ALPHV ransomware gang analysis

par Admin SEC | Jan 26, 2022 | Bulletin d'analyse

Search

Rechercher

Recent Posts

China : Vulnerabilities as a strategic resource

A stalker in the box: infrastructure linking PandorahVNC and Mesh Central

The EV Code Signature Market for eCrime

Kerberos OPSEC: Offense & Detection Strategies for Red and Blue Team – Part 2 : AS_REP Roasting

Matanbuchus & Co: Code Emulation and Cybercrime Infrastructure Discovery

Archives

Sélectionner un mo

Categories

Actualités

Avis de vulnérabilité

Bulletin d'analyse

CERT

Conseil SSI

Cyber Threat Intelligence

Engineering

Evaluation Sécurité

Evenement

Recherche et Développement

Red Teaming

RSSI à temps partagé

ALPHV intends to embrace **a triple extortion scheme** by launching **DDoS** towards victims' assets if the ransom is not paid.

As far as the threat **genealogy** is concerned, **Darkweb forum analysis** allows us to conjecture that at least one actor (affiliate and/or operator and/or web developer) with recent or past ties to **Darkside/BlackMatter/REvil** decided to jump into a new **RaaS** program referred to as **ALPHV**. In addition, we found that another actor could have been somewhat involved in the **LockBit** and/or the **ALPHV RaaS program.** After pivoting from its avatar, we found with medium high confidence that the ransomware brand was inspired by a cult Russian movie where the **Black Cat** gang leaves a cat drawing or an actual cat at the scene of the crime.

Last but not least, we found a running tool being leveraged by affiliates of **ALPHV** to download and run payloads upon an attack, from a remote server, which possesses strong code overlap with the **LockBit's** running tool.

At the end of the document, we provide **actionable intelligence to strengthen relevant layers of defences** seeking to reduce or pre-empt the impact of this emerging threat.

Table of contents

- Intrusion Set
  - Description/Chronology
  - Aliases
  - Primary motivation
  - Goals
  - Targets (identify, location or vulnerability)
  - Attribution/Genealogy
- Analysis
  - Frontend and backend analysis of DLS
  - Analysis of the ransomware-as-a-service program
  - Commonalities between LockBit2.0 and ALPHV
  - TTPs
  - Malware(s)/Tool(s)
  - Vulnerabilities
  - Course of action
- References
- Appendix
  - Malware information
  - Threat actor
  - FAQ dedicated to its affiliates (published on the public DLS of ALPHV)
  - Domain analysis of the ALPHV's infrastructure

Intrusion Set

Description/Chronology

demanding a ransom that needs to be paid, otherwise threat actors publish the collected information or sell it to interested third parties.

Targets (identity, location or vulnerability)

The array below presents known victims hit by **ALPHV** ransomware; please note that it is usually an underestimated list. Upon our analysis we already found some probable victims that remained under the scope of the cybersecurity community so far. From the limited amount of data available one can highlight that, as it is commonly observed, the most targeted countries are primarily American and then European. Another common trait also emerging here is the almost indiscriminate type of sector being targeted.

Victim	Country	Sector	Date
Content available in a Private release	Romania	Heavy industries	23 January 2022
Content available in a Private release	UK	Financial organizations	18 January 2022
Content available in a Private release	Italy	Retail	17 January 2022
Content available in a Private release	United States of America	Construction	17 January 2022
Content available in a Private release	United States of America	Financial organizations	16 January 2022
Content available in a Private release	China	Heavy industries	16 January 2022
Content available in a Private release	United States of America	Heavy industries	16 January 2022

available in a Private release	Netherlands	Insurance services	01 January 2022
Content available in a Private release	Germany	Technologies	01 January 2022
Content available in a Private release	United States of America	Information technologies consulting	31 December 2021
Content available in a Private release	United States of America	Financial organizations	29 December 2021
Content available in a Private release	United States of America	Information technologies consulting	29 December 2021
Content available in a Private release	Australia	Manufacturing	29 December 2021
Content available in a Private release	United States of America	Technologies	29 December 2021
Content available in a Private release	Canada	Energy	29 December 2021
Content available in a Private release	France	Transportation Services	27 December 2021
Content			

Private release	America		2021
Content available in a Private release	France	Information technologies consulting	19 December 2021
Content available in a Private release	Germany	Transportation Services	19 December 2021
Content available in a Private release	Unknown	Unknown	17 December 2021
Content available in a Private release	Philippines	Retail	14 December 2021
Content available in a Private release	United States of America	Mining	10 December 2021
Content available in a Private release	United States of America	Engineering consulting	08 December 2021

Attribution/Genealogy

Attribution of the intrusion set is at first glance contradictory, as on one hand, according to Recorded Future experts the operator of **ALPHV** had been previously a member of the well-known ransomware group **REvil;** while on the other hand, according to the official LockBit Support account on the Russian Cybercrime forum XSS, the **ALPHV** is a rebranding of **Darkside / BlackMatter** ransomware brands (see Figure 1).

