Silence Group Playbook: Protecting Your Infrastructure | Fortinet Blog

By FortiGuard SE Team

Published: 2019-04-15 · Archived: 2026-04-05 18:05:51 UTC

Active since 2016, Silence Group is a cybercriminal organization that targets banks, specifically stealing information used in the payment card industry. There has been ample coverage [1] [2] of this group over the years that highlights their TTPs (Techniques, Tactics, and Procedures) [3]. The aim of this playbook is to provide first responders with relevant, up-to-date analysis, samples, and indicators of compromise which should help security professionals better protect their infrastructures.

Adversary Playbook: The FortiGuard SE Team is releasing this new playbook on the threat actor group known as Silence Group as part of our role in the Cyber Threat Alliance. For more information regarding this series of adversary playbooks being created by CTA members, please visit the Cyber Threat Alliance Playbook Whitepaper.

Silence Group Playbook: Overview

The modus operandi of the Silence Group is simple. It is to make as much money as possible by compromising targets, in this case banks, via a spear phishing strategy, which will then lead to exfiltrating financial data as well as also allow the attackers to “Jackpot” ATMs to withdraw money.

To achieve these goals, the Silence Group is known to utilize publicly available tools that they repurpose, as well as use a technique that the cybersecurity industry refers to as “living off the land.” What this essentially means is that they attempt to operate as long as possible using the preexisting tools or commands built into the operating system of their target to effectively maximize the time they are able to spend within the target environment. This strategy has two benefits: first, using locally available tools helps them better evade detection, and second, it helps them establish a deeper and stronger foothold.

However, the group does not exclusively rely on publicly available tools. They are also known to write their own sets of modular, custom tools. As the motivations and various TTPs of their living-off-the-land strategy have been documented previously, this blog will focus on the details of those custom tools developed exclusively by this group.

