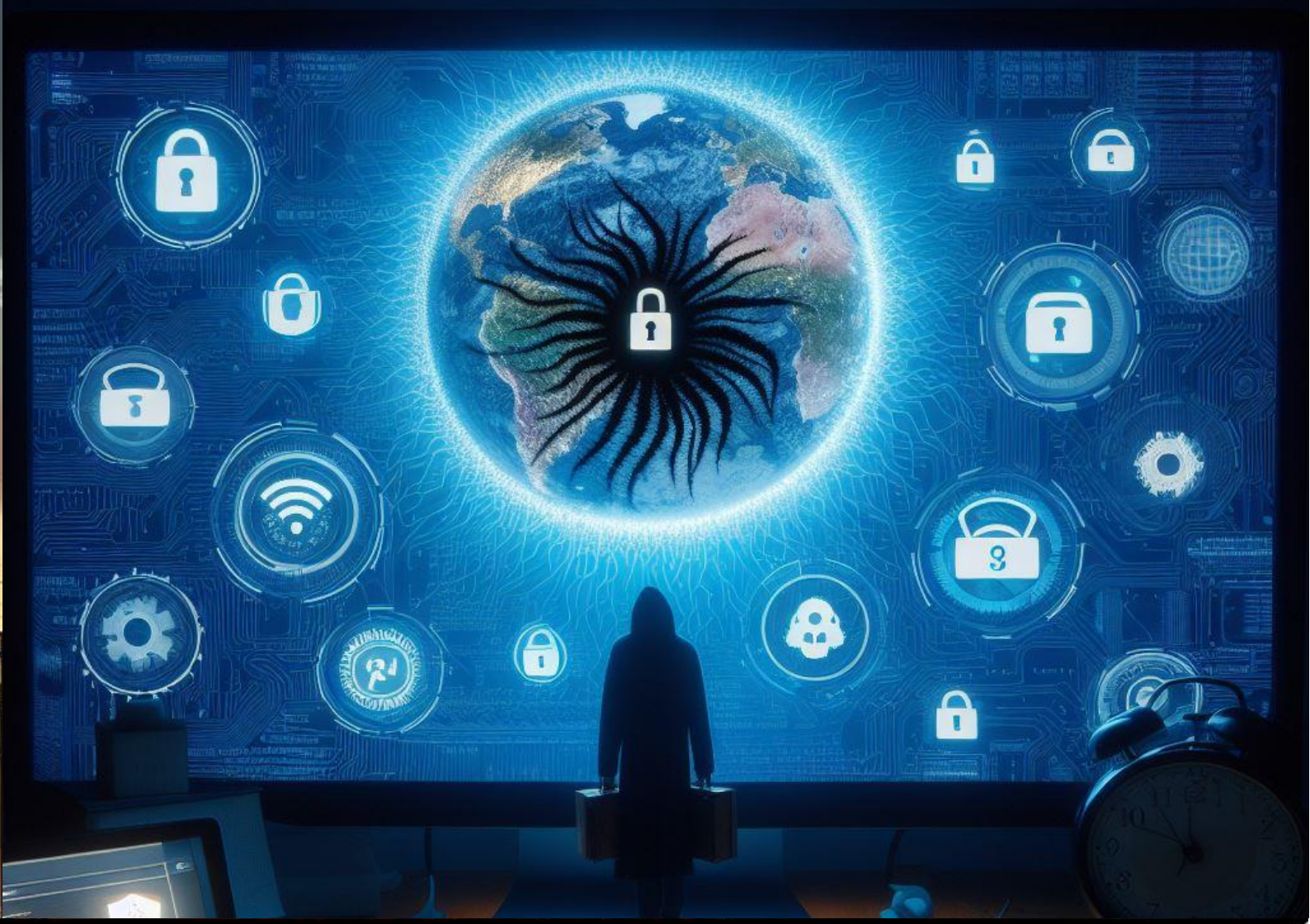


CYBER THREAT INTELLIGENCE

INTRINSEC

ThreeAM ransomware

December 2023

Website
www.intrinsec.com

Blog
www.intrinsec.com/blog

Twitter
@Intrinsec

Table of contents

Key findings

- Intrinsec's CTI analysts unveil a new extortion scheme being tested by ThreeAM via X (previously known as Twitter). Bots could have been used to automatically name and shame amongst followers of its victims' official X accounts.
- We found that the intrusion set intended to set up a dedicated leak site on the clear web.
- We successfully deanonymised the website server used by the intrusion set and found overlaps with the Russian-speaking top tier ransomware ecosystem. We assess it is likely that ThreeAM ransomware works under the wing of the reorganised Conti syndicate (Conti's former TEAM 2, now known as Royal). As shown in the literature, a relationship with Zeon members (former TEAM1) is possible.
- We found a close match with the backend infrastructure used by IcedID malware being deployed by several initial access broker (IAB) known to fuel the ransomware ecosystem such as ALPHV/BlackCat.
- The intrusion set first attempted to deploy LockBit ransomware payloads and used a new Rust-based ransomware called ThreeAM as a fallback.
- Some findings also suggest that LockBit ransomware-as-a-service could be used, in some instances, as a possible smokescreen for cyberespionage and intellectual theft operations by a couple of intrusion sets tied to Russian and Chinese intelligence (Evil Corp and Bronze Starlight, respectively).

Intrinsec's CTI services

Organisations are facing a rise in the sophistication of threat actors and intrusion sets. To address these evolving threats, it is now necessary to take a proactive approach in the detection and analysis of any element deemed malicious. Such a hands-on approach allows companies to anticipate, or at least react as quickly as possible to the compromises they face.

For this report, Intrinsec relied on its Cyber Threat Intelligence service, which provides its customers with high value-added, contextualized and actionable intelligence to understand and contain cyber threats. Our CTI team consolidates data & information gathered from our security monitoring services (SOC, MDR …), our incident response team (CERT-Intrinsec) and custom cyber intelligence generated by our analysts using custom heuristics, honeypots, hunting, reverse-engineering & pivots.

Intrinsec also offers various services around Cyber Threat Intelligence:

- Risk anticipation: which can be leveraged to continuously adapt the detection & response capabilities of our clients' existing tools (EDR, XDR, SIEM, …) through:
  - an operational feed of IOCs based on our exclusive activities.
  - threat intel notes & reports, TIP-compliant.
- Digital risk monitoring:
  - data leak detection & remediation
  - external asset security monitoring (EASM)
  - brand protection

For more information, go to https://www.intrinsec.com/cyber-threat-intelligence.

