2022 Popular Data-Stealing Trojans Review

Antiy CERT

First published: March 16, 2023, 5:15 p.m.

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

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

Contents

1 Overview **1**

2 The Harm of Data-Stealing Trojans **2**

3 The Current Status of the Development of Data-Stealing Trojans **3**

3.1 The Gray Market for Data-Stealing Continues to Grow, And the Cost of Attacks Continues to Decrease 3

3.2 Two-Way Evolution, Specialized Development 3

4 Protective Recommendations **5**

4.1 Endpoint Protection 5

4.2 Website Propagation Protection 5

4.3 Initiate Emergency Response in Time When Attacked 5

5 Popular Data-Stealing Trojans **6**

5.1 Redline 6

5.2 AgentTesla 7

5.3 Formbook 8

5.4 Lokibot 9

5.5 Raccoon 10

5.6 AZORult 11

5.7 Vidar 12

5.8 Pony 13

5.9 Jester 14

6 Summarize **15**

Appendix 1 : References **15**

Appendix 2: About Antiy **16**

1 Overview

Data-stealing Trojans are malicious executors used to steal sensitive data from user systems. Attackers often deploy data-stealing Trojans through phishing, vulnerability exploitation, software bundling, etc., and use the stolen important data to make profits. When a user's system is infected with a data-stealing Trojan, according to the attacker's pre-settings, the data-stealing Trojan will hide, reside, detect, collect, transmit, and monitor in the infected system, thereby transmitting sensitive data according to the attacker's needs, ultimately causing serious consequences such as loss of income and reputation damage to users.

At present, the attackers of data-stealing Trojans have built a complete data-stealing industry chain, including development, analysis, confrontation, sales, attacks and other links, forming a clear internal division of labor system and profit model. Through modular component design, the developers of data-stealing Trojans have produced a series of independent, scalable and easy-to-maintain data-stealing Trojan functional components, and sold these components on the black market at a marked price. Attackers can purchase functional components according to their own intentions to assemble data-stealing Trojans, and then implement completely customized data-stealing attacks, and give feedback to developers based on usage, thereby promoting the iteration and update of data-stealing Trojans.

In this process, data-stealing Trojans have mainly evolved in two directions: one is the "wide-net" data-stealing Trojans that focus on expanding the attack surface, and the other is the "customized" Trojans that focus on high-value targets. Among them, the data-stealing Trojans in the "wide-net" direction mainly rely on various public platforms to launch data-stealing Trojans with certain generality, thereby launching large-scale attacks on ordinary users in order to collect as much user data as possible to make profits; the data-stealing Trojans in the "customized" direction are specially designed for large targets such as government and enterprises, and strengthen their concealment and data collection capabilities in order to steal a large amount of high-value data.

In 2022, Antiy CERT released several analysis reports on data-stealing Trojans. Now, we will sort out the popular data-stealing Trojans in 2022, explain their development status, and summarize effective protection suggestions to help users better perform security protection work.

2 The Harm of Data-Stealing Trojans

In recent years, a large number of APT organizations and attackers have continuously launched cyber attacks against many important industries in China, such as finance, health, public administration, defense, and education. The attack surface covers critical infrastructure, large information systems, and the intranets of enterprises and institutions, causing many cybersecurity incidents that endanger national security and development interests. For example, since October 2021, a hacker group called "AgainstTheWest" (ATW) has attacked platforms such as SonarQube, Gitblit, and Gogs, data-stealing digital assets from many domestic enterprises and institutions, and illegally selling them on overseas hacker forums, resulting in the leakage of a large amount of key source code and data 错误!未找到引用源。, causing huge losses to the relevant units. Once an enterprise is attacked by a data-stealing Trojan, its current business is easily destroyed, such as technology patents being obtained and imitated by competitors, production processes being plagiarized, and customer information being leaked, resulting in loss of customer trust. In addition, attackers may also use the stolen data to blackmail the enterprise, causing more losses.