Figure 2 : *On the left, a screenshot taken on December 28, 2021 from a random channel of the Russian cybercrime Forum XSS. ALPHV operator replied to the trolling post of another user named Kelegen (on the right) claiming that the LockBit Dedicated Leak Site was pwned. The premium account 'ALPHV' was created on December 9, 2021 and has posted so far only this short message.*

An analysis from **Korean Threat Intelligence** **S2W Lab company** pinpointed that like other **RaaS** ransomgangs, a config file is leveraged as an input to endow the ransomware with custom features tailored for the victims (see Analysis for details). Of note is the strong overlap with the config file previously used by **BlackMatter**. From the timeline provided by **S2W** though, they conclude that it would have been too soon for **ALPHV** to rebrand from **BlackMatter** while rewriting from scratch a DLS (Dedicated Leak Site)and a **RUST**-based ransomware. This could substantiate at the first glance an attribution to the **REvil** ransom cartel whom first shutdown occurred in July 2021 and then was hacked and forced offline after a comeback since the end of October this year but there is too little material at the time of writing to conclude.

As far as **BlackMatter** is concerned however, technical evidences such as the encryption routine study and code similarities show that **BlackMatter** signed the come-back of **Darkside** core teams. This revival took place at the moment of **Darkside**'s disappearance following its infamous **Colonial Pipeline** major attack. We shall then recall the genesis of **Darkside,** which was born in August 2020 when pentesters first rent **REvil RaaS** (operated by **Pinchy Spider**) until **Carbon Spider** operated its own variant based on the code of **REvil** that became **Darkside**. To conclude on that first part, we thus underline past ties between **Revil** and **Darkside** as well as more recently between **Darkside** and **BlackMatter**.

As far as the ransomware code is concerned we shall underline that **BlackMatter** is a mashup between LockBit, Darkside, and REvil.

A possible scenario would be that at least one actor (affiliate and/or operator and/or web developer) with recent or past ties to **Darkside/BlackMatter/REvil** decided to jump into a new **RaaS** program referred to as **ALPHV**, but this assumption remains speculative at this stage.

From another interesting conversation on the **RAMP** forum about the withdrawal of **BlackMatter** and assumptions on their next move, an avatar named *BlackCat46* also arouse our interest (see Figure 3). Indeed, it turns out that the latter participated in the past not only in a similar conversation on the Russian cybercrime XSS forum with the same account name, but also in other topics involving the **LockBitSupp** account.

Figure 3 Screenshot taken from Russian cybercrime XSS forum, displaying that LockBit claims to know the operator of ALPHV, a former member of the infamous REvil group, and that BlackCat46 liked this assumption. Its avatar on XSS and Exploit, both major Russian-speaking cybercrime forums, represent a picture of the famous Russian revolutionary LENIN taken in Gorki where he spent the last year of his life.

This could show that the latter has a particular interest in **BlackMatter** and a kind of 'friendship' with the **LockBit** operator; at the very least, a cross-analysis of its avatar content shows a particular tropism for **RaaS** programs.

In addition to that, the most recent avatar on **RAMP** of BlackCat46 is an angry cat, which obviously reminds the free black cat icon that was chosen by **ALPHV** for private onion negotiation sites (also angry). By reverse image search analysis, we found its **RAMP** avatar on an entertainment website illustrating a 1979 cult film upon the Former Soviet Union called 'The Meeting Place Cannot Be Changed.' The plot synopsis is not without remembering what could experience members of **RaaS** programs in which a gang of armed robbers calling itself « The **Black Cat** » keeps evading capture. Even more striking is the bleeding knife website **icon** used for the crime investigation category that turns out to be the very same used on the public DLS of **ALPHV** (see Figure 4). We retrieved the link between those two observed website icons by **ALPHV** on their Private and Public DLS.

Figure 4 : On the left, the profile of BlackCat46 on RAMP forum. On the right, an illustration obtained by reverse image analysis of the BlackCat46 avatar on RAMP forum linked to a cult Russian movie where the Black Cat gang leaves a cat drawing or an actual cat at the scene of the crime. The knife icon of the website used for the crime investigation category matches the one used by ALPHV on their Public DLS.

