NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

April 2021, 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
New malware Saint Bot is being actively distributed recently in the wild via phishing attacks to deploy credential stealers and other malicious payloads	Critical
Lazarus APT Threat Actor Group deployed new malware Vyveva in their latest cyberespionage campaigns striking South African freight logistics company	Critical
Iranian Threat Actor Group APT34 unleashed a new backdoor variant, SideTwist, in their latest cyberespionage campaigns	Critical
APT Threat Actor Groups actively exploited Directory Traversal Vulnerability (CVE-2018-13379) in Fortinet Forti OS servers to access organization networks and deploy Cring ransomware	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

New malware Saint Bot is being actively distributed recently in the wild via phishing attacks to deploy credential stealers and other malicious payloads

Severity: Critical

Date: April 12, 2021

DOMAINS

68468438438[.]xyz

update-0019992[.]ru

380222001[.]xyz

URL's

http://68468438438[.]xyz/soft/win230321[.]exe

http://update-0019992.ru/testcp1/gate.php

http://name1d.site/file.exe\

https://cdn.discordapp.com/attachments/821809080812437507/822009014418276353/mixinte.exe

https://cdn.discordapp.com/attachments/822140450072821791/822146649219661844/z.exe

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Ensure Microsoft Windows Workstations, Microsoft Exchange Server and Microsoft IIS Server are updated with latest security patches.
3. Do not click on links or download untrusted email attachments coming from unknown email addresses.
4. Ensure Domain Accounts follows least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.
5. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.
6. Enable User Account Control (UAC) to mitigate the impact of malware.
7. Keep all systems and software updated to latest patched versions.
8. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
9. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from internet facing cloud or on-premise IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.
10. Limit unnecessary lateral communications between network hoses, segments, and devices.
11. Ensure data backup is done periodically and ensure data backups are done via out-of-band network onto the server with limited or no internet access.
12. Ensure to monitor suspicious activity or intrusion through SIEM solution.

READ

- A deep dive into Saint Bot, a new downloader

HASH (SHA-256)

HASHES (SHA-256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
63d7b35ca907673634ea66e73d6a38486b0b043f3d511ec2d2209597c7898ae8	Yes	Yes	No	No	Yes
b0b0cb50456a989114468733428ca9ef8096b18bce256634811ddf81f2119274	Yes	Yes	Yes	Yes	yes
a98e108588e31f40cdaeab1c04d0a394eb35a2e151f95fbf8a913cba6a7faa63	Yes	Yes	Yes	No	Yes
2d88db4098a72cd9cb58a760e6a019f6e1587b7b03d4f074c979e776ce110403	Yes	Yes	Yes	Yes	Yes
a4b705baac8bb2c0d2bc111eae9735fb8586d6d1dab050f3c89fb12589470969	Yes	No	Yes	Yes	Yes
b7c6b82a8074737fb35adccddf63abeca71573fe759bd6937cd36af5658af864	No	Yes	Yes	Yes	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Lazarus APT Threat Actor Group deployed new malware Vyveva in their latest cyberespionage campaigns striking South African freight logistics company

Severity: Critical

Date: April 09, 2021

DOMAINS

4bjt2rceijktwedi[.]onion

cwwpxpxuswo7b6tr[.]onion

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Ensure Microsoft Windows Workstations, Microsoft Exchange Server and Microsoft IIS Server are updated with latest security patches.
3. Do not click on links or download untrusted email attachments coming from unknown email addresses.
4. Ensure Domain Accounts follows least privilege principle and ensure Two-Factor authentication is enabled on all Business Email Accounts.
5. Ensure to enforce Two-Factor authentication for VPN clients, prior to connecting to Organization's Resources through VPN tunnel.
6. Enable User Account Control (UAC) to mitigate the impact of malware.
7. Keep all systems and software updated to latest patched versions.
8. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
9. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from internet facing cloud or on-premise IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.
10. Limit unnecessary lateral communications between network hoses, segments, and devices.
11. Ensure data backup is done periodically and ensure data backups are done via out-of-band network onto the server with limited or no internet access.
12. Ensure to monitor suspicious activity or intrusion through SIEM solution.

