New Wekby Attacks Use DNS Requests As Command and Control Mechanism

posted by: Josh Grunzweig, Mike Scott and Bryan Lee on May 24, 2016 11:30 AM

filed in: Malware, Threat Prevention, Unit 42
tagged: command and control, DNS, pisloader, Wekby

We have observed an attack led by the APT group Wekby targeting a US-based organization in recent weeks. Wekby is a group that has been active for a number of years, targeting various industries such as healthcare, telecommunications, aerospace, defense, and high tech. The group is known to leverage recently released exploits very shortly after those exploits are available, such as in the case of HackingTeamâ€™s Flash zero-day exploit.

The malware used by the Wekby group has ties to the HTTPBrowser malware family, and uses DNS requests as a command and control mechanism. Additionally, it uses various obfuscation techniques to thwart researchers during analysis. Based on metadata seen in the discussed samples, Palo Alto Networks has named this malware family â€˜pisloaderâ€™ .

Infrastructure

The pisloader malware family was delivered via HTTP from the following URL. At the time of writing, this URL was still active.

http://globalprint-us[.]com/proxy_plugin.exe

Other samples hosted on this domain include the following:

http://globalprint-us[.]com/proxy_web_plugin.exe

MD5: E4968C8060EA017B5E5756C16B80B012
SHA256: 8FFBB7A80EFA9EE79E996ABDE7A95CF8DC6F9A41F9026672A8DBD95539FEA82A
Size: 126976 Bytes
Compile Time: 2016-04-28 00:38:46 UTC

This discovered file was found to be an instance of the common Poison Ivy malware family with the following configuration data:

Command and Control Address: intranetwabcam[.]com
Command and Control Port: 80
Password: admin
Mutex:)!VoqA.I5

The domains witnessed in this attack were all registered very shortly prior to being used. The following domains have been witnessed in this attack:

Domain	Description	Registrant Date
globalprint-us[.]com	Hosted Malware	2016-04-26
ns1.logitech-usa[.]com	pisloader C2	2016-04-26
intranetwabcam[.]com	Poison Ivy C2	2016-04-26

Additionally, the following IP resolutions have been observed.

Domain	IP Address	Registrant Organization	Country of Origin
globalprint-us[.]com	107.180.58[.]70	GoDaddy.com LLC	United States
ns1.logitech-usa[.]com	23.252.166[.]89	NexteCloud L.L.C.	United States
intranetwabcam[.]com	23.252.166[.]99	NexteCloud L.L.C.	United States

Initial Dropper

The following sample was discovered initially and is referenced in the subsequent analysis:

MD5: E8D58AA76DD97536AC225949A2767E05
SHA256: DA3261C332E72E4C1641CA0DE439AF280E064B224D950817A11922A8078B11F1
Size: 126976 Bytes
Compile Time: 2016-04-27 14:37:34 UTC

This particular file has the following metadata properties. The references to â€˜pisload2â€™ led to the naming of this malware family.

