

# Analysis of the RecordBreaker Data-Stealing Trojan Spread via Video Websites

Antiy CERT

First published: June 8, 2023

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

## 1 Attack Campaign Overview

Recently, Antiy CERT detected an attack campaign spreading through video websites. The attackers stole the accounts of video creators with over 100,000 subscribers, posted demonstration videos related to cracked versions of popular software, and tricked victims into downloading the RecordBreaker data-stealing Trojan.

RecordBreaker is the 2.0 version of Raccoon. It receives configuration information from the C2 server, steals sensitive information according to the content of the configuration information, and downloads the payload file according to the URL, and finally delivers Laplas. The Clipper Trojan and a mining Trojan. Because the payload downloaded by the mining Trojan terminates a large number of game processes, Antiy CERT named it the StopGames mining Trojan.

**Spreading data-stealing Trojans through video websites, pirated software download sites, and then using them to deliver other malicious payloads** has become a common attack method. Antiy CERT has introduced this attack method in "Follow-Up Analysis of the Redline Data-Stealing Trojan Spread via Video Websites" 错误!未找到引用源。 and "Analysis of Data-Stealing Samples Spread by Counterfeit Pirated Software" 错误!未找到引用源。. In this attack, the attackers specifically stole the accounts of video creators with more than **100,000 subscribers and published edited demonstration videos** in an attempt to quickly expand the scope of dissemination and increase the success rate of the attack.

Table 1-1 Attack campaign overview

Attack campaign overview	Explanation
Main transmission methods	Video websites, phishing websites

Malicious payload hosting method	Public service platforms such as MediaFire, GitHub, Amazon S3, and Pastebin
Targeted system	Windows operating system
Active time	Active from the end of May 2023
Main features	<p>Steal the accounts of video creators with a certain number of subscribers;</p> <p>Release demonstration videos related to cracked versions of popular software;</p> <p>Set up phishing websites disguised as download sites for cracked versions of popular software;</p> <p>Fill the end of the malicious program with a large amount of junk bytes;</p> <p>Use popular commercial data-stealing Trojans to deliver mining Trojans</p>

It has been proven that Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill malware such as data-stealing Trojans and mining Trojans.

## 2 Technical Review

### 2.1 Mode of Transmission

#### 2.1.1 Publish Video

Attackers steal verified accounts of video creators with a certain number of subscribers to quickly expand the scope of dissemination.

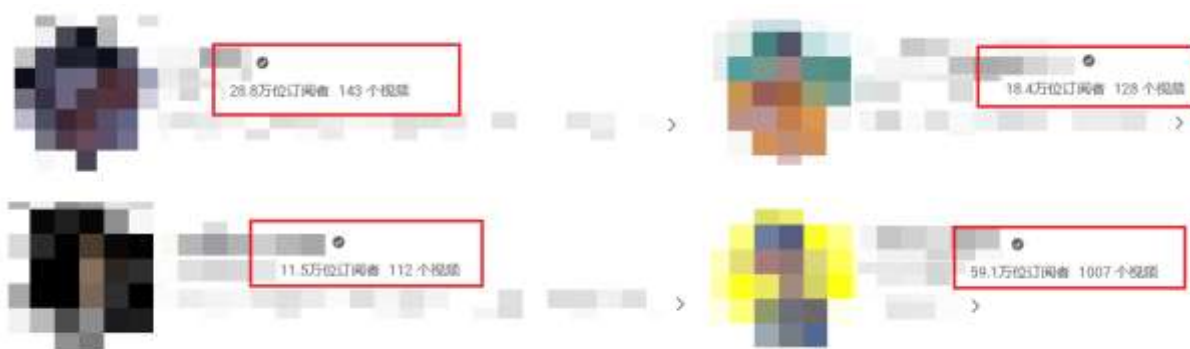


Figure 2-1 2stolen video creator accounts

The attacker used a stolen YouTube account to continuously publish several videos containing cracked versions of popular software.



