MILE TEA: CYBER ESPIONAGE CAMPAIGN TARGETS ASIA PACIFIC BUSINESSES AND GOVERNMENT AGENCIES

POSTED BY: Kaoru Hayashi on September 14, 2016 5:00 PM

FILED IN: Unit 42
TAGGED: APAC, Elirks, Japan, Logedrut, Micrass, MILE TEA

(This blog post is also available in Japanese.)

In June 2016, Unit 42 published the blog post "Tracking Elirks Variants in Japan: Similarities to Previous Attacks", in which we described the resemblance of attacks using the Elirks malware family in Japan and Taiwan.

Since then, we continued tracking this threat using Palo Alto Networks AutoFocus and discovered more details of the attacks, including target information. We've seen examples of this attack campaign, which we've named "MILE TEA" (MIcrass Logedrut Elirks TEA), appearing as early as 2011, and that it has since expanded the scope of targets. It involves multiple malware families and often tricks targets by sending purported flight e-tickets in email attachments. The identified targets include three separate Japanese trading companies, a Japanese petroleum company, a mobile phone organization based in Japan, the Beijing office of a public organization of Japan, and a government agency in Taiwan.

ATTACK OVERVIEW

Figure 1 shows the number of attacks considered as a part of the MILE TEA campaign since 2011. As we can see, the volume of the threats is small in total.

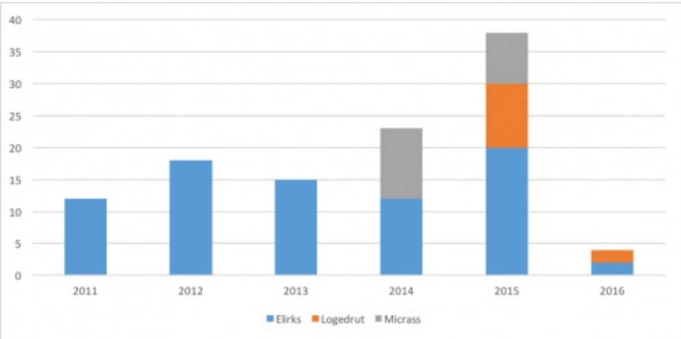


Figure 1 Number of threats used in the attack campaign

In the first three years, most of the reported attacks were from Taiwan. saw infections in a few other countries in Asia, but the number was miniscule. In mid-2013, the target base shifted to Japan. Since 2015, most of the reported attacks are from Japan.

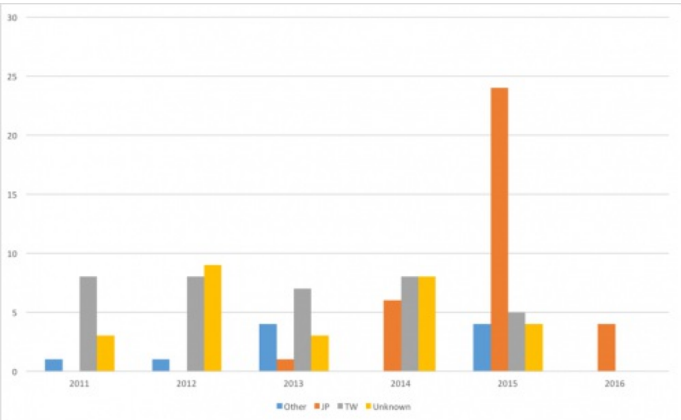


Figure 2 Reports by countries

The primary infection vector is a spear phishing email with a malicious attachment. Although we collected several document based exploit files (RTF, XLS, and PDF) in this attack campaign, most of the attachments were executable files that, interestingly, suggest a custom malware installer. Attackers often use self-extracting executable files or existing installer packages to reduce development costs if they require dropping multiple files. However, in this campaign, the attacker group created its own installer program with the following features:

- Windows executable with folder icon
- Creates directory with pre-determined name in the same path as the installer
- Copies decoy files into the created directory
- Installs a batch file and malware on Temp Dir
- Executes a batch script to delete the installer

Figure 3 shows examples of the custom installer and its different folder icons.

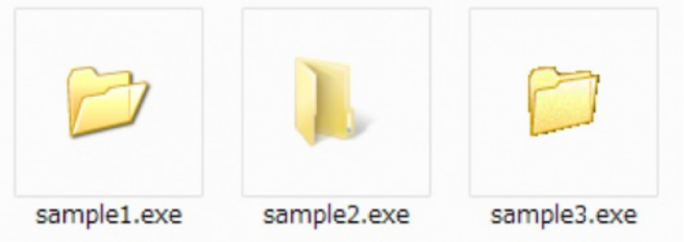


Figure 3 Custom installers with the folder icon

The use of e-flight tickets as phishing lures has been seen repeatedly for a number of years. The following is the list of malicious attachment samples that use this technique. It is the most prevalent lure used by this threat actor to entice targets for this campaign.