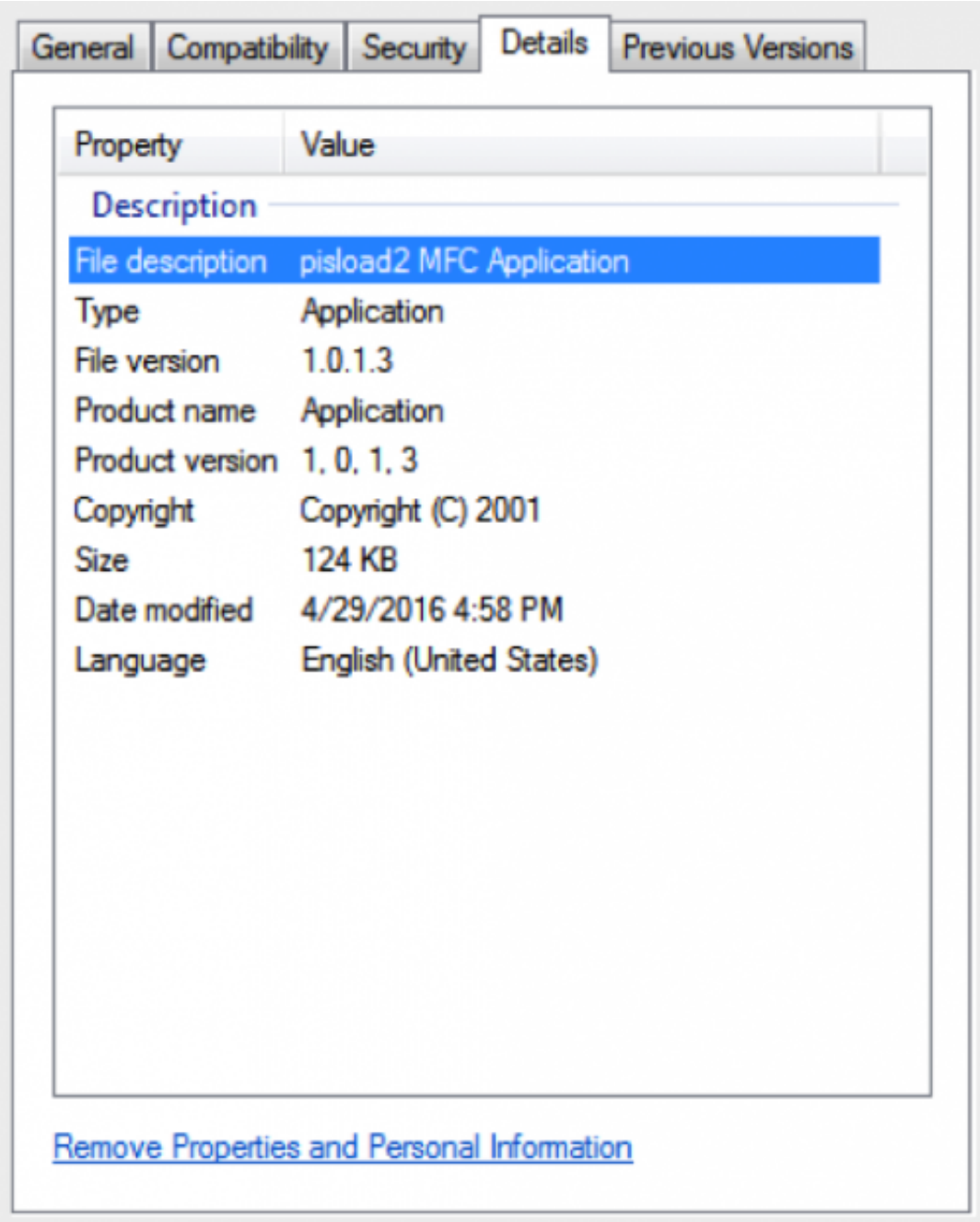

Figure 1 pisloader dropper metadata

The initial dropper contains very simple code that is responsible for setting persistence via the Run registry key, and dropping and executing an embedded Windows executable. Limited obfuscation was encountered, where the authors split up strings into smaller sub-strings and used â€˜strcpyâ€™ and â€˜strcatâ€™ calls to re-build them prior to use. They also used this same technique to generate garbage strings that are never used. This is likely to deter detection and analysis of the sample. The following decompiled code demonstrates this. Comments have been added to show the fully-generated strings.

Figure 2 pisloader dropper building strings and setting persistence

In the above decompiled code, we see that the pisloader is generating the following string, which eventually is called to set the Run registry key.

cmd.exe /c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v lsm /t reg_sz /d â€œ %appdata%\lsm.exeâ€ /f

This particular command will set the HKCU\Software\Microsoft\Windows\CurrentVersion\Run\lsm registry key with a value of â€œ%appdata%\lsm.exeâ€. After this key is set, the malware proceeds to decrypt a two blobs of data with a single-byte XOR key of 0x54. The resulting data is written to the %appdata%\lsm.exe file path.

After this file is written, the malware executes the newly written lsm.exe file, which contains the pisloader payload.

Payload

The following sample was discovered and is referenced in the subsequent analysis:

MD5: 07B9B62FB3B1C068837C188FEFBD5DE9
SHA256: 456FFFC256422AD667CA023D694494881BAED1496A3067485D56ECC8FEFBFAEB
Size: 102400 Bytes
Compile Timestamp: 2016-04-27 13:39:02 UTC

The payload is heavily obfuscated using a return-oriented programming (ROP) technique, as well as a number of garbage assembly instructions. In the example below, code highlighted in red essentially serves no purpose other than to deter reverse-engineering of the sample. This code can be treated as garbage and ignored. The entirety of the function is highlighted in green, where two function offsets are pushed to the stack, followed by a return instruction. This return instruction will point code execution first at the null function, which in turn will point code execution to the â€˜next_functionâ€™ . This technique is used throughout the runtime of the payload, making static analysis difficult.

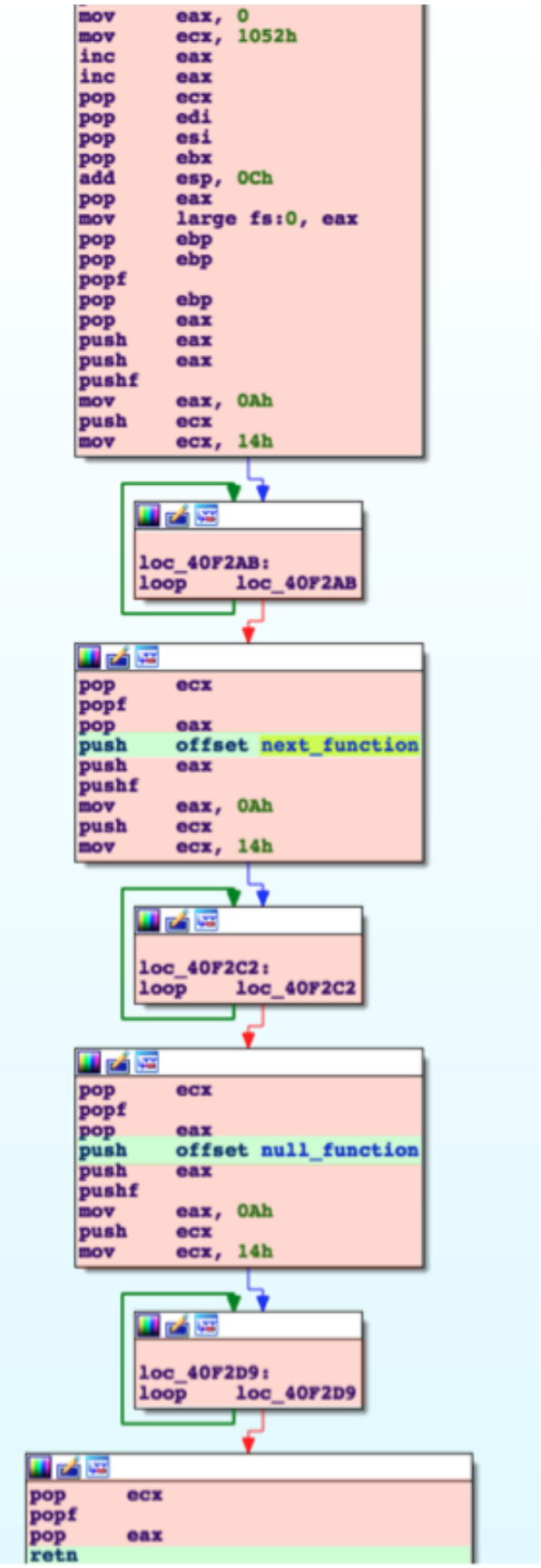

Figure 3 Obfuscated code witnessed in pisloader

The malware is actually quite simplistic once the obfuscation and garbage code is ignored. It will begin by generating a random 10-byte alpha-numeric header. The remaining data is base32-encoded, with padding removed. This data will be used to populate a subdomain that will be used in a subsequent DNS

request for a TXT record.

The use of DNS as a C2 protocol has historically not been widely adopted by malware authors. Notable exceptions include the following:

- FrameworkPOS
- C3PRO-RACCOON
- FeederBot
- Morto
- PlugX Variants

The use of DNS as a C2 allows pisloader to bypass certain security products that may not be inspecting this traffic correctly.

