Analysis of APT organization Confucius's cyber attack against IBO anti-terrorism operations in Pakistan

Fuying Laboratory ⋮

I. Overview

Affected by various factors, Pakistan has long suffered serious threats from local terrorism, and the country has always regarded counter-terrorism as an important national security strategy. In the second half of 2022, Pakistani security forces launched multiple intelligence-based operations (IBOs) in Balochistan, Khyber District, North Waziristan District and other places, raiding and killing several terrorist.

Pakistan's recent high-profile performance in counter-terrorism has aroused the attention of India. On November 30, NSFOCUS Fuying Lab captured a cyber attack against the armed forces in the Multan area of Pakistan. The attacker used the IBO action report in the Rodland area of Multan as a bait to try to deliver a variant Trojan program to take control of the victim device. After analysis, NSFOCUS Technology Fuying Laboratory confirmed that the leader of the incident is the Indian APT organization Confucius.

2. Organizational association

Confucius is an APT organization funded by India. It has been carrying out cyber attacks since 2013. Its main targets are Pakistan, China and other neighboring countries of India. It has a strong interest in targets in the fields of military, government and energy.

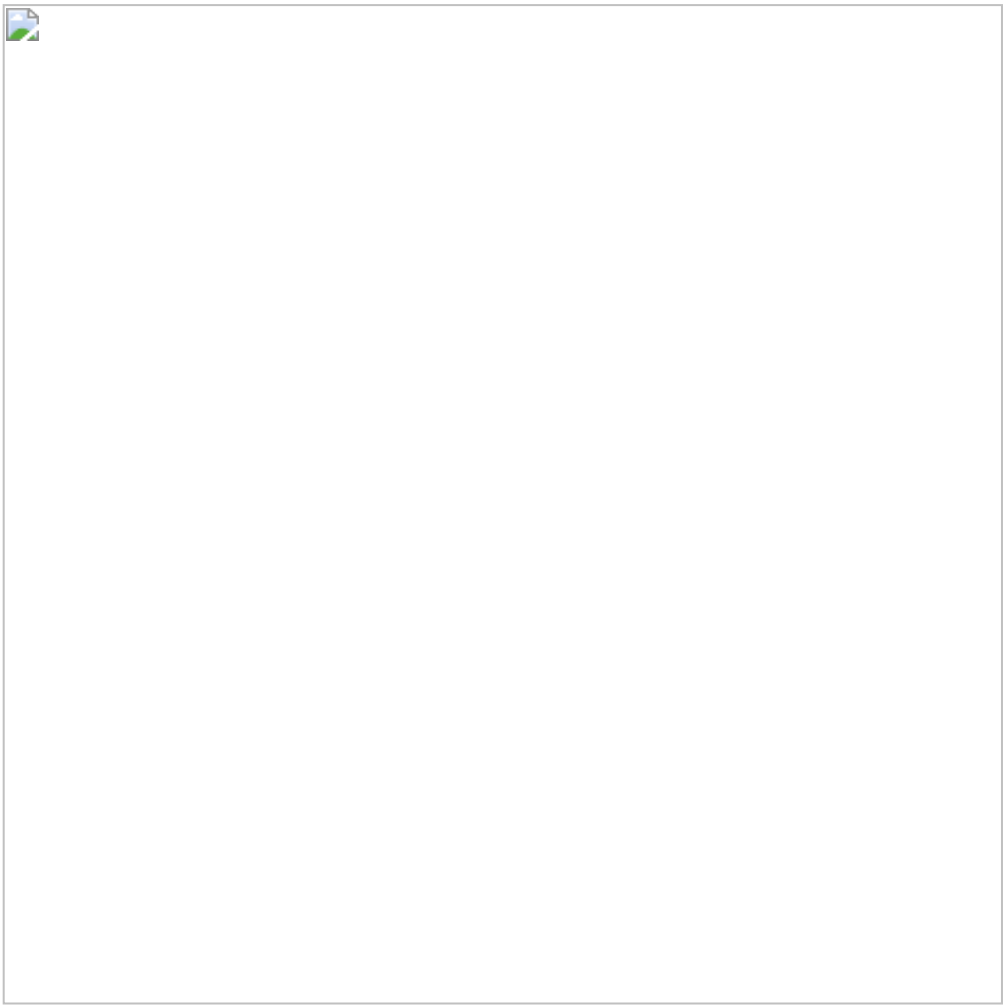
The Confucius organization will use Windows-side Trojan horse programs and Android-side Trojan horse programs to carry out espionage attacks on targets to steal information. The attack tools used include SubBird, CharSpy, and Hornbill, etc., which have strong development and penetration capabilities.

