Antiy IEP Provides Comprehensive Protection Against the Rampant Trojan AutoCAD

Antiy CERT

Completion time of first draft: 11 July, 2022

Time of first release: 12 July, 2022

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

1 Overview

Recently, Antiy CERT has monitored that the Trojan horse of AutoCAD has been active again, and has carried out infiltration and dissemination for the important enterprises in our country.

Autocad is a kind of commercial computer-aided design (CAD) and drawing software application program. because of its wide application field, the value of the products produced by the software after being applied and designed by the professional is huge, which attracts the attention of the attacker. The attacker uses the special programming language AutoLisp to write the secret Trojan for the software development. This language is a special dialect of Lisp language, which is specially used for the extension of AutoCAD software.

The earliest AutoCAD Trojan horse was discovered in 2008, when it used mailboxes to deliver stolen data. For the June 2022 attack activity, only the initial sample is currently captured and the C2 address is invalidated. From the analysis of the initial samples, the attacker uses AutoLisp to write the Trojan, which realizes the functions of information collection, information return, remote download and execution, and persistence. From the perspective of threat analysis, it is not excluded that the attacker will steal other information in the follow-up process, and drop the ransomware or secret Trojan; from the perspective of information returned, the target system time, area code and AutoCAD version can be transmitted back. It is not excluded that the attackers carry out targeted attacks based on such information.

To sum up the above contents, Antiy CERT thinks that the threat of AutoCAD Trojan is high, and attackers can carry out targeted attacks on individuals and enterprises using AutoCAD software, and can cause security threats with great influence.

It has been proved that the Windows version of the Antiy IEP can effectively check and kill the Trojan and effectively protect the user terminal.

2 Overview of AutoCAD Trojan

2.1 The Attacking Principle of Trojan in AutoCAD

In term of Trojan writing, that Trojan in AutoCAD is written by the program language AutoLisp built in the AutoCAD software, which realizes such functions as information acquisition and return, remote download and execution, and persistent resident system; in term of Trojan sample file type, It mainly involves two kinds of file types, Lsp and Fas, among which Lsp file is a text file, which is a program source file written by AutoLisp. However, that Fas file is a compile file formed by compile the Lsp file by visual Lisp, which is not an executable file under normal circumstances and cannot be run directly, and must be loaded by AutoCAD software; Because of the particularity of Lsp and Fas file, it is necessary to load the execution code in AutoCAD software. The loading and execution of AutoCAD trojan horse mainly utilizes two aspects of AutoCAD software. it can trigger trojan horse execution when opening AutoCAD software, creating new graphic files, closing all graphic files, and so on. One is to use software to load files with specific file names under special directories, such as the files named acad and acaddoc involved in the Support folder under the software installation directory, and the other is to use the specific code of AutoLisp.

2.2 The Spreading Form of AutoCAD Trojan

At present, the propagation form of AutoCAD trojan horse can be divided into two types. In the initial delivery, the attacker embeds the compiled Fas file into the cracked version of AutoCAD software or CAD project file, and delivers it in combination with the software sharing website platform or the phishing email attachment, and spreads the target system. Copy itself to other directories or write malicious code into the default loaded Lsp file of AutoCAD software to realize long-term residence. When the target user creates a new folder of graphical items, it copies itself into that folder, enabling horizontal propagation as the target transfers the entire folder of items.

3 Analysis of Attacking Events of AutoCAD

On April 2, 2008, the AutoCAD Forum published the details of the exploitation of the acad.fas file by malware [1]. [1]

On 20 June 2012, ESET published a report on the ACAD / Medre.A worm [2].[2]

On November 28, 2018, Forcepoint published an unusually active report on AutoCAD Trojans, which revealed that the majority of infected machines came from China, India, Turkey and the United Arab Emirates [3].[3]

In June 2022, the penetration and dissemination of AutoCAD Trojan horse to China's important enterprises suddenly intensified, and dozens of enterprises and units have been attacked [4].[4]

4 ATT&CK Mapping Map of Event

For the technical points involved in the attack event of the attacker dropping the AutoCAD Trojan horse to the target system, ATT&CK map is as follows:

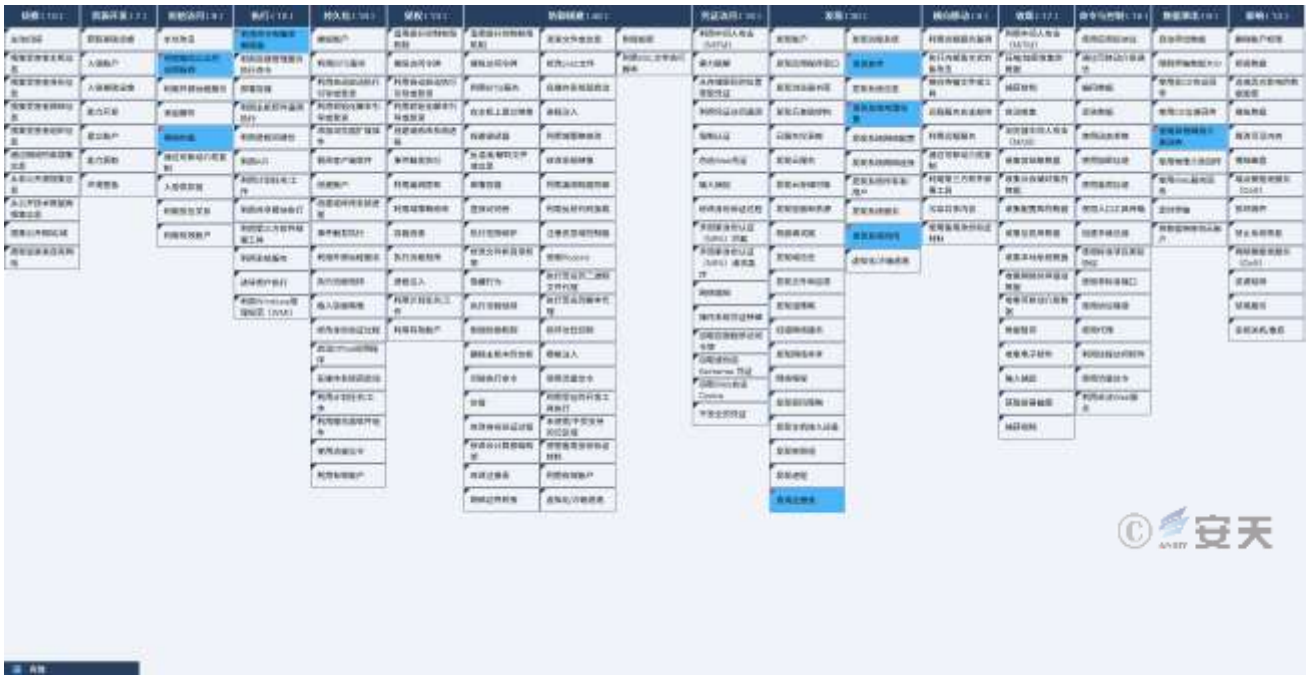

Figure 4-1 ATT & CK mapping map 4-1

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

Table 4-1 Details of Technical Points 4-1

Initial access	Make use of public-facing applications	Embedding Malicious Files into Broken AutoCAD
	Phishing	Deliver AutoCAD design document with CAD stealing drawing trojan horse
Execution	Using command and script interpreters	Using AutoCAD to Load and Execute CAD Graph-stealing Trojan Horse
Findings	Query the registry	View the registry key
	Discovery Software	View AutoCAD software information
	Discover the geographical location of the system	Gets the system zone code
	System discovery time	Gets the current system date
Data seeps out	Use the other network medium to return	Use media not limited to mailboxes to return stolen data

5 Precision protection of Antiy IEP

Aiming at the persistent resident object system, loading malicious files in AutoCAD, registry operation and other behaviors involved in the execution process of AutoCAD Trojan horse, Antiy IEP can realize all-round precise protection. When AutoCAD dynamically loads other files, it is most likely to be used maliciously. when AutoCAD loads suspicious files, Antiy IEP will pop up a window to prompt the user, and the malicious behaviors can be automatically intercepted before they take effect, so as to ensure the environment and data security of the system.

5.1 Full scan detection

Through overall scanning and real-time monitoring, Antiy IEP can effectively check and kill the malicious fas files involved in AutoCAD, and realize the effective protection of terminal security.

Figure 5-1 Overall scan test of wisdom nail 5-1

5.2 Detection of dynamically loaded files

Since the fas file or lsp file can execute the malicious code in the fas file or lsp file only when it is loaded by the corresponding software AutoCAD, through the dynamic loading file detection module, Antiy IEP can intercept the suspicious file loaded by the AutoCAD software in real time, implement security and effective protection of that terminal.

