
July 2023
Cyber Threat
Intelligence Summary
e2e
assure

Contents

In what is traditionally one of the quieter months for the industry, our challenge in bringing you this edition has been what to leave out. Speaking with colleagues across Cyber, we concurred almost unanimously that this has been one of the busiest periods for a while when thinking about newsworthy events in cyber security and technology in general.

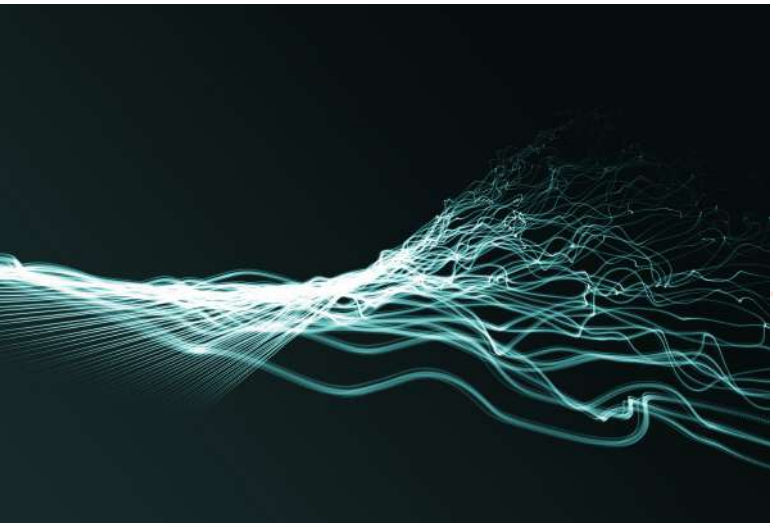
Ahead of our main features, at the time of writing there is speculation from researchers that the recent theft of Microsoft signing keys by China-attributed threat actor STORM-0558, may have much wider impact than was initially indicated. We must stress that at this stage this is unconfirmed and not being purveyors of 'FUD', we'll bring you a conclusive update in next month's edition – or not! If you really can't wait until then, industry veteran Jake Williams aka 'MalwareJake' gives his take on it here.

MOVEit.. and Moveon

The MOVEit breach has been high on the list of talking points for the last couple of months and from Cl0p's perspective, it's certainly been the gift that keeps on giving. Wary of giving them too much exposure, this is the last time we'll cover this event, however it would be remiss of us not to provide you with the latest and hopefully final events of this saga.

Source: bleepingcomputer.com

Energy giant Siemens confirmed a breach and subsequent data loss at the hands of Cl0p. The global provider of ICS, renewable energy systems and cyber security services to the energy industry, appeared on the threat actor's data leak website. With a spokesperson for the victim offering assurances that no critical data was stolen and that business operations remained unaffected.



French energy company and manufacturer of major UPS brand APC, Schneider Electric, also confirmed they had been hit with the company's most recent statement advising that they were 'investigating claims.' Having recently partnered with cyber security firm Bitsight, this would seem like the start of a busy liaison! They join American University UCLA, General Digital (the owners of anti-virus brands Norton, Avast, Avira & AVG), several American state governments and the New York City Department of Education to join the exponentially growing list of victims. The latter reported that the data of up to 45,000 students may have been compromised.

We'll keep monitoring this situation closely but hopefully we've seen the victims' list at its peak as more organisations remediate against this threat.

Crypto mining is back and it's going after Linux

Did Crypto-currency mining ever go away? After prices plummeted across the board since the highs of a few years back we certainly seem to hear less about it, apart from the occasional exchange breach. However this doesn't mean that it's fallen out of favour as a potential attack target. According to Microsoft Security and separately, the team at Palo Alto's Unit 42, the Mirai botnet malware is back with a vengeance. This time it's targeting poorly configured Linux-based systems, including where the popular operating system is embedded in IoT devices.

> .. threat actors behind the attack use a backdoor that deploys a wide array of tools and components such as rootkits and an IRC bot to steal device resources for mining operations.
>
> Rotem Sde-Or, Microsoft Threat Intelligence Community

Microsoft have released Sentinel queries for detection through their Sentinel Content Hub as well as a SSH brute force detection template which can be used in conjunction with Syslog to detect brute force attempts against exposed SSH endpoints.