Introduction

A new ransomware self-called 3AM|ThreeAM|ThreeAMtime was unveiled by Symantec on 13 September 2023. ThreeAM is used as the last stage of a double extortion scheme. Exfiltrated data belonging to victims unwilling to pay ransoms is exposed on a dedicated leak site. Both early literature and our analysis consistently link this new family of ransomware to R&D efforts of ex-Conti members team 2, now rebranded as Royal.

Royal nexus ransomwares were one of the most prolific groups with only LockBit and BlackCat ahead of it. We assess with a low to medium confidence that, although ThreeAM intrusion sets seem to be a less sophisticated subgroup of Royal, displaying lesser operational security, it could make an impact with a high rate of attacks.

Moreover, we identified efforts in achieving new extortion vectors such as the use of X/Twitter bots in addition to the use of Rust language for its ransomware (in the wake of BlackCat/ALPHV) and seems to be a new malware family according to Symantec. These bots are employed to disclose leaked information to the victims' followers.

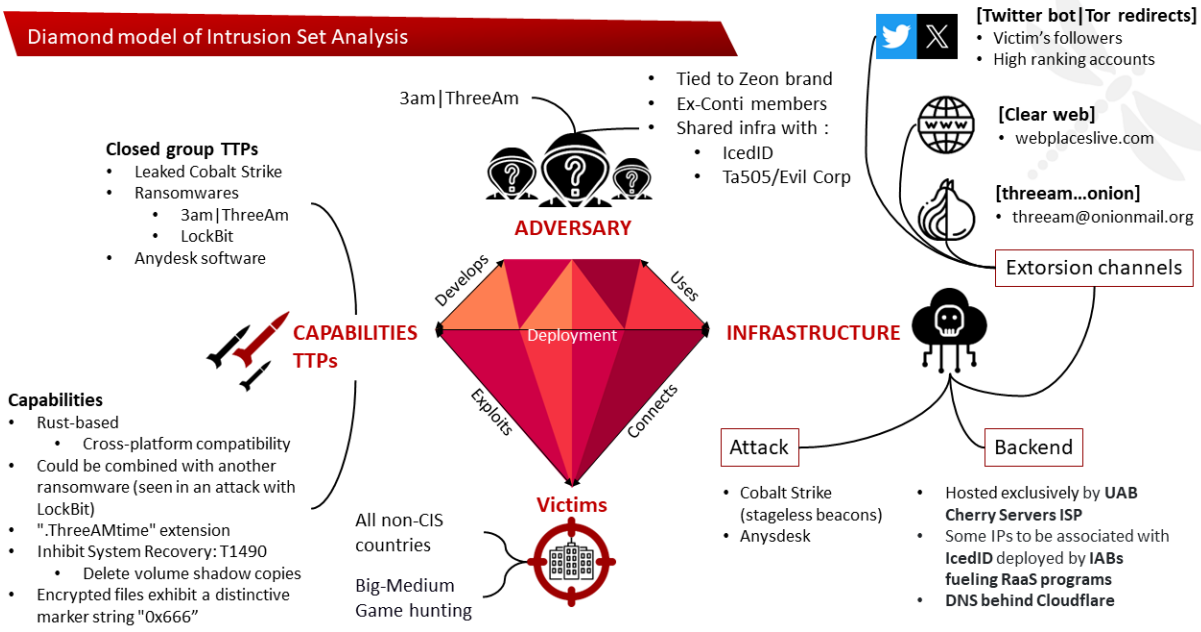


Figure 1 : Diamond model of the intrusion set analysis.

I - Strategical Intelligence

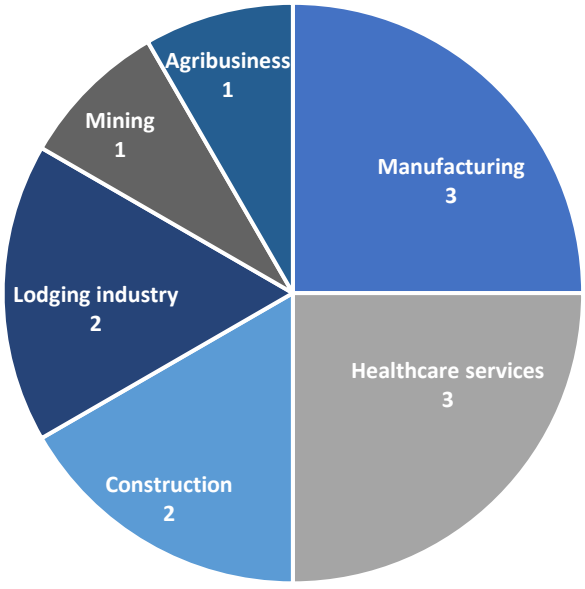
1. Victimology

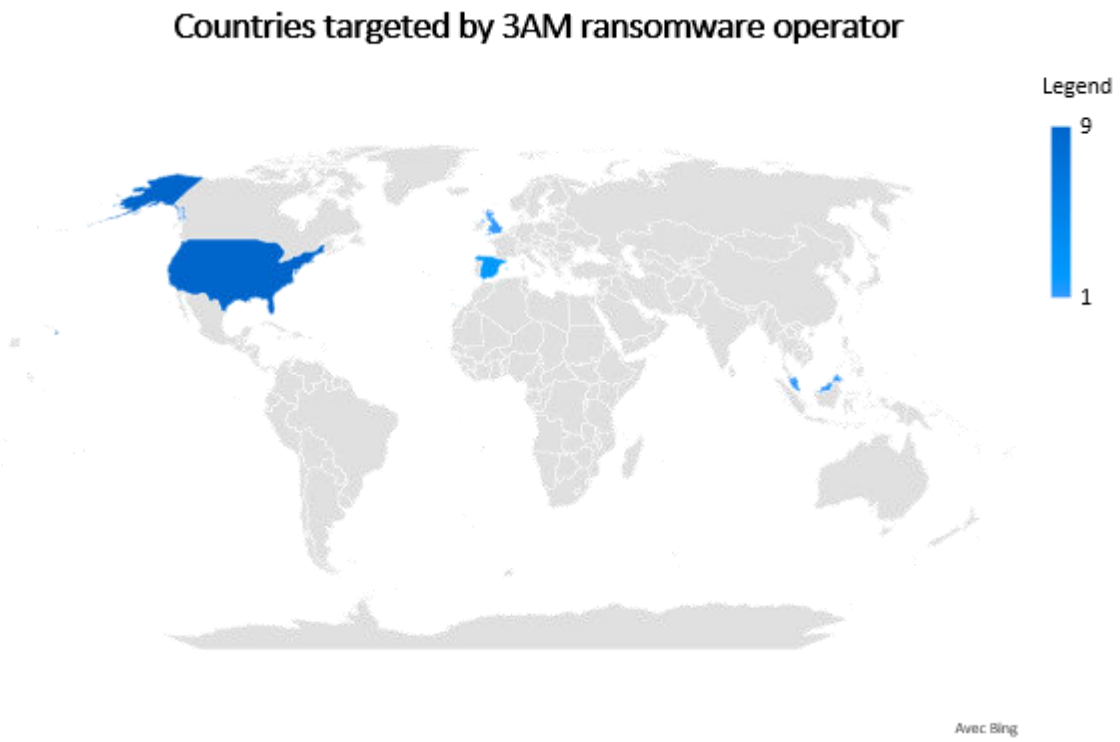
Between 13 September 2023 and 26 October 2023, ThreeAM ransomware has been detected in a dozen attacks against businesses. These companies, mainly operating in manufacturing, construction, and mining sectors, are mostly located in the United States. These sectors may be targeted by the operators of ThreeAM because victims may be deemed more likely to pay to avoid disruption of activity, financial loss and reputational damage.