Based on topics and conversations in which *BlackCat46* is involved, we think that his profile could fit the one of an affiliate being involved in **RaaS** program with pentesting skills. More interesting is that the latter requested help to protect against DDOS attacks on the aforementioned Russian cybercrime forum known as **'Exploit'** (with the same Lenin avatar picture and account name *BlackCat46* than

Dedicated Leak Site (DLS) while negotiation site are unique per victim. For this, a UUID is generated via the command:

cmd /c wmic csproduct get UUID

This command is used to generate an access key being required to reach the correct URL following this scheme:

hxxp://Av3TorUniqueHiddenWebAddress[.]onion/?access-key=${ACCESS_KEY} »

As far as the Public Leak Site of ALPHV is concerned, its technology relies for the frontend on **Angular**, which enhances users experience with single page applications. This extensively used open source framework is coupled to **zone.js** to reduce UI refreshing when change detection occurs.

From our experience, this web technology is not often encountered and translates good skills in terms of web developing. The web developer could be a dedicated person and not necessarily the operator maintaining in operational conditions the infrastructure. As a result, an automated survey of their Public Dedicated Leak Site (**DLS**) by CTI teams is more difficult. Fortunately we found a workaround to provide information on victims that can be ingested in an automated way:

Content available in the Private release

Concerning the backend, this group claims to have learned from other ransom-cartels' mistakes such as **Conti**, which recently saw their servers uncovered by the Prodaft Threat Intel team. Also peculiar is the generation of **a unique onion domain per each new company** hit by **ALPHV** ransomware. This change of modus operandi was most likely driven by the intention to reduce the impact of the aforementioned **DDOS** attack.

ALPHV offer an intricate affiliate program (see appendix) with self-deletion scripts, a built-in Bitcoin mixer integrated, which does not communicate with the ALPHV infrastructure backend. The latter is fragmented into nodes that are interconnected through a whole network of pads within the onion network being behind a Network Address Translation (NAT) so genuine IP addresses are not directly accessible from the internet and are protected by a firewall.

Analysis of the Ransomware-as-a-service program

Since early December 2021, the operator of **ALPHV** has been promoting its **RaaS** program on the underground Russian forums **RAMP** (see an English translation in appendix) inviting other criminals to join ransomware attacks against large companies. The operator mentioned later that only Russian speaking affiliate could join the program either by payment or by skill. It is worth mentioning though that overall, more and more Chinese translations are found on underground forums in a sort of an objective alliance between countries of Commonwealth of Independent States and China black hats against western countries. The operator claims that the malware can encrypt data on systems running Windows, Linux and VMware ESXi, and partners will receive 80% to 90% of the final ransom, depending on the total amount received from the victims.

Figure 5 : ALPHV operator named RANSOM joined the RAMP forum the 8th December, 2021 and depicted the day after its RaaS affiliate program. RAMP is a Russian-speaking underground forum that was launched in July 2021. The operator of RAMP was linked to the operator of Babuk and Payload.bin. N.B: we translated this page into English.

ALPHV operators were also seen on another underground Russian forum known as **Exploit** (see Figure 6) where they were actively recruiting pentesters specialized in Windows/Linux and ESXi. In the same post, they shared two TOX addresses and a jabber address to discuss in a secure environment.

Figure 6 : Screenshot taken from the Exploit underground forum showing the active recruiting process engaged by ALPHV to collaborate with pentesters specialized in Windows/Linux and ESXi. They shared two TOX addresses and a Jabber to discuss in a secure environment.

Focusing now on the ransomware anatomy, the latter encrypts selected files throughout a whitelist and adds custom extensions to infected files (7 length extension such as .sykffle was so far witnessed in the wild for this program and most of the time chosen randomly). A peculiar trait of this ransomware upon deployment is its ability throughout command-line to apply numerous options (reachable via –help). Available features are presented for Windows and Linux systems respectively in Figure 7 and Figure 8.

Figure 7 : Features provided by a representative sample of an ALPHV ransomware sample targeting Windows systems.

and the services and processes to be automatically killed to crank up the impact. Supplying an access token as a parameter is previously seen anti-analysis tactic such as threats like Egregor.

Figure 9 : Screenshot of a representative sample of the config file extracted from a Windows ALPHV ransomware strain. Admin credentials and the victim's name could be stored and could leak upon negotiations to the public even before being exposed on ALPHV's DLS if a payload is pushed towards a third-party platform. Several features that can be enabled or disabled make this ransomware very versatile and impactful, in particular the capability of ESXi VM and Snapshot kill.

