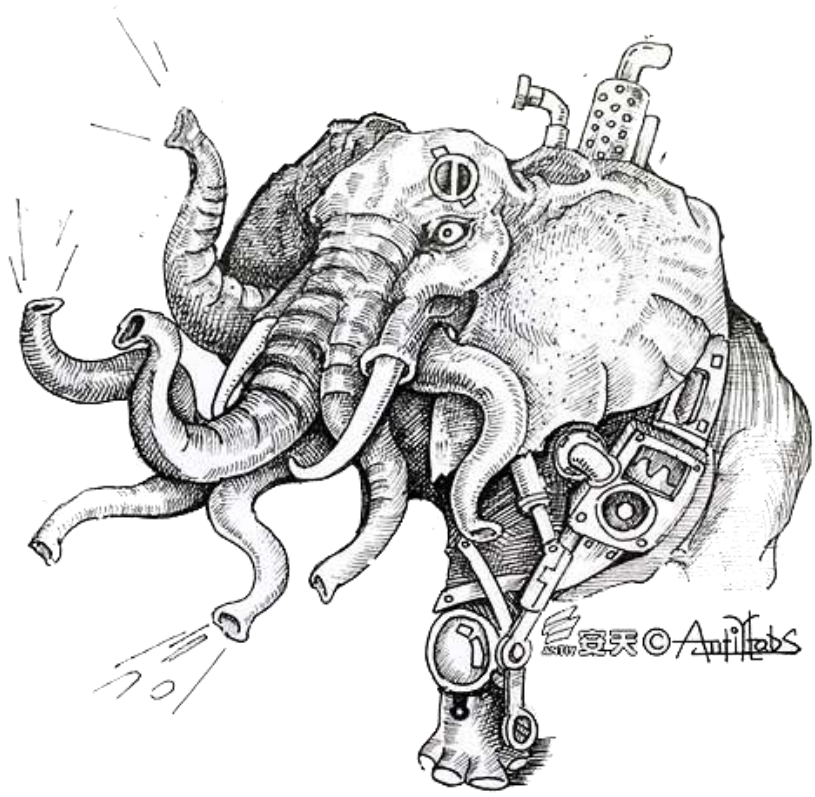
Analysis of the Recent Cyber Attack Activities of the White Elephant Organization

Antiy CERT

The original report is in Chinese, and this version is an AI-translated edition.



Draft Completion Date: September 16, 2022

Initial Release Date: October 24, 2022

Last Updated: October 27, 2022

Scan the QR code to get the latest version of the report.

Contents

1 Overview

In late September 2022, Antiy CERT detected a series of cyberattacks carried out by the White Elephant organization. The attackers deployed decoy documents by attaching malicious links. The documents were primarily targeted at research institutes and contained exploits for the CVE-2017-11882 vulnerability. Triggering the vulnerability released the White Elephant organization's proprietary BADNEWS remote control Trojan. Organize the characteristics of relevant activities as shown in Table 1-1Table 1-1 Attack activity characteristicsCode command 4 collects the document with the suffix name shown in Figure 2-16.

Figure 1-1Collect suffix code

1.1.1 Countermeasures Analysis

Digital Signature

The attacker's Trojan mcods.exe is released in the directory "C:\ProgramData\Microsoft\DeviceSync\mcods.exe". The digital certificate of the Trojan horse is "5Y TECHNOLOGY LIMITED", issued by Sectigo Limited, valid from 8:00:00 on March 31, 2022 to 7:59:59 on March 16 , 2023.

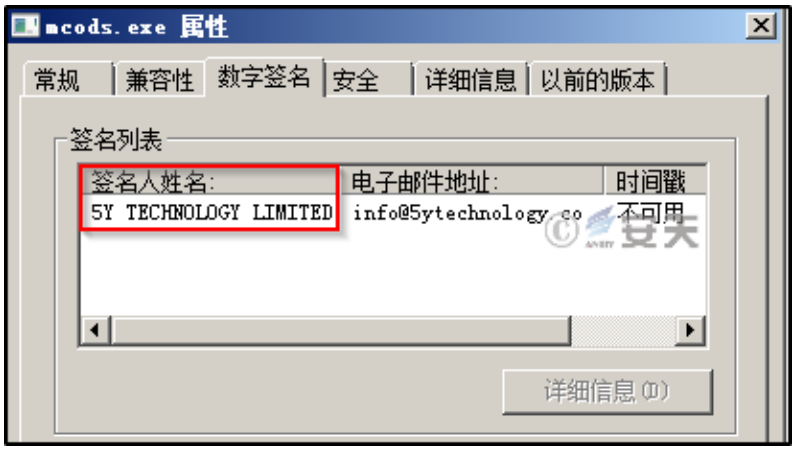


Figure 1-2Digital signature

1. **Encrypted Traffic Data**

The attackers used a custom algorithm to encrypt traffic. The algorithm is AES-CBC-128+Base 64+fixed position embedded "=" and "&" characters. The AES algorithm key is hardcoded: 37FF8272C0EEBC0AE1D90382847618DD

```
v79 = xmmword_435850;                   // 密钥：DD1876848203D9E10ABCEEC07282FF37
strlen(lpMultiByteStr);
kk_cryptFunc(&v67, &v79);               // 加密流量，密钥：DD1876848203D9E10ABCEEC07282FF37
LocalAlloc(0x40u, 0x19000u);
```

