

June 2023

Cyber Threat Intelligence Summary

Welcome to e2e-assure's monthly Threat Intelligence briefing. In these articles, we explore cyber security-related topics that have been prevalent in recent weeks with the aim of spreading awareness and helping you to stay protected. In this month's edition we recap on the MOVEit incident as well as looking at the 'COSMICENERGY' malware and investigate an emerging threat actor from Romania, 'Diicot'. We also re-visit the ever-present issue of Business Email Compromise (BEC) and report on a curious 0-Day exploit that appears to be targeting AV vendor Kaspersky, among others.

Contents

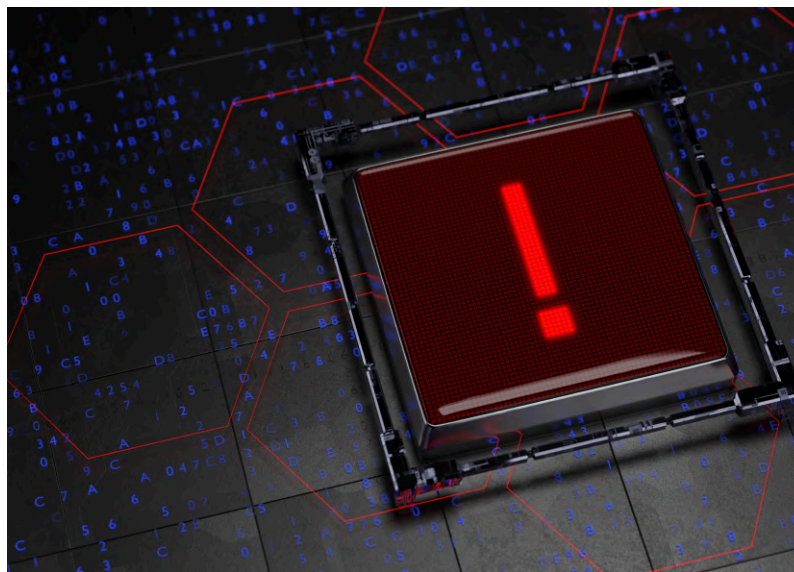
1	MOVEit – a recap and the story so far...	03
2	Operation Triangulation	04
3	'COSMICENERGY'	05
4	Re-visiting Business Email Compromise (BEC)	06
5	Diicot	07
6	Summary	08

Before we dive in, we'd like to bring you attention to an [alert](#) posted by the National Cyber Security Centre ([NCSC](#)) last week. In collaboration with their 5-Eyes and other European partners, NCSC are warning on the persisting threat from the activities of the LockBit ransomware activity group. LockBit continue to be prolific in their activity and has been identified as the most deployed Ransomware globally in 2022. For the [full advisory](#) and for the more technically-minded reader, you should click through to the full advisory on the CISA website, which gives TTPs aligned to the [MITRE ATT&CK](#) framework (v13.1) and a comprehensive history as well as numerous mitigation tips. Don't forget to also visit NCSC's '[Ransomware Hub](#)' which provides a wealth of useful information.

MOVEit – a recap and the story so far...

As we [reported](#) at the beginning of the month, Progress software announced on 31 May that they had discovered a critical SQLi vulnerability in the MOVEit file transfer product, this was supplemented a day later by Rapid7 with a statement indicating that it was being exploited in the wild and had been so for at least four days prior to the disclosure. This vulnerability has been labelled [CVE-2023-34362](#); fast-forward into the next week and the investigation ensuing from the original disclosure uncovers two more critical-rated SQLi vulnerabilities that now have the assignments [CVE-2023-35036](#) and [CVE-2023-35708](#) respectively.

Progress acted swiftly and geared up a remediate process that saw them develop and release patches to affected customers, working closely with specialist third-party organisations and opting to show transparency with regular updates and advice and a dedicated, incident email address for affected partners. Mid-way between these vulnerability disclosures came a [statement](#) from the NCSC's USA counterpart CISA, identifying the actor behind Rapid7's previous statement at the infamous CLOP Ransomware activity group, aka LACETEMPEST, DUNGEONSPIDER, TA505 and 'EvilCorp' who are major players in the Russian cyber crime scene.