By analysing the victimology from exposed victims of ThreeAM ransomware, it seems that its operators prefer to target small and medium enterprises (SME). Ten of its victims are composed of 50 employees maximum with revenues less than $5 million. In fact, SMEs' information systems are less protected because they may lack financial and human means. As opposed to SMEs, Neuraxpharm, another ThreeAM's victim, is a European leader in pharmacy and drugs manufacturing located in Spain and composed of approximately 1 000 employees. Victimology therefore appears somewhat versatile.

Though the number of exposed victims remains limited (and so the dataset), this observation is in line with ransomware tactics evolving of mid-size businesses being most impacted; organisations in the United States are the businesses most likely to be affected by ransomware (see Trellix June 2023).

Industries most targeted by 3AM ransomware





2. Attribution

2.1. What's known in the literature?

The literature provides limited information on the potentially emerging ransomware group identified as **ThreeAM|3AM**, and the available data may appear even contradictory at first glance:

- Orange CyberDefense indicated in their ransomware map that ThreeAM has similarities with **Zeon ransomware.** We found no public elements of proof
- A recent incident response from **Symantec** unveiled that an attacker switched to ThreeAM ransomware as a fallback since this intrusion set had not been able to successfully deploy **LockBit** (UNC2165:Mandiant). Moreover, conflicts on the dark web between LockBit and **Royal** leaders were recently highlighted by Analyst1

In this report we conducted an infrastructure analysis that substantiates the existence of an overlap between the ex-Conti-Ryuk-TrickBot nexus (composed of around 120 people) and the intrusion set reported by **Symantec**. We also study in this report the close relationship between the ex-Conti-Ryuk-TrickBot nexus with the so-called LockBit multinational.

2.2. A complex ecosystem

During our investigation, we found a significant overlap, not only between 'ThreeAM' communication channels and the shared infrastructure of ex Conti-Ryuk-TrickBot nexus, but also in tactics, techniques and procedures (TTPs).

The ex-Conti-Ryuk-TrickBot nexus split into smaller units seeking more mobility and evasion of law enforcement via their smaller cells. Those smaller cells kept their existing malware partnerships to get a foothold into the victim's perimeter such as Emotet, IcedID and Qakbot and developed new ones such as Bumblebee.

It is important to note that this ecosystem reused and shared old Ryuk and Conti ransomware infrastructures for Bumblebee C2 servers, as well as the IcedID botnet to deploy ransomwares.

It is argued that the core of this nexus crystallised around 'Baddie', the actual leader of Royal ransomware. Amidst such restructuring, ransomware rebrands occur and it is even more often than before the Conti leaks in May 2022 (*e.g.,* the recent follow up of Blacksuit taking over Royal RaaS program).

When the Royal ransomware was first discovered in early 2022, it utilised third-party ransomware, such as BlackCat and custom Zeon ransomwares. Since September 2022, the group has started to use its own ransomware. Royal is allegedly managed by the threat actor "Baddie", who also handles several other ransomware families.

ANALYST1 cyber threat analysts reported that according to LockBit, Maksim Yakubets (his ties to the Russian government and the FSB are detailed hereafter), is working with Baddie and Royal ransomware. Amongst all ransomwares used by Evil Corp to avoid attribution since 2017 and 2021 (BitPaymer, DoppelPaymer, WastedLocker, Hades, PhoenixLocker, PayloadBin and Macaw), one of them having the highest impact according to its wall of shame records is LockBit.

According to Mandiant, LockBit ransomware-as-a-service was adopted as a smokescreen by Evil Corp last year to evade US sanctions. In the same vein as Evil Corp, at least one Chinese state sponsored intrusion set (known as BRONZE STARLIGHT aka DEV-0401 / Storm-0401, Slime34) has adopted the same strategy. Bronze Starlight also holds strong technical overlaps with the Chinese Ministry of State Security-affiliated threat group known as APT10 (aka BRONZE RIVERSIDE).

Based on Conti leaks, Trellix furthermore revealed in March 2022 that Conti-TrickBot attempted to collaborate with the LockBit group.

In addition to infrastructure sharing, Vitali Kremez from Advintel said that some Conti's members were absorbed in the LockBit's fold.

II - Tactical Intelligence

1. Tactics, Techniques and Procedures

ThreeAM / 3AM is a rust-based ransomware publicly disclosed by Symantec. Even if rust-based variants are not mainly used by threat actors in the ransomware ecosystem, it is interesting to note that MalwareHunterTeam first observed the rust language in ransomwares when BlackCat appeared in December 2021.

The increasing adoption of Rust for ransomware development is due to its high performance and efficiency, comparable to C++, but with superior memory safety, reducing vulnerability risks. Its cross-platform compatibility (Windows, Linux, and macOS) allows targeting of diverse systems, and its relative novelty in malware development aids in evasion from traditional security detections. Additionally, Rust's growing ecosystem offers extensive resources for malware creation, while its complex syntax and language features make reverse engineering more challenging for security researchers.

In January 2022, Intrinsec's CTI team notably published a blog post on the emergence of the Rust language in malware and a focus on the ALPHV ransomware. Since this day, multiple variants using rust emerged such as RansomExx (June 2022), Hive (July 2022), Luna (ESXi) (July 2022), Nokoyama (September 2022), Zeon (October 2022) or Agenda (aka Qilin) (December 2022). Beyond ransomwares, IBM also analysed a crypter written in Rust linked to ex-Conti-TrickBot nexus (aka ITG23 for IBM).