In addition, there are also many attacks on individual users by launching data-stealing Trojans, such as the "Magic Thief" data-stealing Trojan disguised as common software and widely spread on download websites[2]; black industry organizations use hundreds of fake pirated software download sites to induce users to download and execute data-stealing Trojans[3]. Once the attacker succeeds, the stolen user data is likely to be used by criminals for illegal profit, which in turn exposes the user's legitimate rights and interests to multiple risks, mainly in the following three aspects: First, virtual assets are easily stolen, such as social accounts being used to further spread Trojan payloads, game accounts being robbed, etc. Second, personal property is in danger, such as credit cards may be used by gray industry organizations for money laundering, and account balances may be transferred by criminals. Third, due to the increased risk of fraud, criminals may use users' private information to create scams that are difficult for users to identify, causing users to make wrong decisions.

To avoid the above situation, it is necessary for users to accurately understand the harm of data-stealing Trojans and take effective measures in a timely manner to ensure that data is effectively protected and legally used.

3 The Current Status of the Development of Data-Stealing Trojans

3.1 The Gray Market for Data-Stealing Continues to Grow, And the Cost of Attacks Continues to Decrease

In recent years, attackers have built a relatively complete gray industry chain for data-stealing, formed a relatively standard attack system, achieved internal division of labor, and lowered the threshold for attackers to join through componentized Trojan design, thus expanding rapidly.

At present, the gray industry chain of data-stealing has formed a complete upstream and downstream relationship, with a clear organizational structure and value delivery chain. Its main roles are composed of Trojan writers, analysis and confrontation technology providers, Trojan attackers and data acquirers. One person in the industry chain can play multiple roles, and one role can also be assumed by multiple people. Among them, Trojan writers are responsible for writing data-stealing Trojans; analysis and confrontation technology providers are responsible for providing obfuscation, encryption, anti-detection and other technologies; Trojan attackers purchase data-stealing Trojans to carry out data-stealing attacks; data acquirers purchase stolen data for profit. Among them, Trojan writers and analysis technology providers, as developers of data-stealing Trojans, have specially produced a large number of modular Trojan components, allowing attackers to expand the functions of data-stealing Trojans at low cost and easy to maintain, allowing data-stealing Trojans to integrate multiple malicious functions while having analysis and confrontation capabilities, thereby launching high-level data-stealing attacks.

At present, anonymous networks and cryptocurrencies provide sufficient operating space for the gray industry chain of data-stealing, and attackers continue to join this gray industry chain with sufficient profit support, so it is difficult to ban it in a short period of time. It is expected that the gray industry chain of data-stealing Trojans will continue to grow in the future, making the attack capabilities of data-stealing Trojans stronger, the attack costs lower, and the analysis and confrontation technology more complex. Users need to be highly vigilant and upgrade the protection capabilities of their own data assets in a timely manner to ensure the security of data assets.

3.2 Two-Way Evolution, Specialized Development

There are two main development directions of data-stealing Trojans, namely, "customized" data-stealing Trojans that focus on high-value targets and "wide-net" data-stealing Trojans that focus on expanding the attack surface.

The "customized" data-stealing Trojans mainly target high-value targets, such as governments, enterprises, and organizations. Such targets usually have a large amount of data and the data value is extremely high. Therefore, attackers are often willing to "tailor-make" data-stealing Trojans for specific targets to maximize the success rate of the attack. By adopting a modular Trojan design, attackers can use a variety of data-stealing Trojan components to complete precise operations. For example, in June 2022, after long-term preparation and planning, the Targeted Attack Operations Office (TAO) under the National Security Agency (NSA) of the United States used more than 40 exclusive cyber attack weapons to launch a data-stealing attack on Northwestern Polytechnical University, resulting in a large amount of strategic intelligence leakage[1]. Existing evidence shows that the United States has highly customized the data-stealing Trojans it launched in this attack, realizing the coordinated operation of multiple data-stealing functions. After finding out the necessary information for the attack in advance, it completed the theft of a large amount of sensitive data in a very short time, reflecting the precise attack capability of the "customized" data-stealing Trojan.

