Operation Overtrap Targets Japanese Online Banking Users Via Bottle Exploit Kit and Brand-New Cinobi Banking Trojan

- Posted on:March 11, 2020 at 6:00 am
- Posted in:Malware
- Author:
  Trend Micro

0

By Jaromir Horejsi and Joseph C. Chen (Threat Researchers)

We recently discovered a new campaign that we dubbed "Operation Overtrap" for the numerous ways it can infect or trap victims with its payload. The campaign mainly targets online users of various Japanese banks by stealing their banking credentials using a three-pronged attack. Based on our telemetry, Operation Overtrap has been active since April 2019 and has been solely targeting online banking users located in Japan. Our analysis found that this campaign uses three different attack vectors to steal its victims' banking credentials:

- By sending spam emails with a phishing link to a page disguised as a banking website
- By sending spam emails asking victims to run a disguised malware's executable downloaded from a linked phishing page.
- By using a custom exploit kit to deliver malware via malvertising

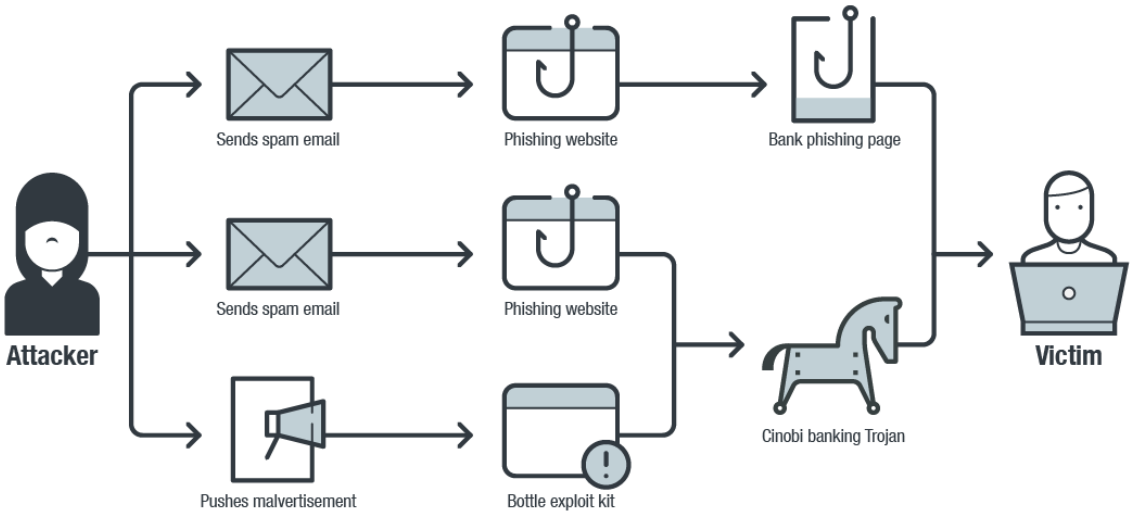

Figure 1. Operation Overtrap three-pronged attack flow

This blog will discuss how we discovered the campaign and introduce the brand-new banking trojan Cinobi. Meanwhile, a detailed look at the different attack vectors associated with this campaign, and a more in-depth analysis of dropped configuration files as well as Cinobi's features, are discussed in our technical brief.

Technical Analysis

Discovering Operation Overtrap

We first discovered the campaign in September 2019 using a then-unidentified exploit kit. Based on our data, Operation Overtrap has been using spam emails to deliver its payload to victims as early as April 2019.

In mid-September, we observed a significant number of victims being redirected to the exploit kit, which targeted Internet Explorer, after they have clicked on links from social media platforms. It should be noted, however, that the way the victims received the links has not been identified. It is also worth mentioning that Operation Overtrap only seems to target Japanese online banking users; it redirects victims with other geolocations to a fake online shop.

Upon analysis, we saw that the exploit kit only dropped a clean binary that does not perform malicious activities on a victim's device. It also immediately closes after infection. It is still unclear why the threat actors behind Operation Overtrap initially delivered a clean binary file; it's possible that they were testing their custom exploit kit during this stage of the campaign's development.

