NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

March 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
A New Threat Actor group “Netbounce” that is affecting Windows, Linux, MacOS platforms with multistage infection mechanism is most likely to be utilized in more malware attacks and hacking campaigns	Critical
Dridex-related network attacks are now on the rise with the combination of Poisonous PowerShell Scripts & old Cutwail botnet back in action	Critical
The updated Emotet Banking Trojan which is one of the most resilient malware in the world, is being wildly distributed	Critical
An APT Threat Actor group “Nobelium” is found to be actively using new malware strains “GoldMax, GoldFinder, Sibot & SUNSHUTTLE” as second-stage payloads for layered persistence in SolarWinds supply-chain attack	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

A New Threat Actor group “Netbounce” that is affecting Windows, Linux, MacOS platforms with multistage infection mechanism is most likely to be utilized in more malware attacks and hacking campaigns

Severity: Critical

Date: March 12, 2021

IP’s

195.181.169[.]92
195.181.164[.]195
195.181.169[.]68
185.59.222[.]228

URL’s

hxxps://packity[.]com/setup[.]exe
hxxp://<UUID>
[.]boostfever[.]com/progwrapper[.]exe
hxxp://cdn[.]boostfever[.]com/progwrapper[.]exe
hxxps://uploadhub[.]io/manager-macos
hxxp://connect[.]netbounce[.]net/manage[.]json
hxxp://cdn[.]boostfever[.]com/ex[.]json
hxxp://newurl[.]netbounce[.]net/ex[.]json
hxxps://update[.]netbounce[.]net/check
hxxp://file[.]netbounce[.]net/p3wrapper[.]exe
hxxp://download[.]netbounce[.]net/p3wrapper[.]exe
hxxp://proxy[.]netbounce[.]net/launch[.]json
hxxp://notif[.]jumpernode[.]com/launch[.]json
hxp://download[.]jumpernode[.]com/p3[.]exe
hxp://proxy[.]jumpernode[.]com/launch[.]json
hxp://proxy[.]jumpernode[.]com/ex[.]json
hxxp://u1[.]boostfever[.]com/check
hxxp://dl[.]installcdn-aws[.]com/pwrap[.]exe
hxxps://m1[.]uptime66[.]com/fetch[.]json

REMEDIATION

1. 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 & Microsoft IIS Server are updated with the latest security patches.
4. Ensure Domain Accounts follows the least privilege principle.
5. Enable User Account Control (UAC) to mitigate the impact of malware.
6. Keep all systems and software updated to the latest patched versions.
7. Ensure to enable File Integrity Monitoring (FIM) on Microsoft Exchange Server.
8. Ensure to monitor suspicious activity or intrusion through the SIEM solution.
9. Do not click on links or download untrusted email attachments coming from unknown email addresses.

DOMAINS

netbounce[.]net
jumpernode[.]com
cdn[.]netbounce[.]net
connect[.]jumpernode[.]com
bin[.]netbounce[.]net
notif[.]jumpernode[.]com
connect[.]netbounce[.]net
download[.]jumpernode[.]com
update[.]netbounce[.]net
proxy[.]jumpernode[.]com
proxy[.]netbounce[.]net
uptime66[.]com
newurl[.]netbounce[.]net
m1[.]uptime66[.]com
file[.]netbounce[.]net
xofinity[.]com
boostfever[.]com
t1[.]xofinity[.]com
cdn[.]boostfever[.]com
uploadhub[.]io
c1[.]boostfever[.]com
Payload hosting domains:
u1[.]boostfever[.]com
applemart[.]biz
installcdn-aws[.]com
demian[.]biz
dl[.]installcdn-aws[.]com

READ

- Whitelist Me, Maybe? “Netbounce” Threat Actor Tries A Bold Approach To Evade Detection

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Dridex-related network attacks are now on the rise with the combination of Poisonous PowerShell Scripts & old Cutwail botnet back in action

Severity: Critical

Date: March 12, 2021

URL

http://updates.ms0ffice[.]net/upd20991.exe

REMEDIATION

1. 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 & Microsoft IIS Server are updated with the latest security patches.
4. Ensure Domain Accounts follows the least privilege principle.
5. Enable User Account Control (UAC) to mitigate the impact of malware.
6. Keep all systems and software updated to the latest patched versions.
7. Ensure to enable File Integrity Monitoring (FIM) on Microsoft Exchange Server.
8. Ensure to monitor suspicious activity or intrusion through the SIEM solution.
9. Do not click on links or download untrusted email attachments coming from unknown email addresses