In the Symantec report, the use of ThreeAM ransomware has been observed only once. This unique deployment came about after a threat actor unsuccessfully attempted to deploy the LockBit ransomware on the target's network. Despite being employed as a fallback option by a LockBit affiliate, the use of ThreeAM ransomware suggests potential interest from future threat actors, hinting at the likelihood of its reappearance in future cyberattacks. Moreover, it is not the first time that Symantec has seen an attacker attempt to deploy two different kinds of ransomware (Conti and Mount Locker) in a single attack. This suggests that threat actors may be seeking to acquire multiple ransomware variants to diversify their capabilities and enhance the success rate of their attacks.

The ransomware initiates its attack by attempting to halt numerous services on the infected computer before launching the encryption process. Subsequently, it strives to eradicate Volume Shadow (VSS) copies once the encryption is successfully completed with the following command "vssadmin[.]exe delete shadows /all /quiet".

During the encryption process, the ThreeAM ransomware adds the ".ThreeAMtime" extension to the encrypted files. Furthermore, the ransom note specifically references ThreeAM.

Upon execution, the malware endeavours to execute a series of commands, primarily aimed at disabling various security and backup-related software on the compromised system. Following a disk scan, the ransomware identifies and encrypts files meeting predefined criteria, subsequently deleting the original files in the process. It could be useful to know that the encrypted files exhibit a distinctive marker string, "0x666" followed by data appended by the ransomware.

2. Infrastructure analysis

Our analysis started after we discovered that the ThreeAM's blog html content (known to be accessible via Tor) could be found on Shodan. More specifically, this html is associated to the IP address 5.199.174[.]149 on port 8889 (2023/09/03).

This aforementioned IP address and port are associated to a nginx product that could be used to proxy network traffic upstream towards a genuine server.

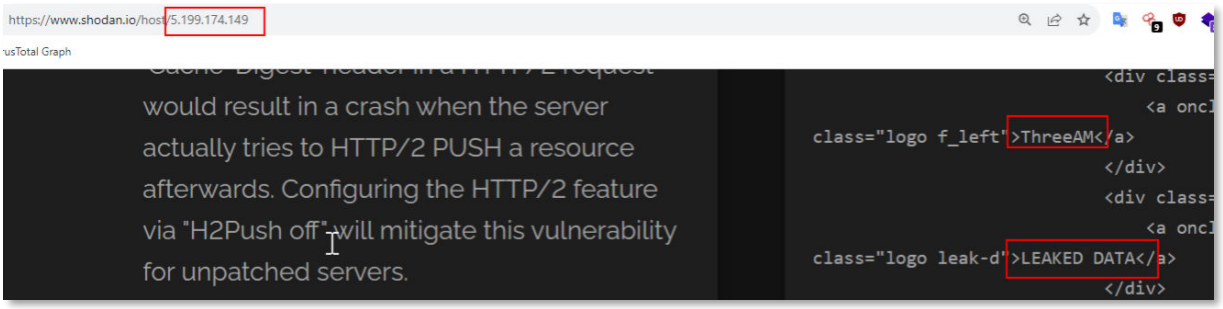


Figure 2 : On the right the HTML code hosted at the ip address 5.199.174[.]149 matching HTML code of the known Dedicated Leak Site of Threeam. The data was indexed by Shodan search engine.

The Apache httpd banner still displayed on this server redirects to Yahoo.com (see the field location hereafter):

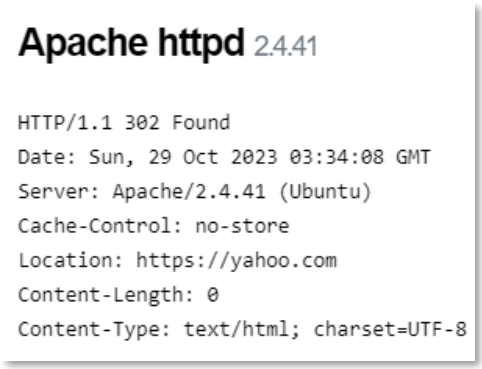


Figure 3 : Apache httpd banner found on 5.199.174[.]149 IP address

By pivoting on Shodan, we found 27 other servers with the very same Apache banner. Almost all of them are hosted by the organisation 'UAB Cherry Servers'. Amongst these servers, 6 stood out. Indeed, we observed a common pattern for these 6 IP addresses with a common port (443), protocol (TCP), product (Apache), product version (2), autonomous system (**AS16125)**, organisation as well as a common text "llc" (which stands for "limited liability company").

5.199.174.185	80 tcp	Apache httpd		2.4.41	HTTP/1.1 302 F	2023-10-21T04:50:24.081(	UAB Cherry Servers	AS16125	Apa
5.199.168.164	443 tcp	Apache httpd	buyhighappllc.com	2	HTTP/1.1 302 F	2023-10-1 buyhighappllc.cc	UAB Cherry Servers	AS16125	Apa
5.199.173.244	443 tcp	Apache httpd	buytechllc.org	2	HTTP/1.1 302 F	2023-10-1 buytechllc.org	UAB Cherry Servers	AS16125	Apa
5.199.161.14	443 tcp	Apache httpd	dating-tips-us-24x365.com	2	HTTP/1.1 302 F	2023-10-1 dating-tips-us-2(	UAB Cherry Servers	AS16125	Apa
5.199.168.79	443 tcp	Apache httpd	datings-tips-de-yamm-365x24.com	2	HTTP/1.1 302 F	2023-10-1 datings-tips-de-y	UAB Cherry Servers	AS16125	Apa
5.199.161.14	80 tcp	Apache httpd		2.4.41	HTTP/1.1 302 F	2023-10-13T22:02:49.6025	UAB Cherry Servers	AS16125	Apa
5.199.174.149	443 tcp	Apache httpd	allappllc.com	2	HTTP/1.1 302 F	2023-10-1 allappllc.com	UAB Cherry Servers	AS16125	Apa
84.32.214.13	443 tcp	Apache httpd	smart-android-online.com	2	HTTP/1.1 302 F	2023-09-2 smart-android-o	UAB Nacionalinis Telekom	AS16125	Apa
5.199.161.85	80 tcp	Apache httpd		2.4.41	HTTP/1.1 302 F	2023-09-25T19:53:09.4932	UAB Cherry Servers	AS16125	Apa
5.199.173.211	443 tcp	Apache httpd	all-app-llc.com	2	HTTP/1.1 302 F	2023-09-2 all-app-llc.com	UAB Cherry Servers	AS16125	Apa
5.199.168.236	443 tcp	Apache httpd	one-tech-llc.com	2	HTTP/1.1 302 F	2023-09-2 one-tech-llc.com	UAB Cherry Servers	AS16125	Apa
5.199.168.204	443 tcp	Apache httpd	buy-high-tech-llc.com	2	HTTP/1.1 302 F	2023-09-2 buy-high-tech-llc	UAB Cherry Servers	AS16125	Apa
5.199.173.52	443 tcp	Apache httpd	bestautotechshop.com	2	HTTP/1.1 302 F	2023-09-2 bestautotechshc	UAB Cherry Servers	AS16125	Apa
5.199.173.211	80 tcp	Apache httpd		2.4.41	HTTP/1.1 302 F	2023-09-24T21:45:09.8307	UAB Cherry Servers	AS16125	Apa
5.199.168.128	80 tcp	Apache httpd		2.4.41	HTTP/1.1 302 F	2023-09-23T23:57:55.8363	UAB Cherry Servers	AS16125	Apa

Figure 4 : XLSX export of Shodan search engine data based on the aforementioned distinctive Apache httpd. It is possible to observe a common pattern based on the port, protocol, product, product version, autonomous system, organisation, and the text "llc" in all associated domains.