Target	Year	SHA256
Japan	2016	71d5bc9404aa2aa40d79cb16837246a31fa3f12b195330a091e3867aa85f1bc6
Taiwan	2015	7b1509051ccacc4676bf491f63c8a8c7c3b42ffd6cbf3d8bb1dd0269424df985
Japan	2014	8c338446764db7478384700df811937dabc3c6747f54fd6325629e22e02de2cc
Taiwan	2014	b393b9774c32de68b35bffd43ace22f9e9d695545de02d8b1d29c8ae38db3488
Taiwan	2014	4607aa975fd9b5aaebe684b26fa31d8ef0840682b148dbcf7f57e9c35d107eb6
Taiwan	2013	f23ab2ee9726c4061b2e0e7f6b9491e384de8103e410871c34b603326b7672da
Taiwan	2013	5de5346613be67e3e3bdf82c215312e30bf5ab07aafd0da0e6967897752e0c1d
Taiwan	2013	1ed808c7909bde7164d81a8c752a62ced116e03cfb6c7502019d84340f04b76a
Taiwan	2012	b6034a3fc6e01729166a4870593e66d9daf0cdff8726c42231662c06358632a7
Taiwan	2012	f18ddcacfe4a98fb3dd9eaffd0feee5385ffc7f81deac100fdbbabf64233dc68

Table 1 Samples of malicious attachments masquerading as E-Ticket

MALWARE

In this MILE TEA campaign, the actor uses the following three malware families as the initial infection by the custom installer. The primary purpose of these families is to establish a bridgehead, collecting system information and downloading additional malware from a remote server.

Malware	Executable Type	Cipher	C2 address from Blog
Elirks	PE, PE64, DLL	TEA, AES	Yes
Micrass	PE	TEA	No
Logedrut	PE, MSIL	DES	Yes

Table 2 Malware characteristics

While many security vendors classify these samples as different malware families, they share functionality, code, and infrastructure, leading us to conclude that they in fact belong to the previously mentioned malware families.

FUNCTIONALITY – BLOG ACCESS

As described in the previous blog post, one of the unique features of Elirks is that it retrieves a command and control (C2) address from a public-facing blog service. When configured, the malware accesses a predetermined blog page, discovers a specific string, and proceeds to decode it with Base64 and decrypts it using the Tiny Encryption Algorithm (TEA) cipher. The same functionality is found in Logedrut, however, instead of using the TEA cipher, it uses DES.

A sample of Logedrut (afe57a51c5b0e37df32282c41da1fdfa416bbd9f32fa94b8229d6f2cc2216486) accesses a free blog service hosted in Japan and reads the following article posted by the threat actor.

2015年 01月 22日

love

doctor fish pKuBzxxnCEeN2CWLAu8tj3r9WJKqbIE+ sech yamatala

Figure 4 Encoded C2 address posted by attacker

The routine called GetAddressByBlog() in Logedrut looks for text between two pre-defined strings. In this particular case, the malware sample will look for test between “doctor fish” and “sech yamatala”. The threat determines encoded text is “pKuBzxxnCEeN2CWLAu8tj3r9WJKqbIE+” and proceeds to handle it using the following function.

```
internal static string GetAddressByBlog(string blogUrl)
{
    Utility.AddLog("GetAddressByBlog");
    string text = Network.HttpGet(blogUrl);
    if (text == null)
    {
        Utility.AddLog("HttpGetError");
        throw new Exception();
    }
    string text2 = Network.m_starttag + "(.*)" + Network.m_endtag;
    Utility.AddLog("Pattern : " + text2);
    Regex regex = new Regex(text2);
    if (!regex.IsMatch(text))
    {
        Utility.AddLog("did not found tag");
        throw new Exception("did not found tag");
    }
    string income = regex.Match(text).Groups[1].Value.Trim();
    Utility.AddLog("Is Match");
    return Utility.DES_DeCrypt(income);
}
```

Figure 5 Code finding encoded C2 address from blog

This code deciphers the string with BASE64 and DES. So far all Logedrut samples use exactly the same key, 1q2w3e4r, for decryption. The following Python code can be used to decode the C2 address.

```
import base64
import Crypto.Cipher.DES

encoded_string = "pKuBzxxnCEeN2CWLAu8tj3r9WJKqblE+"
iv = key = "1q2w3e4r"

decoded_string = base64.b64decode(encoded_string)
des = Crypto.Cipher.DES.new(key, Crypto.Cipher.DES.MODE_CBC, iv)
decrypted_string = des.decrypt(decoded_string)

print decrypted_string
```

CODE – TEA WITH XOR

Elirks and Micrass employ exactly the same TEA cipher. TEA is a block cipher that operates against 64-bit (8 bytes) of data at a time to encrypt and decrypt. The author of the code added and extra cipher operation by XORing data when a block size is less than 64 bits. For example, if the encrypted data length is 248 bits (31 bytes), the code in both malware samples decrypts the first three blocks (64 x 3 = 192 bits) with TEA. The final block is only 56 bits (248 – 192 = 56), so the code uses a simple XOR operation against the remaining data. This supplement to TEA has not been widely used, and all Elirks and Micrass samples have the same static key (2D 4E 51 67 D5 52 3B 75) for the XOR operation. Due to these similarities, we can conclude that the author of both families may be the same, or has access to the same source code.