In this attack, the Confucius attackers followed their common decoy construction mode and used a new version variant program of the organization's known attack tool MessPrint.

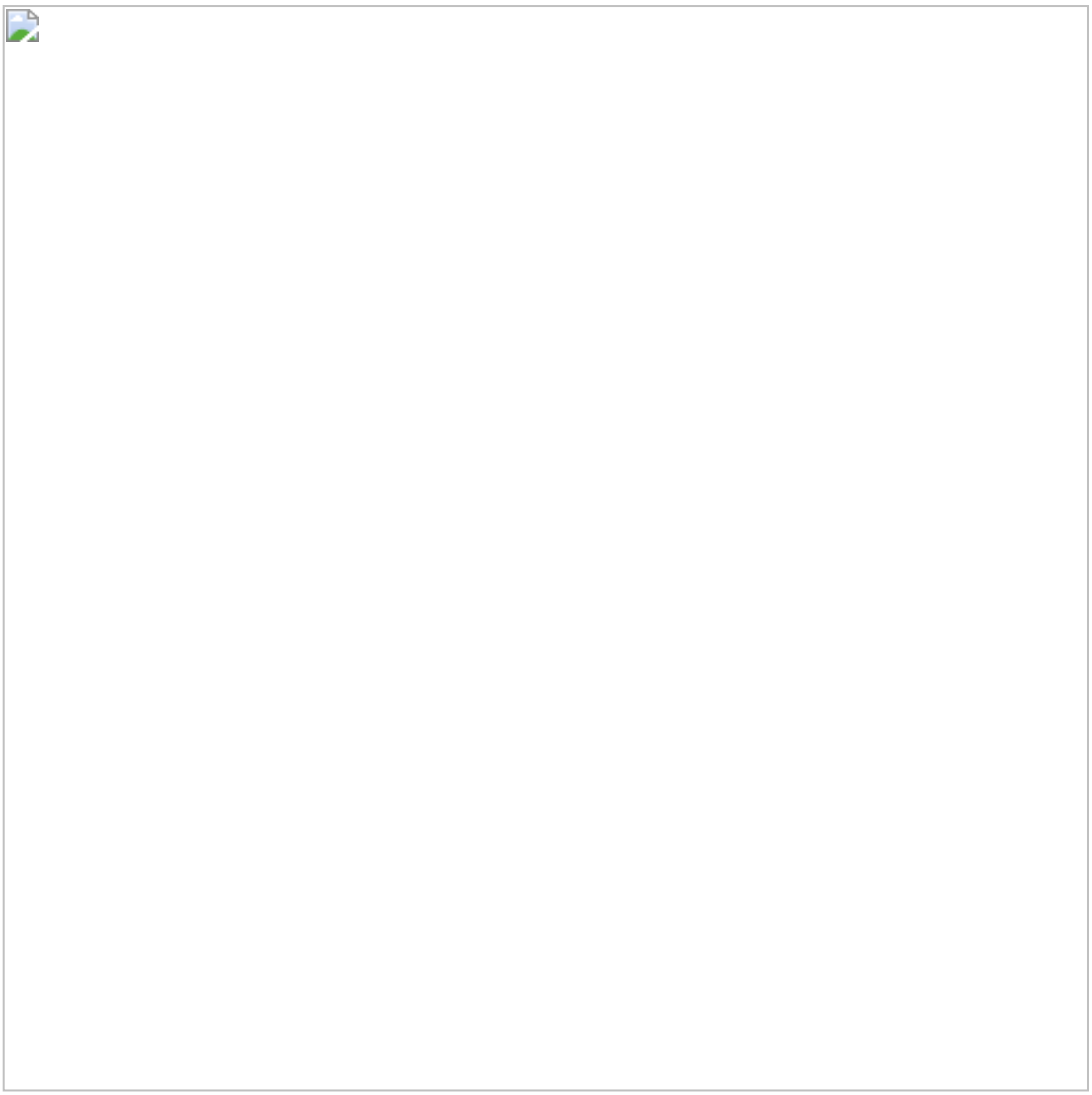
3. Attack process

In this cyber attack incident, the Confucius attackers constructed a phishing document named "IBO_Lodhran.doc" (Intelligence-Based Operations in the Lodland Region) and a phishing document named "US_Dept_of_State_Fund_Allocations_for_Pakistan.doc" (United States Department of State Fund Allocations for Pakistan) , targeting Pakistan's security forces and diplomatic government departments respectively.