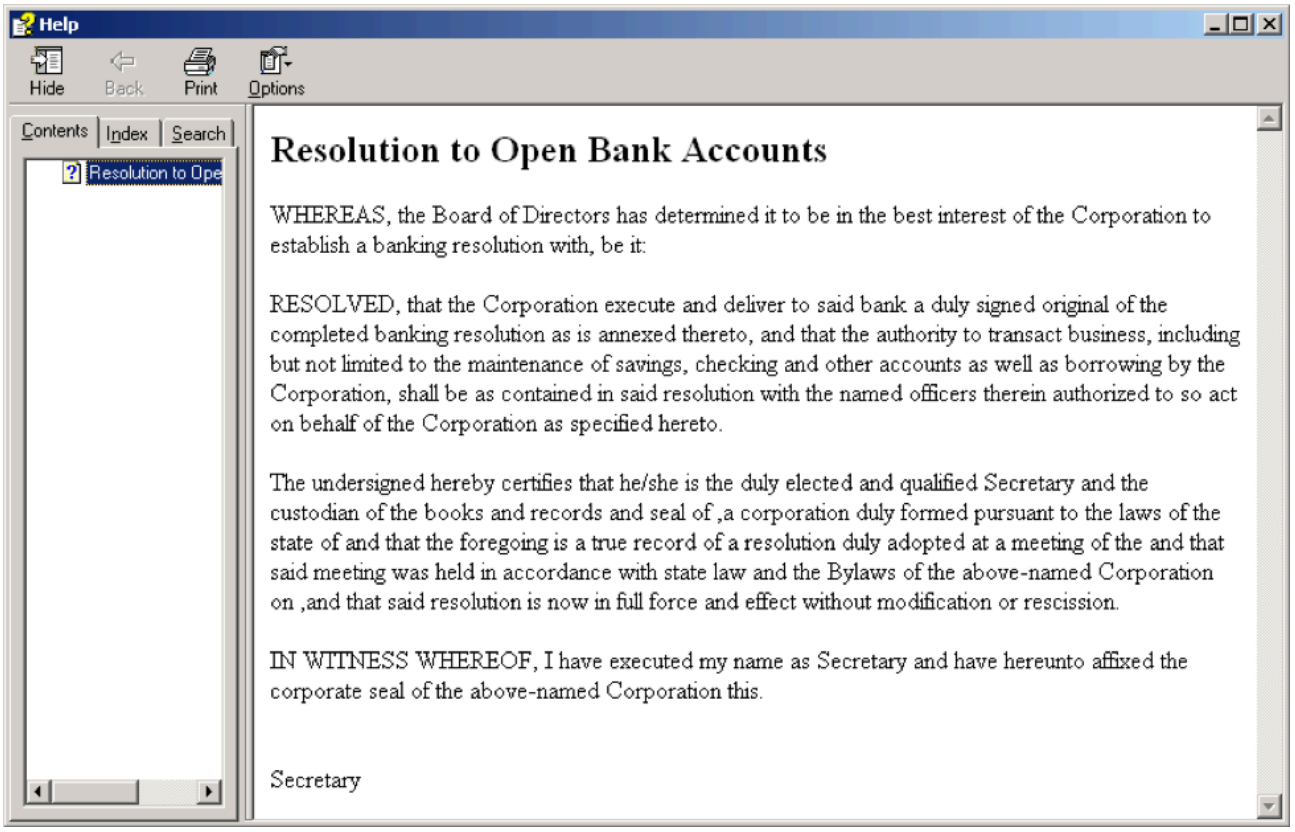
Technical Details

Like most attacks, the typical Silence Group threat begins with a spear phishing email with malicious attachments. The attachments may be in the form of a weaponized Microsoft Word document or a Microsoft-compiled HTML help (CHM) file sent to banks to entice their users to click on the attachments. These malicious emails generally contain infected Word documents or weaponized help files. For example, the following is a help file sent to a user:

[1] https://securelist.com/the-silence/83009/

[2] https://www.group-ib.com/blog/silence

[3] https://reaqta.com/2019/01/silence-group-targeting-russian-banks/



While this screenshot may seem innocuous, when a user inadvertently executes the file's malicious script it contacts a server in the background. The script then initiates the second stage of this attack by downloading and executing a file from that server to the user's machine.

This obfuscated VBS file is then executed within the context of a browser window inside the help files, where it then deobfuscates itself and executes a PowerShell command. Unbeknownst to the user, this new PowerShell command calls out to another server to retrieve a binary file, which it then decrypts into a third-stage downloader. This last downloader is designed to acquire the actual Silence payload that consists of several different modules, depending on which phase of the overall attack the group is currently in. Some modules we describe in the playbook include a proxy, a monitoring agent, an ATM module, and the actual main Silence module itself.

Downloader Stage

The downloader stage of this attack strategy has functionally stayed the same throughout the few years this group has been active. For persistence purposes, the registry key the module sets usually tries to mimic a well-known product to avoid detection. The same can be said for the filename it attempts to rename itself. The downloader itself accepts three distinct commands

Command	Action
'fal', 'false'	Take no action, then query the C&C for a new command after a set amount of time has passed
'del', 'DELETE'	Uninstall
'*http*'	Download the next stage/module

The downloader contacts a separate C&C server to get a command. If the command contains the string 'HTTP', then this module will parse the command and download the specified file. This new file will also be given a seemingly benign name, such as "conhost" or "igfxpers_", with a string appended to it based on the username or a randomly-generated GUID value before being executed.

Main Module

The main module of Silence allows the group to handle the different aspects of their attack.

Command	Action
'htrjyytrn'	Reset everything and reconnect to the C&C from the beginning (htrjyytrn = "reconnect",
'htcnfhn'	Restart the shell (CMD) and prepare pipes for communications (htcnfhn = "restart",
'ytnpflfybq'	Do nothing, similar to a NOP (no operation) command (ytnpflfybq = "no tasks",
'#wget'	Download a file
shell	Start the command interpreter (CMD) and run arbitrary shell commands

Proxy Module

While one set of proxy modules was developed in Delphi, another set was built using the .Net framework. This lends credence to the theory proposed by Group-IB that the Silence group likes to modify existing tools for their own purposes. [1]

The proxy module can be used as a springboard to other networks, or in this case, to dive deeper into the internal bank network. Looking closer at the .Net proxy modules, for example, one can see that the Smart Assembly obfuscator was used to try and hide the module's payload.

