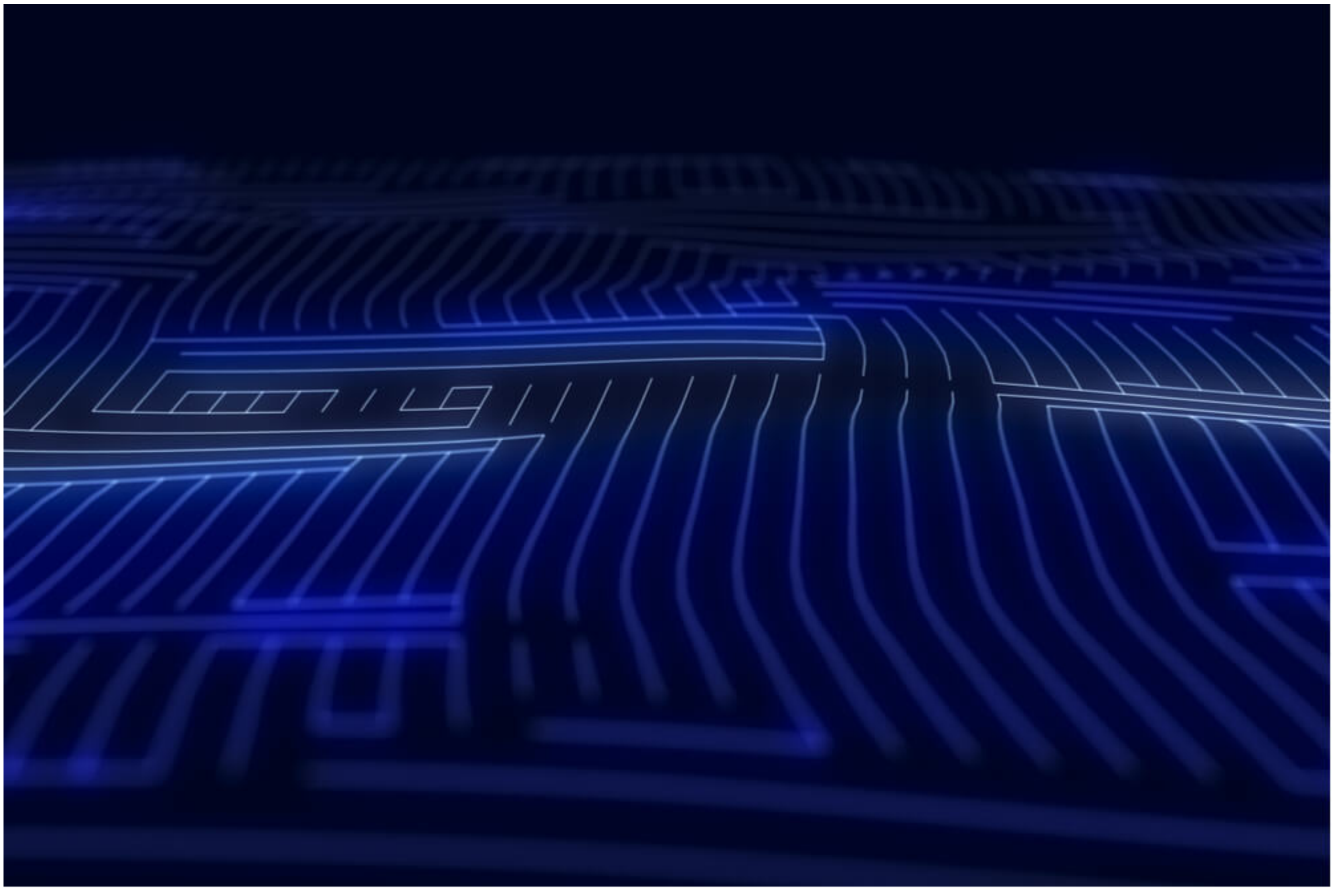
Digging up InvisiMole's hidden arsenal

welivesecurity.com/2020/06/18/digging-up-invisimole-hidden-arsenal

June 18, 2020



ESET researchers reveal the modus operandi of the elusive InvisiMole group, including newly discovered ties with the Gamaredon group

In our tracking of the InvisiMole group, which we discovered, named, and first reported on in 2018, we have found a new campaign targeting high-profile organizations in Eastern Europe. Investigating the attacks, in close cooperation with the affected organizations, we uncovered its updated toolset and previously unknown details about InvisiMole's tactics, techniques and procedures (TTPs).

In this blogpost, we summarize the findings published in full in our white paper, *InvisiMole: The hidden part of the story*.

InvisiMole: The hidden part of the story

Download Research Paper

The InvisiMole group is a threat actor operating at least since 2013. We previously documented its two backdoors, RC2CL and RC2FM, notable for their extensive spying capabilities, but we didn’t know how these backdoors were delivered, spread or installed on the system.

In this recent campaign, the InvisiMole group has resurfaced with an updated toolset, targeting a small number of high-profile organizations in the military sector and diplomatic missions, both in Eastern Europe. According to our telemetry, the attack attempts were ongoing from late 2019 to the time of writing this report.

Thanks to investigating the attacks in cooperation with the affected organizations, we were able to expose the inner workings of the updated InvisiMole toolset.

We discovered InvisiMole’s arsenal is only unleashed after another threat group, Gamaredon, has already infiltrated the network of interest, and possibly gained administrative privileges. This allows the InvisiMole group to devise creative ways to operate under the radar.

For example, the attackers use long execution chains, crafted by combining malicious shellcode with legitimate tools and vulnerable executables. They use DNS tunneling for stealthier C&C communications, and place execution guardrails on the malicious components to hide the malware from security researchers.

Delivery mechanism

During our investigation, we discovered that InvisiMole is delivered to the compromised systems by a .NET downloader detected by ESET products as MSIL/Pterodo, the work of the Gamaredon group. Gamaredon is a threat actor, operating at least since 2013, characterized by rapid development and making little effort to stay under the radar. We recently documented the newest Gamaredon components, distributed through spearphishing emails and used to move laterally as far as possible within the target’s network, while fingerprinting the machines.

Our research now shows Gamaredon is used to pave the way for a far stealthier payload – according to our telemetry, a small number of Gamaredon’s targets are “upgraded” to the advanced InvisiMole malware, likely those deemed particularly significant by the attackers.

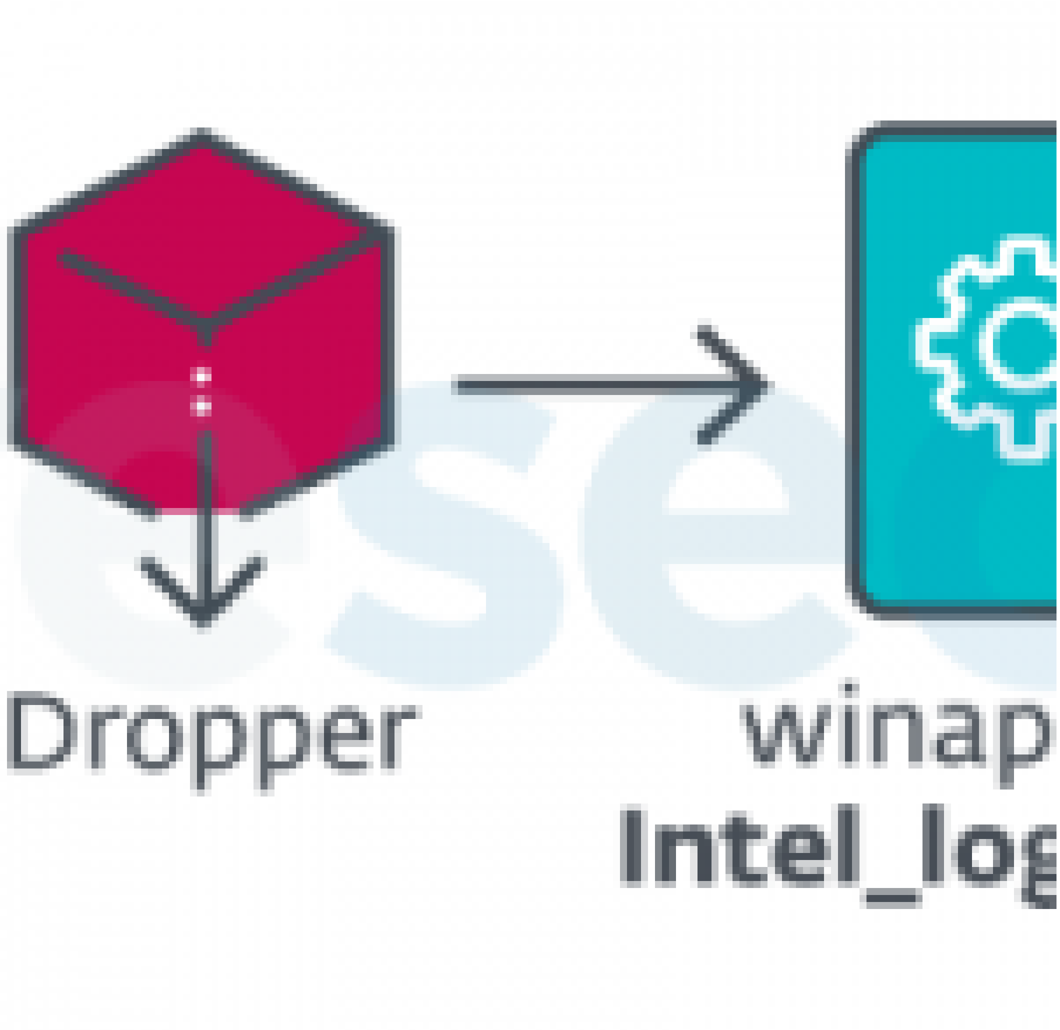


Figure 1. Gamaredon's .NET downloader can "upgrade" the victim's machine to InvisiMole's TCP downloader

As we detail in the white paper, despite the evidence of collaboration, we consider Gamaredon and InvisiMole to be two distinct groups with different TTPs, rather than a single threat actor.

