

ESET RESEARCH

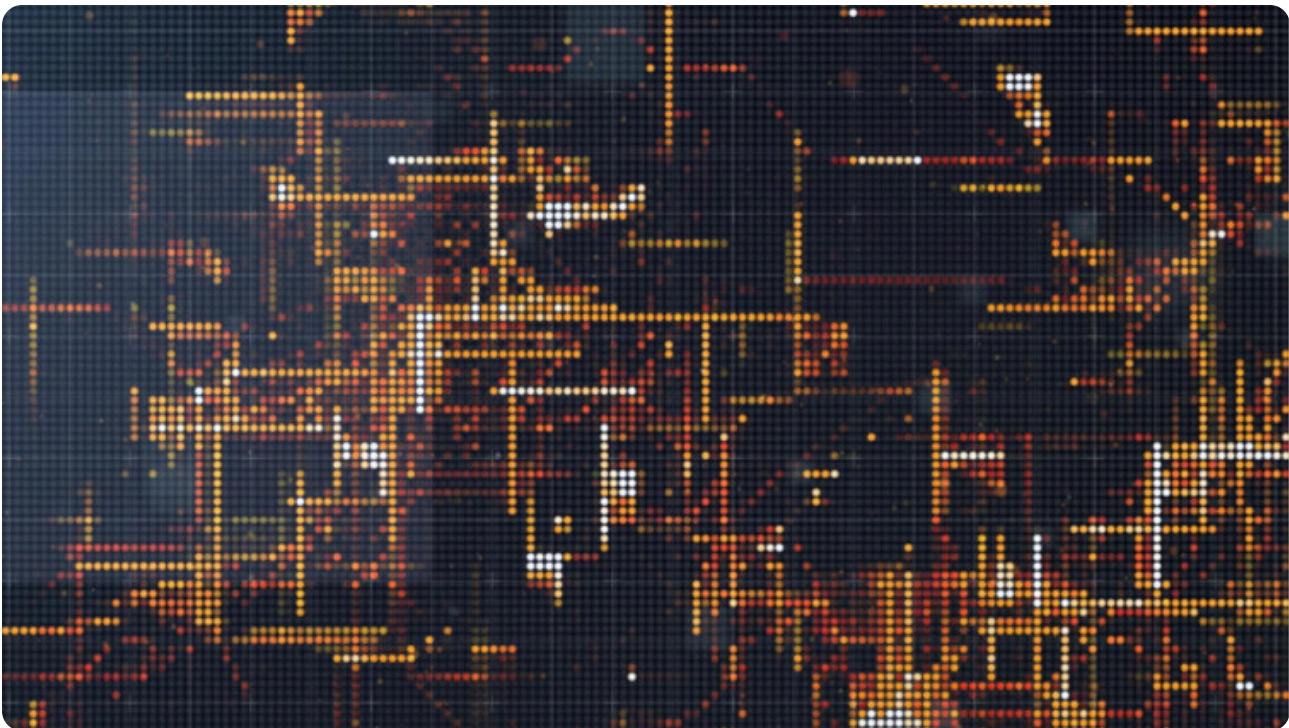
More evil: A deep look at Evilnum and its toolset

ESET research gives a detailed picture of the operations of the Evilnum group and its toolkit deployed in attacks against carefully chosen targets in the fintech sector



Matías Porolli

09 Jul 2020 • 19 min. read



Share Article













Digital Security
Progress. Protected.

APT Activity Report

IRAN-ALIGNED CYBERATTACKS:
RISE IN DISRUPTIVE OPERATIONS

(eset):research

READ NOW



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Accept all and close

Manage cookies

ESET has analyzed the operations of Evilnum, the APT group behind the Evilnum malware previously seen in attacks against financial technology companies. While said malware has been seen in the wild since at least 2018 and documented previously, little has been published about the group behind it and how it operates.

In this article we connect the dots and disclose a detailed picture of Evilnum’s activities. The group's targets remain fintech companies, but its toolset and infrastructure have evolved and now consist of a mix of custom, homemade malware combined with tools purchased from Golden Chickens, a Malware-as-a-Service (MaaS) provider whose infamous customers include FIN6 and Cobalt Group.

Targets

According to ESET’s telemetry, the targets are financial technology companies – for example, companies that offer platforms and tools for online trading. Although most of the targets are located in EU countries and the UK, we have also seen attacks in countries such as Australia and Canada. Typically, the targeted companies have offices in several locations, which probably explains the geographical diversity of the attacks.