Figure 52: Interception of dynamically loaded suspicious files by Zhijia 5-2

5.3 Detection of Registry Operations

Through the register operation detection module, Antiy IEP can intercept the register operation of AutoCAD Trojan horse in real time, prevent it from storing and returning the system information of C2 in the register, and realize the security and effective protection of the terminal.

Figure 5-3 Suspicious operation of interception of registry by Antiy IEP3

The system also has a unified management center, through which management personnel can realize closed-loop operation of viewing, analyzing, handling and confirming security events in the network, which greatly improves the efficiency of security operation and maintenance.

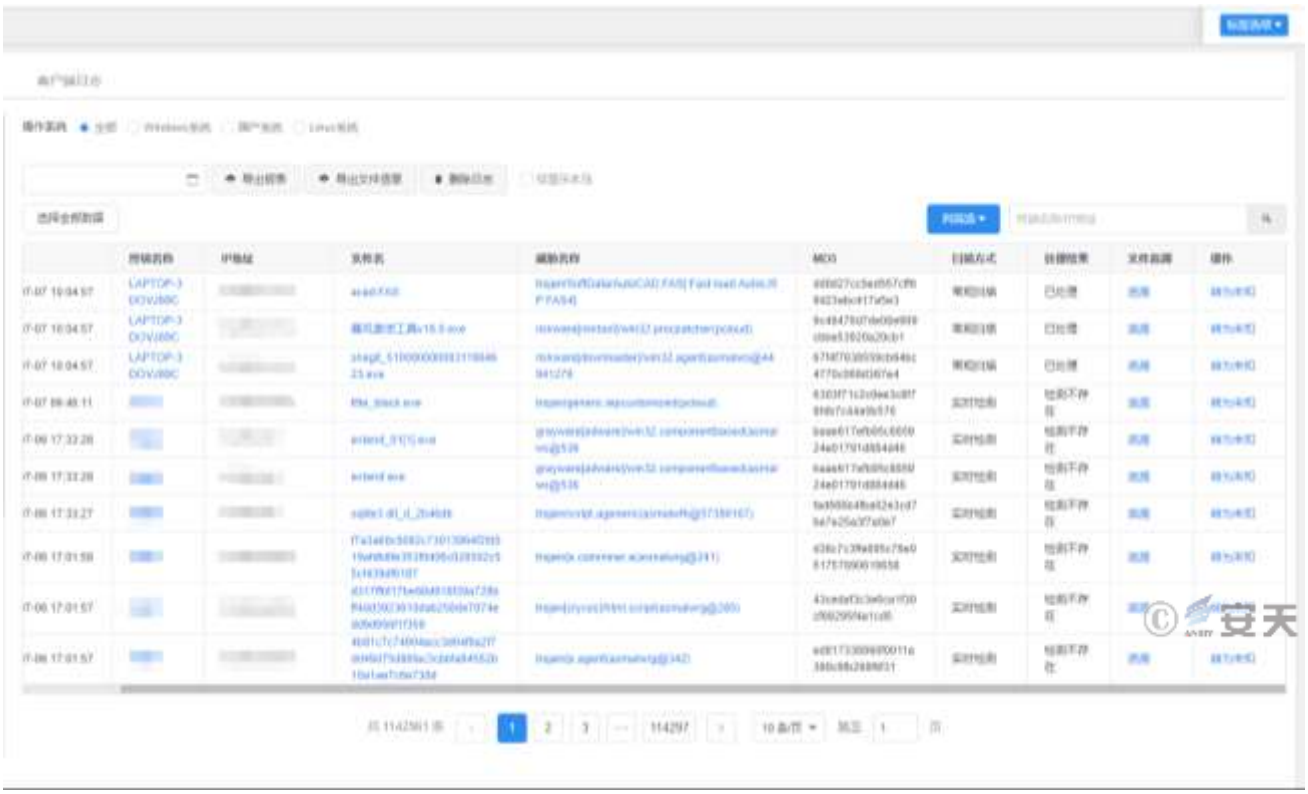

Figure 5-4 Alarm interface of Antiy IEP management center 5-4

Antiy IEP is a terminal security protection product for various government and enterprise units, supporting integrated security protection services for office machines, servers, virtual terminals, mobile devices and other terminals. The products include virus detection and killing, active defense, ransomware protection, host data collection, in-depth security analysis, network control, intrusion protection, threat response, asset management, patch management and configuration reinforcement. Host audit and control, threat visualization and other functions can be integrated to effectively prevent various threats and attacks, and guarantee the security of user business and data.