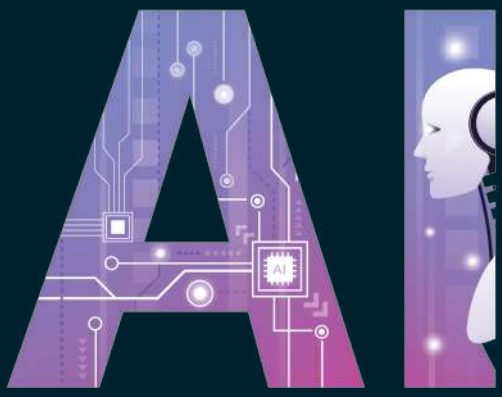
We're continuing to monitor for this activity across our protective estates and have ingested the Microsoft-supplied IOCs into our Threat Intelligence Platforms.

Following initial access via brute-force, a malicious variant of OpenSSH is deployed which in turn pulls down the rootkits 'Diamorphine' and 'Reptile' from a GitHub repo and appends two public keys into the affected devices authorized_keys config file to establish persistence. Using the modified IRC DDoS client 'ZiggyStarTux' for C2 communications is one of the final pieces of the exploit prior to the installation and enablement of Mirai.

The worm has turned – ChatWormGPT evolves

The disruptive AI technology ChatGPT has again been leveraged by cyber criminals intent on cashing in, this time with the evolution of 'WormGPT', a phishing campaign tool being advertised on underground forums as the new solution for business email compromise (BEC).

By producing grammar-perfect emails and a convincing context, the tool is capable of producing results that are worryingly convincing, even to the suspicious eyes of security professionals. Essentially this is a jailbroken version of the tooling; ChatGPT minus its anti-abuse restrictions and ethical framework, opening it up to possibilities for which its creators never intended. Following this vein, researchers at CheckPoint recently published the results of some interesting research around Google's offering in this space, 'Bard' in which they concluded that the platform had a significantly lower anti-abuse mechanism than ChatGPT and imposed almost no restrictions on the creation of phishing emails. Further still, it could be easily manipulated into creating malicious keyloggers and even rudimentary ransomware code.



As we've discussed previously in this monthly series, artificial intelligence and machine learning will continue to lower the barrier of entry for malicious activity and this will not confine itself to the cyber realm. Once accessible only to those with advanced programming skills and considerable resource, this kind of functionality enables rogue operators with little technical prowess the ability to hugely impact victim operations via a click-through web interface.

As cyber defenders we must keep abreast of this evolving landscape and capture every opportunity to level the playing field, including the reversal of the same TTPs deployed by our adversaries. One of our key strategies at e2e-assure is having a highly experienced and extremely capable, in-house development team. The complement of this team comes close to rivalling that of our operations centre, something that we believe makes us unique in the industry and provides us with a huge competitive edge when it comes to innovative practice, response capability and breaking new ground in the art of the possible.

In brief – VirusTotal leak

Google, the owner of one of the world's most popular and frequently accessed malware scanning platforms, VirusTotal was forced to issue a public apology last week in response to the admission that one of its employees had inadvertently made public a list of premium account customer names and email addresses via the platform itself. The list of over 5,000 individuals identified key personnel within strategic cyber and defence divisions of the UK & US governments including the US Cyber Command, the NSA, the Pentagon and the FBI. From the UK, defenders from the Cabinet Office, MOD, GCHQ and the National Cyber Security Centre (NCSC) were revealed. In a twist that will not be lost on threat actors deploying open-source reconnaissance, it was highlighted that some among these number were using public service provider email addresses from Microsoft's Hotmail, Google's Gmail service and even Yahoo.