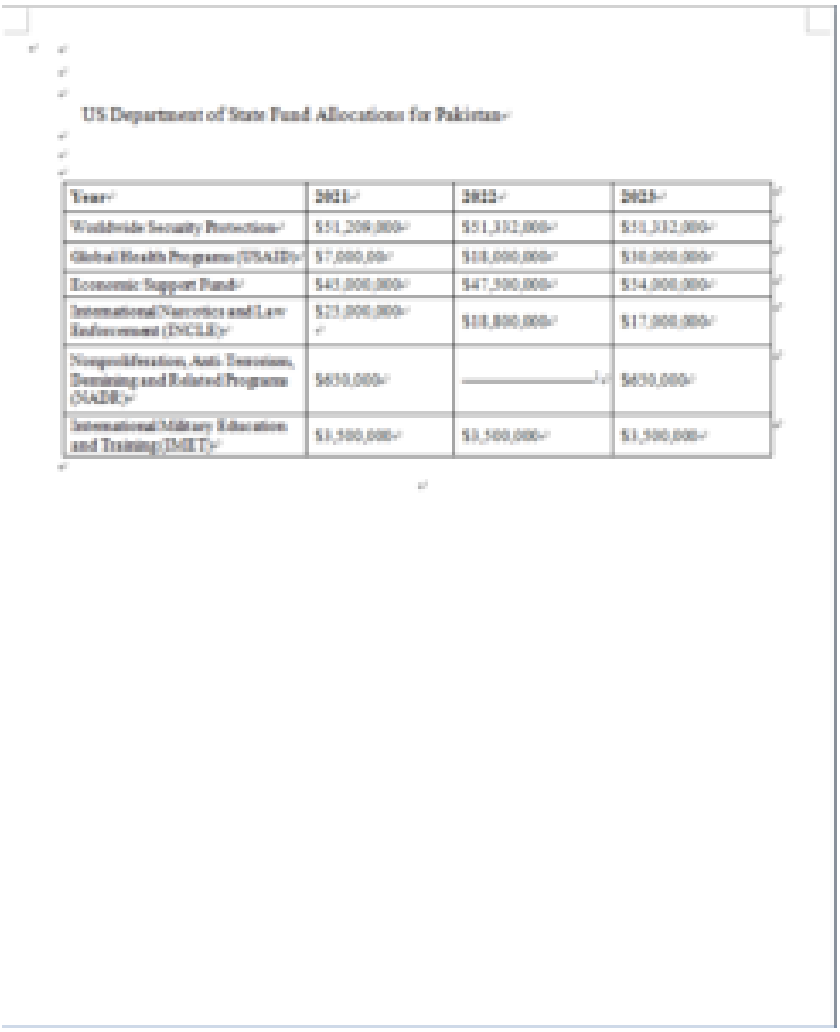
These phishing documents carry intelligence content with a certain degree of authenticity, and use prompt information to induce the victim to start the editing function of the document, and then execute an attack process of implanting a variant Trojan horse.