The main goal of the Evilnum group is to spy on its targets and obtain financial information from both the targeted companies and their customers. Some examples of the information this group steals include:

- Spreadsheets and documents with customer lists, investments and trading operations
- Internal presentations
- Software licenses and credentials for trading software/platforms
- Cookies and session information from browsers
- Email credentials
- Customer credit card information and proof of address/identity documents






According to what we have seen during our investigation, the group has also gained access to IT-related information such as VPN configurations.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

tain a link to a ZIP file
aka shortcut) files that
e displaying a decoy
try to trick the user
pictures (in Windows,
the contents of one of

Name	Date modified	Type	Size
 Credit Card Back.jpg	20/04/05 02:26	Shortcut	62 KB
 Credit Card Front.png	20/03/16 05:09	Shortcut	474 KB
 Driv License Back.jpg	20/03/05 19:49	Shortcut	262 KB
 Driv License Front.jpg	20/03/05 19:49	Shortcut	167 KB
 Utility Bill.jpg	20/03/31 02:46	Shortcut	89 KB

5 items

Figure 1. Malicious LNK files

Once a shortcut file is opened (it doesn't matter which one, as they all do the same thing), it looks in the contents of its own file for lines with a specific marker and writes them to a .js file. Then this malicious JavaScript file is executed and it writes and opens a decoy file with the same name as the shortcut, but with the correct extension. It also deletes the shortcut file. The documents used as decoys are mostly photos of credit cards, identity documents, or bills with proof of address, as many financial institutions require these documents from their customers when they join, according to regulations (this is known as "Know Your Customer"). One such decoy is shown in Figure 2 (blurred for privacy).



decoy



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

...t they have been
...ts are collected actively
...port representatives
... documents from their
...rgets, unless the

...d can deploy other
...nponents or several
... component by other
... referred to as Evilnum.

We have named the group Evilnum as that is the name of their fleecing malware

we have named the group Evilnum as that is the name of their flagship malware, and we'll refer to the various malware pieces as components. An overview of these is shown in Figure 3.

