12
Like
Tweet
0
G+1

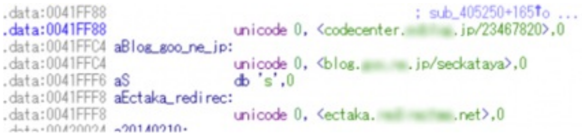
TRACKING ELIRKS VARIANTS IN JAPAN: SIMILARITIES TO PREVIOUS ATTACKS

POSTED BY: Kaoru Hayashi on June 23, 2016 4:00 PM

FILED IN: Cybersecurity, Threat Prevention, Unit 42
TAGGED: APAC, Elirks, Japan, PlugX, Scarlet Mimic

A recent, well-publicized attack on a Japanese business involved two malware families, PlugX and Elirks, that were found during the investigation. PlugX has been used in a number of attacks since first being discovered in 2012, and we have published several articles related to its use, including an analysis of an attack campaign targeting Japanese companies.

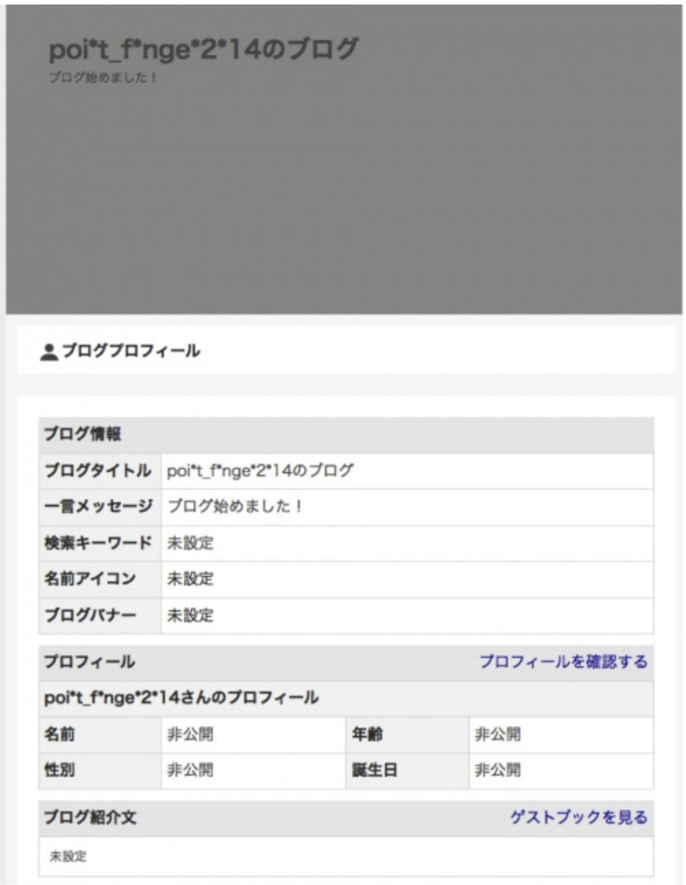
Elirks, less widely known than PlugX, is a basic backdoor Trojan, first discovered in 2010, that is primarily used to steal information from compromised systems. We mostly observe attacks using Elirks occurring in East Asia. One of the unique features of the malware is that it retrieves its C2 address by accessing a pre-determined microblog service or SNS. Attackers create accounts on those services and post encoded IP addresses or the domain names of real C2 servers in advance of distributing the backdoor. We have seen multiple Elirks variants using Japanese blog services for the last couple of years. Figure 1 shows embedded URL in an Elirks sample found in early 2016.



```
.data:0041FF88                              ; sub_405250+165↑o ...
.data:0041FF88                   unicode 0, <codecenter.[redacted].jp/23467820>,0
.data:0041FFC4 aBlog_goo_ne_jp:
.data:0041FFC4                   unicode 0, <blog.[redacted].jp/seckataya>,0
.data:0041FFF6 aS                db 's',0
.data:0041FFF8 aEctaka_redirec:
.data:0041FFF8                   unicode 0, <ectaka.[redacted].net>,0
.data:00420024 a20140210:
```

Figure 1 Embedded URLs in Elirks variant

In another sample found in 2014, an attacker used a Japanese blog service. The relevant account still exists at the time of writing this article (Figure 2).



poi*t_f*nge*2*14のブログ
ブログ始めました！

ブログプロフィール

ブログ情報	
ブログタイトル	poi*t_f*nge*2*14のブログ
一言メッセージ	ブログ始めました！
検索キーワード	未設定
名前アイコン	未設定
ブログバナー	未設定

プロフィール			プロフィールを確認する
poi*t_f*nge*2*14さんのプロフィール			
名前	非公開	年齢	非公開
性別	非公開	誕生日	非公開

ブログ紹介文 ゲストブックを見る
未設定

Figure 2 Blog account created by the attacker in 2014

Link to previous attack campaign

Unit 42 previously identified an Elirks variant during our analysis of the attack campaign called Scarlet Mimic. It is years-long campaign targeting minority rights activists and governments. The

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

CATEGORIES & ARCHIVES

Select a Category
Select a Month
MORE →

RECENT POSTS

Tech Docs: Simplify Firewall Management Using Template Stacks
posted by Carl Mills on June 29, 2016

Prince of Persia – Game Over
posted by Tomer Bar on June 28, 2016

William Saito: Industry 4.0, IoT and Security By Design
posted by Chad Berndtson on June 27, 2016

Watch: CSO Insights from Infosecurity Europe 2016
posted by Richard Cashdan on June 27, 2016

Palo Alto Networks News of the Week –June 25, 2016
posted by Anna Lough on June 25, 2016

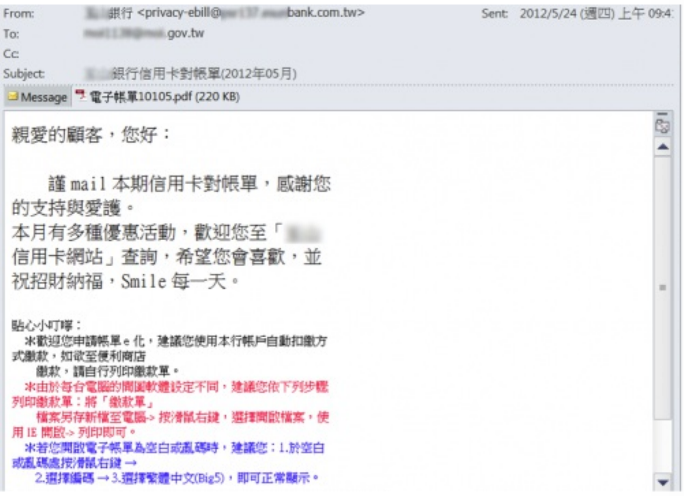
MORE →

malware primarily used in this series of attacks was FakeM. Our researchers described the threat sharing infrastructure with Elirks in the report.

As of this writing, we can note similarities between previously seen Elirks attacks and this recent case in Japan.

Spear Phishing Email with PDF attachment

Figure 3 shows an email which was sent to a ministry of Taiwan in May 2012.



From: [redacted]銀行 <privacy-ebill@[redacted]bank.com.tw> Sent: 2012/5/24 (週四) 上午 09:4

To: [redacted]gov.tw

Cc:

Subject: [redacted]銀行信用卡對帳單(2012年05月)

Message 電子帳單10105.pdf (220 KB)

親愛的顧客，您好：

謹 mail 本期信用卡對帳單，感謝您
的支持與愛護。
本月有多種優惠活動，歡迎您至「[redacted]
信用卡網站」查詢，希望您會喜歡，並
祝招財納福，Smile 每一天。

貼心小叮嚀：
※歡迎您申請帳單 e 化，建議您使用本行帳戶自動扣繳方
式繳款，如欲至便利商店
繳款，請自行列印繳款單。
※由於每台電腦的開啟軟體設定不同，建議您依下列步驟
列印繳款單：將「繳款單」
檔案另存新檔至電腦-> 按滑鼠右鍵，選擇開啟檔案，使
用 IE 開啟-> 列印即可。
※若您開啟電子帳單為空白或亂碼時，建議您：1.於空白
或亂碼處按滑鼠右鍵 →
2.選擇編碼 → 3.選擇繁體中文(Big5)，即可正常顯示。

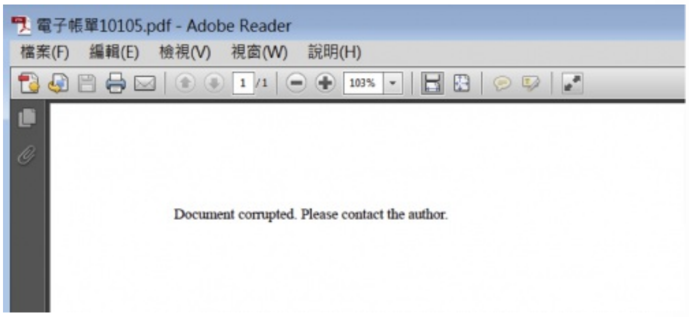
Figure 3 Spear Phishing Email sent to a ministry of Taiwan

The email characteristics were bit similar to the recent case (Table 1).

	2012	2016
Email Sender	Masquerades as an existing bank in Taiwan	Masquerade as an existing aviation company in Japan
Email Recipient	Representative email address of a ministry of Taiwan, which is publicly available.	Representative email address of a subsidiary company, which is publicly available.
Subject	“Bank credit card statement” in Chinese	“Airline E-Ticket” in Japanese
Attachment	PDF file named “Electronic Billing 1015” in Chinese	File named “E-TKT” in Japanese with PDF icon

Table 1 Email characteristics

When a user opened the attached PDF file, the following message is displayed. It exploits a vulnerability in Adobe Flash, CVE-2011-0611 embedded in the PDF and installs Elirks malware on the system.

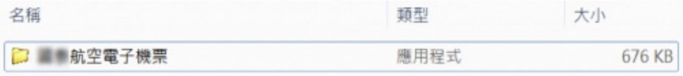

電子帳單10105.pdf - Adobe Reader
檔案(F) 編輯(E) 檢視(V) 視窗(W) 說明(H)
1 /1
103%

Document corrupted. Please contact the author.

Figure 4 opening malicious PDF attachment

Airline E-Ticket

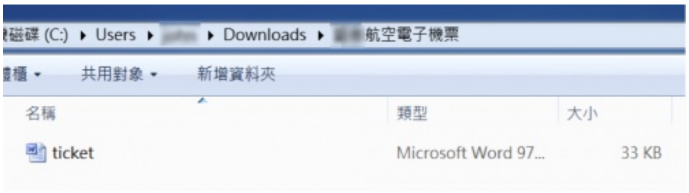
Attackers choose a suitable file name to lure targeted individual or organization. In the recent case, the malicious attachment name in the email was reported as “E-TKT”. We found similar file name in the previous attack in Taiwan in August 2012 (Figure 5).



名稱	類型	大小
[redacted]航空電子機票	應用程式	676 KB

Figure 5 Elirks executable file masquerade as folder of E-Ticket

When opening the file, Elirks executes itself on the computer and creates ticket.doc to deceive users (Figure 6).

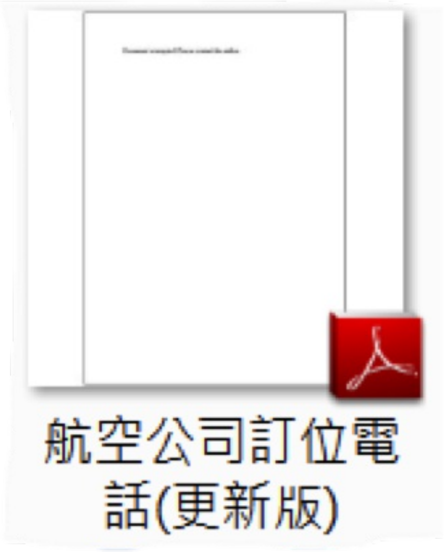


碟磁碟 (C:) ▸ Users ▸ [redacted] ▸ Downloads ▸ [redacted]航空電子機票

名稱	類型	大小
ticket	Microsoft Word 97...	33 KB

Figure 6 doc file created by Elirks

We've also seen another file name related to aviation at Taiwan in March 2012. Figure 7 shows PDF file named "Airline Reservation Numbers (updated version).pdf". When opening the PDF file, it displays the exactly same message with the Figure4, exploits CVE-2011-0611 and installs Elirks.



航空公司訂位電話(更新版)

Figure 7 PDF named "Airline Reservation Number"

CONCLUSION

Currently, we have found no reliable evidence to indicate the same adversary attacked a company in Japan in 2016 and multiple organizations in Taiwan in 2012. However, we can see some resemblances between the two attacks. In both cases, attackers used the same malware family, crafted spear phishing emails in a similar manner, and seem to be interested in some areas related to aviation. We have been seeing multiple Elirks variants targeting Japan in the last few years, potentially indicating an ongoing cyber espionage campaign. We will keep an eye on the threat actors.

Palo Alto Networks customers are protected from Elirks variant and can gather additional information using the following tools:

- WildFire detects all known Elirks samples as malicious
- All known C2s are classified as malicious in PAN-DB
- AutoFocus tags have been created: Elirks

INDICATORS:

Executable File:

8587e3a0312a6c4374989cbcca48dc54ddcd3fbd54b48833afda991a6a2dfdea

0e317e0fee4eb6c6e81b2a41029a9573d34cebeabab6d661709115c64526bf95

f18ddcacfe4a98fb3dd9eaffd0feee5385ffc7f81deac100fdbbabf64233dc68

Delivery PDF:

755138308bbaa9fcb9c60f0b089032ed4fa1cece830a954ad574bd0c2fe1f104

200a4708afe812989451f5947aed2f30b8e9b8e609a91533984ffa55d02e60a2

POST YOUR COMMENT

Name *

Email *

Website

Post Comment

1.866.320.4788

Privacy Policy | Legal Notices | Site Index | Subscriptions