Lazarus covets COVID-19-related intelligence

APT REPORTS 23 DEC 2020 11 minute read

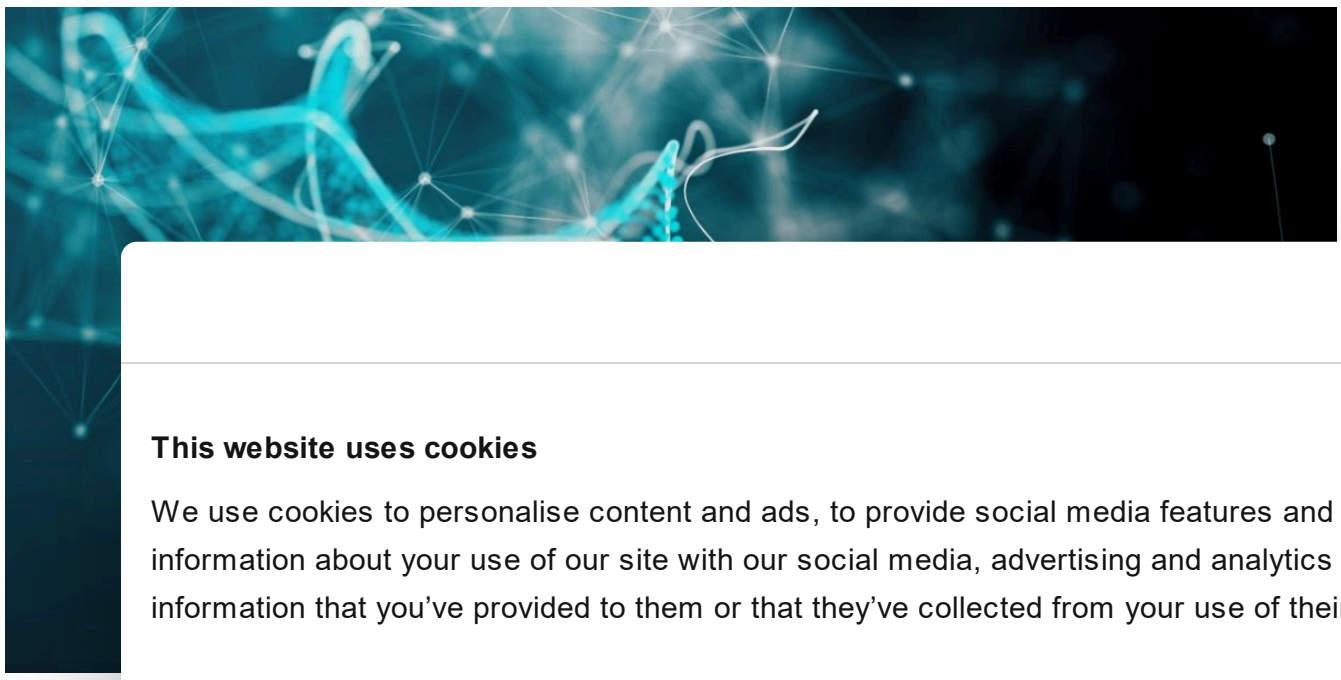

Table of Contents

// AU

SEC

As the C
developi
group, a
COVID-1

While tra
discovered that they recently went after COVID-19-related entities. They attacked a pharmaceutical company at the end of September, and during our investigation we discovered that they had also attacked a government ministry related to the COVID-19 response. Each attack used different tactics, techniques and procedures (TTPs), but we found connections between the two cases and evidence linking those attacks to the notorious Lazarus group.

Relationship of recent Lazarus group attack

In this blog, we describe two separate incidents. The first one is an attack against a government health ministry: on October 27, 2020, two Windows servers were compromised at the ministry. We were unable to identify the infection vector, but the threat actor was able to install a sophisticated malware cluster on these servers. We already knew this malware as 'wAgent'. It's main component only works in memory and it fetches additional payloads from a remote server.

The second incident involves a pharmaceutical company. According to our telemetry, this company was breached on September 25, 2020. This time, the Lazarus group deployed the Bookcode malware, previously reported by ESET, in a supply chain attack through a South Korean software company. We were also able to observe post-exploitation commands run by Lazarus on this target.

