

ScarCraft surveilling North Korean defectors and human rights activists

APT REPORTS

29 NOV 2021

17 minute read

Table of Contents

[Spear-phishing document](#)

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary

Preferences

Statistics

Marketing

Show details

Use necessary cookies only

Allow all cookies

Expert

GREY

The ScarCraft actor we first reported in 2018. ScarCraft is known to target North Korean defectors, journalists who cover North Korea-related news and government organizations related to the Korean Peninsula, between others. Recently, we were approached by a news organization with a request for technical assistance during their [cybersecurity investigations](#). As a result, we had an opportunity to perform a deeper investigation on a host compromised by ScarCraft. The victim was infected by PowerShell malware and we discovered evidence that the actor had already stolen data from the victim and had been surveilling this victim for several months. The actor also attempted to send spear-phishing emails to the victims’ associates working in businesses related to North Korea by using stolen login credentials.

Based on the findings from the compromised machine, we discovered additional malware. The actor utilized three types of malware with similar functionalities: versions implemented in PowerShell, Windows executables and Android applications. Although intended for different platforms, they share a similar command and control scheme based on HTTP communication. Therefore, the malware operators can control the whole malware family through one set of command and control scripts.

We were working closely with a local CERT to investigate the attacker’s command and control infrastructure and as a result of this, we were able better understand how it works. The APT operator controls the malware using a PHP script on the compromised web server and controls the implants based on the HTTP parameters. We were also able to acquire several log files from the compromised servers. Based on said files, we identified additional victims in

[Indicators of compromise](#)

[MITRE ATT&CK mapping](#)

Page 1 of 16

hxxp://[redacted].cafe24[.]com/bbs/probook/do.php?type=hello&direction=send&id=[host_name]

Next, it attempts to download commands from the C2 server with the following format:

hxxp://[redacted].cafe24[.]com/bbs/probook/do.php??type=command&direction=receive&id=


If the HTTP response from the C2 server is 200, it checks the response data and executes the delivered commands.

Delivered data	Description
ref:	Send a beacon to the C2 server: HTTP request: ?type=hello&direction=send&id=
cmd:	If the command data includes ‘start’, execute the given command with cmd.exe and send base64 encoded ‘OK’ with the following POST format. Otherwise, it executes the given command, redirecting the result to the result file (%APPDATA%\desktop.dat), and sends the contents of the file after base64 encoding. HTTP request: ?type=result&direction=send&id=

We discovered additional malware, tools and stolen files from the victim’s host. Due to limited access to the compromised host, we were unable to figure out the initial infection vector.


However, the suspicious writing on the Master Boot Record the last time before collecting the data. Using the victim, a was stolen collected encrypted uploading ‘B14yNKV bearing t Up File S something

13 MAY 2021, 1:00PM

 **GReAT Ideas. Balalaika Edition**


BORIS LARIN, DENIS LEGEZO

26 FEB 2021, 12:00PM

 **GReAT Ideas. Green Tea Edition**


JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA, MOTOHIKO SATO

17 JUN 2020, 1:00PM

 **GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots**

MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU, KURT BAUMGARTNER, DAN DEMETER, YAROSLAV SHMELEV

26 AUG 2020, 2:00PM

 **GReAT Ideas. Powered by SAS: threat actors advance on new fronts**

IVAN KWIATKOWSKI, MAHER YAMOUT, NOUSHIN SHABAB, PIERRE DELCHER, FÉLIX AIME, GIAMPAOLO DEDOLA, SANTIAGO BONTROU



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
			

Show details >

File archiving and uploading log

The other log file, named “s5gRAEs70xTHkAdUjl_DY1fD.dat”, also contains a file uploading history, except for file zipping messages. It processes each file with this procedure: “Up Init > Up Start > Up File Succeed”.

File uploading log

Based on what we found from this victim, we can confirm that the malware operator collected screenshots and exfiltrated them between August 6, 2021 and September 8, 2021. Based on what we found out from the victim, we can summarize the whole infection timeline. We suspect this host was compromised on March 22, 2021. After the initial infection, the actor attempted to

implant additional malware, but an error occurred that led to the crash of the malware. The malware operator later delivered the Chinotto malware in August 2021 and probably started to exfiltrate sensitive data from the victim.

Timeline of the attack on the victim

Windows

As a result of the additional execution of “Chinotto



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

The technical character During runtime, the value; or

It also re at runtime. The malware creates a mutex and fetches the C2 addresses, which are different for each sample we discovered:

```
Mutex: NxaNnkHnJiNAuDCCoCKRAngjHVUZG2hSZL03pw8Y
C2 address: hxxp://luminix.openhaja[.]com/bbs/data/proc1/proc.php
```

In order to generate the identification value of the victim, the malware acquires both computer and user name and combines them in the format ‘%computer name%_%user name%’. Next, it encrypts the acquired string with the XOR key ‘YFXAWSAEAXee12D4’ and encodes it with base64.

