Operation DeputyDog: Zero-Day (CVE-2013-3893) Attack Against Japanese Targets

web.archive.org/web/20130924130243/https://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

September 21, 2013

FireEye has discovered a campaign leveraging the recently announced zero-day CVE-2013-3893. This campaign, which we have labeled 'Operation DeputyDog', began as early as August 19, 2013 and appears to have targeted organizations in Japan. FireEye Labs has been continuously monitoring the activities of the threat actor responsible for this campaign. Analysis based on our Dynamic Threat Intelligence cluster shows that this current campaign leveraged command and control infrastructure that is related to the infrastructure used in the attack on Bit9.

Campaign Details

On September 17, 2013 Microsoft published details regarding a new zero-day exploit in Internet Explorer that was being used in targeted attacks. FireEye can confirm reports that these attacks were directed against entities in Japan. Furthermore, FireEye has discovered that **the group responsible for this new operation is the same threat actor that compromised Bit9 in February 2013.**

FireEye detected the payload used in these attacks on August 23, 2013 in Japan. The payload was hosted on a server in Hong Kong (210.176.3.130) and was named "**img20130823.jpg**". Although it had a .jpg file extension, it was not an image file. The file, when XORed with 0×95, was an executable (MD5: 8aba4b5184072f2a50cbc5ecfe326701).

Upon execution, 8aba4b5184072f2a50cbc5ecfe326701 writes "28542CC0.dll" (MD5: 46fd936bada07819f61ec3790cb08e19) to this location:

C:\Documents and Settings\All Users\Application Data\28542CC0.dll

In order to maintain persistence, the original malware adds this registry key:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\28542CC0

The registry key has this value:

rundll32.exe "C:\Documents and Settings\All Users\Application Data\28542CC0.dll",Launch

The malware (8aba4b5184072f2a50cbc5ecfe326701) then connects to a host in **South Korea** (180.150.228.102). This callback traffic is HTTP over port 443 (which is typically used for HTTPS encrypted traffic; however, the traffic is not HTTPS nor SSL encrypted). Instead, this clear-text callback traffic resembles this pattern:

```
POST /info.asp HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Agtid: [8 chars]08x
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)
Host: 180.150.228.102:443
Content-Length: 1045
Connection: Keep-Alive
Cache-Control: no-cache

[8 chars]08x&[Base64 Content]
```

The unique HTTP header “**Agtid:**” contains 8 characters followed by “08x”. The same pattern can be seen in the POST content as well.

A second related sample was also delivered from 111.118.21.105/css/sun.css on September 5, 2013. The sun.css file was a malicious executable with an MD5 of bd07926c72739bb7121cec8a2863ad87 and it communicated with the same communications protocol described above to the same command and control server at 180.150.228.102.

Related Samples

We found that both droppers, bd07926c72739bb7121cec8a2863ad87 and 8aba4b5184072f2a50cbc5ecfe326701, were compiled on 2013-08-19 at 13:21:59 UTC. As we examined these files, we noticed a unique fingerprint.

These samples both had a string that may have been an artifact of the builder used to create the binaries. This string was “**DGGYDSYRL**”, which we refer to as “DeputyDog”. As such, we developed the following YARA signature, based on this unique attribute:

```
rule APT_DeputyDog_Strings
{
meta:

author = “FireEye Labs”
version = “1.0″
description = “detects string seen in samples used in 2013-3893 0day attacks”
reference = “8aba4b5184072f2a50cbc5ecfe326701″

strings:

$mz = {4d 5a}
$a = “DGGYDSYRL”

condition:

($mz at 0) and $a

}
```

We used this signature to identify 5 other potentially related samples:

MD5	Compile Time (UTC)	C2 Server
58dc05118ef8b11dcb5f5c596ab772fd	2013-08-19 13:21:58	180.150.228.102
4d257e569539973ab0bbafee8fb87582	2013-08-19 13:21:58	103.17.117.90
dbdb1032d7bb4757d6011fb1d077856c	2013-08-19 13:21:59	110.45.158.5
645e29b7c6319295ae8b13ce8575dc1d	2013-08-19 13:21:59	103.17.117.90
e9c73997694a897d3c6aadb26ed34797	2013-04-13 13:42:45	110.45.158.5

Note that all of the samples, except for e9c73997694a897d3c6aadb26ed34797, were compiled on 2013-08-19, within 1 second of each other.

We pivoted off the command and control IP addresses used by these samples and found the following known malicious domains recently pointed to 180.150.228.102.

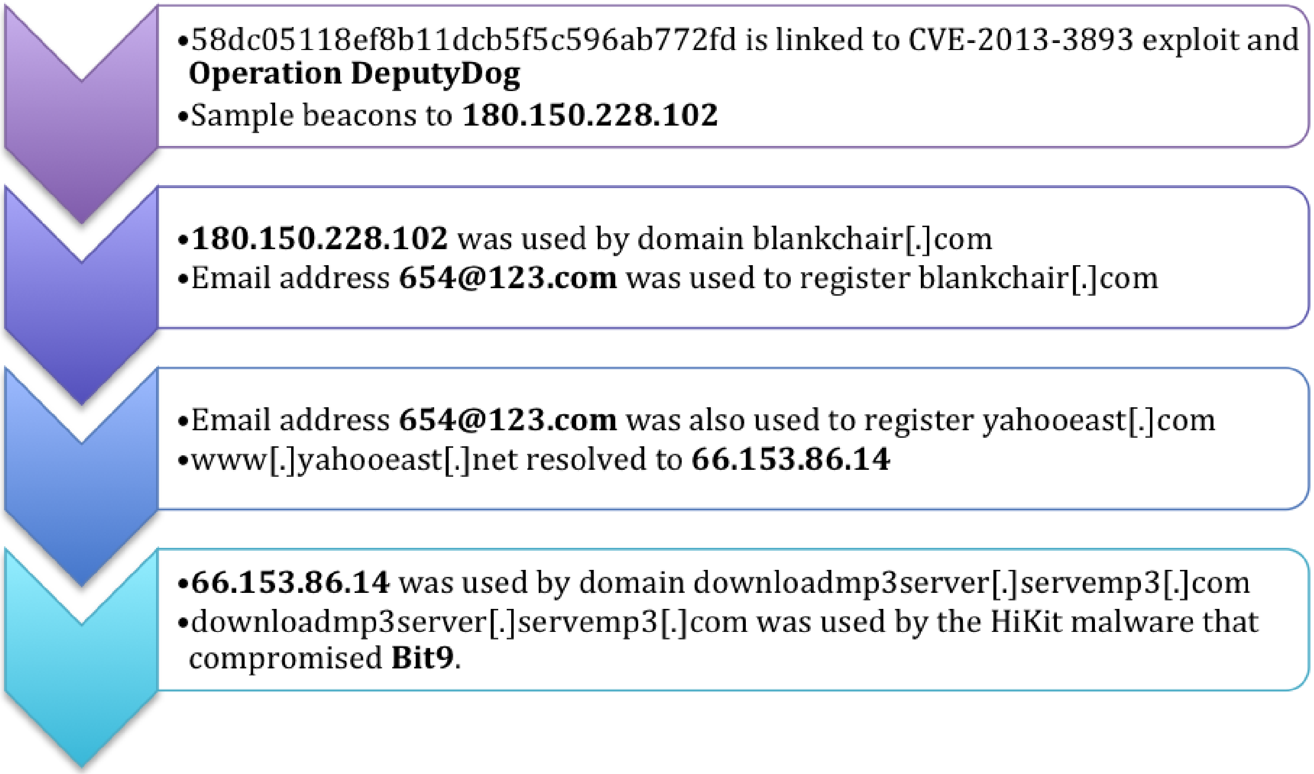
Domain	First Seen	Last Seen
ea.blankchair.com	2013-09-01 05:02:22	2013-09-01 08:25:22
rt.blankchair.com	2013-09-01 05:02:21	2013-09-01 08:25:24
ali.blankchair.com	2013-09-01 05:02:20	2013-09-01 08:25:22
dll.freshdns.org	2013-07-01 10:48:56	2013-07-09 05:00:03

Links to Previous Campaigns

According to Bit9, **the attackers that penetrated their network dropped two variants of the HiKit rootkit**. One of these Hitkit samples connected to a command and control server at downloadmp3server[.]servemp3[.]com that resolved to 66.153.86.14. This same IP address also hosted www[.]yahooeast[.]net, a known malicious domain, between March 6, 2012 and April 22, 2012.

The domain yahooeast[.]net was registered to 654@123.com. This email address was also used to register blankchair[.]com – the domain that we see was pointed to the 180.150.228.102 IP, which is the callback associated with sample 58dc05118ef8b11dcb5f5c596ab772fd, and has been already correlated back to the attack leveraging the CVE-2013-3893 zero-day vulnerability.

Threat Actor Attribution



- 58dc05118ef8b11dcb5f5c596ab772fd is linked to CVE-2013-3893 exploit and **Operation DeputyDog**
- Sample beacons to **180.150.228.102**

- **180.150.228.102** was used by domain blankchair[.]com
- Email address **654@123.com** was used to register blankchair[.]com

- Email address **654@123.com** was also used to register yahooeast[.]com
- www[.]yahooeast[.]net resolved to **66.153.86.14**

- **66.153.86.14** was used by domain downloadmp3server[.]servemp3[.]com
- downloadmp3server[.]servemp3[.]com was used by the HiKit malware that compromised **Bit9**.

Conclusion

While these attackers have a demonstrated previously unknown zero-day exploits and a robust set of malware payloads, using the techniques described above, it is still possible for network defense professionals to develop a rich set of indicators that can be used to detect their attacks. This is the first part of our analysis, we will provide more detailed analysis on the other components of this attack in subsequent blog post.