We could extract and analyse several outputs of both Linux and Windows samples and confirm the conclusions of **S2W** (see Figure 9). Of important note is that every successful attack stores Admin credentials and the victim's name into specific fields of the config file that could become public once payloads are submitted to third-party platforms such as Virustotal (please see an obfuscated example displayed via an open-source script).

Every compiled sample analysed so far would have been compiled via the emerging **Rust** language, instead of a more commonly encountered C/C++ language. Rust is a multi-paradigm programming language, developed by Mozilla in 2010. As a matter of fact, it is the third impactful malware written in **Rust** language, and **the first of a kind as a Ransomware-as-a-service**. Such a peculiar choice was probably made not only because **Rust** is a cross-platform language (Windows, Linux, OSX) but also to better evade existing detection capabilities and reverse engineering methods. Moreover, when compared with C/C++ programming language, as **Rust** applies stricter rules, the latter could be considered more secure by default in the eyes of a programmer. Alternatively the **GoLang** programming language keeps growing fast and is also an open-source project with cross-platform capabilities. The latter was already used for instance by HIVE or NEPHILIM RaaS programs to take advantage of the language's concurrency features to encrypt files faster. However, its ties with Google might restrain some operators of ransomwares, as Google's projects in overall do not fit the political vision they want to display to the public.

There are four types of encryption options as described by BleepingComputer (*i.e.*, Full, Fast, DotPattern and Auto). All samples of **ALPHV** use a combination of AES128-CTR and RSA-2048 encryption to secure their malware against the researchers getting encrypted files back. Amongst the several modes that AES operates with, mostly used is CBC (Cipher Block Chaining) while CTR (CounTeR) was witnessed in the past by a few threats such as **LockerGoga**, **Nefilim** and **REvil**. In the case where (Advanced Encryption Standard) AES is not supported by the OS and if auto mode option is enabled, ChaCha20 encryption is applied instead. So

domain. The latterwas was seen previously also being leveraged by **RegretLocker**, **Wannacry**, **NotPetya** and **Trickbot** (operated by Wizard Spider) as a worm-like malware propagation module to spread over Server Message Block (**SMB**)

- *NetShareEnum*: playing the role of discovering network shares to enumerate DNS hostnames on the network, was encountered within numerous ransomwares such as **Ranzy locker**, **Netwalker**, **Cuba**, **LockBit**, **Blackmatter** and **Conti** (operated by Wizard Spider)
- *EnumdependentServicesW* was found to be shared with **Avaddon**, **LockerGoga** to retrieve the name and status of each service that depends on specified services
- *ARP scanner via the command* ***"arp -a"*** *[T1016]*: scans the targeted device's Address Resolution Protocol (ARP) table which stores information about IP addresses and the corresponding MAC address. The discovery of new networks allows then to fully scan for SMB volumes that can be mounted and eventually encrypted to crank up the impact. Such ARP scanner was previously seen embedded within strains of **Darkside**, **LockBit**, **Ranzy locker**, **Avaddon**, **DopplePaymer**. We can also underline variants of Ryuk and Conti that exhibited more sophisticated behaviours by taking advantage of arp. The former reads ARP tables and wake systems up by sending Wake-on-LAN commands (then use RPC to copy itself to identified network shares) while the latter retrieves the ARP cache to focus only on network shares to which the victims normally connects to. To be noted beyond Ryuk' wake-on-LAN peculiar feature is that other RaaS programs borrowed that capability such as LockBit or Thanos.

Figure 10 Command line tool called arp (available on Linux, MacOS and Windows) was found in the source code of ALPHV ransomware to be used as an ARP scanner feature. The scanner allows to look for details about the network configuration [T1016].

We are discussing the approach to gather **indicators of compromise (IOCs)** and define the infrastructure and TTPs leveraged by affiliates of the ALPHV RaaS program and its operator.

Besides, from TLP WHITE **indicators of compromise** shared by the platform Malware Bazaar (5 samples were available) we could pivot on VT intel to harvest other reported and related **IOCs** (**see the Recommendation section for technical details**). By pivoting on one of the ELF Linux variant samples, a lower sized file named *setup.exe* (see details in VT here) that contrasted with the other ransomware payloads has drawn our attention. As no GUID identifier has been found in this file we sought to pivot around artefacts (unique strings into content file). As such, we could find two other similar files reported into VirusTotal (see Figure 11).

Figure 12 after reversing the runner used by ALPHV' affiliates. It is interesting to note that download and upload functions point to the IP address:

141.136.44[.]54

The latter resolves the host from which was also present the runner *setup.exe*, meaning that ransomware payloads were hosted at the same place. We found out, about the same time, that @malwrhunterteam substantiated this result in one of their tweet. Once the runner is launched with an access-token set as an input, a messagebox like the one shown in Figure 9 pops up and asks the user whether or not "REALLY RUN LOCKER????". If the user chooses "YES", an ALPHV ransomware payload will be downloaded from the remote host- and executed locally.

