Cinobi Banking Trojan Targets Cryptocurrency Exchange Users via Malvertising

trendmicro.com/en_us/research/21/h/cinobi-banking-trojan-targets-users-of-cryptocurrency-exchanges-.html

August 9, 2021

Cyber Threats

We found a new social engineering-based malvertising campaign targeting Japan that delivered a malicious application. The malicious application abused sideloading vulnerabilities to load and start the Cinobi banking trojan.

By: Jaromir Horejsi, Joseph C Chen August 09, 2021 Read time: (words)

In a previous blog entry, we reported on a campaign, which we labeled "Operation Overtrap," that targeted Japan with a new banking trojan called Cinobi. The campaign, which was perpetrated by a group we named "Water Kappa," delivered Cinobi via spam. It also delivered the trojan using the Bottle exploit kit, which included newer Internet Explorer exploits CVE-2020-1380 and CVE-2021-26411 and was used for malvertising attacks that was distributed only to Microsoft Internet Explorer users. Throughout 2020 and the first half of 2021, we observed limited activity from the Bottle exploit kit, with traffic decreasing during the middle of June — possibly indicating that the group was turning to new tools and techniques.

Meanwhile, we found a new social engineering-based malvertising campaign targeting Japan that delivered a malicious application disguised as either a free porn game, a reward points application, or a video streaming application. The malicious application abused sideloading vulnerabilities to load and start the Cinobi banking trojan. We consider this to be a new campaign from Water Kappa that is aimed at users of web browsers other than Internet Explorer.

Looking into the Cinobi sample, we found that the overall functionality remained relatively the same, but the configuration had been updated to include several Japanese cryptocurrency exchange websites as part of the target list. The group started to use Cinobi to steal the credentials of its victim's cryptocurrency account.

