THR34T 1NT3LL1GENC3
AN EXERCISE IN BIG DATA

3
5
8
13
21
34
55
89
144
233
377

Alfred Lee
VP, Product Management
Palo Alto Networks

THE NETFLIX PRIZE

MEANWHILE...

...AT STANFORD

1 CLASS 10 WEEKS

SAME RESULT. HOW?

CHEATING!

IMDb

WHOEVER HAS THE MOST DATA WINS

WE DON’T HAVE BETTER ALGORITHM

WE JUST HAVE MORE DATA.

PETER NORVIG, GOOGLE

WHOEVER HAS THE MOST DATA WINS

HOW DOES THAT APPLY TO NETWORK SECURITY?

OPERATION LOTUS BLOSSOM

OPERATION LOTUS BLOSSOM AT A GLANCE

Target: 3+ year campaign targeting government and military organizations of at least five Southeast Asian nations

Malicious actor: Potentially state-sponsored adversary

Attack method and tools: Used targeted spear phishing emails to install a custom backdoor named Elise

Scope and persistence: 57 separate attacks identified thus far, but activity continues

DATA SOURCE AND METHODOLOGY

ATTACK DATA FROM

>7,500 Palo Alto Networks WildFire subscribers

COMBINED WITH

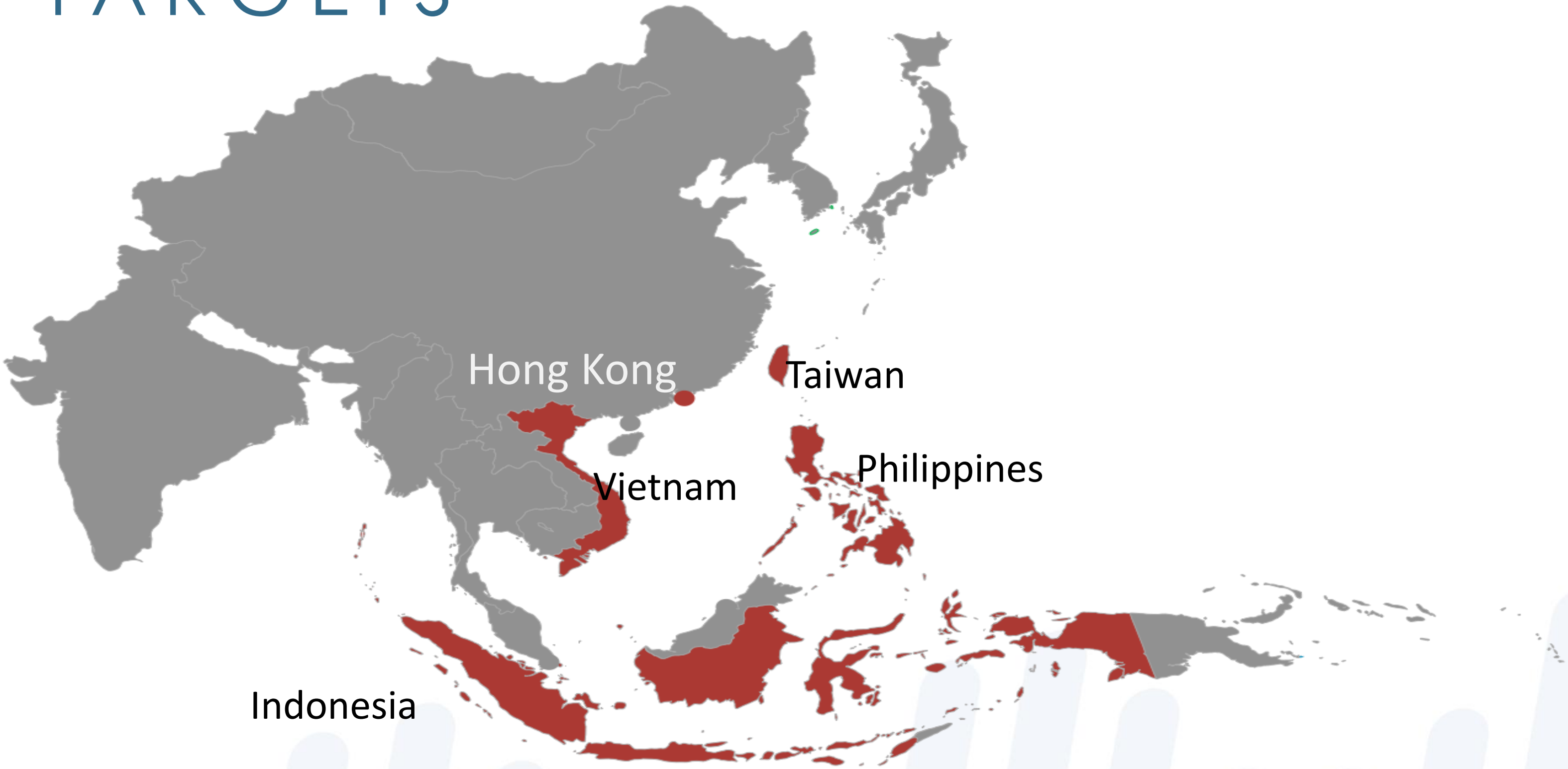
data from Cyber Threat Alliance + open source intelligence

