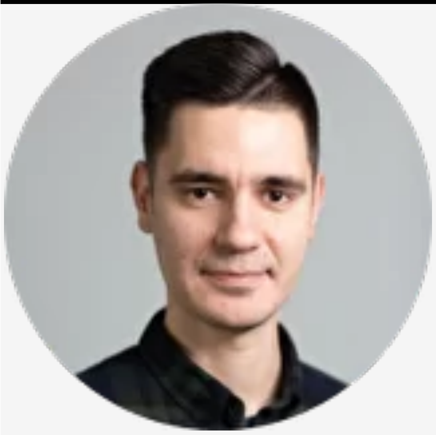
# REvil Twins

## Deep Dive into Prolific RaaS Affiliates' TTPs



Oleg Skulkin
Senior Digital Forensics analyst at Group-IB

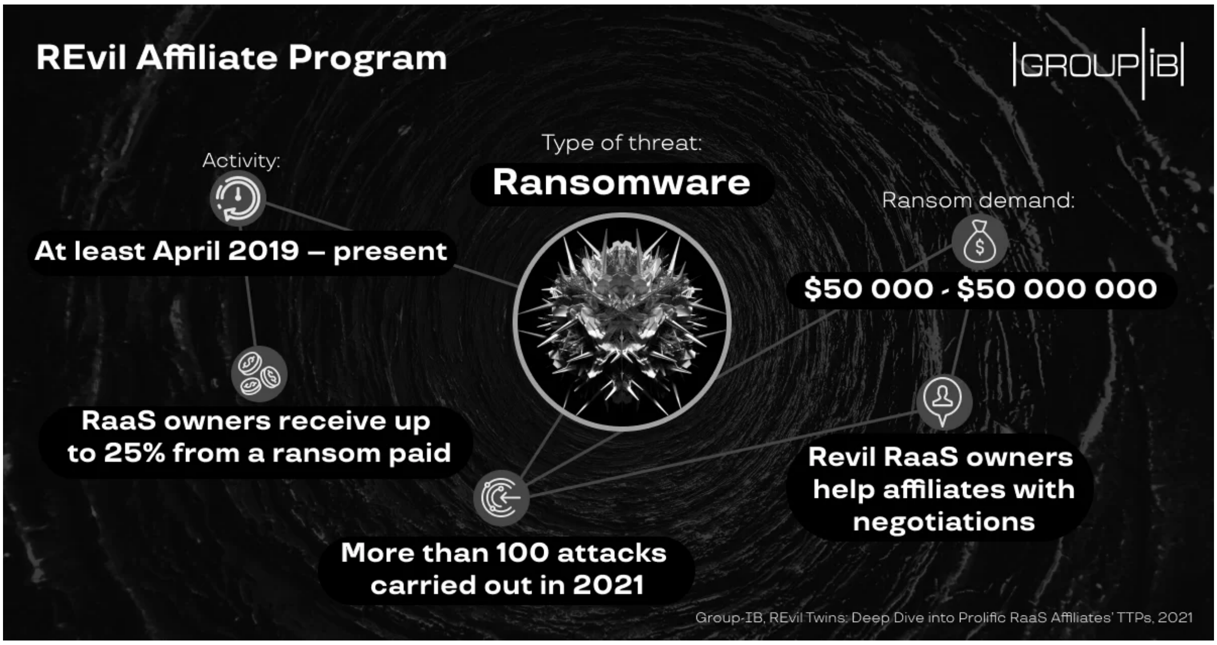
Ransomware continues to dominate the cybercriminal scene in 2021. The number of attacks as well as the ransom demands seem to be growing quickly. According to the Ransomware Uncovered 2020-2021 report, Ransomware-as-a-Service model, which involves the developers selling/leasing malware to the program affiliates for further network compromise and ransomware deployment, became one of the major driving forces behind phenomenal growth of the ransomware market. Group-IB DFIR team observed that 64% of all ransomware attacks it analyzed in 2020 came from operators using the RaaS model.