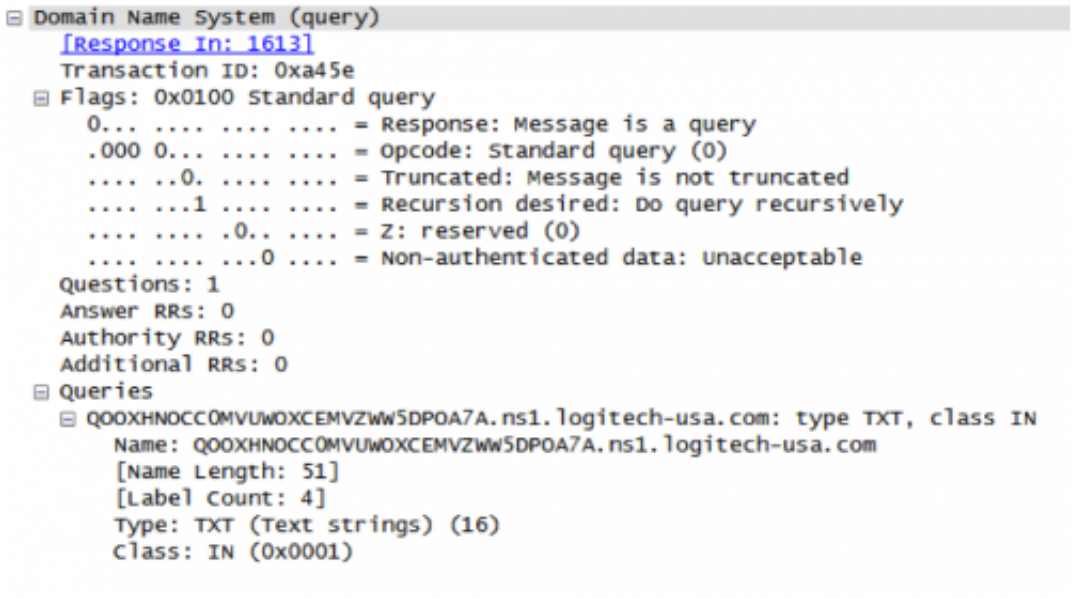

Figure 4 DNS query for TXT record by malware

The pisloader sample will send a beacon periodically that is composed of a random 4-byte uppercase string that is used as the payload. An example of this can be found below:

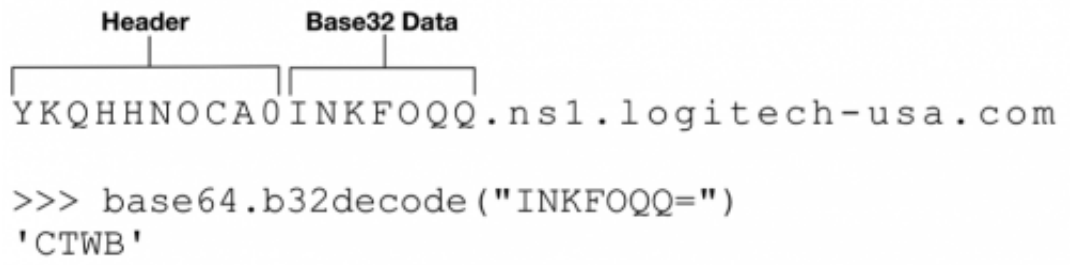

Figure 5 pisloader DNS beacon request

The malware expects various aspects of the DNS responses to be set in a specific way, or else pisloader will ignore the DNS reply. The following DNS flags must be set. Should any additional flags be set, the response will be ignored.

- Response
- Recursion Desired

- Recursion Available

The â€˜Questionsâ€™ field must be set to a value of 0x1. The â€˜Answer Resource Recordsâ€™ field must be set to a value of 0x1. Additionally, the response query subdomain must match the original DNS request.

The remote command and control (C2) server is statically embedded within the malware. A single host of â€˜ns1.logitech-usa[.]comâ€™ is found in this specific sample.

The C2 server will respond with a TXT record that is encoded similar to the initial request. In the response, the first byte is ignored, and the remaining data is base32-encoded. An example of this can be found below.