Figure 1-3Traffic encryption algorithm call

```
if ( a3 )
  *a3 = 0;
v4 = (a1 & 0xFFFFFFF0) + 16;
v8 = rand() % 15 + 1;
result = (__m128i *)malloc(v4 + v8);
v6 = result;
if ( result )
{
  memset(result, v4 - a1, v4);
  if ( a1 )
    memmove(v6, a2, a1);
  kk_aes_cbc_128(v10, key);
  v11 = 0i64;
  kk_aes_encrypt(&v11, v6, v6, v4);
  kk_srand((int)v6->m128i_i32 + v4, v8);
  if ( a3 )
    *a3 = v4 + v8;
  return v6;
```

Figure 1-4Implementation of traffic encryption algorithm

The Trojan's traffic can be decrypted through reverse algorithms to obtain the stolen victim's host basic information.

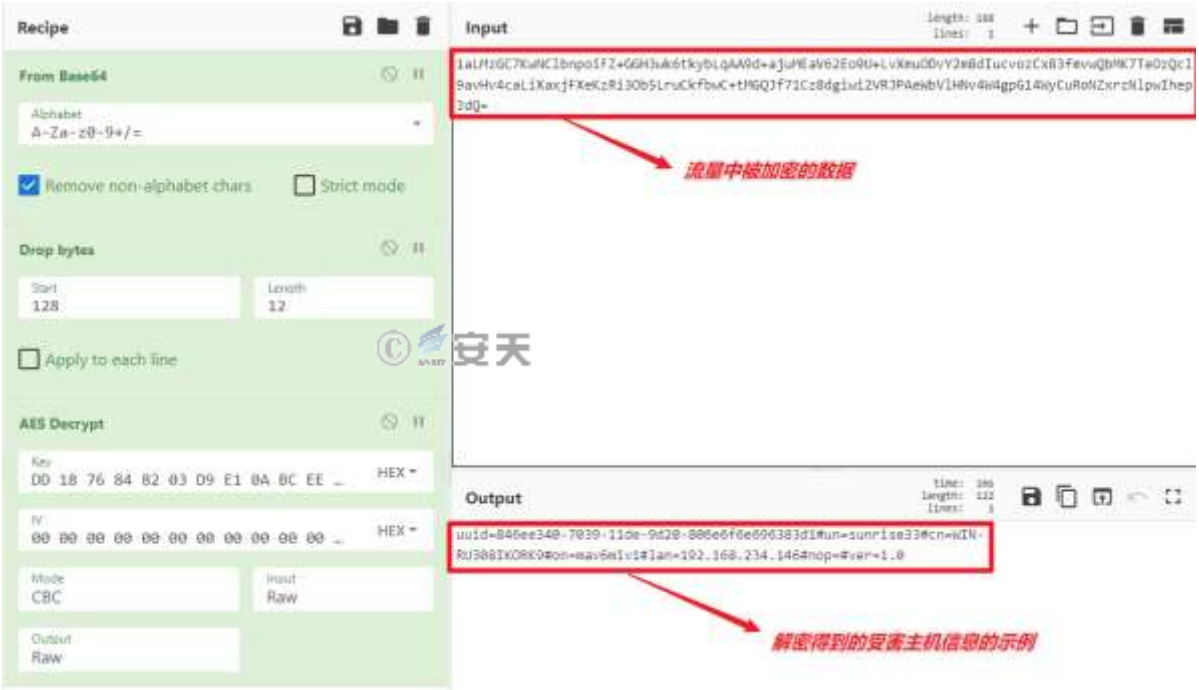


Figure 1-5Decrypted victim host information in traffic

2 Association Traceability

2.1 Trojan Homology

mcods.exe released this time is from the BADNEWS remote control family that White Elephant has used before. The remote control commands and functions of this Trojan horse are exactly the same as those described in the BADNEWS remote control analysis report[0]released by Paloalto Networks in 2018.

Command	Description
0	Kill BADNEWS.
4	Upload edg499.dat, which includes the list of interesting files. Spawn a new instance of BADNEWS after.
5	Upload the file specified by the C2.
8	Upload the TPX498.dat file, which contains the list of collected keystrokes.
13	Copy file to adbFle.tmp, and upload it to the C2.
23	Take screenshot, temporarily store it as TPX499.dat, and upload it to the C2.
33	Download specified file to %TEMP%\up and execute it in a new process

Figure 2-1 Description of BADNEWS remote control capabilities in the Paloalto Networks report

Other details such as the C2 return path and PHP name, encryption key, host basic information and combination format are highly consistent.

