Hunting the Shadows: In Depth Analysis of Escalated APT Attacks

Tsung Pei Kan, Chiu Ming-Chang, Wu Ming-Wei Benson, Fyodor Yarochkin

Academia Sinica, Taiwan, R.O.C.
and Xecure-Lab, Taiwan, R.O.C.
E-mail: research@xecure-lab.com

Abstract

APT attacks are a new emerging threat and have made headlines in recent years. However, we have yet to see full-scale assessment of targeted attack operations. Taiwan has been a long term target for these cyber-attacks due to its highly developed network infrastructure and sensitive political position. We had a unique chance to monitor, detect, investigate, and mitigate a large number of attacks on government and private sector companies. This paper introduces the results of a joint research between Xecure-Lab and Academia Sinica on targeted attack operations across the Taiwan Strait. We have developed a fully automated system, XecScan 2.0 (http://scan.xecure-lab.com) equipped with unique dynamic (sandbox) and static malicious software forensics technology to analyze nature and behavior of malicious binaries and document exploits. The system performs real-time APT classification and associates the analyzed content with existing knowledge base. In our experiments, the XecScan system has analyzed and successfully identified more than 12,000 APT emails, which include APT Malware and Document Exploits. With this presentation we will also analyze and group the samples from the recent Mandiant APT1(61398) Report and will compare the relationships between APT1 samples to the samples discovered in Taiwan and discuss the history behind APT1 Hacker activities. During this presentation we will release a free, publicly accessible portal to our collaborative APT classification platform and access to the XecScan 2.0 APIs.

Keywords: ***APT, targeted attacks, intrusion detection***

1 Introduction

APT attacks got extreme exposure in the media within recent few years due a large number of high-profile compromises being reported and discussed in public.

However what is being massively reported by the media often lacks technical details and only provides insight on targeted attacks from a perspective of North American Obesrver. Taiwan, however, has been using as targeted playground for more that a decade, and many targeted attacks could be easily spotted first on Taiwanese network, and only later would become visible world-wide. Other activities are very specific to Taiwan and typically are not observed anywhere else. In this paper we aim to document and discuss these activities.

A typical APT infrastructure includes a multi-layered botnet operation with backend centers, operated manually. Drop boxes and a large network of compromised machines.

Figure 1. Backend Operations

Figure 1 depicts a typical activity by operators at a backend center.

2 History of targeted attacks in Taiwan

The history of discovery of targeted attacks in Taiwan back to year 2008-2009 when a local information security team (ICST) discovered a botnet sample on one of the government networks. Further analysis led to discovery of similar clones across the other network components. And detection of activity, which was very different from a typical botnet behaviour, such as document collection from compromised machines. Further timing analysis allowed to demonstrate that identified botnet was operated by different group of people not motivated by a financial gain.

Figure 4 depicts over-all landscape of APT samples that we have analysed so far.

