ANTIY

2015 Network Security Retrospect and Prospect

2015

Antiy Annual Security Report

First Edition: 14:21, Dec 8, 2015

Pub Date: 09:00, Jan 7, 2016

Update: 17:30, Jan 7, 2016

Antiy CERT

Content

Introduction

Facing the rapid evolution of threat and defense technology, it’s difficult for us to reveal the cyber security threat landscape via an annual report. For Antiy security research and emergency response center (Antiy CERT), maybe it’s relatively easy to compile an annual report a few years ago, we only needed to extract relative statistical charts from the malware storage and analysis platform to finish the report. In the field of network security, malware automatic analysis is an infrastructure that established earlier, and malware sample sets are easy to collect, which once deviated us from the essence of network security, and weakened our belief on user value protection.

In the light of the in-depth and more sophisticated threat situation, simple statistics has lost its meaning. Since last year, we decided to make a change in annual report editing, and we put forward that the annual report must contain the viewpoint of the editor. Although we have more samples and more date, we still dare not say we have been able to control the big security date. The only thing we can do now is to learn more and think more, and to be a security team with its own viewpoint.

Our work has some limitations. We always focus on advanced persistent threat (APT) attacks and malware defense, but we have shortcomings on web security, vulnerability exploit and other areas. In addition, due to the labor division between various departments, this annual report doesn’t cover much on mobile security, more information on mobile security will be presented by Antiy Mobile Security (AVL TEAM) later.

The Layered APT

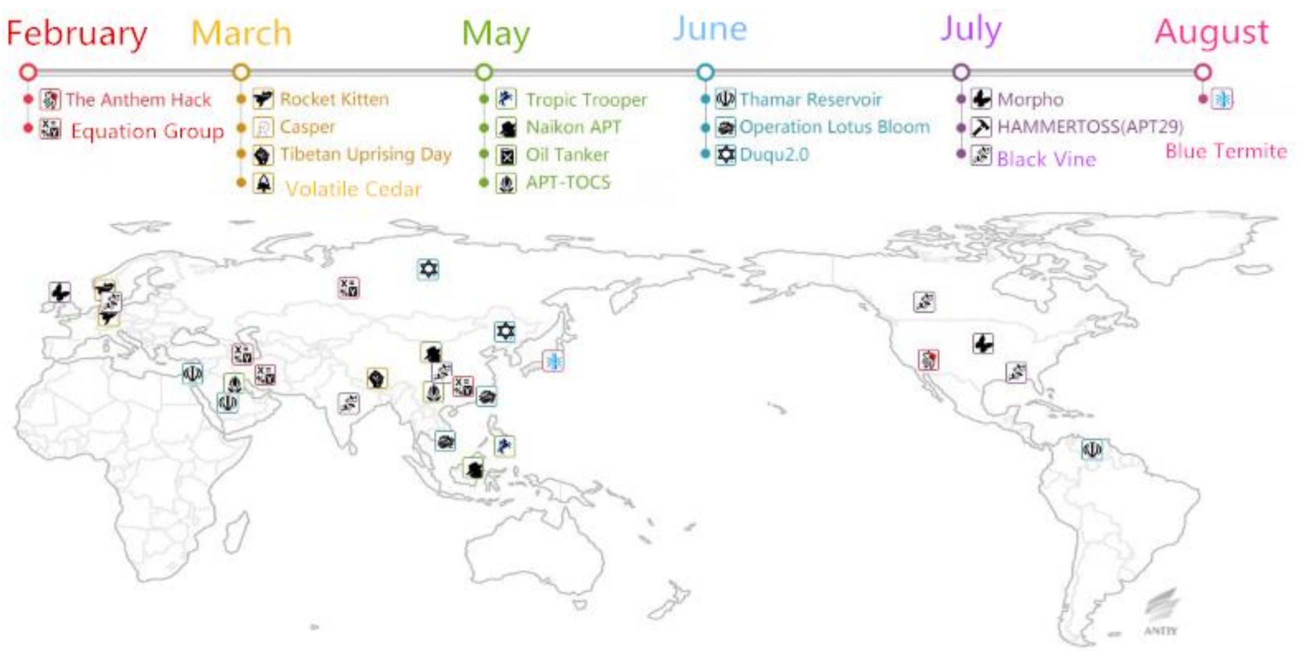


Figure 1 The time and geography of APT incidents in 2015

The exposed APT incidents in 2015

APT attacks are still the mainstream threat in 2015. More than a dozen of APT attacks were exposed, including: Equation Group (became active in February), APT-TOCS and Duqu2.0 (prospered in May and June), Blue Termitex (August). Although the total number of exposed incidents decreased, the impact of these attacks to victims, and the attack method, systematized attack platform, commercial Trojan and penetration platform they exploited improved. This makes Equation, Duqu2.0 and APT-TOCS incidents very representative.

Among the APT attacks in 2015, “Equation” [1] attacks are the most representative ones. This is a group that has been prosperous for more than 20 years. It can not only find more 0 day vulnerabilities than others, but also hold a super information arsenal, enabling it to implant malicious modules to more than a dozen of common bands of hard disks. As an advanced persistent means, it can be used for implanting after infection; also it can be used after integrated with “logistics chain”. Compared with BIOSKIT and BOOTKIT that we analyzed before, this malicious module is more sophisticated. The Equation Group focuses on high value targets. According to the analysis on the relevant hard disk firmware interface, we believe that through take advantage of technical documentation and reverse analysis, we can obtain parametric of relevant interface. Therefore, Antiy CERT believe the acquisition of firmware interface isn’t the result of cooperation of related intelligence agent and industrial community, it’s result of its super analysis ability. While the encryption strategy that the Equation Group exploited shows the tightness of its operation. We did a further discussion on this in EQUATION, COMPONENT ENCRYPTION ANALYSIS report that we published in April, 2015. [2]