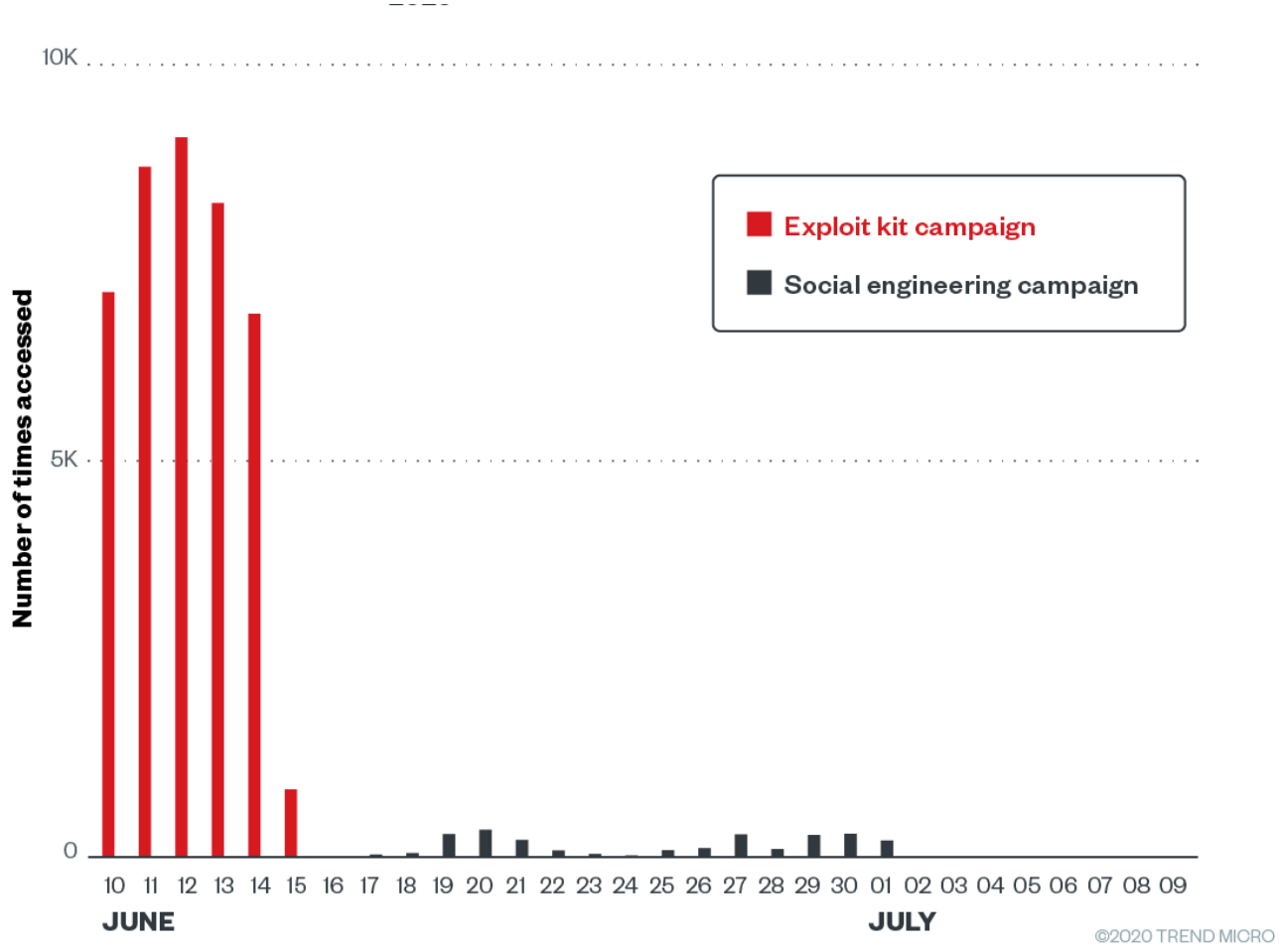

Figure 1. Timeline of Water Kappa's activities

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.

Figure 2. The landing page for downloading the malicious archive, disguised as a streaming application

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.