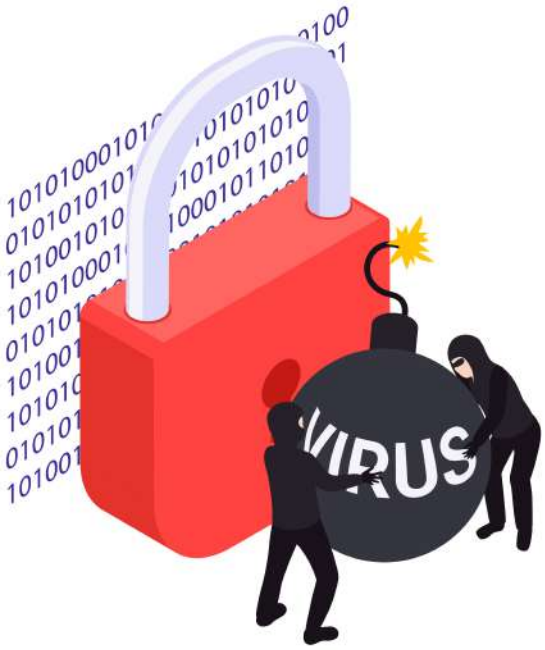
Google affirmed that this was not being treated as malicious and did not relate to a breach, citing a simple case of human error. Reports via threat intelligence organisation RecordedFuture, quoted statements from the UK's MOD, NCSC and the Nuclear Decommissioning Authority which appeared to downplay the incident and indicate that it was being treated as low risk.

'VOLT TYPHOON'

In one of our earliest monthly briefings, we looked at a technique called 'Living Off the Land' or 'LOtL' which describes the practice of a threat actor operating under the radar on a victim machine by making use of legitimate, often operating system-level, tooling available to them on the device. This is a primary TTP and modus operandi of a state-sponsored and highly skilled threat actor attributed to China, known for some time as VANGUARD PANDA and less frequently BRONZE SILHOUETTE, who have achieved prominence most recently under the moniker assigned to them from Microsoft's revised threat actor naming convention, that of VOLT TYPHOON.

By using a command shell on the Microsoft Windows operating system, the threat actor will initially run the unprivileged command:

```
'cmd.exe /C "wmic path win32_logicaldisk
getcaption,filesystem,freespace,size,volumen
ame'
```



To gain information about the system before moving to extract the system password files, and registry hive (via it's shadow copy) in order to perform offline cracking. By using the Powershell command:

'Get-EventLog security -instanceid 4624'

the threat actor enumerates successful logins to the target machine and begins to collect associated user account and host information by running the in-built Windows commands:

arp, ipconfig, net, netsh, wmic and reg

among others to determine the architecture, security posture and wider environment of the victim machine.

Identifying opportunities for further credential theft and then exploiting these by querying the registry for common applications such as OpenSSH, RealVNC and others are among their next steps before a purge of the logs takes place alongside exfiltration via a mapped network share.

Following this vein, but exploiting the different attack surface presented by consumer-grade 'home'-router devices, VOLT TYPHOON have been observed exploiting devices at scale from manufacturers such as D-Link, Netgear, Cisco and ASUS. By taking control of such devices, often in the geographical locale of their intended victim and via an attack on the SSH or HTTP exposed interface; the threat actor turns the device into an effective proxy service for malicious traffic and a jumping-off point for further attacks.

In May of this year, their activities caused enough of a stir in US circles that was sufficient to prompt CISA to release a joint threat briefing alongside all of its 'Five-Eyes' partners, warning of the threat posed by the group. This came shortly after a reported attack on an unnamed US critical national infrastructure (CNI) operator as well as repeated attacks against CNI in the Pacific region. Which some observers fear may be indicative of operations supporting a beachhead campaign amidst rising US-China tensions over Taiwan.

Mitigations – what can you do about it? This group is an 'Advanced'-APT, one of the upper echelon threat groups with strong skill sets, experience and resources, they are expert at penetrating systems and remaining undetected once there.

- Logging is critical, on your edge devices, on internal assets such as domain controllers and proxies, but critically on the endpoint. Watch out for LSASS dumping and other indicators of credential stealing by monitoring Windows log events. These should be sent to a centralised log server, preferably one that is on an isolated network segment.

- Review your firewall configurations for changes, intended or otherwise that may allow external (Internet) access to internal resources. Consider outbound connections to unusual destinations, cross-referencing with your Threat Intelligence Platform, if you have that functionality.