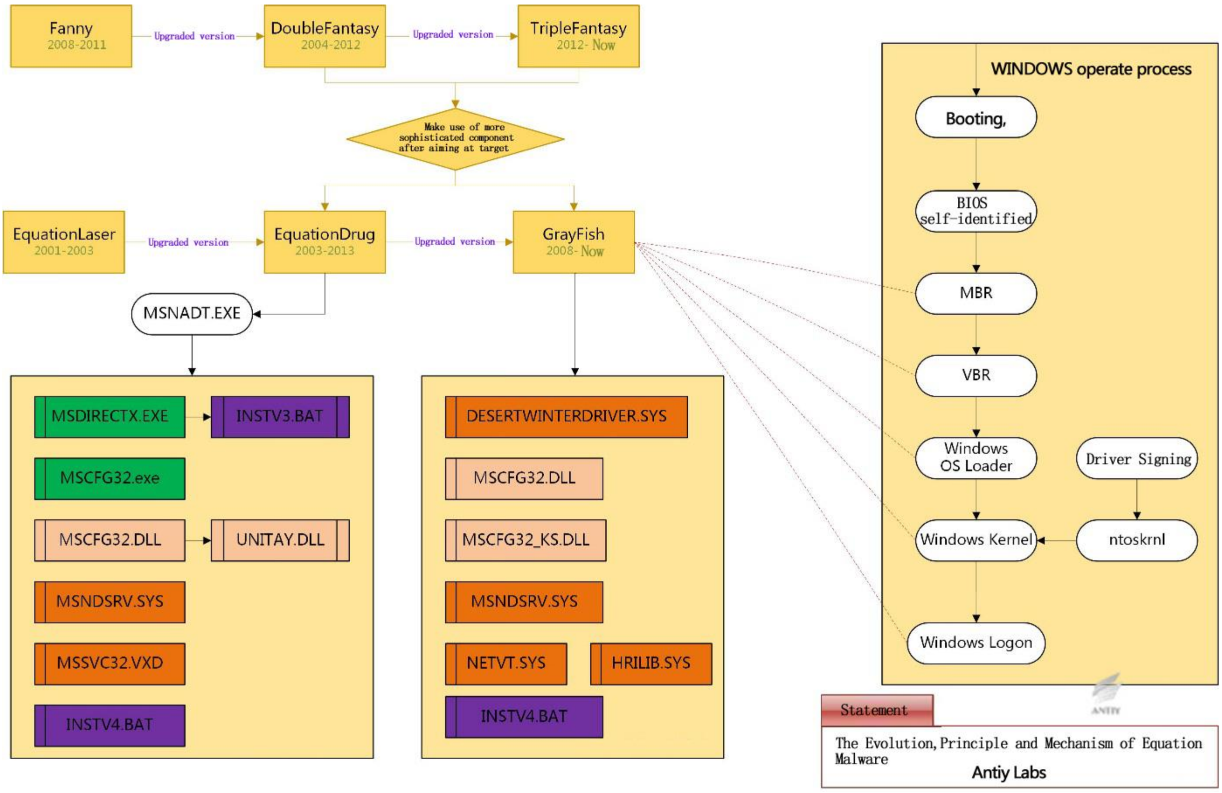


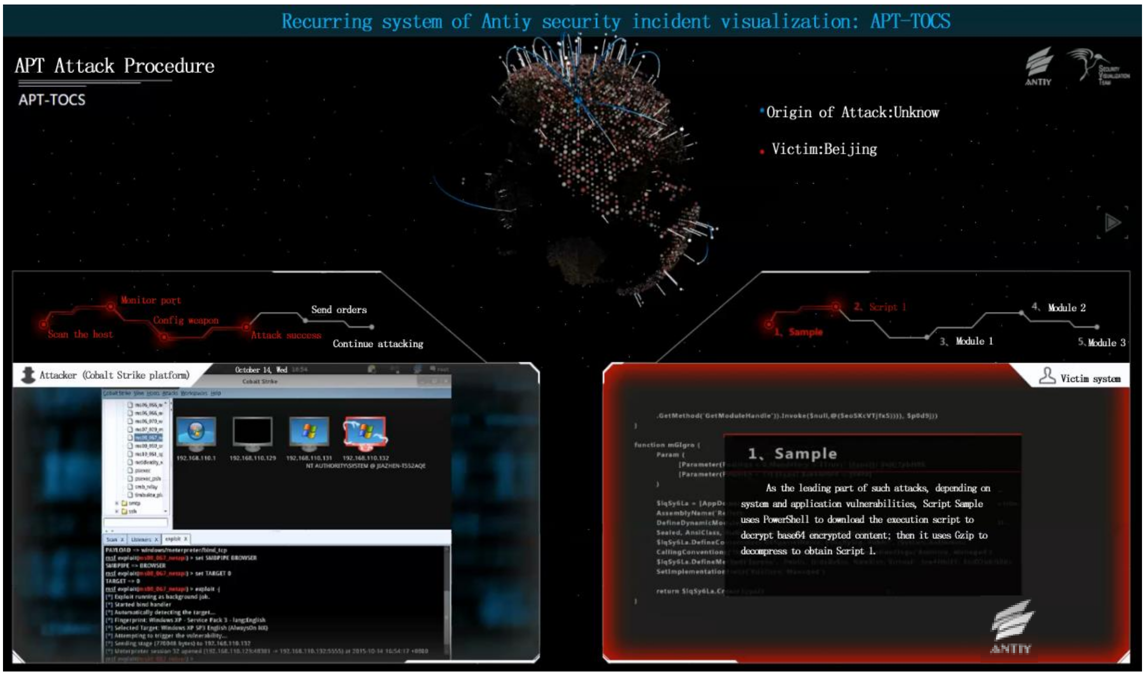
Figure 2 Evolution, principles and mechanisms of malicious code (Equation)

After 2011, there is report on Duqu until early 2015 the new version of Duqu (Duqu2.0) draw our attention again. It even launched penetration attack against Kaspersky. Duqu2.0 will only resident on the memory of infected machine, and there isn't any trace on hard disk. Although the malicious code will be temporarily removed when the system is restarted, attackers can deployment drivers on computers which is connect to internet, so Duqu2.0 can be deployed again via remote desktop session.

Malicious Groups which doesn't' have abundant financial support, advanced weapons and strong attack abilities will find a new path to implement malicious attack. Generally, they will use the open or commercial penetration platform to generate the malicious code and other attack payloads to deploy attack against the target. May 2015, Antiy detected an attack (APT-TOCS) [3] which targeting an official agency of China, the attacker here makes an use of an automated attack test platform Cobalt Strike to generate Shellcode. To some extent, this kind of attack penetration and non-malicious code file can evade detection of host security software and firewall; meanwhile it can fight with trusted computing environment, cloud detection, Sandbox. This kind of attack method can attack multiple platform, such as Windows、Linux、Mac, etc.. According to the analysis to this attack, we believe commercial Trojan and standard penetration platform has been widely used in various targeted attacks. This kind of attack mode which is at low cost not only reduces the requirements for the resource reserves, but also disturbs identification process which on the basis of big date analysis, and it also disable the certain analysis method like "coding psychology".

Increasingly active "commercial weapons"

The traditional APT attack give us an impression that it must be correlated to the superstation of highly professional operation team, strong infrastructure, dedicated 0day vulnerability exploit team and coding team, etc.. Therefore, most researchers put emphasis on these above factors. However, APT-TOCS and other events point another way for nations and groups which has limited resources. It also shows that with the increasing usage of the attack platform, commercial Trojans and open source malicious tools, the usage of cyber arms has become the new trend. According to trace record form Antiy, this kind of threat has existed for more than 5 years, unfortunately there still lacking efficient detection methods and products to this threat. Why we defined the APT-TOCS incident as APT attack is just because it fits all features that APT attack does, at the same time, it has some new features as we stated above. What's more, this kind of "highly-modeled" attack will leave few traces.



```
PAYLOAD => windows/meterpreter/bind_tcp
msf exploit(ms08_067_netapi) > set SMBPIPE BROWSER
SMBPIPE => BROWSER
msf exploit(ms08_067_netapi) > set TARGET 0
TARGET => 0
msf exploit(ms08_067_netapi) > exploit -j
[*] Exploit running as background job.
[*] Started bind handler
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (770048 bytes) to 192.168.110.132
[*] Meterpreter session 32 opened (192.168.110.129:48381 -> 192.168.110.132:5555) at 2015-10-14 16:54:17 +0800
msf exploit(ms08_067_netapi) >
```

1、Sample

As the leading part of such attacks, depending on system and application vulnerabilities, Script Sample uses PowerShell to download the execution script to decrypt base64 encrypted content; then it uses Gzip to decompress to obtain Script 1.

