BreakPoint Labs - Blog

breakpoint-labs.com/blog/cobalt-strike-and-ransomware-tracking-an-effective-ransomware-campaign/

August 31, 2021

Cobalt Strike and Ransomware – Tracking An Effective Ransomware Campaign

Posted on August 31st, 2021

During the course of multiple incident response engagements, we encountered a persistent, unknown ransomware threat group utilizing an obfuscated Golang encryptor [1]. It is believed that the threat actors gained initial access through one or more SonicWall exploits [2], [3]. We can confirm prior sightings that Cobalt Strike was used by these threat actors to further gain access to exploit victim networks. In this blog, we will highlight previously unreported infrastructure that is managed by this unknown threat group.

Indicators of Compromise

Victims are presented with the following ransom note:

```
Hello dear user!

Unfortunately, your files have been encrypted and attackers are taking over 300
GB of your personal data, financial reports and many other documents.

Do not try to recover files yourself, you can damage them without special
software.

We can help you recover your files and prevent your data from leaking or being
sold on the darknet.

Just contact support using the following methods and we will decrypt one non-
important file for free to convince you of our honesty.

Contact us method below:

Use TOR Browser: http://[redacted].onion/[redacted]
```

Hashes

A recent sample of the Golang packed malware was submitted to VirusTotal in mid July 2021 [4]:

MD5	864e4a109565f8d4052b959a12bfa45b
SHA-1	94388841e65c0962e56bf3e37391006d0af20bf4
SHA-256	d6f7eed7e8aeffb0683639a2c5b654d216f98a68de1528ef37685103f6e24550

Domains

The following domains have been attributed to the unknown threat group and have been observed hosting a Cobalt Strike server using TLS/SSL on non-standard ports. It is clear that these threat groups are attempting to blend in with the noise by generating seemingly legitimate domains.

3comnet.biz	cisco-network.org	group-policy.org	releases-upgrade.com
3comnet.net	cisco-updates.com	ibgp-cisco.com	repository-buster.com
advmicrodevice.com	ciscodev.org	intelfirmware.net	routeros-update.com
amibios-updater.com	code-signing.org	juniper-firmware.com	serviceupdate.net
amibios.net	dev-repository.com	juniper-vpn.net	software-repository.com
apps-update.net	dev-service.org	junipervlan.com	software-updater.net
archive-update.com	dev.updatecore.net	mikrotikfirmware.com	ubiquiti-vpn.com
archives-firmwares.com	developmentsdata.com	mikrotikvpn.net	unattended-upgrades.net
bgp-firmware.com	dlinknetwork.com	nvme-updates.com	updatepayments.net

buster-updates.com	dlp-systems.org	poweredge-update.com	veeamdata.com
cisco-cloud.net	esxi-update.net	release-update.net	vpn-updater.com

IP Addresses

The following IP addresses are related to the domains listed above and appear to be a single use.

104.129.26.226	170.130.28.35	173.232.146.43	23.226.132.245
104.129.26.28	170.130.28.37	173.232.98.16	23.94.83.123
104.129.42.67	170.130.55.16	191.101.172.24	45.227.255.15
104.149.216.58	170.130.55.160	192.154.213.119	46.161.27.19
104.223.106.239	170.130.55.32	192.154.213.122	64.188.19.20
107.150.19.211	170.130.55.97	192.154.224.52	64.188.27.154
107.150.19.72	172.245.247.67	192.3.31.17	66.154.102.222
162.218.210.152	172.245.87.3	192.3.99.71	66.154.103.212
162.218.211.139	173.232.146.185	194.165.16.98	66.154.112.36
162.245.191.153	173.232.146.218	198.23.141.117	66.63.162.170
167.160.166.12	173.232.146.39	216.244.83.66	

Am I impacted?

This threat group has been very active and if you or your organization utilized a SonicWall SMA VPN device since late 2020 or early 2021 without limited access, there is a likelihood that your organization has been compromised. If you observe any connections to the

domains listed above, it is very likely you are compromised.

What should I be doing to prevent these actors from disrupting our mission?

1. Back up (or start backing up!) all of your critical business data to an offline location. *We observed these threat actors identifying backup solutions employed by a victim and removing all backup files from an online 3rd party solution provider.*

2. Patch and upgrade your SMA devices immediately. More information can be found here: https://www.sonicwall.com/support/product-notification/urgent-security-notice-critical-risk-to-unpatched-end-of-life-sra-sma-8-x-remote-access-devices/210713105333210/

3. Review all SMA logs looking for suspicious activity – specifically looking for successful authentication attempts from non-US based IP addresses and/or IP addresses that don't originate from Internet service providers such as home or commercial ISPs.

4. Enforce multi-factor authentication for all VPN accounts.

5. Employ signatures to detect the above mentioned domains and hashes.

If you are in need of incident response support or ways to defend against this and other threats, please contact us at https://breakpoint-labs.com/.

References

[1] https://www.crowdstrike.com/blog/new-ransomware-variant-uses-golang-packer/

[2] https://us-cert.cisa.gov/ncas/current-activity/2021/07/15/ransomware-risk-unpatched-eol-sonicwall-sra-and-sma-8x-products

[3] https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001

[4] https://www.virustotal.com/gui/file/d6f7eed7e8aeffb0683639a2c5b654d216f98a68de1528ef37685103f6e24550/detection