Figure 2-3 Video released by the attacker

### 2.1.2 Demo Video

The attackers deliberately recorded a demonstration video and used editing methods to splice the normal installation process of the application software into the process after double-clicking the LauncherPC.exe program, making the entire installation process appear to be normal, thereby luring users to double-click to execute the program.

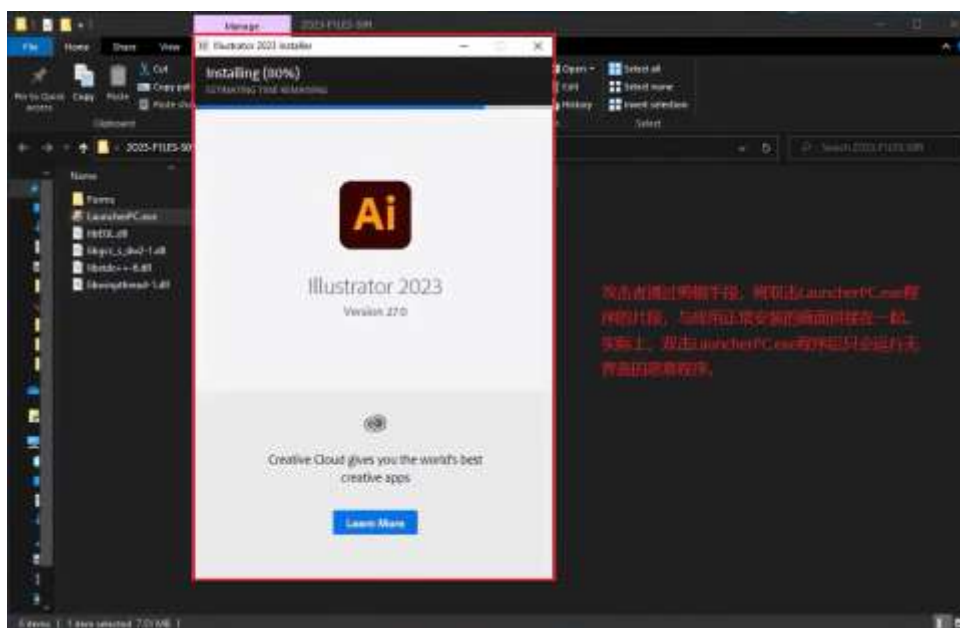


Figure 2-4 Demonstration video

The video description contains a download link for the cracked software resource and includes tags. Users entering keywords from the tags into search engines or video websites will be able to search for related videos. In the description, the attackers advise users to disable their computer security products and emphasize that the resource files are non-malicious.



Figure 2-5 Introduction to the video released by the attacker

### 2.1.3 Download Link

The attackers hosted the files on file hosting platforms such as MediaFire, which would eventually redirect them to the same download address.