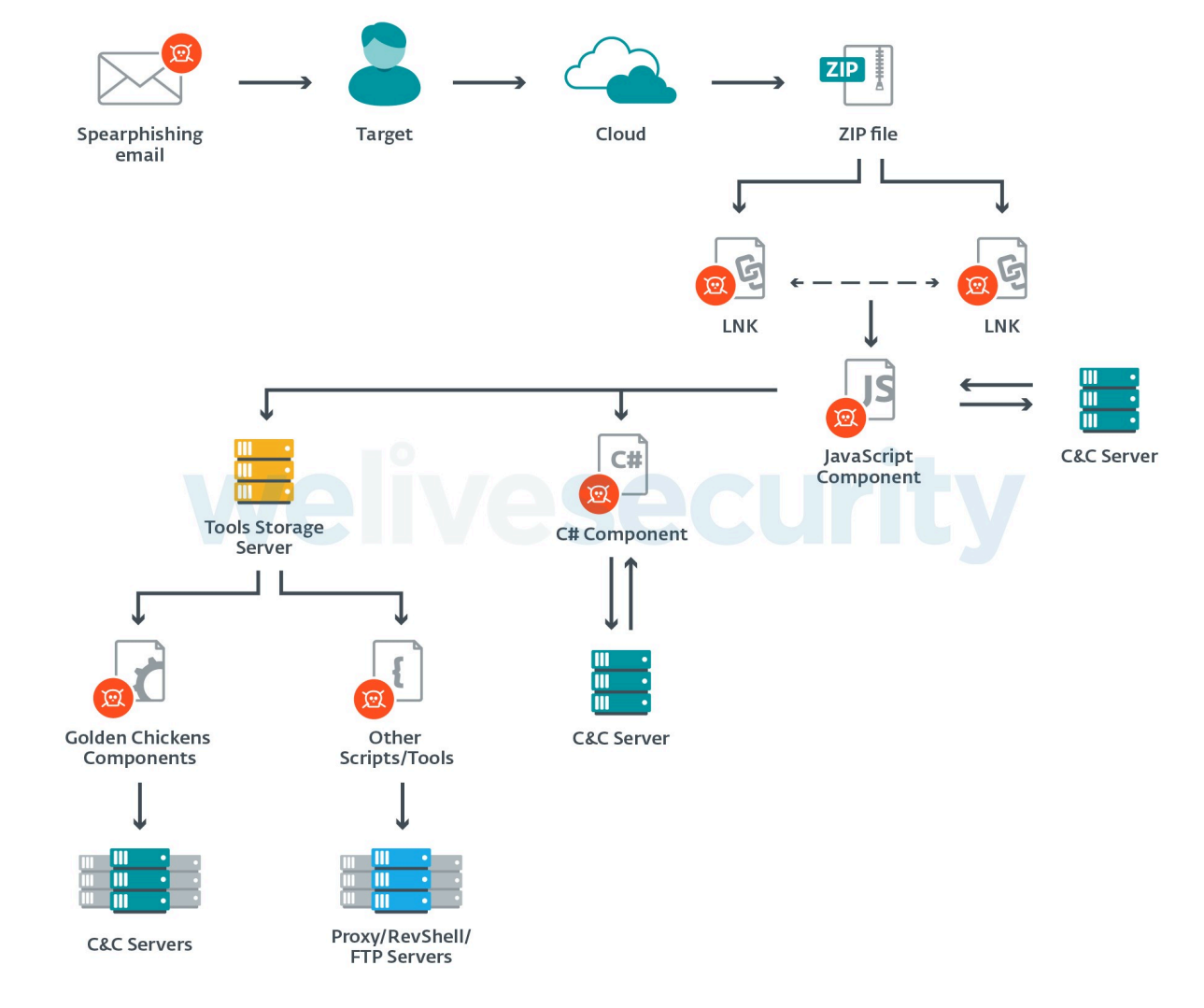


Figure 3. Evilnum components

Each of the various components has its own C&C server, and each component operates independently. The operators of the malware manually send commands to install additional components and use post-compromise scripts and tools if they consider them necessary.

Most servers used by the malware are referenced by IP addresses; domain names have not been used. The only exceptions are the C&C servers used by the Golden Chickens components; malware purchased from a MaaS provider, as we describe later.

Those referenced by an IP address can be split into two groups, based on the hosting provider. The majority of them are hosted with FreeHost, a Ukrainian