Figure 3 Visualization Recurrence of APT-TOCS Attack

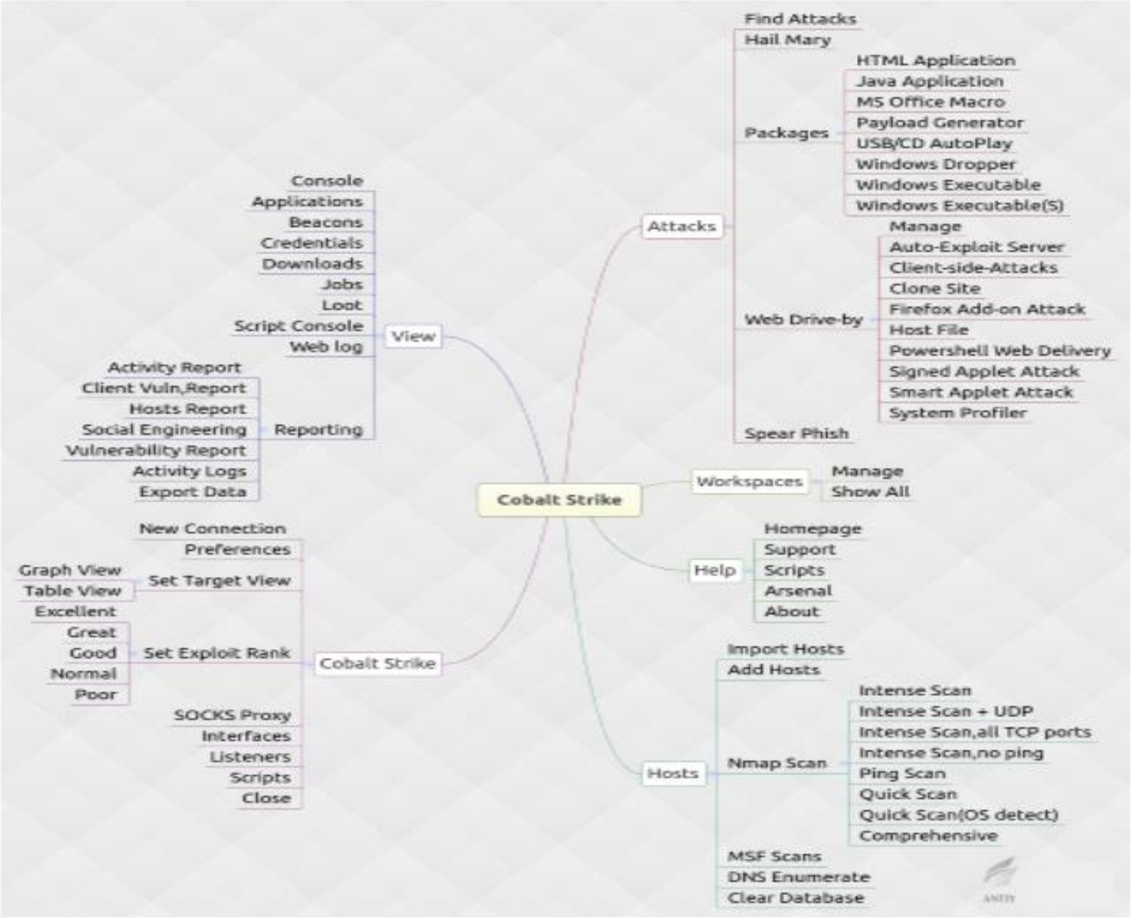


Figure 4 Overlay of Cobalt Strike Penetration Test Platform

The role played by Hacking-Team is different from what Cobalt Strike played in APT-TOCS incident, it's provide tools and strategies for attackers. July 2015, Hacking Team was compromised, as a result more than 400G date was breached. The exposure of a large amount of Trojan, a number of unpublished 0day vulnerability, e-mail, business contract, project material and recording means the cyber environment is going to confront a catastrophe. The exposure of such kind of multi-platform Trojan can dramatically improve the coding ability of black industrial, and the exposed vulnerability will be applied in common attacks soon.

Antiy AVL TEAM also find commercial Trojans like Biige are applied in attacks which against certain important agencies and individuals. As we've pointed out in this year's APT-TOCS incidents report, given that cyber-attack technology can be replicated in a very low cost, there already exist the risk of cyber arms proliferation. With the appearance of commercial penetration attack test platform, on the one hand, it can be used in system security detection, on the other hand, for nations, industry and organizations that has limited security budget, it's nightmare. When it comes to how to solve this issue, on the one hand we believe the establishment of more connection and consensus is indispensable; and on the other hand, countries which with the most competitive abilities in deal with this kind of threat should take more responsibility in controlling cyber arms proliferation ".

The layered abilities of APT

Now some super APT organizations have a large amount of available 0day vulnerabilities and attack equipment, while at the same time, some of the attack organization is the use of existing platforms and commercial Trojan to launch an attack. Therefore, there arises a question: the attack tactics, capabilities and technical reserves of the attacks which detected recently various a lot, then which criteria should be used in APT definition?

Considering the technical capacity, resources reserve, means of attack and other factors, means of attack, the level of attack abilities of APT organizations are subcategorized as A^{2}PT (“Advanced” APT), APT, standard APT, lightweight APT ,etc. by Antiy. A^{2}PT, just as its name implies is advanced APT, the name is derived from *Why Stuxnet Is not APT* (Michael Cloppert). Take a glimpse at all APT incidents which occurred in 2015, the “equation” as we stated above is known as “the most sophisticated network attack in the world” because it can modify firmware to establish a persistent fulcrum; on the basis of Duqu and Stuxnet, there establish a systematic attack infrastructure to support Duqu2.0, and even the world-class Security Company- Kaspersky is one of the victims of Duqu2.0. The attack abilities of these organizations are obviously advanced than any other malicious organizations, so they are named as A^{2}PT or GPT (God Mode of APT attacks) by some peers.

While attacks which with the support of high level of resource reserves and attack abilities, such as HAVEX is undoubtedly a classic APT representatives.

However, there also exist some organizations whose attack abilities and resources reverse are not so comparable with the attack organizations we stated above. The attackers of the these organizations can only launch an attack by take advantage of existing attack platform or commercial Trojan to generate malicious code. Such kind of attacks is known as APT-TOCS incident. The result of a preliminary analysis to this incident shows that the attacker has a high level and long-lasting, targeted attacks intentions, but after deeper analysis, we found that the high level it’s revealed is derived from an automated test platform-Cobalt Strike. So APT-TOCS incidents are characterized in high level of attack, persistence ability and lower R & D costs, that’s what we defined as "standard APT".

At the end of 2015, Antiy published the analysis report on two universities in China which is compromised by HangOver two years ago, this makes researchers to further recalled this "EXE specialized" APT attacks organizations. This rough level of attack abilities cannot be compared not only with the "equation", but also other known APT attack organization. Previously based on the “HangOver action” capture and analysis, and event correlation and visualization subsequent reproduction work, we put this on "human wave tactics" enough “advanced” APT attack, called lightweight APT attacks. According to the capture and analysis to “HangOver operation” before, and the correlation and visualization work Antiy did, we called this kind of APT attacks as lightweight APT attacks.