The "wide-net" data-stealing Trojans focus on expanding the attack surface and data-stealing from as many ordinary users as possible by using public communication methods. For example, in the Redline data-stealing Trojan in 2022 , the attacker uploaded a large number of hot content such as "cracked videos" and "game plug-ins" on video websites to increase exposure, thereby luring a large number of users to download and execute the Trojan to steal secrets [5]. In order to increase the benefits of a single attack, this type of Trojan steals a very wide range of data, including but not limited to users' work files, personal notes, payment accounts, purchase records, social accounts, medical information, voice information, etc. Ultimately, the stolen data will be sold by the attacker or used for other criminal activities to make a profit, causing huge social harm.

It should be noted that in addition to being used separately, these two types of data-stealing Trojans can also be used in combination by attackers. Attackers can first use the "wide-net" type of data-stealing Trojans to find high-value targets, and then create "customized" data-stealing Trojans to carry out targeted attacks, thereby gaining more benefits.

Although the two types of data-stealing Trojans have their own specialized development directions, the evolution direction of their basic technologies is the same, namely the diversification of penetration methods, the expansion of data-stealing capabilities, and the complexity of analysis and confrontation. The diversification of penetration methods means that attackers will try to discover and exploit more security risks and increase the ways to invade user systems; the expansion of data-stealing capabilities means that Trojan developers will add more functions to Trojans based on the feedback data of attackers while ensuring the data-stealing capabilities, thereby increasing the profits

gained in a single attack; the complexity of analysis and confrontation means that the analysis and confrontation technology providers will develop more effective obfuscation, encryption, anti-killing and other technologies, thereby increasing the success rate of attacks.

4 Protective Recommendations

In order to effectively defend against Trojan attacks and improve security protection, Antiy recommends taking the following protective measures:

4.1 Endpoint Protection

1. Install terminal protection system: install anti-virus software. It is recommended to install Antiy Intelligent Endpoint Protection System (IEP) ;

2. Deploy an intrusion detection system (IDS): Deploy traffic monitoring software or equipment to facilitate the discovery and tracking of malicious code. Antiy Persistent Threat Detection System (PTD) uses network traffic as the detection and analysis object, and can accurately detect a large number of known malicious codes and network attack activities, and effectively discover suspicious network behaviors, assets and various unknown threats;

4.2 Website Propagation Protection

1. It is recommended to use genuine software downloaded from the official website. If there is no official website, it is recommended to download from a trusted source and scan with anti-virus software after downloading.

2. It is recommended to use a sandbox environment to execute suspicious files and execute them only when safety is ensured. Antiy PTA uses a combination of deep static analysis and sandbox dynamic loading and execution to effectively detect, analyze and identify various known and unknown threats.

4.3 Initiate Emergency Response in Time When Attacked

Contact the emergency response team: If you are attacked by a data-stealing Trojan, it is recommended to isolate the attacked system in time and protect the site while waiting for security engineers to check the computer; Antiy 7*24 hours service hotline: 400-840-9234.

5 Popular Data-Stealing Trojans

5.1 Redline

The Redline data-stealing Trojan was first discovered in March 2020. In addition to spreading itself through common phishing emails and software bundling, the Redline data-stealing Trojan also spreads itself through a new method of posting phishing videos on video websites. Attackers upload a large number of videos on hot topics such as cracked software, game plug-ins, and cryptocurrency tutorials on video websites, luring users to download and launch malicious payloads through phishing links in the video descriptions. After users are infected with the Redline data-stealing Trojan, in addition to data-stealing important data from software such as FTP, VPN, instant messaging software, and remote connection tools, the Trojan will also steal users' video website accounts and use the stolen accounts to post phishing videos again, thus forming an attack mode of "posting videos → data-stealing accounts → further spreading with stolen accounts".