#	Result	Protocol	Host	URL	Body	Caching	Content-Type
2	200	HTTPS	[redacted]	/l.php?u=http%3A%2F%2Fagnbub.uauovk.club%2F…	289	private…	text/html; charset="utf-8"
3	200	HTTPS		/ajax/bz	0	private…	text/html; charset="utf-8"
4	200	HTTPS		/ajax/bz	0	private…	text/html; charset="utf-8"
5	302	HTTP	agnbub.uauovk.club	[redacted]	3		text/html; charset=UTF-8
6	200	HTTP	sales.inteleksys.com	/cate.html	618	max-ag…	text/html
7	200	HTTP	sales.inteleksys.com	/file/ajax.min.js	2,143	max-ag…	application/javascript
8	200	HTTP	sales.inteleksys.com	/file/main.js	19,275	max-ag…	application/javascript
9	200	HTTP	sales.inteleksys.com	/file/1.gif	41,746	max-ag…	image/gif
10	200	HTTP	sales.inteleksys.com	/conn.php?callback=?&data1=10&data2=0&data3=2…	54		text/html; charset=UTF-8
11	200	HTTP	sales.inteleksys.com	/file/swf.swf	0	max-ag…	application/x-shockwave-flash
12	200	HTTP	sales.inteleksys.com	/file/swf.swf	7,699	max-ag…	application/x-shockwave-flash
13	200	HTTP	sales.inteleksys.com	/conn.php?ge=1	31,744		text/html; charset=UTF-8

Figure 2. A screengrab that shows exploit kit network traffic in September 2019

```
.text:00401000 ; int __stdcall WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int nShowCmd)
.text:00401000 _WinMain@16     proc near               ; CODE XREF: ___tmainCRTStartup+115↓p
.text:00401000
.text:00401000 hInstance       = dword ptr  4
.text:00401000 hPrevInstance   = dword ptr  8
.text:00401000 lpCmdLine       = dword ptr  0Ch
.text:00401000 nShowCmd        = dword ptr  10h
.text:00401000
.text:00401000                 xor     eax, eax
.text:00401002                 retn    10h
.text:00401002 _WinMain@16     endp
```

Figure 3. A screengrab that shows a clean file dropped by Operation Overtrap's exploit kit

Operation Overtrap's Custom Exploit Kit: Bottle Exploit Kit

On September 29, 2019, we observed that the exploit kit ceased to drop a clean file, and instead, delivered a brand-new banking trojan that we dubbed "Cinobi." We also noted that the threat actors behind Operation Overtrap have stopped redirecting victims from social media and began to use a Japan-targeted malvertising campaign to push their custom exploit kit.

Another researcher later discovered the custom exploit kit, which was named the Bottle Exploit Kit (BottleEK). It exploits CVE-2018-15982, a Flash Player use after free vulnerability, as well as CVE-2018-8174, a VBScript remote code execution vulnerability. Victims will be infected with BottleEK's payload if they access this particular exploit kit's landing page with unpatched or outdated browsers. Our telemetry shows that BottleEK was the most active exploit kit detected in Japan in February 2020.

