Top Content

Analysis of

ThreatBook

Act With Intelli

Published Nov

#ThreatBook Securi

Summary

APT-C-60 is disclose reported that the earliest attack time rgets human resources and trade nonitoring by ThreatBook Intellige the Group has been active since December 2021. In June this year, the Group launched targeted attacks on targets in S. Korea. With analysis of the attacks, the findings are as follows:

- The targets of this batch of attacks include Dr. Bernhard Seliger, the representative of the Hanns Seidel Stiftung, and politicians who may be related to the 2022 Pyeong Chang Peace Forum.

- ThreatBook extrac lysis of related samples, IPS, and igence detection. TDP, TIP, API, OneDNS, ection of this attack activity and group

Details

On June 20, 2022, as follows. The attacker pretended i fense to induce the target person to dow .

The downloaded file nd malicious lnk files. The bait files r se environment of the office causes th

According to the ma lesktop-iag9k61, we also found attack on the early stage of the Pyeong Chang Peace Forum in February 2022 by APT-C-60. The bait file used is as follows.

In the two attacks, the bitbucket.org site used for payload hosting and file uploading included user IDs: grand9_neat, Miravos, sorakas. Storage files related to the current attack have been deleted.

Sample Analysis

The payload executi g from the downloaded compre ided into three parts: Lnk file with r smon.db) with file information acquisit rojan (TaskControler.dll) w ction. Subsequent sections are to anal

Malware Lnk

Taking "Online ques th Korea.docx.lnk" as an example, the

The command-line of Lnk file is as follows. Call mshta to execute remote javascript.

Javascript resource jumps through the html index code.

Obfuscated javascript code after the jump is as follows.

By jacking the COM 0-A3A5-00C04FD706EC, th The CLSID is bound to the service ated to Windows scheduled tasks, ar os starts.

mssysmon.db

Taking "mssysmon.d rmation is as follows.

Analyze the landing re function is provided by tdstart e the unique instance running by creating a 576B6".

Decrypt the C&C configuration, which contains multiple URL address. The Trojan heartbeat interval is 6 hours.

Traverse c:\Program Files\ directory, acquire file directory information, and send it to the C&C server. C&C

http://162.222.214

https://c.statcounte

Traverse the %AppD he .mui file and load msiobj.dll file. oad it again. The download address i

http://185.207.206

https://bitbucket.or

https://bitbucket.or

The loading logic in ry is as follows. Rename the downlo and then load and call msiobj0.dll!ExtF , and delete the mui file.

TaskControler.dll

Taking "TaskControler.dll" as an example to analyze, the sample information is as follows.

for the encryption and decryption of the communication field in the subsequent C&C communication.

Before running the T using the mutex "9ABKD3409ABACL

Open the %AppData ings directory. If it does not exist, crea

After that, the Trojar %AppData%\Roamin tory , and runs the attack payload i

Decrypt C&C 160.2 t to obtain the internet IP. Acquire information of host and user into the core Trojan work logic. When it is detected and judged that the system has been started for more than 6 hours, the main thread is to go online with C&C, set a ten-minute heartbeat interval, and schedule working thread by event object signals.

The working thread is composed of five independent threads which respectively complete the corresponding functions: task request, result feedback, screen

partially parsed as follows.

There are also post …&b004=*", "c001=*&c002=*&… cation, which respectively represe… wnloading action and file uploading.

In the file uploading … ssing of screenshot files and file conten… and converted to decimal strings; the… en converted to decimal strings.

By parsing C&C com… ve the functions such as file director… ess termination, DLL loading, screenshot… tory deletion and cmd shell.

The full RAT parsing is as follows.

Support encrypted file download. The download file landing path is temp%\wcts66889.tmp, which needs to be decrypted by AES. AES128 key={21 A4

Association Analys

This sample is basi e landing payload in the previous APT-C- ntroler.dll is the same as the histori e code behavior and communication proc e historical attack time analysis of the onent directory and payload traversal loa "extension", "%AppData%\Roami e, it is more credible to attribute

Appendix - IOC

C2

131.226.4.22:80

160.20.147.118:80

URL

http://185.145.97.

http://131.226.4.2

http://162.222.214

http://185.145.97.

http://185.145.97.

http://185.145.97.

http://185.207.206

http://82.221.129.

http://82.221.129.

http://82.221.136.

https://160.20.147 b2/command.asp

https://160.20.147 b2/result.asp

https://bitbucket.org/grand9_neat/well/downloads/19132.bmp

https://bitbucket.org/grand9_neat/well/downloads/19164.bmp

https://bitbucket.org:443/grand9_neat/well/downloads/19164.bmp

https://bitbucket.org/miravos/style/downloads/1932.bmp

https://bitbucket.org/miravos/style/downloads/1964.bmp

https://bitbucket.org/sorakas/mod/downloads/1932.bmp

Hash

13f09fd98259e663...ae57ed09c77

266ee1b357cad72...0d813c22b3009

74b34adf28552f38...b891e7740ad91

7c4fb90eeb997555...c4ac50ffd906

7ec34297e0c4e5b1...271544f87244e0

92912bfb10b47595...1db642457328da

9bb60e54c09934c5...4519025d1f9b0

a995f4e4e5bec985...530bedef5e74f6

b2dd50760765abfb...bc4390c30a26fc

bc879fe3e928ca9c...b312cf9f7dd04

bffacbb0b54a3b1dc...0f7b63ba4fa4

dbc1754de49824d1...cfc6f450c2c0e4

e869e82a9f44d81b...86726ab22c500

edec420761cd95ba...3e0cb1fa4cf84

ee862a3d57e45a2...f0819cc7496664

f50cd82717837a5b...0ae90fb37e01

File Path

%appdata%\Microsoft\Vault\UserProfileRoamings\

%appdata%\Microsoft\Vault\

%appdata%\Microsoft\Internet Explorer\UserData\

%AppData%\Microsoft\HTML Help\

ThreatBook Selecte
First-ever Gartner®
Jun 4, 2025

m Alerts to Action: N
R+TIP Security···
13, 2025

Explore content

Career | Productivity | Project Management

Show more