- Deploy 'Impossible Travel' alerting rules, available in Microsoft O365 – these rules will alert on successful logins to the same account from geographical endpoints between which is would be impossible to travel within the timeframe threshold, indicating that an unauthorised third-party has gained access to that account.

Tip – consider tuning these rules to allow for legitimate logins from geographically dispersed entities, such as a VPN provider. This may occur when one device is accessing a corporate resource via your home wifi, while another is simultaneously connected to a corporate VPN which terminates in another country.

- In modern, Enterprise editions of Windows, ensure that Credential Guard is enabled and EDR is running in block mode. Use the following queries to detect the creation of domain controller installation media (indicative of a ShadowCopy theft operation), the establishment of internal proxies and in the final example, a query that will alert on the SHA-256 hashes of custom binaries known to be deployed by VOLT TYPHOON:

- DeviceProcessEvents
| where ProcessCommandLine has_all ("ntdsutil", "create full", "pro")

- DeviceProcessEvents
| where ProcessCommandLine has_all ("portproxy", "netsh", "wmic", "process call create", "v4tov4")

```
| where SHA256 in
('baeffeb5fdef2f42a752c65c2d2a52e84fb57efc906d981f89dd518c314e231c',
'b4f7c5e3f14fb57be8b5f020377b993618b6e3532a4e1eb1eae9976d4130cc74',
'4b0c4170601d6e922cf23b1caf096bba2fade3dfcf92f0ab895a5f0b9a310349',
'c0fc29a52ec3202f71f6378d9f7f9a8a3a10eb19acb8765152d758aded98c76d',
'd6ab36cb58c6c8c3527e788fc9239d8dcc97468b6999cf9ccd8a815c8b4a80af',
'9dd101caee49c692e5df193b236f8d52a07a2030eed9bd858ed3aaccb406401a',
'450437d49a7e5530c6fb04df2e56c3ab1553ada3712fab02bd1eeb1f1adbc267',
'93ce3b6d2a18829c0212542751b309dacbdc8c1d950611efe2319aa715f3a066',
'7939f67375e6b14dfa45ec70356e91823d12f28bbd84278992b99e0d2c12ace5',
'389a497f27e1dd7484325e8e02bbdf656d53d5cf2601514e9b8d8974befddf61',
'c4b185dbca490a7f93bc96eefb9a597684fdf532d5a04aa4d9b4d4b1552c283b',
'e453e6efc5a002709057d8648dbe9998a49b9a12291dee390bb61c98a58b6e95',
'6036390a2c81301a23c9452288e39cb34e577483d121711b6ba6230b29a3c9ff',
'cd69e8a25a07318b153e01bba74a1ae60f8fc28eb3d56078f448461400baa984',
'17506c2246551d401c43726bdaec800f8d41595d01311cf38a19140ad32da2f4',
'8fa3e8fdbaa6ab5a9c44720de4514f19182adc0c9c6001c19cf159b79c0ae9c2',
'd17317e1d5716b09cee904b8463a203dc6900d78ee2053276cc948e4f41c8295',
'472ccfb865c81704562ea95870f60c08ef00bcd2ca1d7f09352398c05be5d05d',
'3e9fc13fab3f8d8120bd01604ee50ff65a40121955a4150a6d2c007d34807642')
```

At e2e-assure, in addition to ingesting Indicators of Compromise (IOCs) relating to VOLT TYPHOON and every other known threat actor, we also regularly perform active threat hunting across all our protective estates, looking for potential bad activity, malicious artefacts and evidence of TTPs corresponding to threat activity groups.

Our Analysts and Consultant teams receive some of the best training available and often cite this activity as one of the most insightful (and their favourite!) part of the job. If you'd like to learn more about how we undertake threat hunting or track threat activity groups, stay in touch through our social media and subscribe to this monthly briefing to stay tuned.

Let's connect!

That's it for this month's edition of e2e-assure's Threat Intelligence briefing.

Thanks for reading and please drop us an email to **cti@e2e-assure.com** if you'd like to be better informed about Cyber Threat Intelligence and how we exploit these to provide the ultimate level of protection to critical mission.