Operation Poisoned Hurricane

Introduction

Our worldwide sensor network provides researchers at FireEye Labs with unique opportunities to detect innovative tactics employed by malicious actors and protects our clients from these tactics. We recently uncovered a coordinated campaign targeting Internet infrastructure providers, a media organization, a financial services company, and an Asian government organization. The actor responsible for this campaign utilized legitimate digital certificates to sign their tools and employed innovative techniques to cloak their command and control traffic.

Hurricane Electric Redirection

In March of 2014, we detected Kaba (aka PlugX or SOGU) callback traffic to legitimate domains and IP addresses. **Our initial conclusion was that this traffic was the result of malicious actors 'sleeping' their implants, by pointing their command and control domains at legitimate IP addresses.** As this is a popular technique, we did not think much of this traffic at the time.

Further analysis revealed that the HTTP headers of the traffic in question contained a Host: entry for legitimate domains. As we have previously observed malware families that forge their HTTP headers to include legitimate domains in callback traffic, we concluded that the malware in this case was configured in the same way.

An example of the observed traffic is as follows:

```
POST /C542BB084F927229348B2A34 HTTP/1.1
Accept: */*
CG100: 0
CG103: 0
CG107: 61456
CG108: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C)
Host: www.adobe.com
Content-Length: 0
Cache-Control: no-cache
```

As we continued to see this odd traffic throughout the summer we began a search for malware samples

responsible for this behavior. Via this research, we found a malware sample that we believe was responsible for at least some of the strange traffic that we had observed. The identified sample had the following properties:

```
MD5: 52d2d1ab9b84303a585fb81e927b9e01
Size: 180296
Compile Time: 2013-10-15 05:17:37
Import Hash: b29eb78c7ec3f0e89bdd79e3f027c029
.rdata: d7b6e412ba892e9751f845432625bbb0
.text: ed0dd6825e3536d878f39009a7777edc
.data: 1bc25d2f0f3123bedea254ea7446dd50
.rsrc: 91484aa628cc64dc8eba867a8493c859
.reloc: f1df8fa77b5abb94563d5d97e5ccb8e2
RT_VERSION: 9dd9b7c184069135c23560f8fbaa829adc7af6d2047cf5742b5a1e7c5c923cb9
```

This sample was signed with a legitimate digital certificate from the 'Police Mutual Aid Association'. This certificate has a serial number of `'06 55 69 a3 e2 61 40 91 28 a4 0a ff a9 0d 6d 10'`.

Analysis of this Kaba sample revealed that it was configured to directly connect to both www.adobe.com and update.adobe.com. Obviously, this configuration does not make a lot of sense, as the actor would not be able to control their implants from anywhere on the Internet since they did not have direct control over these domains – **unless the attackers were able to re-route traffic destined for these domains from specific victims.** Indeed, further analysis of this Kaba variant revealed that it was also configured to use specific DNS resolvers. This sample **was configured to resolve DNS lookups via Hurricane Electric's nameservers of 216.218.130.2, 216.218.131.2, 216.218.132.2 and 216.66.1.2.**

We found this interesting, so we investigated how these Hurricane Electric's nameservers were configured. **Subsequently, we found that anyone could register for a free account with Hurricane Electric's hosted DNS service.** Via this service, anyone with an account was able to register a zone and create A records for the registered zone and point those A records to any IP address they so desired. **The dangerous aspect of this service is that anyone was able to hijack legitimate domains such as adobe.com. Although these nameservers are not recursors and were not designed to be queried directly by end users, they were returning results if queried directly for domains that were configured via Hurricane Electrics public DNS service. Furthermore, Hurricane Electric did not check if zones created by their users were already been registered or are otherwise legitimately owned by other parties.**