Figure 12 Screenshot of the runner setup.exe found to be tight to the ALPHV threat arsenal. Four main functions are at play (DownloadAndRun, FullInfo, Start, UploaddDedInfo and UploadFiles). Both the runner and the payloads are hosted at hxxp://141.136.44[.]54/files/.

Commonalities between LockBit2.0 and ALPHV

After investigations via VT Intelligence we found that the second hash shown in Figure 11 was detected by some antivirus as **LockBit** ransomware. We thus decided to pursue the research in that direction and pivot around that IOC. After having unravelled the infrastructure behind that IOC, one can observe in Figure 13 that *i* the occurrence **LockBit** is often used in namings *ii* the runner.exe (setup.exe) possesses numerous variants, *iii* URLs follow the same pattern observed for **ALPHV** (*i.e., http://ip_address/files/toolname.exe*) and *iv* the payload name 4mmc.exe was also used by **ALPHV** (see here an example).

We checked that the payloads do indeed correspond to **LockBit** weaponized strains. Moreover we found that the hash value of the tool referred to as *screensaver.exe* was reported by The DFIR report back in June 2020 upon an attack by **LockBit** ransomware in which an executable that allows to lock out access to the desktop was dropped but was not used.

Figure 13 : Screenshot taken from Virustotal Intelligence platform after having pivoted around the second hash highlighted in Figure 11 (see blue colour). One can observe several IOCs that belong to the infamous LockBit ransomware as well as some of its toolset, namely a screensaver locker, and a runner for downloading payloads for encryption that is similar to the one that ALPHV used

As we found no direct link of this infrastructure with recent attacks perpetrated by **LockBit** affiliates, the latter could also have been used as a test infrastructure by **ALPHV**. This is substantiated by the filename LockBit_gay.exe (see Figure 13) submitted the VT on 2021-11-08, which could indicate that an imposter essentially rebranded the tool used by **LockBit'** affiliates and used it for **ALPHV's** campaigns. The word 'gay' is not without recalling the recent flooded **Babuk's** new ransomware forum (**RAMP**), crippled by a comment spammer with gay orgy porn GIFs. Not only the filenames (setup.exe), their size (in a range of 15-15.5 KB) but also the source code is obviously strongly overlapping as demonstrated in Figure 14. The main change arises from the adaptation of the code with the aim to include the anti-analysis tactic required for running a payload of ALPHV (*i.e.*, the aforementioned unique accesstoken).

Figure 14 Source Code Differencing via Git Diff. Reverse engineering analysis shows that the source code of the LockBit's arsenal (in red) and the ALPHV's arsenal (in green) are strongly overlapping. The main change arises from the adaptation of the code to include the unique accesstoken per victim required for running a payload of ALPHV.

It is hard to conclude at this stage to conclude whether or not **ALPHV** is a 'new' group or not. However, it suggests that **ALPHV** at the very least borrowed a part of

that by pivoting on their public DLS we found a section dedicated to **ALPHV** affiliates that provides a procedure on how to leverage the ransomware payloads on different operating systems upon an attack (see appendix).

Tactic	Technique	Procedure
		In some cases ransomware w deployed via **ScreenConnect** l via **PSEXEC** (being embedded ransomware code after a compression via zlib). **ALPHV** significantly the remote administration tool **PsExec** [T1 well as the PowerShell langua [T1086]
Execution [TA0002]	System Services: Service Execution [T1569.002]	
	Command and Scripting Interpreter: Windows Command Shell [T1053.003]	ALPHV can use the Windows command line to : • Delete volume shadow copie disable recovery • Modify window registry
	Windows Management Instrumentation [T1047]	The adversary uses WMI to ex various behaviours, such as gathering information for Disc
	Shared Modules [T1129]	Fsutil was executed to modify SymLink Evaluation behaviour change the type of symbolic li can be created on the system. Symbolic links create a file in c directory that acts as a shortc another file or folder
Credential access [TA0006]	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay [T1557.001]	Symantec has reported suspic Server Message Block (SMB) r occurred onto the patient zero
	OS Credential Dumping: LSA Secrets [T1003.004]	Symantec has reported attem remote Local Security Authorit registry dump from a remote machine on the network upon attack
Collection [TA0009]	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and	Threat actors may have lever LLMNR/NBT-NS Poisoning and