Domain names resolving the IP addresses displaying the distinctive banner we found are registered with NameCheap, Inc. Those domains were secured via TLS certificates issued by **Google Trust Services LLC and transferred to Cloudflare, probably to hide IP addresses used by the attacker's servers**. The common text "**llc**" that we found in all domains associated with these IP addresses stands for limited liability company. 'LLC' permutations could be leveraged to mimic domains often encountered in the USA and thus blend into legitimate domains used by American business web structures.

In the literature, we found that Bridewell recently identified the backend infrastructure of Alphv/blackcat. This infrastructure displays several common features with the one we cover in this report:

- In both infrastructures can be found 'llc' permutations in the C2 domains (potentially for meterpreter according to Bridewell)
- Domains records point to Cloudflare
- They are both hosted on the UAB Cherry Servers ISP
- They use the same subnet of IP addresses

It is important to recall that ALPHV/BlackCat works under the wing of *Baddie* (the head of Royal as mentioned earlier). Bridewell reports that "a number of these IPs [are] associated with IcedID malware, which is deployed by a number of Initial Access brokers (IAB) and threat actors such as those deploying Emotet and using IcedID". ALPHV/BlackCat (but also Quantum: Conti Team2) was pushed in 2022 by Emotet. Proofpoint added that Emotet's operators used a 'lite' variant of IcedID with functionality dedicated only to ransomware spreading (without banking modules).

Like ALPHV/BlackCat, we assess that ThreeAM may or will be capable of deploying its ransomware via initial access gained by IcedID, itself deployed via Emotet or other IABs used by the former CONTI group. All those elements could point to a shared infrastructure providing reverse proxy features to hide the genuine infrastructure going upstream.

During our investigation, we also discovered that the name & shame ThreeAM's blog html content later pointed to another IP address **5.199.173[.]56**. This IP belongs to a subnet that is very close to the first subnet we investigated (5.199.174[.]149).

We then found the same HTML code in the web cache of Google, which suggests that ThreeAM intended to set up a clear web version of its name and shame blog. It is thus more probable that the

previous IP address 5.199.174[.]149 also pointed at the clear web DLS instead of the known one anonymised via Tor network.

Our analyst also found a self-signed trusted let's encrypt certificate displaying as domain name subject "webplaceslive.com" on the new IP address (5.199.173[.]56). The TLS certificate was then issued by **Google Trust Services LLC and transferred to Cloudflare to get protected (as seen before)**. It secures the http traffic between the internet and a WordPress CMS (version 6.1.1).

From passive DNS replication, we found that two domains out of twenty-five were flagged as malicious in the past while resolving 5.199.173[.]56. The first one wirelessrepaid626[.]com was found in Formbook configurations amongst 65 other domains. This phishing campaign associated with the id 'qq2u' occurred in July 2022.

2022-05-11	9 / 89	VirusTotal	wirelessrepaid626.com
2022-04-04	7 / 89	VirusTotal	online365-support.com

Figure 5 : Passive DNS replication from VirusTotal unveiling two domains over twenty-five being flagged as malicious in the past (around mid-2022) while resolving 5.199.173[.]56.

Trellix reported at the beginning of this year that cyberattacks targeting Ukraine increased by a 20-fold by the end of 2022, fuelled by Russia-linked Gamaredon activity. This includes phishing email campaigns and the leverage of Formbook info stealer malware or as a downloader. The massive use of Formbook is also substantiated and tracked as UAC-0041 by the CERT-UA. It was also reported by the Counterterrorism group (CTG) that UAC-0041 targeted Cert-UA via malicious documents (Excel documents) attached in phishing emails to load other malwares, such as stealers or ransomwares.

As far as the Gamaredon's infrastructure is concerned, it is interesting to note that Gamaredon also partly used "Hosted on the UAB Cherry Servers ISP".

2.1. Attacker's infrastructure

To shed light on the attack infrastructure that ThreeAM's ransomware affiliates rely upon, we pivoted on the indicators of compromise gathered upon a recent incident response.

The first IP address **85.159.229[.]62** that we investigated is hosted by the hosting infrastructure named Stark industries Solution Ltd (AS44477). We already extensively covered this infrastructure used by several cybercriminal actors in previous analysis.

By pivoting on Shodan on an associated SSL certificate displaying the field "*CN=**DESKTOP-2NFCDE2***" we were able to identify 425 other potentially malicious servers. This hostname (***DESKTOP-2NFCDE2***) is associated to a service leveraged by several malwares such as **Aurora stealer**, **RecordBreaker** stealer payload stagers, **FUDcrypter** and **njRAT** payload stager.

By pivoting on that IP address, we found that ThreeAM's intrusion set has more recently used a custom Cobalt Strike HTTP Request URI (http(s)://85.159.229[.]62/g.pixel.**ThreeAMtime**). It is worth noting

that 'ThreeAMtime' is the same extension as the one given by this ransomware to the encrypted files. "g.pixel" could be a randomly chosen prefix from a default array of strings.

According to Censys, this IP address also displayed an open 7070/TCP port where the TLS certificate issuer indicated "Anydesk". This legitimate remote access application for RDP connectivity and remote system control has been extensively used by the Conti's nexus and is mentioned in their internal procedures for persistence. The official documentation of this tool states that *"TCP Port 7070 is used for listening by default. This port is open when installing AnyDesk".* As recalled this year by the CISA, threat actors deploying Royal ransomware were often seen deploying not only Anydesk but also LogMeIn and Atera for persistence purposes.