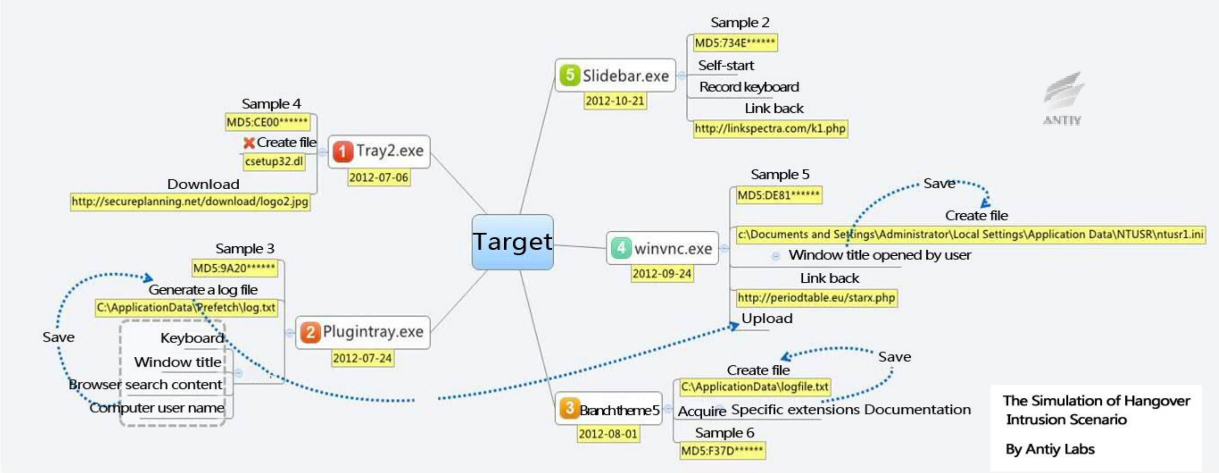


Figure 5 The landscape of a compromised host of Antiy in HangOver incident

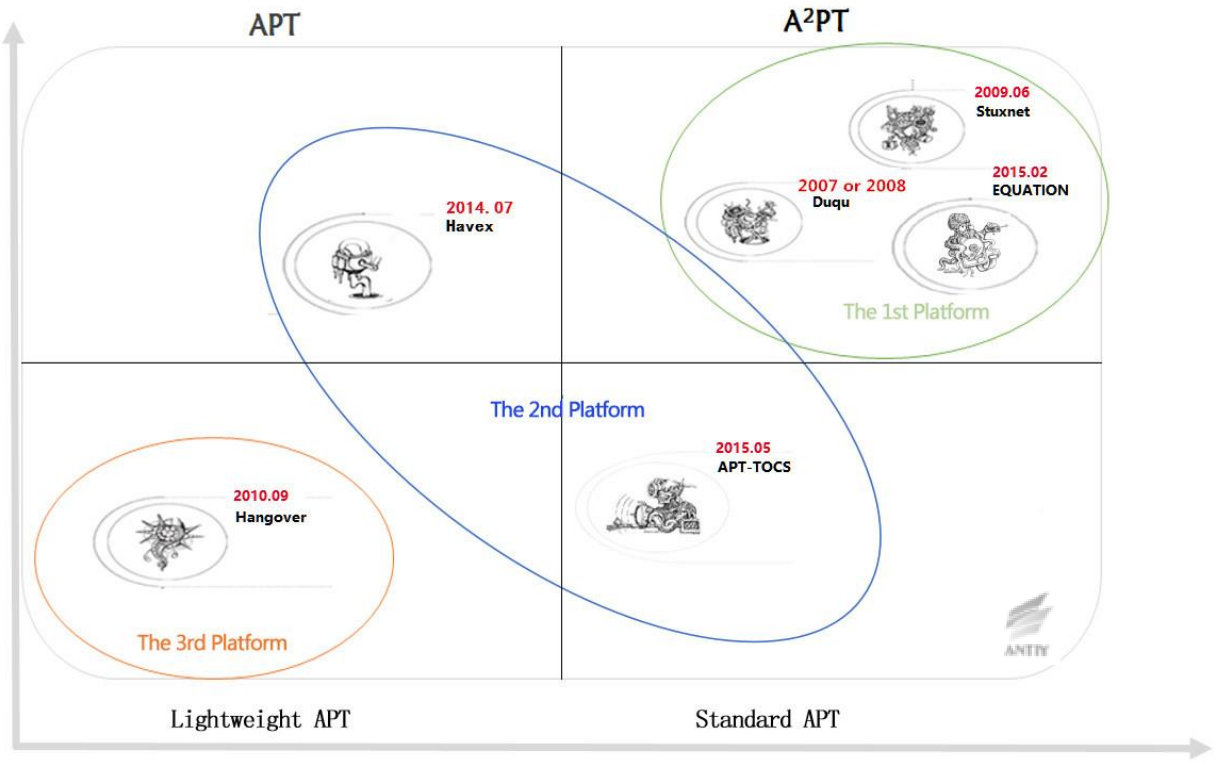


Figure 6 Schematic plot of attack abilities in APT attacks

Do not misunderstand APT

We’ve emphasized that APT isn’t a new concept, this word is put forward by the U. S. Air Force Colonel Greg Rattray in 2006 for the first time, APT is not the only nominatum of this kind of attack, and it is recognized just because it’s gained more attention than any other concepts. From the point of view of technique, there have been some emerging manufacturers put forward advanced sere technique (AET), it summarizes some basic features of the attack evasion techniques. The purpose of the provider is to sell its products. AET describes a specific type of attack techniques and methods. And historically, the more meaningful concept is "directional threat", in the eyes of some researchers, “directional threats” is more accurate than APT. Advisory agencies including IDC still didn’t define APT as separate division, but the providers and products of APT have been categorized as anti-orientation threat area. And in this case, APT is still being highly focused due to its political and economic background. Political context refers to: superpowers need to compete with its rival via APT; economic context refers to: emerging providers need to categorize the market in detail with the support of a concept. So we are easy to be misled if we only take a look at APT from the point of view of American providers such as FireEye.

During the procedure of consistent tracking analyzing against APT incidents, Antiy has been trying to avoid two tendencies: one is the neglecting of some APT attack because of our limited techniques in certain aspects; another is we will easily declare that we have discovered APT incidents just because the attackers in the incidents hold more sophisticated techniques. Now, we cannot define an attack as APT on the basis of social engineering techniques which occurs in the attack. For example, December 2nd, 2015, Antiy early-warning monitor system perceived such information: a well-known writer posted a message on Sina Weibo, he said someone is transmitting malicious link via the private letter function of Sina Weibo on the excuse of sending "interview outline" to user, and some is sending malicious links to target user via Baidu network disk [4]. Apparently, this event is consistent with the orientation threat we mentioned above, but after a deep analysis, we believe this incident isn’t belongs to APT incidents. To define an incident as APT attack, researchers must do a deep analysis, capture more, and take into consideration of more factors.

We still insist on using “suspected APT attack” on the interface of Shadow Box and other products. The reason is that we believe, APT attack can’t be determined based on the simple conditions. APT determination should first consider the attacker and the victim, the motives and consequences, and then the attack processes and tools. A clever attack technique, or the use of several suspected 0 day vulnerabilities, are not enough to characterize an attack as APT. Otherwise, an analyst with limited data acquisition capabilities is unable to find the large coverage of an attack, claiming that he/she finds an APT event.

We need to rethink the “advanced” and “persistent” of APT attacks. “Advanced” is not an absolute, but a relative concept. It may be with respect to the limited resources of the attacker, as well as the gap between defending and attacking capabilities. “Persistent” is reflected by concrete actions, mapping to some specific behaviors, such as encrypted communications, covert channel and the like. From the microscopic point of view, persistence may not be realized through the sustained links or heartbeats, but continuous capabilities or the capability to repeatedly enter. From microscopic point of view, this persistence is not terminated due to the defender’s removal, but depending on the wills and cost support abilities of the attacker.

Breached Data and Privacy Are Being Imported to Underground Economy Infrastructure

In 2015, data breaches resulted from the cyberattacks are still rampant. Medical, health care, telecom operators and other industries, personnel management, social security, taxation and other government departments are severely affected. Identity card, social security, phone, credit card, medical, financial, insurance and other related information are hackers’ targets. From now, database drag attacks, excessive acquisition of terminal Trojans and APPs, hijacking traffic information, have become the three main channels of data breach. Behind the information leakage, there is a complete chain of interest. Such user information is used for fraud, phishing, or precision marketing.

Every “database drag” incident is the cause for concern, but in fact, damages relying on such data are often already reached earlier. When exposed, their “values” have already decreased. Many data are fully utilized by attackers, and resold many times before exposure. Currently, the underground industry chain of data breach has matured, and has complete labor division procedures, which often include: database drag, data wash, data collision, another data wash, and other stages. Currently, the underground industry has formed an “integrated service proxy mechanism” docking with the demands. After the “demand side” put forward the goal, the “business agent” will find the “attacker”, the “attacker” successfully drags the database and gets the commission. Then, the attacker washes the data, extracting those (pre-deposit or virtual currency accounts) can be turned to cash. After that, these data will be used for collision, trying to land other valuable websites, and then those collide successfully will be used repeatedly.

Over time and mutual exchange, the attacker organization and hacker gang will have an increasingly larger database, with increasingly rich data types and more serious harm.