The backdoor continuously queries the C2 server, awaiting commands from the malware operator. We observed an early version of Chinotto malware (MD5 55afe67b0cd4a01f3a9a6621c26b1a49) which, while it also follows this simple principle, uses a hard-coded backdoor command ‘scap’. This means this specific sample is only designed for exfiltrating the victim’s screenshot.

The Chinotto malware shows fully fledged capabilities to control and exfiltrate sensitive information from the victims.

Command	Description
---------	-------------

ref:	Send beacon to the C2 server: http://[C2 URL]?ref=id=%s&type=hello&direction=send
cmd:	Execute Windows commands and save the result to the %APPDATA%\s5gRAEs70xTHkAdUjl_DY1f.dat file after encrypting with a one-byte XOR key
down:	Download file from the remote server
up:	Upload file
state:	Upload log file (s5gRAEs70xTHkAdUjl_DY1fD.dat)
regstart:	Copy current malware to the CSIDL_COMMON_DOCUMENTS folder and execute command to register file to run registry: "reg add HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v a2McCq /t REG_SZ /d %s /f"
cleartemp:	Remove files from folder "%APPDATA%\s5gRAEs70xTHkAdUjl_DY1fD"
updir:	Archive directory and upload it. Archive is XOR encoded using the same key used when

init:



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

scap:

Necessary



Preferences



Statistics



Marketing



run:

chdec:

Show details >

update:

wait: Sleep for 30 minutes

wakeup: Wake up after 2.5 seconds

Another malware sample (MD5 [04ddb77e44ac13c78d6cb304d71e2b86](#)) that demonstrated a slight difference during runtime was discovered from the same victim. This is the same fully featured backdoor, but it loads the backdoor command using a different scheme. The malware checks for the existence of a ‘*.zbpiz’ file in the same folder. If it exists, it loads the file’s content and uses it as a backdoor command after decrypting. The malware authors keep changing the capabilities of the malware to evade detection and create custom variants depending on the victim’s scenario.

In addition, there are different Windows executable variants of the Chinotto malware. Apart from the conventional Chinotto malware mentioned above, a different variant contains an embedded PowerShell script. The spawned PowerShell command has similar functionality to the PowerShell we found from the victim. However, it contains additional backdoor commands, such as uploading and downloading capabilities. Based on the build timestamp of the malware, we assess that the malware author used the PowerShell embedded version from mid-2019 to

FROM THE SAME AUTHORS

Grandoreiro, the global trojan with grandiose goals

Stealer here, stealer there, stealers everywhere!

Exotic SambaSpy is now dancing with Italian users

BlindEagle flying high in Latin America

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

mid-2020 and started to use the malicious, PowerShell-less Windows executable from the end of 2020 onward.

Android Chinotto

Based on the C2 communication pattern, we discovered an Android application version of Chinotto malware (MD5 [56f3d2bcf67cf9f7b7d16ce8a5f8140a](#)). This malicious APK requests excessive permissions according to the AndroidManifest.xml file. To achieve its purpose of spying on the user, these apps ask users to enable various sorts of permissions. Granting these permissions allows the apps to collect sensitive information, including contacts, messages, call logs, device information and audio recordings. Each sample has a different package name, with the analyzed sample bearing “com.secure.protect” as a package name.

The malware sends its unique device ID in the same format as the Windows executable version of Chinotto.

Beacon URI pattern: `[C2 url]?type=hello&direction=send&id=[Unique Device ID]`

Next, it receives a command after the following HTTP request:

Retrieve commands: `[C2 url]?type=command&direction=receive&id=[Unique Device ID]`

If the device sends data from the C2 server in a “ERROR” or “Fail” state, the malware starts to connect backdoor.

Command

ref:

down

UriP

UploadInf



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

file path

- Sms.txt: Save all text messages with JSON format
- Callog.txt: Save all call logs with JSON format
- Contact.txt: Save all contact lists with JSON format
- Account.txt: Save all account information with JSON format

Upload collected file after archiving. The archived file is encrypted by AES with the key “3399CEFC3326EEFF”.

UploadFile

?type=file&direction=send&id=

Execute command ‘cd /sdcard;ls -alR’, save the result to the temporary file (/sdcard/.temp-file.dat) and upload it. Upload all thumbnails and photos after encrypting via AES and the key “3399CEFC3326EEFF”.

