Threat Intelligence | OceanLotus uses social security topics as bait to conduct APT attacks

Original 404 Advanced Threat Intelligence Know Chuangyu 404 Laboratory

July 9, 2024 11:16

Author: Know Chuangyu 404 Advanced Threat Intelligence Team
Time: July 9, 2024

1 Overview

Recently, the Advanced Threat Intelligence Team of Zhichuangyu 404 discovered an attack sample targeted by the OceanLotus organization. The sample used words such as social security and provident fund adjustment to attract victims to click. At the same time, we found that this sample was similar to the OceanLotus APT organization discovered in 2023, which imitated APT29 attacks. Activity analysis is very consistent.

2. Organizational background

OceanLotus, also known as APT32, is an advanced persistent threat (APT) organization that has been active since 2012 and mainly targets government agencies, companies, media and activists in East and Southeast Asia. The organization has diverse attack methods and possesses a large number of self-developed weapons. It often combines open source tools at different stages of attack activities to achieve attack goals.

3. Sample chain

The sample chain is shown below:

4. Sample Overview

The sample found this time is called "Notice on Adjustment and Reduction of Social Security, Occupational Annuity, and Provident Fund Payment Bases.docx" (hereinafter referred to as the bait file). The bait file has four built-in contents, namely lnk parameters, hta script, The four parts of the dropper program and bait document cooperate with each other to achieve the set functional goals.

LNK file properties

The overall command flow is to execute the hta file with the lnk parameter, the hta file executes the dropper program & decoy document, the dropper decrypts and loads the shellcode and executes the final Cobalt_Strike RAT program. The function details of each part are described as follows:

4.1 LNK files

The LNK file is the original payload and is used to start the overall release chain. The CMD command is executed through ShellExec. The CMD command function in the LNK file is:

1. Make sure that 360 Security Guard related files do not exist

2. Copy itself to NTUSER.DAT{23e7c2f3-52ef-4b7b-b203-3bfaa90a833d}.TM.alf and start it through mshta.exe. The copy logic is divided into two types, and different execution logic is distinguished according to whether there is an LNK file with the original file name. If the LNK file with the original file name exists, copy it directly; if the LNK file with the original file name does not exist, traverse %USERPROFILE% the path to find the LNK file with the original file name, and then copy the file to it NTUSER.DAT{23e7c2f3-52ef-4b7b-b203-3bfaa90a833d}.TM.alf and start it through mshta.exe. The distinguishing code in this section can be used to detect the following functions:

   (1) Whether the file name has been changed

   (2) Maybe the original landing file is in %USERPROFILE% the path

LNK file parameters

4.2 NTUSER.DAT{23e7c2f3-52ef-4b7b-b203-3bfaa90a833d}.TM.alf

This file is stored at the end of the LNK file and is started by the mshta.exe program. Based on the behavior, it is guessed that mshta.exe starts the HTA by locating the mark point, so there is no need to extract the HTA file to start the HTA file.

The HTA file has four functions: locating and saving the dropper program, locating and saving the decoy document, running the decoy document, and repairing the dropper program. Each functional module is described as follows:

1. Locate and save the dropper program

First load itself (NTUSER.DAT{23e7c2f3-52ef-4b7b-b203-3bfaa90a833d}.TM.alf) and set the file cursor to offset： 11742 read 249374 size data, save the read data to %appdata%\Lenovo\devicecenter\extends\modules\showdesk\LenovoDesk.exe , then read 1032190 size data and save it to %appdata%\Lenovo\devicecenter\extends\modules\showdesk\QuickDeskBand.dll .

Set the cursor and read the dropper content & document content dropper program starting address

2. Locate and save the bait document

Save the dropper's subsequent data to the local computer %temp%\关于社保、职业年金、公积金缴存基数调整和补扣的通知.docx and start the file.

Decoy file offset

3. Repair dropper program

4.3 Bait documents

Part of the bait document is as follows:

4.4 dropper&COBALT_STRIKE RAT

The previously saved dropper program is used to decrypt and start Cobalt_Strike. The startup of the dropper program is implemented in the parameter part of lnk.

Start white file

Functions QuickDeskBand.dll loaded after the white file (LenovoDesk.exe) is run . ShowBatteryGauge

Load black files

After the black file is loaded, it is run in dllmain to decrypt the subsequent payload. When ShowBatteryGauge exports its main function, LenovoDesk.exe is written into the registry run startup item:

Set run startup items

After QuickDeskBand.dll is loaded, it will inevitably enter dllMain to run. In dllMain, the main program path is first obtained, and the last 15 characters are used as the key to decrypt the data.

Decrypt data using file name as key

The decrypted data is IP dotted decimal data. By RtlIpv4StringToAddressA converting the dotted decimal IP address into data in HEX address form, the data in HEX address form is COBALT_STRIKE data. Then Cobalt_Strike is started immediately by setting the callback of the enumeration font.

Decode CS data

Cobalt_Strike is a paid penetration testing product that allows attackers to deploy an agent called "Beacon" on the victim machine. Beacons provide attackers with a rich set of capabilities, including but not limited to command execution, keystroke logging, file transfers, SOCKS proxies, privilege escalation, mimikatz, port scanning, and lateral movement. Beacon is in-memory/fileless in that it consists of stageless or multi-stage shellcode that, once loaded by exploiting a vulnerability or executing a shellcode loader, reflexively loads itself into the process's memory without touching it. disk.

Supports C2 and segmentation over HTTP, HTTPS, DNS, SMB named pipes, and forward and reverse TCP, and beacons can be daisy-chained. Cobalt Strike comes with a toolkit for developing shellcode loaders called Artifact Kit.

Due to the powerful functions and compatibility of this platform, many APT organizations also include CS in their arsenal. In previous APT32 attack activities, we often found that they used CS as a RAT program.

The final CS Beacon of the two LNK files is the same and the related key configuration information is as follows:

From the Metadata metadata, it can be found that its HTTP Header is forged around dhgate.

- Host: www.dhgate.com
- Host: shoppingcart.dhgate.com

5. Summary

From the above sample analysis, we can find that the sample captured this time is consistent in many aspects with the attack activities launched by the organization using the BMW topic as bait in 2023.

First, the lnk parameter format is very consistent.

Sample parameter analysis and comparison

Secondly, the configuration files of Cobalt Strike are relatively consistent. Except for the URL, the disguised host is also the same.

Configuration file comparison

In summary, we believe that the samples captured this time and the attack samples used by the OceanLotus organization using BMW bait in 2023 should belong to the same organization.

6. IOC

Hash :

- f04971c65d68319fbe1285b4a83afed6 QuickDeskBand.dll

- 2d6b3b3e13600721fc9f398cd7df05ca Bait Document

7. Reference links

[1] Analysis of OceanLotus APT organization imitating APT29 attack activities