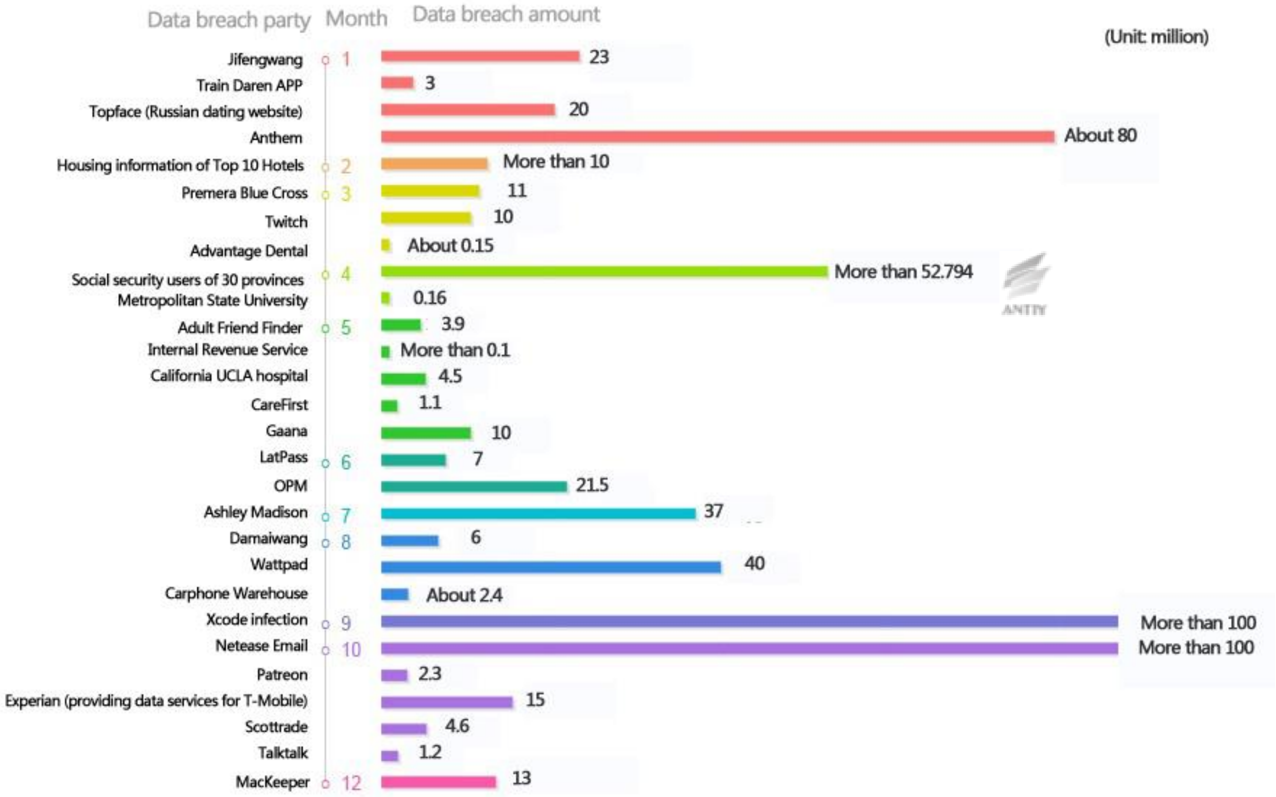


Figure 7 Significant data breaches in 2015

Not all data were obtained from the “database drag” attacks, they can also be acquired directly from the terminals and traffic. In 2015, among information leaks caused by malware, XcodeGhost event [5] needs all IT professionals to reflect. As of September 20, 2015, the cumulative total of 692 kinds of APPs found to be contaminated, including WeChat, DiDi Taxi, Netease Cloud Music and other popular applications. Despite the belief that the stolen information has "limited values", but on the one hand, the number is very large, the subsequent risks may also be very serious; on the other hand, contaminate the products via implanting malicious code to the development tool is worthy of our vigilance. At the same time, this incident uses the unofficial supply chain, reflecting the low security awareness of some IT employees.

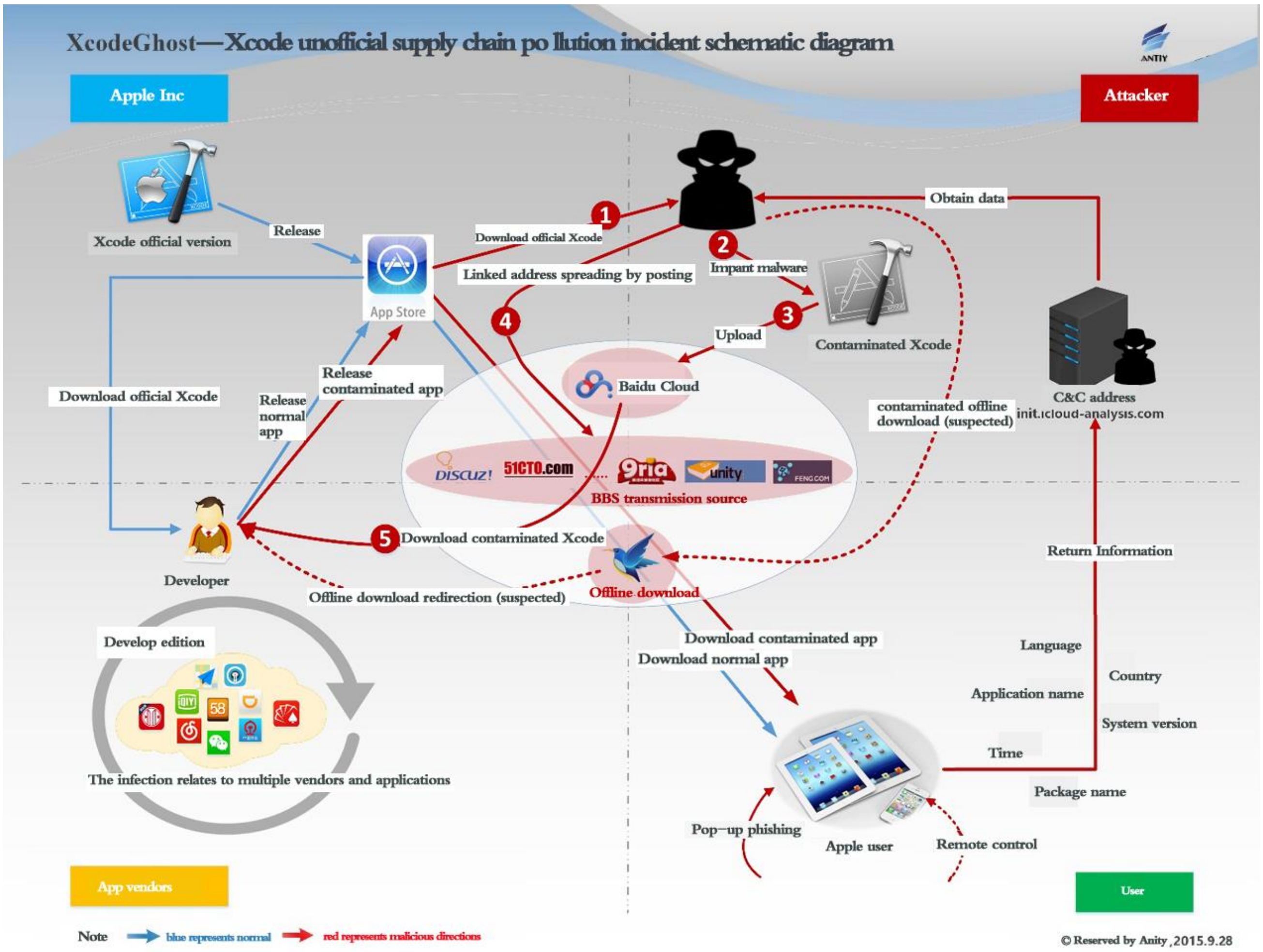


Figure 8 Antiy's unofficial supply chain pollution schematic drawing in XcodeGhost incident report

SMS intercepted Trojans appeared constantly with new varieties in 2015, and stolen user’s contacts, SMS, equipment information, etc. by combining with viral social engineering means, such as the "Album Trojan" analyzed by Antiy this year. [6] From the aspect of PC, the Tepfer Trojan family that emerged in 2011 is still active now with hundreds of th Tepfer ousands of varieties. The Tepfer Trojan family can steal more than 60 kinds of TP client software saved passwords, more than 10 kinds of browser saved passwords, 31 kinds of Bitcoin information; and it can get multiple mail client saved passwords, which can spread through spam, automatic stealing and upload without interaction.

Large amount of data breach, on the one hand, makes user's virtual property threatened, on the other hand, also make various fraud and precise phishing attacks easier. Most of previous fraud behaviors adopted the form of a wide net, and a large amount of data breach improves hacker's social library that can use leaked information to match and precisely locate users, which can make fraud and phishing attacks more deceptive.

Looking from the past, most of the activities at traffic side are achieved by hijacking and diddling to click pages, but this general traffic hijack also equips with the ability of traffic side stealing, which is a highly threat for HTTPS network. What's more, the HTTPS over the past two years, also exposed a lot of project implementation problems, including the challenge of CDN, etc.

A person's identity is almost permanent and relationship is basically stable, and the impact of data breach is difficult to dilute in a short time. A notable case is that, with the scale expansion of dark industry of network, these data will continue to import into the "infrastructure" of dark industry of network, which may make it equip with the ability that beyond the public safety and security vendors. Meanwhile, it is possible that the dark industry of network can change to serve for dark industry and "white-hat" at the same time in the form of "threat information".

Responsible Vulnerability Disclosure Mechanism and More Exquisite Vulnerability Emergency Guidance Are Needed

In 2015, Antiy sent 7780 vulnerabilities to CNVD (China National Vulnerability Database) totally, but frankly speaking, this is not what we are specialized in.

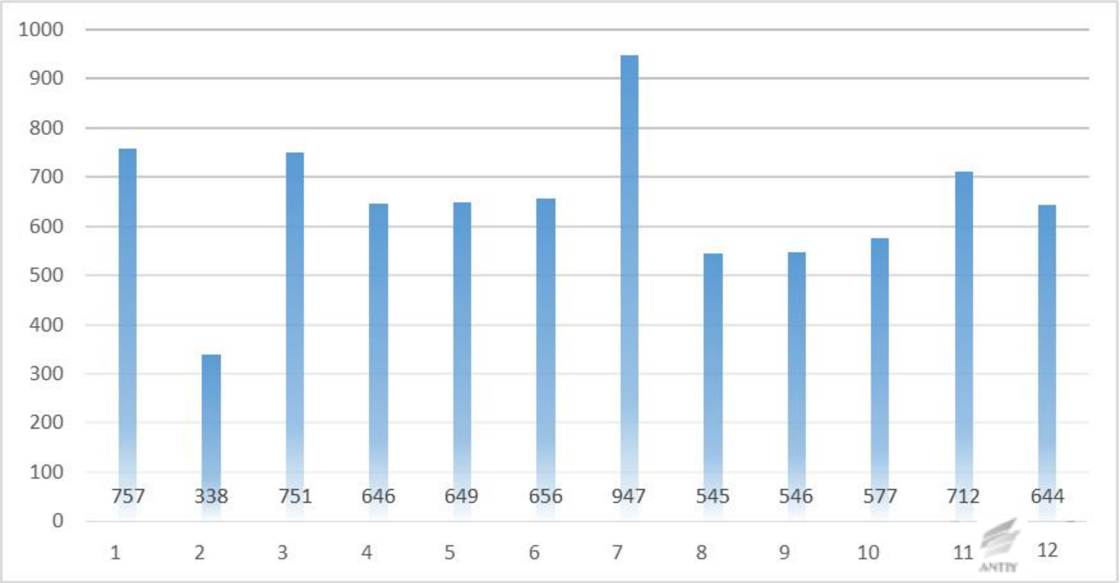


Figure 9 Reported vulnerabilities by Antiy per month in 2015

Google's security team found a vulnerability of Windows 8.1 and released details of it on the 90th day on condition that Microsoft has not yet repaired it. This accident has aroused great discussion of vulnerability disclosure ways. Microsoft said that Google completely put personal interests above user security, and some people think that

Google's behavior has fully respected users. In order to seek a balance between protecting user security and users' right to know, some vulnerability discourse ways tend to be more flexible. For example, some vulnerability platforms have blocked out some sensitive information in this year's vulnerability information such as IP address, domain names, and try to make manufacturers with vulnerabilities avoid Microsoft embarrassment. There is a fierce debate on a pseudo base-station in 2015. As the infrastructure and important system vulnerabilities with huge repairing cost and lacking of fast repair, how to conduct a responsible disclosure is a problem that needs to discuss. "Ghost" was found in early 2015, existing in GLib repository. GLib is the lowest API in Linux system and almost any other runtime library will depend on it. Apart from the encapsulation system services provided by Linux operating system, GLib offers many other service functions. "Ghost" vulnerability affects almost all Linux operating system and some researchers assume that it is as influential as "Bash Shellshock".

Adobe Flash security has always been controversial which is known as "Arsenal in dark industry of network". APT28 and Pawn storms also use the zero-day vulnerabilities of Adobe Flash to attacks with the reported Flash vulnerabilities up to more than 300 in 2015 annual report. Hacking - Team data breach pushed the damage and impact of Flash damage to the vertice of that year and the exposed three vulnerabilities can affect all versions of Flash in almost all platforms. The second found vulnerability (CVE - 2015-5122) is dubbed as "the most beautiful Flash vulnerability over the past four years by hackers.

At the end of 2015, the so-called "Damage King" Java deserialization broke out. Early on Jan.28, 2015, a report that Java deserialization vulnerability can use the commonly used Java library Apache Commons Collections to realize arbitrary code execution, which did not cause much attention. It is able to realize the remote code execution and leak database after access permissions in WebLogic, WebSphere, JBoss, Jenkins and OpenNMS. Nine months after the disclosure of this vulnerability, there is still not an effective patch with its harmful effects for a long time. At present, a large number of government portal websites and information management system are severely influenced by this vulnerability and the WebLogic and JBoss application servers are the most influential.

The forecasting ability of serious vulnerability is falling, from the "HeartBleed" in 2014 and "Bash Shellshock" to "Ghost" in 2015 and in the following fast tracking of vulnerabilities, some industries began to gradually lose patience to guide the user to prevent and fine traditional emergency disposal. It does not need to attract much attention, but is essential for institutions and industry users.

Ransomware leading PC malware threat awareness, becoming user’s nightmare

In 2015, Antiy captured 3109 PC new malware families and 2243062 kinds of new varieties, which covered the million-level of sample HASH. Compared with 2014, the total number of malware is increased, but cannot be compared with the explosive growth from 2006 to 2012.

What needs to illustrate is that we are unable to ensure statistics being fully accurate and the decrease of the number of new families cannot fully reflect the actual situation of malware. It is the result of relying on automatic naming and a large number of samples can only be given general names. Although we still try our best to maintain a complete naming system. When facing with rapid expansion of malware and its open source and trading over the past years, almost all the security vendors lose the associative and following up ability to name adoptive families based on strict coding.

Manufacturers always name malware by compiler or according to its behavior, such as Agent, which is a proof of this dilemma. And there is not enough information of some short WebShell to determine its evolution and association. Today, we should analyze on the basis of practice and search the relationship between malware and security events and malware through the association of vectors and behaviors, rather than automation.

In the Top 10 malware family variations, Trojans program takes up six seats and the other four are dominated by a relatively lightweight Hacktool and Grayware (also called PUA, i.e., applications that do not need).The proportion has changed a lot compared with the list of Trojan monopoly situation in 2014. In the case of more diverse channels of Internet economy, some operations of the attackers are tended to be more hidden. The main functions of listed malware is to download, bundling, espionage, remote control, etc., for instance, Mauritius/Win32 Badur is a Trojan that downloads and installs a large number of applications for benefits, which can download software and install specified applications in user system by a silent way to get benefits from vendors or promoters.

This year, three ads program ranked apart from AdLoad that is named by behavior (not all families have homology). Two other advertising programs are Eorezo and Browsefox with a large family affinity and the digital signatured samples take up 32.9% and 79.9% respectively. They spread through bundling with other programs, downloading websites and downloaders, etc. and the installation mode is usually silent installation. The main functions are to redirect browser hijackers and domain name and display a variety of online advertising company ads by modifying user search results for a benefit. The eighth prank program ArchSMS is actually a ransomware that has been infected widely, which will pop up warning window, notify the user that system disk is formatted (actually not format, so it is regarded as prank application) to threaten users to send messages.

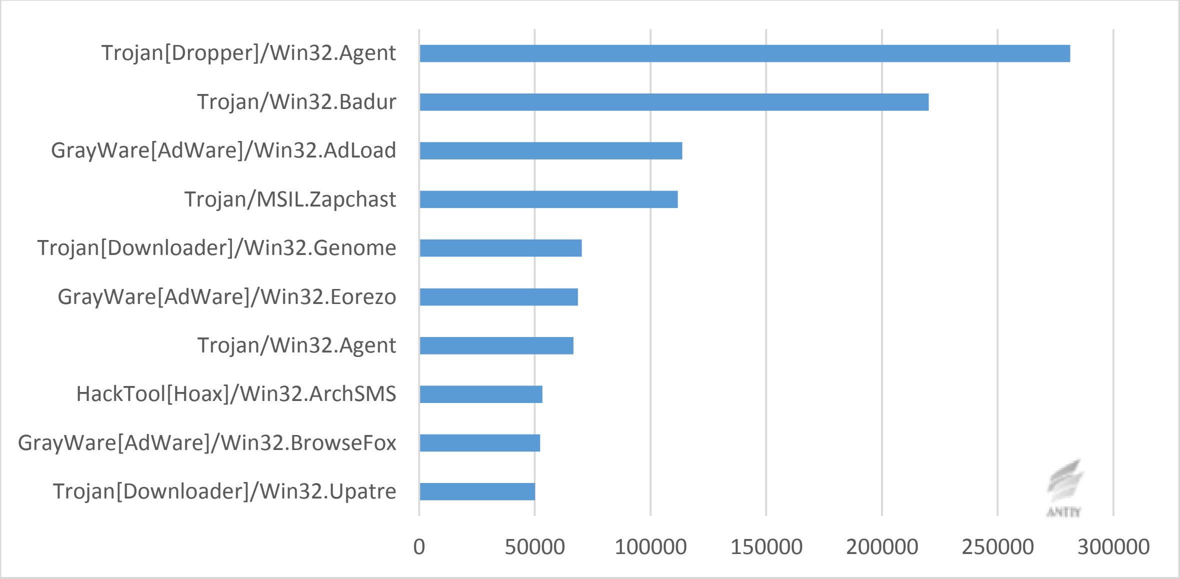


Figure 10 Ranking list of malware family variation number in 2015

In the 2015 PC platform malware behavior classification list (HASH), the advertising behavior for benefits still ranked first, and the download behaviors are still more because of its concealment and practical quantity, the bundling behavior and backdoor got the third and fourth place and the high-profile ransomware ranked ninth. Antiy CERT issued a report named “Uncover real ransomware” [7] on August 3, 2015, which introduced ransomware’s mode of transmission, form of ransom, historical evolution and corresponding defensive strategy in detail. On December 4, 2015, we released an analysis report of “Blackmailer Trojans spreads JS script by mails” according to a ransomware that based on JS script to spread by email [8].

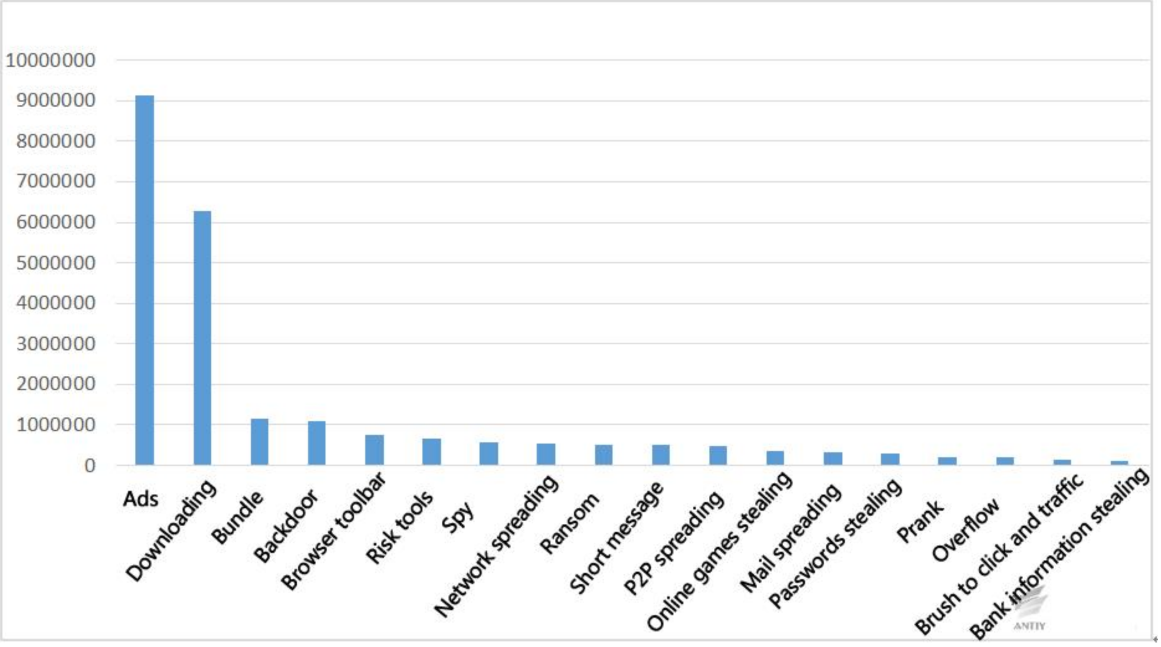


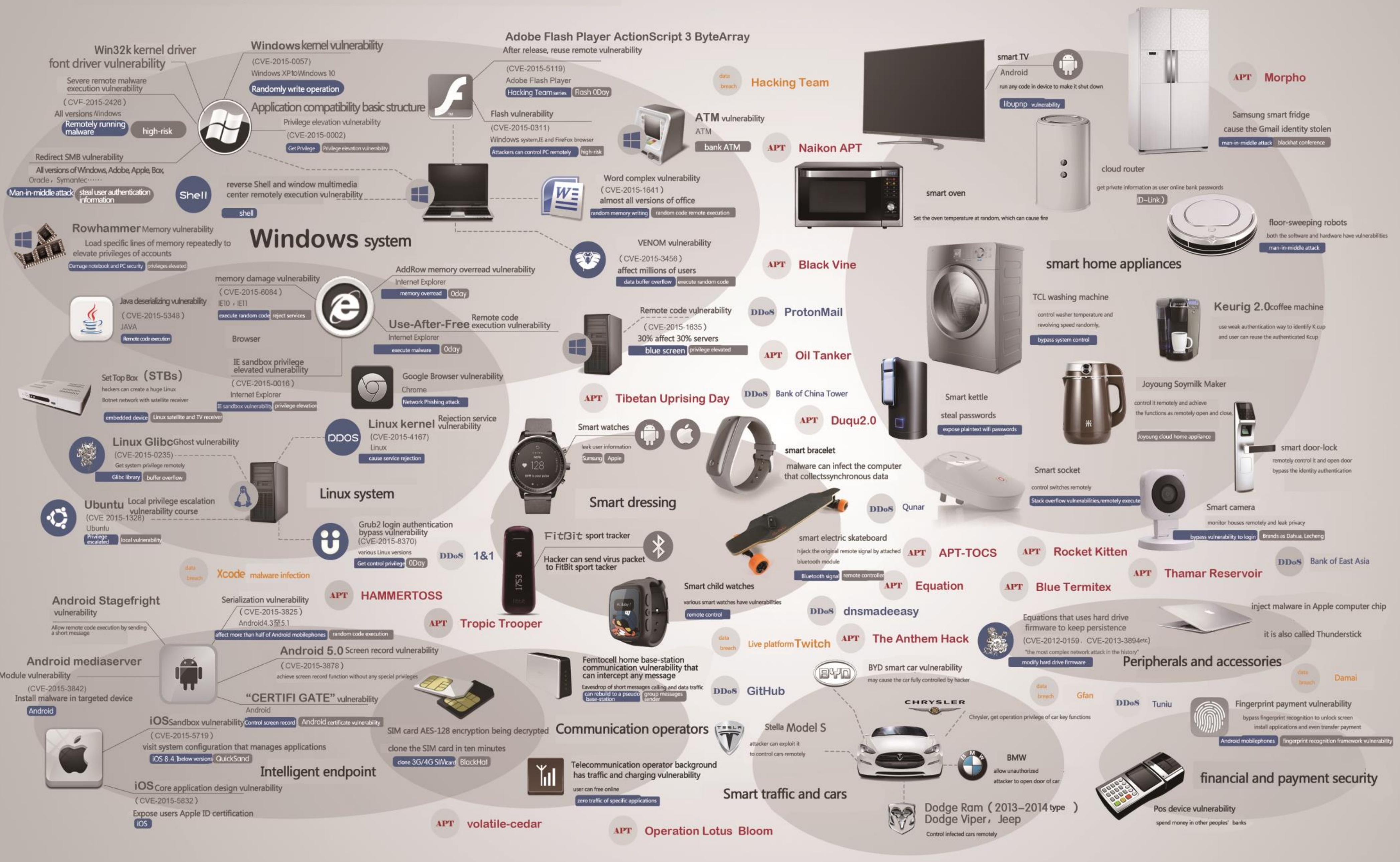
Figure 11 Ranking list of 2015 PC malware behavior