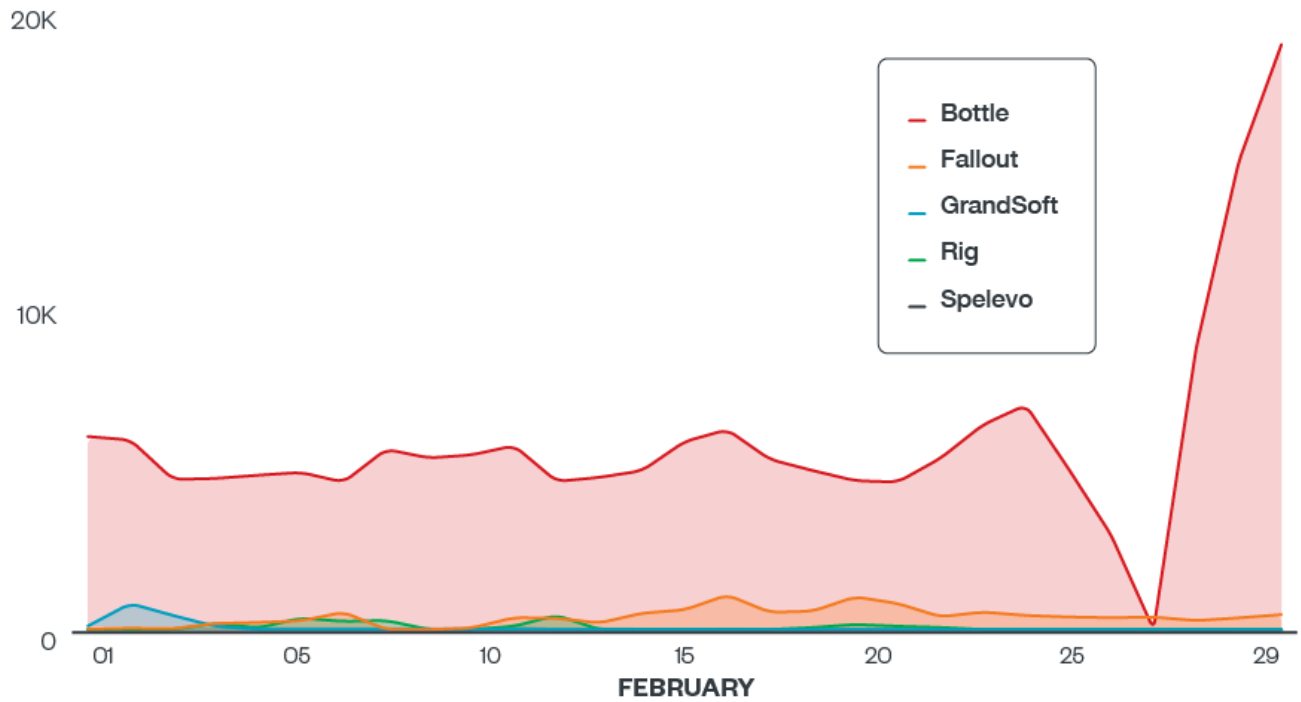

Figure 4. Exploit kit activity observed in Japan on February 2020 (Data obtained from Trend Micro Smart Protection Network™)

Brand-new banking malware: Cinobi

Operation Overtrap used a new banking malware we've decided to call Cinobi. Based on our analysis, Cinobi has two versions — the first one has a DLL library injection payload that compromises victims' web browsers to perform form-grabbing.

This Cinobi version can also modify web traffic sent to and received from targeted websites. Our investigation found that all the websites that this campaign targeted were those of Japan-based banks.

Aside from form-grabbing, it also has a webinject function that allows cybercriminals to modify accessed webpages. The second version has all the capabilities of the first one plus the ability to communicate with a command-and-control (C&C) server over the Tor proxy.

Cinobi's four stages of infection

Each of Cinobi's four stages contains an encrypted position-independent shellcode that makes analysis slightly more complicated. Each stage is downloaded from a C&C server after certain conditions have been met.

First stage

The first stage of Cinobi's infection chain, which has also been analyzed by another cybersecurity researcher, starts by calling the "GetUserDefaultUILanguages" function to check if the infected device's local settings are set to Japanese.

```
:0000185C                call    dword ptr [eax+edi+117h] ; GetUserDefaultUILanguage
:00001863                mov     ecx, 411h
:00001868                cmp     ax, cx
:0000186B                jnz     loc_26B3        ; is Japanese locale
```

Figure 5. Screengrab of Cinobi's check to determine the device's language settings using "GetUserDefaultUILanguages"

Cinobi will then download legitimate unzip.exe and Tor applications from the following locations:

- ftp://ftp[.]cadwork.ch/DVD_V20/cadwork.dir/COM/unzip[.]exe
- https://archive[.]torproject[.]org/tor-package-archive/torbrowser/8.0.8/tor-win32-0.3.5.8[.]zip

After extracting the Tor archive into the "\AppData\LocalLow\" directory, Cinobi will rename tor.exe to taskhost.exe and execute it. It will also run tor.exe with custom torrc file settings.