[1] https://www.group-ib.com/blog/silence

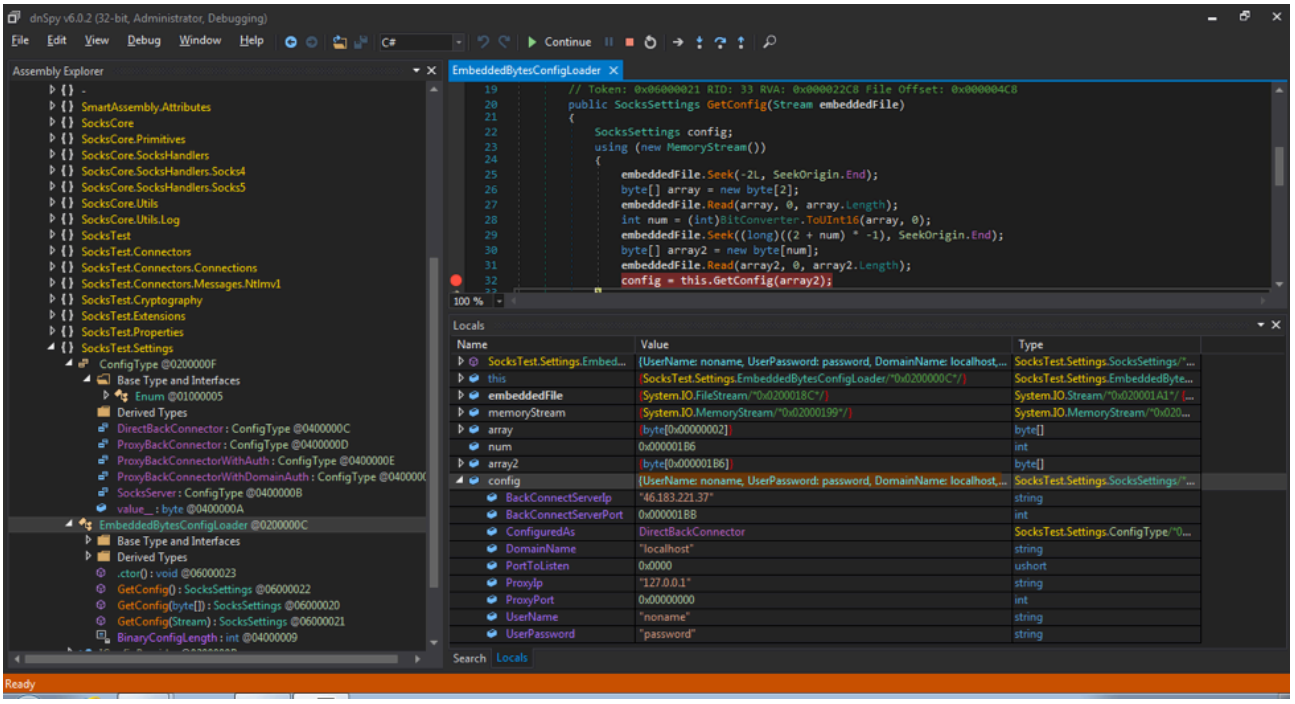


Figure 1. Screenshot of Proxy Module

Debugging the module leads to a configuration file being loaded. The connection details can be seen in the screenshot above using a password of such as “password”.

Monitor Module

The monitor module has one function. It gives the authors the capability to spy on the infected machines. Screenshots are taken and interprocess communications are used to transfer the data to the main module. In this way, it can function similarly to a video stream.