UNIT 42 USED THE AUTOFOCUS SERVICE

to quickly identify relationships between attacks, including:

- Shared Infrastructure (IP addresses, domains)
- Backdoor behavior and attack mechanisms
- Targeted organizations and regions

TARGETS



LOTUS BLOSSOM ADVERSARY

Consistent with cyber espionage conducted by nation states:

Extensive resources

Custom-built tools

Persistence

Well-funded

Likely attempting to gain inside information on government and military operation of nation states in Southeast Asia.

ELISE BACKDOOR

Developed by the Lotus Blossom Group for their needs:

Custom-built, low detection Windows backdoor

- ✓ File system control
- ✓ Execute shell commands
- ✓ Download and execute additional tools

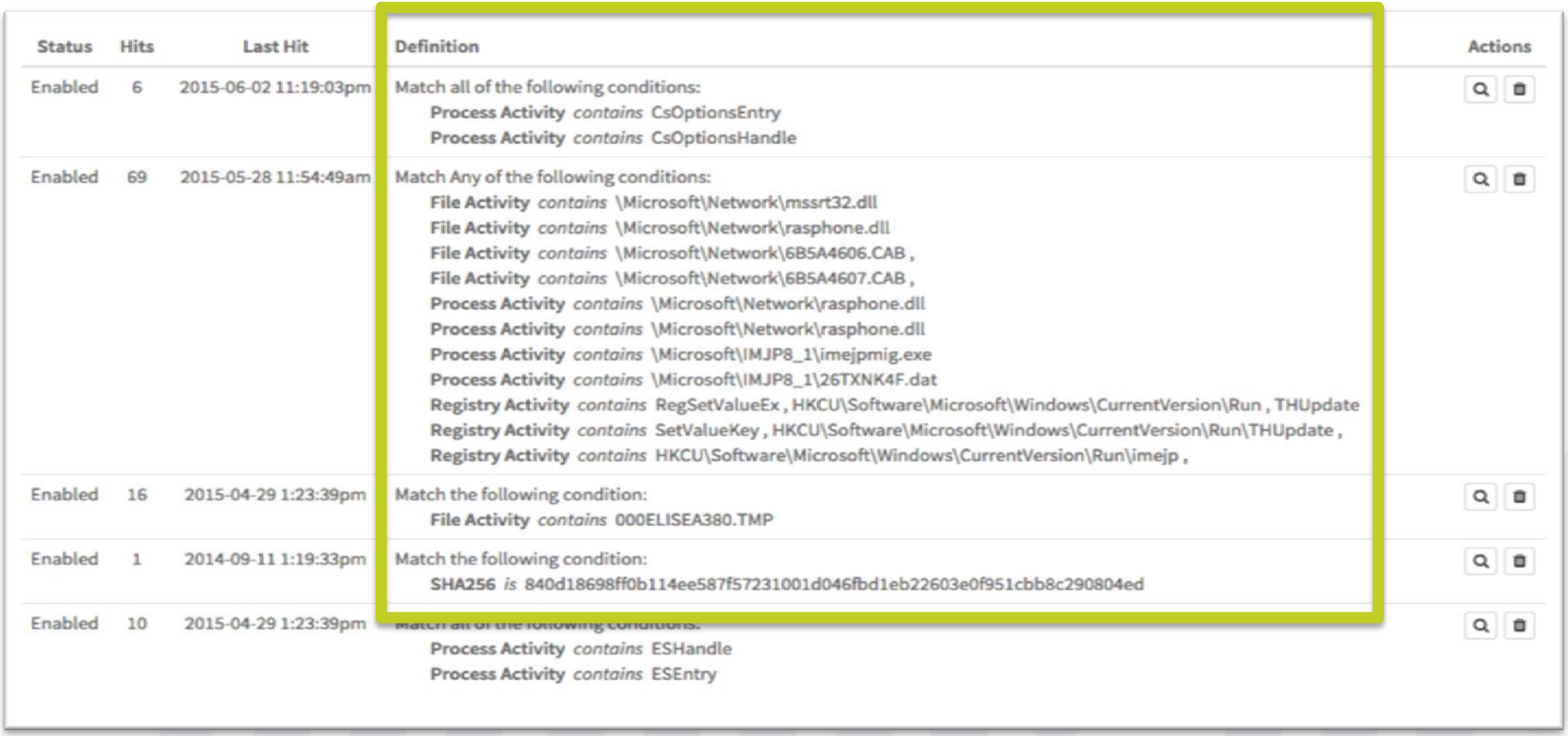
HTTP-based command and control

Each target identified by campaign code

- ✓ Uniquely identifies the malware reporting to the C2

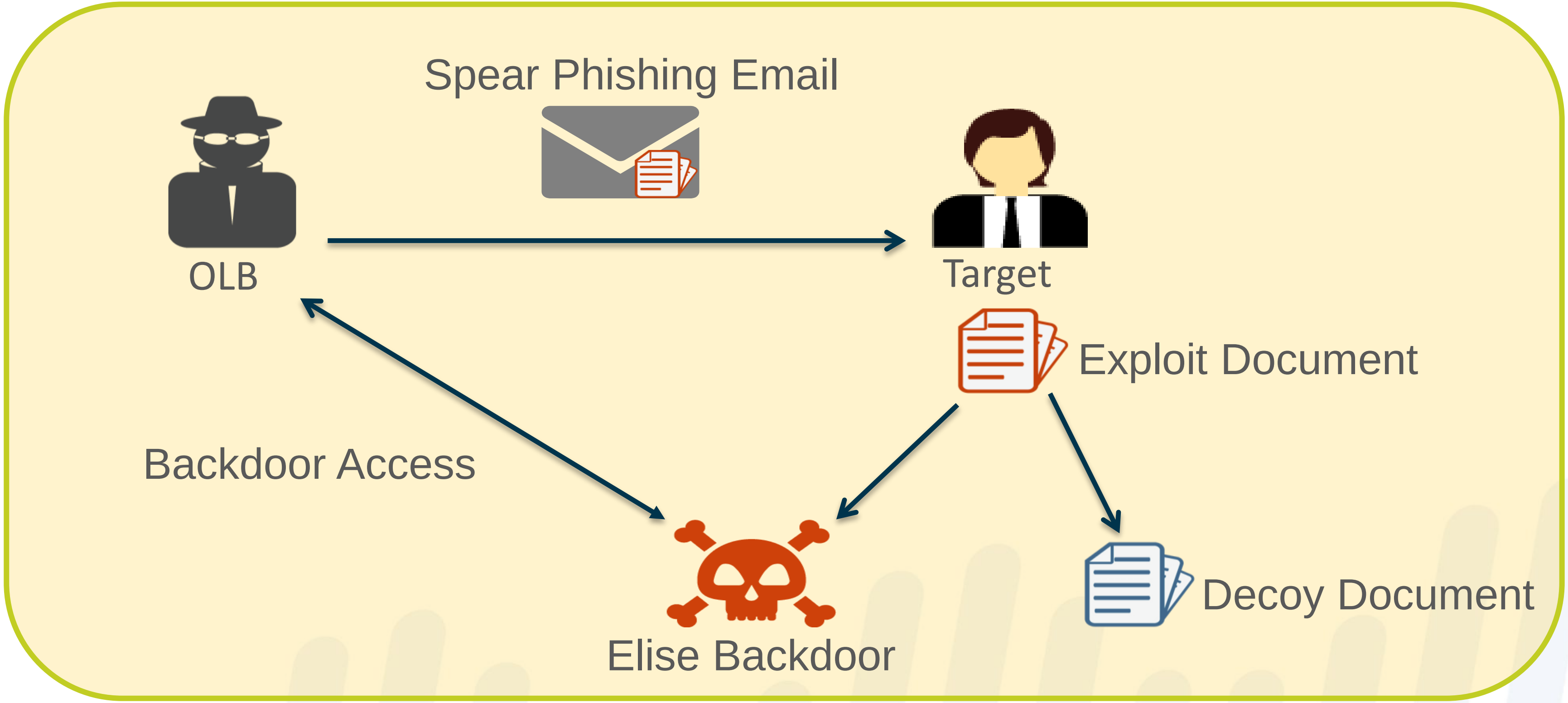
Named by author for the Lotus Elise