Both attacks leveraged different malware clusters that do not overlap much. However, we can confirm that both of them are connected to the Lazarus group, and we also found overlaps in the post-exploitation process.

wAgent malware cluster

The malware cluster has a complex infection scheme:

Unfortur
seems t
samples
compres

Accordi
command line shell by calling the Thumbs export function with the parameter:

```
c:\windows\system32\rundll32.exe  C:\Programdata\Oracle\javac.dat, Thumbs 8IZ-VU7-109-S2MY
```

The 16-byte string parameter is used as an AES key to decrypt an embedded payload – a Windows DLL. When the embedded payload is loaded in memory, it decrypts configuration information using the given decryption key. The configuration contains various information including C2 server addresses, as well as a file path used later on. Although the configuration specifies two C2 servers, it contains the same C2 server twice. Interestingly, the configuration has several URL paths separated with an '@' symbol. The malware attempts to connect to each URL path randomly.

C2 address in the configuration

When the malware is executed for the first time, it generates identifiers to distinguish each victim using the hash of a random value. It also generates a 16-byte random value and reverses its order. Next, the malware concatenates this random 16-byte value and the hash using '@' as a delimiter. *i.e.: 82UKx3vnjQ791PL2@29312663988969*

POST parameter names (shown below) are decrypted at runtime and chosen randomly at each C2 connection. We've previously seen and reported to our Threat Intelligence Report customers that a very similar technique was used when the Lazarus group attacked cryptocurrency businesses with an evolved downloader malware. It is worth noting that Tistory is a South Korean blog posting service, which means the malware author is familiar with the South Korean internet environment:

*plugin course property **tistory** tag vacon slide parent manual themes product notice portal articles category doc entry isbn tb idx tab maincode level bbs method thesis content blogdata tname*

The malware encodes the generated identifier as base64 and POSTs it to the C2. Finally, the agent fetches the next payload from the C2 server and loads it in memory directly. Unfortunately, we couldn't obtain a copy of it, but according to our telemetry, the fetched payload
the malw

```
cmd.exe
cmd.exe
cmd.exe
cmd.exe
cmd.exe
cmd.exe
```

Per

Using th
persiste
the follo

```
rundll32
```

4GO-R19
are save
It is resp
the com

the infection:

- *C:\Windows\system32\[random 2 characters]svc.drv*

This file is disguised as a legitimate tool named SageThumbs Shell Extension. This tool shows image files directly in Windows Explorer. However, inside it contains an additional malicious routine.

While creating this file, the installer module fills it with random data to increase its size. The malware also copies cmd.exe's creation time to the new file in order to make it less easy to spot.

For logging and debugging purposes, the malware stores information in the file provided as the second argument (*c:\programdata\oracle\~TMP739.TMP* in this case). This log file contains timestamps and information about the infection process. We observed that the malware operators were checking this file manually using Windows commands. These debugging messages have the same structure as previous malware used in attacks against cryptocurrency businesses involving the Lazarus group. More details are provided in the Attribution section.

After that, the malware decrypts its embedded configuration. This configuration data has a similar structure as the aforementioned wAgent malware. It also contains C2 addresses in the

same format:

- *hxxps://iski.silogica[.]net/events/serial.jsp@WFRForms.jsp@import.jsp@view.jsp@cookie.jsp*
- *hxxp://sistema.celllab[.]com.br/webrun/Navbar/auth.jsp@cache.jsp@legacy.jsp@chooseIcon.jsp@customZoom.jsp*
- *hxxp://www.bytecortex.com[.]br/eletronicos/digital.jsp@exit.jsp@helpform.jsp@masks.jsp@Functions.jsp*
- *hxxps://sac.najatelecom.com[.]br/sac/Dados/ntlm.jsp@loading.jsp@access.jsp@local.jsp@default.jsp*

The malware encrypts configuration data and stores it as a predefined registry key with its file name:

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\Emulate – [random 2 characters]svc*

It also takes advantage of the Custom Security Support Provider by registering the created file path to the end of the existing registry value. Thanks to this registry key, this DLL will be loaded by lsass.exe during the next startup.

- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa – Security Packages :*
  kerbe

Finally, th
searche
charact
embedd
payloads

Book

The phar
COVID-1
previous
possibly
the Laza
Bookcod
vector f
similar to

Bookcode infection procedure

Although we didn't find the piece of malware tasked with deploying the loader and its encrypted Bookcode payload, we were able to identify a loader sample. This file is responsible for loading an encrypted payload named gmslogmgr.dat located in the system folder. After decrypting the payload, the loader finds the Service Host Process (svchost.exe) with *winmgmt, ProfSvc* or *Appinfo* parameters and injects the payload into it. Unfortunately, we couldn't acquire the encrypted payload file, but we were able to reconstruct the malware actions on the victim

FROM THE SAME AUTHORS

A cascade of compromise: unveiling Lazarus' new campaign

Following the Lazarus group by tracking DeathNote campaign

BlueNoroff introduces new methods bypassing MoTW

Kimsuky's GoldDragon cluster and its C2 operations

machine and identify it as the Bookcode malware we reported to our Threat Intelligence Report customers.

Upon execution, the Bookcode malware reads a configuration file. While previous Bookcode samples used the file *perf91nc.inf* as a configuration file, this version reads its configuration from a file called *C_28705.NLS*. This Bookcode sample has almost identical functionality as the malware described in the comprehensive report recently published by Korea Internet & Security Agency (KISA). As described on page 57 of that report, once the malware is started it sends information about the victim to the attacker's infrastructure. After communicating with the C2 server, the malware provides standard backdoor functionalities.

Post-exploitation phase

The Lazarus group's campaign using the Bookcode cluster has its own unique TTPs, and the same mo

- Extra
  dump
- Using
- Using

After ins
system a
registry

- exe /
  "%te
- exe /
  "%te

In the lat
acquiring
executed

- exe /c "netstat -aon | find "ESTA" > %temp%\~431F.tmp
- exe /c "net use \\172.[redacted] "[redacted]" /u:[redacted] > %temp%\~D94.tmp" 2>&1"
- wmic /node:172.[redacted] /user:[redacted] /password:"[redacted]" process call create "%temp%\engtask.exe" > %temp%\~9DC9.tmp" 2>&1"

Moreover, Lazarus used ADfind in order to collect additional information from the Active Directory. Using this utility, the threat actor extracted a list of the victim's users and computers.

Infrastructure of Bookcode

As a result of closely working with the victim to help remediate this attack, we discovered an additional configuration file. It contains four C2 servers, all of which are compromised web servers located in South Korea.

- hxxps://www.kne.co[.]kr/upload/Customer/BBS.asp
- hxxp://www.k-kiosk[.]com/bbs/notice_write.asp
- hxxps://www.gongim[.]com/board/ajax_Write.asp
- hxxp://www.cometnet[.]biz/framework/common/common.asp

The BlueNoroff cryptocurrency hunt is still on

One of those C2 servers had directory listing enabled, so we were able to gain insights as to how the attackers manage their C2 server:

Attacker files listed on a compromised website

We discovered several log files and a script from the compromised server, which is a "first-stage" C2 server. It receives connections from the backdoor, but only serves as a proxy to a "second-stage" server where the operators actually store orders.

File name	Description
_ICEBIRD007.dat	A log file containing the identifier of victims and timestamps.
~F05990302ERA.jpg	Second-stage C2 server address: hxxps://www.locknlockmall[.]com/common/popup_left.asp

Logic of the C2 script

Besides implant control features, the C2 script has additional capabilities such as updating the next-stage C2 server address, sending the identifier of the implant to the next-stage server or removing a log file.

table_nm value	Function name	Description

table_qna	qnaview	Set [id]_209 variable to TRUE and save the "content" parameter value to [id]_211.
table_recruit	recuritview	If [id]_209 is SET, send contents of [id]_211 and reset it, and set [ID]_209 to FALSE.
table_notice	notcieview	Set [id]_208 and save the "content" parameter value to [id]_210.
table_bVoice	voiceview	If [id]_208 is SET, send contents of [id]_210 and reset it, and set [id]_208 to FALSE.
table_bProduct	productview	Update the ~F05990302ERA.jpg file with the URL passed as the "*target_url*" parameter.
table_community	communityview	Save the identifier of the implant to the log file. Read the second-stage URL from *~F05990302ERA.jpg* and send the current server URL and identifier to the next hop server using the following format: *bbs_type=qnaboard&table_id=[base64ed identifier] &accept_identity=[base64 encoded current server IP]&redirect_info=[base64ed current server URL]*
table_fre		

Attri

We asse
Lazarus
both inci
malware
the Laza

- Both
appe
- Both
- Both

Here is a
the malw
attack:

Debugging log from ministry of health case	Debugging log of cryptocurrency business case
15:18:20 **Extracted Dll :** *[random 2bytes]*svc.drv	**Extracted Dll :** *[random 2bytes]*svc.dll
15:59:32 **Reg Config Success !**	Extracted Injecter : *[random 2bytes]*proc.exe
16:08:45 **Register Svc Success !**	**Reg Config Success !**
16:24:53 Injection Success, Process ID : 544	**Register Svc Success !**
	Start Injecter Success !

