.

INTRODUCTION

The initial infection is spread primarily through spear-phishing campaigns delivering emails containing malicious attachments or links. In recent campaigns attackers phishing emails claiming to contain proof of a traffic violation, to steal sensitive information.

In recent campaigns, the attackers delivered phishing emails with malicious links claiming to contain proof of a traffic violation and tricked the victim to Click on photo proof of their traffic violation on a compromised website. By clicking the photo victim unknowingly ends up downloading a malicious JavaScript file which when opened, automatically communicates with the malicious actor’s C2 server to download TrickBot to the victim’s system. Also, in one of the recent campaigns, the malware performed host enumeration for reconning vulnerabilities in the UEFI firmware.

For persistence and defence evasion the TrickBot malware injects into svchost.exe process creates a scheduled task on the system, modifies registry entries masquerades TrickBot downloader as Microsoft Word document icon uses AES (256 bits) encryption algorithm in its loader and configuration files for obfuscating its functionality disables Windows Defender.

Trickbot malware performs person-in-the-browser attacks to steal information such as login credentials, some of the modules spread the malware laterally across a network by abusing the SMB protocol, data exfiltration, crypto mining, host enumeration etc. The Trickbot malware also acts as a dropper/downloader for dropping other malware families such as Ryuk, Conti, Emotet.

SNORT Rules

Click here.

READ

- US Department of Homeland Security's CISA and the FBI warn security teams to guard against the advanced Trojan malware.
- CISA advisory on TrickBot Malware

Remote Command Execution (RCE) vulnerability (CVE-2020-9020) in Iteris’ Vantage Velocity field unit version 2.3.1, 2.4.2 and 3.0 were actively exploited in a malware attack and Hacking campaign

Severity: Critical

Date: March 18, 2021

URL'S

- http://198[.]23[.]238[.]203/arm
- http://198[.]23[.]238[.]203/arm7
- http://198[.]23[.]238[.]203/mips
- http://198[.]23[.]238[.]203/mipsel
- http://198[.]23[.]238[.]203/powerpc
- http://198[.]23[.]238[.]203/sh4
- http://198[.]23[.]238[.]203/sparc
- http://198[.]23[.]238[.]203/m68k
- http://198[.]23[.]238[.]203/x86_64
- http://198[.]23[.]238[.]203/x86_32

IP’s

- 51[.]81[.]24[.]157
- 198[.]23[.]238[.]203

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Ensure Microsoft Windows Workstations are updated with latest security patches.
3. Ensure Microsoft Exchange Server and Microsoft IIS Server are updated with latest security patches.
4. Do not click on links or download untrusted email attachments coming from unknown email addresses.
5. Ensure Domain Accounts follows least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.
6. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.
7. Enable User Account Control (UAC) to mitigate the impact of malware.
8. Keep all systems and software updated to latest patched versions.
9. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
10. Ensure to monitor suspicious activity or intrusion through SIEM solution

READ

- Satori: Mirai Botnet Variant Targeting Vantage Velocity Field Unit RCE Vulnerability

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
0d74227dbc3bdd74a3854d81e47cf6048da2d95c3010b953de407e5989beb066	Yes	Yes	Yes	Yes	Yes
fe8e5e7041dfda470f9e2ad9abe9e0da3e43ddb5b24209e42ce0e3ebee1a7bfe	Yes	Yes	Yes	Yes	Yes
320d7067d60f9ed7e7f3e9408a5d3b0a6fdccddde494c0a2a4f4e77aecb80814	Yes	Yes	Yes	No	Yes
fbe314dc3b284ce2db1f37478338fdba8130bf44e484f5028ca92eb9326417e4	Yes	Yes	Yes	No	Yes
3c62d16451db32f72464a854d6aceb7c7ba2f07c38850f6a247a5243c0f473cb	Yes	Yes	Yes	No	Yes
13ce782d393f2b4ce797747d12f377afad9d6e56c10f52948034a234654a9d30	Yes	Yes	Yes	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Threat actor groups are using a new exfiltration technique to harvest sensitive information from e-commerce websites & hide the captured credit card data in JPG file format

Severity: Critical

Date: March 17, 2021

RECOMMENDATIONS

1. Implement mechanisms to ensure the integrity of the file system using the FIM solution.
2. Limit User Access & Permissions to the website.
3. Configure directory browsing to prevent malicious users from viewing the contents of every directory on the website.
4. Restrict PHP execution in directories that hold images or allow uploads.
5. Ensure Linux servers and workstations are updated with the latest security patches.
6. Ensure Domain Accounts follows the least privilege principle and ensure two-factor authentication is enabled on all Business Email Accounts.
7. Keep all systems and software updated to the latest patched versions.
8. Ensure to monitor suspicious activity or intrusion through SIEM solution.

INTRODUCTION

The Threat Actors frequently come up with creative techniques to disguise their malicious behaviour and steal sensitive data from e-commerce websites. Recently the attackers have compromised e-commerce website running CMS Magento 2 by using new exfiltration technique to harvest sensitive information from e-commerce websites & hide captured credit card data in JPG file by injecting malicious PHP code to capture POST request data from the site visitors.

This new technique injects malicious PHP code into the file ./vendor/Magento/module-customer/Model/Session.PHP and to load the rest of the malicious code onto the compromised environment, the getAuthenticates a function is created and called. The code further creates the image file (pub/media/tmp/design/file/default_luma_logo.jpg) to store the captured data. The PHP code uses the Magento code framework and uses Magento functions getPostValue & is logged in to capture the checkout page data including email address if a customer was logged in as a user. The captured POST data is encoded with base64 before saving it to the created image file. All the information submitted by the victim on the checkout page is stored within the Customer_ parameter, including full names, addresses, payment card details, telephone numbers, and user agent details.

In previous exfiltration technique, the attackers injected malicious PHP code in one of the Magento files: ./app/code/core/Mage/Payment/Model/Method/Cc.php and used PHP function file_get_contents to obfuscate the URL and load JavaScript skimmer.

These Credit Card Skimmer threats pose a severe risk of exposing sensitive data and PII data to the attackers, ultimately leading to PCI compliance issues. Also, put customers at risk of identity theft or credit card fraud.

READ

- Magecart hackers hide captured credit card data in JPG file
- Magento 2 PHP Credit Card Skimmer Saves to JPG

DATA BREACH HIGHLIGHTS

The European Banking Authority (EBA), a regulatory agency of the European Union headquartered in Paris., has suffered security breach followed by data breach incident

March 08, 2021

- Hackers compromised Microsoft Exchange servers at the EU Banking Regulator EBA
- Cyber-attack on the European Banking Authority

Qualys, Inc. the California based cloud security and compliance service provider, suffered data breach

March 03, 2021

- Clop ransomware gang leaks data allegedly stolen from cybersecurity firm Qualys
- Qualys Update on Accellion FTA Security Incident

SITA, a multinational information technology company providing IT and telecommunication services to the air transport industry, has suffered data breach

March 05, 2021

- Millions of travelers of several airlines impacted by SITA data breach
- SITA statement about security incident