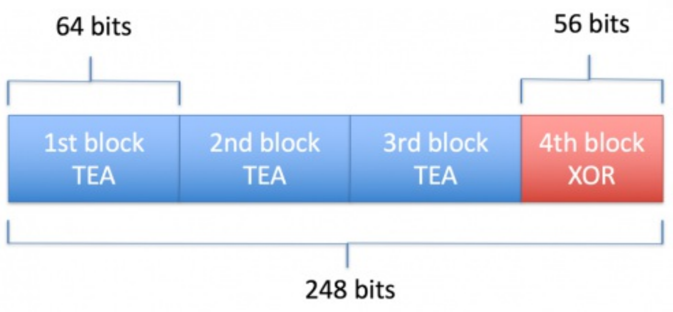


Figure 6 TEA with XOR Cipher in Elirks and Micrass

INFRASTRUCTURE – C2 SERVERS

Based on our analysis, we see that only a handful samples share the same infrastructure directly. The threat actors carefully minimize reusing C2 domains and IP addresses among their malware samples, and yet they prefer using servers located in Hong Kong no matter where the target resides.

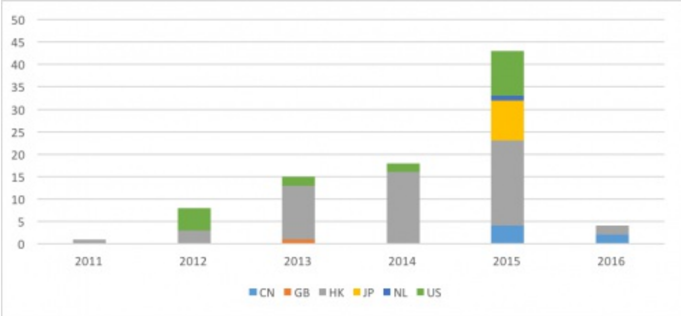


Figure 7 Location of C2 servers

TARGET ANALYSIS

IDENTIFYING TARGETS FROM SPEAR-PHISHING EMAILS

We found a spear phishing email sent to a government agency in Taiwan on March 2015. The email sender masquerades as an airline company, and the RAR archive attachment contains the custom installer named Ticket.exe that drops Ticket.doc and Micrass malware.

Figure 8 Spear-phishing email sent to an agency in Taiwan

During the analysis of the email, we came across an article in a Taiwan newspaper from February 2014 that alerted the public about a similar email message being widely distributed that contained a malicious attachment. The only difference between the email messages in Figure 8 and in the news article was the date. The adversary reused the email message more than a year ago.

IDENTIFYING TARGETS FROM DECOY FILES

The most interesting part of this attack campaign is that the threat actor has been using stolen documents from previously compromised organizations to perform additional attacks since early 2015. These documents are not publicly available nor do they look to be created from scratch by the attacker. Because they contain sensitive data tying to the specific business, it is unlikely that a third party would be able to craft them.

The following figure shows the decoy file installed by a sample identified in early April 2015. The file is a weekly report created at the end of March 2015 by a salesperson at a Japanese trading company. The report includes various sensitive information specific to their business.

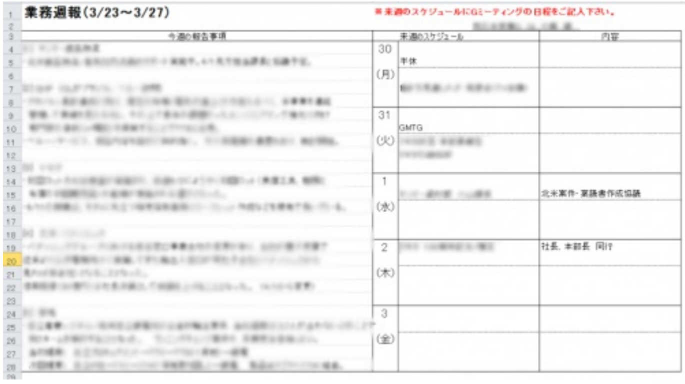


Figure 9 Weekly report from a Japanese trading company

The properties identified within the document indicate that the company name matches the context, and the person who last modified it is the same individual seen in the document itself. Because of this, the file appears legitimate and it’s very unlikely that this document would ever be made publicly available. The threat actor almost certainly stole this document soon after it was created, and reused it as the decoy for next target within a week of the theft.

