NETWORK INTELLIGENCE
Global cybersecurity provider

Digest

July 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
APT Threat Actor Group SideCopy were found targeting Indian Government personnel with new custom remote access trojans	High
Revil ransomware developers and their affiliates successfully exploited zero-day vulnerability in Kaseya VSA server resulting in supply chain attack	Critical
APT Threat Actor Group IndigoZebra were actively targeting various Central-Asia countries via ongoing spear-phishing campaign	High

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

APT Threat Actor Group SideCopy were found targeting Indian Government personnel with new custom remote access trojans

Severity: High

Date: July 12, 2021

URL

hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/css/
hxxps://londonkids[.]in/echoolz/assets/css/front/hwo/html/
hxxps://londonkids[.]in/echoolz/assets/css/front/kwy/css/
hxxps://londonkids[.]in/echoolz/assets/css/front/kwy/html5/
hxxps://londonkids[.]in/echoolz/assets/css/front/tfs/css/
hxxps://londonkids[.]in/echoolz/assets/css/front/tfs/html5/
hxxps://iiieyehealth[.]com/fonts/times/files/css/
hxxp://mfahost[.]ddns[.]net/soccer/read_cmd.php
hxxp://mfahost[.]ddns[.]net/soccer/file_scan.php
hxxp://mfahost[.]ddns[.]net/soccer/file_move.php

DOMAINS

mmfaa[.]ddns[.]net
freewindowssoftware[.]com
filehubspot[.]com
digitalfilestores[.]com
afghannewsnetwork[.]com
newsindia[.]ddns.net
mmfaa[.]ddns[.]net
vmi296708[.]contaboserver[.]net
5-135-125-106[.]cinfuserver[.]com
mailupdater[.]net
nscinfo[.]ddns[.]net
vmi192147[.]contaboserver[.]net

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. Inspect the sender email address in the header to ensure the address matches with the purported sender.
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. Use application control configured to block execution of mshta.exe if it is not required for a given system or network to prevent potential misuse by adversaries
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. Limit unnecessary lateral communications between network hosts, segments, and devices.
13. Implement unauthorized execution prevention by disabling macro scripts from Microsoft Office files, monitor and/or block inbound connections from Tor exit nodes and other anonymization services.
14. Ensure to monitor suspicious activity or intrusion through SIEM solution.

READ

- InSideCopy: How this APT continues to evolve its arsenal
- SideCopy cybercriminals use new custom Trojans in attacks against India's military

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

APT Threat Actor Group SideCopy were found targeting Indian Government personnel with new custom remote access trojans

Severity: High

Date: July 12, 2021

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
8a10797ac7f84d09cfb4cb3a6a1e75473dc81dab757c0000036a861575216e5c	No	Yes	No	Yes	Yes
124677d655b829892bfe73877ca2a2289bbf623cf404ae50f73f255866205adc	Yes	Yes	No	Yes	Yes
df542d57b80c6bb0cdfff0e009ed410e4241d91624cb7b38c1b806bd6df103d8	No	No	No	No	No
49796c18a09c100118b7d678dc76bea283a70d6ba695224db9364ff740597103	No	No	No	No	No
54759951089f44a3918e164b8bf29c8f388cfd41f9930f81b8103852947fed93	Yes	Yes	No	Yes	Yes
e16153ee38bc971c4fd94f4d35996d0ef41a33bb53d5028170da48712904a3e7	Yes	Yes	No	Yes	Yes
a55d19aabd1b56c5d583311da142314df09400b7a1eea4dcd49474524a8f879b	Yes	Yes	Yes	Yes	Yes
df47ca45bdf2f910a0ebae49d29549240066f77d0abb735cf1afe41368cb0d85	Yes	Yes	No	Yes	Yes
b74e20c912e5c1529ec73bcd89776d4f81e56663edcfaccc82ecac50e34d5284	No	Yes	No	Yes	Yes
ee58d8ecc5dce13f4eee1e6164654f82a5eb339dc3c6e023b69ea7d6df5b930f	No	No	No	Yes	No
75033494867c133e7470c348cc36da13b18aa20d13612619540a9a909aa29f4	No	No	No	No	No
75033494867c133e7470c348cc36da13b18aa20d13612619540a9a909aa29f48	No	Yes	Yes	Yes	Yes
16e153921beabc0bc5bc1b161e19afb14e39cfe9991dcd04f20a923ed1d27989	No	No	No	yes	No
1a2cf862d210f6d0b85fbf71974f3e1fbe1d637e2ef81f511ea64b55ed2423c7	Yes	Yes	Yes	Yes	Yes
5e804c0a24a5f471635bed760fee8bba15a3d69fc6ddac306ef0da364b58aa34	Yes	Yes	No	Yes	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Revil ransomware developers and their affiliates successfully exploited zero-day vulnerability in Kaseya VSA server resulting in supply chain attack