	Modify Registry [T1112]	Modification of the registry oc upon an attack. According to Symantec attackers were also tweak the maximum limit of concurrent requests machine modifying the Windows regist further help spreading via PsE Please note that we found tha actually a capacity of the ransomware itself and not a h operated command (see App
Discovery [TA0007]	System Information Discovery [T1082]	**ALPHV** runs commands to col system information via **WMIC**, order to collect Universally Un Identifiers (UUIDs) from each machine. These are then used generate the 'access token' th makes up part of the unique T address victims are instructed
	System Network Connections Discovery [T1049]	**ALPHV** attempts to propagate mounting hidden partitions th the 'net use' command. As aforementioned admin creder are embedded into the config within the payload
	Ingress Tool Transfer [T1105]	**ALPHV** affiliates bring their ow external **tools** into a compron network
Exfiltration [TA0010]	Exfiltration Over Web Service [T1567]	Double extortion: exposure of sensitive data on a DLS**. ALPHV victim data not only if the vi do not pay, but also once Thr Intel teams accesses their ch or discusses their operations** posture recalls recent threats proclaimed by several **RaaS** g as chat logs were leaked and by CTI teams and renowned c journalists that weakened the leverage of the malicious neg
Impact [TA0040]	Inhibit System Recovery [T1490]	According to @malwrhunterte could be the first **ransomware** does **VM snapshots cleaning**
	Data Destruction [T1485]	latter deletes also **shadow cop the Recycle Bin**

sensitive data

Triple extortion: As an additior extortion method, the threat a threaten to **DDoS** victims unles pay a ransom

Malware(s)/Tool(s)

- **ConnectWise** (formerly known as **ScreenConnect**), that is a legitimate remote administration tool was leveraged. This tool was already seen abused in the past by other ransomcartels such as Revil upon the recent massive attack against Kaseya and APTs since 2016
- **Another legitimate tool Keystore explorer** that can be used to create and navigate KeyStores via its intuitive graphical interface was reported. Though it is not yet clear if there is any link with **ALPHV** at this stage (see here), one could conjecture that this tool was leveraged to generate unique key pairs for each victim but should be considered as a false positive.
- **7zip** and **Rclone** were reported by SpearTip as the toolset use for exfiltration of data

Vulnerabilities

- **No known vulnerabilities are yet reported** to be leveraged by the affiliates of this **RaaS** program to the best of our knowledge. We should mention though that **SentinelOne** telemetry indicated "*a primary delivery of BlackCat is via 3rd party framework/toolset (e.g., Cobalt Strike) or via exposed (and vulnerable) applications*"
- We should mention that other entry vector remain extensively used **RDP** brute force attacks or unsecure **RDP/VPN** connections. It is also likely that this advanced threat actor, if not already, could rapidly leverage an Initial Access Broker to provide to its affiliates a foothold on a victim' network. Keep in mind that such **Initial Access Brokers (IABs)** could also leverage the last vulnerability that defrayed the chronicle being **LOG4SHELL**

Course of action

Avoid IABs or affiliates to breach into your network

- Focus efforts on patching/monitoring the most impactful flaws reported in information bulletins produced by Intrinsec CTI Team about last TTPs of such ecosystem (*PrintNightmare, Proxy|logon|Shell|Oracle, PetitPotam, LogShell, VMWare*)
- Enable hardware MFA keys whenever possible on critical assets requiring the most protection
- Identify then document an organization's people, information and in particular exposed assets such as VPN, RDP, web servers, etc… (*N.B.,* the latter shall always be up to date)

- Do not forget BYOD security management: security policies deployment and enforcement, compliancy, inventory, network access control
- Cobalt Strike, being maybe the most prolific post-exploitation framework tool both leveraged not only by red teamers and top-tier RaaS affiliates but also by several APTs, it is worth putting efforts to become capable of detecting its capabilities

Detect **ALPHV** affiliates before your data gets exfiltrated and then encrypted

- Craft fake documents (financial, cyber insurance, employee data falling under GDPR) that will beacons back alerting blue teams only with very high rates of true positives thanks to Canarytokens**.** As such, Incident Response teams would be more efficient in preempting/expelling threats by being involved at early stages of an attack
- Monitor IOCs & commands that we capitalized, vetted and made available on our GitHub. Please note that if you are an Intrinsec SOC (Security Operation Center) customer, the IOCs related to this campaign are being integrated into our MISP
- Block globally network & system IOCs

Detect **ALPHV** affiliates before your data gets encrypted while being exfiltrated

- Ensure blue teams can carry out threat detection of **RClone** (leveraged by **ALPHV** for data exfiltration) with relevant Sigma rules such as here and here

Detect **ALPHV** affiliates while encrypting data to reduce the impact

- It is worth mentioning here 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 that can be triggered by **ALPHV** payloads or by other similar type of threats.