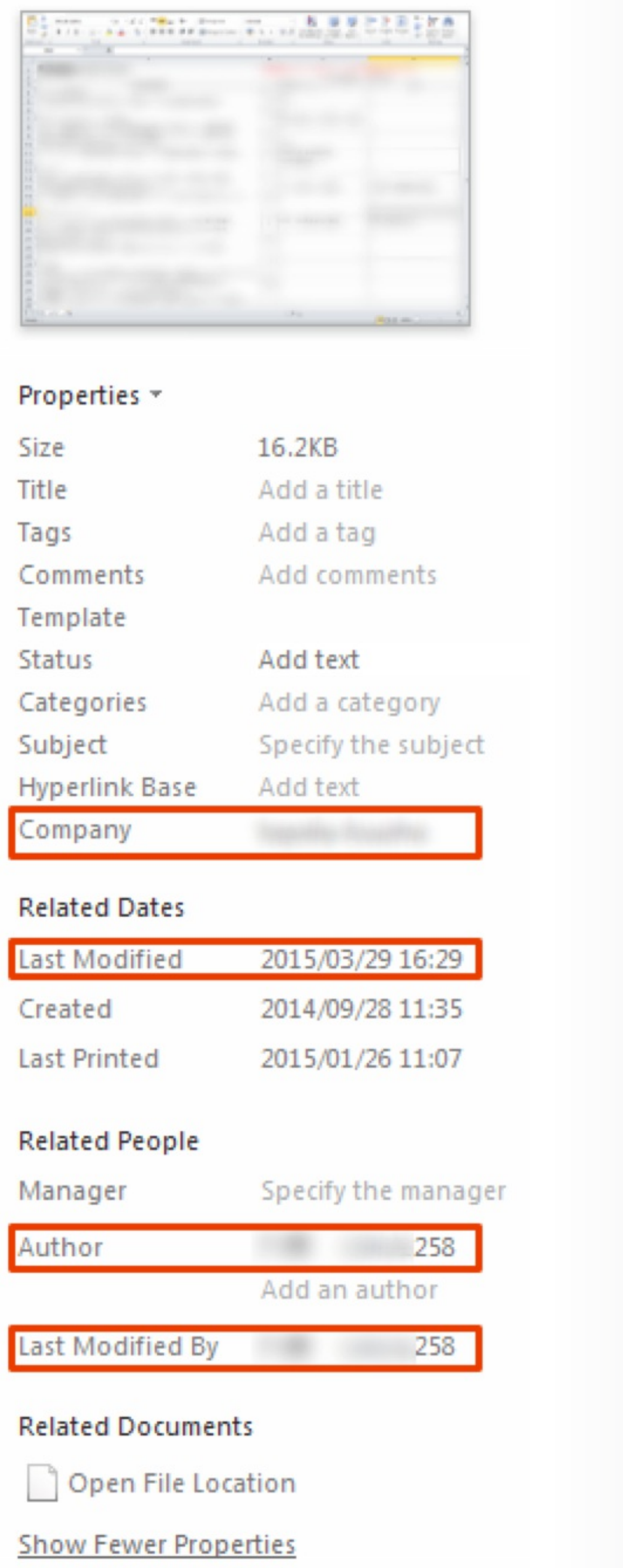


Figure 10 Property of the decoy document

Another installer found in Japan in May 2015 also contained sensitive information. The decoy looks to be a draft version of a legitimate contract addendum between the subsidiary of a Japanese petroleum company based in Australia, and a China-based company. The document provides details of the deal, including price. It contains a bunch of tracked changes by what appears to be two Japanese speaking individuals. We have confirmed that one of the individuals was a manager of an overseas project of the parent company in Japan by the official release of personnel change in 2013. The file is also considered to be stolen from a target organization and used for decoy for the next attack.

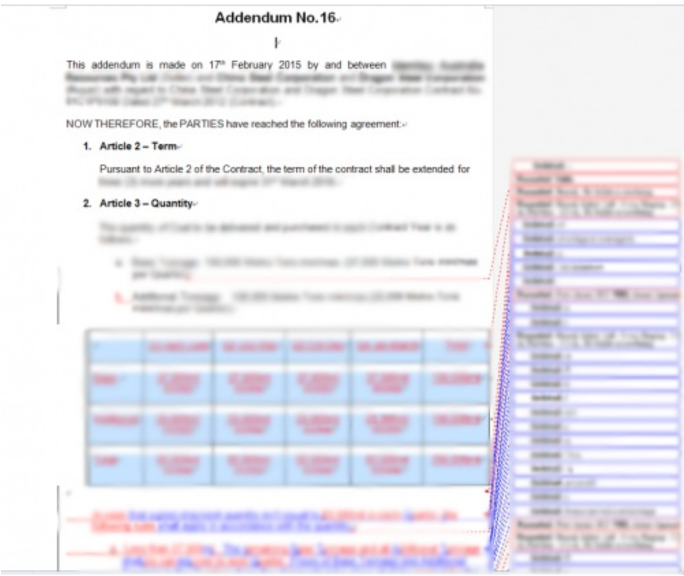


Figure 11 Contract addendum decoy file

In addition to those examples, we found the following decoy files that are likely stolen from previously compromised organizations.