Tips for phishing documents



IBO_Lodhran.doc phishing document content

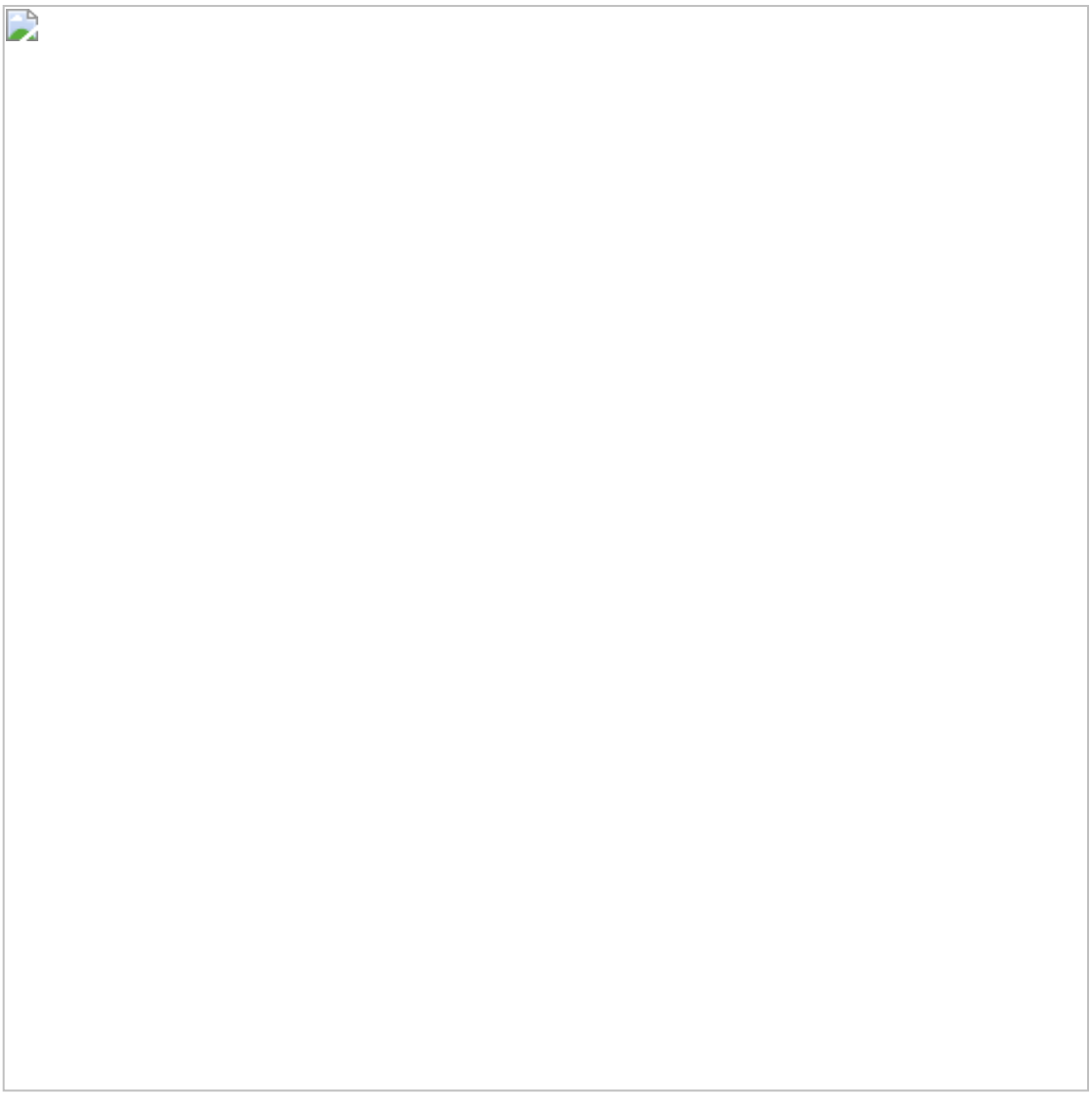


US Department of State Fund Allocations for Pakistan

Year	2021	2015	2025
Worldwide Security Protection	$51,209,000	$51,332,000	$51,332,000
Global Health Programs (USAID)	$7,000,00	$10,000,000	$10,000,000
Economic Support Fund	$43,000,000	$47,500,000	$14,000,000
International Narcotics and Law Enforcement (INCLE)	$23,000,000	$18,800,000	$17,000,000
Nonproliferation, Anti-Terrorism, Demining and Related Programs (NADR)	$650,000	———————	$650,000
International Military Education and Training (IMET)	$1,500,000	$1,500,000	$1,500,000