From the IP address 185.202.0[.]111 we could find a **PowerShell script on VirusTotal** associated by the community and several Yara rules to **Cobalt Strike** (SHA256:832a3c90b047e7c5dcfd373d238d16e33e238354d9b1af673003af22f4376e4c). VirusTotal extracted additional information regarding a Cobalt Strike beacon such as embedded URLs:

Scanned	Detections	Categories	URL
2020-10-01	1 / 79	C2	http://185.202.0[.]111/updates.rss
2023-09-13	2 / 90	C2	http://185.202.0[.]111/submit.php

In its report, Symantec mentions the use of Cobalt Strike but did not mention how beacons were implanted. As such, we downloaded the PowerShell script to further investigate (see code analysis section below).

Another interesting finding was retrieved from a Shodan pivot. We observed a Socks4 service on port 8000/TCP. This service is usually used as a tunneling tool by threat actors. It is interesting to note that Cobalt Strike, once loaded onto memory, allows SOCKS proxying towards a C2 Team server listening with a SOCKS4A. The signature associated with this Socks4 service was displayed on two IP addresses showing such a proxy hallmark since mid-2022. This timeline of activity is in line with the one known for Zeon ransomware, which was observed in September 2022 according to Trend Micro but could have first spiked even earlier in late January 2022.

Figure 6 : A SOCKS4A service was found on port 8000 of one of the IP addresses shared in the analysis report of Symantec. Based on this heuristic we could discover another potential IP address of ThreeAM under the same subnet being 185.202.0[.]79 via Shodan search engine (see screenshot).

We then sought to pivot on another IP address 212.18.104[.]6 shared in the Symantec's paper. We found a service being exposed on port 5000/TCP with the html title OpenBullet2 (both correlated via Censys and Fofa). This finding is interesting because even if it is not new that threat actors leverage open source tools to automatise pentesting campaigns for credential stuffing of DDoS campaigns, the usage of OpenBullet2 is not documented (to the best of our knowledge) for top tier ransomware members and remains speculative. It is possible indeed that the legitimate web-testing software supports other types of campaigns not directly fuelling this ecosystem.

As it was the case for **85.159.229[.]62**, the IP address 212.18.104[.]6 is hosted by the rogue Stark industries Ldt infrastructure.

Once again, we found a TLS certificate associated with the RDP service signed for ''DESKTOP-TCRDU4C", which is a common name for a machine. This name is associated with other malicious activities which happened around mid-2022 according to Shodan:

- Icedid/Bazaiso (used as a precursor by Royal & BlackSuit but also XingLocker that rebranded as Quantum, Conti or REvil)
- LoBshot (associated to TA505). As a reminder, TA505 is linked to a former affiliate of the infamous Dridex botnet (with banking trojan capabilities). Dridex is known for having been operated by a group named "**Evil Corp**". TA505 is also known for having been used for initial access in big-game hunting campaigns (ransomware campaigns targeting high-value targets). Though it was for a short amount of time, TA505 was an affiliate of the TrickBot botnet (currently down). Moreover, TA505 is known for having ties with FIN11, which operates the CL0P ransomware, involved in recent landmark attacks.

Several fingerprints of Cobalt strike were found to be hosted on this same IP address. On Port 88 we found a default POST http request URI based on "Submit.php". The beacon watermark is 987654321. It also corresponds to a cracked version of the pentesting tool according to our database. For this specific version, not a lot of information is publicly available regarding intrusion sets that could have leveraged it. However Microsoft reported that 566 unique beacons were collected from their telemetry.

3. Code analysis

We investigated the PowerShell file source code. It is possible to see at first glance that the payload $s is obfuscated. The subsequent section uses the Invoke-Expression cmdlet 'iex' to execute the payload, which consists of leveraging some classes to convert a base64 encoded string to a memory stream.

```
$s=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAAOy9Wa/qSr .....[redacted]AA==

IEX (New-Object IO.StreamReader(New-Object
IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd()
```

To unveil the genuine code executed, we simply removed the IEX command to only read the stream (IEX is an alias for the Invoke-Expression cmdlet that will execute the command provided on the local machine; The new-object cmdlet creates an instance of a .NET Framework or COM object).

The code retrieves a delegate for the VirtualAlloc function and stores it in the $var_va variable so this function can be called within the PowerShell script. This method, referred to as stageless, was seen in the wild, leveraged by threat actors employing PowerSploit for DLL Injection, and by other fileless malware.

In other words, Cobalt Strike beacon is directly injected into memory using shellcode (*i.e.*, executable instructions) fooling lots of AVs/EDRs. We already encountered this same evasion technique, which was then used to deploy other ransomware families such as Cring ransomware.

These steps can be achieved Via Cobalt Strike Framework to generate a stageless Beacon as a Windows PowerShell script and then further handmade obfuscated payload to bypass AV detections. Cobalt Strike Beacon backdoor provides the attackers with remote control of the infected system. To go further in the analysis, we retrieved the code by forcing the writing of the payload into the disk.

Once it was written on the disk, we were able to analyse statically the payload. The file is about 260,6 KB in size and is a 64-bit DLL. It was compiled around 2019-12-05. It corresponds to the binary linked in VirusTotal to this URL with the SHA256 as 2b3b97a1c8875df0de7f03a2697745bf2a98668081403d57bdfd21b87c8300c0. Though, this hash is not mentioned in the Symantec's paper, we assess with low-medium confidence that it is aligned with known TTPs leveraged by offensive profiles recruited by top tier ransomware programs such as ex-Conti or LockBit and thus ThreeAM as well.

From the binary we could extract CobaltStrike Beacon's configuration key figures. Among these, we found that:

- The watermark is 305419896 (hex: 0x12345678), which means that a leaked version of Cobalt Strike was employed. This watermark is one of the most prolific ones encountered since 2020. It has been heavily used in the past by TrickBot as mentioned by Intel471 in order to deploy Ryuk, Maze, Wastedlocker (Evil Corp), etc. It could also have been employed by two Chinese state-sponsored APTs (APT41 and APT27). Its use had significantly decreased since June 2022 according to Shodan trends.
- A predefined pattern – /submit.php?id= – in the URI was found. The ID value is randomly generated from a default string array, "updates.rss".

4. Communication channels

4.1. X / Twitter

Intrinsec's CTI analysts discovered that ThreeAM leverages two communication channels on X (ex-Twitter). A dedicated account with the alias *ThreeAM1st* was indeed created 10 August 2023 (as presented below). This recently created X account has neither followers (except us) nor followers. A relationship between this account and the ransomware group was not established (publicly) to the best of our knowledge and at the time of writing.

Figure 7 : https://Twitter.com/ThreeAM1st Intrinsec discovered an X account that belongs to ThreeAM ransom group. This account is leveraged only to add pressure on new victims by amplifying the leak via the followers of the victims and official channels.