CONNECTING ELISE WITH AUTOFOCUS

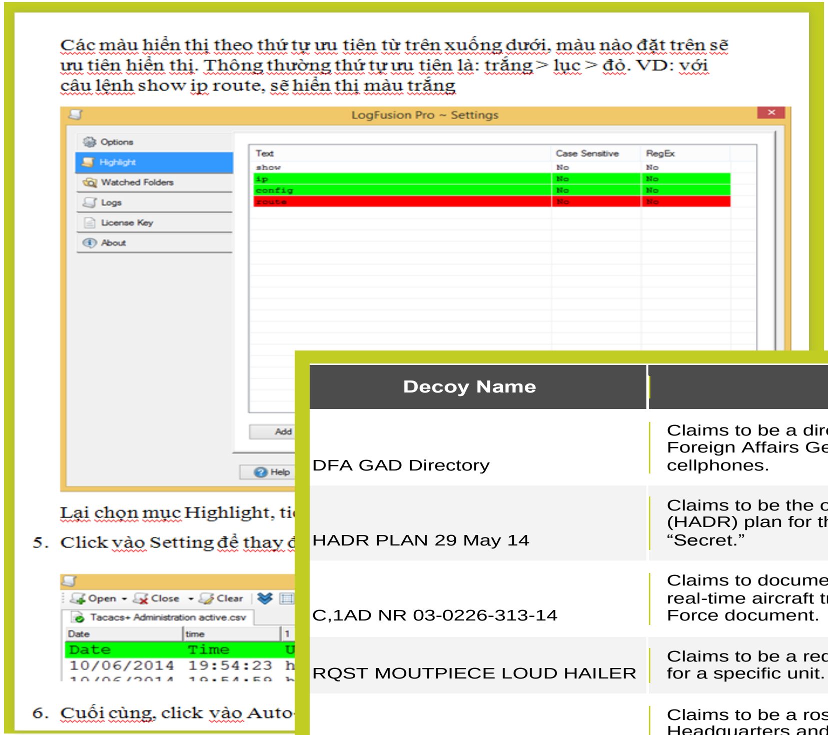


Status	Hits	Last Hit	Definition	Actions
Enabled	6	2015-06-02 11:19:03pm	Match all of the following conditions: **Process Activity** *contains* CsOptionsEntry **Process Activity** *contains* CsOptionsHandle	🔍 🗑
Enabled	69	2015-05-28 11:54:49am	Match Any of the following conditions: **File Activity** *contains* \Microsoft\Network\mssrt32.dll **File Activity** *contains* \Microsoft\Network\rasphone.dll **File Activity** *contains* \Microsoft\Network\6B5A4606.CAB , **File Activity** *contains* \Microsoft\Network\6B5A4607.CAB , **Process Activity** *contains* \Microsoft\Network\rasphone.dll **Process Activity** *contains* \Microsoft\Network\rasphone.dll **Process Activity** *contains* \Microsoft\IMJP8_1\imejpmig.exe **Process Activity** *contains* \Microsoft\IMJP8_1\26TXNK4F.dat **Registry Activity** *contains* RegSetValueEx , HKCU\Software\Microsoft\Windows\CurrentVersion\Run , THUpdate **Registry Activity** *contains* SetValueKey , HKCU\Software\Microsoft\Windows\CurrentVersion\Run\THUpdate , **Registry Activity** *contains* HKCU\Software\Microsoft\Windows\CurrentVersion\Run\imejp ,	🔍 🗑
Enabled	16	2015-04-29 1:23:39pm	Match the following condition: **File Activity** *contains* 000ELISEA380.TMP	🔍 🗑
Enabled	1	2014-09-11 1:19:33pm	Match the following condition: **SHA256** *is* 840d18698ff0b114ee587f57231001d046fbd1eb22603e0f951cbb8c290804ed	🔍 🗑
Enabled	10	2015-04-29 1:23:39pm	Match all of the following conditions: **Process Activity** *contains* ESHandle **Process Activity** *contains* ESEntry	🔍 🗑

ATTACK LIFECYCLE



DECOY DOCUMENTS



Các màu hiển thị theo thứ tự ưu tiên từ trên xuống dưới, màu nào đặt trên sẽ ưu tiên hiển thị. Thông thường thứ tự ưu tiên là: trắng > lục > đỏ. VD: với câu lệnh show ip route, sẽ hiển thị màu trắng

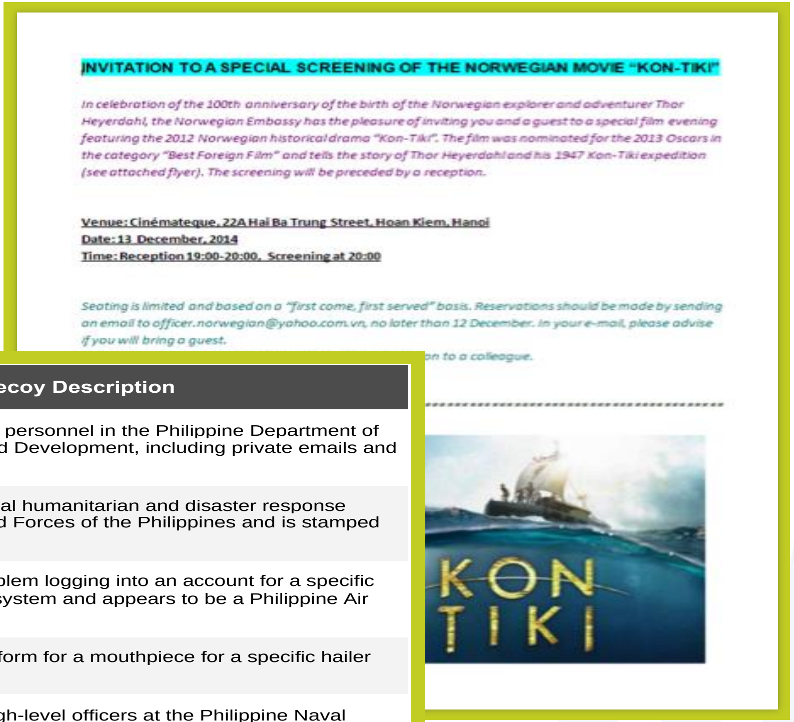
Text	Case Sensitive	RegEx
show	No	No
🟩 ip	No	No
🟩 config	No	No
🟥 route	No	No

Lại chọn mục Highlight, ti

5. Click vào Setting để thay đ

```
Date          time          1
Date          Time          U
10/06/2014    19:54:23      h
10/06/2014    19:54:58      h
```

6. Cuối cùng, click vào Auto



INVITATION TO A SPECIAL SCREENING OF THE NORWEGIAN MOVIE "KON-TIKI"

In celebration of the 100th anniversary of the birth of the Norwegian explorer and adventurer Thor Heyerdahl, the Norwegian Embassy has the pleasure of inviting you and a guest to a special film evening featuring the 2012 Norwegian historical drama "Kon-Tiki". The film was nominated for the 2013 Oscars in the category "Best Foreign Film" and tells the story of Thor Heyerdahl and his 1947 Kon-Tiki expedition (see attached flyer). The screening will be preceded by a reception.

Venue: Cinémateque, 22A Hai Ba Trung Street, Hoan Kiem, Hanoi
Date: 13 December, 2014
Time: Reception 19:00-20:00, Screening at 20:00

Seating is limited and based on a "first come, first served" basis. Reservations should be made by sending an email to officer.norwegian@yahoo.com.vn, no later than 12 December. In your e-mail, please advise if you will bring a guest.

on to a colleague.

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.

TAIWAN DECOY DOCUMENTS

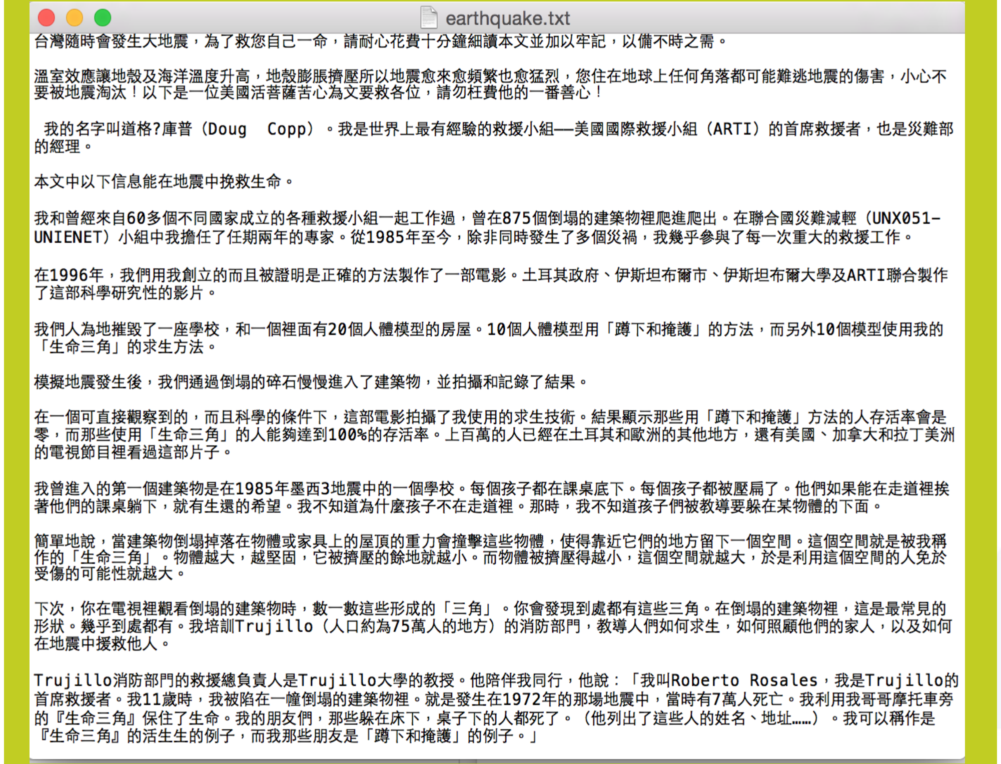
Taiwan target: Government ministry

3 Decoy documents used in Taiwan campaigns

- Earthquake.txt”

- 三高患者注意保暖.doc

- 員工通訊錄（最新）.xls



台灣隨時會發生大地震，為了救您自己一命，請耐心花費十分鐘細讀本文並加以牢記，以備不時之需。

溫室效應讓地殼及海洋溫度升高，地殼膨脹擠壓所以地震愈來愈頻繁也愈猛烈，您住在地球上任何角落都可能難逃地震的傷害，小心不要被地震淘汰！以下是一位美國活菩薩苦心為文要救各位，請勿枉費他的一番善心！

 我的名字叫道格?庫普（Doug Copp）。我是世界上最有經驗的救援小組——美國國際救援小組（ARTI）的首席救援者，也是災難部的經理。

本文中以下信息能在地震中挽救生命。

我和曾經來自60多個不同國家成立的各種救援小組一起工作過，曾在875個倒塌的建築物裡爬進爬出。在聯合國災難減輕（UNX051-UNIENET）小組中我擔任了任期兩年的專家。從1985年至今，除非同時發生了多個災禍，我幾乎參與了每一次重大的救援工作。

在1996年，我們用我創立的而且被證明是正確的方法製作了一部電影。土耳其政府、伊斯坦布爾市、伊斯坦布爾大學及ARTI聯合製作了這部科學研究性的影片。

我們人為地摧毀了一座學校，和一個裡面有20個人體模型的房屋。10個人體模型用「蹲下和掩護」的方法，而另外10個模型使用我的「生命三角」的求生方法。

模擬地震發生後，我們通過倒塌的碎石慢慢進入了建築物，並拍攝和記錄了結果。

在一個可直接觀察到的，而且科學的條件下，這部電影拍攝了我使用的求生技術。結果顯示那些用「蹲下和掩護」方法的人存活率會是零，而那些使用「生命三角」的人能夠達到100%的存活率。上百萬的人已經在土耳其和歐洲的其他地方，還有美國、加拿大和拉丁美洲的電視節目裡看過這部片子。

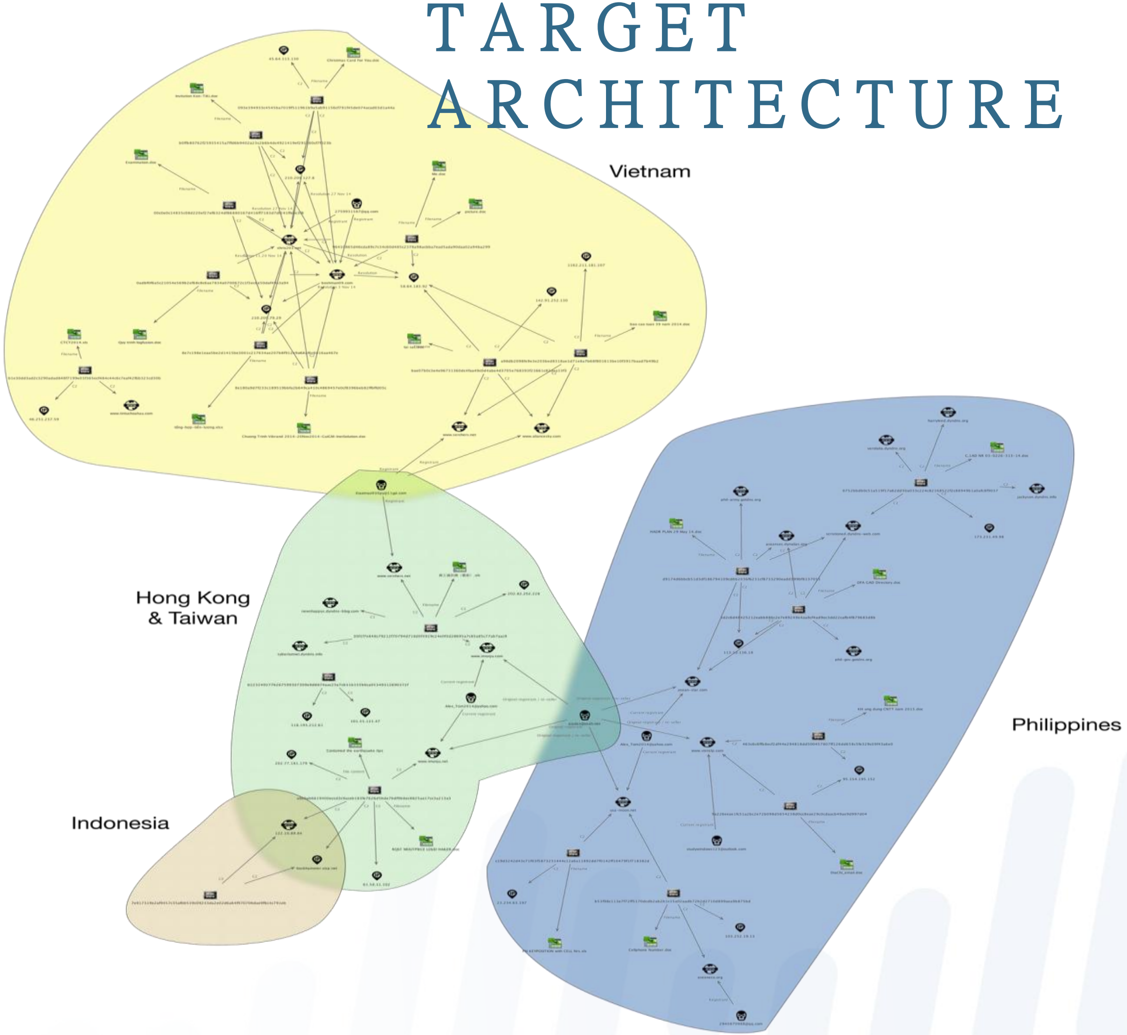
我曾進入的第一個建築物是在1985年墨西3地震中的一個學校。每個孩子都在課桌底下。每個孩子都被壓扁了。他們如果能在走道裡挨著他們的課桌躺下，就有生還的希望。我不知道為什麼孩子不在走道裡。那時，我不知道孩子們被教導要躲在某物體的下面。

簡單地說，當建築物倒塌掉落在物體或家具上的屋頂的重力會撞擊這些物體，使得靠近它們的地方留下一個空間。這個空間就是被我稱作的「生命三角」。物體越大，越堅固，它被擠壓的餘地就越小。而物體被擠壓得越小，這個空間就越大，於是利用這個空間的人免於受傷的可能性就越大。

下次，你在電視裡觀看倒塌的建築物時，數一數這些形成的「三角」。你會發現到處都有這些三角。在倒塌的建築物裡，這是最常見的形狀。幾乎到處都有。我培訓Trujillo（人口約為75萬人的地方）的消防部門，教導人們如何求生，如何照顧他們的家人，以及如何在地震中援救他人。

Trujillo消防部門的救援總負責人是Trujillo大學的教授。他陪伴我同行，他說：「我叫Roberto Rosales，我是Trujillo的首席救援者。我11歲時，我被陷在一幢倒塌的建築物裡。就是發生在1972年的那場地震中，當時有7萬人死亡。我利用我哥哥摩托車旁的『生命三角』保住了生命。我的朋友們，那些躲在床下，桌子下的人都死了。（他列出了這些人的姓名、地址……）。我可以稱作是『生命三角』的活生生的例子，而我那些朋友是「蹲下和掩護」的例子。」

TARGET ARCHITECTURE



Separate, but overlapping infrastructure

Each targeted nation largely has its own C2 servers

Connected by emai addresses used to register domains

WHO'S BEHIND OPERATION LOTUS BLOSSOM?

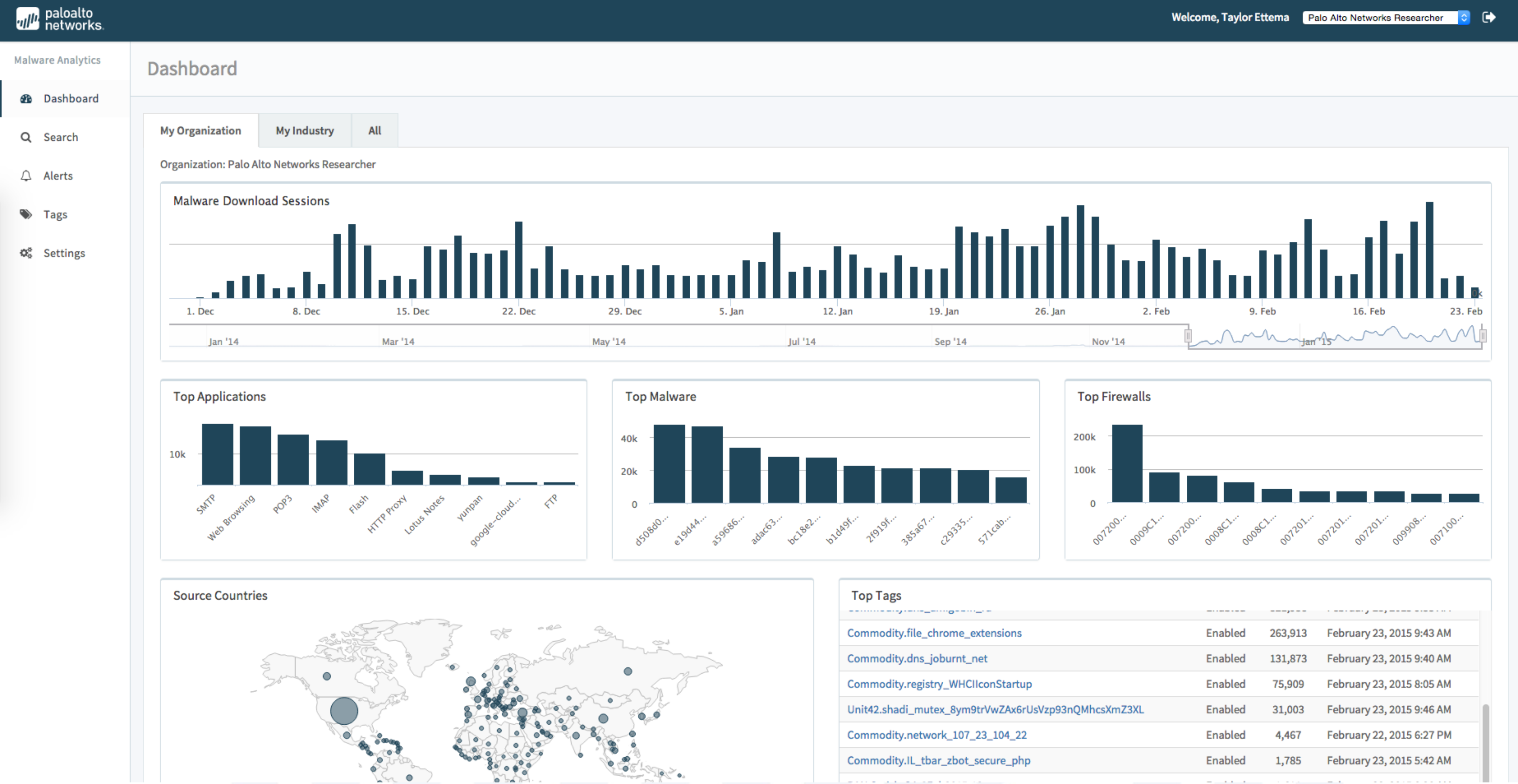
- Specific organization behind these attacks is still unknown.
- Adversary is well resourced.
- Adversary has strong interest in government and military targets of Southeast Asia.
- Circumstances suggest nation state backing, rather than a criminal enterprise.

