

December 2023

Cyber Threat Intelligence Summary



Contents

1 Rhysida	03
2 ESXi Ransomware	05
3 Russia – Update	06
4 IN BRIEF	07
5 2024	08
6 Summary	09

Welcome to the final edition of 2023! It's been a whirlwind of a year since our first edition back in April, power plays on the global stage have transformed our view of the world and inevitably cyber operations have played a large part of that. We've seen governments and CNI attacked by a relentless wave of attacks from Russia, finally called out by the UK and USA governments as we'll cover later, the ongoing conflicts in Ukraine and the Middle East spawning a rise in hacktivism and Ransomware & Extortion attacks continuing exponentially and seemingly unabated.

Replacing our usual, Threat Actor 'Deep Dive' this month is a look ahead to key predictions for 2024. We've got some exciting revisions planned around threat actors for the new year, so while you may not see it this month or next, you'll have to stay tuned into the Spring to discover what new insights we're planning to share!

Before we dive in, we wanted to highlight this year's [Christmas Challenge from GCHQ](#), which if nothing else should keep the kids occupied while they wait for a large man in red to breach your perimeter defences.

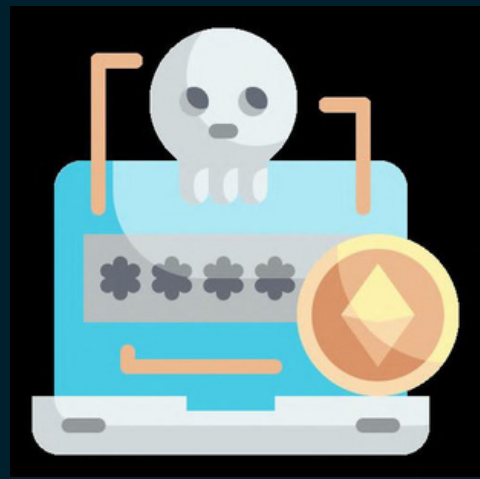
Rhysida

Since their rise to prominence in the early part of this year, Russia-attributed Rhysida (aptly named after a nightmare-inducing bug) have rapidly established themselves as a serious contender for the title of this year's most prolific ransomware operator, and certainly where the UK is concerned.

Favouring the abuse of external-facing services such as RDP and VPN endpoints, the group have also been seen to leverage phishing & more targeted spear-phishing campaigns as a way of gaining initial access and establishing persistence on victim networks. Another, current tactic of Rhysida is that of 'Living off the Land', something we've covered extensively in e2e-assure publications; in essence, this is the manipulation of legitimately installed software and operating system tooling present on the victim machine, with the aim of furthering the attacker objectives. Although not impossible to detect, this presents a challenge for defenders in separating nefarious from legitimate use. *(ProTip: Behavioural Analysis & Anomaly Detection are key here!)*



The group are also known to target virtual infrastructures and backup infrastructures and seek out credentials to support these objectives. Once this access is gained, Rhysida have been observed to specifically target .vmdk (virtual machine disk) files while simultaneously removing snapshots. Understanding that large swathes of corporate infrastructure is virtualised and attacking this as their primary objective increases their operational effectiveness while removing options for recovery. To proactively mitigate against this tactic and ransomware generally, organisations should follow the '3-2-1' rule – three dataset copies (1 x production, 2 x backup), two different medias and (at least) one offsite backup, preferably in the cloud, for ease of recovery.