READ

- Dridex Campaign Propelled by Cutwail Botnet and Poisonous PowerShell Scripts

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
a32cb8a2260c89b904f4e2a3ab30432ffd94d7a56a4a7ae4b3bac2d1b8a90f68	Yes	Yes	Yes	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

The updated Emotet Banking Trojan which is one of the most resilient malware in the world, is being wildly distributed

Severity: Critical

Date: March 09, 2021

IP's

5.2.136[.]90
37.46.129[.]215
70.32.89[.]105
110.172.180[.]180
132.248.38[.]158
138.197.99[.]250
152.170.79[.]100
157.245.145[.]87
161.49.84[.]2
190.55.186[.]229
190.247.139[.]101
203.157.152[.]9

REMEDIATION

1. 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 & Microsoft IIS Server are updated with the latest security patches.
4. Keep all systems and software updated to the latest patched versions.
5. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through the Web Application Firewall (WAF).
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 the Organization's Resources through a VPN tunnel.
8. Ensure that service accounts and service principals with administrative rights use high entropy secrets, like certificates, stored securely. Monitor for changes to secrets used for service accounts and service principals as part of the security monitoring program.
9. Reduce surface area by removing/disabling unused or unnecessary applications and service principals. Reduce permissions on active applications and service principals, especially application (AppOnly) permissions.
10. Follow the best practices of your identity federation technology provider in securing your SAML token signing keys.
11. Enable User Account Control (UAC) to mitigate the impact of malware.

READ

- Attack Chain Overview: Emotet in December 2020 and January 2021
- World's Most Dangerous Malware Emotet Disrupted through Global Action

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
209a975429304f771ef8a619553ffd9b8fc525a254157cbba47f8e64ec30df79	Yes	Yes	Yes	No	Yes
2a8dcfc8f1262e1c6b5f65c52cdccdbcd40ff6218f4f25f82bd3eb025593dbc0	Yes	Yes	Yes	No	Yes
2cb81a1a59df4a4fd222fbcb946db3d653185c2e79cf4d3365b430b1988d485f	Yes	Yes	Yes	Yes	Yes
36df660c8e323435d2bc7a5516adcadfbd0b220279f634725e407da9f2b9d4f5	Yes	Yes	Yes	No	Yes
3788c8a783fbbd61fa60d41b78568c095a8587db728a61bff67c3ffebfad82a4	Yes	Yes	Yes	Yes	Yes
704759a244e3f27481f6ad225a0e1c30ae46e411e01612d68ca76fe2fd8cee54	Yes	Yes	Yes	Yes	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

The updated Emotet Banking Trojan which is one of the most resilient malware in the world, is being wildly distributed

Severity: Critical

Date: March 09, 2021

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
7a18e87591637a8e962386b9c72aed584037a953ce7fe5ae51edba7a0ca57c1a	Yes	Yes	Yes	No	Yes
96a1fea9853e6f77d4449da325dfdb1545b905bdb7ba227d24e6a1a5f8cb3bd4	Yes	Yes	Yes	No	Yes
a9668efdb68bf251dae8623cb4f3dc8b9b7f42d77927d287633af94a72e9d1dc	Yes	Yes	Yes	Yes	Yes
fc3c1ce6491bca2b028ae8806ca84d4b9dcb577fb2551aa871ca23eca19b10f5	Yes	Yes	Yes	No	Yes
3788c8a783fbbd61fa60d41b78568c095a8587db728a61bff67c3ffebfad82a4	Yes	Yes	Yes	Yes	Yes
0a0bf0cab20ec7fb530738c4e08f8cd5062ea44c5da3d8a3e6ce0768286d4c51	Yes	Yes	Yes	Yes	Yes
2a0a1e12a8a948083abe2a0dcbf9128b8ec7f711251f399e730af6645e86d5c8	Yes	Yes	Yes	No	Yes
3b3a9517b61d2af8758e60d067c08edd397ad76b25efe1cbd393229088567002	Yes	Yes	Yes	No	Yes
3bbda08f5e15c5cb4472c6e610f2063eb68f54c0234a2197bc4633f4344ab27f	Yes	No	Yes	No	Yes
3e2fd3a5d790a0d4efe1100af08e3e2011f26416154ec11f1315db2ca6ca71bd	Yes	Yes	Yes	Yes	Yes
4eb1928c08d16a9407dbf89ad1279886379a0415bdd7760a3b2d0697f7d287c6	Yes	Yes	Yes	Yes	Yes
95bc30b35aa2d2baa80b50e970707197a26bd19d7772cbf65ff3d0300fe8e789	Yes	Yes	Yes	Yes	Yes
97c395e1bd0c35e9b8e6f9d97b470abdfdacec25e0e4e3b987e3813fb902de9f	Yes	No	Yes	No	Yes
bbb9c1b98ec307a5e84095cf491f7475964a698c90b48a9d43490a05b6ba0a79	Yes	Yes	Yes	Yes	Yes
bd1e56637bd0fe213c2c58d6bd4e6e3693416ec2f90ea29f0c68a0b91815d91a	Yes	Yes	Yes	Yes	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