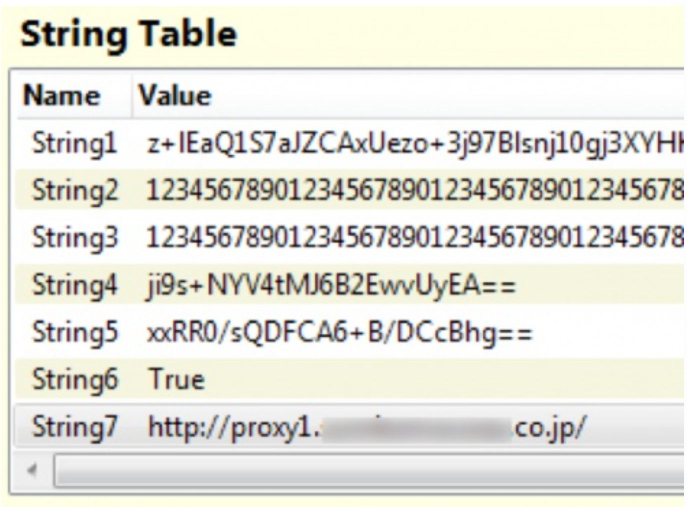
Organization	Type of document
Beijing Office of a public organization of Japan	Budget Report
Another Trading Company in Japan	Internal investigation document
Mobile phone organization in Japan	Inventory of new smartphones

Table 3 Potential source of another decoy file

We cannot confirm whether those files were stolen as part of the MILE TEA campaign or not. Either way, it's difficult to imagine that the threat actor sent those internal documents to entirely different organization or industries. One plausible explanation would be that the threat actors target different persons or departments within same organization or industry.

IDENTIFYING TARGET FROM MALWARE

So far, we have described two trading companies in Japan that are possibly targeted. In addition to these two companies, there is another company in Japan that could be involved in the attack campaign as well. A sample of Logedrut was identified and is capable of communicating with C2 through an internal proxy server in the compromised organization. The sample contains an internal proxy address for a trading company in Japan as seen in String7 in the image below. Thus, the sample is specially crafted for this specific enterprise.



String Table

Name	Value
String1	z+IEaQ1S7aJZCAxUezo+3j97Blsnj10gj3XYHI
String2	12345678901234567890123456789012345678
String3	12345678901234567890123456789012345678
String4	ji9s+NYV4tMJ6B2EwvUyEA==
String5	xxRR0/sQDFCA6+B/DCcBhg==
String6	True
String7	http://proxy1.[illegible]co.jp/

Figure 12 Internal proxy address in Logedrut

CONCLUSION

MILE TEA is five-year-long targeted attack campaign focused on businesses and government agencies in Asia Pacific and Japan. The threat actor behind this maintains and uses multiple malware families, including a custom installer. The actor is interested in organizations that conduct business in multiple countries. The trading companies cover an immensely broad area, from commodity products to aviation around the world. Another possible target is a Japanese petroleum company that has multiple offices and subsidiary companies in overseas countries. A public organization in Japan and a government agency in Taiwan were also targeted.

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

1. WildFire accurately identifies all malware samples related to this operation as malicious.
2. Domains used by this operation have been flagged as malicious in Threat Prevention.
3. AutoFocus users can view malware related to this attack using the "Micrass", "Elirks", and "Logedrut" tags.

INDICATORS OF COMPROMISE

Note: We omitted some hashes containing potentially stolen documents from the compromised organization.

Windows Executable Custom Installer
064474ac22dd28bf2211ca6602946409925b11f1cfa5e593487bf65e033f1057
136978934c8a61e4adff415d4f8f6cd39d110cfa27df2c18367c7036c36e006a
1ed808c7909bde7164d81a8c752a62ced116e03cfb6c7502019d84340f04b76a
37e79e1ee7cde57cf3af80c54851fa3f9bea3a7208c5cdb5bd290d832f1c50c6
4607aa975fd9b5aaebe684b26fa31d8ef0840682b148dbcf7f57e9c35d107eb6
47c489ad097ea2813a993f05d0422361196efa8a7fec08c3f0c0d1d19db9f6a9
5135377eb6db61ace45e88eca753fb08ae4e185176940e786050c0514a775294
5de5346613be67e3e3bdf82c215312e30bf5ab07aafd0da0e6967897752e0c1d
71d5bc9404aa2aa40d79cb16837246a31fa3f12b195330a091e3867aa85f1bc6
7b1509051ccacc4676bf491f63c8a8c7c3b42ffd6cbf3d8bb1dd0269424df985
7b3980734ccef487a7ee1f89fcc19a397782e5f38ecd0549c871e8acd918f092
87a6ec28357409e547f22edba03c1874500636f9860069db51bfe7a351d20481
8c338446764db7478384700df811937dabc3c6747f54fd6325629e22e02de2cc
91569b8a68d004a7d8ef031846dca3e9facb4401d3fac23d4009fcb2e4c4f2c4
ade2eabdf113abeff41a79a7bbbd097187a8e69e16c9e622a53f9f68edc69ec2
b6034a3fc6e01729166a4870593e66d9daf0cdff8726c42231662c06358632a7
b693be834ffdb1865abfd2fe5e3c6f29134579ef2ecbc2837cb1b85bd7e757e0
d50a419daff4290f3870b66ff94050a0cbcd76e278d5c4015a79a6b578e44724
d6935edeb50cab2f1ae90776e4c8bdd709ec78ccc71b1e94f079fb9770b7c220
e32eb45287443d510b1a30009abd14701c4306b817b4c4d83ff1377b4312d807
f18ddcacfe4a98fb3dd9eaffd0feee5385ffc7f81deac100fdbbabf64233dc68
f23ab2ee9726c4061b2e0e7f6b9491e384de8103e410871c34b603326b7672da