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

as a backdoor without
cks that we have seen,
fit and used the JS

May 2018 in [this](#)
ve illustrate these

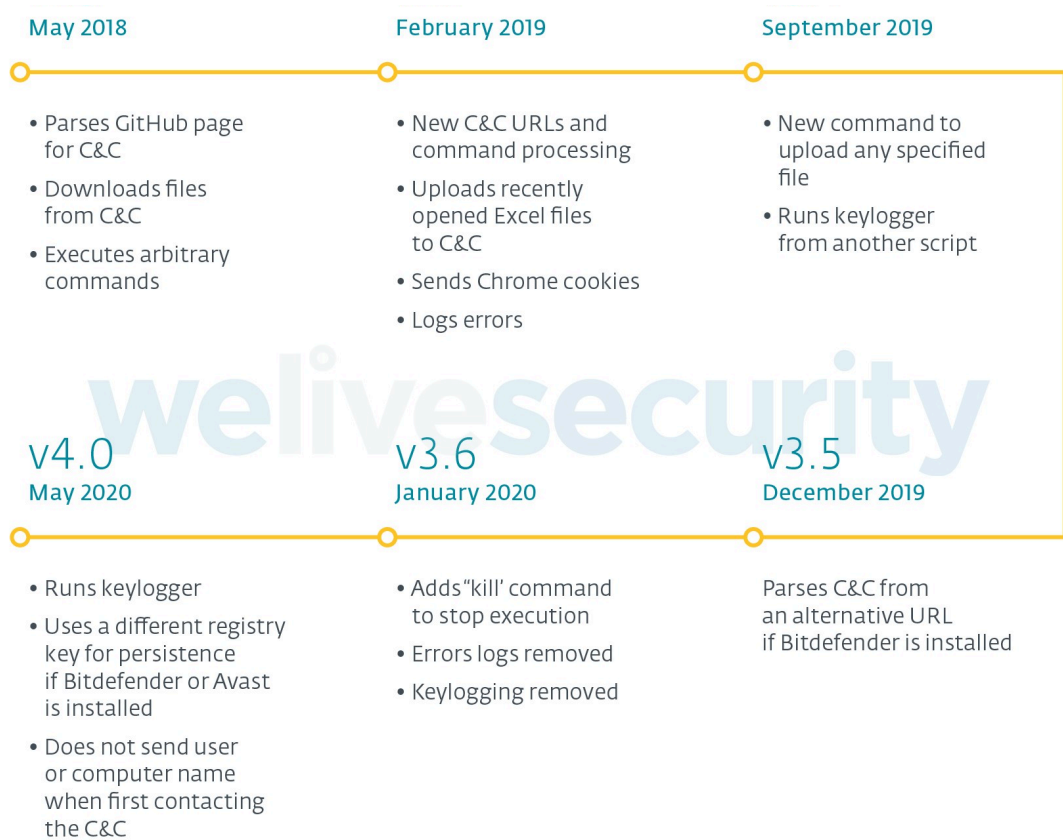
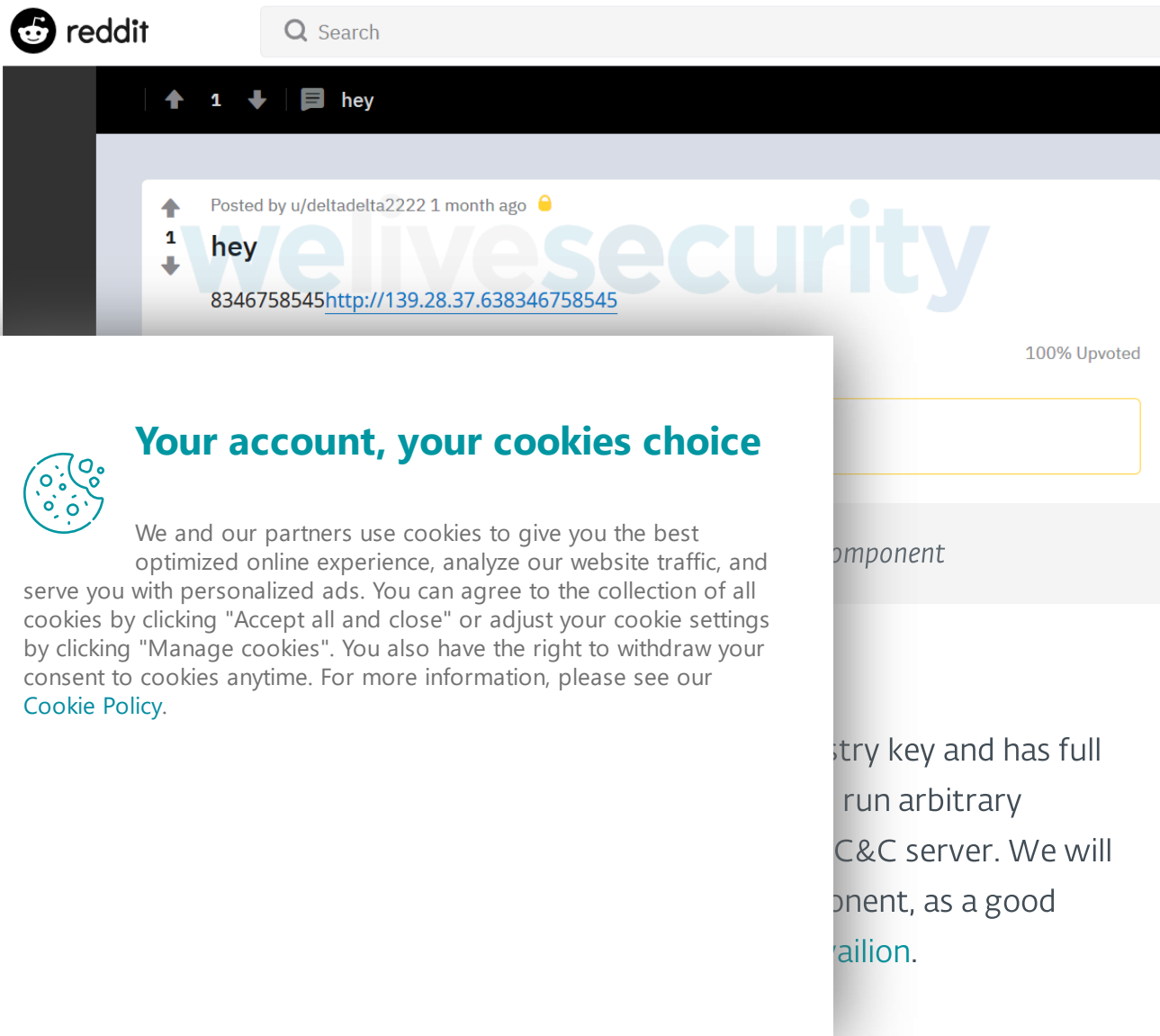


Figure 4. Timeline of changes in JS component

Differences between version 1.3 and the others are noteworthy, as the server-side code for the C&C was changed and commands are different. In that early version it was not possible to upload files to the C&C, only to download files to the victim’s computer. Also, as new versions appeared, the malware was extended with some Python scripts (see the *Post-compromise toolset* section) and external tools such as [ChromeCookiesView](#).