For security managers, The product provides a flexible and efficient system management center, supports the integrated management of terminal security through the management center, and helps managers to understand the security situation of terminals within the network and view details of security events. And quickly delivers the policy adjustment and handling instruction to the terminal.

6 Sample analysis

After the malicious sample is loaded, it will try to connect with the C2 address, and obtain the slb. fas file after the connection succeeds. Loading files and deleting them; obfuscating them according to the acquired date and GUID and setting the values of dqs and dlr in the registry key; sending data back to C2 involves CAD software version,

time and system area, It is speculated that malicious attackers will carry out targeted theft activities based on the data returned.

6.1 Sample labels

Table 6-1 Fas Sample Label 6-1

Virus name	Trojan / JS.Duxfas
File MD5	Dd0d27cc5ed557cff69d23abc417a5e3
Original name of file	Acad.fas
File size	16.2 KB (16,629 bytes)
File format	Softdata / AutoCAD.FAS [: Fast-load AutoLISP FAS4]
Compile time	2021-09-03
Compiled Language	Autolisp / Visual Lisp
Vt First Upload Time	2022-06-16 02: 04: 44
Vt test result	14 / 56

Table 6-2 Fas Sample Labels 6-2

Virus name	Trojan [Downloader] / Acad.Qfas
File MD5	033216e77f7543ee7a1d44be2889dd21
Original name of file	Acad.fas
File size	10.2 KB (10,464 bytes)
File format	Softdata / AutoCAD.FAS [: Fast-load AutoLISP FAS4]
Compile time	September 3, 2016
Compiled Language	Autolisp / Visual Lisp
Vt First Upload Time	2018-11-30 22: 39: 10
Vt test result	29 / 58

Table 6-3 Lsp Sample Label 6-3

Virus name	Trojan / JS.Duxlsp
File MD5	D0cb6645e97cf8a574e34e3ae5126054
Original name of file	Acad.lsp
File size	2.26 KB (2,312 bytes)

File format	Text / ISO _ IEC.UTF8 [: No bom]
File source code programming language	Autolisp / Visual Lisp
Vt First Upload Time	2022-05-17 12: 15: 46
Vt test result	1 / 57

6.2 Analysis of acad.lsp samples

6.2.1 Connecting C2

Create an XMLHTTP object for subsequent requests for C2 addresses:

Figure 6-1 Creating an XMLHTTP object 6-1

Request the C2 address and save the response as a slb.fas file (a partial sample saves the response as tf.fas):

Figure 6-2 Connecting C2 and taking subsequent loads 6-2

6.2.2 Return message

Access C2 through GET and submit relevant data, including CAD software version, time and system area. it is speculated that the attacker may return corresponding data for the submitted data, and then carry out targeted theft activities.

Figure 6-3 Submission of relevant data when requesting C2 6-3

6.2.3 Load the downloaded file

Load the slb. fas file, and then delete it.

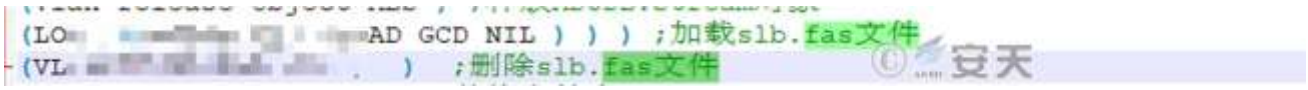

Figure 6-4 Delete after loading 6-4

6.2.4 Persistent residencies

By copying itself and modifying the variables of the AutoCAD software system, the long-term residence of the target system is realized.

Figure 6-5 Copy itself and Modify AutoCAD Software System Variables 6-5

6.3 Dynamic analysis of acad.fas samples

After the sample is loaded, request the domain name of C2: Y.szmr.org, submit the obtained information through GET, and the C2 server returns the encrypted data. This process only returns data at the first request, and according to the dynamic monitoring results, the subsequent C2 connection fails, and the next load function analysis cannot be performed.

