Analysis of THREATNEEDLE C&C Communication (feat. Google TAG Warning to Researchers)

By S2W

Published: 2021-01-29 · Archived: 2026-04-05 21:26:39 UTC

4 min read

Jan 27, 2021

Author:

(Sojun Ryu)
Modified History
- 01/28/2021 **IoC Updated**
- 01/28/2021 **Report Updated**

Malware mentioned in "North Korean hackers have targeted security researchers via social media report" published by Google Threat Analysis Group (TAG) is considered to be a **ThreatNeedle** which is dubbed by Kaspersky. We already disclosed the deep analysis regarding C2 communication of ThreatNeedle at **DCC 2019** and **Kaspersky SAS Lightning Talk 2019**.
In addition, the malware and C2 communication have in common with Operation MalBus.

Additional Reference for Operation MalBus
> MalBus Actor Changed Market from Google Play to ONE Store

We briefly delivers only the essential fact in Medium, and for other details, please refer to the **attached PDF file** which is presented at DCC and Kaspersky SAS.

DOWNLOAD REPORT

Below is tweet from Seongsu Park of Kaspersky GReAT team stating that this malware is ThreatNeedle.

ThreatNeedle is already known that it has been used by the Lazarus group along with Manuscrypt from the past. Most of them operate through HTTP communication, and C&C servers are written in languages such as ASP and JSP. ThreatNeedle downloaded during the infection process receives commands from the C&C server and performs malicious actions, and the overall process is as follows.

The definition of each term is as below.

Troy → ThreatNeedle malware installed on Victim
Proxy → Control Page of C&C Server (.ASP, .JSP)
favicon.icon → Store IDs of Infected devices (only Troy's ID)
build.xnl → Store Time, IP, ID of all authenticated connections (Troy and Manager)
desktops.inf → Store URL of MID server
[TroyID] → Identification value for each infected devices randomly generated when infected with ThreatNeedle
[TroyID].jpg → Store Victim who has [TroyID] information or command result
[TroyID].bmp → Store Attacker's command

Troy(ThreatNeedle) → Proxy(C&C Page)

The infected device information is transmitted to Proxy server and waits until specific command is received. Communication with the proxy is possible only when a specific type of parameter is transmitted, and Troy's connection is processed by the proxy's **handleTroy function**. The action for each commands are as follows.

Query Structure: [Field 1]=[**Cmd**]&[Field 2]=?&[Field 3]=[**TroyID**]&[Field 4]=[Packet ID]&[Field 5]=[**Buffer Size**]&[Field 6]=[**Buffer**]

- **Cmd**, **TroyID**, **Buffer Size** and **Buffer** are actually used, but the 2nd and 4th field are not in use.

Proxy initially receives the command 71 from Troy and saves the information of infected devices as **[TroyID].jpg** file on the Proxy server. After checking the connection with the MID by using the command 81, the ID of the infected device, that is, Troy ID, is saved in **favicon.icon***. After that, if there is a command file called **[TroyID].bmp**, it is read and transmitted to Troy. After the initial authentication is completed, the attacker's remote control command is stored in **[TroyID].bmp** encoded with **base64^0xA4**, and the result of executing the command is stored in the same encoding method in **[TroyID].jpg**. Files used in this process are immediately deleted.

> ***favicon.icon** → store IDs of Infected devices

Proxy → MID

When 'Troy' connects to the 'Proxy', and the command 81 is executed, Proxy sends its information to MID. An 'attacker' is capable of identifying the logs stored on MID server in order to identify the 'Proxy' servers that are connected with 'Troy.' In order to communicate with 'MID', specific command value and Proxy ID authentication from **[Figure 1]** should be executed. Commands are sent and received only when the MID server is active.

Query Structure: id=[**CMD**]&field=[0 or ProxyURL]&buffer=[ProxyID]&iframe=[1 or 0]&frame=[0 or 1] [&uframe=3]

- There are **111** and **112** for **CMD**. 111 is used to update MID server and 112 is used when Troy is connected.

Manager → Proxy

The attacker sends commands to ‘Troy’ through the ‘Manager’. Adversary is capable of handling C&C infrastructure such as collecting the stored log file on Proxy server and updating MID server.

Query Structure: [Field 1]=**[Cmd]**&[Field 2]=[Target TroyID]&[Field 3]=**[TroyID]**&[Field 4]=[Additional Information]&[Field 5]=**[Buffer Size]**&[Field 6]=**[Buffer]**

- Cmd, TroyID, Buffer Size and Buffer are always used, but the 2nd/4th fields are used only for the certain command.