5.1.1 Family Overview

Table5-1 Redline basic information overview

Data-stealing Trojan family	**Redline**
Compiled language	C #
First discovered	March 2020
Targeted platform	Windows
Main transmission method	Phishing, account theft
Adversarial analysis methods	File information obfuscation, process injection, sandbox escape
Main data-stealing target	System data, browser, email, FTP , VPN , remote connection tools, instant messaging software
Other malicious features	Bundle and distribute other malware, persistence

5.1.2 Typical Cases

- Attackers use the video platform YouTube to spread the Redline malware [1]

In 2022, attackers posted a large number of phishing videos on YouTube about various hot topics such as pirated software, operation tutorials, cryptocurrency, game cheating, etc., in an attempt to trick victims into downloading and running the Redline data-stealing Trojan. The victims' accounts were also stolen to further spread the phishing videos.

5.2 AgentTesla

The AgentTesla Trojan first appeared in 2014. Its early version was sold publicly as a keylogger. Later, its development team turned to the black market for sale, expanded its data-stealing capabilities, and continuously updated it, making it gradually become one of the most popular data-stealing Trojans [6].

From the analysis of the samples captured so far, it can be seen that in addition to the usual data-stealing functions, the malware also has multiple functions such as keylogging, screenshots, persistence, etc., and can disable some system functions to keep itself hidden.

According to Antiy's analysis results, the AgentTesla samples captured in 2022 have been upgraded in terms of anti-detection, anti-debugging, anti-sandbox, etc., using multi-layer payloads and multiple encryption methods for analysis and confrontation, and supporting multiple feedback methods such as Tor anonymous network, email, FTP and HTTP.

5.2.1 Family Overview

Table 5-2 AgentTesla basic information overview

Data-stealing Trojan family	**AgentTesla**
Compiled language	.NET
First discovered	2014
Targeted platform	Windows
Main transmission method	Phishing
Mainly analyzes countermeasures	Payload obfuscation, multi-layer payload loading, process injection
Main data-stealing target	System data, browser, email, FTP, VPN, remote connection tools, instant messaging software, database, downloader
Other malicious behavior	Disable system functions and persistence

5.2.2 Typical Cases

- OPERA1ER uses AgentTesla to steal secrets from African financial institutions

As of March 2022, the APT organization OPERA1ER has used data-stealing Trojans including AgentTesla to launch hundreds of attacks on African financial institutions, of which at least 30 were successful. The estimated amount involved has exceeded US$30 million, causing a huge blow to the customer trust of the relevant institutions.

5.3 Formbook

Formbook has been sold as a malware-as-a-service (MaaS) on hacker forums since 2016 and remains active today. [7]In October 2020, Formbook's developers announced that the stealer had been renamed Xloader and had introduced some functional improvements.

The data-stealing Trojan can automatically collect sensitive data from the browser, email client, instant messaging client, and FTP client in the target system, and can perform keylogging and screenshots. At the same time, the Trojan has certain adversarial detection, adversarial analysis, and anti-tracing capabilities, mainly including payload obfuscation, process injection, and sandbox escape. In addition, the data-stealing Trojan also has functions such as updating, sending malware, remote command execution, and persistence.

5.3.1 Family Overview

Table 5-3 Formbook/Xloader basic information overview

Data-stealing Trojan family	**Formbook / Xloader**
Compiled language	C/C++
First discovered	2016
Targeted platform	Phishing
Main transmission method	Windows
Mainly analyzes countermeasures	Payload obfuscation, process injection, sandbox escape
Main data-stealing target	Browser, email, instant messaging software, FTP
Other malicious behavior	Bundling and delivering other malware, remote command execution, and persistence

5.3.2 Typical Cases

- UAC-0041 group uses Formbook to attack Ukrainian government agencies

In March 2022, a cyberattack named "UAC-0041" by the Ukrainian Computer Emergency Response Team (CERT-UA) used "war and financial assistance issues" as the content of the email to deliver a large number of bait documents to Ukrainian government agencies and units. The document carries macro code with download function. Once the victim enables the macro, the macro will download the Formbook data-stealing Trojan from the attacker's server and execute it, allowing the attacker to carry out further cyber attacks.