Severity: Critical

Date: July 06, 2021

FILE NAME's

c:\kworking\agent.exe
C:\kworking\agent.crt
C:\windows\mpsvc.dll
C:\windows\msmpeng.exe
C:\windows\cert.exe
/dl.asp
/cgi-bin/KUpload.dll
/userFilterTableRpt.asp
/Kaseya/WebPages/ManagedFiles/VSATicketFiles/Screenshot.jpg
/Kaseya/webpages/managedfiles/vsaticketfiles/agent.crt
/Kaseya/webpages/managedfiles/vsaticketfiles/ag

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 and Microsoft IIS Server are updated with the latest security patches.
4. Ensure Linux workstations & servers are updated with the latest security patches.
5. Ensure Oracle WebLogic server is updated with the latest security patches.
6. It is recommended that all Kaseya VSA on-premise servers remain offline until a patch is released.
7. Use the Kaseya VSA Detection Tool for analyzing systems (either VSA server or managed endpoint) and to determine whether any indicators of compromise (IOC) are present
8. Implement allow listing to limit communication with remote monitoring and management (RMM) capabilities to known IP address pairs, and or Place administrative interfaces of RMM behind a virtual private network (VPN) or a firewall on a dedicated administrative network.
9. Use Yara rules for hunting Revil ransomware activity.
10. Use the RRA security audit self-assessment tool to better understand, defend against and recover from ransomware attacks targeting IT, OT and ICS assets.
11. 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.
12. Limit unnecessary lateral communications between network hosts, segments, and devices.
13. Ensure to monitor suspicious activity or intrusion through SIEM solution.

READ

- Thousands attacked as REvil ransomware hijacks Kaseya VSA
- REvil ransomware hits 1,000+ companies in MSP supply-chain attack
- Coop supermarket closes 500 stores after Kaseya ransomware attack

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

Revil ransomware developers and their affiliates successfully exploited zero-day vulnerability in Kaseya VSA server resulting in supply chain attack