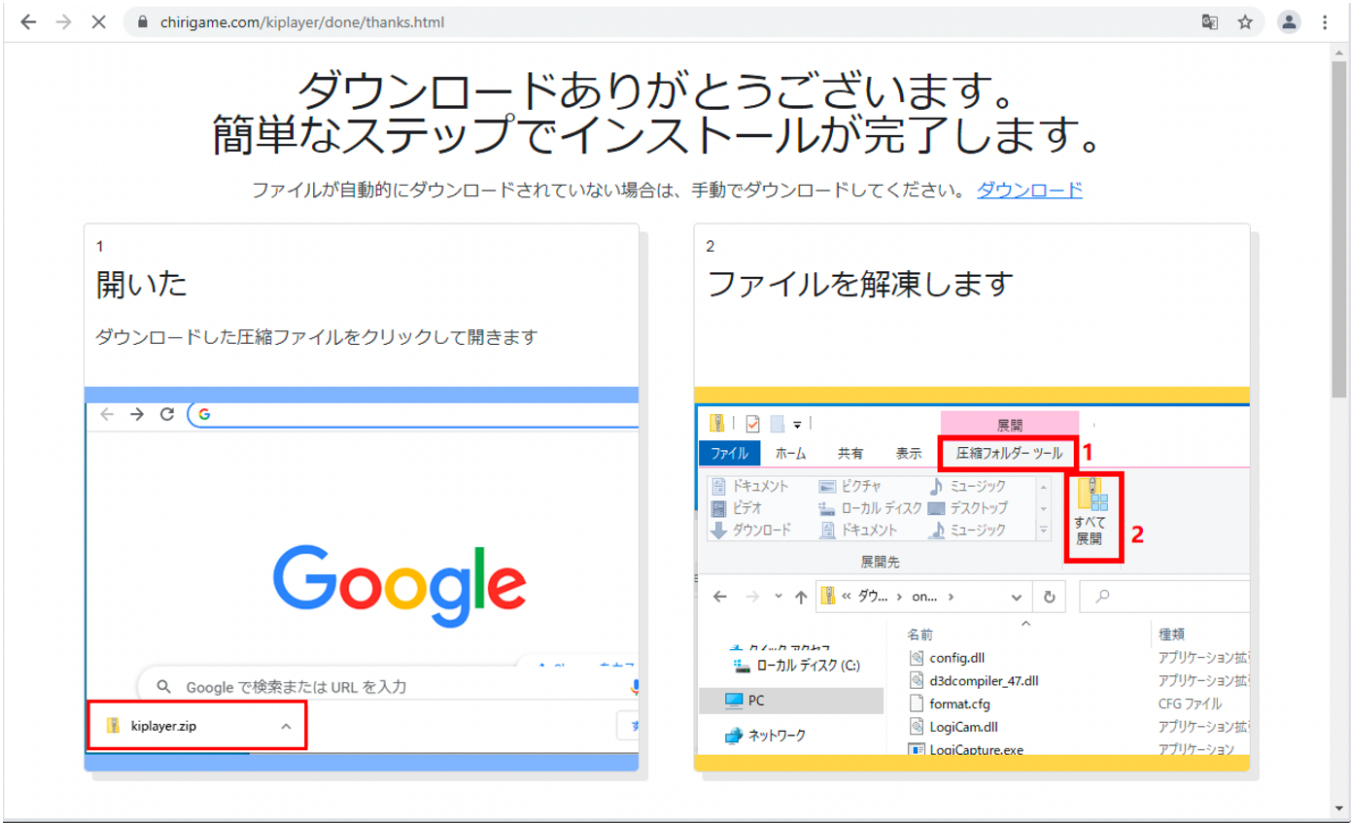

Figure 3. Instructions for executing the streaming application

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.

Figure 4. Error shown when the application or game website is accessed from a non-Japanese IP address

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.

[cef3_2987]		<DIR>	07/28/2021 19:51
avcodec-55	dll	11,681,944	10/19/2018 22:22
avdevice-55	dll	124,040	10/19/2018 22:22
avfilter-4	dll	789,128	10/19/2018 22:22
avformat-55	dll	1,698,952	10/19/2018 22:22
avutil-52	dll	345,736	10/19/2018 22:22
cfg	config	15,895	07/09/2021 15:08
config	dll	34,304	07/09/2021 15:08
d3dcompiler_47	dll	3,466,856	08/27/2018 23:06
format	cfg	1,050	07/09/2021 15:07
LogiCam	dll	358,024	10/19/2018 22:22
LogiCapture	exe	4,287,624	10/19/2018 22:22
LogiCapture.exe	config	18,899	06/21/2021 21:46
LogiCapture.exe	manifest	2,015	08/27/2018 23:06
Native.LogiCapture.exe	manifest	51,703	08/27/2018 23:06
openh264-1.5.0-win32msvc	dll	619,008	06/21/2021 21:03
swresample-0	dll	104,072	10/19/2018 22:22
swscale-2	dll	448,136	10/19/2018 22:22
VHMediaCOM	dll	4,402,312	10/19/2018 22:22
Xjs	dll	34,304	07/09/2021 15:07
XjsEx	dll	454,280	10/19/2018 22:22

Figure 5. Contents of the ZIP archive containing the game; malicious files are marked in red