Regarding the pharmaceutical company incident, we previously concluded that Bookcode is exclusively used by the Lazarus group. According to our Kaspersky Threat Attribution Engine (KTAE), one of the Bookcode malware samples (MD5 0e44fcafab066abe99fe64ec6c46c84e) contains lots of code overlaps with old Manuscrypt variants.

Kaspersky Threat Attribution Engine results for Bookcode

Moreover, the same strategy was used in the post-exploitation phase, for example, the usage of ADFind in the attack against the health ministry to collect further information on the victim's environment. The same tool was deployed during the pharmaceutical company case in order to extract the list of employees and computers from the Active Directory. Although ADfind is a common tool for the post-exploitation process, it is an additional data point that indicates that the attac

Conc

These tw
While th
after str
as vacci

Indicat

wAgent

dc3c266
26545f5
9c6ba96

wAgent

4814b06d05695074 9d07be2c799e8dc2 %programdata%\oracle\javac.io, %appdata%\ntuser.dat

wAgent compromised C2 servers

```
http://client.livesistemas[.]com/Live/posto/system.jsp@public.jsp@jenkins.jsp@tomas.jsp@story.
hxxps://iski.silogica[.]net/events/serial.jsp@WFRForms.jsp@import.jsp@view.jsp@cookie.jsp
hxxp://sistema.celllab[.]com.br/webrun/Navbar/auth.jsp@cache.jsp@legacy.jsp@chooseIcon.jsp@cus
hxxp://www.bytecortex.com[.]br/eletronicos/digital.jsp@exit.jsp@helpform.jsp@masks.jsp@Functio
hxxps://sac.najatelecom.com[.]br/sac/Dados/ntlm.jsp@loading.jsp@access.jsp@local.jsp@default.j
```

wAgent file path

```
%SystemRoot%\system32\[random 2 characters]svc.drv
```

wAgent registry path

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Application\Emulate - [random 2
```

Bookcode injector

```
5983db89609d0d94c3bcc88c6342b354    %SystemRoot%\system32\scaccessservice.exe, rasprocservice.
```

Bookcode file path

```
%SystemRoot%\system32\C_28705.NLS

%SystemRoot%\system32\gmslogmgr.dat
```

Bookcode compromised C2 servers

```
hxxps://www.kne.co[.]kr/upload/Customer/BBS.asp
hxxp://www.k-kiosk[.]com/bbs/notice_write.asp
hxxps://www.gongim[.]com/board/ajax_Write.asp
hxxp://www.cometnet[.]biz/framework/common/common.asp
hxxps://www.locknlockmall[.]com/common/popup_left.asp
```

MITRE ATT&CK Mapping.

Tactic	Technique.	Technique Name.
Execution	T1059.003 T1569.002	Command and Scripting Interpreter: Windows Command Shell System Services: Service Execution
Persistence	T1547.005 T1543.003	Boot or Logon Autostart Execution: Security Support Provider Create or Modify System Process: Windows Service
Privilege Escalation	T1547.005	Boot or Logon Autostart Execution: Security Support Provider
Defense Evasion		
Credential Access		
Discovery		
Lateral Movement	T1021.002	SMB/Windows Admin Shares
Command and Control	T1071.001 T1132.001	Application Layer Protocol: Web Protocols Data Encoding: Standard Encoding
Exfiltration	T1041	Exfiltration Over C2 Channel

BACKDOOR LAZARUS MALWARE DESCRIPTIONS MALWARE TECHNOLOGIES MEDICAL THREATS TARGETED ATTACKS

Lazarus covets COVID-19-related intelligence

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

Type your comment here

Name *

Email *

Comment

// LATEST POSTS

SAS

The Cry… APT: Inv…

BORIS LARIN…

…houls

…es of

// LA…

THR…

…PS

04 SEP 202…

60 MIN

Inside the Dark Web: exploring the human side of cybercriminals

ANNA PAVLOVSKAYA

The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise

OLEG GOROBETS, ALEXANDER LISKIN

Cybersecurity's human factor – more than an unpatched vulnerability

OLEG GOROBETS

Building and prioritizing detection engineering backlogs with MITRE ATT&CK

ANDREY TAMOYKIN

// REPORTS

Beyond the Surface: the evolution and 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.

BlindEagle flying high in Latin America

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.

// SU
MAILS
The hott
cribe

kaspe

Industrial threats
Web threats
Vulnerabilities and exploits
All threats

Security technologies
Research
Publications
All categories

Encyclopedia
Threats descriptions
KSB 2023

Privacy Policy | License Agreement | Cookies