Despite the differences, the core functionalities remain the same in all versions, including the retrieval of the C&C server’s address from GitHub, GitLab or Reddit pages created specifically for that purpose. Figure 5 shows an example of a Reddit page that is parsed by the malware to retrieve a C&C address.



C# Component: Evil, not so evil

In March 2019, [Palo Alto Networks described malware](#) with very similar functionality to the JS component, but coded in C#. That version (2.5) obtained the address of its C&C by dividing a number by 666, and was therefore named Evilnum by Palo Alto Networks researchers. Since then there have been new versions of the C# malware, the latest of them being version 4.0, which we first saw in April 2020. The number 666 is not used anymore and the PDB paths of the executables show that the developers call their malware “Marvel”. However, we will continue to name the malware Evilnum to avoid creating confusion.

The latest version comes bundled in an MSI file (Windows Installer) and runs independent of the JS component. Furthermore, it has different C&Cs than the JS component. However, in all cases that we have seen, the C# component was downloaded and executed after the JavaScript malware gained initial access. The structure of this component is shown in Figure 6.

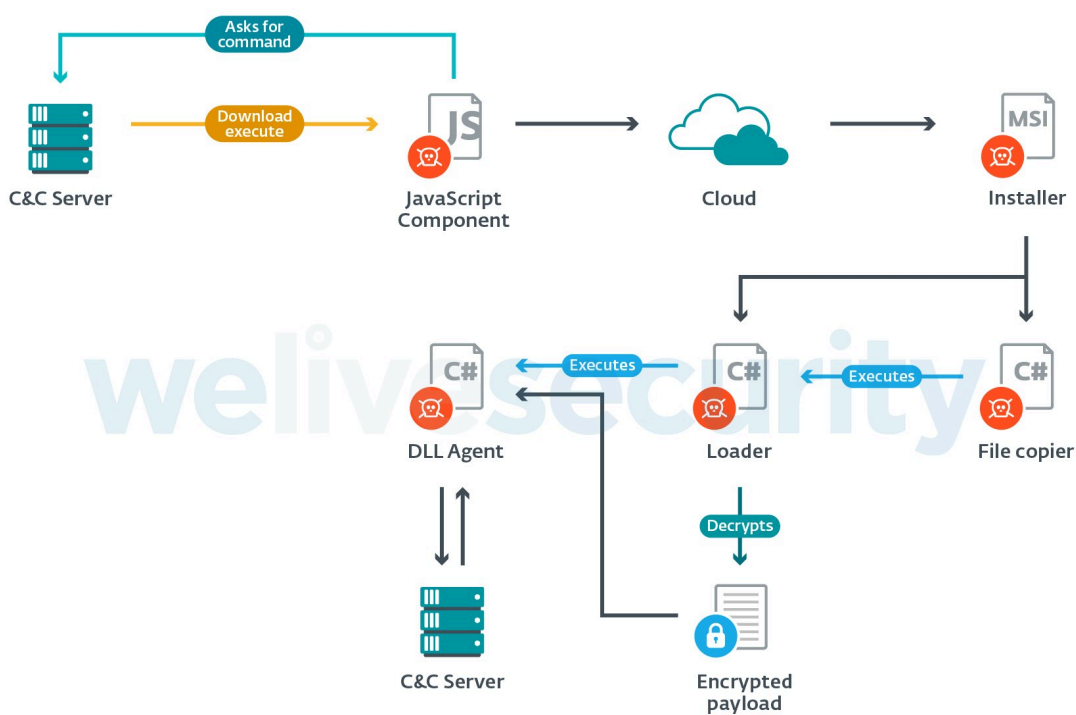


Figure 6. Parts of the C# component

When the MSI file is executed, three malicious components, along with some .NET Framework library files, are written to disk in



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

the first to be executed in %LOCALAPPDATA% (es). The loader is then system.Memmory.dll, # component. AES strings in the payload. ne strings in all of the

ext. A GET request is gains the text ed. Otherwise, a GitLab

The following capabilities are present in version 4.0.

malware authors who offer not only their malicious binaries, but also any necessary infrastructure (such as the C&C servers) and even technical support to their criminal customers.

In this case the MaaS provider is known as Golden Chickens and has other customers (apart from this group), such as [FIN6](#) and [Cobalt Group](#). Older versions of all the components that we describe in the following sections were seen previously, in an [attack against eCommerce merchants that Visa attributed to FIN6](#) in February 2019. We believe that FIN6, Cobalt Group and Evilnum group are not the same, despite the overlaps in their toolsets. They just happen to share the same MaaS provider.