HWP hash	HWP file name	Dropped payload hash
f17502d3e12615b0fa8868472a4eabfb	코로나19 재감염 사례-백신 무용지물.hwp (Covid-19 reinfection case- Useless vaccine.hwp)	72e5b8ea33aeb083631d1e8b302e76af (Visual Basic Script)
c155f49f0a9042d6df68fb593968e110	계정기능 제한 안내.hwp (Notice of limitation of account.hwp)	5a7ef48fe0e8ae65733db64ddb7f2478 (Windows executable)

The Visual Basic Script created by the first HWP file (MD5 [f17502d3e12615b0fa8868472a4eabfb](#)) has similar functionalities to the Chinotto malware. It also uses the same HTTP communication pattern. The second payload dropped from the malicious HWP is a Windows executable executing an embedded PowerShell script with the same functionalities. These discoveries reveal related activity dating back to at least mid-2020.

Infrastructure

In this campaign, the actor relied solely on compromised web servers, mostly located in South Korea. During this research we worked closely with the local CERT to take down the attacker's infrastructure. The actor used the same infrastructure to deliver the Chinotto malware to the client's server. The actor's direction was to install the malware on the client's server.

```
$type  
$sho  
$con  
$bti  
$dir  
$dat  
  
if ($?) {  
    $bt  
}  
if ($?) {  
    $ty  
}  
if ($?) {  
    $di  
}  
if ($?) {  
    $dd  
}  
..  
$con  
$con
```

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

In order to use the script, the operator must send the 'type' parameter. The 'type' parameter carries four values: hello, command, result, and file.

Value of 'type' param	Description
hello	Report and control the client status
command	Hold the command from the operator or retrieve the command from the client
result	Upload the command execution result or retrieve the command
file	Upload file to the C2 server

'hello' type

When the script receives the 'type=hello' parameter, it checks the value of 'direction'. In this routine, the script checks the status of the client. The malware operator saves the client status to a specific file, the 'shakest' file in this case. If the 'send' value is being received, the client status is set to 'ON'. If 'receive' is set as well, the client's status log file is sent (likely in order to

When uploading command execution results coming from the implant, the script sets the ‘type’ parameter to ‘result’. If the ‘direction’ parameter equals ‘send’, it saves the value of the ‘data’ parameter to the individual result file: “[botid]-result“. The ‘receive’ value of the ‘direction’ parameter means retrieving the individual result file. The script then sends the result file to the operator after encoding it with base64.

‘file’ type

The last possible ‘type’ command is ‘file’. This value is used for exfiltrating files from the victim. If a file upload succeeds, the script sends the message ‘SEND SUCCESS’. Otherwise, it sends ‘There was an error uploading the file, please try again!’.

We discovered that the malware operator used a separate webpage to monitor and control the victims. From several compromised C2 servers we see a control page carrying a ‘control.php’ file name.

The control page in the left pane is able to

Victims

We began our investigation of North Korean defectors and human rights activists

Additionally, we found that from an IP address in 2021 and that it was to be either

Analyzing other C2 servers, we found more information about possible additional victims. Excluding connections coming from Tor, there are only connections coming from South Korea. Based on the IP addresses, we could distinguish four different suspected victims located in South Korea, and determine their operating system and browser used based on user-agent information:

Victim A connected to the C2 server from July 16 to September 5 and has outdated versions of Windows OS and Internet Explorer. Victim B connected to this server on September 4 and operates Windows 8 and Internet Explorer 10. While we were investigating the C2 server, Victim D kept connecting to it, using Windows 10 with Chrome version 78.

I'm under attacking by a extremelyhigh complex and organized by agents.

Reply

// LATEST POSTS

SAS

The Crypto Game of Lazarus APT: Investors vs. Zero-days

BORIS LARIN, VASILY BERDNIKOV

MALWARE DESCRIPTIONS

Grandoreiro, the global trojan with grandiose goals

GREAT

CRIMEWARE REPORTS

Stealer here, stealer there, stealers everywhere!

GREAT

CRIMEWARE REPORTS

Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia

KASPERSKY

// LATEST

04 SEP 2024

Inside the world of the human cybercriminals

ANNA PAVLOVA

// RECENT

Beyond the expansion of the SideWinder APT group

Kaspersky analyzes SideWinder APT’s recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

APT trends report Q2 2024

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.

New product

Let’s go Next: redefine your business's cybersecurity


k

Kaspersky Next

// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

Email

 **Subscribe**

☐ I agree to provide my email address to “AO Kaspersky Lab” to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

kaspersky

THREATS

- APT (Targeted attacks)
- Secure environment (IoT)
- Mobile threats
- Financial threats
- Spam and phishing

CATEGORIES

- APT reports
- Malware descriptions
- Security Bulletin
- Malware reports
- Spam and phishing reports

OTHER SECTIONS

- Archive
- All tags
- Webinars
- APT Logbook
- Statistics



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >