The EPS Awakens - Part 2 « Threat Research

By by Ryann Winters , FireEye Threat Intelligence | Threat Research, Targeted Attack

On Wednesday, Dec. 16, 2015, FireEye published The EPS Awakens, detailing an exploit targeting a previously unknown Microsoft Encapsulated Postscript (EPS) *dict* copy use-after-free vulnerability that was silently patched by Microsoft on November 10, 2015. The blog described the technical details of the vulnerability, and the steps needed to bypass the EPS filter and obtain full read and write access to the system memory.

In this follow-up blog, we discuss the operational details of the spear phishing campaigns associated with the exploit. Specifically, we detail the lures, attachments, targeting and malware, and examine the China-based advanced persistent threat (APT) group responsible for one of the observed attacks.

Activity Summary

Between November 26, 2015, and December 1, 2015, known and suspected China-based APT groups launched several spear phishing attacks targeting Japanese and Taiwanese organizations in the high-tech, government services, media and financial services industries. Each campaign delivered a malicious Microsoft Word document exploiting the aforementioned EPS *dict* copy use-after-free vulnerability, and the local Windows privilege escalation vulnerability CVE-2015-1701. The successful exploitation of both vulnerabilities led to the delivery of either a downloader that we refer to as IRONHALO, or a backdoor that we refer to as ELMER.

Thanksgiving Day Parade

On November 26, 2015, a suspected China-based APT group sent Japanese defense policy-themed spear phishing emails to multiple Japanese financial and high-tech companies. As shown in Figure 1, the emails originated from the Yahoo! email address **mts03282000@yahoo.co[.]jp**, and contained the subject "**新年号巻頭言の送付**" (Google Translation: Sending of New Year No. Foreword).

```
XMailer: YahooMailWebService/0.8.111_67
Date: Thu, 26 Nov 2015 12:11:23 +0900 (JST)
From: mts03282000@yahoo.co[.]jp
Reply-To: mts03282000@yahoo.co[.]jp
Subject: 新年号巻頭言の送付
To: <redacted>
```

Figure 1. November 26, 2015 Phish SMTP header

Each phishing message contained the same malicious Microsoft Word attachment. The malicious attachment resembled an article hosted on a legitimate Japanese defense-related website, as both discussed national defense topics and carried the same byline. The lure documents also used the Japanese calendar, as indicated by the 27th year in the Heisei period. This demonstrates that the threat actors understand conventional Japanese date notation.

IRONHALO Downloader

Following the exploitation of the EPS and CVE-2015-1701 vulnerabilities, the exploit payload drops either a 32-bit or 64-bit binary containing an embedded IRONHALO malware sample. IRONHALO is a downloader that uses the HTTP protocol to retrieve a Base64 encoded payload from a hard-coded command-and-control (CnC) server and uniform resource locator (URL) path.

The encoded payload is written to a temporary file, decoded and executed in a hidden window. The encoded and decoded payloads are written to files named igfxHK[%rand%].dat and igfxHK[%rand%].exe respectively, where [%rand%] is a 4-byte hexadecimal number based on the current timestamp.

Artifact	Filename	MD5 Hash
IRONHALO	AcroRd32Info.exe.exe	a8ccb2fc5fec1b89f778d93096f8dd65
Encoded payload	igfxHK[%rand%].dat	<varies>
Decoded payload	igfxHK[%rand%].exe	<varies>

Table 1. IRONHALO artifacts

IRONHALO persists by copying itself to the current user's Startup folder. This variant sends an HTTP request to a legitimate Japanese website using a malformed User-Agent string, as shown in Figure 2. The threat actors likely compromised the legitimate site and attempted to use it as a staging server for second-stage payloads.

```
GET /syougyou/images/index.php HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0(compatible;MSIE 8.0;Windows NT 6.1)
Connection: Keep-Alive
Host: www.<redacted>[.]com
Cache-Control: no-cache
```

Figure 2. IRONHALO HTTP GET request

December to Remember

On December 1, 2015, threat actors launched two additional spear phishing attacks exploiting the undisclosed EPS vulnerability and CVE-2015-1701. Unlike the Nov. 26 campaign, these attacks targeted Taiwanese governmental and media and entertainment organizations. Moreover, the exploit dropped a different malware payload, a backdoor we refer to as ELMER.

Lure Number One

The first spear phishing message was sent to a Taiwanese governmental employee on Dec. 1. The attachment was created using the traditional Chinese character set, and contained a flowchart that appeared to be taken from the legitimate Taiwanese government auction website **hxxp://shwoo.gov[.]taipei/buyer_flowchart.asp**. The image, shown in Figure 3, is a flowchart detailing how to place a trade on the Taipei Nature and Cherish Network website.

民眾於首頁「會員登入」加入會員。

註冊完成，系統寄發一封 Email 確認信函，請開啟信箱依指示操作完成 Email 驗證。
（※僅完成 Email 驗證，尚無法出價）

Email 驗證完成，系統將再依您所留認證手機號碼寄發一封簡訊(內有 6 位數之認證碼)，請在收到簡訊後於網站首頁登入會員帳號並進入「修改資料」區輸入手機簡訊上之認證碼，完成手機認證後，成為正式會員。

每次詢問或出價前均須登入會員。

1. 競價最高者得標，得標會員應自行至網站首頁上方【自己的得標紀錄】查詢，並列印繳款單（為清楚列印條碼，建議以雷射印表機列印）。
2. 決標後得標訊息公告於網站首頁上方【查詢得標案】。

於得標後次日起 10 日內，自行持繳款單至郵局劃撥繳款。

得標會員至遲於貨款匯入指定網拍專戶後次日起 10 日內預約領貨，領貨時持繳款單據正本及身分證件(驗畢歸還)至拍賣機關指定物品放置處領貨。

Figure 3: Lure Image

Lure Number Two

The second December spear phishing attack targeted Taiwan-based news media organizations. The emails originated from the address **dpptccb.dpp@msa.hinet[.]net** (Figure 4), and contained the subject **DPP's Contact Information Update.** Based on the email address naming convention and message subject, the threat actors may have tried to make the message appear to be a legitimate communication from the Democratic Progressive Party (DPP), Taiwan's opposition party.

```
Date: Tue, 1 Dec 2015 12:03:37 +0800 (cst)
From: <dpptccb.dpp@msa.hinet.net>
To: <redacted>
Mime-version: 1.0
Content-type: multipart/mixed; boundary=----
=_part_159596_1670144893.1448942617906
X-mailer: hinet webmail v2.1509a
X-originating-ip: 216.169.136.210
```

Figure 4. December 1 Lure 2 SMTP Header

Unlike the previous exploit documents, this malicious attachment did not contain any visible text when opened in Microsoft Word.

ELMER Backdoor

The exploit documents delivered during the December campaigns dropped a binary containing an embedded variant of a backdoor we refer to as ELMER. ELMER is a non-persistent proxy-aware HTTP backdoor written in Delphi, and is capable of performing file uploads and downloads, file execution, and process and directory listings.

To retrieve commands, ELMER sends HTTP GET requests to a hard-coded CnC server, and parses the HTTP response packets received from the CnC server for an integer string corresponding to the command that needs to be executed. Table 2 lists the ELMER backdoors observed during the December campaigns.

ELMER Variant	C2 Location
6c33223db475f072119fe51a2437a542	121.127.249.74:443
0b176111ef7ec98e651ffbabf9b35a18	news.rinpocheinfo[.]com:443

Table 2. ELMER variants

The ELMER variant **6c33223db475f072119fe51a2437a542** beaconed to the CnC IP address **121.127.249.74** over port 443. However the ELMER sample **0b176111ef7ec98e651ffbabf9b35a18** beaconed to the CnC domain **news.rinpocheinfo[.]com** over port 443. Both samples used the hard-coded User-Agent string "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)", as shown in Figure 5.

```
GET hxxp://news.rinpocheinfo[.]com:443/cxgid/winxpsp3/33663168/336631680/index.php
HTTP/1.0
Accept: */*
Accept-Language: en-us
Host: news.rinpocheinfo[.]com:443
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1)
Content-Length: 0
Connection: Keep-Alive
```

Figure 5. ELMER beacon

APT16

While attribution of the first two spear phishing attacks is still uncertain, we attribute the second December phishing campaign to the China-based APT group that we refer to as APT16. This is based on the use of the known APT16 domain **rinpocheinfo[.]com**, as well as overlaps in previously observed targeting and tactics, techniques and procedures (TTPs).

Background

Taiwanese citizens will go to the polls on January 16, 2016, to choose a new President and legislators. According to recent opinion polls, the Democratic Progressive Party (DPP) candidate Tsai Ing-wen is leading her opponents and is widely expected to win the election. The DPP is part of the pan-green coalition that favors Taiwanese independence over reunification with the mainland, and the party's victory would represent a shift away from the ruling Kuomintang's closer ties with the PRC. Since 1949, Beijing has claimed Taiwan as a part of China and strongly opposes any action toward independence. The Chinese government is therefore concerned whether a DPP victory might weaken the commercial and tourism ties between China and Taiwan, or even drive Taiwan closer to independence. In 2005, the Chinese government passed an "anti-secession" law that signified its intention to use "non-peaceful" means to stymie any Taiwanese attempt to secede from China.

Targeting Motivations

APT16 actors sent spear phishing emails to two Taiwanese media organization addresses and three webmail addresses. The message subject read "DPP's Contact Information Update", apparently targeting those interested in contact information for DPP members or politicians. The Chinese government would benefit from improved insight into local media coverage of Taiwanese politics, both to better anticipate the election outcome and to gather additional intelligence on politicians, activists, and others who interact with journalists. This tactic is not without precedent; in 2013, the New York Times revealed it had been the target of China-based actors shortly after it reported on the alleged mass accumulation of wealth by then-Prime Minister Wen Jiabao and his family. The actors likely sought information on the newspaper's sources in China, who could be silenced by the government.

Compromising these Taiwanese news organizations would also allow the actors to gain access to informants or other protected sources, who might then be targeted for further intelligence collection or even retribution. The

webmail addresses, while unknown, were possibly the personal-use addresses of the individuals whose corporate domain emails were targeted. As corporate networks become more secure and users become more vigilant, personal accounts can still offer a means to bypass security systems. This tactic exploits users' reduced vigilance when reading their own personal email, even when using corporate IT equipment to do so.

On the same date that APT16 targeted Taiwanese media, suspected Chinese APT actors also targeted a Taiwanese government agency, sending a lure document that contained instructions for registration and subsequent listing of goods on a local Taiwanese auction website. It is possible, although not confirmed, that APT16 was also responsible for targeting this government agency, given both the timeframe and the use of the same n-day to eventually deploy the ELMER backdoor.

We've Been Here Before

One of the media organizations involved in this latest activity was targeted in June 2015, while its Hong Kong branch was similarly targeted in August 2015. APT16 actors were likely also responsible for the June 2015 activity. They sent spear phishing messages with the subject "2015 Taiwan Security and Cultural Forum Invitation Form" (2015台灣安全文化論壇邀請函), and used a different tool – a tool that we refer to as DOORJAMB – in their attempt to compromise the organization. A different group, known as **admin@338**, used LOWBALL malware during its Hong Kong activity. Despite the differing sponsorship, penetration of Hong Kong- and Taiwan-based media organizations continues to be a priority for China-based threat groups.

The difference in sponsorship could be the result of tasking systems that allocate targeting responsibility to different groups based on their targets' geographic location. In other words, while media organizations are important targets, it is possible that two separate groups are responsible for Hong Kong and Taiwan, respectively. The suspected APT16 targeting of the Taiwanese government agency – in addition to the Taiwanese media organizations – further supports this possibility.

Conclusion

Table 3 contains a summary of the phishing activity detailed in this blog.

Campaign Date	APT Group	Targeted Industries	Exploit	Malware
11/26/2015	Suspected Chinese APT	Japanese Financial and High-Tech	EPS Use-After-Free CVE-2015-1701	IRONHALO
12/1/2015	Suspected Chinese APT	Taiwan Governmental Agency	EPS Use-After-Free CVE-2015-1701	ELMER
12/1/2015	APT16	Taiwan Media and Entertainment	EPS Use-After-Free CVE-2015-1701	ELMER

Table 3. Activity summary

These clusters of activity raise interesting questions about the use of an identical silently-patched vulnerability, possibly by multiple threat groups. Both Japan and Taiwan are important intelligence collection targets for China, particularly because of recent changes to Japan's pacifist constitution and the upcoming Taiwanese election. Based

on our visibility and available data, we only attribute one campaign to the Chinese APT group APT16. Nonetheless, the evidence suggests the involvement of China-based groups.