Spreading and updating mechanisms

We document three ways that InvisiMole spreads within compromised networks:

- Using the BlueKeep vulnerability in the RDP protocol (CVE-2019-0708)
- Using the EternalBlue vulnerability in the SMB protocol (CVE-2017-0144)
- Using trojanized documents and software installers, crafted using benign files stolen from the compromised organization

To craft the trojanized files, InvisiMole first steals documents or software installers from the compromised organization, and then creates an SFX archive that bundles the file with the InvisiMole installer. The original file is then replaced with the weaponized version, while its name, icon and metadata are preserved. The attackers rely on the users to share and execute these files.

This lateral movement technique is especially powerful if the trojanized file happens to be a software installer placed on a central server – a common way to deploy software in larger organizations. That way, InvisiMole is organically distributed to many computers that use this server.

Regardless of the spreading method, the first InvisiMole component deployed on the newly-compromised machines is always InvisiMole's TCP downloader – a simple addition to the toolset that downloads the next stage of the infiltration.

The second addition to the updated InvisiMole toolset, the DNS downloader, has the same functionality but is designed for long-term, covert access to the machine. It uses a stealthier method of C&C communication, using a technique called *DNS tunneling* (see Figure 2).

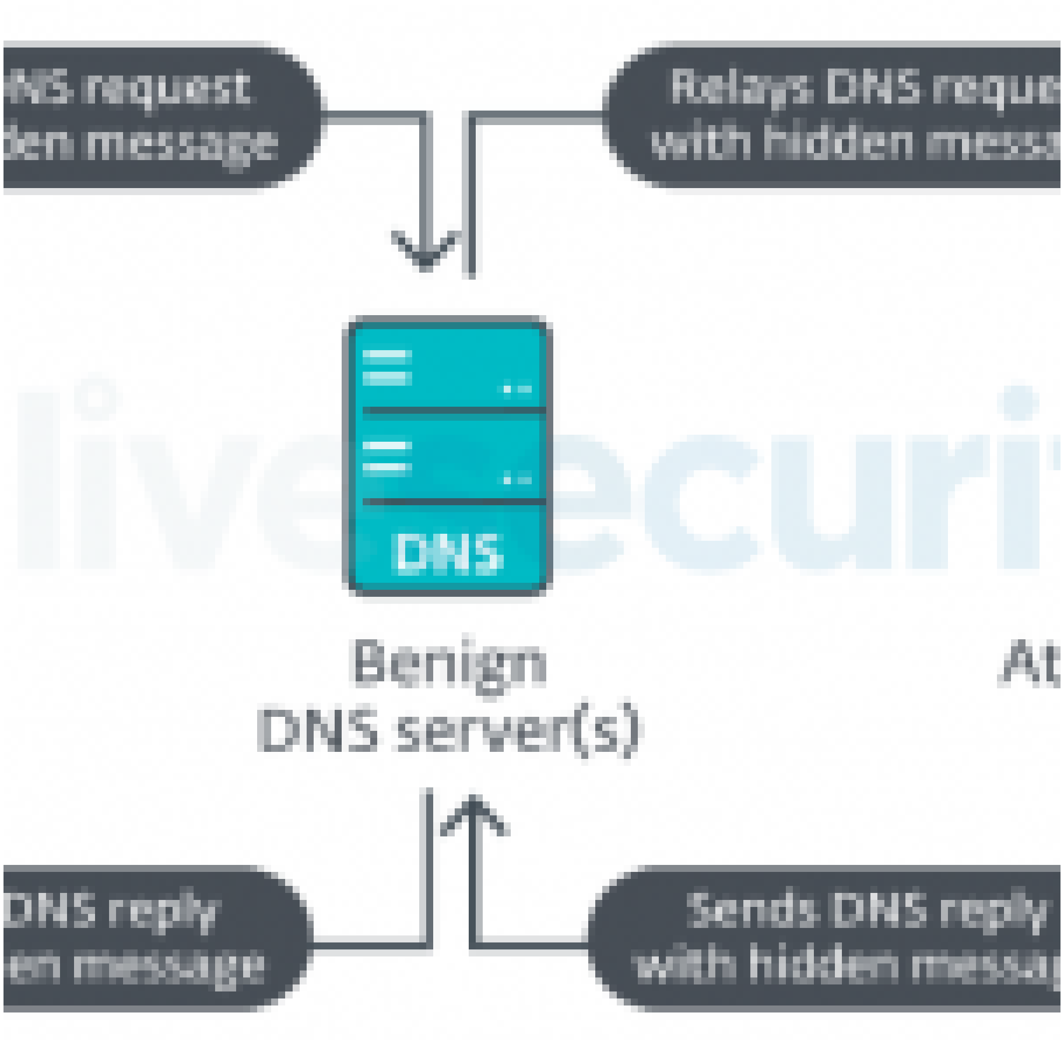


Figure 2. DNS tunneling

With DNS tunneling, the compromised client does not directly contact the C&C server; it only communicates with the benign DNS server(s) the victim machine would normally communicate with, where it sends requests to resolve a domain to its IP address. The DNS server then contacts the name server responsible for the domain in the request, which is an attacker-controlled name server, and relays its response back to the client.