The Golden Chickens tools come as ActiveX components (OCX files) and all of them contain TerraLoader code, which serves as a common loader for the various payloads available to Golden Chickens' customers. These tools are used by Evilnum as follows:

- The attackers manually send a command to the JS or C# component to drop and execute a batch file from one of their servers.
- That batch file writes a malicious INF file and supplies it as a parameter to the Microsoft utility `cmstp.exe`, which executes a remote scriptlet specified in the INF file. This technique has been documented in the MITRE ATT&CK knowledge base as [CMSTP](#); an example of how this technique is used may be found [here](#). This technique has been used in the past by [Cobalt](#), another financially motivated group.
- The remote scriptlet contains obfuscated JS code that drops an OCX file and executes it via `regsvr32.exe`.

The TerraLoader code performs several integrity checks before dropping the payload. These checks implement anti-debugging techniques and try to identify anomalies to prevent execution in sandboxed environments. Some of these techniques range from detecting incorrect parameters, filenames and extensions, to detecting hardware breakpoints or identifying specific modules loaded into the subject process. Should these checks all pass, the actual payload is decrypted and executed.

We have seen Evilnum deploy the following Golden Chickens payloads in their attacks:

- [More_eggs](#)



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Some tools used by the group are older versions of the versions used in the previous loader, so we suggest

[More_eggs](#) is a JavaScript backdoor that communicates with a C&C server and

From this point on, messages will be encrypted before they are XORed.

TerraStealer and TerraTV

TerraStealer is also known as SONE or Stealer One. It scans for many browsers, email, FTP and file transfer applications, to steal cookies and credentials. One of the binaries we analyzed had logging activated. Part of one such log is shown in Figure 9.

```
Anti2=ok
cYear=ok
cApi=ok
Ntdll_Extra=ok
K32_Init=ok
MSVCRT_Init=ok
seed_randomized
TheBat_Scan=ok
MailBird_Scan=ok
eM_Client_Scan=ok
InternetExplorer_ALL=ok
GoogleSearch=ok
MozillaProfileSearch=ok
Mozilla_Mail_Scan=ok
SQLITE3_Delete_DLL=ok
Crypt32_End=ok
DES_FREE=ok
#WinSCP=ok
#FileZilla=ok
#CoreFTP=ok
#FlashFXP=ok
CyberDuck_Scan=ok
FTP_Nav_Commander_Scan=ok
network_up
bHeader: [hwid]B22C-997F[/hwid] [pcname]WIN-8P:
wholeLogins:
Go_POST: 0
Outlook_All=ok
MAPI_Get_AddressBook=ok
Advapi32_End=ok
Winhttp_End=ok
Ws2_32_End=ok
Dnsapi_End=ok
finish parse
```

Figure 9. TerraStealer log

Another component used by this group is a variant of TerraTV. It runs a legitimate application, so that the malware is not detected by security software, so that the malware can remain on the computer undetected.

The group has split the malware components into two parts. The first part is a legitimate application with the PID 35046373333503532\.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

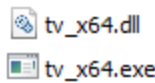


Figure 10. TeamViewer files dropped by TerraTV

ACTIVEDS.dll is not signed and it is where the malicious code resides. There is a Windows DLL with that same name in the system folder, but since the malicious DLL is in the same directory as the TeamViewer executable, it is found first, and therefore is loaded instead of the Windows DLL. This is known as [DLL search order hijacking](#). This ACTIVEDS.dll hooks several API calls in the TeamViewer executable to hide the application’s tray icon and to capture login credentials. The part of the code where the hooks are set is shown in Figure 11.

```
v15 = 0;
hModule = LoadLibraryW_0(LibFileName);           // kernel32.dll
if ( !hModule )
    return (GetLastError_0)();
v16 = LoadLibraryW_0(aUser32Dll_0);
if ( !v16 )
    return (GetLastError_0)();
v13 = LoadLibraryW_0(aShell32Dll_0);
if ( !v13 )
    return (GetLastError_0)();
v12 = LoadLibraryW_0(aGdi32Dll_0);
if ( !v12 )
    return GetLastError_0(0, v13, hModule);
v0 = GetProcAddress_0(hModule, aCreateprocessw);
dword_743EC7D4 = SetHook(v0, sub_743D6370);
v1 = GetProcAddress_0(hModule, aCreatemutexw);
dword_743EC7D0 = SetHook(v1, sub_743D5F00);
v2 = GetProcAddress_0(v13, aShellexecuteex);
dword_743EC7BC = SetHook(v2, sub_743D63D0);
v3 = GetProcAddress_0(v13, aShellNotifyico);
dword_743EC7B4 = SetHook(v3, sub_743D5EE0);
v4 = GetProcAddress_0(v16, aShowwindow);
dword_743EC7AC = SetHook(v4, sub_743D6460);
v5 = GetProcAddress_0(v16, aCreatewindowex);
dword_743EC7B8 = SetHook(v5, sub_743D6090);
v6 = GetProcAddress_0(v16, aCreatedialogpa);
dword_743EC7C0 = SetHook(v6, sub_743D6300);
v7 = GetProcAddress_0(v16, aIswindowvisibl);
dword_743EC7C8 = SetHook(v7, sub_743D5EF0);
v8 = GetProcAddress_0(v16, aSetwindowtextw);
dword_743EC7B0 = SetHook(v8, writeIDPass);
v9 = GetProcAddress_0(v16, aDefwindowprocw);
dword_743EC7C4 = SetHook(v9, sub_743D6100);
```