In this blog post, we would like to focus on one of the most active ransomware collectives, **REvil, and their RaaS program**, which attracts more and more affiliates due to the shutdown of other RaaS. Group-IB's DFIR experts took a deep dive into the modus operandi of **REvil affiliates** and shared some information on various affiliates' tactics, techniques and procedures observed, so defenders can tune their detection capabilities accordingly.

# Meet REvil RaaS

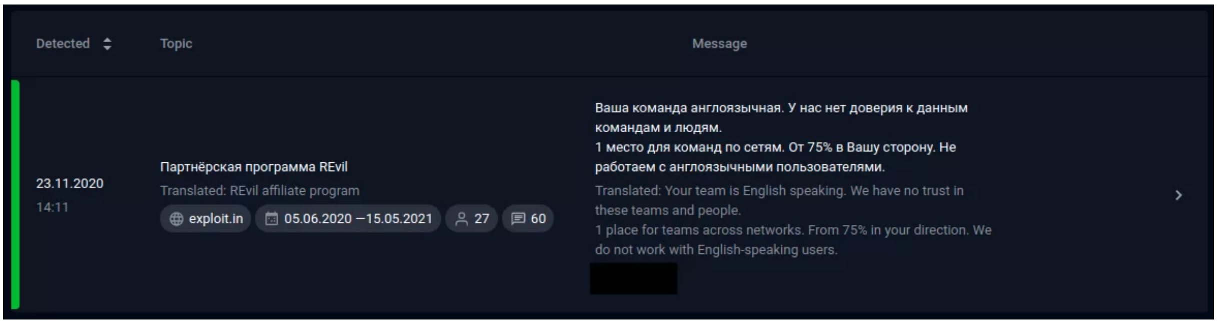
The affiliate program of **REvil ransomware** (also known as Sodinokibi or Sodin) emerged as early as in **2019**. Ever since, the affiliate program has been actively recruiting partners of different skills, who attacked various organizations all around the world except for Russia and CIS, which gives reasonable ground to believe that REvil developers and operators are most likely Russian speaking.

REvil affiliates have been extremely active lately. REvil affiliates are not concerned about the industry of the targeted companies. Acer, Honeywell, Quanta Computer, JBS, Sol Oriens – these are just some of the big-name companies hit by the affiliates of this ransomware-as-a-service program. From relatively modest amounts in the early days, their ransom demands increased to tens of millions of dollars now/today. Not long ago, they demanded as much as USD 50,000,000 from Acer, and, according to the public reports, were paid USD 11,000,000 by JBS.


REvil Affiliate Program
GROUP IB
Activity:
At least April 2019 – present
Type of threat:
Ransomware
Ransom demand:
$50 000 - $50 000 000
RaaS owners receive up to 25% from a ransom paid
Revil RaaS owners help affiliates with negotiations
More than 100 attacks carried out in 2021
Group-IB, REvil Twins: Deep Dive into Prolific RaaS Affiliates' TTPs, 2021