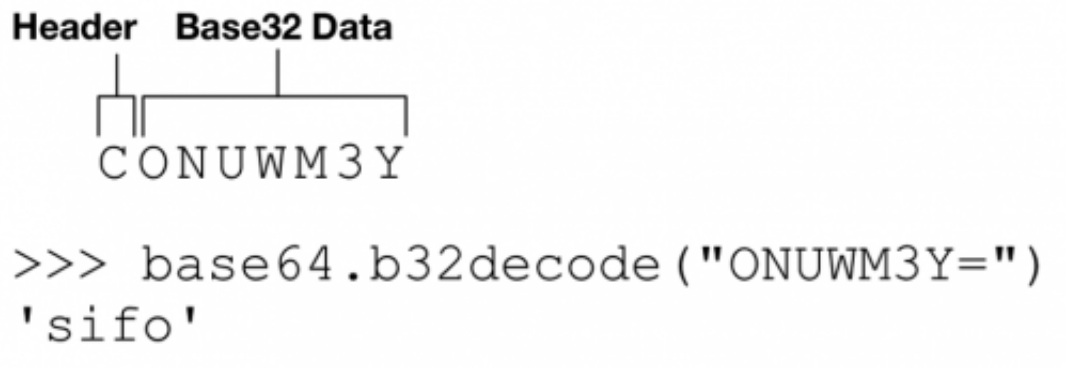

Figure 6 Example TXT response by C2 server

The following commands, and their descriptions are supported by the malware:

- sifo â€“ Collect victim system information
- drive â€“ List drives on victim machine
- list â€“ List file information for provided directory
- upload â€“ Upload a file to the victim machine
- open â€“ Spawn a command shell

Some examples of these commands being used can be seen below. A mock DNS server was used to generate the commands and receive the resulting data.

Example sending the â€˜driveâ€™ command:

```
1 [+] Sending Command: drive | Encoded: CMRZGS5TF
2 [+] Raw Data Received: UMAVMGAGD0IE5FY7CDHJOHYRB2LR6A
3 [+] Decoded Data Received: A:\|C:\|D:\|
```

Example sending the â€˜openâ€™ command:

```
1  [+] Sending Command: open | Encoded: CN5YGK3Q
2  [+] Raw Data Received: ULCBMGAGCAJVUWG4TPONXWM5BAK5UW4ZDPO5ZSAW2WMVZHG2LP
```

```
3  [+] Raw Data Received: ATABMGAGCBNYQDMLRRFY3TMMBRLUGQUQ3POB4XE2LHNB2CAKDD
4  [+] Raw Data Received: HTPDMGAGCCFEQDEMBQHEQE22LDOJXXG33GOQQEG33SOBXXEYLU
5  [+] Raw Data Received: BNJWMGAGCDNFXW4LRAEBAWY3BAOJUWO2DUOMQHEZLTMVZHMZLE
6  [+] Raw Data Received: UARCMGAGCEFYGQUDIKIM5FYVLTMVZHGXCKN5ZWQICHOJ2W46TX
7  [+] Raw Data Received: UJRAMGAGC0MVUWOXCEMVZWW5DPOA7A
8  [+] Decoded Data Received: Microsoft Windows [Version 6.1.7601]
9  Copyright (c) 2009 Microsoft Corporation. All rights reserved.
10
11 C:\Users\Josh Grunzweig\Desktop>
```

Example sending the â€˜sifoâ€™ command:

```
1 [+] Sending Command: sifo | Encoded: CONUWM3Y
2 [+] Raw Data Received: FUBWMGAGIANQ6TCNZSFYYTMLRRFYYTKMZGMM6VOSKOFVGEUTCW
3 [+] Raw Data Received: PGHRMGAGIBGJHEWSKPJNICAW2KN5ZWQICHOJ2W46TXMVUWOXJG
4 [+] Raw Data Received: MMAZMGAGI0N46TMLBRFQZTE
5 [+] Decoded Data Received: l=172.16.1.153&c=WIN-LJLV2NKIOKP [Josh Grunzweig]&o=6,1,32
```