We analysed this X account of ThreeAM and its replies. During this investigation, our analysts found a tweet mentioning one of its victims named Intech, which is a full-service marketing company located in La Crosse, WI, USA. This company holds a Twitter account since 2012 with 153 followers and 1098 followers. ThreeAM chose to reply to the second-to-last tweet of this company dated 18 December 2018 at 6:53 PM as shown in the screenshot below.

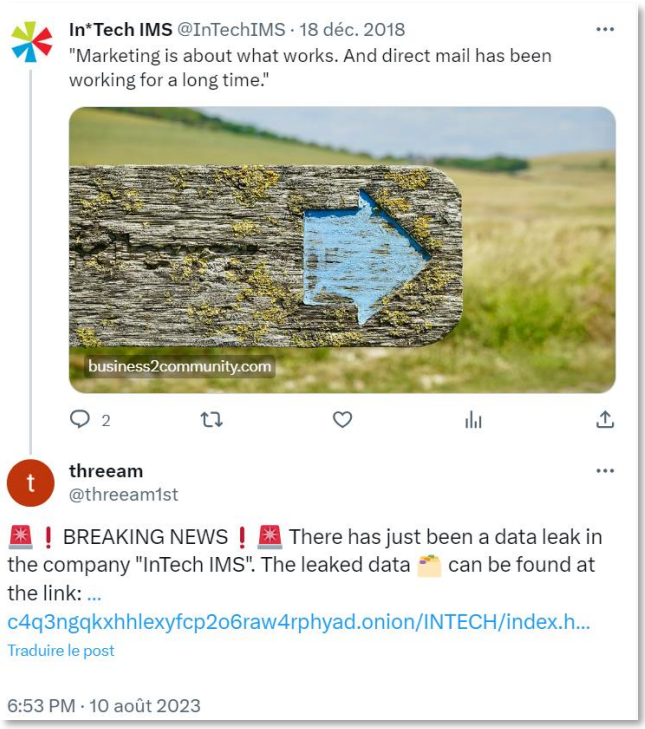


Figure 8 : A reply of the ransomware group ThreeAM was found on the X (ex-Twitter platform) account of one of its victims named INTECH IMS. Numerous replies with the same message content were found on several other accounts, naming and shaming InTech IMS to redirect to their DLS.

What we found intriguing was that it was not the first reply by ThreeAM on X regarding this victim. Indeed, the same name and shame of IN-Tech IMS was first spotted on a post of @CCQFulfillment, a US company fulfilling warehousing, distribution, cross-docking, direct mail, and printing services 5:36 PM · 10 August 2023 (not a claimed victim of ThreeAM).

An analysis of all the same name and shame posts is summarised below. It unveils that ThreeAM replied to some of the followers of the victim. More precisely we found that in total, 10 over 36 X/Twitter accounts got a reply from ThreeAM. It is important to note that since then, it is possible that some of the 26 others unfollowed IN Tech IMS. To the best of our knowledge, this strategy which has not yet been reported by the cybersecurity community, probably seeks to coerce the victims into paying the ransom or agree on paying higher ransoms.

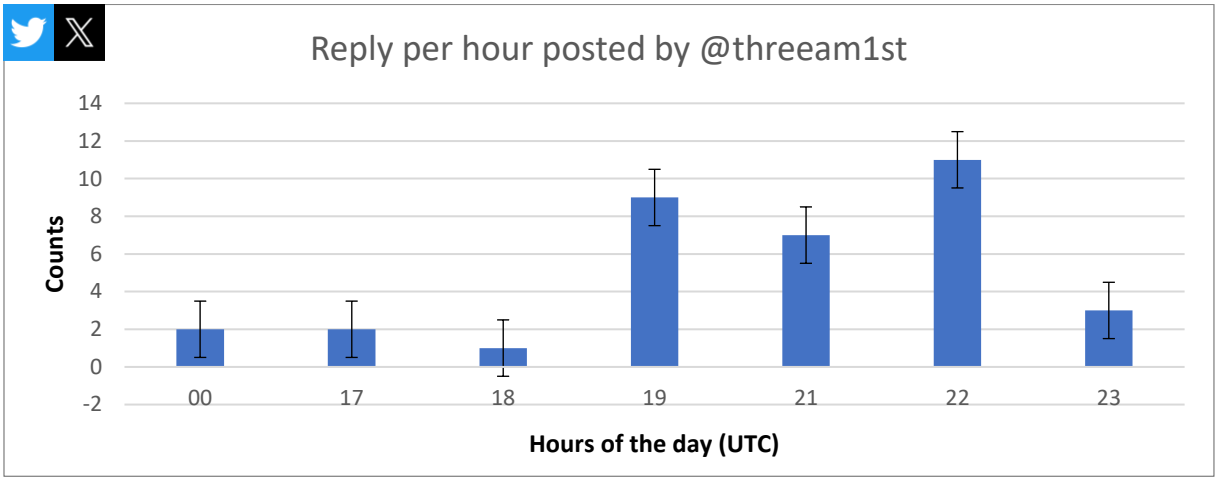


Figure 9 : Counts of the same reply observed being posted by ThreeAM on threads of (some) followers of the victim IN Tech IMS. This graph supports that the name and shame campaign on X (ex-Twitter) occurred late along August 10, 2023, from around 5p.m. until midnight. For your information, the time difference in Moscow is +1 hour.

We assess with good confidence that an X/Twitter bot was used to conduct such a name and shame campaign. This assessment is based on the following observations:

- The high frequency at which the same post was replied to numerous X-account's threads (sometimes several per minute)
- The global volume compared to a normal human use (86>50 per day)
- The after-work hours activity, since it is likely that ThreeAM operates from an eastern Russian-speaking country. It is worth noting that an analysis of the Conti leaks showed that threat actors of this ecosystem are used to working from 10 a.m. to 6 p.m. Moscow time, five days a week.

4.2. Clear & Tor ransomware websites

It is known that ThreeAm operators own an official name and shame blog hosted on a server anonymised via TOR encryption layers. This blog is leveraged in a double extorsion scheme and remains active at the time of writing this analysis.

A Google dork based on the contact email (ThreeAM@onionmail[.]org) communicated by the ThreeAM intrusion set in the ransom notes uncovered a clear web version of the anonymised version. From the Google cache, we could assess with high confidence that the html content matches with the TheeAm's victim INTECH.

At the time of writing, this website is not available. This could be due to either an unsuccessful test or a successful one and as such it will be reactivated in a near future.

Conclusion

We hope that our research helps to grasp the recent timeline and relationships between smaller cells coerced by the Conti leaks in which ThreeAm ransomware probably fits. These cells keep on going by conducting R&D to produce new ransomwares and extortion techniques.