Figure 6-6 requests C2 and returns data 6-6

Subsequently, the tf.fas file will be created in a directory, and the file will be loaded by the command of AutoCAD, and the file will be presumed to be the result of encrypted data decryption. In addition, several test of loading acad. Fas have found that that encrypt data returned each time is inconsistent, and the created tf.fas file is inconsistent.

Figure 6-7 Loading the newly created fas file 6-7

After the file is loaded, another C2 domain name is requested: Cl.jzvu.info, which is currently invalid and has no sample associated for further analysis.

Figure 6-8 Connection C2 6-8

7 Threat screening

1. Check whether there are files such as "acad.lsp, acad.fas, acaddoc.lsp, acaddoc.fas, acadapp.fas, acadapp.fas, slb.fas, tf.fas" in the system where AutoCAD software is installed, and conduct security detection for corresponding files;
2. Open the window of loading application program by the command of AutoCAD, and scan the file loaded by the terminal protection system.
3. Manually check whether the loaded text files (lsp, mnl, etc.) contain domain names such as "szmr.org, jzvu.info," and delete the corresponding files if any;
4. Host that have been or are establishing communication with "* .szmr.org," "* .jzvu.info," "zxb.isduun.com" are filtered through traffic monitor devices to quickly identify infected machines within a network.

8 Recommendations for protection

1. Install the terminal protection system: Install the anti-virus software, and it is recommended to install the terminal protection system of Antiy IEP;
2. It is recommended to use the genuine AutoCAD software downloaded from the official website. If there is no official website, it is suggested to download from trusted sources;
3. For the AutoCAD project files from email or other abnormal trusted sources, security threat detection shall be conducted immediately after the files are checked and received;
4. Enterprises and public institutions banned domain names: * .szmr.org, * .jzvu.info, zxb.isdun.com.
5. In the process of using AutoCAD, the "Security - Unsigned Executable File" window pops up, and for files that are not self-compiled, all click the "No load" button;

Figure 8-1 Unsigned Executable File Load Prompt 8-1

6. Do not use the administrator's authority to run AutoCAD, and prevent the malicious code from obtaining high-authority execution;

7. Never run an unknown Lsp file without pre-checking the code [5].[5]

9 IoCs

Domain name	Sq.szmr.org Sqer.szmr.org Sl.szmr.org Y.szmr.org Cl.jzvu.info Zq.jzvu.info Cwcl.jzvu.info	Zxb.isdun.com Zl.jzvu.info Qx.jzvu.info Bj.jzvu.info Hs.jzvu.info Cs.jzvu.info Errzy.jzvu.info
Ip	67.229.124.42	67.229.124.46
Hash	9e3ff6c011d8ef185645a3e589809480 163d077a2757d6786796fe4898e40fa8 0fd6ddda97a70ca1125388bf20db1b4f 1467 CDA463858AC68AAB1037B3ED3D69 033216e77f7543ee7a1d44be2889dd21	194474ee50cbbe9f6b3fbe16c87b74 Dd0d27cc5ed557cff69d23abc417a5e3 64bfd144a9e4a3ab3f688bc35107cf19 Ce5c5bbd9f7725e52fad9a4564169116

Appendix I: References

[1] Virus using acad.fas (virus using acad.fas)

https: / / forms.autodesk.com / t5 / autocad-forum / virus-using-acad-fas / td-p / 2220982

[2] Eset Uncoves ACAD / Medre.A Worm: Tens Of Thousands Of AutoCAD Design Files Leaked in Suspended Industrial Espionage (ESET reveals ACAD / Medre. A worm: Tens of thousands of AutoCAD design files leaked

due to industrial espionage)

https: / / www.eset.com / int / about / newsroom / press-releases / announcements / eset-uncoves-acromedrea-worm-tens-of-tides-of-autocad-design-files-leaked-in-suspended-industri /

[3] Autocad Malware-Computer Aided Theft (AutoCAD malware-computer aided theft)

https: / / www.forcepoint.com / blog / x-labs / autocad-malware-computer-aided-theft

[4] On the Urgent Early Warning of Trojan Horse in CAD

https: / / nic.hzu.edu.cn / 2022 / 0606 / c878a227021 / Page.htm

[5] About safety and virus protection

https: / / knowledge.autodesk.com / zh-hans / support / autocad / learn-explore / caas / CloudHelp / cloudhelp / 2019 / CHS / AutoCAD-Core / files / GUID-9C7E997D-28F8-4605-8583-09606610F26D-html

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 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.