Example listing the contents of the C:\ drive:

```
  [+] Sending Command: list C:\ | Encoded: CNRUXG5BAIM5FY
  [+] Raw Data Received: QKTUMGAGLAGB6CIUTFMN4WG3DFFZBGS3T4GIYDCNJPGAZS6MRW
  [+] Raw Data Received: EKNPMGAGL0EAYTIORUGA5DKN34GB6DEMS6
1 [+] Raw Data Received: RKMAMGAGLAGF6GC5LUN5SXQZLDFZRGC5D4GIYDAOJPGA3C6MJQ
2 [+] Raw Data Received: NMSIMGAGL0EAZDCORUGI5DEMD4GI2HYMZSLY
3 [+] Raw Data Received: OHRWMGAGLAGB6EE33POR6DEMBRGUXTAMZPGI3CAMJWHIZDIORQ
4 [+] Raw Data Received: DPDUMGAGL0GJ6DA7BSGJPA
5 [+] Raw Data Received: WIKGMGAGLAGF6GE33PORWWO4T4GIYDCNBPGA3C6MRYEAYDAORS
6 * Truncated*
7 [+] Decoded Data Received: 0|$Recycle.Bin|2015/03/26 14:40:57|0|22^1|autoexec.bat|2009/06/10 21:42:20|24|32^0|Boot|2015/03/26
8 16:24:02|0|22^1|bootmgr|2014/06/28 00:21:34|391640|39^1|BOOTSECT.BAK|2015/03/26 16:35:39|8192|39^1|config.sys|2009/06/10
9 21:42:20|10|32^0|Documents and Settings|2009/07/14 04:53:55|0|9238^1|Example.log|2016/02/09
10 20:17:55|0|32^1|pagefile.sys|2016/04/25 14:09:20|1660411904|38^0|PerfLogs|2009/07/14 02:37:05|0|16^0|Program Files|2016/02/29
   15:59:43|0|17^0|ProgramData|2016/02/02 17:28:04|0|8210^0|Python27|2016/02/25 16:39:37|0|16^0|Recovery|2015/03/26
   14:39:57|0|8214^0|System Volume Information|2016/02/29 16:00:19|0|22^0|Users|2015/03/26 14:39:58|0|17^0|Windows|2016/02/12
   10:20:21|0|16^^end^
```

The sifo command above uses the printf format string of â€˜l=%s&c=%s&o=%sâ€™ . This is consistent with previous versions of HTTPBrowser, which is another malware family frequently used by the Wekby group.

Additionally, a number of commands themselves, such as the â€˜listâ€™ , â€˜driveâ€™ , and â€˜uploadâ€™ commands are consistent with HTTPBrowser. The formatted responses from these commands are also identical. A known HTTPBrowser sample was spotted with similar metadata as the discussed pisloader sample, which adds further credibility that pisloader is likely a variant of this malware family.

Additionally, the code used to generate these commands is available via GitHub.

Conclusion

The Wekby group continues to target various high profile organizations using sophisticated malware. The pisloader malware family uses various novel techniques, such as using DNS as a C2 protocol, as well as making use of return-oriented programming and other anti-analysis tactics.

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

- WildFire correctly identifies all pisloader samples as malicious
- A pisloader AutoFocus tag has been created in order to track this malware family
- All domains/IPs used in this attack have been flagged as malicious.
- An IPS rule has been created to detect pisloader DNS traffic

Appendix

External Resources

- https://blog.anomali.com/evasive-maneuvers-the-wekby-group-attempts-to-evade-analysis-via-custom-rop
- http://www.volexity.com/blog/?p=158
- https://www.secureworks.com/research/threat-group-3390-targets-organizations-for-cyberespionage
- https://www.zscaler.com/blogs/research/chinese-cyber-espionage-apt-group-leveraging-recently-leaked-hacking-team-exploits-target-financial-services-firm
- https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html

SHA256 Hashes

da3261c332e72e4c1641ca0de439af280e064b224d950817a11922a8078b11f1
930772d6af8f43f62ea78092914fa8d6b03e8e3360dd4678eec1a3dda17206ed
6852ba95720af64809995e04f4818517ca1bd650bc42ea86d9adfdb018d6b274
9200f80c08b21ebae065141f0367f9c88f8fed896b0b4af9ec30fc98c606129b
4d62caef1ca8f4f9aead7823c95228a52852a1145ca6aaa58ad8493e042aed16
1b341dab023de64598d80456349db146aafe9b9e2ec24490c7d0ac881cecc094
456fffc256422ad667ca023d694494881baed1496a3067485d56ecc8fefbfaeb

Domains

ns1.logitech-usa[.]com
globalprint-us[.]com
intranetwabcam[.]com
login.access-mail[.]com
glb.it-desktop[.]com
local.it-desktop[.]com
hi.getgo2[.]com