REvil RaaS Program Overview

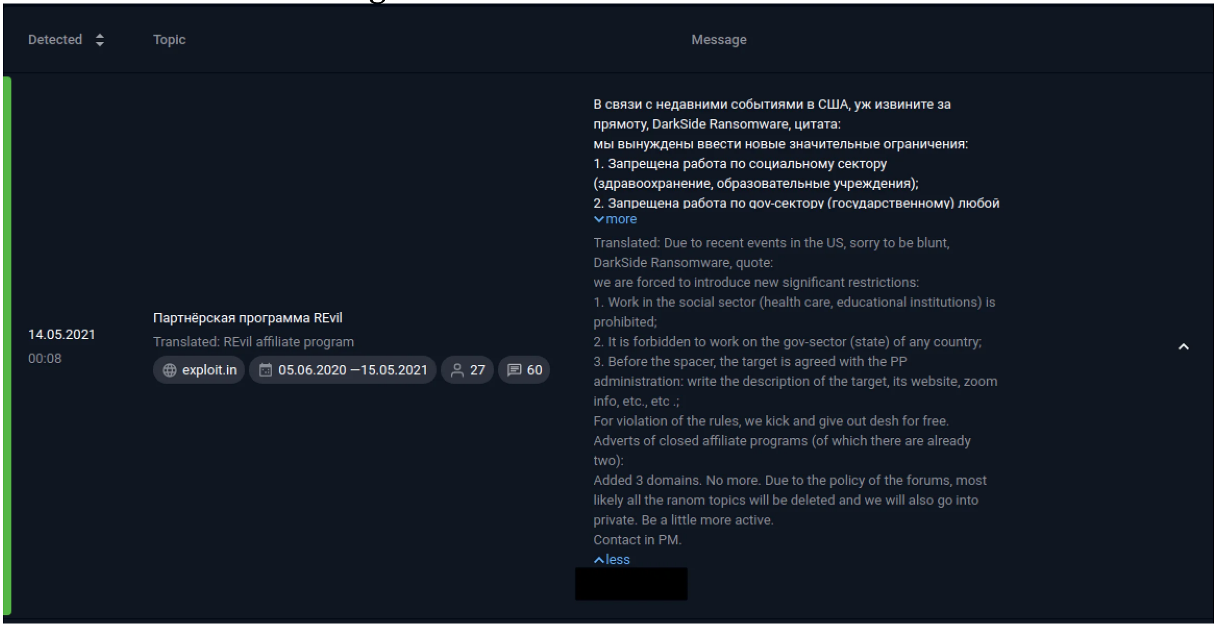
According to a message, that a user, allegedly related to the REvil RaaS program, left in a thread dedicated to REvil RaaS program on exploit.in, REvil affiliates get at least **75%** from the ransom paid by the victims. The post was then deleted. Nevertheless, Group-IB's Threat Intelligence & Attribution system was able to retrieve the original post.



| Detected | Topic | Message |
|---|---|---|
| 23.11.2020<br>14:11 | Партнёрская программа REvil<br>Translated: REvil affiliate program<br>exploit.in 05.06.2020 –15.05.2021 27 60 | Ваша команда англоязычная. У нас нет доверия к данным командам и людям.<br>1 место для команд по сетям. От 75% в Вашу сторону. Не работаем с англоязычными пользователями.<br>Translated: Your team is English speaking. We have no trust in these teams and people.<br>1 place for teams across networks. From 75% in your direction. We do not work with English-speaking users.<br>[redacted] |

Source: Group-IB Threat Intelligence & Attribution system

In May 2021, this user left a message in the same thread urging REvil affiliates not to attack social sector and government companies. In addition, the user addressed the affiliates of the closed RaaS programs. This indicates that more partners are joining REvil, so it is fair to expect the growth in the number and scale of attacks involving this ransomware strain.



| Detected | Topic | Message |
|---|---|---|
| 14.05.2021<br>00:08 | Партнёрская программа REvil<br>Translated: REvil affiliate program<br>exploit.in 05.06.2020 –15.05.2021 27 60 | В связи с недавними событиями в США, уж извините за прямоту, DarkSide Ransomware, цитата:<br>мы вынуждены ввести новые значительные ограничения:<br>1. Запрещена работа по социальному сектору (здравоохранение, образовательные учреждения);<br>2. Запрещена работа по gov-сектору (государственному) любой<br>more<br>Translated: Due to recent events in the US, sorry to be blunt, DarkSide Ransomware, quote:<br>we are forced to introduce new significant restrictions:<br>1. Work in the social sector (health care, educational institutions) is prohibited;<br>2. It is forbidden to work on the gov-sector (state) of any country;<br>3. Before the spacer, the target is agreed with the PP administration: write the description of the target, its website, zoom info, etc., etc .;<br>For violation of the rules, we kick and give out desh for free.<br>Adverts of closed affiliate programs (of which there are already two):<br>Added 3 domains. No more. Due to the policy of the forums, most likely all the ranom topics will be deleted and we will also go into private. Be a little more active.<br>Contact in PM.<br>less<br>[redacted] |

Source: Group-IB Threat Intelligence & Attribution system

# TTPs of REvil Affiliates

It is interesting to note that, while frequently hitting big corporations, some REvil affiliates are going after companies with relatively small revenues. This fact is very important from the TTPs perspective: on rare occasions, the initial access is gained through a brute force attack against public-facing RDP-servers or just using valid accounts obtained from a third party.