ATM Module

The crux of this operation revolves around the ATM module, also known as Atmosphere. It makes it possible for the authors to remotely cash out ATM machines. Once on an infected computer, this module searches all running processes for a legitimate one called "atmapp.exe", which is proprietary ATM software.

```
.text:00401136                 push    offset Type     ; "BIN"
.text:0040113B                 push    65h ; 'e'       ; __int16
.text:0040113B ;   } // starts at 4010EF
.text:0040113D ;   try {
.text:0040113D                 mov     byte ptr [ebp+var_4], 7
.text:00401141                 call    Get_Resource
.text:00401146                 add     esp, 1Ch
.text:00401149                 lea     eax, [ebp+var_12]
.text:0040114C                 lea     ecx, [ebp+var_28]
.text:0040114F                 push    eax
.text:00401150                 call    sub_401528
.text:00401155                 lea     eax, [ebp+var_80]
.text:00401158                 push    offset aAtmappExe ; "atmapp.exe"
.text:0040115D                 push    eax
.text:0040115D ;   } // starts at 40113D
.text:0040115E ;   try {
.text:0040115E                 mov     byte ptr [ebp+var_4], 8
.text:00401162                 call    Search_Processes
.text:00401167                 pop     ecx
.text:00401168                 pop     ecx
.text:00401169                 push    eax
.text:0040116A                 lea     ecx, [ebp+var_28]
.text:0040116A ;   } // starts at 40115E
.text:0040116D ;   try {
.text:0040116D                 mov     byte ptr [ebp+var_4], 9
.text:00401171                 call    sub_401311
.text:00401176                 lea     ecx, [ebp+var_80]
.text:00401176 ;   } // starts at 40116D
.text:00401179 ;   try {
.text:00401179                 mov     byte ptr [ebp+var_4], 8
.text:0040117D                 call    sub_4013BB
.text:00401182                 lea     ecx, [ebp+var_28]
.text:00401185                 call    sub_4016F8
.text:0040118A                 push    eax             ; char
.text:0040118B                 lea     eax, [ebp+var_80]
.text:0040118E                 push    offset aFoundedDPreces ; "Founded %d precesses."
```

ATM Module

Once "atmapp.exe" is found, the Atmosphere module will take the dll DLL it was storing in its resources and inject it into the running process. Some of the functionality included in the dll DLLmay have been based on an existing GitHub project (https://github.com/TsudaKageyu/minhook) (to learn more about the open source malware development and how adversaries are taking advantage of it, please see our Q4 Threat Landscape Report). Once the injection process has been completed, the malicious dll DLL will run in the ATM process space, thereby effectively gaining control of the ATM, a process known as “Jackpotting.”

IDA View-A | Strings window | Hex View-1

Address	Length	Type	String
.data:10012604	0000001A	C	DEFAULT command processed
.data:10012620	00000017	C	NONE command processed
.data:10012638	0000000E	C	System error!
.data:10012648	00000019	C	Dispense failed. CODE:%d
.data:10012664	00000017	C	Multi Dispensing start
.data:1001267C	00000021	C	Dispense failed. Unknown reason.
.data:100126A0	00000014	C	Dispense failed. %d
.data:100126B4	00000012	C	Manual Dispensing
.data:100126C8	00000026	C	Display Balance -> exception, code:%d
.data:100126F0	0000002B	C	Display Balance 1try -> exception, code:%d
.data:1001271C	0000003E	C	CommandProcessor::ProcessCommand ->\nSetMaximumDispenseSize:%
.data:1001275C	00000017	C	NULL command processed
.data:10012774	00000032	C	ICommandProcessor::ProcessCommand -> start method
.data:100127A8	00000017	C	Processing command #%d
.data:100127C0	00000017	C	Received `%d` commands
.data:100127D8	00000014	C	exception cauch: %d
.data:100127EC	00000008	C	Exiting
.data:100127F4	00000008	C	Pausing
.data:100127FC	00000013	C	trying to dispense
.data:10012810	0000002D	C	R2CommandProcessor::ProcessGetRealBalance()1

Figure 3. Strings for ATM module

From this point on, threat researchers assume that the authors hire money mules to pick up cash from infected ATMs while moving on to their next target.

Global Distribution

Distribution for the various samples used by the Silence Group is not restricted to one current geographical location. As shown in the example below, we can see that distribution includes the following countries (based off of geo-IP information):

Australia, Canada, France, Ireland, Latvia, The Netherlands, Poland, Spain, Sweden, and The United States.