References:

- *https://www.bleepingcomputer.com/news/security/**ALPHV**-blackcat-this-years-most-sophisticated-ransomware/*
- *https://github.com/cdong1012/Rust-Ransomware*
- *https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-**ALPHV**-rust-ransomware*
- *https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809*
- *https://id-ransomware.blogspot.com/2021/12/blackcat-ransomware.html*

Appendix

Figure 15 : Screenshot highlighted the registry key adding in ransomware code aiming at exalting the spreading via PsExec upon the attack.

In some of those payloads, a reverse engineering analysis unravelled attempts to bypass Windows User Account Control (UAC) to stealthy execute code with elevated permissions [T1218.003]. This technique is also known as the COM Elevation Moniker that allows running applications under UAC to activate COM classes with elevated privileges. More precisely, we found a globally unique identifier (CLSID) {3E5FC7F9-9A51-4367-9063-A120244FBEC7} (128-bit hexadecimalnumbers within a pair of curly braces can be retrieved in the registry path *"WorkstationHKEY_LOCAL_MACHINESOFTWAREClassesAppID{3E5FC7F9-9A51-4367-9063-A120244FBEC7}")* that could be associated with the Cmstplua.dll (aka Connection Manager Admin API Helper for Setup). Such CLSID is usually leveraged for detecting bypass UAC via an auto-elevated COM interface.

In the same vein as was reported by Sophos in April 2020 in the case of LockBit 2.0 ransomware, ALPHV will ensure to exalt damages by checking whether or not its process owns Administrator rights (via OpenProcessToken function). If not the latter masquerades as Windows Explorer (explorer.exe) by calling CoInitializeEx (initializing the COM library). Then, the hex value CLSID is added to the moniker and executed. We also found another typical string referred to as "evation:Administrator!new:" that is similar to the expected value "Elevation:Administrator!new:" as indicated in the Microsoft documentation, which allows apps running under UAC to activate COM classes with elevated privileges (see Figure 16) :

Figure 16 : UAC bypass via the COM Elevation Moniker.

Such UAC bypass capability was previously seen in the threat landscape embedded into ransomwares such as MedusaLocker, Avaddon, Revil, Darkside, BlackMatter. Note that strong TTP overlapping was reported between MedusaLocker and Avaddon but also Darkside and BlackMater as aforementioned.

[TTPs of a LINUX' payload]

In the same vein here is a JSON file format compatible with the MITRE ATT&CK Navigator of the shared **TTPs** of a representative payload targeting **Linux** systems (**VMWare ESXi**).

ransomware.

All software is written from scratch, the decentralization of all web resources is architecturally laid down. A unique onion domain is generated for each new company. For each advertiser, an entrance is provided through its own unique onion domain (hello LockBit).

Own datacenter for hosting leak files over 100 TB.

We are already cooperating with top recovery companies that worked with darks, revils, etc.

There is a support on chats, which sits 24 by 7, but if you wish, you can negotiate yourself.

SECURITY

We are in every possible way ready for existence in modern conditions, meeting all the requirements for the security of infrastructure and advertisements. In the affiliate program all possible links with forums are architecturally excluded (hello revil), algorithms for self-deletion of data upon expiration of the limitation period are laid down, a built-in mixer is integrated with a real break in the chain (not to be confused with Wasabi, BitMix and others), because you get completely clean coins from foreign exchanges. The wallets to which your coins were sent are unknown for our backend. The infrastructure is fragmented into the so-called. nodes that are interconnected through a whole network of pads within the onion network and are located behind NAT + FW. Even when receiving a full-fledged cmdshell, the attacker will not be able to reveal the real IP address of the server. (hi Conti)

SOFTWARE

The software is written from scratch without using any templates or previously leaked source codes of other ransomware. The choice is offered:

4 encryption modes:

-Full – full file encryption. The safest and slowest.

-Fast – encryption of the first N megabytes. Not recommended for use, the most unsafe possible solution, but the fastest.

-DotPattern – encryption of N megabytes through M step. If configured incorrectly, Fast can work worse both in speed and in cryptographic strength.

*-Auto. Depending on the type and size of the file, the locker (both on windows and * nix / esxi) chooses the most optimal (in terms of speed / security) strategy for processing files.*

-SmartPattern – encryption of N megabytes in percentage steps. By default, it encrypts 10 megabytes every 10% of the file starting from the header. The most optimal mode in the ratio of speed / cryptographic strength.