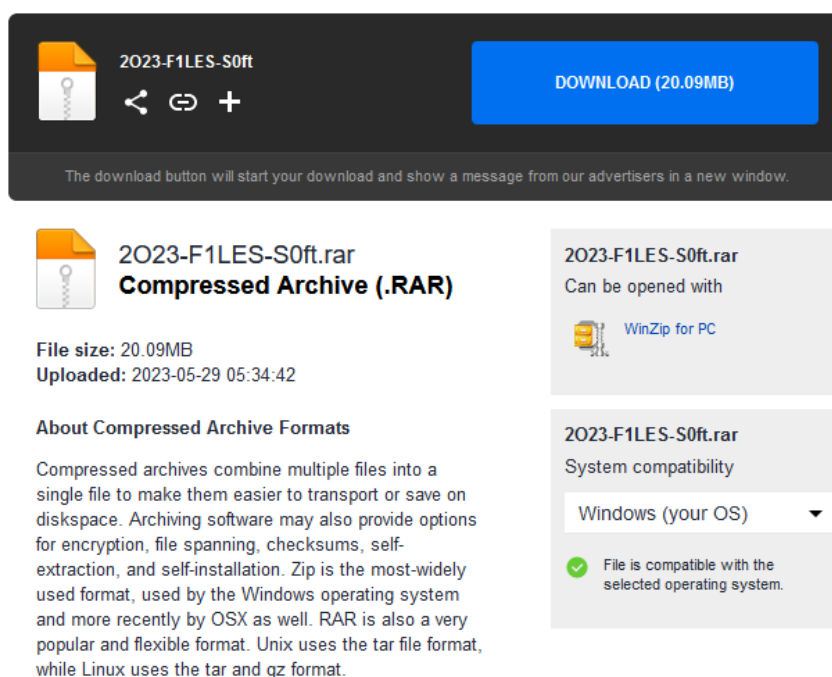


Figure 2-6 Files hosted in MediaFire

The attackers set up multiple phishing download sites, all of which were related to popular software cracking programs.

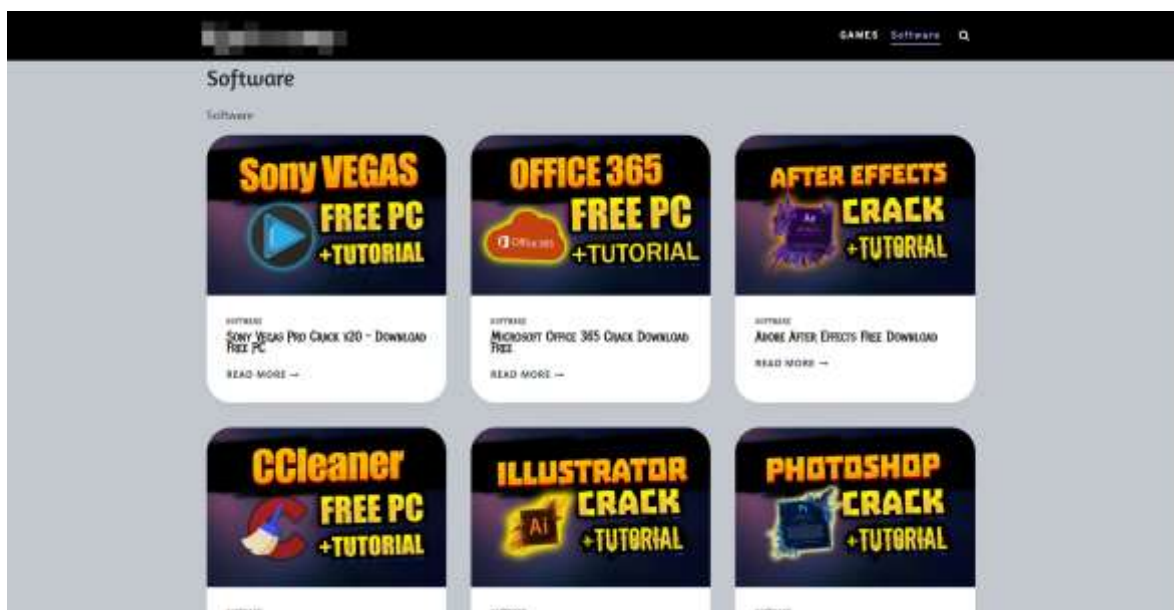


Figure 2-7Download Station

The download site seems to have released a variety of cracking programs, but the final download address of the same download site is the same. The attacker hosted the compressed package file on GitHub, Amazon S3 and others can be used in platforms for storing files.



Figure 2-8Final download address

## 2.2 Spread Malicious Programs

In this attack, the attacker used popular commercial data-stealing Trojans such as RecordBreaker, which have the function of downloading and executing other payloads, to steal sensitive information from the victim host and deliver Laplas The following figure shows the flow chart of this attack activity.