The actual C&C communication is embedded in the DNS requests and replies, unbeknownst to the benign DNS server that operates as an intermediary in the communication.

Execution chains

The most notable feature of the newest InvisiMole toolset is its long execution chains, used to deploy the final payloads – the updated RC2CM and RC2CL backdoors, and the new TCP and DNS downloaders.

We reconstructed four execution chains, used by the attackers in various situations – based on the OS version of the victim's computer, and on whether they were able to gain administrative privileges on the system:

- The *Control Panel misuse chain* uses a rare technique known from Vault 7 leaks, used to achieve covert execution in the context of the Control Panel.
- The *SMInit exploit chain* exploits a vulnerability in the legitimate Total Video Player software. It is used in cases where the attackers haven't managed to obtain administrative privileges on the system.
- The *Speedfan exploit chain* exploits a local privilege escalation vulnerability in the speedfan.sys driver to inject its code to a trusted process from kernel mode.
- The *Wdigest exploit chain* is InvisiMole's flagship chain, the most elaborate, used on the newest versions of Windows, where the attackers have administrative privileges. It exploits a vulnerability in the Windows wdigest.dll library and then uses an improved *ListPlanting* technique to inject its code into a trusted process.

The vulnerable executables used in these chains are all introduced to the system by InvisiMole – the variation of this technique with a vulnerable driver has been previously referred to as *Bring Your Own Vulnerable Driver* by fellow researchers. For the other cases, we have named the technique *Bring Your Own Vulnerable Software*.

We document these tactics in detail in the *Execution chains* section of our white paper.

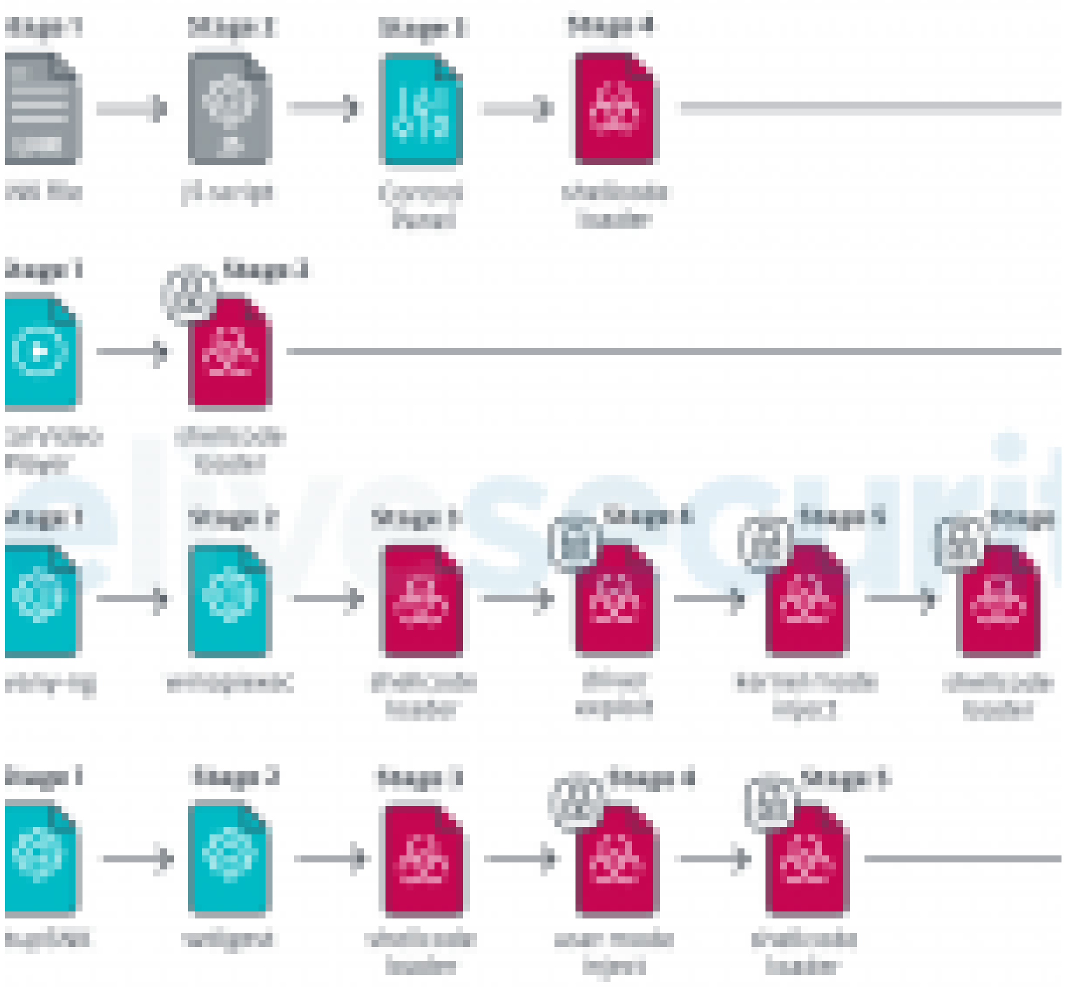


Figure 3. InvisiMole's execution chains; padlocks indicate use of per-machine encryption

Note the heavy use of legitimate tools and per-victim encryption, shown in the overview of these four chains in Figure 3. It is the tactic of InvisiMole's operators to exclusively install legitimate tools, and reserve the malicious payloads for later stages.