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

...s by the TeamViewer ...w) is hooked with a ...le ... , and TeamViewer ... of the malware can ... remotely control the computer, via its GUI, at any time.

Post-compromise toolset

The malicious components previously mentioned are frequently extended with several additional tools in the Evilnum group's arsenal. In most of the compromises we have seen, the attackers utilized publicly available tools, but have also developed some custom scripts. Usually they keep their tools in password-protected archives on their servers and decompress them on a victim's PC as needed.

Python-based tools

- Reverse shell over SSL script: A very short script that takes the server and port as command line arguments.
- SSL proxy that uses [PythonProxy](#), [junction](#), [plink](#) and [stunnel](#). It can also connect to an FTP server or use [pysoxy](#). We have seen the script being used with the "proxy" setting and 185.62.189[.]210 as the server.
- [LaZagne](#) to retrieve stored passwords
- [IronPython](#) along with libraries for taking screenshots, keylogging and recording DirectSound audio

Other publicly available tools

- PowerShell scripts: for example, [Bypass-UAC](#)
- Several NirSoft utilities; for example, [Mail PassView](#), to retrieve passwords from email clients, and [ProduKey](#), to get Microsoft Office and Windows Licenses

Conclusion

The Evilnum group has been operating for at least two years and was active at the time of this writing. It has an infrastructure for its operations with several different servers: one for communications with the JS component, another for the C# component, a different one for storing its tools and exfiltrated data, proxy

It provides trading and very specific and not as attack chain, have metry data we were uncovering some other groups share the associated with any

and samples can be subject, contact us at



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Special thanks to [Ignacio Sanmilian](#) for his help with the analysis of the Golden Chickens components.

MITRE ATT&CK techniques

Tactic	ID	Name	Description
Initial Access	T1192	Spearphishing Link	Emails contain a link to download a compressed file from an external server.
	T1191	CMSTP	cmstp.exe is used to execute a remotely hosted scriptlet that drops a malicious ActiveX file.
	T1059	Command-Line Interface	cmd.exe is used to execute commands and scripts.
	T1129	Execution through Module Load	The malicious payload for the version 4.0 C# component is loaded from a DLL. TerraTV loads a malicious DLL to enable silent use of TeamViewer.
	T1061	Graphical User Interface	TerraTV malware allows remote control using TeamViewer.
	T1086	PowerShell	Evilnum group executes LaZagne and other PowerShell scripts after their JS component has compromised a target.
Execution			



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

Evilnum group uses svr32.exe to execute Golden Chickens tools.

Initial compromise and post-compromise use several PowerShell, Python and PowerShell scripts.

cmd.exe is used to install a malicious C# component.

Users are lured to open LNK files that will install a

		malicious JS component.
	T1047	Windows Management Instrumentation WMI is used by the JS component to obtain information such as which antivirus product is installed.
	T1220	XSL Script Processing More_eggs malware uses msxsl.exe to invoke JS code from an XSL file.
	T1060	Registry Run Keys / Startup Folder Registry Run keys are created in order to persist by the JS and C# components, as well as More_eggs
Persistence	T1108	Redundant Access Evilnum components are independent and provide redundancy in case one of them is detected and removed.
	T1179	Hooking TerraTV malware hooks several API calls in TeamViewer.
	T1038	DLL Search Order Hijacking TerraTV malware has TeamViewer load a malicious DLL placed in the TeamViewer directory, instead of the original Windows DLL located in a system folder.
	T1088	Bypass User Access Control A PowerShell script is used to bypass UAC.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

...e of the Golden Chickens
...ponents are malicious
...ed executables. Also,
...um group uses legitimate
...ed) applications such as
...p.exe or msxsl.exe as
...fense evasion
...hanism.