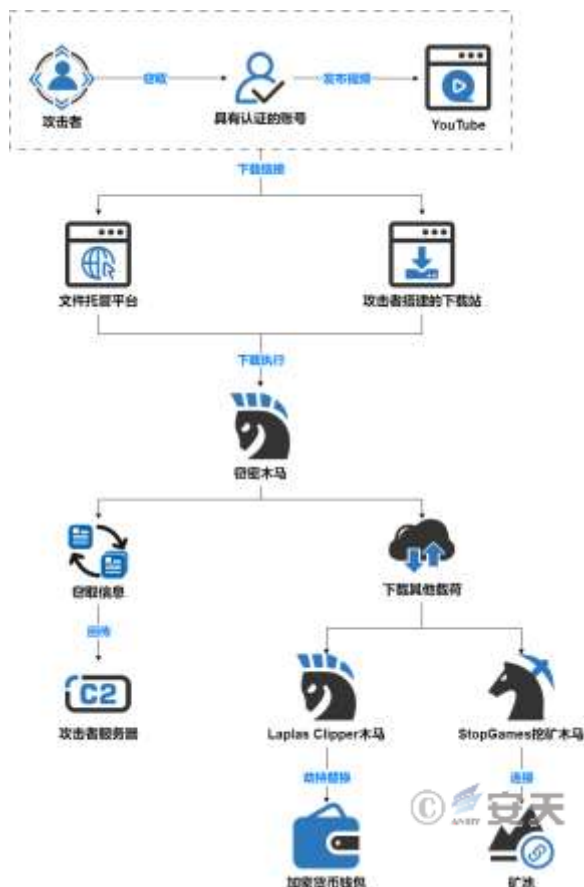


Figure 2-9 Attack flowchart

### 3 Sample Analysis

Attackers add a large amount of junk bytes to the end of the malicious program, expanding the file size to around 1 GB. This is to confuse users into thinking that the program contains application software components and cracking programs, and to prevent users from uploading the program to multi-engine scanning platforms or online sandboxes for detection.

偏移	十六进制	符号
00a8:1400	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1410	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1420	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1430	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1440	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1450	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1460	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1470	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1480	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1490	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:14a0	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:14b0	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:14c0	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:14d0	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:14e0	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:14f0	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1500	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000
00a8:1510	30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30	00000000000000000000

Figure 3-12

### 3.1 RecordBreaker Data-Stealing Trojan

This malicious program belongs to the RecordBreaker family of data-stealing Trojans and is version 2.0 of the popular Raccoon family. Upon execution, it receives configuration information from a C2 server, steals data from the target browser, and executes functions based on identifiers in the configuration information.



Figure 3-3Identifiers

The RecordBreaker data-stealing trojan are shown in the following table.

Table 3-1 Identifiers and functions

Identifier	Function
libs_	Download the required dynamic library files
ews_	Steal data from designated browser extensions
wlts_	Steal secrets from a designated crypto wallet
sstmnfo_	Collect system information and installed application information



scrnsht_	Screenshot
tlgrm_	Steal information from Telegram
grbr_	Steal information from specified file
dscrd_	Steal information from discord
ldr_	Download and execute other payloads

Attackers used the RecordBreaker data-stealing trojan to obtain payload files from the created GitHub projects.

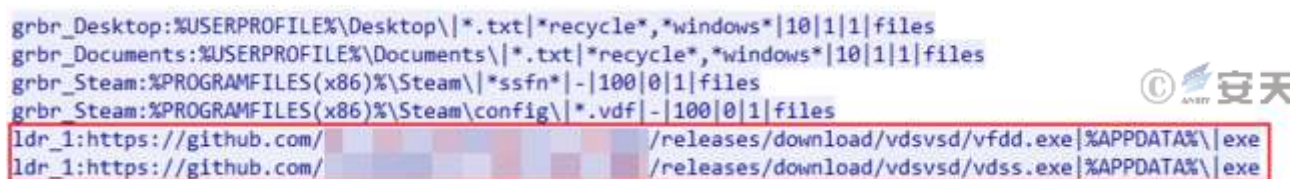


Figure 3-4Download and execute other payloads

Among them, vdss.exe is Laplas Clipper Trojan. fvfd.exe is a mining Trojan used for subsequent mining activities.