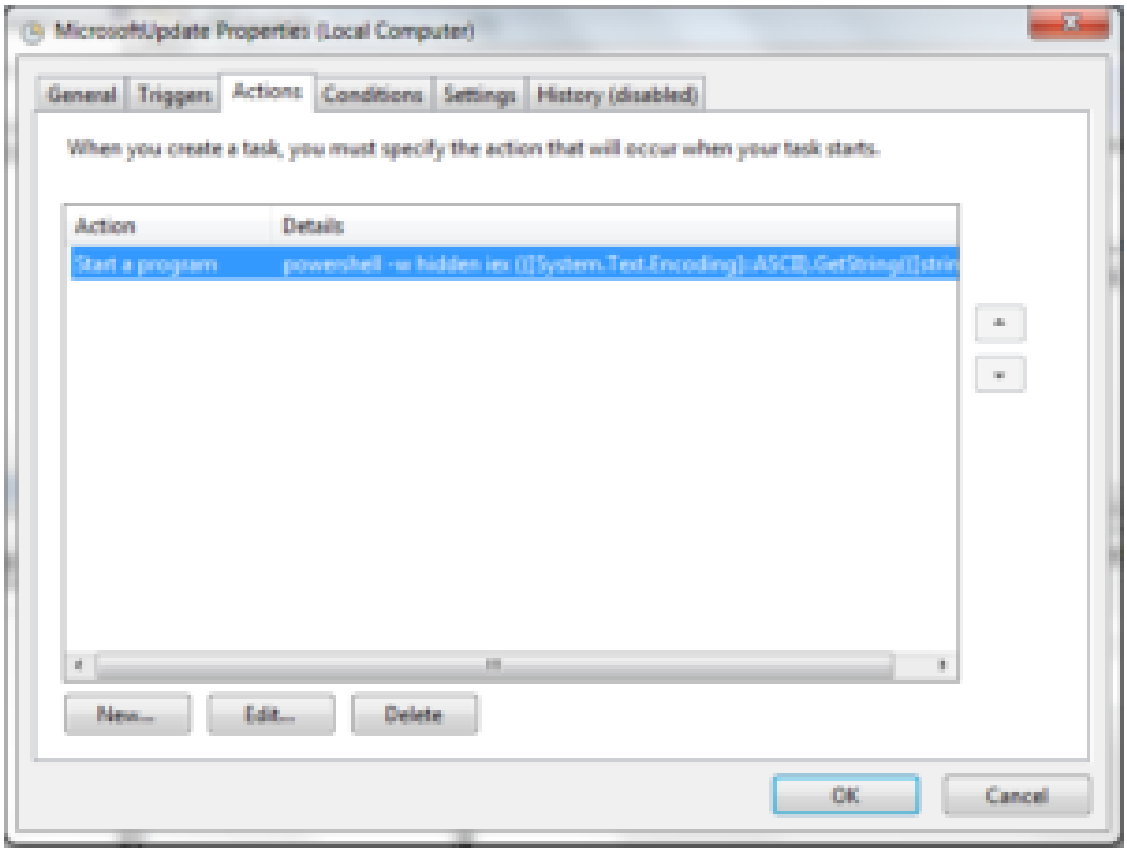
Figure 3.3 US_Dept_of_State_Fund_Allocations_for_Pakistan.doc phishing document content

The typical attack flow in this incident is shown in the figure below.



Typical attack flow of this incident

When the macro in the above phishing document is executed, the document releases an encrypted file named gist.txt to the specified directory, and sets a scheduled task to run every 30 minutes to run the file regularly.



Scheduled tasks for phishing document settings

The running gist.txt is actually a powershell Trojan horse. First, it initiates a link to the fixed location tcp://142.234.157[.]195:8080 to test connectivity, and uploads the local user name, computer name, mac The address, system information and other content are used as registration information; then a piece of encrypted data is downloaded from the fixed location http://microsoftonedriver[.]com:8989/enc.txt, decrypted into VERSION.dll and loaded and executed with the help of rundll32 component.

The VERSION.dll file is the main Trojan program used by Confucius attackers in this incident, and its connection CnC is tcp://info-updates.ddns[.]net:8080.

4. Trojan horse analysis

The main Trojan horse program VERSION.dll that appeared in this incident is a variant program of a known attack component of Confucius. For the convenience of follow-up tracking, Fuying Lab temporarily named the attack component MessPrint.

Compared with the previous version, the new version of the MessPrint Trojan program used by Confucius has changed a lot in terms of functions and countermeasures, and its main version number has also been upgraded from 2.XX to 3.1.0.

