



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](#)

33

Like

Tweet

8

G+

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 [HackingTeam'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 'pisloader'.

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

Other samples hosted on this domain include the following:

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

Command and Control Port: 80

Password: admin

Mutex:]!VoqA.l5

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
intranetwbcam[.]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	NexiteCloud L.L.C.	United States
intranetwbcam[.]com	23.252.166[.]99	NexiteCloud 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 'pisload2' led to the naming of this malware family.

Home
Government
Partners
Unit 42 Threat Intelligence
Technical Documentation
Advanced Endpoint Protection



Get Updates

Sign up to receive the latest news, cyber threat intelligence and research from Unit 42.

Business Email

Submit

SUBSCRIBE TO THE RESEARCH CENTER BLOG

Subscribe

CATEGORIES & ARCHIVES

Select a Category

Select a Month

MORE →

RECENT POSTS

[Prevention: Changing the Math of Cybersecurity Through Automated Defense](#)

posted by [Ryan Gillis](#) on July 4, 2016

[Palo Alto Networks News of the Week – July 2, 2016](#)

posted by [Anna Lough](#) on July 2, 2016

[Channel Scoop – July 1, 2016](#)

posted by [Lang Tibbils](#) on July 1, 2016

[Here's a Look at the First Palo Alto Networks Intern Tech Week!](#)

posted by [Courtney Taku](#) on July 1, 2016

[Recent MNKit Exploit Activity Reveals Some Common Threads](#)

posted by [Anthony Kasza](#) on June 30, 2016

MORE →

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 'next_function'. This technique is used throughout the runtime of the payload, making static analysis difficult.

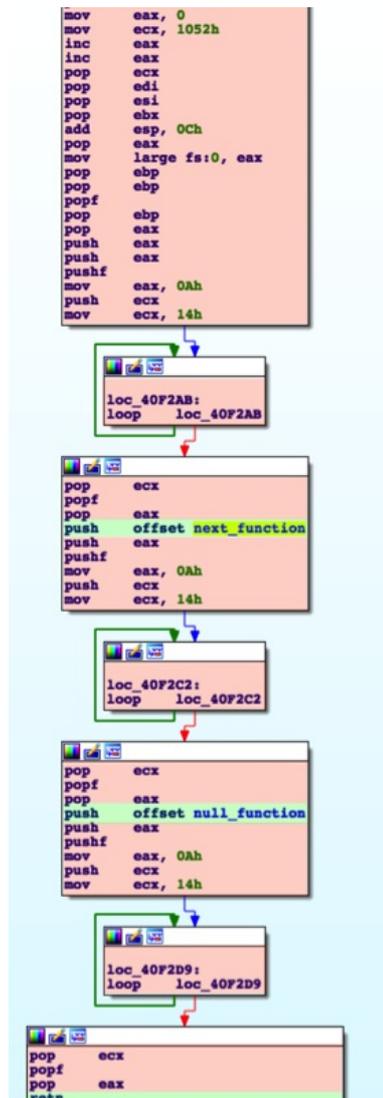


Figure 3 Obfuscated code witnessed in pisloader

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.


```

1 [+] Sending Command: open | Encoded: CNSYGK3Q
2 [+] Raw Data Received: ULCBMGAGCAJVUWG4TPONXWMSBAKSUW4ZDPO5ZSAW2WMV
3 [+] Raw Data Received: ATABMGAGCBNYQDMLRRFY3TMMBRLUGUQ3POB4XE2LHNE
4 [+] Raw Data Received: HTPDMGAGCCFEQDEMBQHEQE22LD0JXXG33GOQQEG33S0B
5 [+] Raw Data Received: BNJWMGAGCDFXW4LRAEBAWY3BA0JUW02DUOMQHEZLTMV
6 [+] Raw Data Received: UARCMGAGCEFYGQUDIKIM5FYVLTVMZHGXCCKN5ZWQICH0J
7 [+] Raw Data Received: UJRAMGAGC0MVUOXCEMVZWW5DPOA7A
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 'sifo' command:

```

1 [+] Sending Command: sifo | Encoded: CONUWM3Y
2 [+] Raw Data Received: FUBWMGAGIANQ6TCNZSFYITMLRRFYTKMZGMM6VOSKOFVC
3 [+] Raw Data Received: PGRHMGAGIBGJHEWSKPJNICAW2KN5ZWQICH0J2W46TXMVU
4 [+] Raw Data Received: MMAZMGAGI0N46TMLBRFQZTE
5 [+] Decoded Data Received: l=172.16.1.153&c=WIN-LJLV2NKIOKP [Josh Gr

```

Example listing the contents of the C:\ drive:

```

1 [+] Sending Command: list C:\ | Encoded: CNRUXG5BAIM5FY
2 [+] Raw Data Received: QKTUMGAGLAGB6CIUTFMN4WG3DFZFZBGS3T4GIYDCNJPGA
3 [+] Raw Data Received: EKNPMGAGL0EAYTIORUGA5DKN34GB6DEMS6
4 [+] Raw Data Received: RKMAMGAGLAGF6GC5LUN5SXQZLDFZRGCS5D4GIYDA0JPGA
5 [+] Raw Data Received: NMSIMGAGL0EAZDCORUGI5DEMD4GI2HYMZSLY
6 [+] Raw Data Received: OHRWMGAGLAGB6EE33POR6DEMBRGUXTAMZPGI3CAMJWHI
7 [+] Raw Data Received: DPDUMGAGL0GJ6DA7BSGJPA
8 [+] Raw Data Received: WIKGMGAGLAGF6GE33PORW04T4GIYDCNBPGA3C6MRYE^
9 * Truncated*
10 [+] Decoded Data Received: 0|$Recycle.Bin|2015/03/26 14:40:57|0|22^

```

The sifo command above uses the printf format string of 'l=%s&c=%s&o=%s'. 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 'list', 'drive', and 'upload' 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
456ffcc256422ad667ca023d694494881baed1496a3067485d56ecc8fefbfaeb

```

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



2 COMMENTS

 Share your thoughts



Marcus on May 26, 2016 9:39 AM said

Great article, well written.



Yasir Irfan on May 28, 2016 10:27 PM said

Very informative and well crafted

POST YOUR COMMENT

Name *

Email *

Website