RTF File

b8795e8dcbe4198160bab1c75505652a15569d6dd6e74b1eae2321edaa00f5b6

XLS File

b393b9774c32de68b35bffd43ace22f9e9d695545de02d8b1d29c8ae38db3488
b5b2974251e6bb963c0a37f12a167efd5ba702c142cd9f5571090f8838be4335

PDF File

200a4708afe812989451f5947aed2f30b8e9b8e609a91533984ffa55d02e60a2
5806703c28991675aee2e1204f748ce7e2814ea8f2a7ef925693fb52b0ef4d9c
755138308bbaa9fcb9c60f0b089032ed4fa1cece830a954ad574bd0c2fe1f104
bfe0e6ce5d33c498b9d048c33d5943ed4619383eea00ca6b3c613407b7b5ae96
ee6564baf5c5c61f95b8840c1d8a47e84c0704de8062e51c5fa3cf550612a879

Elirks

027ff8faf7952d791e39c9dda392dfce1094a4ceece46dbd2f53cf2ad5f8bc21
0cae035a40fcfc760a2f47b98ab27feaba9cee95d59467ab09b32063ac17df5b
0cffc3fb0b4ebf2a4b8cad4fb2a477737e4f8ca0b45494e541b2f92ee9719fa8
0e317e0fee4eb6c6e81b2a41029a9573d34cebeabab6d661709115c64526bf95
0f1f6838c591a0456881fbcd65d511932d2fa6c16fcb27eb4a793240ef0c25de
1194650bdfeb03940e07718726cfeb49645b089899e216a79cbafe7fae01678a
138993de871eefc72967b61b7c030649e1881be8adacbee933636fb4fc2ae444
1434fa8719602b252bb12e1e0023e86becada3b86ed07e1f7836fdf057dcebf5
1fb47c308bfed89069a4dca561cf818910c25bf2e6bf2679992f01e2da393506
24ae29defeb167cba2dc8b647514e9c44c027c6f2ad6c789ec836358c1007f74
262d7106f1a227f278bcb344bc20186ff4231e1513aa61bd25c1da833cc142c5
27a836f9db61b63a7d90b9c13ec5e7dfdada65eae2860e748ba5dd4ca6918b9b
2dd6ff42d53b01c6f1c4ee3336c3ada53739de587adc78fb011237f926326f61
38ae57f7e565dc51544c7b7c9b890eddeb3da7632a623e16cba5bdfd6141e241
3acc6fec0e7275b3774af1274872d42c0afc330cf48d543ff8fdf4bb4b37ed73