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

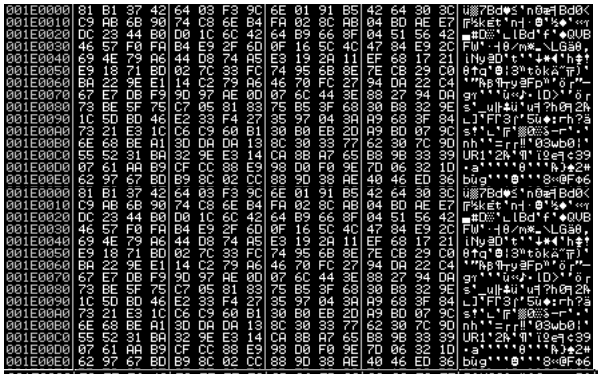

Figure 7. The encrypted format.cfg shellcode

Figure 7. The encrypted format.cfg shellcode

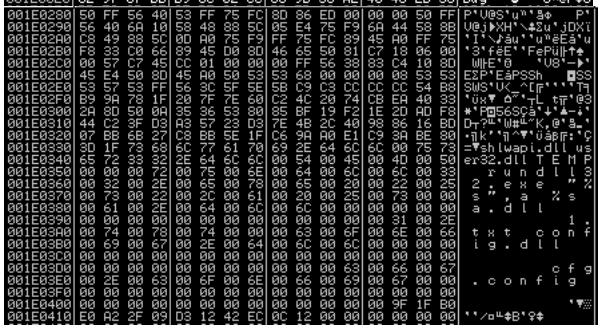

Figure 8. The decrypted format.cfg shellcode; strings with file names and rundll32 command are visible

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 blogpost from 2020).

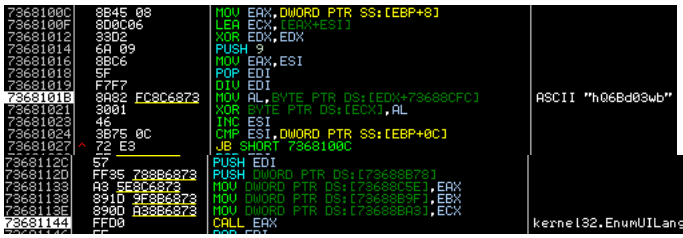

Figure 9. Routine in config.dll that decrypts the cfg.config shellcode

Figure 10. Call instruction in Config.dll that executes the decrypted cfg.config shellcode

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.

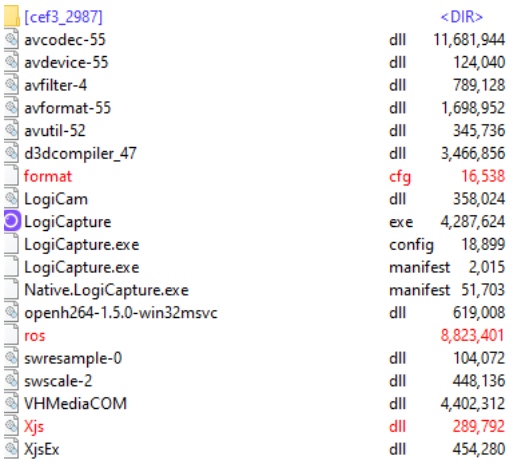

Figure 11: The refactored Cinobi banker

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.