READ

- (Are you) afreight of the dark? Watch out for Vyveva, new Lazarus backdoor

HASH (SHA1)

HASHES (SHA1)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
92F5469DBEFDCEE1343934BE149AFC1241CC8497	No	No	No	No	No
DAD50AD3682A3F20B2F35BE2A94B89E2B1A73067	No	No	No	No	No
69529EED679B0C7F1ACC1FD782A4B443CEC0CF83	No	No	No	No	No
043ADDFB93A10D187DDE4999D78096077F26E9FD	N0	No	No	No	No
1E3785FC4FE5AB8DAB31DDDD68257F9A7FC5BF59	No	No	No	No	No
4D7ADD8145CB096359EBC3E4D44E19C2735E0377	no	No	No	No	No

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Lazarus APT Threat Actor Group deployed new malware Vyveva in their latest cyberespionage campaigns striking South African freight logistics company

Severity: Critical

Date: April 09, 2021

HASH (SHA1)

HASHES (SHA1)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
A5CE1DF767C89BF29D40DC4FA6EAECC9C8979552	No	No	No	No	No
66D17344A7CE55D05A324E1C6BE2ECD817E72680	No	No	No	No	No

HASH (SHA-256)

HASH (SHA-256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
1ac66a1de8cbbfa5748b2fb3cb0926e9a5f880d3062adc39c44752537e82bca0	Yes	Yes	Yes	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Iranian Threat Actor Group APT34 unleashed a new backdoor variant, SideTwist, in their latest cyberespionage campaigns

Severity: Critical

Date: April 09, 2021

DOMAINS

sarmsoftware[.]com

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 download/open documents pretending to be regarding job opportunities delivered via unknown social media accounts.
5. Do not click on links or download untrusted email attachments coming from unknown email addresses.
6. Ensure Domain Accounts follows 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 VPN tunnel.
8. Enable User Account Control (UAC) to mitigate the impact of malware.
9. Keep all systems and software updated to latest patched versions.
10. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through Web Application Firewall (WAF).
11. Limit unnecessary lateral communications between network hoses, segments, and devices.
12. Ensure to monitor suspicious activity or intrusion through SIEM solution.

READ

- Iran's APT34 Returns with an Updated Arsenal

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
13c27e5049a7fc5a36416f2c1ae49c12438d45ce50a82a96d3f792bfdacf3dcd	Yes	No	No	No	Yes
11dae9f628d35e003d6c08669cf9f4f35ce6e00fdd376bd7579423cecfe0279c	Yes	Yes	Yes	Yes	Yes
1f47770cc42ac8805060004f203a5f537b7473a36ff41eabb746900b2fa24cc8	Yes	No	Yes	No	Yes
47d3e6c389cfdbc9cf7eb61f3051c9f4e50e30cf2d97499144e023ae87d68d5a	Yes	No	Yes	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

APT Threat Actor Groups actively exploited Directory Traversal Vulnerability (CVE-2018-13379) in Fortinet Forti OS servers to access organization networks and deploy Cring ransomware

Severity: Critical

Date: April 08, 2021

DOMAINS

yunti163[.]top

win[.]yunti163[.]top

leddger[.]online

justinstalledpanel[.]com

lf2f5a3d[.]justinstalledpanel[.]com

device-5a0b2709-e188-4a2a-b1a1-9ea453e9b241[.]remotewd[.]com

IP's

129.227.156[.]216
129.227.156[.]214
198.12.112[.]204
45.67.231[.]128

REMEDIATION

1. Block the threat indicators at their respective controls.
2. Upgrade FortiOS to latest versions 5.4.13, 5.6.13, 6.0.12, 6.2.7, 6.4.5
3. Ensure Microsoft Windows Workstations, 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. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from internet facing cloud or on-premise IT infrastructure and ensure these remote services are only allowed through VPN tunnels.
10. Ensure data backup is done periodically and ensure data backups are done via out-of-band network onto the server with limited or no internet access.
11. Limit unnecessary lateral communications between network hoses, segments, and devices.
12. Ensure to monitor suspicious activity or intrusion through SIEM solution.