Severity: Critical

Date: July 06, 2021

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
2093c195b6c1fd6ab9e1110c13096c5fe130b75a84a27748007ae52d9e951643	Yes	Yes	No	No	No
36a71c6ac77db619e18f701be47d79306459ff1550b0c92da47b8c46e2ec0752	No	No	No	No	No
33bc14d231a4afaa18f06513766d5f69d8b88f1e697cd127d24fb4b72ad44c7a	No	No	No	No	No
8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd	Yes	Yes	Yes	No	Yes
d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e	Yes	Yes	Yes	No	Yes
e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2	Yes	Yes	Yes	No	Yes
df2d6ef0450660aaae62c429610b964949812df2da1c57646fc29aa51c3f031e	No	Yes	Yes	Yes	Yes
dc6b0e8c1e9c113f0364e1c8370060dee3fcbe25b667ddeca7623a95cd21411f	Yes	Yes	Yes	Yes	Yes
d8353cfc5e696d3ae402c7c70565c1e7f31e49bcf74a6e12e5ab044f306b4b20	Yes	Yes	Yes	Yes	Yes
d5ce6f36a06b0dc8ce8e7e2c9a53e66094c2adfc93cfac61dd09efe9ac45a75f	Yes	Yes	Yes	Yes	yes
cc0cdc6a3d843e22c98170713abf1d6ae06e8b5e34ed06ac3159adafe85e3bd6	Yes	Yes	Yes	Yes	Yes
aae6e388e774180bc3eb96dad5d5bfefd63d0eb7124d68b6991701936801f1c7	Yes	Yes	Yes	Yes	Yes
66490c59cb9630b53fa3fa7125b5c9511afde38edab4459065938c1974229ca8	Yes	Yes	Yes	No	Yes
0496ca57e387b10dfdac809de8a4e039f68e8d66535d5d19ec76d39f7d0a4402	Yes	Yes	Yes	Yes	Yes
81d0c71f8b282076cd93fb6bb5bfd3932422d033109e2c92572fc49e4abc2471	Yes	Yes	Yes	Yes	Yes

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

APT Threat Actor Group IndigoZebra were actively targeting various Central-Asia countries via ongoing spear-phishing campaign

Severity: High

Date: July 05, 2021

URL's

infodocs[.]kginfocom[.]com/gin/kw.asp
infodocs[.]kginfocom[.]com/gin/tab.asp
ousync[.]kginfocom[.]com/sync/kw.asp
uslugi[.]mahallafond[.]com/hall/kw.asp
6z98os[.]id597[.]link/css/art.asp
hwyigd[.]laccessal[.]org/news/art.asp
hwyigd[.]laccessal[.]org/news/js.asp
help[.]2019mfa[.]com/help/art.asp
m[.]usascd[.]com/uss/word.asp
ns01-mfa[.]ungov[.]org/un/art.asp
dcc[.]ungov[.]org/crss/art.asp
index[.]google-upgrade[.]com/upgrade/art.asp
mofa[.]ungov[.]org/momo/art.asp
update[.]ictdp[.]com/new/art.asp
post[.]mfa-uz[.]com/post/art.asp
cdn[.]muincxoil[.]com/cdn/js.asp
cdn[.]muincxoil[.]com/cdn/art.asp
tm[.]2019mfa[.]com/css/p_d.asp

DOMAINS

infodocs[.]kginfocom[.]com
ousync[.]kginfocom[.]com
uslugi[.]mahallafond[.]com
6z98os[.]id597[.]link
hwyigd[.]laccessal[.]org
help[.]2019mfa[.]com
m[.]usascd[.]com
ns01-mfa[.]ungov[.]org
dcc[.]ungov[.]org
index[.]google-upgrade[.]com
mofa[.]ungov[.]org
update[.]ictdp[.]com
post[.]mfa-uz[.]com
cdn[.]muincxoil[.]com
tm[.]2019mfa[.]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 the 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. Monitor DNS traffic for irregular requests & responses moving in and out of network
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. Limit unnecessary lateral communications between network hosts, segments, and devices.
13. Ensure to monitor suspicious activity or intrusion through SIEM solution.

READ

- IndigoZebra APT continues to attack Central Asia with evolving tools
- Dropbox Used to Mask Malware Movement in Cyberespionage Campaign
- IndigoZebra APT Hacking Campaign Targets the Afghan Government

NETWORK INTELLIGENCE
Global cybersecurity provider

SECURITY ADVISORY

APT Threat Actor Group IndigoZebra were actively targeting various Central-Asia countries via ongoing spear-phishing campaign

Severity: High

Date: July 05, 2021

HASH (SHA-256)