Figure 3-5 Malicious payloads in GitHub

## 3.2 Laplas Clipper Trojan

The vdss.exe program is also filled with a lot of garbage bytes to 1.18 GB. This program belongs to Laplas Clipper Trojan family. Because cryptocurrency addresses are long and difficult to remember, many users are accustomed to copying and pasting addresses when using them. The Clipper Trojan exploits this by monitoring the clipboard contents of the victim host, matching the wallet address based on a regular expression, and replacing the address with the attacker's wallet address to steal cryptocurrency.



```
^(?:([1-9A-HJ-NP-Za-km-z]{32,33})|(3[1-9A-HJ-NP-Za-km-z]{32,33})|(bc1q
[023456789acdefghjklmnpqrstuvwxy]{38,58})|(q[a-z0-9]{41})|(p[a-z0-9]{41})|(L
[a-km-zA-HJ-NP-Z0-9]{33})|(M[a-km-zA-HJ-NP-Z0-9]{33})|(1tc1q[a-zA-Z0-9]{38})|(0x
[a-fA-F0-9]{40})|(bnb1[0-9a-z]{38})|(D[5-9A-HJ-NP-U]{1}[1-9A-HJ-NP-Za-km-z]{32})|
(4[0-9AB][1-9A-HJ-NP-Za-km-z]{93})|(8[0-9AB][1-9A-HJ-NP-Za-km-z]{93})|(r
[0-9a-zA-Z]{33})|(t1[a-km-zA-HJ-NP-Z1-9]{33})|(X[1-9A-HJ-NP-Za-km-z]{33})|(ronin:
[a-fA-F0-9]{40})|(T[A-Za-z1-9]{33})|(tz[1-3][1-9A-HJ-NP-Za-km-z]{33})|(admin1
[a-z0-9]{+})|(cosmos1[a-z0-9]{38})|(R[a-zA-Z0-9]{33})|([A-Z2-7]{58})|
([1-9A-HJ-NP-Za-km-z]{44}))$
```

Figure 3-6Regular expressions

The cryptocurrency wallet addresses matched by this regular expression are shown in the following table.

Table 3-2Matching cryptocurrencies

Bitcoin (BTC)	Bitcoin Cash (BCH)	Litecoin (LTC)	Ethereum (ETH)
Dogecoin (DOGE)	Monero (XMR)	Ripple (XRP)	Zcash (ZEC)
Dash (DASH)	Ronin (RON)	Tron (TRX)	Tezos (XTZ)
Cardano (ADA)	Cosmos (ATOM)		

## 3.3 StopGames Mining Trojan

The vfvfd.exe program is the StopGames mining trojan. When running, it injects a malicious payload into the specified process. The malicious payload executes Base 64-encoded commands and adds paths such as % UserProfile % and % SystemDrive % to the Windows The malware then downloads the configuration information hosted by the attacker on Pastebin in the Defender exclusions. The configuration information includes the download address of the mining-related program and the information used by the attacker for mining.



Figure 3-7 Configuration information hosted on Pastebin

The malicious payload downloads programs related to mining hosted by the attacker on GitHub based on the download address in the configuration information. Among them, lolMiner.exe and xmrig.exe are open-source mining programs, while WatchNew.exe is used to monitor the running status of the mining programs to ensure that mining activities continue. The malicious payload adds the WatchNew.exe program to the scheduled tasks to achieve persistence.



Figure 3-8 Mining-related programs hosted on GitHub

The WatchNew.exe program is shown in the figure below.