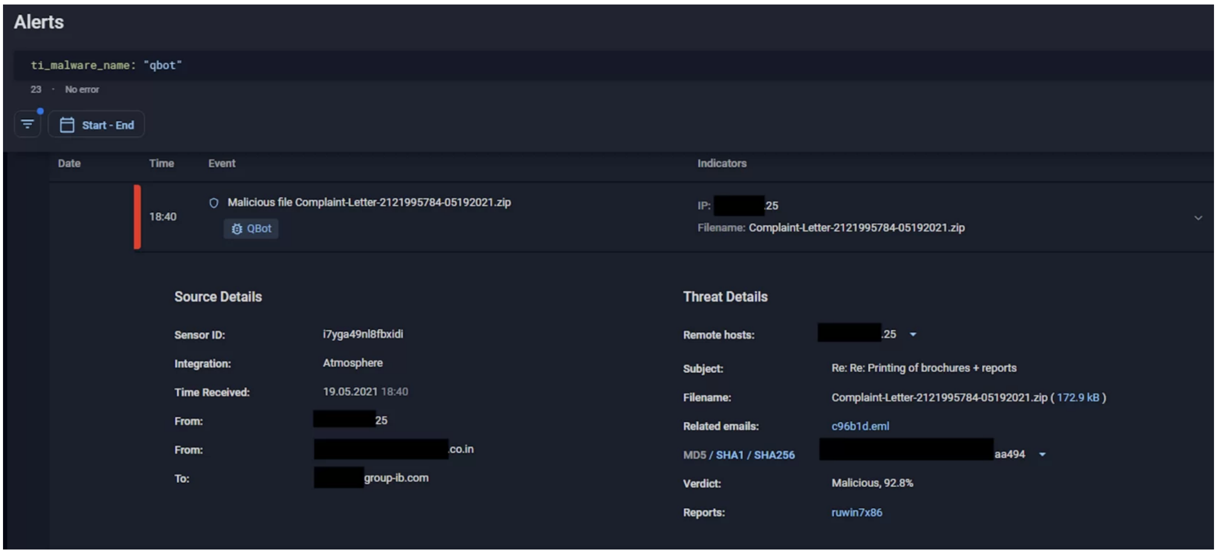
What's more, REvil affiliates didn't always focus on Big Game Hunting (targeting big companies). Even in December 2020 some of REvil affiliates used malvertising to trick victims into downloading an archive with a malicious JS-file. When executed, it abuses Windows Command Prompt to run a malicious PowerShell command, which finally leads to REvil execution on the target host. The same technique was used for Gootkit trojan distribution.

**Detection tips:** Monitor WScript.exe running scripts from uncommon locations, as well as WScript.exe spawning cmd.exe and/or powershell.exe or performing external network connections.

Just like many other ransomware operators, REvil affiliates used commodity malware to obtain initial access to the target networks. Two recent examples are IcedID and Qakbot – both already have a long history of being involved in the ransomware operations. In the past, IcedID was known to have been used by Maze, Egregor and Conti affiliates, while Qakbot – by ProLock, Egregor and DoppelPaymer.

Both trojans are distributed via massive spam campaigns. Potential victim receives an email with a weaponized Microsoft Office document, if it's opened and malicious macros is enabled, the trojan binary is downloaded and executed on the host, usually via rundll32.exe or regsvr32.exe.

Phishing remains of the most popular vectors for ransomware attacks. According to the Ransomware Uncovered 2020-2021 report, 29% of attacks in 2020, analyzed by Group-IB DFIR team, started with spear phishing.