5.4 Lokibot

The LokiBot data-stealing Trojan has been sold on hacker forums since 2015 and remains active today[8]. Since the server source code of Lokibot was leaked, a large number of derivative versions have emerged, resulting in a large number of variants and a wide range of spread. Attackers often use phishing emails, software bundling, and other methods to deliver the Lokibot data-stealing Trojan. In addition to the usual data-stealing functions, LokiBot can also deploy and execute other malware in the infected system and persist, posing more threats to the victim.

5.4.1 Family Overview

Table 5-4 Lockibot basic information overview

Data-stealing Trojan family	**Lokibot**
Compiled language	C/C++
First discovered	2015
Targeted platform	Windows
Main transmission method	Phishing, file bundling
Mainly analyzes countermeasures	Reflection mechanism loading, file permission modification, payload obfuscation, process injection
Main data-stealing target	System data, browsers, password managers, remote administration tools, email, electronic notes
Other malicious behavior	Remote code execution, bundling and distribution of other malware, persistence

5.4.2 Typical Cases

- Attackers targeted multiple Korean institutions with the Lockibot Trojan [8]

In April 2022, Antiy CERT detected a data-stealing attack targeting multiple institutions, including the Korean Scholarship Foundation and heavy industry enterprises. The attacker used phishing emails to deliver malicious

payloads, with the subject being "Request for quotation for basic industry", in order to induce victims to decompress and execute the LokiBot data-stealing Trojan in the compressed package, resulting in the leakage of user privacy and data.

5.5 Raccoon

Raccoon has been sold in the "Malware as a Service (MaaS) " model on underground forums since early 2019. In early July 2022, the developer of the stealer released an upgraded version, Raccoon Stealer v2, written in C language, which integrates a variety of data-stealing functions and analysis and confrontation technologies. In addition to common data-stealing functions such as data-stealing passwords and sensitive files, the stealer can also steal cryptocurrencies.

What is different is that some samples of this data-stealing Trojan do not adopt a persistence strategy, but will directly delete themselves after data-stealing. It is speculated that this is determined by the customization options in the Trojan configuration.

5.5.1 Family Overview

Table 5-5Raccoon basic information overview

Data-stealing Trojan family	Raccoon
Compiled language	C/C++
First discovered	2019
Targeted platform	Windows
Main transmission method	Phishing, file bundling
Mainly analyzes countermeasures	Self-deletion, byte padding, payload obfuscation
Main data-stealing target	System data, browsers, password managers, remote administration tools, email, electronic notes
Other malicious behavior	Data-stealing cryptocurrency

5.5.2 Typical Cases

- Attackers build a large number of phishing websites and use SEO pollution to release the Raccoon data-stealing Trojan

In July 2022, attackers generated a large number of phishing websites related to cracking software and optimized SEO to make these phishing websites appear at the front of Google search results. After uninformed users download and launch the so-called "cracking program" (actually the Raccoon Stealer v2 data-stealing Trojan), the data-stealing Trojan will steal the user's browser account password, payment information, cryptocurrency, etc. At present, a large number of users' data have been leaked.

5.6 AZORult

The AZORult data-stealing Trojan was first discovered in July 2016 and was once one of the best-selling Trojan viruses on Russian hacker forums. Although the main seller of AZORult publicly announced at the end of 2018 that it would permanently stop selling this Trojan virus, due to the previous source code leak, AZORult is still widely used and has multiple variants. For example, Gazorp can directly generate the AZORult data-stealing Trojan payload, and Hermes ransomware uses the AZORult data-stealing Trojan as a downloader to spread itself. In addition to the usual data-stealing function, the data-stealing Trojan can also disable Windows security functions and bundle and distribute other malicious codes as a downloader.