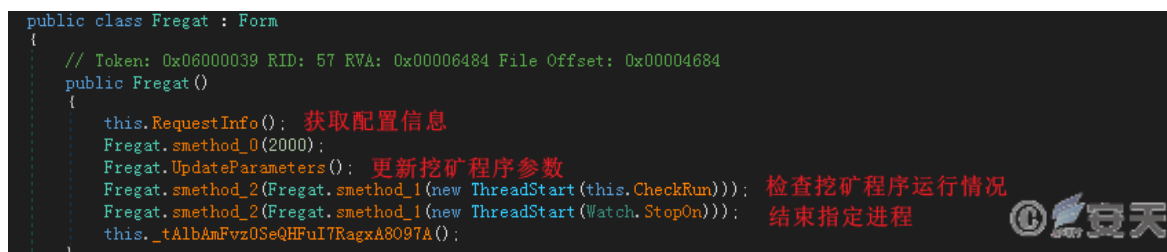


Figure 3-9 WatchNew.exe overall functional structure

The program creates a thread that iterates through all currently running processes in the system, compares them with the specified 124 process names, and terminates any processes with the same name. The list of processes

terminated by the program contains a large number of game processes. The attacker believes that games occupy a large amount of CPU resources when running, which will affect their mining efficiency.

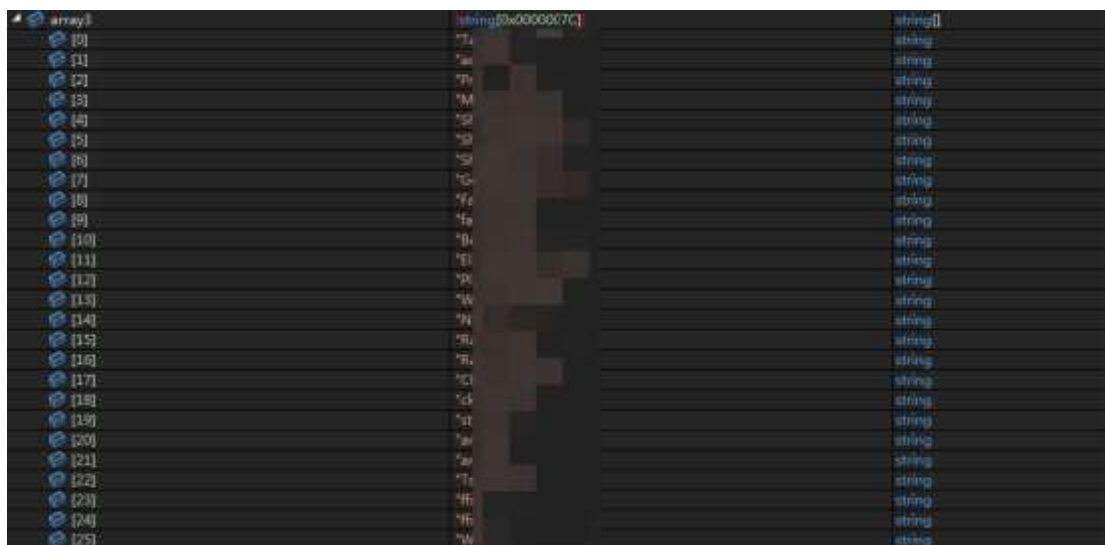


Figure 3-10 There are a large number of game process names in the list of terminated processes.

The hash rate curve of the attacker's cryptocurrency wallet shows that the attacker began the attack at the end of May, and the number of victim hosts used for mining has been on the rise.