...nection to a proxy server
...t up with post-
...romise scripts.

...yption, encoding and
...bfuscation are used in many

Defense Evasion	T1140	Obfuscate/Decode Files or Information	Obfuscation are used in many Evilnum malware components.
	T1107	File Deletion	Both JS and C# components delete temporary files and folders created during the initial compromise.
	T1143	Hidden Window	TerraTV runs TeamViewer with its window and tray icon hidden.
	T1036	Masquerading	The C# component has its payload in <code>system.memmory.dll</code> , which masquerades as a benign .NET Framework DLL.
	T1112	Modify Registry	Evilnum modifies the registry for different purposes, mainly to persist in a compromised system (for example, by using a registry's Run key).
	T1027	Obfuscated Files or Information	Encryption, encoding and obfuscation is used in many Evilnum malware components.
	T1497	Virtualization/Sandbox Evasion	The Golden Chickens components implement several integrity checks and evasion techniques.
	T1003	Credential Dumping	Scripts and tools such as LaZagne are used to retrieve stored credentials.



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

The C# component retrieves stored passwords from Chrome.

Some Python scripts have been used for keylogging.

Evilnum malware steals cookies from Chrome.

The `eggs` queries the registry to know if the user has admin privileges.

Discovery	T1063	Security Software Discovery	Both the JS and C# components search for installed antivirus software.
	T1518	Software Discovery	TerraStealer malware looks for specific applications.
	T1082	System Information Discovery	Information about the system is sent to the C&C servers.
Collection	T1074	Data Staged	Data is stored in a temporary location before it is sent to the C&C.
	T1005	Data from Local System	The JS component (v2.1) has code to exfiltrate Excel files from the local system.
	T1114	Email Collection	TerraStealer malware targets email applications.
	T1056	Input Capture	Keystrokes are logged with a Python script.
	T1113	Screen Capture	Screenshots are taken by some Evilnum malware components.
	T1043	Commonly Used Port	HTTP and HTTPS are used for C&C communication.
	T1132	Data Encoding	Some of the data sent to the C&C is base64-encoded.

The JS and C# components can obtain a new C&C by visiting third-party webpages if the original C&C is down.

Evilnum malware uses independent C&C servers for various components.

EvilTV malware uses RemoteViewer to give control of the compromised computer to the attackers.

Files are uploaded to/downloaded from a C&C



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

	T1000	Remote File Copy	Evilnum uses a C&C server.
	T1071	Standard Application Layer Protocol	HTTP and HTTPS are used for C&C.
	T1032	Standard Cryptographic Protocol	More_eggs malware uses RC4 to encrypt data to be sent to the C&C.
	T1102	Web Service	GitHub, GitLab, Reddit and other websites are used to store C&C server information.
Exfiltration	T1022	Data Encrypted	Some Evilnum components encrypt data before sending it to the C&C.
T1048	Exfiltration Over Alternative Protocol	Scripts are manually deployed by the malware operators to send data to an FTP server.	
	Exfiltration Over Command and Control Channel	Data is exfiltrated over the same channel used for C&C.	

Let us keep you up to date

Sign up for our newsletters



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).

ESET RESEARCH
CloudScout: Evasive
Panda scouting cloud
services

ESET RESEARCH
ESET Research
Podcast:
CosmicBeetle

ESET RESEARCH
Embargo
ransomware:
Rock’n’Rust

Discussion

What do you think?
9 Responses


Upvote


Funny



Love


Surprised


Angry



Sad







0 Comments 1 Login ▼



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 



Name



• Share

[Best](#) [Newest](#) [Oldest](#)

 BY 

Award-winning news, views, and insight from the ESET security community

- About us
- Contact us
- Legal Information
- RSS Feed

- ESET
- Privacy Policy
- Manage Cookies



Your account, your cookies choice

We and our partners use cookies to give you the best optimized online experience, analyze our website traffic, and serve you with personalized ads. You can agree to the collection of all cookies by clicking "Accept all and close" or adjust your cookie settings by clicking "Manage cookies". You also have the right to withdraw your consent to cookies anytime. For more information, please see our [Cookie Policy](#).