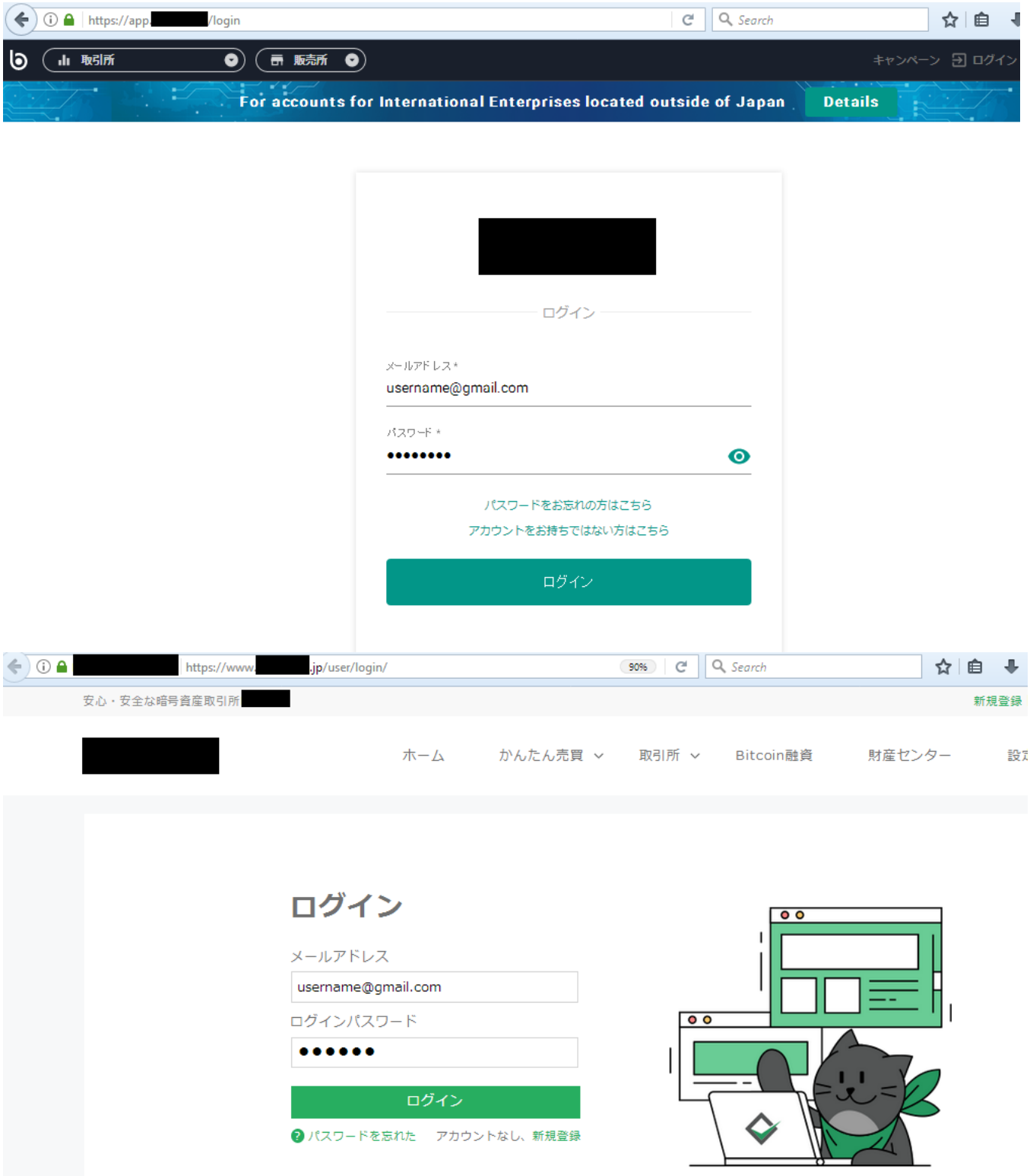

Figure 12. The targeted websites of companies dealing with cryptocurrencies

@#!%.v)W.*çV«kÌ.¥.t..#...1...https://api.[redacted]/login?__bf=12021-07-26 10:36:05{"mail":"username@gmail.com","password":"87654321","g-recaptcha-response":"03AGdBq25aMFANa314xH2lWzV0at6SPG5CwIxH0-eejkquGXefUZLPV8zv9Bhx2p-RqQrjiA0tNms_cCbCzbxkD9BwuvP1clkTwJdYFiY-qQe5afac0HKNJFTpCu2niI-QphPLXykwVKY_gxiB1rl0nHeGRzjUoQQ_uT4YMkkZ9VxMRKo9p13JAKmNP6cFtOIhz_Lv7bImUx-cxkz-PD_E_ILCVp_DnIGTA3LJ-ZHSEvzpRAjITYB7rTRQA24v3M2rtO50qbQsQtcYbCbKjLtR9h6k9qZSBAOtPsQmSwCci0mAlP3K1GhFNCVpYBLsbVd8mE0kGq1CJigLv5RM3apRm9kANI9JVI-s384WiOgeaOgZLJuearMQv1qZvfR1rV1wM6JXbtzuyYfWHGmHsxEa2sbVM6lNe-f01QsETShJA7csDE42MRuoh4IQb75HtlAeE7T0otrev5K4qbxkfe7ec5ciqoHI81Voow"}