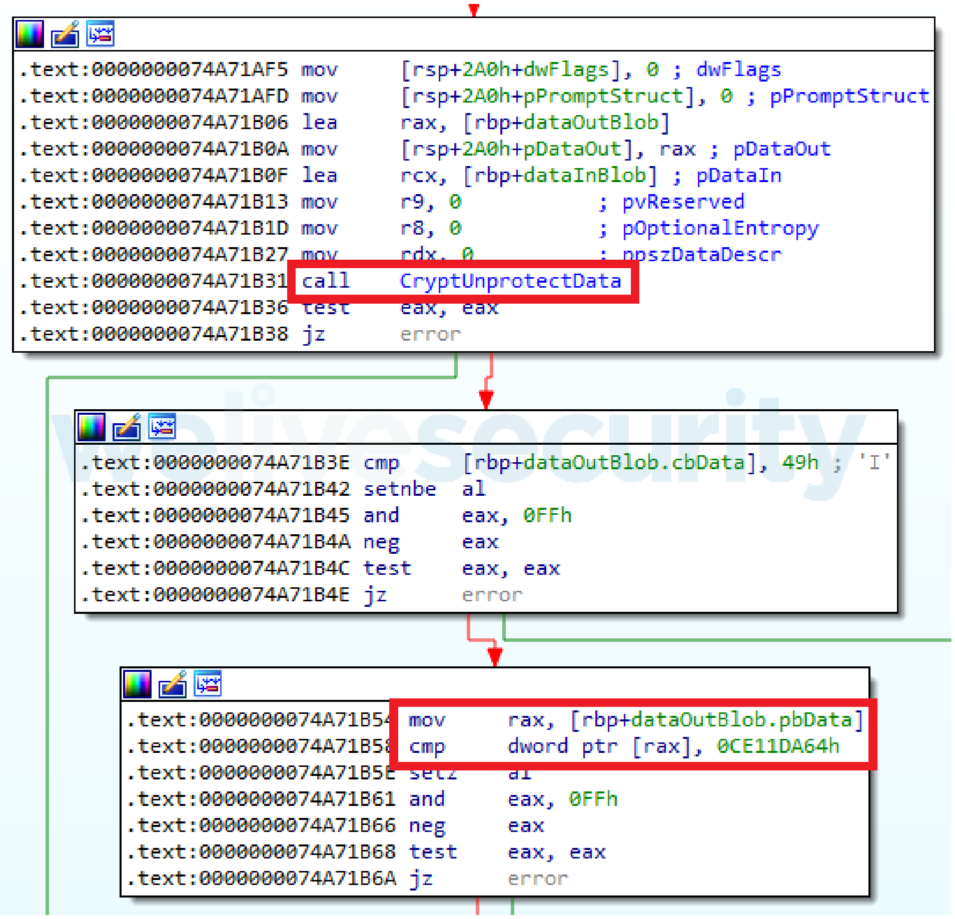
To place execution guardrails and encrypt the payloads individually per-victim, InvisiMole uses a Windows feature called Data Protection API (DPAPI), specifically:

- the CryptProtectData API for data encryption
- the CryptUnprotectData API for data decryption

This symmetric encryption scheme uses a key derived from the user's logon secrets, so the decryption must be performed on the same computer where the data were encrypted.

Figure 4 shows a fragment of a typical InvisiMol loader that uses CryptUnprotectData for decryption and then checks whether the decrypted blob starts with a characteristic InvisiMole four-byte magic value:

- 64 DA 11 CE for 64-bit payloads
- 86 DA 11 CE for 32-bit payloads



```
.text:0000000074A71AF5 mov     [rsp+2A0h+dwFlags], 0 ; dwFlags
.text:0000000074A71AFD mov     [rsp+2A0h+pPromptStruct], 0 ; pPromptStruct
.text:0000000074A71B06 lea     rax, [rbp+dataOutBlob]
.text:0000000074A71B0A mov     [rsp+2A0h+pDataOut], rax ; pDataOut
.text:0000000074A71B0F lea     rcx, [rbp+dataInBlob] ; pDataIn
.text:0000000074A71B13 mov     r9, 0           ; pvReserved
.text:0000000074A71B1D mov     r8, 0           ; pOptionalEntropy
.text:0000000074A71B27 mov     rdx, 0          ; ppszDataDescr
.text:0000000074A71B31 call    CryptUnprotectData
.text:0000000074A71B36 test    eax, eax
.text:0000000074A71B38 jz      error
```

```
.text:0000000074A71B3E cmp     [rbp+dataOutBlob.cbData], 49h ; 'I'
.text:0000000074A71B42 setnbe  al
.text:0000000074A71B45 and     eax, 0FFh
.text:0000000074A71B4A neg     eax
.text:0000000074A71B4C test    eax, eax
.text:0000000074A71B4E jz      error
```

```
.text:0000000074A71B54 mov     rax, [rbp+dataOutBlob.pbData]
.text:0000000074A71B58 cmp     dword ptr [rax], 0CE11DA64h
.text:0000000074A71B5E setz    al
.text:0000000074A71B61 and     eax, 0FFh
.text:0000000074A71B66 neg     eax
.text:0000000074A71B68 test    eax, eax
.text:0000000074A71B6A jz      error
```

Figure 4. Fragment of a characteristic InvisiMole loader

The DPAPI feature, intended for local storage of credentials such as Wi-Fi passwords or login passwords in web browsers, is abused by InvisiMole to protect its payload from security researchers. Even if they find InvisiMole's components in telemetry or on malware sharing platforms, they can't decrypt them outside the victim's computer.