5.6.1 Family Overview

Table 5-6 AZORult basic information overview

Data-stealing Trojan family	AZORult
Compiled language	C/C++ , Delphi
First discovered	July 2016
Targeted platform	Windows
Main transmission method	Phishing, file bundling
Mainly analyzes countermeasures	Payload obfuscation and encrypted traffic transmission
Main data-stealing target	System data, browsers, password managers, remote administration tools, emails, electronic notes, source code
Other malicious behavior	Distribute other malicious programs, disable Windows security features, and remotely control

5.6.2 Typical Cases

- Attackers use AZORult to launch phishing email attacks on German car companies

In May 2022, a report by Check Point, a foreign security company, mentioned that attackers disguised themselves as car dealers to send phishing emails to car manufacturers, with malicious payloads disguised as car invoices attached to the emails. After the malicious payload is executed, it will download the AZORult data-stealing Trojan from the hosting server to steal data.

5.7 Vidar

The Vidar data-stealing Trojan was first discovered in December 2018. The developer mainly sells it through hacker forums and anonymous communication software, with prices ranging from $130 to $750. Because Vidar has a strong homology with the existing data-stealing Trojan Arkei, the core codes of the two are basically the same, such as the overall structure and communication protocol. It is speculated that Vidar is an updated version or branch version of Arkei. Currently, both Vidar and Arkei are kept updated.

5.7.1 Family Overview

Table 5-7 Vidar basic information 8

Data-stealing Trojan family	**Vidar**
Compiled language	C/C++
First discovered	December 2018
Targeted platform	Windows
Main transmission method	Phishing, software bundling
Mainly analyzes countermeasures	Payload obfuscation and sandbox avoidance
Main data-stealing target	System data, FTP, browser, mail client, source code, instant messaging, electronic notes, remote control client
Other malicious behavior	Data-stealing cryptocurrency, persistence

5.7.2 Typical Cases

- Attackers used a flaw in Google's advertising process to deliver the Vidar

In December 2022, attackers used Google's advertising service to deliver the Vidar data-stealing Trojan. The attackers directed the ads to their phishing websites by misspelling them and redirecting them to specific services. Unsuspecting users would directly visit the phishing websites through the ads, thus having their secrets stolen.

- Attackers use media or social platforms as C&C servers to transmit Vidar data-stealing Trojan control information

In January 2023, the Vidar data-stealing Trojan used well-known media platforms such as Tiktok, Telegram, Steam, etc. to transmit C&C server information. Its method was to create a large number of one-time accounts and put the content to be transmitted in the unique information columns such as the account's profile and personal signature for the payload to access and read.

5.8 Pony

The Pony data-stealing Trojan, also known as Fareit or Siplog, was first discovered in 2011. It is one of the long-standing Trojan families that is mainly active in Europe and the United States. Therefore, it is rarely introduced on the Chinese Internet [9].

This data-stealing Trojan has many functions, covering more than 110 applications, and can disable Windows security features, steal cryptocurrencies, act as a downloader to drop other malicious payloads and persist.

In addition, Pony uses a large number of analysis and confrontation technologies, such as anti-debugging, multi-layer payload nesting, payload obfuscation, etc., and has a relatively strong detection bypass capability.

5.8.1 Family Overview

Table 5-9

Data-stealing Trojan family	**Pony / Fareit / Siplog**
Compiled language	.NET、ASM
First discovered	2011
Targeted platform	Windows
Main transmission method	Phishing, software bundling
Mainly analyzes countermeasures	Anti-debugging, multi-layer payload nesting, payload obfuscation
Main data-stealing target	System data, FTP , browser, mail client, source code, instant messaging
Other malicious behavior	Disable security software, steal cryptocurrency, send other malicious programs, persistence

5.8.2 Typical Cases

- Conti ransomware group exposed to use Pony to carry out large-scale theft attacks

In March 2022, a Ukrainian security researcher released a large amount of internal information of the Conti ransomware organization , including internal chat records, the organization's training materials, and internal source code. It shows that the Conti ransomware organization used Pony to steal a large number of credentials of email service providers including gmail.com, mail.ru, yahoo.com, etc. for cyber attack activities.

5.9 Jester

The Jester data-stealing Trojan family has a shorter existence than other data-stealing Trojans. Its developers have been selling the Jester data-stealing Trojan since July 20, 2021, and subsequently developed and sold clipboard hijackers, mining Trojans, botnets and other tools.