As we continued this research, we identified 21 legitimate fully qualified domain names that had been

hijacked via this technique by at least one APT actor. In addition to the adobe.com domain mentioned above, another one of the poisoned domains is www.outlook.com. A lookup of this domain via Google's DNS resolvers returns expected results:

```
$ dig +short @8.8.8.8 www.outlook.com
www.outlook.com.glbdns2.microsoft.com.
www-nameast.outlook.com.
157.56.240.246
157.56.236.102
157.56.240.214
157.56.241.102
157.56.232.182
157.56.241.118
157.56.240.22
```

A quick lookup of these addresses reveal that Microsoft owns them:

```
157.56.240.246 | 8075 | 157.56.0.0/16 | MICROSOFT-CORP-MSN-A | US |
MICROSOFT.COM | MICROSOFT CORPORATION
157.56.236.102 | 8075 | 157.56.0.0/16 | MICROSOFT-CORP-MSN-A | US |
MICROSOFT.COM | MICROSOFT CORPORATION
157.56.240.214 | 8075 | 157.56.0.0/16 | MICROSOFT-CORP-MSN-A | US |
MICROSOFT.COM | MICROSOFT CORPORATION
157.56.241.102 | 8075 | 157.56.0.0/16 | MICROSOFT-CORP-MSN-A | US |
MICROSOFT.COM | MICROSOFT CORPORATION
157.56.232.182 | 8075 | 157.56.0.0/16 | MICROSOFT-CORP-MSN-A | US |
MICROSOFT.COM | MICROSOFT CORPORATION
157.56.241.118 | 8075 | 157.56.0.0/16 | MICROSOFT-CORP-MSN-A | US |
MICROSOFT.COM | MICROSOFT CORPORATION
157.56.240.22 | 8075 | 157.56.0.0/16 | MICROSOFT-CORP-MSN-A | US |
MICROSOFT.COM | MICROSOFT CORPORATION
```

However, as recently as August 4, 2014 a lookup of the same www.outlook.com domain via Hurricane Electric's resolvers returned entirely different results[1]:

```
$ dig +short @216.218.130.2 www.outlook.com
59.125.42.167
```

$ dig +short @216.218.131.2 www.outlook.com 59.125.42.167

$ dig +short @216.218.132.2 www.outlook.com 59.125.42.167

$ dig +short @216.66.1.2 www.outlook.com 59.125.42.167

$ whois -h asn.shadowserver.org 'origin 59.125.42.167' 3462 | 59.125.0.0/17 | HINET | TW | HINET.NET | DATA COMMUNICATION BUSINESS GROUP

Passive DNS research on the 59.125.42.167 IP address revealed that multiple APT actors have previously used this IP address.

IP Address	Domain	First Seen	Last Seen
59.125.42.167	ml65556.gicp[.]net	2014-06-23	2014-07-23
59.125.42.167	wf.edsplan[.]com	2014-05-12	2014-05-14
59.125.42.167	gl.edsplan[.]com	2014-05-12	2014-05-14
59.125.42.167	unix.edsplan[.]com	2014-05-12	2014-05-14

Additional researched uncovered more Kaba samples that were configured to leverage Hurricane Electric's public DNS resolvers. Another sample has the following properties:

```
MD5: eae0391e92a913e757ac78b14a6f079f
Size: 184304
Compile Time: 2013-11-26 17:39:25
Import Hash: f749528b1db6fe5aee61970813c7bc18
Text Entry: 558bec83ec1056ff7508ff1518b00010
.rdata: 747abda5b3cd3494f056ab4345a909e4
.text: 475c20b8abc972710941ad6659492047
.data: d461f8f7b3f35b7c6855add6ae59e806
.rsrc: b195f57cb5e605cb719469492d9fe717
.reloc: d6b23cb71f214d33e56cf8f6a10c0c10
RT_VERSION: 9dd9b7c184069135c23560f8fbaa829adc7af6d2047cf5742b5a1e7c5c923cb9
```

This sample is signed with a recently expired digital certificate from 'MOCOMSYS INC'. This certificate has a serial number of '`03 e5 a0 10 b0 5c 92 87 f8 23 c2 58 5f 54 7b 80`'.

