Cinobi Banking Trojan Targets Cryptocurrency Exchange Users via Malvertising

By Joseph C Chen (words)

Published: 2021-08-09 · Archived: 2026-04-05 22:35:29 UTC

Infection Routine

The campaign's infection routine begins when a user received malvertisements that are disguised as advertisements of either Japanese animated porn games, reward points applications, or video streaming applications. While we have observed five different themes of their malvertisements, all of them attempt to trick victims into downloading the same archive with the same malware.

These malvertisements are likely cloned from legitimate websites by the malicious actor. Minor modifications are then applied, such as the removal of some buttons and the changing of certain information sections. The only buttons that are left lead to the new page — created by the malicious actor — that instructs the victims how to download and execute the application.

After clicking on the button with the text "index.clientdownload.windows" (as shown in figure 2), the landing page starts downloading the ZIP archive, which is followed by instructions for the victim on how to open, extract, and execute the main executable file. The other four malicious ads look visually different, but their behavior and landing page is similar.

It is important to note that the access to the website is filtered based on the IP address. Non-Japanese IP addresses will see the following error message from Cloudflare.

Analysis of the malware

After extracting the ZIP archive, we noticed the listing seen in Figure 5. The files that we decided were interesting enough to be analyzed are marked in red.

Most files are legitimate ones taken from an older version of the "Logitech Captureopen on a new tab" application, dated 2018. The legitimate and signed LogiCapture.exe (08FB68EB741BF68F3CFC29A4AD3033D75AD57798ED826D926344015BDB8B0EBB) is instructed in LogiCapture.exe.config via custom application settingsopen on a new tab to load the Xjs.dll library. Xjs.dll loads the format.cfg file, decrypts the shellcode, and executes it.

The shellcode embedded into format.cfg copies config.dll and cfg.config to the temporary directory %TEMP%, renames these files to a.dll and 1.txt, and executes the export function named "a" of the a.dll library via the following command:

```
rundll32.exe "%TEMP%\a.dll",a %TEMP%\1.txt
```

Config.dll (renamed to a.dll) resolves necessary APIs, loads the content of cfg.config (which is renamed to 1.txt), decrypts it with a XOR key, and executes the shellcode. The decrypted cfg.config is the first stage of the Cinobi banking trojan (as explained in our initial blogpostnews article from 2020).

The Cinobi banking trojan is split into four stages, with each stage downloading additional components and possibly performing environment or anti-virtual machine (VM) checks. There are two command-and-control (C&C) servers, with one of them returning stages 2 to 4, while the other one returns the configuration files.

The malicious actor became more active in summer 2021 — we noticed a few more versions with slight differences from the ones described earlier. In addition to the application archive with four added malicious files (as shown in Figure 5), we also notice a refactored version of the archive with just three files (xjs.dll, format.cfg, and a file named "ros"), only three stages, and a single C&C server serving the configuration files.

In the refactored version, Xjs.dll decrypts and loads format.cfg, which is the first stage of the Cinobi banker. This stage, unlike our description from last year's blog entry, does not download Tor and other additional stages from the first C&C server. Instead, it reads and extracts files from the file called "ros", which is an encrypted package containing stages 2 and 3, a configuration file containing the C&C server, and an archive with Tor.

The most important of these is the configuration file containing websites targeted by the form-grabbing functionality. At the time of writing, we noticed that the banking trojan targets users of 11 Japanese financial institutions, with at least three of these involved in cryptocurrency trading.

When a victim using an infected machine accesses one of the websites mentioned in the configuration file and sends the filled-out form back to the server, the form-grabbing feature of the banker gets activated. In the following screenshots, we show examples of login forms with filled data.

After clicking the submit button, a text file with an encrypted request briefly appears in the folder with the installed banking trojan. After the decryption of the temporary created text file, the highlighted stolen credentials can be seen.