40cc76ef34c03a04ad393b68c2110b0e58ec0a7b9da16fd5005993bd8700b951
45496be07ab8a3fad86980219073a28576106c8bca5c8fd70c882eef0e9df428
53a3c1aa683d296c88bd6565a8b417f09e392ceae4c285464859df1953e75382
569ee23acc18b5ff0f18f02d5010d0e9e9870a9b5845c3618e6f31ee4552c475
58f2790133e5987f6f3eb960c5ad547e149a037b1f5a56526026d8a22f7fa51e
5b01d16a4d39cc30a6dd501d214c8ee4916e46ab338c3437f4cf1ae6f71d1ae6
5d4b91593d1cc110c966a3b3bcca6c02492e6df5dff83cd0653f9ffca9d5256e
5e4377e4d0998c09db357d8cd393c949af66a3cd7592a427752dc876430dbef2
633e849407f22fae3e5c6d2bf1921f1b11074229c797ea1e57a85cbc05880c84
636c3af6ca45f5ebc413fdde9e706603151e4ce081bc73addf666ba6c9d198ba
688e33d45ae76dbbbd0f7462f4736453c36abfbf3d6fd1cca02a8e7ef0ea610a
7902d0cbf32897815c10a68c97f27d23cde38111f1e0167d942d5c6d15423719
7bf2ce5acd108ac5f326ba303dac3096ced8afd3e7c88dc14e58765161fd2c00
82f4bd3abd557513e51b84f85d1ac03cfbd049284416640f624aea08821bcf7c
84117f538361883e7ba3dd6d7825059f1b9378c71726fb70189cbd3d66812997
84fcca9d2f61c4a8b94d4a6ef8a12cf36422ddf409ce860047f1d6f8b193f71c
8587e3a0312a6c4374989cbcca48dc54ddcd3fbd54b48833afda991a6a2dfdea
8597beac6316597dbefb5d5193bdf72fabeebeca9466c1aef6289550c765614b
85a227dd905a3fb458e35c76adfede77a03e65c43b4dff8162f5e438f4e55d65
8616976726d25f25646964edd23e9355efc746a11c5a11ef7d14ab6115b72d75
87f1ca62e1af433342fca7665cda0e608aadf8852e7384654e8074380f34fd0d
8b413fe0149e3bbbef8c40f2fe2c835ea6d8399867d392099984853a772d38ae
8bc8dd186369542d4e97c9967cea667de226b4738c3d6a2249e19a6fbff2109f
8c0a2226d378baa1a682b782163143ce612b790d7cbd46d08a83ebb3bf866f4f
8cbe7a11ae59e607fdba324316925ff1bf16d10b4d8af271901e63873bc2bfb6
91569b8a68d004a7d8ef031846dca3e9facb4401d3fac23d4009fcb2e4c4f2c4
9384bded640a8dda65558f92e8ef34f73ec13540160bf149aa3986e01dc688bb
93c5bd2914a1ebd9584dbe1e0d8de1060e0bea2fa51789ede5f11da25ae5c65b
9d212233e669d61fb1c432c9889f4c723819ece549954ff6f741921534ed6336
9f979a94f47f70c833ac9c3195fc245d58b7830f7b6857e875e07e67c3aa835e
a20b019095b3135f40c075b0bdb1e1ef1c6e7fbb0ce3e643a2222c70e4a1254d
a29a1dfa7142efdcfbc39e35f15d1718502050d81302afd1ba464d705a9afab3
a6f74c22bd7a808a79fbf2e7e71a02aa9755b0bfad2c2888b51e4161dbf8c069
ab1f5290d36fcedb249bb3ed1251663130607fc578a1bf910d9a60eb8ba7de1a
b03ae41d7082405a9f4d74792c7438b0a450dee7fa67f63fcc11c050bc527c68
b6856d07881e24eef676e8766eba258d6ed47359b34134e98be58190927ba22c
bf49ec24eb1bd4e09f4e60a3b72bda0907c2400e3221e3fee28eeff76136b8df
bff33857480038d9ee24cc848140636616a04c90bb863673bb4720ff5a61b5c3
c1c64b167303518f5cf762ae76b6a4026248767e394e0cbc9bc961cd37833937
c4407ce7718eecaa0d09df1352e3bbe13fa9600628bd0a42dbee26d7ff4534a0
c949f811b2d67ab76564223b0c4ae40179b14f892c4f6f6ab5de363dbf4df17f
cd4789bf41c8498ff83b13a53d83cb503e27b3283b2c2585d793a5ea6771d8aa
d1617e66d84da7371884ad31a21f099754784ca585622d3197778d9886d56232
d5db887a8875346a118288062d36ad44eadb2e5d345e2cbf5233f8f36ecf3809
d642f5b4cbfa29ca268b18ed76efc3efef0f4b3866e67b6ef6af32f6cca468bb
d7cd8432b89148bc21e3a9e76970fb8d33b4103af9c94599ca8401c5e6d71a97
e01441c1eb568ca57cb59c1e814b22d5611a53f714bc85eb2be00b08d9b6f13f
e44bd67d0828c375760ebe16a62e73b5eff1540ff587a6c358a63d7d5ab5f5cf
e4ab42e5900ed193f305d6e3a28ac8743b64d1ac5dc2e0e1ef1a927322933c81
e50692aa80020ade381d6fa8751e0f1eabab78e8860c47d95c6bc1e224b02f6c
e929a008dd9c58e2814ecfb84be2cd8df8a809aa2ec64a4a82553047e0507ee5
eaeb778224f16311af071d3f82a4f04eacb6b73b97b001fcd40051a8963050fc
ee9b8e6902b62e76138c9ed8a6d376f35a0361f85519e47b45ee776cf0474f28
f18ddcacfe4a98fb3dd9eaffd0feee5385ffc7f81deac100fdbbabf64233dc68
f6cb59b697cd27359f12228cf11ae5aa21b17e1845ae8007c668319672cdfb33
fdcaac1a818a088e41bcf764493e203089e21bd35521da1c3c999e90eccb99a8

Logedrut

2d9c0f32401404ab515690e052d378b0acdd22e30ce8a6a2ce6e5088b2c62795
4591134a77b3532c85576e7b1942476eb73775d118e49ad215dbbe1c42761760
66c9e75398c202c5c2b917fd0fe9a3089c6a1fa5e74a64c6a2c2b5d6acaf2f14
843b14a44374987ebdd735d23ac89f8aef8c6972510d53d283eb79004c5e3ec7
8be58e9b58727e9195c037810a5e57ec6a9107547e2d4e4b75e299c5f4ad9be0
a205027c7f1241dce0807de7733a23ffc398c64bd2130f2fd17316c2860b5dc1
a74604f65d92579295b4fa16f6cca91fc2a66387eb1c1744b22081fb05aefa16
afe57a51c5b0e37df32282c41da1fdfa416bbd9f32fa94b8229d6f2cc2216486
c267e01e047a0ddfa96fb5c65483532c44647dc7153c149aeeb9833b9952f7b5
cc8844b46972af665739e8fe689412621737bc87ca9f700e873622006d8fc62a
d1373c0be7cdb76b2735d0df87d81db09eb3583f145cdcfe4ac6d1d217de9781
e8186a03a53cba3cfe6b0ea3bcbc7893eb1da84e612060ecfffb8110fa0199a2