This sample used Hurricane Electric's public DNS resolvers to route traffic to the hijacked domains of www.adobe.com and update.adobe.com. We also noted that this sample was configured to connect directly to 59.125.42.168 – **one IP address away from the IP that received traffic from the hijacked www.outlook.com domain.**

Passive DNS research revealed that this IP hosted the same set of known APT domains listed above:

IP Address	Domain	First Seen	Last Seen

59.125.42.168	ml65556.gicp[.]net	2014-04-23	2014-07-24
59.125.42.168	wf.edsplan[.]com	2014-04-23	2014-05-14
59.125.42.168	gl.edsplan[.]com	2014-05-04	2014-05-14
59.125.42.168	unix.edsplan[.]com	2014-05-04	2014-05-14

While this problem does not directly impact users of www.adobe.com, www.outlook.com, or users of the other affected domains, it should not be dismissed as inconsequential. **Actors that adopt this tactic and obfuscate the destination of their traffic through localized DNS hijacks can significantly complicate the job of network defenders.**

Via our sensor network, we observed the actor responsible for this activity conducting a focused campaign. We observed this actor target:

- Multiple Internet Infrastructure Service Providers in Asia and the United States
- A Media Organization based in the United States
- A financial institution based in Asia
- An Asian government organization

Google Code Command and Control

Furthermore, we also discovered this same actor conducting a parallel campaign that leveraged Google Code for command and control. On August 1, 2014 we observed a malicious self-extracting executable (aka sfxrar) file downloaded from 211.125.81.203. This file had the following properties:

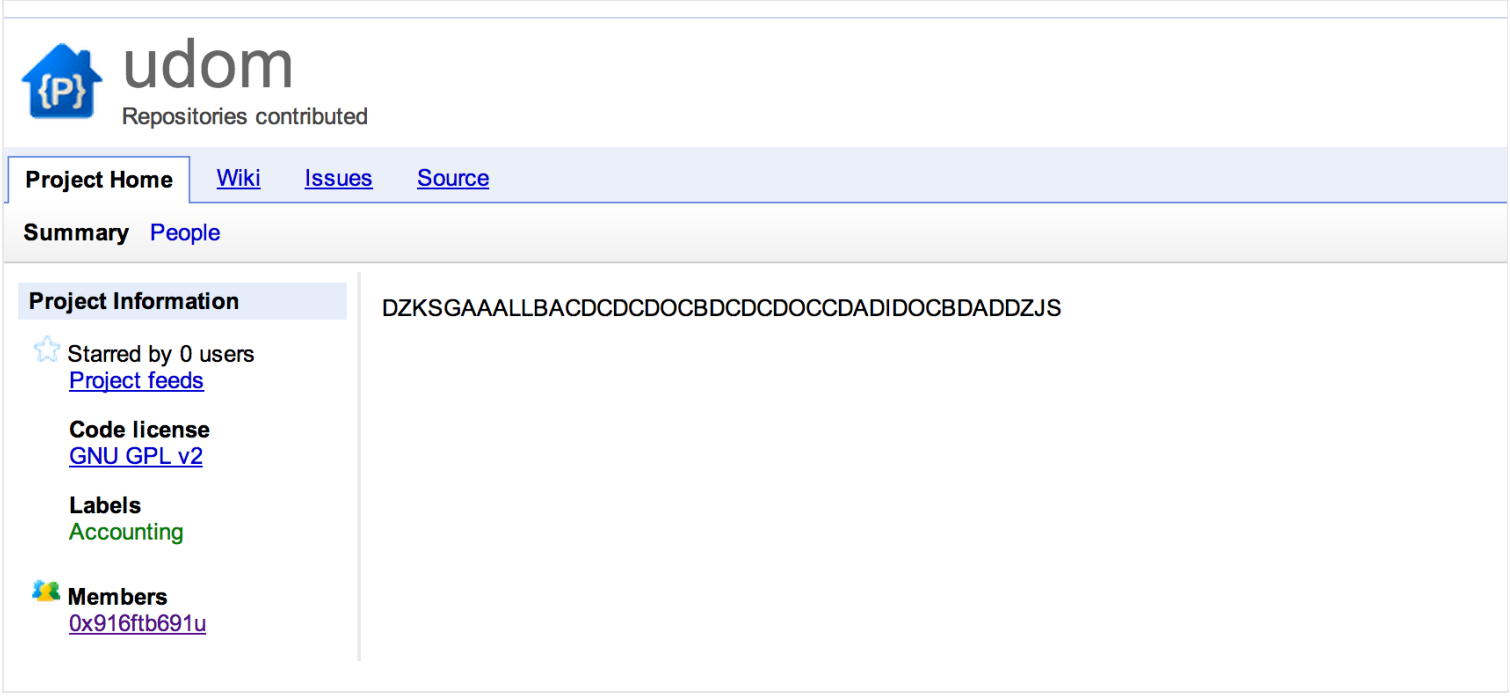
```
MD5: 17bc9d2a640da75db6cbb66e5898feb1
Size: 282800 bytes
```