The Jester has a variety of basic data-stealing functions and obfuscation techniques, and attackers mainly spread it through phishing. In addition to data-stealing common sensitive content such as communication records, FTP, and browser data, the Jester also bundles a clipboard hijacker to hijack the clipboard and change the encrypted wallet address in the infected system to the attacker's encrypted wallet address to steal cryptocurrency.

After analysis, it was found that the Lilith botnet captured by Antiy in 2022 and the Jester data-stealing Trojan were developed by the same group [10][11]. Currently, the group remains highly active and Antiy will continue to pay attention to its subsequent activities.

5.9.1 Family Overview

Table 5-10Overview of basic information of Jester data-stealing Trojan

Data-stealing Trojan family	Jester
Compiled language	.NET
First discovered	2021
Targeted platform	Windows
Main transmission method	Phishing, software bundling
Mainly analyzes countermeasures	Sandbox escape, payload obfuscation, multi-layer payload nesting
Main data-stealing target	System data, FTP , browser, email client, instant messaging
Other malicious behavior	Data-stealing cryptocurrency

5.9.2 Typical Cases

- CERT-UA warns of malicious spam spreading Jester data-stealing Trojan

In May 2022, the Ukrainian Computer Emergency Response Team (CERT-UA) detected a malicious spam campaign aimed at spreading a data stealer called Jester. According to the investigation, the malicious email discovered by the Ukrainian CERT was titled "Chemical Attack" and contained a Microsoft Excel file with a malicious link.

6 Summarize

By tracking the common attack process of data-stealing Trojans, we found that attackers currently use phishing emails, phishing websites, public websites and other means to invade the victim's host. After the invasion is successful, they collect important data of the target system (including but not limited to password credentials, privacy information, important files, digital assets, etc.) and send it back to the attacker, causing serious consequences such as privacy leakage and economic losses to users.

Antiy CERT will continue to pay attention to the relevant technical changes and characteristics of data-stealing Trojans, share the latest analysis results and propose solutions in a timely manner. Antiy Intelligent Endpoint Protection System (IEP) not only has the functions of virus detection and active defense, but also provides terminal control and network control capabilities, which can effectively defend against such threat attacks and ensure the security of user data.

Appendix 1: References

[1]. Data Breach Incident Concerning China by ATW Organization and Response Considerations
https://www.antiy.cn/research/notice&report/research_report/20230219.html

[2]. Risk Warning About the Large-Scale Spread of the "Magic Thief" Data-Stealing Trojan
https://www.antiy.cn/research/notice&report/research_report/20220913.html

[3]. Analysis of Stealer Samples Used to Spread Counterfeit and Pirated Software
https://www.antiy.cn/research/notice&report/research_report/20210628.html

[4]. Investigation Report on the Cyber Attack on Northwestern Polytechnical University by the US NSA
https://www.cverc.org.cn/head/zhaiyao/news20220927-NPU2.htm

[5]. Analysis of the RedLine Data-Stealing Trojan Spread via Video Websites
https://www.antiy.cn/research/notice&report/research_report/20221115.html

[6]. Analysis of a New Variant of the Commercial Data-Stealing Trojan AgentTesla
https://www.antiy.cn/research/notice&report/research_report/20210812.html

[7]. Analysis Report on a Unit That Was Attacked by the FormBook Data-Stealing Trojan
https://www.antiy.cn/research/notice&report/research_report/20211021.html

[8]. Analysisof Espionage Attack Targeting Multiple Korean Institutions
https://www.antiy.cn/research/notice&report/research_report/20220415.html

[9]. Crazy Secret Thief——TEPFER
https://www.antiy.com/response/tepfer.html

[10]. Analysis of the Active Jester Stealer Trojan and the Hacker Group Behind It
https://www.antiy.cn/research/notice&report/research_report/20220510.html

[11]. Follow-up Analysis of Lilith Botnet and the Jester Hacker Group Behind It
https://www.antiy.cn/research/notice&report/research_report/20220902.html

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.