Conclusion

The new malvertising campaign shows that Water Kappa is still active and continuously evolving their tools and techniques for greater financial gain — this one also aims to steal cryptocurrency. In order to minimize the chances of being infected, users need to be wary of suspicious advertisements on shady websites, and as much as possible, download applications only from trusted sources.

Trend Micro solutions that offer a multilayered defense systemproducts can help organizations protect their employees from these kinds of campaigns by detecting, scanning, and blocking malicious URLs.

Indicators of Compromise

The complete indicators for this attack can also be found in this appendixopen on a new tab.

SHA256	File name	Note	Analysis
124FE26D53E2702B42AE07F8AEC5EE4E79E7424BCE6ECDA608536BBF0A7A2377	oneroom_setup.zip	Malicious game archive	Trojan.Win32
E667F9C109E20900CC8BADD09EDE6CDCE0BDC77164CFD035ACE95498E90D45E7	oneroom_game.zip	Malicious game archive	Trojan.Win32
93FFE7CF56FEB3FB541AEF91D3FC04A5CF22DF428DC0B7E5FEB8EDDDC2C72699	Magicalgirl.zip	Malicious game archive	Trojan.Win32
AD13BB18465D259ACC6E4CEBA24BEFF42D50843C8FD92633C569E493A075FDDC	kiplayer.zip	Malicious streaming archive	Trojan.Win3
A9EF18B012BD20945BB3533DEEC69D82437BF0117F83B2E9F9E7FACC5AA81255	oneroom_game_v7.zip	Malicious game archive	Trojan.Win32
6C1F4FFA63EE7094573B0F6D1BD51255F603BC8958757405C8C998416537D587	Xjs.dll	First shellcode loader	Trojan.Win32
1366E2AC6365E4B76595A19760438D876E01DB40C60EC3F42849F0218B724F1B	Xjs.dll	First shellcode loader	Trojan.Win32
0B3E5E2406490DF17A198A8340B103BB331A5277461234F3F90ED257E418C1F8	Xjs.dll	First shellcode loader	Trojan.Win32
3E0FAEE93F6EF572537735C7F2D82D151C5A21EB30EACC576B3B66320C74FD34	format.cfg	Encrypted shellcode	Trojan.Win32

DB6CBE4EE82F87008B34D1D4E9AA6EE3C9CCD21CB7A0B60925D5DA8D1295A269	format.cfg	Encrypted shellcode	Trojan.Win32
3B7FB5EC8180AD74871EB9F5B59E6E98A188CE84BA3BD6ADD9B4BCFCCB80C137	format.cfg	Encrypted shellcode	Trojan.Win32
52E2B9CBA4E1BEE1EB3ED9D03BC33EADB6C8D6AAC8598679AA95690E587BE7C4	config.dll	Cinobi 1st stage loader; 32bit	Trojan.Win32
F5AD9E32A84DF617ABA3786F19BA7DAB4B4BD8A27627232D3AACE760511AEDF7	config.dll	Cinobi 1st stage loader; 32bit	Trojan.Win32
45C7C36E7E8B832815D8B03651EDC14F864B52E1C599E5336A1AAA0BD47FF3E3	cfg.config	Encrypted 1st stage of Cinobi; 32bit	Trojan.Win3
522C59BACE844A3D76B674842373DDBF959FC5B352317B024DBF225F536A641E	cfg.config	Encrypted 1st stage of Cinobi; 32bit	Trojan.Win32
16AB933AD01D73120EE5B764C12057FF7F6DC3063BBC377CDB87419A30532323	N/A	2nd and 3rd stage loader; 32bit	Trojan.Win32
9D10AC2A2C7C58F1E1D4B745746AA5F0CE699C0DB87CCCA43418435FAA03AD1B	N/A	2nd stage encrypted; 32bit	Trojan.Win32
C4039CD7DB24158BE51DA9010E6A367F5253F40F007B656407FB69D279732784	N/A	3nd stage encrypted; 32bit	Trojan.Win32
2A6FE431326ACCAF31EA7CA7CD1214AD5EFCA891619859BCF60671A62C8D81F4	N/A	Cinobi 4th stage (last); 32bit	TrojanSpy.Wi
258EDBBAC7E78B4F51433807B237FC0ED7F76031795EA48A4FEFB38949F9B3B6	N/A	2nd and 3rd stage loader; 64bit	Trojan.Win64
A3010F206656752FAD70EF7637947933152E7ADC883B43D0832B2234C8E6F968	N/A	2nd stage encrypted; 64bit	Trojan.Win64