A valid certificate from 'QTI INTERNATIONAL INC' was used to sign this sfxrar. This certificate had a serial number of '`2e df b9 fd cf a0 0c cb 5a b0 09 ee 3a db 97 b9`'. The sfxrar contained the following files:

File	Size	MD5
msi.dll	11680	029c8f56dd89ceeaf928c3148d13eba7
msi.dll.dat	115218	62834d2c967003ba5284663b61ac85b5
setup.exe	34424	d00b3169f45e74bb22a1cd684341b14a

Setup.exe is a legitimate executable from Kaspersky used to load the Kaba (aka PlugX) files – msi.dll and msi.dll.dat.

These Kaba files are configured to connect to Google Code – specifically code.google.com/p/udom/. On August 1, this Google Code project contained the encoded command "DZKSGAAALLBACDCDCDOCBDCDCDOCCDADIDOCBDADDZJS".[2]



These Kaba files are configured to connect to Google Code – specifically code.google.com/p/udom/. On August 1, this Google Code project contained the encoded command "DZKSGAAALLBACDCDCDOCBDCDCDOCCDADIDOCBDADDZJS".

```
def NewPlugx_C2_redir_decode(s):
```

rvalue = ""
for x in range(0, len(s), 2):
tmp0 = (ord(s[x+1]) – 0×41) << 4

rvalue += chr(ord(s[x]) + tmp0 – 0×41) return rvalue

The command 'DZKSGAAALLBACDCDCDOCBDCDCDOCCDADIDOCBDADDZJS' decodes to 222.122.208.10. **In a live environment, the Kaba implant would then connect to this IP address via UDP.**

Further analysis of project at code.google.com/p/udom/ revealed the project owner, 0x916ftb691u, created a number of other projects. We decoded the commands hosted at these linked projects and found that they issued the following decoded commands:

112.175.143.22
59.125.42.167
153.121.57.213
61.82.71.10
202.181.133.169

61.78.32.139

61.78.32.148

202.181.133.216

59.125.42.168

119.205.217.104

222.122.208.10

112.175.143.16

222.122.208.9

27.122.13.204

It is likely that other yet to be discovered Kaba variants are configured to connect to these related Google Code projects and then redirect to this list of IP addresses.

Passive DNS analysis of these IP addresses revealed connections to the following known malicious infrastructure:

IP Address	Domain	First Seen	Last Seen
27.122.13.204	bq.cppcp[.]com	2014-03-21	2014-05-08
112.175.143.16	uj.verisignss[.]com	2013-06-30	2013-08-13
112.175.143.16	www.verifyss[.]com	2013-06-30	2013-07-22
112.175.143.16	uj.byonds[.]com	2013-06-24	2013-07-22
112.175.143.16	uj.verifyss[.]com	2013-06-30	2013-07-22
59.125.42.168	ml65556.gicp[.]net	2014-04-23	2014-07-24
59.125.42.168	wf.edsplan[.]com	2014-04-23	2014-05-14
59.125.42.168	gl.edsplan[.]com	2014-05-04	2014-05-14
59.125.42.168	unix.edsplan[.]com	2014-05-04	2014-05-14
59.125.42.167	ml65556.gicp[.]net	2014-06-23	2014-07-23
59.125.42.167	wf.edsplan[.]com	2014-05-12	2014-05-14
59.125.42.167	gl.edsplan[.]com	2014-05-12	2014-05-14
59.125.42.167	unix.edsplan[.]com	2014-05-12	2014-05-14
61.78.32.148	door.nexoncorp[.]com	2014-04-30	2014-06-22
61.78.32.148	verisignss[.]com	2014-04-30	2014-06-22
61.78.32.148	th.nexoncorp[.]com	2014-04-30	2014-06-22
61.78.32.148	tw.verisignss[.]com	2014-04-30	2014-06-22
61.78.32.148	sd.nexoncorp[.]com	2014-04-30	2014-06-22
61.78.32.148	mail.nexoncorp[.]com	2014-04-30	2014-06-22
112.175.143.22	door.nexoncorp[.]com	2014-04-01	2014-04-30
112.175.143.22	th.nexoncorp[.]com	2014-04-01	2014-04-30
112.175.143.22	sd.nexoncorp[.]com	2014-04-01	2014-04-30
112.175.143.22	mail.nexoncorp[.]com	2014-04-01	2014-04-30
112.175.143.22	verisignss[.]com	2013-12-29	2014-04-30
112.175.143.22	tw.verisignss[.]com	2013-12-29	2014-04-30

Relationships Between Campaigns

As mentioned above the Kaba variant eae0391e92a913e757ac78b14a6f079f shared a common import hash of f749528b1db6fe5aee61970813c7bc18 with many of the samples listed in this post. This samples was to use Hurricane Electric's nameservers as well as connect directly to the IP address 59.125.42.168.

Note that we identified the same C2 IP 59.125.42.168 via our analysis of the malicious Google Code projects. Specifically, the Google Project at code.google.com/p/tempzz/, which is linked to the project at code.google.com/p/udom/, issued an encoded command that decoded to 59.125.42.168.

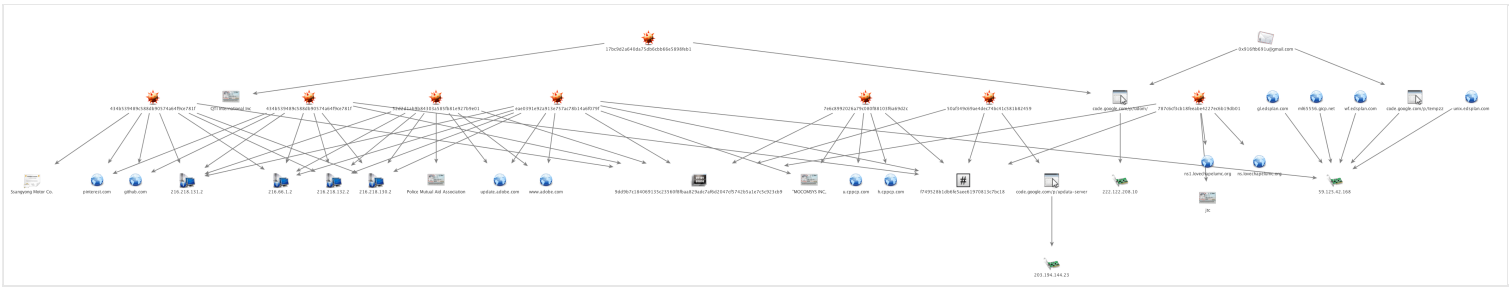
We also identified another related Kaba variant that connected to code.google.com/p/updata-server. This variant had the following properties:

```
MD5: 50af349c69ae4dec74bc41c581b82459
Size: 180600 bytes
Compile Time: 2014-04-01 03:28:31
Import Hash: f749528b1db6fe5aee61970813c7bc18
.rdata: 103beeefae47caa0a5265541437b03a1
.text: e7c4c2445e76bac81125b2a47384d83f
.data: 5216d6e6834913c6cc75f40c8f70cff8
.rsrc: b195f57cb5e605cb719469492d9fe717
.reloc: f7d9d69b8d36fee5a63f78cbd3238414
RT_VERSION: 9dd9b7c184069135c23560f8fbaa829adc7af6d2047cf5742b5a1e7c5c923cb9
```

This sample was signed with a valid digital certificate from 'PIXELPLUS CO., LTD' and had a serial number of '`0f e7 df 6c 4b 9a 33 b8 3d 04 e2 3e 98 a7 7c ce`'.

In addition to sharing the same Import hash of f749528b1db6fe5aee61970813c7bc18 seen in other samples listed throughout this post, 50af349c69ae4dec74bc41c581b82459 contained a RT_VERSION resource of 9dd9b7c184069135c23560f8fbaa829adc7af6d2047cf5742b5a1e7c5c923cb9. This same RT_VERSION was used in a number of other related samples including:

MD5	C2	Uses Hurricane Electric
7e6c8992026a79c080f88103f6a69d2c	h.cppcp[.]comu.cppcp[.]com	NO
52d2d1ab9b84303a585fb81e927b9e01	www.adobe[.]comupdate.adobe[.]com	YES
787c6cf3cb18feeabe4227ec6b19db01	ns.lovechapelumc[.]orgns1.lovechapelumc[.]org	NO



Conclusion

These coordinated campaigns demonstrate that APT actors are determined to continue operations. As computer network defenders increase their capabilities to identify and block these campaigns by deploying more advanced detection technologies, threat actors will continue to adopt creative evasion techniques.

We observed the following evasion techniques in these campaigns:

- The use of legitimate digital certificates to sign malware
- The use of Hurricane Electrics public DNS resolvers to redirect command and control traffic
- The use of Google Code to obfuscate the location of command and control servers

While none of these techniques are necessarily new, in combination, they are certainly both creative and have been observed to be effective. Although the resultant C2 traffic can be successfully detected and tracked, **the fact that the malware appears to beacon to legitimate domains may lull defenders into a false sense of security.** Network defenders should continue to study the evolution of advanced threat actors, as these adversaries will continue to evolve in pursuit of their designated objectives.

Related MD5s

17bc9d2a640da75db6cbb66e5898feb1
eae0391e92a913e757ac78b14a6f079f
434b539489c588db90574a64f9ce781f
7e6c8992026a79c080f88103f6a69d2c
52d2d1ab9b84303a585fb81e927b9e01
787c6cf3cb18feeabe4227ec6b19db01
50af349c69ae4dec74bc41c581b82459
d51050cf98cc723f0173d1c058c12721

Digital Certificates

MOCOMSYS INC, (03 e5 a0 10 b0 5c 92 87 f8 23 c2 58 5f 54 7b 80)
PIXELPLUS CO., LTD., (0f e7 df 6c 4b 9a 33 b8 3d 04 e2 3e 98 a7 7c ce)

Police Mutual Aid Association (06 55 69 a3 e2 61 40 91 28 a4 0a ff a9 0d 6d 10)
QTI INTERNATIONAL INC (2e df b9 fd cf a0 0c cb 5a b0 09 ee 3a db 97 b9)
Ssangyong Motor Co. (1D 2B C8 46 D1 00 D8 FB 94 FA EA 4B 7B 5F D8 94)
jtc (72 B4 F5 66 7F 69 F5 43 21 A9 40 09 97 4C CC F8)

Footnotes

[1] As of August 4, 2014 Hurricane Electric was no longer returning answers for www.outlook.com or the other affected domains.
[2] This same encoding algorithm was previously described by Cassidian at http://blog.cassidiancybersecurity.com/post/2014/01/plugx-some-uncovered-points.html

This entry was posted in Targeted Attack, Threat Research and tagged advanced attack, APT, evasion techniques, kana, plugx by Ned Moran, Joshua Homan and Mike Scott. Bookmark the permalink.