Alerts

```
ti_malware_name: "qbot"
```

23 · No error

Start - End

| Date | Time | Event | Indicators |
|---|---|---|---|
| | 18:40 | Malicious file Complaint-Letter-2121995784-05192021.zip<br>QBot | IP: [redacted].25<br>Filename: Complaint-Letter-2121995784-05192021.zip |

Source Details

| | |
|---|---|
| Sensor ID: | i7yga49nl8fbxidi |
| Integration: | Atmosphere |
| Time Received: | 19.05.2021 18:40 |
| From: | [redacted]25 |
| From: | [redacted].co.in |
| To: | [redacted]group-ib.com |

Threat Details

| | |
|---|---|
| Remote hosts: | [redacted].25 |
| Subject: | Re: Re: Printing of brochures + reports |
| Filename: | Complaint-Letter-2121995784-05192021.zip ( 172.9 kB ) |
| Related emails: | c96b1d.eml |
| MD5 / SHA1 / SHA256 | [redacted]aa494 |
| Verdict: | Malicious, 92.8% |
| Reports: | ruwin7x86 |

Detection of Qakbot in action by Group-IB Atmosphere - an intel-driven cloud Email protection that detonates and hunts for the most advanced email threats. Request a free trial of Group-IB Atmosphere here.

**Detection tips:** Monitor winword.exe or excel.exe spawning suspicious processes, like rundll32.exe, regsvr32.exe or mshta.exe, focus on rundll32.exe and regsvr32.exe running files without .dll extension.

Let's look at some common examples and start from IcedID. Commonly it uses capabilities of another threat actor – Shathak (which is also known for distributing Qakbot), and is distributed via weaponized Microsoft Word documents. Malicious macros drops an .hta file and abuses mshta.exe to run it:

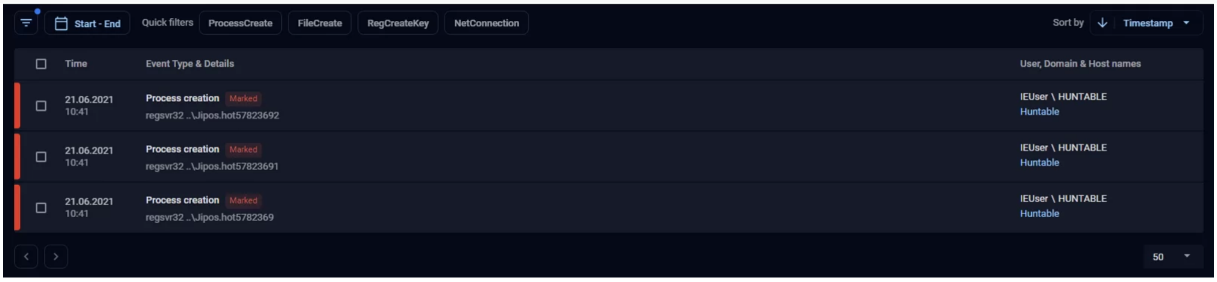
```
"C:\Windows\SysWOW64\mshta.exe" "C:\Users\Public\leftSwapStorage.hta"
```

As a result, it downloads the initial IcedID DLL and runs it via rundll32.exe:

```
"C:\Windows\System32\rundll32.exe"
"C:\users\public\leftSwapStorage.jpg,PluginInit"
```

The second trojan has similar delivery mechanism. Most commonly, it is distributed via weaponized Microsoft Excel spreadsheets. Once malicious macros is enabled, Qakbot's initial DLL is downloaded and run via regsvr32.exe:

```
regsvr32 -s ..\Post.storg
```



| □ | Time | Event Type & Details | User, Domain & Host names |
|---|---|---|---|
| □ | 21.06.2021<br>10:41 | Process creation Marked<br>regsvr32 ..\Jipos.hot57823692 | IEUser \ HUNTABLE<br>Huntable |
| □ | 21.06.2021<br>10:41 | Process creation Marked<br>regsvr32 ..\Jipos.hot57823691 | IEUser \ HUNTABLE<br>Huntable |
| □ | 21.06.2021<br>10:41 | Process creation Marked<br>regsvr32 ..\Jipos.hot5782369 | IEUser \ HUNTABLE<br>Huntable |

Group-IB Threat Hunting Framework's Huntpoint detecting Qakbot's DLL execution

**Detection tips:** Persistent DLLs for both trojans are commonly located in user's profile subfolders, so you can hunt for rundll32.exe or regsvr32.exe running suspicious DLLs from such locations.