E037839A3DACC3153754A156136E9EAD2F4C52939FE869B3981C4BB5114202C8	N/A	3rd stage encrypted; 64bit	Trojan.Win64
F8B80978D4548139E824863DD661E40AF4C2523C3E93547E4F167A749E108280	N/A	Cinobi 4th stage (last); 64bit	TrojanSpy.Wi
B157BEAC5516D05A014527B3F0FE4B01683CAAC9FFF6608B67A8BA62DF5EF838	N/A	2nd and 3rd stage loader; 32bit	Trojan.Win3
2384FDA35A293B5F5B32B09E8DC455E7CE40A92D25CD9BACEEAB494785426B46	N/A	2nd stage encrypted; 32bit	Trojan.Win3
9FF65052FE93A884D7BCE36E87F4DE104839F72F26AF66785B2D98EAB706C816	N/A	3nd stage encrypted; 32bit	Trojan.Win32
31C936D08E9BA8FDA86844F67363223BDB6A917F530571ABCB3F584874909FEA	N/A	Cinobi 4th stage (last); 32bit	TrojanSpy.W
00F24AC0AD19DC3EE05A112F7650AABA16041020263EA851C90F3C0A61C7EC57	N/A	2nd and 3rd stage loader; 64bit	Trojan.Win64
B0E5BB79CDFAD284D88BC26DB4289A51F114CC71C928E8A9951DC8C498A243B9	N/A	2nd stage encrypted; 64bit	Trojan.Win64
095E85EBE2155798FB3A5FBD57196CF377B56FB2176CFF3A776302DCB806237D	N/A	3rd stage encrypted; 64bit	Trojan.Win64
B36BFF265EE47D31E4C70EE78BADCFCC0DE89643DA61C1BF16BA2D6F36A62936	N/A	Cinobi 4th stage (last); 64bit	TrojanSpy.Wi
E41AB2DE9CCFFE3AADDB32C224114D88D2E61C02D52F89829B544F49B672D74D	N/A	2nd stage loader; 32bit	Trojan.Win32
59DF3B32A0D3FEFB15C6AAB7D9254E597484A486156CBC1F403A376A8A0C25FB	N/A	2nd stage encrypted; 32bit	Trojan.Win32

043720F493CA7A2B2E18CCD7AEC8CB8D577F544AAE02975BFE313046E839F107	N/A	2nd stage loader; 64bit	Trojan.Win64
83F7D60D172628E421EF038566F449E8708573201C8F23398F0F06B5F33123DA	N/A	2nd stage encrypted; 64bit	Trojan.Win64
58C60164AAA23777E5A8DBBA25C4466A5B1ECA54EF8CF02BA2CD1AB7084753BE	N/A	Cinobi 3rd stage (last); 32bit	TrojanSpy.W
F3DA0C082EB271A2F0DD54F2A3260BFC02BDF311EBCB1C619D479FCBB1E9F6F5	N/A	Cinobi 3rd stage (last); 64bit	TrojanSpy.Wi

IP Address/Domain/URL	Note
www[.]chirigame[.]com	Malvertising domain
www[.]supapureigemu[.]com	Malvertising domain
www[.]getkiplayer[.]com	Malvertising domain
www[.]magicalgirlonlive[.]com	Malvertising domain
a7q5adiilsjkujxk[.]onion	Cinobi banker’s C&C serving stages 2-4
5lmt6t4kaymuwvm5[.]onion	Cinobi banker’s C&C serving configuration files