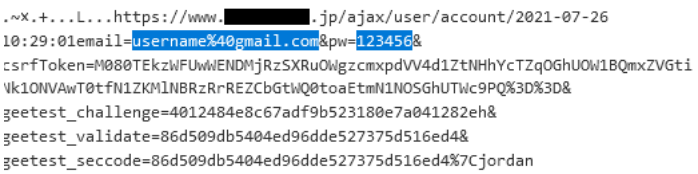

Figure 13. The decrypted requests; login credentials are highlighted in blue

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 system 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 appendix.

URLs

SHA256	File name	Note	Analysis
124FE26D53E2702B42AE07F8AEC5EE4E79E7424BCE6ECDA608536BBF0A7A2377	oneroom_setup.zip	Malicious game archive	Trojan.Win32.S
E667F9C109E20900CC8BADD09EDE6CDCE0BDC77164CFD035ACE95498E90D45E7	oneroom_game.zip	Malicious game archive	Trojan.Win32.S
93FFE7CF56FEB3FB541AEF91D3FC04A5CF22DF428DC0B7E5FEB8EDDDC2C72699	Magicalgirl.zip	Malicious game archive	Trojan.Win32.S
AD13BB18465D259ACC6E4CEBA24BEFF42D50843C8FD92633C569E493A075FDDC	kiplayer.zip	Malicious streaming archive	Trojan.Win32.S
A9EF18B012BD20945BB3533DEEC69D82437BF0117F83B2E9F9E7FACC5AA81255	oneroom_game_v7.zip	Malicious game archive	Trojan.Win32.S
6C1F4FFA63EE7094573B0F6D1BD51255F603BC8958757405C8C998416537D587	Xjs.dll	First shellcode loader	Trojan.Win32.S
1366E2AC6365E4B76595A19760438D876E01DB40C60EC3F42849F0218B724F1B	Xjs.dll	First shellcode loader	Trojan.Win32.S
0B3E5E2406490DF17A198A8340B103BB331A5277461234F3F90ED257E418C1F8	Xjs.dll	First shellcode loader	Trojan.Win32.S
3E0FAEE93F6EF572537735C7F2D82D151C5A21EB30EACC576B3B66320C74FD34	format.cfg	Encrypted shellcode	Trojan.Win32.S
DB6CBE4EE82F87008B34D1D4E9AA6EE3C9CCD21CB7A0B60925D5DA8D1295A269	format.cfg	Encrypted shellcode	Trojan.Win32.S
3B7FB5EC8180AD74871EB9F5B59E6E98A188CE84BA3BD6ADD9B4BCFCCB80C137	format.cfg	Encrypted shellcode	Trojan.Win32.S