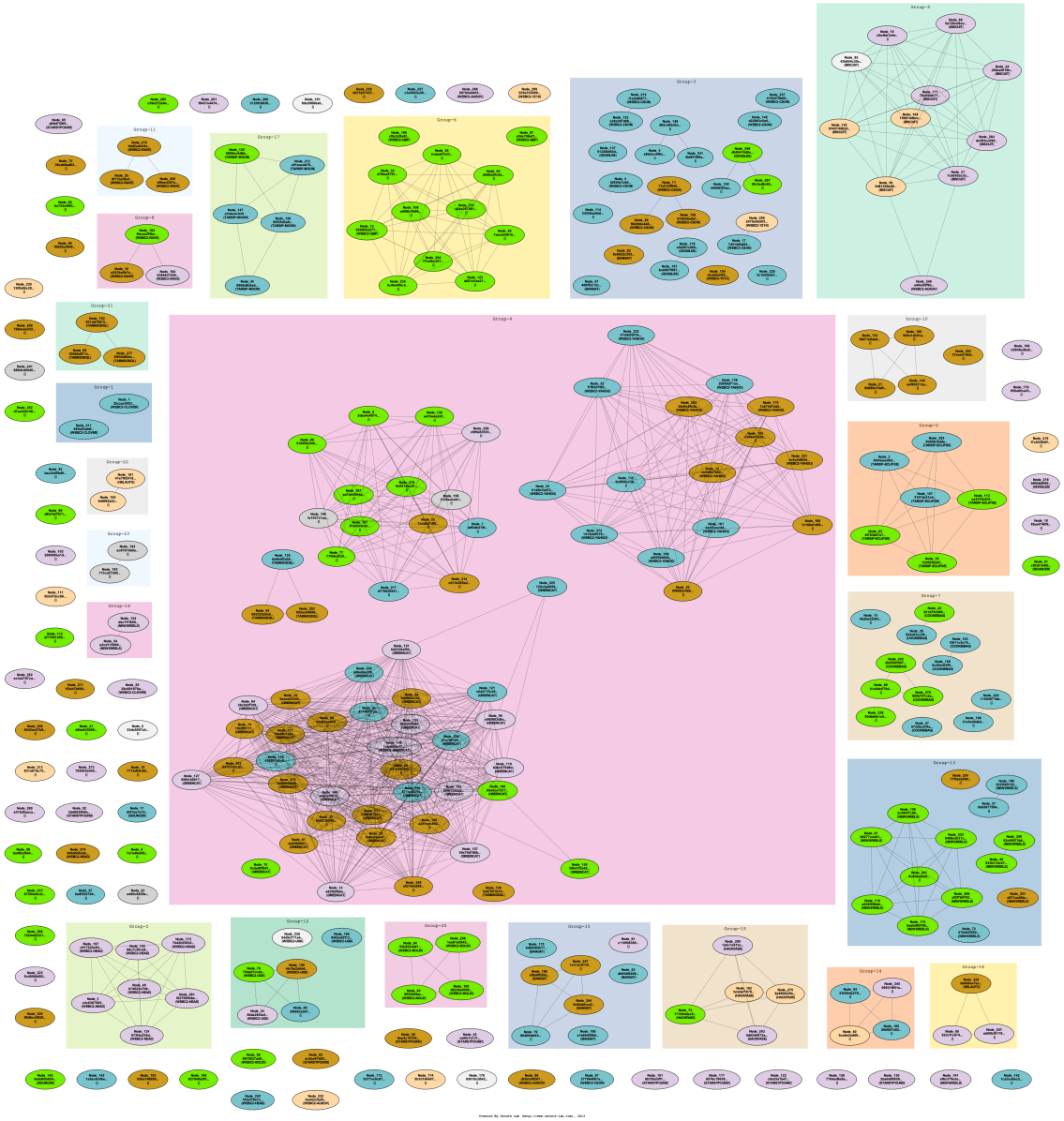

Figure 2. Landscape of APT samples in Taiwan

However, based on similarity of behaviour patterns we can break them down into several distinct groups. These groups

are discussed in the next section.

3 Case studies

3.1 The ST Group

The ST group activity is very widespread across taiwan and briefly could be broken into following sub categories: the ELISE group (uses car names for executables) the CSJ group, the Evora group. Then the STCreator backdoor, which uses a large number of related binaries: STDominate, Broderna, STMounter, STSetup, STEntity, STScountlib.

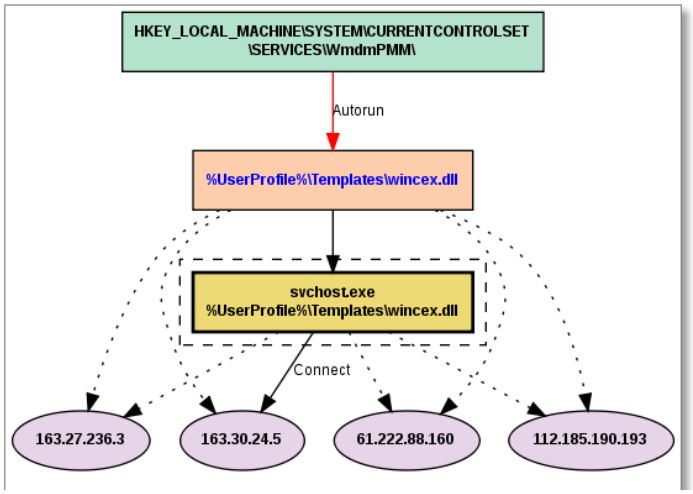

Figure 3. APT0LSTU ELise

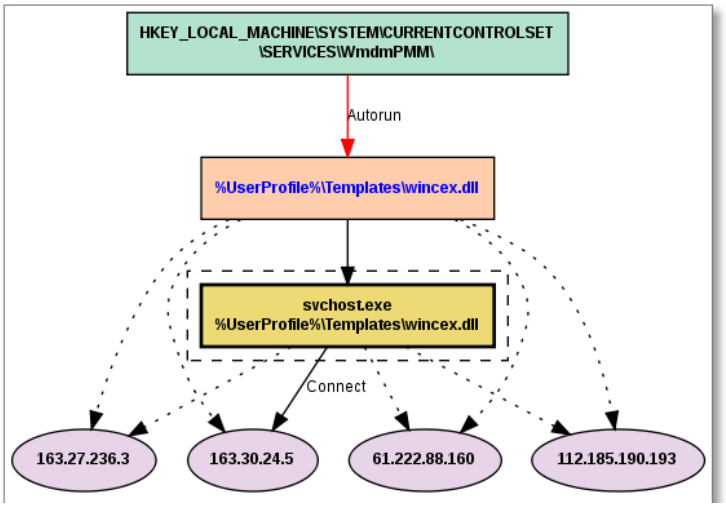

Figure 4. APT0LSTU

Then the Emissary group and a group we named as config007 (uses sumsvc, insconfig conmponents)

3.2 APT and social networks

Use of social networks, such as Plurk messaging platform in APT attacks was initially discussed in a publication by secureworks team.

`http://www.secureworks.com/cyber-threat-intelligence/threats/chasing_apt/`

we had a unique chance to perform additional analysis of the incident and identified few 'vawes' of the abuse. We refer to the abuse activity reported by secureworks as 'activity A', and new variations as 'activity B' and 'activity C'.

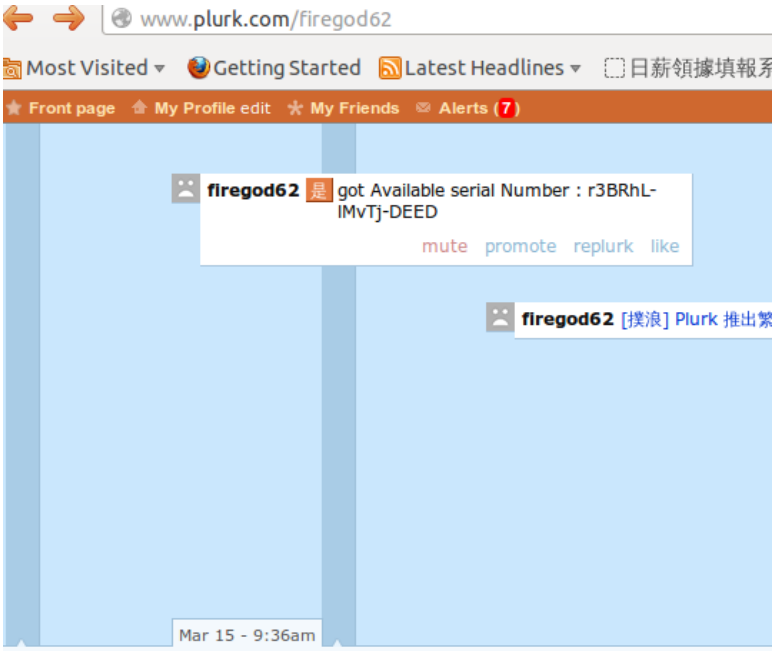

Figure 5. Activity A

Figure 6. Activity B

Accounts and IP addresses associated with 'activity A' phase:

ppth05t h05tppt@hotmail.com 2011-09-07 12:53:44 email: 1 karma: 0.0
user is banned
phoenixbomb phoenixbomb@126.com 2011-11-19 04:11:46 email: 1 karma: 0.0
details: 3774 2011-11-19 04:11:47 phoenix bomb 2011-11-19 04:14:45 cn sha$78gn0$0e29e116fa1558
automatic999 h05tppt@gmail.com 2011-12-12 06:48:17 email: 1 karma: 0.0
user is banned
swissmade999 ppth05t@yahoo.com.tw 2011-12-12 06:51:53 email: 1 karma: 0.0
user is banned
yoxiyoxi mwixinggan@yaho.com.tw 2011-12-27 06:41:18 email: 1 karma: 0.0
user is banned
ddtvnn sss.jj@hotmail.com 2012-02-15 02:08:26 email: 1 karma: 0.0
details: 3774 2012-02-22 06:52:49 fei liu 2012-02-22 06:53:39 tr_ch sha$t56pq$553e6d03cd01c91a
htconex81 htconex81@yahoo.com 2012-03-19 01:14:54 email: 1 karma: 0.0
details: 3774 2012-07-05 07:50:26 htconex81 htconex81 2012-07-05 07:50:34 cn sha$h6zyr$d4f9f9e
lgoptimus22 lgoptimus22@yahoo.com.tw 2012-03-19 01:20:28 email: 1 karma: 0.0
details: 3774 2012-07-05 07:32:25 lgoptimus22 lgoptimus22 2012-07-05 07:49:28 cn sha$4okze$440
terms86 terms86@yahoo.com.tw 2012-03-21 00:57:04 email: 1 karma: 38.51
details: 3774 2012-07-31 09:15:53 terms86 terms86 2012-07-31 08:41:58 cn sha$ikwy3$6c18cc9177c
farms21 farms21@yahoo.com.tw 2012-03-21 01:06:08 email: 1 karma: 18.1
details: 3774 2012-07-31 09:16:25 farms21 farms21 2012-07-30 02:36:46 cn sha$a5tuy$86520d28160
heres34 heres34@yahoo.com.tw 2012-03-21 01:09:26 email: 1 karma: 0.0
details: 3774 2012-07-31 09:16:50 heres34 heres34 2012-07-31 01:55:21 cn sha$yvw3h$b9c03d36370
zandy191 zandy191@yahoo.com.tw 2012-03-21 01:16:31 email: 1 karma: 0.0
details: 3774 2012-03-21 01:16:32 zandy191 zandy191 None cn sha$wdqf0$654a6e620eefb8398df30c44
caodan tccp521@yahoo.com.tw 2012-05-11 01:37:51 email: 1 karma: 0.0
details: 3774 2012-05-11 01:37:52 cao dan 2012-05-11 01:43:49 cn sha$5ev57$eef17d73d6db281e8cf
mannings840 mannings840@yahoo.com.tw 2012-05-11 08:46:36 email: 1 karma: 0.0
user is banned

zhihuirensheng ppth05t@hotmail.com 2011-09-26 07:13:42 email: 1 karma: 0.0
user is banned
godhorse2012 greenhouse20111011@gmail.com 2011-10-14 03:23:06 email: 1 karma: 0.0
user is banned

h05tppt@hotmail.com 220.130.59.159 1 ppth05t 2011-09-07 12:53:44
zhihuirensheng 220.130.59.159
phoenixbomb@126.com 220.130.59.159 0 phoenixbomb 2011-11-19 04:11:46
h05tppt@gmail.com 220.130.59.159 0 automatic999 2011-12-12 06:48:17
ppth05t@yahoo.com.tw 220.130.59.159 0 swissmade999 2011-12-12 06:51:53
mwixinggan@yaho.com.tw 220.130.59.159 0 yoxiyoxi 2011-12-27 06:41:18
sss.jj@hotmail.com 220.130.59.159 0 ddtvnn 2012-02-15 02:08:26
htconex81@yahoo.com 220.130.59.159 1 htconex81 2012-03-19 01:14:54
lgoptimus22@yahoo.com.tw 220.130.59.159 1 lgoptimus22 2012-03-19 01:20:28
terms86@yahoo.com.tw 220.130.59.159 1 terms86 2012-03-21 00:57:04
farms21@yahoo.com.tw 220.130.59.159 1 farms21 2012-03-21 01:06:08
heres34@yahoo.com.tw 220.130.59.159 1 heres34 2012-03-21 01:09:26
zandy191@yahoo.com.tw 220.130.59.159 1 zandy191 2012-03-21 01:16:31
tccp521@yahoo.com.tw 220.130.59.159 1 caodan 2012-05-11 01:37:51
mannings840@yahoo.com.tw 220.130.59.159 0 mannings840 2012-05-11 08:46:36
angela886.chen@gmail.com 122.117.204.210 0 angela888888 2010-12-06 07:28:00
708h.b.c@gmail.com 122.117.204.210 1 zxzxy 2011-09-20 07:44:02

```
rob_bailey97@yahoo.com 122.116.140.118 1 Guncannon_Century 2010-09-28 03:40:45
firegod62@yahoo.com.tw 122.116.140.118 1 firegod62 2011-02-15 01:36:01
hercules663@yahoo.com 122.116.140.118 1 hercules663 2011-04-15 07:54:56
blackpool2012@hotmail.com 122.116.140.118 1 blackpool2012 2011-04-25 12:42:01
astrotwins@hotmail.com 122.116.140.118 1 astrotwins 2011-05-17 02:09:38
heizeming100@yahoo.com.tw 122.116.140.118 1 heizeming100 2011-05-17 02:14:02
meihei51@ms68.hinet.net 122.116.140.118 1 meihei51 2011-05-17 02:22:00
vaughan301@yahoo.com.tw 122.116.140.118 1 vaughan301 2011-05-17 02:33:36
devasto1130@live.com 122.116.140.118 1 devasto1130 2011-05-17 02:39:24
```