An APT Threat Actor group “Nobelium” is found to be actively using new malware strains “GoldMax, GoldFinder, Sibot & SUNSHUTTLE” as second-stage payloads for layered persistence in SolarWinds supply-chain attack

Severity: Critical

Date: March 05, 2021

DOMAINS

srfnetwork[.]org
reyweb[.]com
onetechcompany [.]com
avsvmcloud[.]com

IP's

185[.]225[.]69[.]69

REMEDIATION

1. 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 & Microsoft IIS Server are updated with the latest security patches.
4. Keep all systems and software updated to the latest patched versions.
5. Kindly enable deep inspection for outbound FTP and HTTP traffic passing through the Web Application Firewall (WAF).
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 the Organization's Resources through VPN tunnel.
8. Ensure that service accounts and service principals with administrative rights use high entropy secrets, like certificates, stored securely. Monitor for changes to secrets used for service accounts and service principals as part of your security monitoring program.
9. Reduce surface area by removing/disabling unused or unnecessary applications and service principals. Reduce permissions on active applications and service principals, especially application (AppOnly) permissions.
10. Follow the best practices of your identity federation technology provider in securing your SAML token signing keys.
11. Enable User Account Control (UAC) to mitigate the impact of malware

READ

- GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM’s layered persistence
- Microsoft reveals 3 new malware strains used by SolarWinds hackers
- New SUNSHUTTLE Second-Stage Backdoor Uncovered Targeting U.S.-Based Entity; Possible Connection to UNC2452

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
70d93035b0693b0e4ef65eb7f8529e6385d698759cc5b8666a394b2136cc06eb	No	No	No	No	No
0e1f9d4d0884c68ec25dec355140ea1bab434f5ea0f86f2aade34178ff3a7d91	No	No	No	No	No
247a733048b6d5361162957f53910ad6653cdef128eb5c87c46f14e7e3e46983	No	No	No	No	No
f28491b367375f01fb9337ffc137225f4f232df4e074775dd2cc7e667394651c	No	No	No	No	No
611458206837560511cb007ab5eeb57047025c2edc0643184561a6bf451e8c2c	No	No	Yes	Yes	Yes
611458206837560511cb007ab5eeb57047025c2edc0643184561a6bf451e8c2c	No	No	Yes	No	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

1st March to 7th March | Trac- ID: NII21.03.0.2

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
March 04, 2021	Ubuntu Linux	USN-4757-2: wpa_supplicant and hostapd vulnerability	• Ubuntu 14.04 ESM	Kindly update to fixed version
March 03, 2021	Ubuntu Linux	USN-4757-1: wpa_supplicant and hostapd vulnerability	• Ubuntu 20.10 • 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 04, 2021	Red Hat Enterprise Linux	RHSA-2021:0736	• Red Hat Enterprise Linux for x86_64 8 x86_64	Kindly update to fixed version
March 04, 2021	Red Hat Enterprise Linux	RHSA-2021:0735	• 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

1st March to 7th March | Trac- ID: NII21.03.0.2

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

ORACLE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
March 05, 2021	Oracle Linux	ELSA-2021-0706 - SUMM: container tools:2.0 security update	▪ Oracle Linux 8 (aarch64) ▪ Oracle Linux 8 (x86_64)	Kindly update to fixed version
March 05, 2021	Oracle Linux	ELSA-2021-0735 - SUMM: nodejs:10 security update	▪ Oracle Linux 8 (aarch64) ▪ Oracle Linux 8 (x86_64)	Kindly update to fixed version

NETAPP

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
March 04, 2021	NetApp Products	CVE-2020-11945 Squid Vulnerability in NetApp Products	• None of te products are affected.	Kindly update to fixed version
March 04, 2021	NetApp Products	CVE-2020-16119 Linux Kernel Vulnerability in NetApp Products	• None of the products are affected.	Kindly update to fixed version