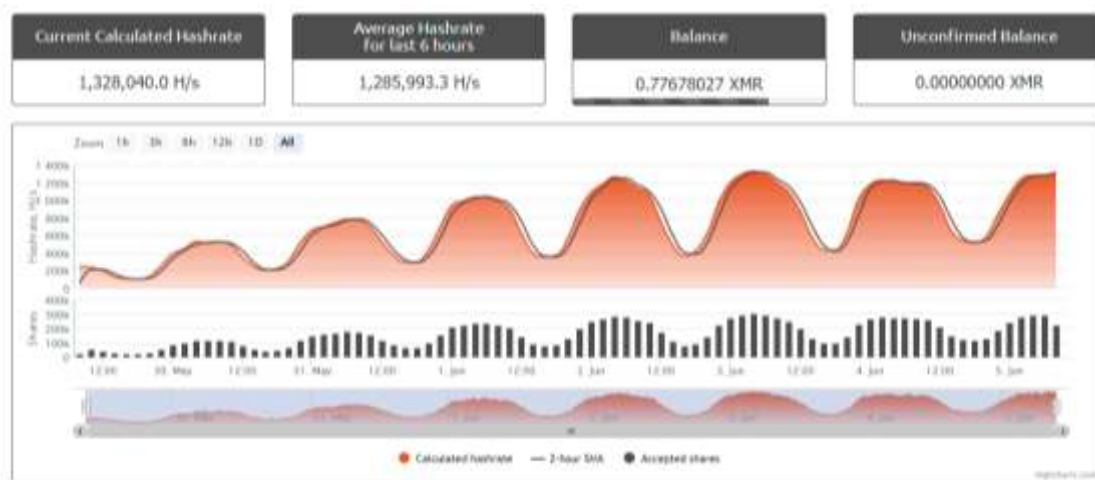


Figure 3-11 Mining computing power

## 4 Protective Recommendations

To effectively defend against such attacks and improve security protection, Antiy recommends that government and enterprise organizations take the following protective measures:

## 4.1 Website Transmission 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 it with anti-virus software after downloading;
2. It's recommended to execute suspicious files in a sandbox environment, and only execute them on the host when safety is ensured. The Antiy Persistent Threat Analysis System (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.

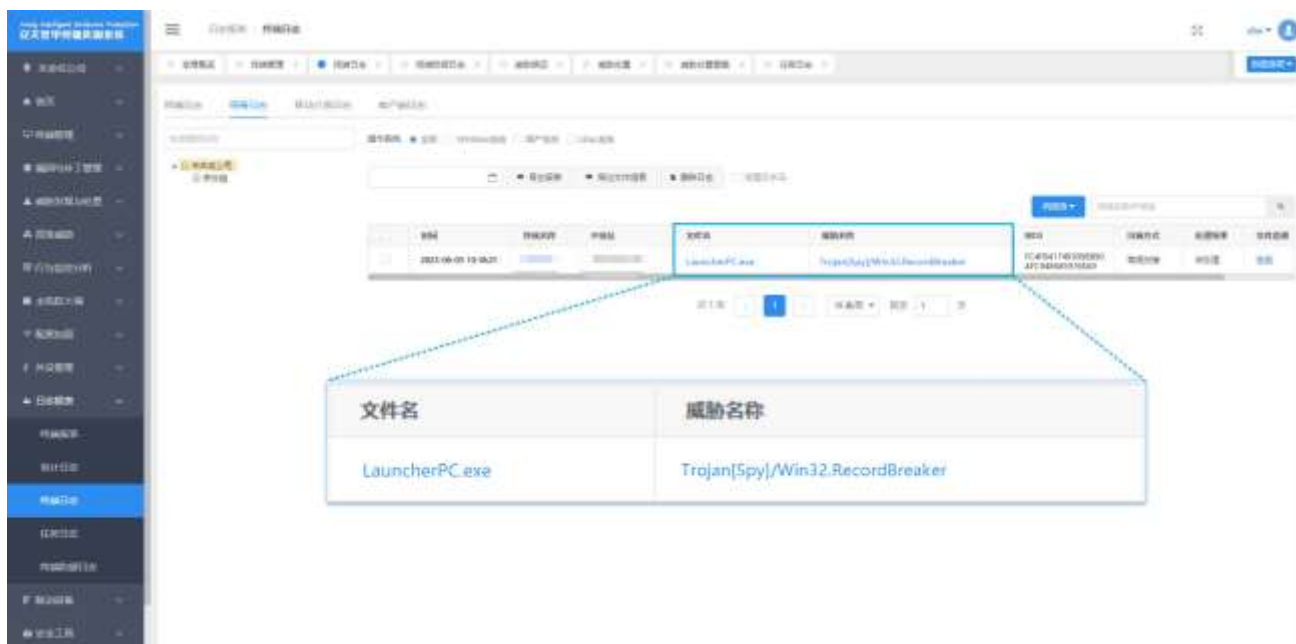
## 4.2 Endpoint Protection

1. Install terminal protection system: Install anti-virus software. It is recommended to install Antiy Intelligent Endpoint Protection System.
2. Strengthen passwords: Avoid using weak passwords. We recommend using passwords that are 16 characters or longer, including a combination of uppercase and lowercase letters, numbers, and symbols. Avoid using the same password for multiple accounts.