2.2 Digital Certificate Homology

The digital certificate used by this Trojan has also been used in other attacks by the White Elephant organization:

Table 3-1 Digital certificate of the mcods.exe Trojan

User	5Y TECHNOLOGY LIMITED
Fingerprint	0b26d02a94f4c8e14222a966b005bb7d30b45786
Valid from	March 31 , 2022 , 8:00:00 AM
Validity expires	March 16 , 2023 , 7:59:59 AM
Serial number	25ba18a267d6d8e08ebc6e2457d58d1e

3 Attack Mapping from a Threat Framework Perspective

This series of attacks involved 14 technical points across all 10 phases of the ATT&CK framework. Specific behavioral descriptions are detailed in Table 4-1.

Table 3-1 Technical behavior description of recent attacks by the White Elephant organization

ATT&CK Phase	Specific behavior	Notes
Reconnaissance	Collect victim identification information	Collect the victim's organization and disguise themselves as the victim's interested identity
Resource development	Acquire infrastructure	Purchase a server and build a fake website and C2 service
Initial access	Phishing	Send links to fake websites to targets via spear phishing emails
Execute	Exploit host software vulnerabilities to execute	Malicious documents exploit CVE -2017-11882 vulnerability
Persistence	Boot or log in with autostart	Shellcode adds the BadNews Trojan to the registry startup items
Defense evasion	Execute signed binary agent	The Trojan file is digitally signed
Discover	Discover files and directories	The Trojan collects document files with the specified suffix on the local machine
	Discover the system's geographic location	When the Trojan runs, it will first determine whether the local time zone is China.
Collect	Collect local system data	The Trojan collects information about the local system, network, files, software, etc.
	Input capture	The Trojan has keystroke logger functionality
	Take a screenshot	The Trojan has a screenshot function
Command and Control	Use application layer protocols	The Trojan communicates using the HTTP protocol
	Use encrypted channels	The Trojan horse will encrypt the data using a custom encryption algorithm before sending the communication package
Data exfiltration	Use C2 channel for backhaul	The stolen data is sent back to the C2 server

Map the threat behavior technical points involved to the ATT&CK framework as shown in Table shown.

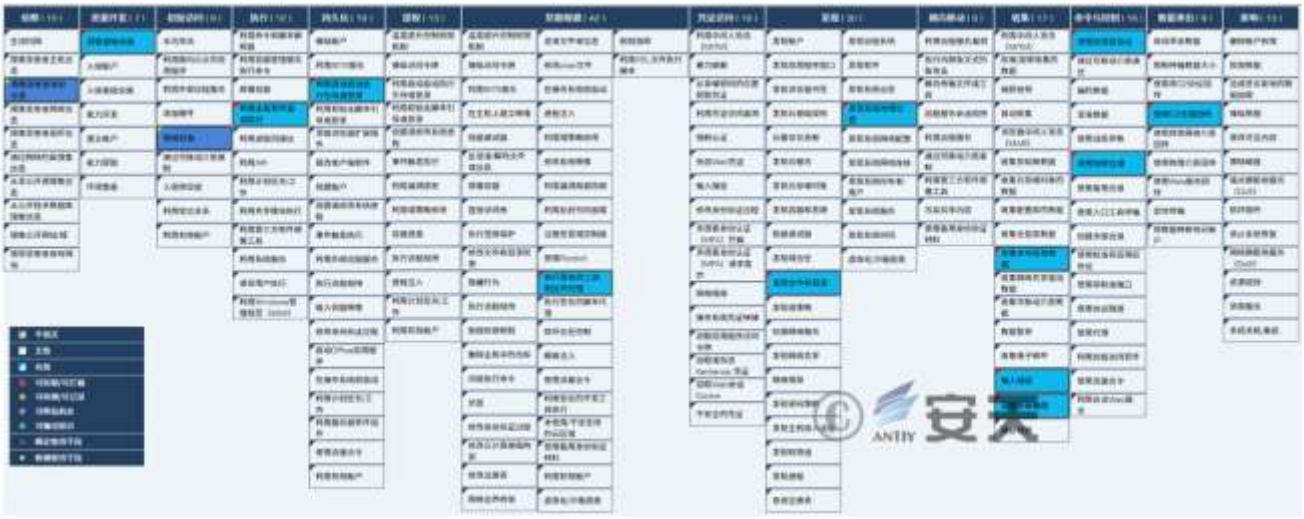


Figure 3-1 ATT&CK mapping of recent White Elephant attack activities

4 Summary

Based on current analysis, Antiy CERT believes this is an attack campaign originating from the White Elephant APT group in India. The attackers are suspected of delivering a specialized remote control Trojan through phishing attacks, and the related attack methods and code are consistent with previous attacks by the White Elephant organization.

Appendix 1: References

Patchwork Continues to Deliver BADNEWS to the Indian Subcontinent

https://unit42.paloaltonetworks.com/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/

Appendix 2: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container

and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis

against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.