HASHES (SHA - 256)	DETECTED BY ANTIVIRUS				
	Symantec	TrendMicro	McAfee	Quick Heal	Microsoft
7bd75383dfab3948ce06a7f533870946934c87fb1c7b8035b69b4f2a166bd5b0	Yes	Yes	Yes	No	yes
295b987c8926399c063ff20d2484477fe31cd2188b604a919dbfa11d9c34b988	Yes	No	Yes	Yes	Yes
86a0761fa0f6b15d9d5342882e09992270358766d5c11ef1b8d848c7f4075c79	Yes	No	Yes	Yes	Yes
935051367363838fcadd8856e08575e740bdf8af0d2271b81e6ba4d231b3a531	Yes	Yes	Yes	Yes	No
27312973aefcfa2511573a28ff42ef12ecbfcf56db42bf4d1371b0a1f1f2732c	No	Yes	Yes	No	No
78e7c41458e1ddf336f0d2e9625abbdc0b3e86db18aee7377af5711bc927da35	Yes	Yes	No	No	No
52a53e7e250fa9faa823d26421ca8af42ac40c27bac1d5af65b452c8987cda72	Yes	Yes	Yes	No	Yes
ab1983217880dad9c0481aab5b06e1fe4b9caaf8d56d8a03bf794aca18f2e4c6	Yes	No	Yes	No	Yes
fc3cdc3932d69c05c735040245f94fafe22b79cd865bb7d23c4364a3f4e8c774	Yes	No	Yes	No	Yes
e683c86fd40eac23bc6435f479518ea5d80f90da294d5ad21d024dd7acc8a6ac	Yes	Yes	Yes	Yes	yes
c82e0a487203457026e61b77d1becb97e8e0d2d8a30ee17d1d8827f9ece87607	Yes	Yes	Yes	Yes	Yes
784cf7d224974f7e2c43cf10580c42a2521556608a5dd4a11247d09a77f5c8df	Yes	Yes	Yes	Yes	Yes
c0082f8f1e49c0805c4eaacf5cf5b99ae30eeea585fd77cbd50904927052a18c	Yes	Yes	Yes	Yes	Yes
f6942682162769091569d0129f0b77dd7176672b0e978a29416efe3d3859d0f9	Yes	No	Yes	No	Yes
c9d5dc956841e000bfd8762e2f0b48b66c79b79500e894b4efa7fb9ba17e4e9e	No	Yes	Yes	Yes	No

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

28th June to 04th July | Trac- ID: NII21.07.0.1

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

UBUNTU

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
June 30, 2021	Ubuntu Linux	USN-4905-2: X.Org X Server vulnerability	• Ubuntu 14.04 ESM	Kindly update to fixed version

RED HAT

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
June 29, 2021	Red Hat JBoss Web Server	RHSA-2021:2561	• JBoss Enterprise Web Server 5 for RHEL 8 x86_64 • JBoss Enterprise Web Server 5 for RHEL 7 x86_64	Kindly update to fixed version
June 29, 2021	Red Hat JBoss Web Server	RHSA-2021:2562	• JBoss Enterprise Web Server Text Only Advisories x86_64	Kindly update to fixed version

NETWORK INTELLIGENCE
Global cybersecurity provider

Security Patch Advisory

28th June to 04th July | Trac- ID: NII21.07.0.1

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

ORACLE

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
June 28, 2021	Oracle Linux	ELSA-2021-9335 - qemu security update	• Oracle Linux 7 (aarch64) ▪ Oracle Linux 7 (x86_64)	Kindly update to fixed version
June 29, 2021	Oracle Linux	ELSA-2021-9329 - docker-engine docker-cli security update	• Oracle Linux 7 (x86_64)	Kindly update to fixed version

NETAPP

	TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
June 29, 2021	NetApp Products	CVE-2019-25044 Linux Kernel Vulnerability in NetApp Products	• NetApp SolidFire & HCI Management Node	Kindly update to fixed version
June 29, 2021	NetApp Products	CVE-2019-4588 IBM DB2 Vulnerability in NetApp Product	• None of the products are affected.	Kindly update to fixed version