As already mentioned, many affiliates abuse external remote services, as well as exploit public-facing applications to obtain initial access to the target network. It's important to note that the RaaS affiliates rarely perform brute force or password spraying attacks against such instances themselves, rather they buy accesses from the brokers.

**Detection tips:** Usually, there's some time from the first successful unauthorized access to the access, from which actual post-exploitation starts, so if you don't have multi-factor authentication for publicly accessible RDS or VPN, make sure your team monitoring successful logins from uncommon locations.

Brute force or password spraying are not always the case. REvil affiliates may obtain valid account from various sources, for example, information stealers. For instance, REvil RaaS owners even bought KPOT stealer source code, so they can use it to benefit their affiliates.

Affiliates may exploit various vulnerabilities in public-facing applications and are known to use web-shells to maintain initial access. According to the media reports, the threat actors may have obtained access to Acer network using ProxyLogon vulnerability in the company's Microsoft Exchange server – it's very common for those who exploit it to upload a web-shell to maintain access.

Once the initial foothold is gained, the threat actors commonly continue with obtaining additional credentials and internal reconnaissance.

Two most common network scanning tools observed during Group-IB's incident response engagements were Advanced IP Scanner and SoftPerfect Network Scanner. In some cases, affiliates downloaded these tools directly from the official websites, using compromised host.

**Detection tips:** The threat actors hardly rename network-scanning tools, so it's easy to search for file names or, if such tools are renamed, focus on the product names and descriptions, which still allow you to detect them.

In many cases, network scanning wasn't the only activity performed during the reconnaissance stage. Usually, the affiliates need to collect information about Active Directory, so it's quite common to see evidence of using such tools, as AdFind, ADRecon and Sharphound during the incident investigation.

**Detection tips:** Popular Active Directory reconnaissance tools commonly observed to be used by REvil affiliates have very typical command line arguments, which can be used for building detections.

Like many other threat actors, including state-sponsored adversaries, REvil affiliates use a wide range of living-of-the-land techniques, including the abuse of PowerShell, WMI and other built-in tools.

For example, they used Get-ADComputer cmdlet to collect information about Windows computers in the infrastructure:

```
Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name,
DNSHostName, OperatingSystem, LastLogonDate | Export-CSV
C:\temp\AllWindows.csv -NoTypeInformation -Encoding UTF8
```

To collect information about sessions on a Remote Desktop Session Host server, the threat actors used qwinsta command:

```
qwinsta /server:%COMPUTERNAME%
```

Another built-in command was abused by the REvil affiliates to collect information about domain controllers:

```
nslookup -q=srv _kerberos._tcp
```

To collect information about installed applications, including security products, the adversaries ran WMI queries:

```
get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name
```

**Detection tips:** REvil affiliates often use various built-in tools to collect information about the target network, most of them aren't used by system and network administrators very often, so uncommon executions should be easily detected.

As for the REvil affiliates detect evasion techniques, in many cases the threat actors didn't disable them at first, preferring to switch them in detection-only mode, so no malicious tools they were using were blocked. This allowed affiliates to use very common and easy-detectable tools for credential dumping, such as Mimikatz and LaZagne. In some cases, they wanted to be more stealth, and used ProcDump to obtain LSASS process dump.

Another notable example of credential access observed during some of the incidents is searching for passwords in various files in the user profiles, for example, text files.

Depending on the actor, there are multiple post-exploitation tools used, including:

- Cobalt Strike
- Metasploit
- CrackMapExec
- PowerShell Empire
- Impacket

All aforementioned tools also enable REvil affiliates to move laterally, especially if they already gathered elevated credentials.

**Detection tips:** Usually the threat actors use post-exploitation tools in a quite common way, so if you focus on regular command line arguments typical of Cobalt Strike, PowerShell Empire and others, you'll most likely successfully detect them.