- "C:\Users\<username>\AppData\LocalLow\<random_name>\Tor\taskhost.exe" –f
- "C:\Users\<username>\AppData\LocalLow\<random_name>\torrc"

It will download the second stage of the malware payload from a .onion C&C address and save it in a randomly named .DLL file within the "\AppData\LocalLow\" folder. The filename of the first stage downloader is saved into a .JPG file with a random name.

```
00000000: 43 00 3A 00 5C 00 74 00|65 00 6D 00 70 00 5C 00  | C.:.\.t.e.m.p.\.
00000010: 73 00 76 00 63 00 68 00|6F 00 73 00 74 00 2E 00  | s.v.c.h.o.s.t...
00000020: 62 00 69 00 6E 00      |                         | b.i.n.
```

Figure 6. Screengrab of the .JPG file that contains the filename of the first stage downloader

After this, Cinobi will run the second stage of its downloader on the victim's machine.

```
"rundll32.exe" "C:\Users\[redacted]\AppData\LocalLow\foepcyof\foepcyof
\foepcyof.dll",q8WnHQTl C:\Users\[redacted]\AppData\LocalLow\foepcyof
\foepcyof\foepcyof.dll
```

Figure 7. Screengrab of code showing Cinobi running the second stage of its downloader on the victim's machine

Second stage

Cinobi will connect to its C&C server to download and decrypt the file for the third stage of its infection chain. We observed that the filename of the third stage starts with the letter C, followed by random characters. Afterward, it will download and decrypt the file for the fourth stage, which has a filename that starts with the letter A, followed by random characters.

After these, Cinobi will download and decrypt a config file (<random_name>.txt) that contains a new C&C address.

Cinobi uses RC4 encryption with a hardcoded key.

```
00000000: C5 2A BB 83 C7 40 BB 01|1D 9B 38 A9 AA 5C F2 96  | Å*»ƒÇ@»..▯8©ª\ò▯
00000010: 68 74 74 70 3A 2F 2F 34|77 36 79 6C 6E 69 61 6D  | http://4w6ylniam
00000020: 75 36 78 37 65 33 61 2E|6F 6E 69 6F 6E 2F 63 6F  | u6x7e3a.onion/co
00000030: 6E 6E 65 63 74 2E 70 68|70 0D 0A 68 74 74 70 3A  | nnect.php..http:
00000040: 2F 2F 6C 6F 63 61 6C 68|6F 73 74 2F 6D 61 69 6E  | //localhost/main
00000050: 44 6F 6D 61 69 6E 2F 63|6F 6E 6E 65 63 74 2E 70  | Domain/connect.p
00000060: 68 70                  |                         | hp
```

Figure 8. Screengrab of code showing Cinobi's decoded config file

Next, Cinobi will run the downloaded third stage infection file using the UAC bypass method via the CMSTPLUA COM interface.

Third stage

During the third infection stage, Cinobi will copy malware files from "\AppData\LocalLow\" to the "%PUBLIC%" folder. It will then install the fourth stage of the downloader (which was downloaded during the second stage) as Winsock Layered Service Provider (WSCInstallProviderAndChains).

```
:00001CC4                push    [ebp+arg_0]
:00001CC7                lea     eax, [ebp+var_530] ; C:\Users\Public\foepcyof\Afoepcyof.dll
:00001CCD                push    eax
:00001CCE                mov     eax, [ebp+var_34]
:00001CD1                call    dword ptr [eax+13Bh] ; WSCInstallProviderAndChains
```

Figure 9. Screengrab of code showing the installation of the infection's fourth stage on the victim machine as "WSCInstallProviderAndChains"

Cinobi will then perform the following actions:

- Change spooler service config to "SERVICE_AUTO_START"
- Disable the following services:
  - UsoSvc
  - Wuauserv
  - WaaSMedicSvc
  - SecurityHealthService
  - DisableAntiSpyware
- Copy and extract Tor files to "%PUBLIC%" folder
- Rename tor.exe to taskhost.exe
- Create torrc in "%PUBLIC%" with the content "DataDirectory C:\Users\Public\<random_nam>\data\tor"
- Create .JPG file with the original dropper name
- Remove files from "\AppData\LocalLow\," remove original dropper file

Fourth stage

Cinobi will call the **WSCEnumProtocols** function to retrieve information about available transport protocols. It will also call the **WSCGetProviderPath** function to retrieve the DLL path of the original transport provider. This function is called twice. The first call will return the malicious provider (as the fourth stage of the malware has already been installed during the third stage of infection). The second call will return the original transport provider ("%SystemRoot%\system32\mswsock.dll") and resolve and call its WSPStartup function. Cinobi will then check the name of the process in which the malicious DLL provider gets injected. In practice, Cinobi should be injected into all processes that make network connections using Windows sockets.