To the present day, targeting appears to be favouring education, healthcare, manufacturing, information technology, and government sectors while remaining indiscriminate in other commercial areas, with multiple verticals across the globe coming under attack. In stooping to the lowest of lows, the group gained notoriety for an attack in the US on Prospect Medical Holdings which operates ambulances nationwide, followed by an attack on London's King Edward VII Hospital in late November, allegedly resulting in the exfiltration of medical PII relating to members of the UK Royal Family. Also featuring heavily in the news is the Rhysida-linked attack on the British Library, which may have passed the containment stage but appears to be very much ongoing in the eradication and recovery phases of the attack. Repeated attacks on such entities has drawn official responses including a **tri-service statement** from the USA's CISA, MS-ISAC and FBI. Our CTI team have been tracking Rhysida since their inception and have deployed layers of protection to customers including the use of applied intelligence and the sharing of vetted IOCs. While many of these remain restricted to the community, two tlp:clear artefacts that we can share with you here are email addresses associated with the group which you should be looking out for in your logs. These are: *rhysidiaeverywhere[[@onionmail.org](mailto:rhysidiaeverywhere@onionmail.org)]* and *rhysidiaofficial[[@onionmail.org](mailto:rhysidiaofficial@onionmail.org)]*, for a complete solution talk to our CTI team!



ESXi Ransomware

As evidenced by Rhysida in our previous section, ransomware that specifically targets virtual infrastructure, of which the most common is VMware's ESXi, is on the increase. From what was a proof of concept attack constrained to state-attributed actors only a small number of years ago, this tactic has ballooned to become almost commonplace in a threat actors' arsenal. According to [RecordedFuture](#) who witnessed only two such attacks in 2020, the number of attacks where ESXi ransomware featured in 2022 numbered well over a thousand, with figures for 2023 not yet available but anticipated to show a similar rise.



ALPHV, LockBit, and BlackBasta are some of the other, prominent criminal groups leveraging this tactic and with all three groups operating successful ransomware-as-a-service (RaaS) models, it's inevitable that this will only grow in popularity. The objectives appear to be gaining administrative credentials, enabling SSH and pivoting to root access to gain complete control of a system, from where the attacker has unrestricted access to not only the hypervisor but also its child virtual machines.

Understanding that this can often equate to the full, corporate environment is key to acknowledging why this has become such a favoured process among adversaries.

Defending against such an attack requires a defence-in-depth approach as multiple layers come in to play, starting with TPM at the hardware level – if it's there, enable it and draw upon the benefits such as host attestation, driver validation and Secure Boot. Next is the hypervisor itself, ensure the management network it resides on is properly segmented from other operational networks and crucially, that of the virtual machines. Disable SSH and shell access; if the former is a necessity, strictly control IP-based access, set session timeouts and enforce key-only (password-less) authentication. Critically, enable the **VMkernel.Boot.execlnstalledOnly** setting via `esxcli` to restrict execution of binaries by the VMkernel to only those that have been packaged and signed as part of an official VMware or vendor VIB package. More information on [this](#) can be found in this VMware Docs article.

This is the technique deployed by the ALPHV affiliate ScatteredSpider with devastating effect against MGM earlier this year, encrypting over one hundred ESXi servers in the first few hours of the attack, highlighting the necessity for real-time detection and response, which in that case may have limited the scope and success of the attack. Other groups have gone further still and developed their own ransomware strains to achieve this objective, such as the Qilin group who target critical national infrastructures (CNI) and victims in the education and healthcare sectors. The practice of double-extortion seems to have become commonplace among almost all Ransomware operators in 2023, compounding the pressure placed on defenders by threatening to leak data, post-exfiltration. You can read more on this practice in [this article](#) from our friends at BleepingComputer.

Russia – Update

There has been no cessation of activity from the Bears in the East, if anything the threat from Russian-attributed or backed threat activity groups has magnified in recent months which has finally prompted statements from the UK Government and confirming what is already widely known but until this month, not formally acknowledged by those in power. On 7th December, the NCSC, NCA, Foreign & Home Secretaries along with the Deputy Prime Minister Oliver Dowden, released [this statement](#) exposing attempts by Russia's FSB intelligence service to deploy cyber operations with the intent of interference in UK politics and democratic process. The statement goes further, specifically identifying a unit called 'Centre 18' within the FSB and announcing sanctions in conjunction with the US State Department, against two individuals serving within that department. Ruslan Aleksandrovich Peretyatko and Andrey Stanislavovich Korinets are accused of additionally being members of well known threat activity group 'STARBLIZZARD' aka 'Callisto' which itself is purported to be under the direct control of Centre 18.