READ

- New Cring ransomware deployed targeting unpatched Fortinet VPN devices
- Vulnerability in Fortigate VPN servers is exploited in Cring ransomware attacks

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
f7d270ca0f2b4d21830787431f881cd004b2eb102cc3048c6b4d69cb775511c8	No	Yes	Yes	No	yes
92bd29da3dcdc6bf90864ff36825823ebf1617ff3fea799e5a1764ca9bfccc1f	No	No	No	No	No
1a41c18bbdef02b4e182705c2c9e4471010db7e77c40ed752197f48a8cf150ba	Yes	Yes	Yes	No	Yes
0b9aa3787d62268f14d7533e93e7baa8dbdc7beaf6b53aa54e722950a5e40b13	Yes	Yes	No	No	Yes
3f14e4691b7429b25ec2950db6677df3a9b278e17f6df067d29aba129a5a7d18	Yes	No	No	No	No
21c04b9ed17c4f831b64a659bc530502f6931865cf7ad1db45b78629ec809e7e	Yes	Yes	Yes	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

APT Threat Actor Groups actively exploited Directory Traversal Vulnerability (CVE-2018-13379) in Fortinet Forti OS servers to access organization networks and deploy Cring ransomware

Severity: Critical

Date: April 08, 2021

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
eb88d6c8507c09231dfa7a63b774dcb460ed8c64804c33f42cf52ecd657d7cd4	Yes	Yes	Yes	No	Yes
0fdecd6d7d472011098746f5d8c245a9dfa0a56e9366814c5c2a29720915c89b	Yes	Yes	Yes	No	Yes
8d2f2ee24882afe11f50e3d6d9400e35fa66724b321cb9f5a246baf63cbc1788	Yes	Yes	Yes	Yes	Yes

HASH (MD5)

HASHES	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
44d5c28b36807c69104969f5fed6f63f	No	No	No	No	No

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

29th March to 4th April | Trac- ID: NII21.04.0.1

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
April 01, 2021	Ubuntu Linux	USN-4900-1: OpenEXR vulnerabilities	• Ubuntu 20.10 • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS • Ubuntu 16.04 LTS	Kindly update to fixed version
April 01, 2021	Ubuntu Linux	USN-4899-1: SpamAssassin vulnerability	• Ubuntu 20.04 LTS • Ubuntu 18.04 LTS • Ubuntu 16.04 LTS	Kindly update to fixed version

RED HAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
March 30, 2021	Red Hat JBoss Middleware	RHSA-2021:1044	• Red Hat JBoss Middleware Text Only Advisories for MIDDLEWARE 1 x86_64	Kindly update to fixed version
March 29, 2021	Red Hat Enterprise Linux	RHSA-2021:1024	• Red Hat Enterprise Linux for x86_64 8 x86_64 • Red Hat Enterprise Linux for ARM 64 8 aarch64	Kindly update to fixed version

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

29th March to 4th April | Trac- ID: NII21.04.0.1

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

ORACLE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
April 01, 2021	Oracle Linux	ELSA-2021-9150 - openssl security update	• Oracle Linux 6 (x86_64)	Kindly update to fixed version
April 01, 2021	Oracle Linux	ELSA-2021-9151 - openssl security update	▪ Oracle Linux 8 (aarch64) ▪ Oracle Linux 8 (x86_64)	Kindly update to fixed version

NETAPP

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
April 01, 2021	NetApp Products	CVE-2020-27543 Node.js Vulnerability in NetApp Products	• None of te products are affected.	Kindly update to fixed version
April 01, 2021	NetApp Products	CVE-2020-27618 GNU C Library (glibc) Vulnerability in NetApp Products	• ONTAP Select Deploy administration utility	Kindly update to fixed version