Hunting the Shadows: In Depth Analysis of Escalated APT Attacks

Fyodor Yarochkin, Academia Sinica
Pei Kan PK Tsung, Academia Sinica
Ming-Chang Jeremy Chiu, Xecure Lab
Ming-Wei Benson Wu, Xecure Lab
Agenda

• Why Taiwan?
• The “Lstudio” player... fun 😊
• Taking a peek at Weaponry
• APT in a Cloud
• Victimology or ... chicken-logy?
who we are

Based in Taiwan
Interests in Computer Forensics
Access to some raw network traffic data (fun!)
Get to fish interesting things (PROFFIIITT!)
A few words before we move on.

- With this research we are primarily interested in understanding the Ops and victims of discussed targeted attacks. We **DO NOT** attempt to perform any attribution of potential attackers.
Taiwan has been a frontline of APT battlefield for some time.

Cabinet says computers under attack

A Cabinet spokesman said Beijing is waging a campaign designed to access databases in Taiwan through malware infected with trojan horses.

A spy ring of hackers based in China’s Hubei and Fujian provinces has successfully spread 23 different Trojan horse programs to the networks 10 private high-tech companies here to use them as a springboard to break into at least 30 different government agencies and 50 private companies.”
Many interesting things could be observed (though this is not “Lstudio” group)
Elirks: earlier campaign

Reported by Dell/Secureworks as Elirks http://www.secureworks.com/cyber-threat-intelligence/threats/chasing_apt/
Elirks evolution

http://tw.myblog.yahoo.com/jw!uzrxZwSGHxowPMGZAaj4I5
http://blog.yam.com/minzhu0906/article/54726977
http://diary.blog.yam.com/bigtree20130514/article/10173342
http://tw.myblog.yahoo.com/jw!

Alex: Natalie win the competition award like 1Sa65j4W, well known for the series of 937B.

ブログをはじめました！
コメント大歓迎です。
これからどうぞよろしくお願いします！
Elixirks 2.0 – silly to reuse the address-space

Managed by the same IP addresses (easy to cross-correlate)
Another on-going Campaign
On average, 48 APT emails a week!
The “Lstudio” group:
Exploring fun things in a greater detail :)
They start with a boring spearphiiiiissh
Almost clean :)
The APT Landscape in Taiwan
We’ll examine the “LStudio” group today

- Unique indicators of the “LStudio” group:
  - Debug symbols (.pdb)
  - “horse” label and generator tag

- Some curious discoveries from the “Lstudio” backend data center ... ;-)}
LStudio binaries have cute things

http://scan.xecure-lab.com

f:\tools\code\CSJ\Elise\Release\EliseDLL.pdb
CSJ-Elise ..

Process Memory Report

Process Name  Address
svchost.exe

%USERPROFILE%\Templates\wince.dll
The analyzed code segment has behavior, APT-Malware

118.163.217.37 (118.163.217.37)
118.163.217.37 (http://118.163.217.37)
118.163.60.73 (http://118.163.60.73)
140.105.135.71 (140.105.135.71)
http://
Host: %s
%s %=expires=Thu, 01-Jan-1970 0
net user
net localgroup administrators
net view
netstat -ano
tasklist /v
net start
systeminfo
0x03, Connect Failed!
\000ELISEA310.TMP

Malware Behavior Graph

HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\Wmdm\PMM
Autorun
%UserProfile%\Templates\wince.dll

svchost.exe
%UserProfile%\Templates\wince.dll

118.163.217.37
140.105.135.71
118.163.60.73

http://118.163.60.73:443/2995ebc9/page_12180912.html
They love fast cars 😊
FASST CARS 😊

Evora
Lstudio Operations and C2

daily operational windows

CSJ (CyberShuttle) → Broderna → IISLinker

Protocol

Data Struct
OP CODE
CRC

JSON
XML

3 C2/Per client

Protocol

Blog / Web via HTTP
JSON via HTTP
XML via HTTP

ELISE
EVORA
STCreator
Emissary
“Lstudio” payload Generator

Horse Label

Generator-Tag

Owner

Generator

APT Exploit delivery via email
We don’t say victim

肉雞 = G
The typical botnet model
Very advanced Zoo-management skills :)

![Image of chickens in a rocky area with trees and foliage in the background.](image-url)
APT advanced farming :)  
- Operated by roughly 25 “farmers”
- Has controlled over 5,884 machines
- International coverage over 30 countries
- Utilizes 4 different Botnet software families
- Active since 2007
The “Lstudio” Chicken Cloud 😊

APT Botnet A

Data Channel
(First phase backdoor)

Command Channel
(Second phase backdoor)

Configurable Bounce

APT Cloud
Backend Data Center

Farmer Group A

Farmer Group B

Farmer Boss?

APT Botnet B
.. And who are the Chicken ?! 😊
International Chicken Farm Corp.
chicken farms went international

5,884 chickens

+ US 6%
+ TW 84%
+ KR 1%
+ CN 1%
Share some Chicken 😊

KMT？

KMT？

http://www.cna.com.tw

http://www.appledaily.com.tw/
When you travel, your chicken travel too... 😊
Let's look at some travelers 😊
ANOTHER DISCOVERY!!
.. do have 9 to 5 job ;)...
Just like some security researchers do 😊
AND THE LAST .. SOME HANDY TOOLS TO SHARE 😊
XecScan: Free API

**Information**

**Malware**: APT00N00
The analyzed sample has these behaviors: Ability with network behavior, APT-Malware

**CVE**
Sample Time: 2012-09

**Malware File**: %USERPROFILE%\68d3bf4e11a65a6ba8170c3b77cc49cb.EXE
- MD5: 68d3bf4e11a65a6ba8170c3b77cc49cb [VT](Download)
- Build Time: 2012-09-18 20:30:16 [Download]

**Autorun**: HKEY_CURRENT_USER\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWSLOAD\%

**Mutex**: blog.yam.com [VT UQ TU]

**C&C**: blog.yam.com

**Agent Name**: http://blog.yam.com/minzhu0906/article/54726877

**URL String**: BLOG.YAM.COM
Yara: a swiss-knife of static sigs ;)

Yara Rule

```
meta:
  author = "XsecScan 2.0 beta"
  date = "2013-07-06 02:26:40"
  description = "scan.xecure-lab.com"
  hash0 = "68d3bf4e11a65a6ba8170c3b77cc49cb"

strings:
  $string0 = "blog.yam.com"
  $string1 = "http://blog.yam.com/minzhu0908/article/54726977"
  $string2 = "BLOG.YAM.COM"
  $string3 = ""

condition;
  any of them
```

Snort Rule

```
alert udp $HOME_NET any -> any 53 (msg:"APT.C2 blog.yam.com"; flow:to_server; byte_test:1,8,0xF8,2;
```

Similar Malware
Yara use

Easy to integrate with your scripts
Integration with a proxy server is possible via icap yara plugin: https://github.com/fygrave/c_icap_yara

Raw network traffic monitoring project (and http/DNS indexing):
https://github.com/fygrave/eyepkflow
More cool tools

Moloch  https://github.com/aol/moloch

Yara mail  
https://github.com/kevthehermit/yaraMail

Yara pcap  
https://github.com/kevthehermit/YaraPcap
Conclusions

Complex infrastructure
Operates since 2007
Multiple software versions
Multiple back-ends
Victims – government and private sector
Mainly Taiwan but also seen world-wide
Questions?

benson.wu@xecure-lab.com
jeremy.chiu@xecure-lab.com
pk@hitcon.org
f@plurk.com