A new variation of suspicious activity was sharing mainly the same group of IP addresses to access social network sides, however the pattern changed significantly, and other public services (such as yahoo blogs, yam.com and so on) were also involved in the operation.

```
http://tw.myblog.yahoo.com/jw!uzrxZwSGHxowPMGZAaj4I50- http://blog.yam.com/minzhu0906/article/
http://diary.blog.yam.com/bigtree20130514/article/10173342
http://tw.myblog.yahoo.com/jw!uzrxZwSGHxowPMGZAaj4I50-
 http://blogs.yahoo.co.jp/sakasesi2013/31805794.html
http://www.plurk.com/mdbmdb
```

Details of some of the users:

```
mdbmdb freezdoor@gmail.com 114.32.3.160 2012-09-15 01:38:33 email: 1 karma: 0.0 plurks: 4
Jasonborn20 mlgb321@yahoo.com.tw 114.32.3.160 2012-12-02 02:54:30 email: 0 karma: 0.0 plurks:
```

4 Released Tools

With this paper we would also like to release a few tools to the APT analysing community, which automate such tasks as binary analysis, clustering and intelligence mapping.

4.1 Xecscan

Xecscan is an online platform with RESTful API, which performs static and dynamic analysis of samples trying to identify and map families of these clusters and attribution to different APT groups. The platform also allows automated generation of Yara and Snort signatures (Figures 9 **?? ??**.

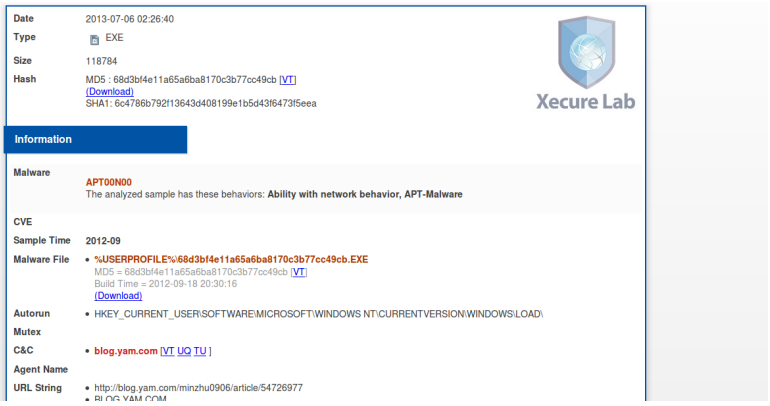

Figure 7. Xecscan screen

The xecscan API would be available at scan.xecure-lab.com on the day of the presentation.

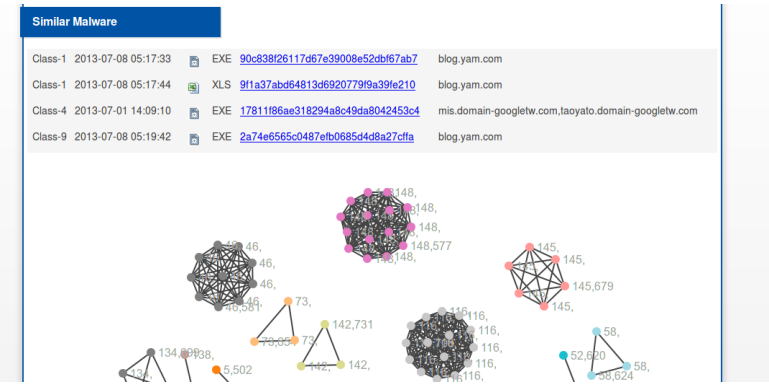

Figure 8. Xecscan screen

Figure 9. Xecscan screen - Yara rules

4.2 APT Cloud Intelligence Platform

We would also like to open access to our APT Cloud Intelligence Platform, a simple query-able framework to mine or submit APT related data (domain names, executables and so on). The APTCI platform would be available at www.aptci.com on the day of the presentation.

5 Conclusion

While APT attacks are extremely popular in the media, we believe what is being discussed is only a tip of the iceberg. With this paper we attempted to provide some additional insight on APT attacks from a perspective of forensic investigation on Taiwan national networks.