Supporting this statement is a [strong technical advisory](#) from the NCSC which details the group's profile and methodologies while also helpfully providing a mapping to observed Mitre ATT&CK techniques.



Elsewhere in the world, Russian activity group 'Solntsepyok' (literal translation: Sunshine) and believed to be a pseudonym of the better known 'Sandworm' team claimed a catastrophic attack on Kyivstar, Ukraine's largest mobile operator, rendering its network inaccessible to over 24 million users. The very real-world consequence of this was that national air raid alerts also failed, resulting in a ballistic missile attack that wounded over fifty people. While the Russian state officially denied any involvement in the attack, Solntsepyok claimed online that it had destroyed 4,000 servers, 10,000 endpoints and all cloud storage and backup solutions in the attack, which would certainly fit with Sandworm's modus operandi. Lesser Russian group Killnet also claimed responsibility for the attack, although this group has a documented history of claiming attribution to the attacks of larger groups.

Not to be outdone, or indeed mis-attributed the Ukrainian state-run Defence Intelligence Directorate (GUR) has in the last month claimed successful attacks on two Russian departments, both in the CNI space. On 23 November they released a [statement](#) confirming an intrusion against Rosaviatsia, Russia's equivalent to the CAA claiming the exfiltration of a large trove of documents without revealing any technical details. In other coup for the agency, on 12 December they revealed another successful smash & grab against the Russian Federal Tax service (FNS). According to Daryna Antoniuk, a Ukrainian freelance reporter for RecordedFuture, this was an offensive operation not dissimilar to those of Sandworm in which the Ukrainians completely destroyed core components of the Russian tax system as well as impacting a third-party database provider. These are thought to be the first operations in which the Ukrainian state has confirmed direct responsibility, historically allowing hacktivist groups to claim attribution.

Our CTI team continues to closely monitor the situation in Russia and collate the artefacts of cyber activity from this conflict and others around the world, enabling threat assessments internally and to our customers and we work closely alongside our security operations centre (SOC) to maintain the highest level of vigilance from these high-skilled threat groups.



In brief!

Your monthly round-up of the best of the rest, information we gathered that didn't make the final cut, but we feel are still worthy of a mention –

- [Tor project axes 1000s of 'malicious' relays](#)
- [NCSC submits RFC9424 to formalise 'Pyramid of Pain'](#)
- [...and gives pressies to vulnerability researchers!](#)
- [Microsoft Threat Intelligence warns of Christmas-themed phishing activity from STORM-0539](#)
- [Law firm MSP hit by Citrixbleed impacting many clients](#)
- [UK Council spends £1.1M on attack recovery and receives ICO reprimand](#)



2024...

As the year draws to a close, the rapid evolution of the cyber arena most certainly does not and with the advent of AI alone, 2024 is already shaping up to be another year of attacks, counter attacks and the innovative manipulation of software designed to action the objectives of the world's cyber operators.

For the most detailed assessment of the year ahead, we urge you to head over to LinkedIn and fully take on board **Jane Frankland's** brilliant article – **'Key Cybersecurity Trends for 2024: My Predictions'**. Jane is an award-winning cybersecurity leader, author, and women's change agent and is a key Strategic Advisor to e2e-assure's Executive Committee.



From the outset of the article, Jane makes strong and insightful statements around pivotal technologies such as Artificial Intelligence as shown in this small excerpt:

"AI and machine learning will play a significant role in driving innovation and optimising processes across industries. The proliferation of IoT devices and sensors will accelerate, allowing organisations to collect and leverage data for improved operational efficiency and real-time monitoring. As

a result, data privacy and security will remain critical concerns, leading organisations to implement robust measures and compliance frameworks to protect sensitive information and maintain trust in digital interactions."



Let's connect!

That's a wrap! As a final note of 2023, we in the CTI Team would like to thank you for your readership and along with all of our teams at e2e-assure, wish you a very happy & safe (and adversary-free) holiday period. We'll be back at the end of January 2024 with some exciting new changes and additions to the format that we're already looking forward to sharing. See you on the other side!

We welcome any feedback you have at cti@e2e-assure.com