In addition, lateral movement was enabled by leveraging Remote Desktop Protocol. The affiliates even enabled it on hosts where it wasn't available using WMI and PowerShell:

```
(Get-WmiObject Win32_TerminalServiceSetting -Namespace
root\cimv2\TerminalServices).SetAllowTsConnections(1,1)
```

```
(Get-WmiObject -Class "Win32_TSGeneralSetting" -Namespace
root\cimv2\TerminalServices -Filter "TerminalName='RDP-
tcp'").SetUserAuthenticationRequired(0)
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp' -name "UserAuthentication" -Value 1
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

REvil affiliates are notorious for exfiltrating data before the actual ransomware deployment. A common tool used by the threat actors is WinSCP. In many cases, they just install it on the server, and use SMB protocol to access data of interest on other hosts, exfiltrating it to the adversary-controlled servers.

Another example is installing cloud storage related applications, for example, MEGASync. At the same time, the threat actors may use web-browser to access similar cloud storages to use them for data exfiltration.

**Detection tips:** Monitor your environment for uncommon applications installations, which can potentially be used for data exfiltration, such as FTP/SFTP and cloud storage clients. Also, take into consideration connection to cloud storage related websites from uncommon places.
In addition, before the actual ransomware deployment, many affiliates take care of available backups, either wiping them or running REvil executables on the corresponding servers in the first order.

Usually the threat actors try to deploy ransomware as widely as possible, and use PsExec or Group Policy modification to run a scheduled task to run it. Of course, before it, they fully disable security products or just add a piece of ransomware to exclusions.

# Conclusion

As you can see, REvil affiliates share tactics, techniques and procedures with other threat actors involved in the so-called Big Game Hunting. It's not surprising, as many affiliates from other RaaS jumped on the REvil train. Given that more threat actors are joining REvil affiliate program, we've mapped their affiliates TTPs in accordance with MITRE ATT&CK to better prepare for their attacks and know what techniques are needed to mitigate security risks associated with REvil.

# REvil affiliates TTPs and relevant mitigation techniques in accordance with MITRE ATT&CK

| Tactics | Technique | Mitigations | Group-IB Solutions |
|---|---|---|---|
| **Initial Access** | Phishing: Spearphishing Attachment (T1566.001) | Restrict Web-Based Content (M1021), User Training (M1017) | Threat Hunting Framework, Group-IB Education |
| | Exploit Public-Facing Application (T1190) | Update Software (M1050), Vulnerability Scanning (M1016) | Security Assessment |
| | External Remote Services (T1133) | Limit Access to Resource Over Network (M1035), Multi-factor Authentication (M1032) | |
| **Execution** | Command and Scripting Interpreter: PowerShell (T1059.001) | Antivirus/Antimalware (M1049), Code Signing (M1045), Disable or Remove Feature or Program (M1042), Privileged Account Management (M1026) | Threat Hunting Framework |
| | Command and Scripting Interpreter: Windows Command Shell (T1059.003) | Execution Prevention (M1038) | |
| | Command and Scripting Interpreter: Visual Basic (T1059.005) | | |
| | Command and Scripting Interpreter: JavaScript | | |
| | User Execution: Malicious File (T1204.002) | Execution Prevention (M1038), User Training (M1017) | Threat Hunting Framework, Group-IB Education |
| | Windows Management Instrumentation (T1047) | Privileged Account Management (M1026), User Account Management (M1018) | Threat Hunting Framework |
| **Persistence** | Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001) | | Threat Hunting Framework |
| | External Remote Services (T1133) | Limit Access to Resource Over Network (M1035), Multi-factor Authentication (M1032) | Security Assessment |
| | Scheduled Task/Job: Scheduled Task (T1053.005) | Operating System Configuration (M1028), Audit (M1047 | Threat Hunting Framework |