However, thanks to direct cooperation with the affected organizations, we were able to recover the payloads and reconstruct four of InvisiMole's execution chains, which are described in detail in the white paper.

Conclusion

When we first reported about InvisiMole in 2018, we highlighted its covert workings and complex range of capabilities. However, a large part of the picture was missing.

After discovering new activity in late 2019, we gained the opportunity to take a proper look under the hood of InvisiMole's operations and piece together the hidden parts of the story. Analyzing the group's updated toolset, we observed continuous development and substantial improvements, with special focus on staying under the radar.

Our investigation also revealed a previously unknown cooperation between InvisiMole and the Gamaredon group, with Gamaredon's malware used to infiltrate the target network and deliver the sophisticated InvisiMole malware to targets of special interest.

Having provided a detailed report on InvisiMole's TTPs, we will continue to track the group's malicious activities.

ESET detection names and other Indicators of Compromise for these campaigns can be found in the full white paper, InvisiMole: The hidden part of the story.

Acknowledgements to fellow ESET malware researchers Matthieu Faou, Ladislav Janko and Michal Poslušný for their work on this investigation.

MITRE ATT&CK techniques

Note: For better readability, we have separated the RC2FM and RC2CL backdoors into their respective ATT&CK mapping tables, because of their rich capabilities. The first mapping pertains to InvisiMole's supporting components used for delivery, lateral movement, execution chains, and for downloading additional payloads.

InvisiMole

Tactic	ID	Name	Description
Execution	T1196	Control Panel Items	InvisiMole's loader is masked as a CPL file, misusing control panel items for execution.
T1106	Execution through API	InvisiMole has used ShellExecuteW and CreateProcessW APIs to execute files.	
T1129	Execution through Module Load	InvisiMole implements a custom loader for its components (InvisiMole blobs).	
T1203	Exploitation for Client Execution	InvisiMole has delivered vulnerable Total Video Player software and wdigest.dll library and exploited their stack overflow and input validation vulnerabilities, respectively, to gain covert code execution.	
T1085	Rundll32	InvisiMole has used rundll32.exe as part of its execution chain.	
T1053	Scheduled Task	InvisiMole has used Windows task scheduler as part of its execution chains.	
T1064	Scripting	InvisiMole has used a JavaScript file named Control.js as part of its execution chain.	
T1035	Service Execution	InvisiMole has registered a Windows service as one of the ways to execute its malicious payload.	

Tactic	ID	Name	Description
T1204	User Execution	InvisiMole has been delivered as trojanized versions of software and documents, using deceiving names and icons and relying on user execution.	
Persistence	T1050	New Service	InvisiMole has registered a Windows service named clr_optimization_v2.0.51527_X86 to achieve persistence.
T1060	Registry Run Keys / Startup Folder	InvisiMole has placed a LNK file in Startup Folder to achieve persistence.	
T1053	Scheduled Task	InvisiMole has scheduled tasks under names MSST and \Microsoft\Windows\Autochk\Scheduled to achieve persistence.	
T1023	Shortcut Modification	InvisiMole has placed a LNK file in Startup Folder to achieve persistence.	
Privilege Escalation	T1088	Bypass User Account Control	InvisiMole can bypass UAC to obtain elevated privileges.
T1068	Exploitation for Privilege Escalation	InvisiMole has exploited CVE-2007-5633 vulnerability in speedfan.sys driver to obtain kernel mode privileges.	
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	InvisiMole decrypts strings using variations of XOR cipher. InvisiMole decrypts its components using the CryptUnprotectData API and two-key triple DES.
T1480	Execution Guardrails	InvisiMole has used Data Protection API to encrypt its components on the victim’s computer, to evade detection and make sure the payload can only be decrypted (and then loaded) on one specific compromised computer.	
T1143	Hidden Window	InvisiMole has executed legitimate tools in hidden windows and used them to execute malicious InvisiMole components.	
T1066	Indicator Removal from Tools	InvisiMole has undergone technical improvements in attempt to evade detection.	
T1202	Indirect Command Execution	InvisiMole has used winapiexec tool for indirect execution of Windows API functions.	