Handle or DLL substring: Apuidraut.dll

Process	PID	Type	Name
VBoxService.exe	660	DLL	C:\Users\Public\puidraut\Apuidraut.dll
svchost.exe	1324	DLL	C:\Users\Public\puidraut\Apuidraut.dll
spoolsv.exe	1656	DLL	C:\Users\Public\puidraut\Apuidraut.dll
taskhost.exe	2996	DLL	C:\Users\Public\puidraut\Apuidraut.dll
Fiddler.exe	3292	DLL	C:\Users\Public\puidraut\Apuidraut.dll

Figure 10. Screengrab of processes where the malicious DLL provider has been injected

Best practices against spam and vulnerabilities

Operation Overtrap uses a variety of attack vectors to steal banking credentials. Users and organizations need to adopt best practices to protect their systems against messaging-related threats and avoid malicious advertisements. An example of a best practice is to have a central point for reporting suspicious emails. Organizations, through their IT teams, need to have a

centralized information gathering system, and all employees must be aware of the reporting procedure for suspicious emails. Meanwhile, users can avoid malicious advertisements by avoiding clicking on suspicious links or pop-ups and updating software via official channels.

Organizations will benefit from regularly updating systems (or use virtual patching for legacy systems) to prevent attackers from taking advantage of security gaps. Additional security mechanisms like firewalls and intrusion detection and prevention systems will help thwart suspicious network activities such as data exfiltration or C&C communication.

Trend Micro Solutions

Organizations can consider Trend Micro™ endpoint solutions such as Trend Micro Smart Protection Suites and Worry-Free™ Business Security. Both solutions can protect users and businesses from threats by detecting malicious files and spammed messages as well as blocking all related malicious URLs. Trend Micro Deep Discovery™ has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs.

Trend Micro™ Hosted Email Security is a no-maintenance cloud solution that delivers continuously updated protection that stops spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network. It protects Microsoft Exchange, Microsoft Office 365, Google Apps, and other hosted and on-premises email solutions.

For defending against malvertising campaigns in general, users can employ Trend Micro™ Maximum Security, which protects consumers via a multi-layered defense that delivers highly effective and efficient protection against ever-evolving threats. Trend Micro™ Smart Protection Suites also protect businesses against these types of threats by providing threat protection techniques designed to eliminate security gaps across multiple users and endpoints.

You may read our in-depth analysis of Operation Overtrap in this technical brief, which also contains details about possible links to other phishing campaigns and the indicators of compromise.

Related Posts:

- **Latest Trickbot Campaign Delivered via Highly Obfuscated JS File**
- **New Exploit Kit Capesand Reuses Old and New Public Exploits and Tools, Blockchain Ruse**

Tags: banking malwarebanking TrojanBottle exploit kitBottleEKCinobiexploit kitOperation Overtrap

Security Predictions for 2020

- Cybersecurity in 2020 will be viewed through many lenses — from differing attacker motivations and cybercriminal arsenal to technological developments and global threat intelligence — only so defenders can keep up with the broad range of threats.
  Read our security predictions for 2020.

Business Process Compromise

- Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Recent Posts

Popular Posts

February Patch Tuesday: Fixes for Critical LNK, RDP, Trident Vulnerabilities

Angler and Nuclear Exploit Kits Integrate Pawn Storm Flash Exploit

Stay Updated

Email Subscription

Your email here

Subscribe

- Home and Home Office
- |
- For Business
- |
- Security Intelligence
- |
- About Trend Micro

- Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국, 台灣
- Latin America Region (LAR): Brasil, México
- North America Region (NABU): United States, Canada
- Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

- Privacy Statement
- Legal Policies