CLOP confirmed the attribution in a message shared with Reuter's reporter [Raphael Satter](#) on June 5, later [shared on Twitter](#). Worldwide, the victims list so far numbers around 106, with the UK entities [including](#) the BBC, British Airways, Ernst & Young, Ofcom, Boots and Transport for London (TfL), many of whom used Zellis to manage payroll functions, who in turn used the affected software supplied by Progress. In a partial response, the US Government have placed a \$10M bounty on CLOP, offering the reward for any information leading to a conviction, however given the international element and the state of current relations with Russia, we feel this is optimistic at best. There has yet to be any significant developments from the threat actor with regard to the stolen data;



we maintain a watching brief and will bring you further developments as they occur. Over the course of this intrusion e2e-assure have curated and vetted a comprehensive list of relevant IOCs and TTPs which we have been sharing with our customers via our bespoke Cumulo platform. If you'd like access to this data or to know more about the ways in which we can help you stay protected, please get in touch today!

Operation Triangulation

At the beginning of the month, researchers from Kaspersky reported that they had detected an attack chain utilising 'zero-click' functionality, targeting Apple's iOS operating system on devices worldwide, including its own. The attack, which Kaspersky say is ongoing and could have been active since at early as 2019, involves a specially-crafted iMessage which gives an attacker full control over the device. It notes that the most recent version of iOS seemingly vulnerable is 15.7, while at the time of writing the current version is 16.5.1 .

Kaspersky have sensibly stayed away from any political attribution, however that hasn't stopped Russia's FSB accusing Apple of collusion with the NSA, stating that they had "uncovered a reconnaissance operation by American intelligence services carried out using Apple mobile devices." Apple responded with an immediate denial, with a spokesman saying "We have never worked with any government to insert a backdoor into any Apple product and never will." The FSB provided no proof of their assertions but obviously saw this as an opportunity for point-scoring too good to pass up.

Two zero-day exploits have been identified as part of the intrusion set and have been classified as [CVE-2023-32434](#) & [CVE-2023-32439](#) both of which have been addressed in recent Apple software releases – update your devices now! We think there is a lot more to come from this story and will bring you it as it develops.



'COSMICENERGY'

Renowned threat intelligence firm Mandiant released a [blog post](#) on 25 May, warning of a new OT/ICS (Operational Technology/Industrial Control System)-oriented malware discovered when a Russia-based individual uploaded a sample to VirusTotal (a rookie error, or a case of showing off new toys?) which has been named COSMICENERGY due to its alleged capabilities against components used in the supply and distribution of electricity.

Mandiant's article was very quickly followed by a number of others from across the IT press industry, who in some cases were perhaps hasty in the production of 'FUD'-sown articles, comparing the malware to 'Industroyer' and its follow-on namesake 'IndustroyerV2' which were famously deployed in anger against the Ukrainian power grid in 2016 & 2022.

At a high-level the malware contains two main components, the Python-coded 'PIEHOP' and 'LIGHTWORK' which is written in C++. PIEHOP connects to a Microsoft SQL Server and deploys LIGHTWORK to issue commands to an IEC-104 (a specific Remote Terminal Unit component) over the TCP protocol.

Except it doesn't. Both Mandiant and later Dragos noted in their reports that both modules

contain programming logic errors or incomplete code that would prevent them from working as intended, with the latter asserting that in its current form, COSMICENERGY does not pose an immediate threat to OT.

What is far more likely is that this is a red-teaming exercise tool developed by a Russian entity, for use in crisis simulation exercises, however it may be the case that an as-yet unknown threat actor has redeployed code developed for this purpose and used it to form the basis of a new malware that is still in rudimentary form.

If you're reading this any think you may be affected, there are some easy wins to be implemented that will prevent this and similar malware from executing as intended –

- Increase monitoring on all MS SQL hosts, ensuring these are sent to a monitored solution
- Restrict access to TCP/1433 on MS SQL servers and TCP/2404 on IEC-104 RTUs
- Ensure that explicit firewall rules control the above traffic, between named endpoints



At e2e-assure we have colleagues specially trained in the cyber-defence of ICS environments, set up a call with us to better understand how we are able to help keep you protected in these environments.

Carpet-Bombing - DDoS evolves

Microsoft's Digital Crimes Unit have recently released updates highlighting that this practice continues unabated, with a 38% increase in the three year period ending May 2022, with adjusted losses of \$2.7Bn in the final year alone, according to the FBI. Microsoft specifically observes a trend in attackers utilising Cybercrime-as-a-service (CaaS) platforms such as BulletProftLink which provides a premium, turnkey solution that comprises templates, hosting and automation services. The attacker pays a fee, hits 'Go' and in return receives the credentials and IP address of their victim.

A novel feature of this platform is the ability to purchase IP address space aligned with the victim's geographical locale; the advantages to this are two-fold, aside from the obvious fact that it aids the attacker in covering their tracks, it also brings the potential to avoid 'Impossible Travel' tripwires designed to flag logins in two, distinct locations where the travel between the two in the given timeframe would be impossible, without a Tardis.