Tactic	ID	Name	Description
T1027	Obfuscated Files or Information	InvisiMole has obfuscated strings and code to make analysis more difficult, and encrypted its components to thwart detection.	
T1055	Process Injection	InvisiMole has injected its code into trusted processes using an improved ListPlanting technique and via APC queue.	
T1108	Redundant Access	InvisiMole has deployed multiple backdoors on a single compromised computer.	
T1085	Rundll32	InvisiMole has used rundll32.exe as part of its execution chain.	
T1064	Scripting	InvisiMole's loader uses a JavaScript script as a part of setting up persistence.	
T1063	Security Software Discovery	InvisiMole's DNS plugin avoids connecting to the C&C server if selected network sniffers are detected running.	
T1099	Timestomp	InvisiMole has modified timestamps of files that it creates or modifies.	
T1036	Masquerading	InvisiMole has attempted to disguise its droppers as legitimate software or documents, and to conceal itself by registering under a seemingly legitimate service name.	
Discovery	T1046	Network Service Scanning	InvisiMole has performed network scanning within the compromised network using its Portscan and BlueKeep components, in order to search for open ports and for hosts vulnerable to the BlueKeep vulnerability.
T1518	Software Discovery	InvisiMole's DNS downloader attempts to detect selected network sniffer tools, and pauses its network traffic if any are detected running.	
T1082	System Information Discovery	InvisiMole's DNS downloader collects computer name and system volume serial number.	
T1124	System Time Discovery	InvisiMole can collect the timestamp from the victim's machine.	

Tactic	ID	Name	Description
Lateral Movement	T1210	Exploitation of Remote Services	InvisiMole has exploited EternalBlue and BlueKeep vulnerabilities for lateral movement.
	T1080	Taint Shared Content	InvisiMole has replaced legitimate software or documents in the compromised network with their trojanized versions, in an attempt to propagate itself within the network.
Command and Control	T1043	Commonly Used Port	InvisiMole's downloader uses port 443 for C&C communication. InvisiMole's DNS plugin uses port 53 for C&C communication.
	T1090	Connection Proxy	InvisiMole's TCP downloader is able to utilize user-configured proxy servers for C&C communication.
	T1024	Custom Cryptographic Protocol	InvisiMole's TCP and DNS downloaders use a custom cryptographic protocol for encrypting network communication.
	T1132	Data Encoding	InvisiMole's DNS downloader uses a variation of base32 encoding to encode data into the subdomain in its requests.
	T1008	Fallback Channels	InvisiMole's TCP and DNS downloaders are configured with several C&C servers.
	T1105	Remote File Copy	InvisiMole's TCP and DNS downloaders can download additional files to be executed on the compromised system.
	T1071	Standard Application Layer Protocol	InvisiMole's DNS downloader uses DNS protocol for C&C communication.
	T1095	Standard Non-Application Layer Protocol	InvisiMole's TCP downloader uses TCP protocol for C&C communication.
	T1065	Uncommonly Used Port	InvisiMole's TCP downloader uses port 1922 for C&C communication.

RC2CL backdoor

Tactic	ID	Name	Description

Tactic	ID	Name	Description
Execution	T1059	Command-Line Interface	RC2CL backdoor can create a remote shell to execute commands.
T1106	Execution through API	RC2CL backdoor uses CreateProcess and CreateProcessAsUser APIs to execute files.	
Privilege Escalation	T1134	Access Token Manipulation	RC2CL backdoor can use CreateProcessAsUser API to start a new process under the context of another user or process.
T1088	Bypass User Account Control	RC2CL backdoor can disable and bypass UAC to obtain elevated privileges.	
Defense Evasion	T1090	Connection Proxy	RC2CL backdoor can be configured as a proxy relaying communication between other compromised computers and C&C server.
T1140	Deobfuscate/Decode Files or Information	RC2CL backdoor decrypts strings using variations of XOR cipher.	
T1089	Disabling Security Tools	RC2CL backdoor is able to disable Windows firewall.	
T1107	File Deletion	RC2CL backdoor can delete dropped artifacts, and various files on-demand following a delete command. RC2CL backdoor can safely delete files to thwart forensic analysis.	
T1112	Modify Registry	RC2CL backdoor hides its configuration within registry keys.	
T1027	Obfuscated Files or Information	RC2CL backdoor obfuscates/encrypts strings and code to make analysis more difficult.	
T1099	Timestomp	RC2CL backdoor modifies timestamps of files that it creates/modifies.	
T1497	Virtualization/Sandbox Evasion	RC2CL backdoor is able to detect virtualized environments.	
Discovery	T1087	Account Discovery	RC2CL backdoor can list account information and session information.

Tactic	ID	Name	Description
T1010	Application Window Discovery	RC2CL backdoor can list information about active windows.	
T1083	File and Directory Discovery	RC2CL backdoor can list files, and specifically recently opened files, and list information about mapped/unmapped drives.	
T1046	Network Service Scanning	RC2CL backdoor is able to scan the compromised network for hosts vulnerable to EternalBlue vulnerability.	
T1057	Process Discovery	RC2CL backdoor can list running processes.	
T1012	Query Registry	RC2CL backdoor can query registry to obtain information about installed software, applications accessed by users, applications executed on user login/system start, recently opened files,	
T1063	Security Software Discovery	RC2CL backdoor modifies its behavior if Bitdefender firewall is enabled, or if selected AV processes are detected running.	
T1518	Software Discovery	RC2CL backdoor can list installed software, recently accessed software by users, software executed on each user login and/or each system start.	
T1082	System Information Discovery	RC2CL backdoor can list information about loaded drivers, computer name, OS version, memory status, local time, system and process DEP policy.	
T1016	System Network Configuration Discovery	RC2CL backdoor can list IP table; configured proxy information; information about enabled wireless networks for geolocation of the victims.	
T1007	System Service Discovery	RC2CL backdoor can list system service information.	
Collection	T1123	Audio Capture	RC2CL backdoor can record the sounds from microphones on a computer. RC2FM misuses a legitimate lame.dll for MP3 encoding of the recordings.