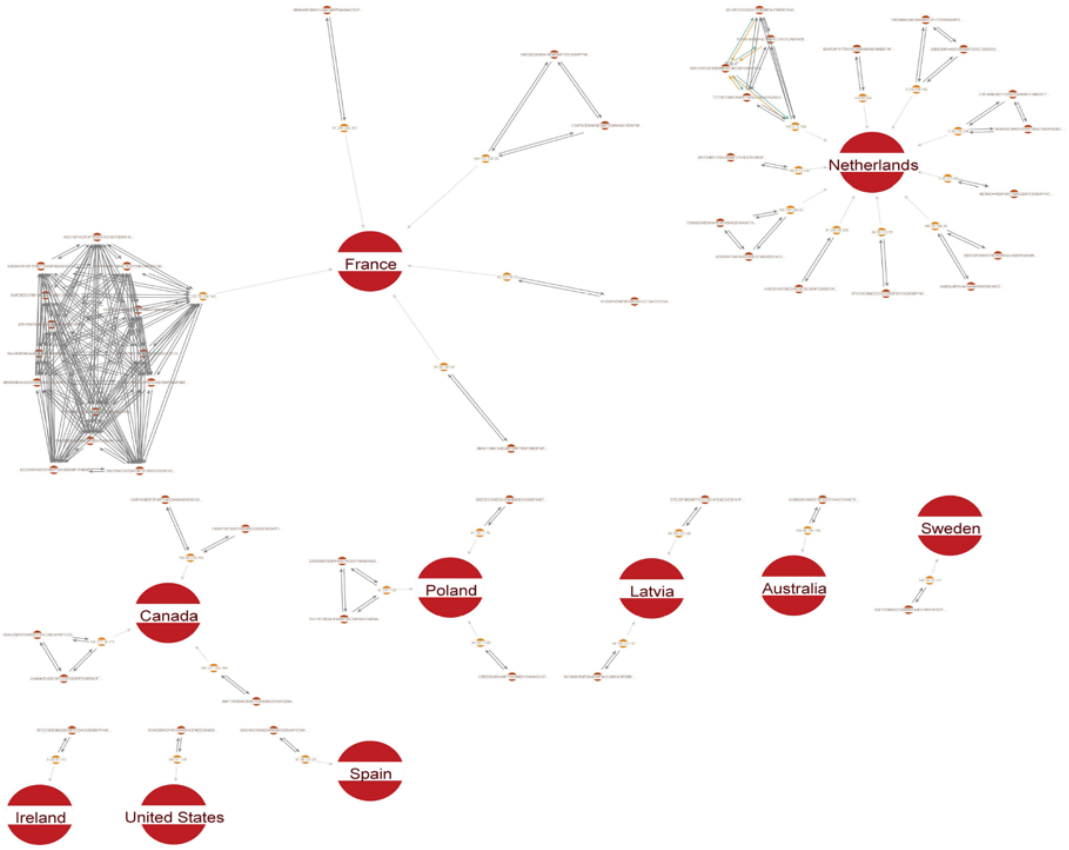


Figure 4. Geographic distribution of command and control and download sites used by Silence Group

We have observed samples distributed in various global locations, with a concentration in the EMEA region. One IP address in France (137.74.224.142) was the primary download site or command and control for over 15 samples. Another interesting observation is that The Netherlands has had over 10 different unique IP addresses that were either used as download sites or as command and control servers.

An interesting Silence Group correlation

During our investigation, we noticed some anomalous behavior with certain IP addresses, specifically Canadian IP addresses. Although they are different in scope, we decided to see if there was any correlation to known actors, bulletproof hosts, or web hosts.

Due to time constraints, and to keep the blog succinct, we will not go into too much detail for the purposes of this playbook. However, after cursory analysis, a peculiar detail stood out for the following IP addresses:

144.217.14.173 (Montreal, QC, Canada)

158.69.218.119 (Montreal, QC, Canada)

144.217.162.168 (Montreal, QC, Canada

These addresses were all associated with a single web hosting organization. When we decided to investigate a little further, we discovered additional connections to netblocks from this same web hosting organization in the

following countries: Australia, Canada, France, The Netherlands, Spain, and Ireland.