| | Valid Accounts (T1078) | Password Policies (M1027), Privileged Account Management (M1026) | Security Assessment |
| **Defense Evasion** | Process Injection (T1055) | Behavior Prevention on Endpoint (M1040), Privileged Account Management (M1026) | Threat Hunting Framework |
| | Access Token Manipulation (T1134) | Privileged Account Management (M1026), User Account Management (M1018) | |
| | Deobfuscate/Decode Files or Information (T1140) | - | |
| | Obfuscated Files or Information (T1027) | Antivirus/Antimalware (M1049) | |
| | Signed Binary Proxy Execution: Mshta (T1218.005) | Execution Prevention (M1038) | |
| | Signed Binary Proxy Execution: Regsvr32 | Exploit Protection (M1050) | |
| | Signed Binary Proxy Execution: Rundll32 (T1218.011) | | |
| | Impair Defenses: Disable or Modify Tools (T1562.001) | Restrict File and Directory Permissions (M1022), Restrict Registry Permissions (M1024) | |
| | Valid Accounts (T1078) | Password Policies (M1072), Privileged Account Management (M1026) | |
| **Credential Access** | OS Credential Dumping (T1003) | Active Directory Configuration (M1015), Credential Access Protection (M1043), Operating System Configuration (M1028), Privileged Account Management (M1026), Privileged Process Integrity (M1025), User Training (M1017) | Threat Hunting Framework, Group-IB Education |
| | Brute Force (T1110) | Account Use Policies (M1036), Multi-factor Authentication (M1032) | Security Assessment |
| | Credentials from Password Stores (T1555) | Password Policies (M1027) | Threat Hunting Framework |
| | Unsecured Credentials (T1552) | Active Directory Configuration (M1015), Audit (M1047), Operating System Configuration (M1028), Privileged Account Management (M1026), Password Policies (M1027), Update Software (M1017), User Training (M1017) | Threat Hunting Framework, Group-IB Education |
| **Discovery** | Account Discovery (T1087) | Audit (M1047), Network Segmentation (M1030) | Threat Hunting Framework |
| | Domain Trust Discovery (T1482) | Audit (M1047), Network Segmentation (M1030) | |
| | Permission Groups Discovery (T1069) | - | |
| | Process Discovery (T1057) | - | |
| | Remote System Discovery (T1018) | - | |
| **Lateral Movement** | Lateral Tool Transfer (T1570) | Filter Network Traffic (M1037), Network Intrusion Prevention (M1031) | Threat Hunting Framework |
| | Remote Services: Remote Desktop Protocol (T1021.001) | Audit (M1047), Disable or Remove Feature or Program (M1042), Limit Access to Resource Over Network (M1035), Multi-factor Authentication (M1032), Network Segmentation (M1030), Operating System Configuration (M1028), Privileged Account Management (M1026), User Account Management (M1018) | |
| | Remote Services: SMB/Windows Admin Shares (T1021.002) | Filter Network Traffic (M1037), Limit Access to Resource Over Network (M1035), Password Policies (M1027), Privileged Account Management (M1026) | |
| | Remote Services: Windows Remote Management (T1021.006) | Disable or Remove Feature or Program (M1042), Network Segmentation (M1030), Privileged Account Management (M1026) | |
| | Use Alternate Authentication Material: Pass the Hash (T1550.002) | Privileged Account Management (M1026), Update Software (M1051), User Account Control (M1052), User Account Management (M1018) | |
| **Command and Control** | Application Layer Protocol: Web Protocols (T1071.001) | Network Intrusion Prevention (M1031) | Threat Hunting Framework |
| | Data Encoding (T1132) | | |
| | Encrypted Channel (T1573) | Network Intrusion Prevention (M1031), SSL/TLS Inspection (M1020) | |
| | Proxy (T1090) | Filter Network Traffic (M1037), Network Intrusion Prevention (M1031), SSL/TLS Inspection (M1020) | |
| **Exfiltration** | Exfiltration Over C2 Channel (T1041) | Network Intrusion Prevention (M1031) | Threat Hunting Framework |
| | Exfiltration Over Web Service (T1567) | Restrict Web-Based Content (M1021) | |
| | Transfer Data to Cloud Account | Filter Network Traffic (M1037) | |
| **Impact** | Data Encrypted for Impact (T1486) | Data Backup (M1053) | Threat Hunting Framework |
| | Inhibit System Recovery (T1490) | Data Backup (M1053), Operating System Configuration (M1028) | |

Group-IB, REvil Twins: Deep Dive into Prolific RaaS Affiliates' TTPs, 2021