2 encryption algorithms:

-ChaCha20

-AES

In auto mode, the software detects the presence of AES hardware support (exists

– ReadyNAS, Synology

Since recently binaries have been leaking to analysts, and premium VT allows you to download samples and receive readme in chats, random people may appear who can disrupt negotiations (hello darkside), when launching the software it is MANDATORY to use the –access-token flag. The cmdline arguments are not passed to the AVers, which will keep the privacy of the correspondence with the victim. For the same reason, each encrypted computer generates its own unique ID used to separate chats.

There is a function of automatic downloading of files from the MEGA service, you give a link to the files, they are automatically downloaded to our servers.

You can get a full description of all functionality in the FAQ section.

ACCOUNT

If there is no activity for two weeks, your account will be frozen and subsequently deleted. To avoid this, we recommend that you notify the administration about possible vacations, pauses and other things.

The rate is dynamic and depends on the amount of a single payment for each company, namely:

– up to 1.5M $ – 80%

– up to $ 3.0M – 85%

– from $ 3.0M – 90%

After reaching the $ 1.5M mark in terms of the sum of all payments on your account, you will have access to hosting services for files of companies' leaks, dialing and DDoS'a absolutely free.

FAQ dedicated to its affiliates (published on the public DLS of **ALPHV**)

Wed Nov 17 2021

How – To

*How to start a locker on ESXi or * nix?*

1. *Downloading the build via scp*

scp sample_alfa_x86_64_linux_encrypt_app root@10.0.0.1:/tmp/

- *We go via ssh and give execution rights*

cd /tmp/ && chmod +x sample_alfa_x86_64_linux_encrypt_app

- *Launch the locker **ALWAYS** with the token (obtained when creating the build) and in the background (**&**)*

/tmp/sample_alfa_x86_64_linux_encrypt_app –access-token XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX&

- *To display the speed and encryption process, override the functions specified*

folder with the locker and start ALWAYS with the token (obtained when creating the build)

./sample_alfa_x86_64_linux_encrypt_app.exe –access-token XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

- *To display the speed and encryption process, override the functions specified when creating the build, you can use the flags:*

-p, –paths <PATHS> – forced indication of paths

-v, –verbose – output the log to the console

–no-net – do not encrypt network shares

–no-prop – do not use the worm's functionality (self-propagation by getting a list of ip in the arp table and trying to psexec with accounts hammered in for impersonation)

–ui – launch with a graphical interface

How to run Windows locker on one PC using drag and drop?

1. *Load the build and run cmd / powershell as administrator, go to the folder with the locker and start ALWAYS with the token (obtained when creating the build) and the flag* ***–drag-and-drop-target***

./sample_alfa_x86_64_linux_encrypt_app.exe –access-token XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX –drop-drag-and-drop-target

- *A .bat file will appear in the folder with the locker, onto which you can drag files, folders, disks, etc.*

How to run Windows locker in the whole domain?

1. *Load the build on the* ***PDC*** *and run cmd / powershell as administrator, go to the folder with the locker and copy it to C: WINDOWS sysvol sysvol * yourdomain * scripts*

copy sample_alfa_x86_64_linux_encrypt_app.exe C:WINDOWSsysvolsysvol*yourdomain*scriptslocker.exe

** The locker.exe file must be accessible via \ yourdomain netlogon locker.exe*

- *In the group policy editor, change the Default Group Policy or create a new one and link to Default.*
- *Change Computer / User Configuration > Preferences > Control Panel Settings > Scheduled Tasks*
- *When creating a new task on the General tab, fill in the name, description (optional), tick the Run with highest privileges checkbox and select the user SYSTEM*
- *On the Actions tab, click New and fill in the fields as follows:*

A complete list of functions is available via -h, –help

Domain analysis of the ALPHV's infrastructure

When investigating first the status of the host (resolved by the IP address *141.136.44[.]54*), the latter was found to be up and located in Lithuania Vilnius. Besides, all common ports are securely filtered or closed but the 80 (http), amongst which, a RDP port is available and very often used as the entry vector by brute forcing weak accounts. Passive HTTP server banners reveals that the attacker has set up an Apache server (with a current version installed being 2.4.29 though a 2.4.52 version was released the 2021-12-20) on an Ubuntu Linux distribution. The attackers have added a module to compress the traffic as shown by a passive analysis of the banners (content-encoding: gzip), most likely to lure malware scanners and keep surmise while upload/download operations get faster.

We found two domains that resolved to that the given IP address:

support-global-it-ss[.]com

hosting-global-it-ss[.]com

The homepages indicates that those websites proposes IT support services, which seem to belong to the same structure and could be legitimate. No direct link with the malicious activities emanating from the given IP could be established.