Micrass

4bcc727506706634b56cad358828037189898097c363e2ea2147ec253b81a009
674865c337f23ab23b7c866893d179467e5f834ee95a0952aaeb7fa7f3d34573
68ec202ebce297031a7d02ab0417ec01c5fc0a94171b1443d3bfd6ad5f27055e
6b2fea7284bcc4f505b124d216bb33f723a1c93f3a3d5d9a10307d4069950cfb
70c37934e89eb796724a36f32ff654b01341531c980cee09d26c16a1320fcdf7
7b3980734ccef487a7ee1f89fcc19a397782e5f38ecd0549c871e8acd918f092
80db64dc96c59893203074e36852537c0f617e5a5fa73548d65618a16b5f6b4e
94ec1723693c21ff239b33c555dc1e4589a3310fa11bb9fe8b742a9231c36134
a68735dccb378eba908f487906050bacedd73fa8f6503623048f03d71071170c
b7f72805660dc2f76c75d7440cfdf98831ccb5e49985b2f476a0c7b336c618c4
bf58614f2e5b195ce1ee1c096c1b6b560e81d2a31e7ad04522d5d705c2788293
cf7d2d2efaf0eb483cc3152b568ebc45ca0540de2ee57ce3536ae20d7d4a268d
e205a7287d624ef4690da26d9ec44f008ee17efd8ff83c18364e8727215ee4f1
e4351c9f8862677bfc1d2992922ac9985a05504f6050e6916fd7bae3b1501810
e78f1d60aea0652d65275c40e88be9409eb9117dc5c1f8aac122eed338054f16

Command and Control Servers

124rsdtw4r23rsae.4pu[.]com
account.yahoo-account-tw[.]com
asp.domain-googletw[.]com
atashaerlanmuscle.nikitacommonprofessional.cloudns[.]info
billyxcatch.garfieldmercyscream.cloudns[.]eu
chargewike.google-robot[.]com
dns.pchome-shop[.]com
dockcharge.msn2013[.]com
dueyamata.ddo[.]jp
ewr235rew.gsn-operation[.]com
flights.marketddy[.]com
googlehostlogin.hopto[.]org
hiair.henet-web[.]net
hotlogin.ddo[.]jp
indication.google-robot[.]com
islam.youtubesitegroup[.]com
jumpintothesea.seesaa[.]net
kmtgogogo.bluestartw[.]com
likyamaha.msn2013[.]com
lovetamakata.mywww[.]biz
lovetamaya.mywww[.]biz
lovetrick2014.redirectme[.]net
mail-asp.domain-googletw[.]com
mails.domain-googletw[.]com
makoidata.msn2013[.]com
mis.domain-googletw[.]com
pls.utvsoft[.]com
press.ufoneconference[.]com
rdane.msn2013[.]com
reposibility2014.ddo[.]jp
sce.hopto[.]org
server.henet-web[.]net
servers.domain-googletw[.]com
service.net-seed[.]com
sftp.domain-googletw[.]com
siteadmin.yahoo-account-tw[.]com
takamato.4pu[.]com
taoyato.domain-googletw[.]com
tomatopota.4pu[.]com
trains.pchome-shop[.]com
trustlogin.ddo[.]jp
trustly.google-robot[.]com
twitter.google-robot[.]com
vmail.net-seed[.]com
webmail.domain-googletw[.]com
www.vaseline.dumb1[.]com
xuite.henet-web[.]net
yahamata.google-robot[.]com
yourservers.blog-pixnet[.]com
zoe.minidns[.]net
101.1.25[.]40
101.1.25[.]58
101.1.25[.]90
103.17.119[.]137
103.20.192[.]248

103.245.209[.]125
103.245.209[.]153
103.245.209[.]21
103.245.209[.]62
103.28.45[.]241
103.39.109[.]30
103.39.109[.]51
103.39.109[.]66
103.39.109[.]68
103.59.45[.]54
113.10.246[.]154
113.10.246[.]172
113.10.246[.]176
128.199.34[.]140
142.91.119[.]136
173.254.227[.]138
175.45.22[.]122
175.45.22[.]233
180.43.171[.]205
202.82.225[.]161
203.124.14[.]131
206.161.216[.]144
210.209.81[.]170
210.209.81[.]172
210.209.81[.]173
210.209.81[.]188
210.209.81[.]192
210.209.81[.]249
210.209.86[.]136
210.209.86[.]158
210.209.86[.]162
210.209.86[.]175
210.209.86[.]176
210.209.86[.]185
23.253.46[.]64
54.178.93[.]212
59.106.98[.]139
59.188.239[.]110
59.188.87[.]17
59.188.87[.]34
74.126.176[.]218
74.126.177[.]92
74.126.183[.]170
95.211.14[.]53
96.46.0[.]178
96.46.0[.]180
96.46.10[.]179
96.46.10[.]181
96.46.10[.]235
96.46.10[.]237