52E2B9CBA4E1BEE1EB3ED9D03BC33EADB6C8D6AAC8598679AA95690E587BE7C4	config.dll	Cinobi 1st stage loader; 32bit	Trojan.Win32.C
F5AD9E32A84DF617ABA3786F19BA7DAB4B4BD8A27627232D3AACE760511AEDF7	config.dll	Cinobi 1st stage loader; 32bit	Trojan.Win32.C
45C7C36E7E8B832815D8B03651EDC14F864B52E1C599E5336A1AAA0BD47FF3E3	cfg.config	Encrypted 1st stage of Cinobi; 32bit	Trojan.Win32.C
522C59BACE844A3D76B674842373DDBF959FC5B352317B024DBF225F536A641E	cfg.config	Encrypted 1st stage of Cinobi; 32bit	Trojan.Win32.C
16AB933AD01D73120EE5B764C12057FF7F6DC3063BBC377CDB87419A30532323	N/A	2nd and 3rd stage loader; 32bit	Trojan.Win32.C
9D10AC2A2C7C58F1E1D4B745746AA5F0CE699C0DB87CCCA43418435FAA03AD1B	N/A	2nd stage encrypted; 32bit	Trojan.Win32.C
C4039CD7DB24158BE51DA9010E6A367F5253F40F007B656407FB69D279732784	N/A	3nd stage encrypted; 32bit	Trojan.Win32.C
2A6FE431326ACCAF31EA7CA7CD1214AD5EFCA891619859BCF60671A62C8D81F4	N/A	Cinobi 4th stage (last); 32bit	TrojanSpy.Win3
258EDBBAC7E78B4F51433807B237FC0ED7F76031795EA48A4FEFB38949F9B3B6	N/A	2nd and 3rd stage loader; 64bit	Trojan.Win64.C
A3010F206656752FAD70EF7637947933152E7ADC883B43D0832B2234C8E6F968	N/A	2nd stage encrypted; 64bit	Trojan.Win64.C
E037839A3DACC3153754A156136E9EAD2F4C52939FE869B3981C4BB5114202C8	N/A	3rd stage encrypted; 64bit	Trojan.Win64.C
F8B80978D4548139E824863DD661E40AF4C2523C3E93547E4F167A749E108280	N/A	Cinobi 4th stage (last); 64bit	TrojanSpy.Win6
B157BEAC5516D05A014527B3F0FE4B01683CAAC9FFF6608B67A8BA62DF5EF838	N/A	2nd and 3rd stage loader; 32bit	Trojan.Win32.C
2384FDA35A293B5F5B32B09E8DC455E7CE40A92D25CD9BACEEAB494785426B46	N/A	2nd stage encrypted; 32bit	Trojan.Win32.C

9FF65052FE93A884D7BCE36E87F4DE104839F72F26AF66785B2D98EAB706C816	N/A	3nd stage encrypted; 32bit	Trojan.Win32.C
31C936D08E9BA8FDA86844F67363223BDB6A917F530571ABCB3F584874909FEA	N/A	Cinobi 4th stage (last); 32bit	TrojanSpy.Win
00F24AC0AD19DC3EE05A112F7650AABA16041020263EA851C90F3C0A61C7EC57	N/A	2nd and 3rd stage loader; 64bit	Trojan.Win64.C
B0E5BB79CDFAD284D88BC26DB4289A51F114CC71C928E8A9951DC8C498A243B9	N/A	2nd stage encrypted; 64bit	Trojan.Win64.C
095E85EBE2155798FB3A5FBD57196CF377B56FB2176CFF3A776302DCB806237D	N/A	3rd stage encrypted; 64bit	Trojan.Win64.C
B36BFF265EE47D31E4C70EE78BADCFCC0DE89643DA61C1BF16BA2D6F36A62936	N/A	Cinobi 4th stage (last); 64bit	TrojanSpy.Win6
E41AB2DE9CCFFE3AADDB32C224114D88D2E61C02D52F89829B544F49B672D74D	N/A	2nd stage loader; 32bit	Trojan.Win32.C
59DF3B32A0D3FEFB15C6AAB7D9254E597484A486156CBC1F403A376A8A0C25FB	N/A	2nd stage encrypted; 32bit	Trojan.Win32.C
043720F493CA7A2B2E18CCD7AEC8CB8D577F544AAE02975BFE313046E839F107	N/A	2nd stage loader; 64bit	Trojan.Win64.C
83F7D60D172628E421EF038566F449E8708573201C8F23398F0F06B5F33123DA	N/A	2nd stage encrypted; 64bit	Trojan.Win64.C
58C60164AAA23777E5A8DBBA25C4466A5B1ECA54EF8CF02BA2CD1AB7084753BE	N/A	Cinobi 3rd stage (last); 32bit	TrojanSpy.Win
F3DA0C082EB271A2F0DD54F2A3260BFC02BDF311EBCB1C619D479FCBB1E9F6F5	N/A	Cinobi 3rd stage (last); 64bit	TrojanSpy.Win6

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