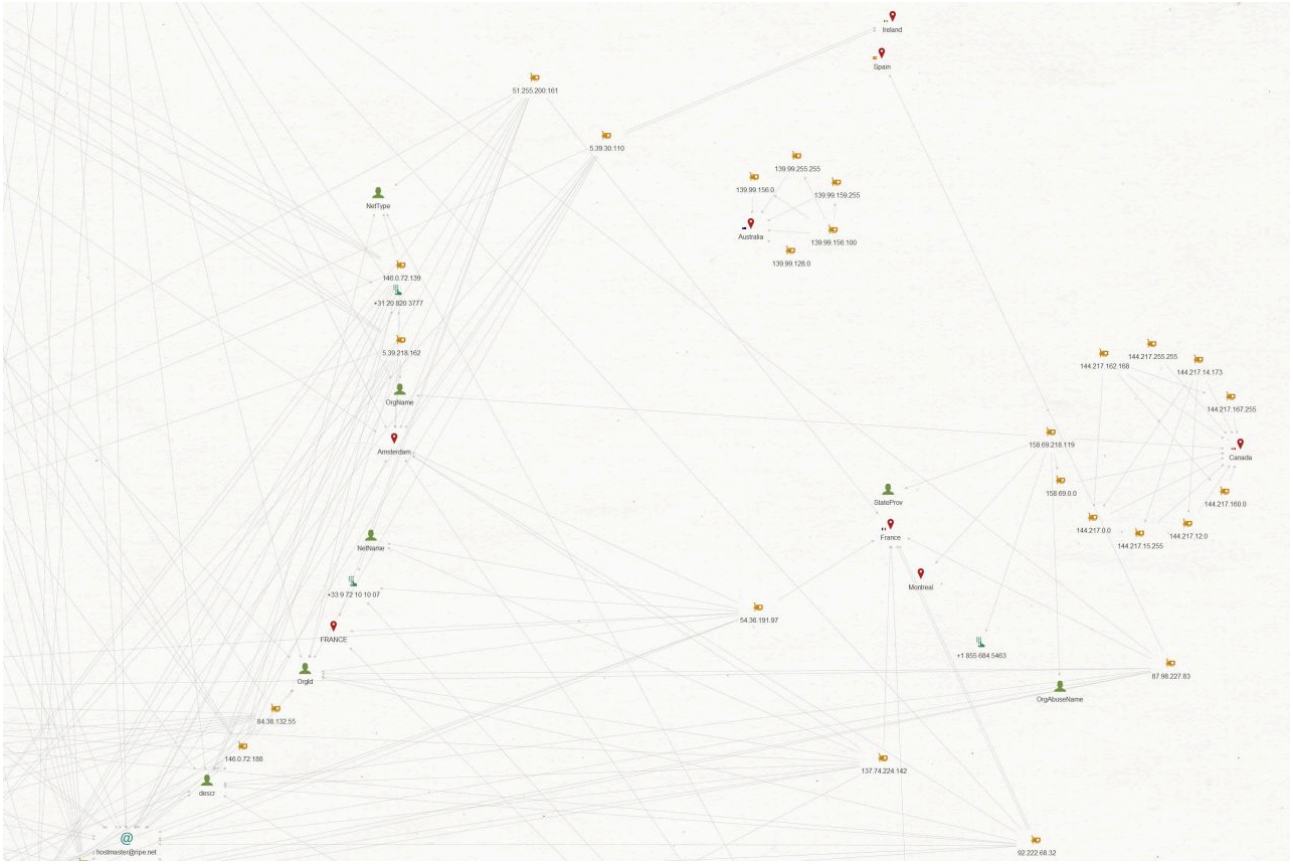


Figure 5. Global sites

Remarkably this list constitutes a whopping 60% of the countries we identified in our initial analysis. Please note, however, that this correlation does not construe or interpret that this organization is in any way involved or even aware of the situation. This is likely either entirely coincidental, the result of Silence Group actors simply being familiar with the publicly available services of a well-known hosting service, or due to the efforts of another bad actor, such as a bulletproof downstream host that is reselling those services.

Although many IP addresses with multiple country connections to this hosting company have been observed, it remains unclear as to how they are connected to each other, or if this is possibly even simply due to circumstance (automatic assignment by the web host, etc.)

For further information regarding the samples used in our research, including indicators of compromise that have been analyzed and mapped according to the specifications of the MITRE ATT&CK framework, please refer to our latest playbook on the Silence Group here.

Note: MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

Learn more about FortiGuard Labs and the FortiGuard Security Services portfolio. Sign up for our weekly FortiGuard Threat Brief.

Know your vulnerabilities – get the facts about your network security. A Fortinet Cyber Threat Assessment can help you better understand: Security and Threat Prevention, User Productivity, and Network Utilization and Performance.

Read about the FortiGuard Security Rating Service, which provides security audits and best practices.