Another, perhaps unique, feature of the [BulletProftLink](#) platform is their use of public blockchain nodes to host phishing sites.



The decentralised nature inherent in the designs presents new challenges to law enforcement when thinking about takeover and takedown operations.

Top targets for BEC activities remain C-Suite executives, Finance & HR staff and those in specific roles that may afford a greater level of access such as Sysadmins and network engineers; thankfully there are a number of measures in both the technical and human arenas that businesses can deploy in order to stay better protected:

- Implement SPF, DKIM records and a DMARC solution against your domains
- Review and strengthen policies around payroll, supplier remittance and HR functions
- Encourage staff to take verification offline with a phone-call or other 'human' verifications
- Hold regular phishing simulations and give staff the confidence to 'see it, say it'
- Talk to e2e-assure about a holistic monitoring solution that factors in all of your business processes. We have years of experience in protecting some of the most hostile operating environments and are ready to bring the benefits of this experience to your business.

Diicot

Diicot, aka Mexals are a Romanian threat actor, active since at least 2020 that cheekily take their name from the Romanian Directorate for Investigating Organized Crime and Terrorism, a national law enforcement agency tasked with tackling the rising tide of that country's cyber crime activities.

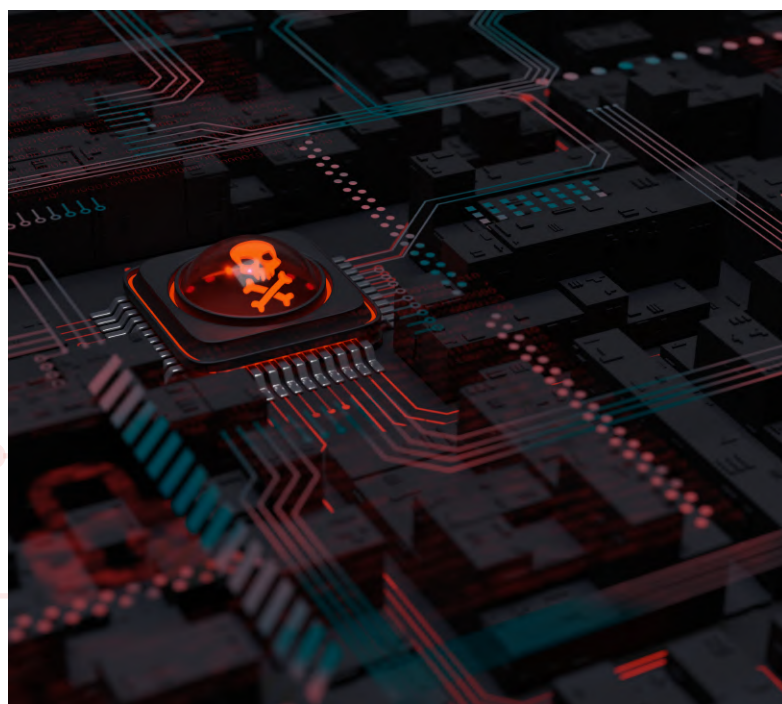


Previously known for 'Cytojacking', the practice of hijacking electronic devices to engage them in mining for cryptocurrency, the group appear to have expanded into the deployment of a Mirai-based botnet named 'Cayosin' which specifically targets routers running the highly-popular open-source OS, OpenWRT. Researchers at Cado Security in the UK has also noted the group's activities in targeting SSH servers with password authentication enabled, which is likely tied to the Cayosin deployments.

Once a system has been breached, a script is deployed to check that the device has at least

a four-core CPU before deploying the mining software XMRig. Another executable is deployed to copy over an attacker-controlled SSH key, thereby achieving persistence on the infected machine. Subsequently, lateral movement techniques are employed, using ZMap to scan the immediate network for additional victims against which SSH brute-force attacks are undertaken.

The group rely heavily on the Discord platform for their C2 infrastructure, presenting defenders with another opportunity for detection. The specific webhooks used in the activity are contained within our IOC set for this threat actor and can be shared on request. To mitigate such attacks, create explicit firewall rules that only allow SSH access to vulnerable devices from allowed endpoints, perform SSH hardening such as password-less authentication with deployed keys and preventing SSH root login completely. Talk to us for more advice!





Let's connect!

Thanks for taking the time to read our briefing, we're happy to provide further information on any of the topics we've covered here.

We love having conversations about and helping people with Cyber Threat Intelligence, drop us an email - cti@e2e-assure.com