Those smaller cells can also rely on Lockbit ransomware-as-a-service, which can be used as a smokescreen for cyberespionage.

The top tier ransomware ecosystem thus remains an impactful and fast evolving ecosystem. Proactive measures need to be adopted in order to steer clear of such threats.

III - Actionable content

1. Indicators of compromise

Value	Type	Description
079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22	SHA256	LockBit ransomware sample
307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e	SHA256	ThreeAM/3AM ransomware sample
680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4	SHA256	Cobalt Strike
991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af	SHA256	Cobalt Strike
ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc	SHA256	Cobalt Strike
832a3c90b047e7c5dcfd373d238d16e33e238354d9b1af673003af22f4376e4c	SHA256	Cobalt Strike
185.202.0[.]111	IP address	ThreeAM/3AM attack infrastructure
185.202.0[.]79	IP address	IP address with the same socks4 service found for 185.202.0[.]111 IP address
212.18.104[.]6	IP address	ThreeAM/3AM attack infrastructure
85.159.229[.]62	IP address	ThreeAM/3AM attack infrastructure
5.199.174[.]149	IP address	ThreeAM/3AM backend infrastructure (DLS)
5.199.173[.]56	IP address	ThreeAM/3AM backend infrastructure (DLS)
5.199.168[.]164	IP address	ThreeAM/3AM infrastructure
5.199.161[.]14	IP address	ThreeAM/3AM infrastructure
5.199.161[.]85	IP address	ThreeAM/3AM infrastructure
5.199.168[.]125	IP address	ThreeAM/3AM infrastructure
5.199.168[.]204	IP address	ThreeAM/3AM infrastructure
5.199.168[.]236	IP address	ThreeAM/3AM infrastructure
5.199.168[.]79	IP address	ThreeAM/3AM infrastructure
5.199.173[.]211	IP address	ThreeAM/3AM infrastructure
5.199.173[.]244	IP address	ThreeAM/3AM infrastructure
5.199.173[.]52	IP address	ThreeAM/3AM infrastructure

2. Recommendations

To prevent your organisation from being infected, Intrinsec's CTI recommends the following measures.

2.1. Detection of stageless beacon

This Yara rule could effectively be used to detect the default usage of Cobalt Strike stageless beacons. Moreover, the monitoring of the following PowerShell events should be enabled:

- **EID 4104** Script Block Logging:
  - This event can be considered noisy, so care should be taken in the detection engineering process to take account of its verbosity.
  - Script blocks exceeding the maximum length of an event log message are fragmented into multiple entries.
  - Unlike **EID 4103**, this event does not record the output of the script.
- **EID 4103 Module Logging**:
  - Generates a large volume of events.
  - Records the output of the executed commands.

2.2. To prevent initial access brokers or affiliates breaches

- Focus efforts on patching/monitoring the most impactful flaws reported in information bulletins produced by Intrinsec's CTI Team (*VMWare, CitrixBleed, etc*). Given the recent observation of LockBit's attacks targeting Citrix NetScaler VPN devices, we are providing more detailed recommendations below.
- Enable hardware MFA keys whenever possible and especially on critical assets requiring the most protection.
- Identify and document organisation's exposed assets such as VPN, RDP, web servers, etc…
- Train your teams to detect phishing & social engineering methods.
- Use a WAF to filter and monitor incoming web traffic (*N.B.,* the WAF shall always be up to date) for web servers and apps.
- Strengthen the security monitoring of Windows workstations with an EDR or at least Sysmon and a reinforced audit policy.
- Conduct vulnerability scans regularly on exposed servers to confirm whether it is vulnerable against known attack schemes.
- Reinforce perimeter filtering (email/browsing) with sandboxing for all attachments and downloaded files, plus SSL inspection.
- Maintain and regularly assess a disaster recovery plan, including global backup capabilities (onsite and offsite).
- Reinforce authentication with strong authentication means wherever possible, a password reinforcement policy, an audit in place and transmission of logs to the SIEM.
- Do not forget BYOD security management: security policy deployment and enforcement, compliancy, inventory, network access control.
- Work on detecting Cobalt Strike's capabilities and other post-exploitation framework tools.

2.3. Defend against CitrixBleed

CitrixBleed is said to have been exploited in the Lockbit attack which has targeted the US branch of the Chinese bank ICBC. CitrixBleed was also recently mentioned after Lockbit's alleged attack against BOEING. Although public conclusions of incident responses have not (yet) been made public, we assess that it is likely that Lockbit's affiliates are opportunistically exploiting this n-day vulnerability, as already observed in the past with the same or competing VPN technology. It is worth noting that since the Conti leak, some of the members of the ex-Conti-Ryuk-TrickBot nebula, known to exploit VPN technologies vulnerable to n-day vulnerabilities are suspected to have switched to LockBit (according to Vitali Kremez) in their attacks.

Recently, cybersecurity researcher Kevin Beaumont reported on a coordinated attack campaign exploiting CitrixBleed vulnerability for initial access purposes. It seems in this campaign that once the attacker has gained a foothold on the victim's network, he/she hands over this access to other teams with offensive **capabilities**. These teams then establish persistent access via remote administration tools such as LogMeIn, AnyDeks, Atera.

Remediations were shared by the CISA in a public release available here.

2.4. To detect **ThreeAM|3AM** affiliates before your data gets exfiltrated and encrypted

- Craft fake documents (financial, cyber insurance, employee data falling under GDPR) that will alert blue teams once opened, using services such as, for example, Canarytokens.
- Monitor network & system IOCs provided in this report.

2.5. To detect **ThreeAM|3AM** affiliates' data exfiltration

Ensure **RClone** detection (used by **such ecosystem** for data exfiltration) with relevant Sigma rules such as those provided here and here.

2.6. To detect **ThreeAM|3AM** affiliates' in progress encryption and reduce its impact

It is worth mentioning that an open-source tool has been recently developed by the CTO of Nextron Florian Roth for deception purposes (available on GitHub). Named "Raccine", this tool can detect and stop any Windows process trying to delete the shadow volumes on a system. Such a move can be performed by **ThreeAM|3AM's** payloads or by other similar threats.

3. Sources

- https://Twitter.com/bleepincomputer/status/1701936238888878452?s=46&t=j5mEwvRLGb4QhLYNi4_W0Q
- https://www.bridewell.com/insights/news/detail/unravelling-alphv-(blackcat)-ransomware?utm_source=Twitter&utm_medium=organicsocial&utm_term=cti&utm_content=cti-ransomware&utm_campaign=threatintelligence
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3AM-ransomware-LockBit