AUTOFOCUS

AUTOFOCUS™

ACTIONABLE INTELLIGENCE HAS ARRIVED.

Introducing AutoFocus™. Available exclusively to Palo Alto Networks customers through a limited-time Community Access program.

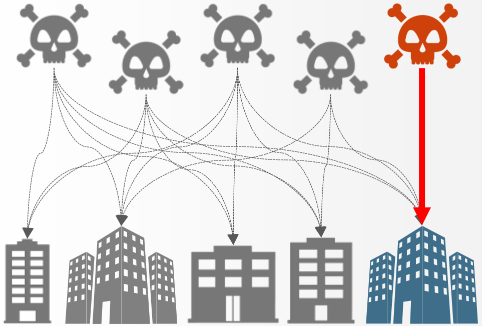


Organization: Palo Alto Networks Researcher

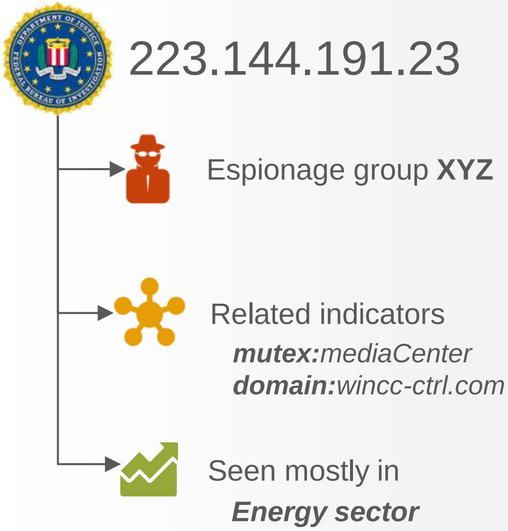
Commodity.file_chrome_extensions	Enabled	263,913	February 23, 2015 9:43 AM
Commodity.dns_joburnt_net	Enabled	131,873	February 23, 2015 9:40 AM
Commodity.registry_WHCIIconStartup	Enabled	75,909	February 23, 2015 8:05 AM
Unit42.shadi_mutex_8ym9trVwZAx6rUsVzp93nQMhcsXmZ3XL	Enabled	31,003	February 23, 2015 9:46 AM
Commodity.network_107_23_104_22	Enabled	4,467	February 22, 2015 6:27 PM
Commodity.IL_tbar_zbot_secure_php	Enabled	1,785	February 23, 2015 5:42 AM

Actionable threat intelligence

Unique or targeted events



Context around indicators of compromise



223.144.191.23

Espionage group **XYZ**

Related indicators

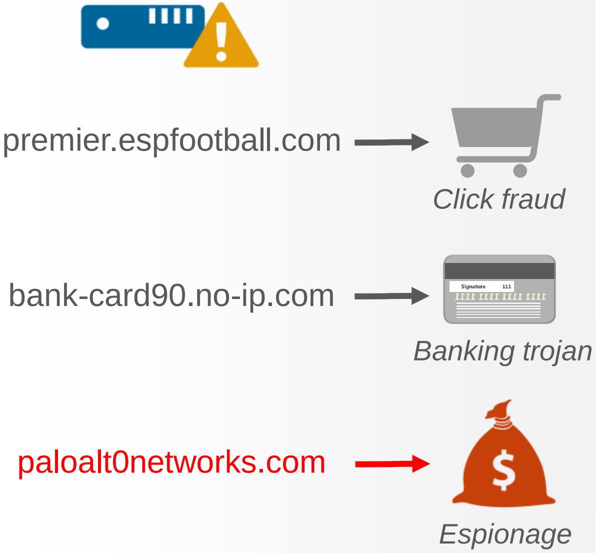
mutex:*mediaCenter*

domain:*wincc-ctrl.com*

Seen mostly in

Energy sector

Context around incidents on your network



premier.espfootball.com → *Click fraud*

bank-card90.no-ip.com → *Banking trojan*

paloalt0networks.com → *Espionage*

WildFire

32,000
Devices worldwide using WildFire

2.5M
Samples analyzed per day

20K
Unique malware found per day

AutoFocus

660
Users

460M
Samples

110B
Artifacts

(as of August 2015)

paloalto
NETWORKS

the network security company™