Tactic	ID	Name	Description
T1005	Data from Local System	RC2CL backdoor can collect data from the system, and can monitor changes in specified directories.	
T1074	Data Staged	RC2CL backdoor can store collected data in a central location for a later exfiltration.	
T1113	Screen Capture	RC2CL backdoor can capture screenshots of the victim’s screen. RC2CL backdoor can also capture screenshots of separate windows.	
T1125	Video Capture	RC2CL backdoor can access victim’s webcam and capture photos/record videos.	
Command and Control	T1008	Fallback Channels	RC2CL backdoor is configured with several C&C servers. Via a backdoor command, it is possible to extend the list and change which C&C server is used.
T1105	Remote File Copy	InvisiMole can download additional files to be executed on the compromised system.	
T1065	Uncommonly Used Port	RC2CL backdoor uses port 1922 for C&C communication.	
Exfiltration	T1002	Data Compressed	RC2CL backdoor can create zlib and SFX archives. It misuses a copy of the legitimate WinRAR tool for compression and decompression.
T1022	Data Encrypted	RC2CL backdoor uses variations of XOR cipher to encrypt data.	
T1041	Exfiltration Over Command and Control Channel	RC2CL backdoor exfiltrates collected information over its C&C channel.	

RC2FM backdoor

Tactic	ID	Name	Description
Execution	T1059	Command-Line Interface	RC2FM backdoor can create a remote shell to execute commands.

Tactic	ID	Name	Description
	T1106	Execution through API	RC2FM backdoor supports a command that uses ShellExecute and CreateProcess APIs to execute files.
Privilege Escalation	T1088	Bypass User Account Control	RC2FM backdoor can bypass UAC to obtain elevated privileges.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	RC2FM backdoor decrypts strings using variations of XOR cipher.
	T1107	File Deletion	RC2FM backdoor can delete dropped artifacts, and various files on-demand following a delete command.
	T1143	Hidden Window	RC2FM backdoor uses CREATE_NO_WINDOW creation flag to execute malware in a hidden window.
	T1112	Modify Registry	RC2FM backdoor hides its configuration within registry keys.
	T1027	Obfuscated Files or Information	RC2FM backdoor obfuscates/encrypts strings and code to make analysis more difficult.
	T1055	Process Injection	RC2FM backdoor can inject itself into ctfmon.exe , dwm.exe , sihost.exe and taskhost.exe processes.
	T1085	Rundll32	RC2FM backdoor uses rundll32.exe to load a stub DLL into which it then injects itself.
	T1099	Timestamp	RC2FM backdoor modifies timestamps of files that it creates/modifies.
	T1497	Virtualization/Sandbox Evasion	RC2FM backdoor is able to detect virtualized environments.
Discovery	T1083	File and Directory Discovery	RC2FM backdoor collects information about mapped drives. It can list files in a specific folder.
	T1057	Process Discovery	RC2FM backdoor can list running processes.

Tactic	ID	Name	Description
T1082	System Information Discovery	RC2FM backdoor collects computer name and system volume serial number.	
T1016	System Network Configuration Discovery	RC2FM backdoor lists information about configured proxy servers.	
Collection	T1123	Audio Capture	RC2FM backdoor can record the sounds from microphones on a computer. It misuses a legitimate lame.dll for MP3 encoding of the recordings.
T1025	Data from Removable Media	RC2FM backdoor can collect jpeg files from connected MTP devices.	
T1056	Input Capture	RC2FM backdoor can collect keystrokes.	
T1113	Screen Capture	RC2FM backdoor can capture screenshots of the victim’s screen.	
Command and Control	T1043	Commonly Used Port	RC2FM backdoor uses port 80 for C&C communication.
T1090	Connection Proxy	RC2FM backdoor can use proxies configured on the local system, for various installed and portable browsers, if direct connection to the C&C server fails.	
T1008	Fallback Channels	RC2FM backdoor is configured with several C&C servers. It is possible to update the C&C server by a backdoor command.	
T1105	Remote File Copy	InvisiMole can download additional files to be executed on the compromised system.	
T1071	Standard Application Layer Protocol	RC2FM backdoor uses HTTP for C&C communication.	
Exfiltration	T1022	Data Encrypted	RC2FM backdoor uses variations of XOR cipher to encrypt data.
T1041	Exfiltration Over Command and Control Channel	RC2FM backdoor exfiltrates collected information over its C&C channel.	

18 Jun 2020 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion