


# Tracking Elirks Variants in Japan: Similarities to Previous Attacks

 [researchcenter.paloaltonetworks.com/2016/06/unit42-tracking-elirks-variants-in-japan-similarities-to-previous-attacks/](https://researchcenter.paloaltonetworks.com/2016/06/unit42-tracking-elirks-variants-in-japan-similarities-to-previous-attacks/)

Kaoru Hayashi



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](#).

Eliorks, 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 Eliorks 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 Eliorks variants using Japanese blog services for the last couple of years. Figure 1 shows embedded URL in an Eliorks sample found in early 2016.

```
.data:0041FF88                                     ; sub_405250+165fo ...  
.data:0041FF88                                     unicode 0, <codecenter.blog.jp/23467820>,0  
.data:0041FFC4 aBlog_goo_ne_ip:                   unicode 0, <blog.goo.ne.jp/seckataya>,0  
.data:0041FFC4                                     db 's',0  
.data:0041FFF6 aS  
.data:0041FFF8 aEctaka_redirc:                   unicode 0, <ectaka.web-net.net>,0  
.data:0041FFF8                                     ; 00140210
```

*Figure 1 Embedded URLs in Eliorks 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).



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 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.



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.

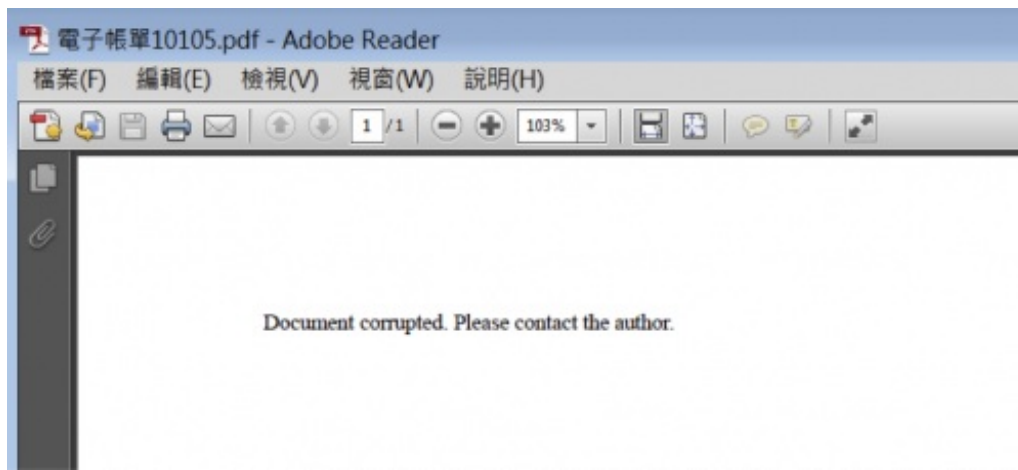


Figure 4 opening malicious PDF attachment

### 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
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).

磁碟 (C:) > Users > [User] > Downloads > 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.

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: [Eliorks](#)

## Indicators:

### Executable File:

8587e3a0312a6c4374989cbcca48dc54ddcd3fbd54b48833afda991a6a2dfdea  
0e317e0fee4eb6c6e81b2a41029a9573d34cebeabab6d661709115c64526bf95  
f18ddcacfe4a98fb3dd9eaffd0feee5385ffc7f81deac100fdbbabf64233dc68

### Delivery PDF:

755138308bbaa9fcb9c60f0b089032ed4fa1cece830a954ad574bd0c2fe1f104  
200a4708afe812989451f5947aed2f30b8e9b8e609a91533984ffa55d02e60a2