- **Features**

The main functions of the MessPrint variant Trojan that appeared this time are divided into three parts: operation log recording, victim host information upload and command execution.

After the Trojan runs, first create a log file named log.txt in the C:\ProgramData directory, and when the Trojan runs to each stage, the prompt information will be recorded in the log file. We did not find this recording function in the previous version of the Trojan horse program, so it is speculated that this version of the Trojan horse is a test version and was directly used by Confucius attackers in network attack activities.

Subsequently, the Trojan horse program collects various information of the victim's host, and aggregates the information into a piece of encrypted data and sends it to the CnC. The information collected by this Trojan is shown in the table below.

List of information collected by Trojans

Host information collected by the MessPrint variant Trojan	**content example**
hostname\username	WIN-SBSB6AEF44L\superlove
adapter mac address	00:0C:29:D0:13:FA
OS major version	Windows 7
operating system bits	version x64
List of current process PID and path	PID NO:300—— C:\Windows\System32\smss.exe PID NO:396—— C:\Windows\System32\csrss.exe
List of installed software	AddressBook Connection Manager

The above information directly uses the fixed symbol #$#* as the delimiter, and uses the fixed symbol iqaz as the end symbol at the end.

The above information will be encrypted by the following encryption method before being sent to CnC:

1. XOR 0x1D byte by byte;
2. Base64 transcoding;

The subsequent communication between the variant Trojan horse program and the CnC follows the above encryption method.

After sending the host information, the variant Trojan horse program and CnC use keywords such as "check_status", "verified", "hi" and "order" for multiple rounds of confirmation, and finally enter the command execution mode. In the command execution part, the MessPrint Trojan horse can respond to the following commands and parameters issued by CnC, and perform commands such as file download, program operation, and CMD command execution.

List of Trojan CnC commands

CnC command	Command parameter 1	command parameter 2	Features
DWN	Where to save the file		Download the file sent by CnC to the specified location
ALT	program location	Program running parameters	Run the program specified by CnC
app	cmd command		Run the CMD command specified by CnC
black	sleep time		Sleep for specified time

Through analysis, it is found that this version of the MessPrint Trojan program has made many changes in the functional part. On the one hand, it protects the CnC communication process through encryption, and on the other hand, it greatly reduces the file stealing and shell rebound functions in the previous version of the Trojan horse.

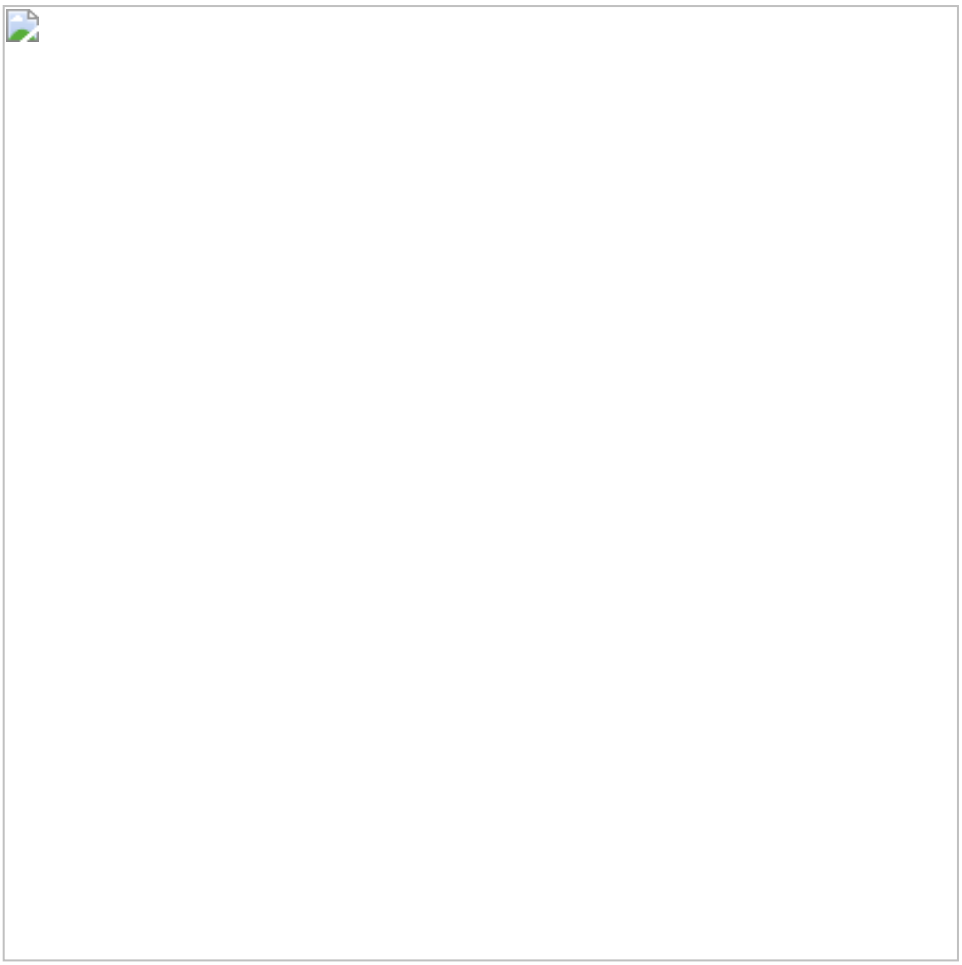
The above changes indicate that the positioning of the Trojan horse program has changed from a full-featured spyware to a Stub-type backdoor Trojan horse, and the subsequent spy Trojan horse functions are separated into independent components through component splitting. This change is very common in the development of APT attack components in recent years. APT attackers can use this refinement to reduce the exposure risk of the overall framework.