## 4.3 Initiate Emergency Response Promptly When Attacked

Contact the emergency response team: If you are attacked by malware, it is recommended to isolate the attacked host in a timely manner and protect the site while waiting for security engineers to investigate the computer; Antiy 24/7 service hotline: 400-840-9234.

**It has been proven that Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill malicious software such as data-stealing Trojans and mining Trojans.**



### Figure 4-1Antiy IEP achieves effective protection for user systems

## 5 ATT&CK Mapping Diagram Corresponding to the Incident

Regarding the complete process of the attacker delivering the data-stealing Trojan, Antiy sorted out the ATT&CK mapping corresponding to this attack incident as shown in the figure below:

[illegible]

### Figure 5-1 Mapping of technical characteristics to ATT&CK

The following table lists the techniques used by the attackers:

ATT&CK Stages/Categories	Specific behavior	Notes
Resource development	Get infrastructure	Obtain the C2 server
	Hack accounts	Steal YouTube accounts
	Environmental preparation	Host malicious payloads
Initial access	Phishing	Use phishing websites to spread malicious programs
	Use a valid account	Post videos using stolen YouTube accounts
Execute	Induce users to execute	Induce users to execute malicious programs
Persistence	Utilize scheduled tasks / jobs	Create a scheduled task for persistence
Defense evasion	Deobfuscate/decode files or information	Decode payload information
	Counterfeit	Counterfeit applications
	Obfuscate files or information	Obfuscate payload information
	Process injection	Processinjection
	Virtualization/sandbox escape	Fill with junk bytes
Credential access	Get the credentials from where the password is stored	Steal credentials from a specified location
	Steal application access tokens	Steal secrets from designated applications
	Steal Web Session Cookies	Steal cookie information in the browser
Credential access	Insecure credentials	Steal insecure credentials
Discover	Discover files and directories	Discover files and directories
	Discover process	Iterate over running processes
	Discover software	Discover software installed on the system
	Discover system information	Discover system information
Collect	Automatic collection	Automatic collection of information
	Collect local system data	Collect local system data
	Screen capture	Screenshot
Command and Control	Use application layer protocols	Use application layer protocols
Data exfiltration	Automatic exfiltration of data	Automatic exfiltration of data

	Use C2 channel for backhaul	Use C2 channel for backhaul
Influence	Resource hijacking	Occupy CPU resources for mining

## 6 IoCs

IoCs
FC4FB41749309B890AFC948645976EA9
854D15EDE01BB7DBC9B19EC8DAF54295
AA6CF53B4389F2EAC3AD5718B7300F80
E72D497C94BB1ED882AC98931F70E82E
hxxps://software.cc
hxxps://crackprogs.com
hxxps://expertstudiopro.com
hxxps://crackallsofts.com
hxxps://hotsoft.bio
hxxps://pastebin.com/raw/gvPycg8H
159.69.123.169
85.192.40.252

## Appendix 1: References

[1]. Follow-Up Analysis of the Redline Data-Stealing Trojan Spread via Video Websites

[https://www.antiy.cn/research/notice&report/research\\_report/20221115.html](https://www.antiy.cn/research/notice&report/research_report/20221115.html)

[2]. Analysis of Data-Stealing Samples Spread by Counterfeit Pirated Software

[https://www.antiy.cn/research/notice&report/research\\_report/20210628.html](https://www.antiy.cn/research/notice&report/research_report/20210628.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 cyberspace 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.