- **confrontation**

In the MessPrint Trojan that appeared this time, the developers of Confucius added a lot of anti-analysis techniques, which made the analysis of the Trojan more difficult.

The MessPrint Trojan mainly uses an exception-based control flow obfuscation technology. This obfuscation changes the ordinary linear process into a try-throw-catch structure, so that the two pieces of code that were originally linearly connected are divided into non-adjacent ones. try and catch block. In this way, the c++ object is thrown at a specific location, so that the execution process needs to jump to the code that can be directly executed under the linear structure through the C++ exception handling of VS.

The following figure shows the basic logic of this exception-based control flow obfuscation:



Confusion ideas used by the MessPrint Trojan

This obfuscation method can be used for static analysis of some decompilation tools, because most pseudocodes cannot normally restore the above exception handling process.

In addition, the Confucius developer also abused some common code obfuscation techniques in the MessPrint Trojan, such as stack inflation, redundant instructions, and meaningless code, further hindering static analysis. Considering the large number of development traces in this version of the MessPrint Trojan, we speculate that the Confucius developers had no choice but to enable the development version of the program, hoping to use obfuscation to reduce the loss caused by exposure.

V. Summary

As a direct demonstration of the country's armed forces in peacetime, Pakistan's recent series of IBO anti-terrorism operations have made India very sensitive. The APT attacks captured this time also show that India has begun to invest its cyber attack forces in related reconnaissance activities.

Through the analysis of this Confucius attack incident, on the one hand, we found that Confucius developers are still maintaining a relatively active pace of attack component development, and on the other hand, it also confirmed that APT group developers are generally splitting and framing attack components. Due to the gradual improvement of the APT capture, analysis, and disclosure process by the defender in recent years, APT attackers have to use a framework to rebuild attack tools, and control the use of components at all levels through level-by-level delivery to reduce the risk of complete exposure. risk.

6. IoC

Phishing document:

c75b8c150054b5ba27cf08c46e13354e

23537d81e9cd285b41185a0e4c3d37c1

Encrypted powershell Trojan file:
ab34c3eb8635fc13e4a586cba3c7469d

powershell Trojan CnC:

142.234.157[.]195:8080

Download address:
http[:]//microsoftonedriver[.]com:8989/enc.txt

MessPrint variant Trojan horse program:
65d9b142924d4e74cb729166f41b16fa

MessPrint Trojan CnC:
info-updates.ddns[.]net:8080

About Fuying Lab

Research targets include Botnet, APT advanced threats, DDoS countermeasures, WEB countermeasures, popular service system vulnerabilities, identity authentication threats, digital asset threats, black industry threats and emerging threats. Identify risks by controlling live network threats, mitigate threat damage, and provide decision-making support for threat confrontation.