Threats Will Diffuse and Generalize in Depth

In 2013, we use the word Malware/Other to illustrate that security threats evolve to new areas as the smart devices, and Malware/Other has been targeted as the main trend of threat. In these two years, in addition to the familiar Windows, Linux and other Unix systems, iOS and Android platform, etc., security threats have permeated in smart cars, smart home appliances, smart dressing to large cities.

In 2015, this kind of security threat has become very common, however, we still adopt the same way as our annual report published in 2014, here is a figure to show the situation of 2015 threat generalization.

2015 Network Security Threat Distribution



Windows system

Win32k kernel driver
font driver vulnerability
Severe remote malware
execution vulnerability
（CVF-2015-2426）
All versions Windows
Remotely running malware
high-risk

Windows kernel vulnerability
(CVE-2015-0057)
Windows XP to Windows 10
Randomly write operation

Application compatibility basic structure
Privilege elevation vulnerability
(CVE-2015-0002)
Get Privilege
Privilege elevation vulnerability

Redirect SMB vulnerability
All versions of Windows, Adobe, Apple, Box,
Oracle，Symantec……
Man-in-middle attack
steal user authentication information

Shell
reverse Shell and window multimedia
center remotely execution vulnerability
shell

Rowhammer Memory vulnerability
Load specific lines of memory repeatedly to
elevate privileges of accounts
Damage notebook and PC security
privileges elevated

Adobe Flash Player ActionScript 3 ByteArray
After release, reuse remote vulnerability
(CVE-2015-5119)
Adobe Flash Player
Hacking Team series
Flash 0Day

Flash vulnerability
(CVE-2015-0311)
Windows system,IE and FireFox browser
Attackers can control PC remotely
high-risk

ATM vulnerability
ATM
bank ATM

Word complex vulnerability
（CVE-2015-1641）
almost all versions of office
random memory writing
random code remote execution

VENOM vulnerability
（CVE-2015-3456）
affect millions of users
data buffer overflow
execute random code

Browser

memory damage vulnerability
（CVE-2015-6084）
IE10，IE11
execute random code
reject services

AddRow memory overread vulnerability
Internet Explorer
memory overread
0day

Use-After-Free Remote code execution vulnerability
Internet Explorer
execute malware
0day

Java deserializing vulnerability
（CVE-2015-5348）
JAVA
Remote code execution

IE sandbox privilege
elevated vulnerability
（CVE-2015-0016）
Internet Explorer
IE sandbox vulnerability
privilege elevation

Google Browser vulnerability
Chrome
Network Phishing attack

Remote code vulnerability
（CVE-2015-1635）
30% affect 30% servers
blue screen
privilege elevated

Linux system

Set Top Box （STBs）
hackers can create a huge Linux
Botnet network with satellite receiver
embedded device
Linux satellite and TV receiver

Linux Glibc Ghost vulnerability
(CVE-2015-0235)
Get system privilege remotely
Glibc library
buffer overflow

DDOS
Linux kernel Rejection service vulnerability
(CVE-2015-4167)
Linux
cause service rejection

Ubuntu Local privilege escalation
vulnerability course
(CVE 2015-1328)
Ubuntu
Privilege escalated
local vulnerability

Grub2 login authentication
bypass vulnerability
(CVE-2015-8370)
various Linux versions
Get control privilege
0Day

data breach Xcode malware infection

Intelligent endpoint

Android Stagefright
vulnerability
Allow remote code execution by sending
a short message

Serialization vulnerability
（CVE-2015-3825）
Android4.3至5.1
affect more than half of Android mobilephones
random code execution

Android mediaserver
Module vulnerability
(CVE-2015-3842)
Install malware in targeted device
Android

Android 5.0 Screen record vulnerability
（CVE-2015-3878）
achieve screen record function without any special privileges

“CERTIFI GATE” vulnerability
Android
Control screen record
Android certificate vulnerability

iOS Sandbox vulnerability
（CVE-2015-5719）
visit system configuration that manages applications
iOS 8.4.1below versions
QuickSand

iOS Core application design vulnerability
（CVE-2015-5832）
Expose users Apple ID certification
iOS

Smart dressing

Smart watches
leak user information
Samsung
Apple

smart bracelet
malware can infect the computer
that collectssynchronous data

FitBit sport tracker
Hacker can send virus packet
to FitBit sport tacker

smart electric skateboard
hijack the original remote signal by attached
bluetooth module
Bluetooth signal
remote controller

Smart child watches
various smart watches have vulnerabilities
remote control

Communication operators

SIM card AES-128 encryption being decrypted
clone the SIM card in ten minutes
clone 3G/4G SIMcard
BlackHat

Femtocell home base-station
communication vulnerability that
can intercept any message
Eavesdrop of short messages calling and data traffic
can rebuild to a pseudo base-station
group messages sender

Telecommunication operator background
has traffic and charging vulnerability
user can free online
zero traffic of specific applications

smart home appliances

smart TV
Android
run any code in device to make it shut down
libupnp vulnerability

smart oven
Set the oven temperature at random, which can cause fire

cloud router
get private information as user online bank passwords
(D–Link)

Samsung smart fridge
cause the Gmail identity stolen
man-in-middle attack
blackhat conference

floor-sweeping robots
both the software and hardware have vulnerabilities
man-in-middle attack

TCL washing machine
control washer temperature and
revolving speed randomly,
bypass system control

Keurig 2.0coffee machine
use weak authentication way to identify K cup
and user can reuse the authenticated Kcup

Smart kettle
steal passwords
expose plaintext wifi passwords

Joyoung Soymilk Maker
control it remotely and achieve
the functions as remotely open and close,
Joyoung cloud home appliance

smart door-lock
remotely control it and open door
bypass the identity authentication

Smart socket
control switches remotely
Stack overflow vulnerabilities,remotely execute

Smart camera
monitor houses remotely and leak privacy
bypass vulnerability to login
Brands as Dahua, Lecheng

Peripherals and accessories

Equations that uses hard drive
firmware to keep persistence
(CVE-2012-0159，CVE-2013-3894etc)
"the most complex network attack in the history"
modify hard drive firmware

inject malware in Apple computer chip
it is also called Thunderstick

Smart traffic and cars

BYD smart car vulnerability
may cause the car fully controlled by hacker

Stella Model S
attacker can exploit it
to control cars remotely

CHRYSLER
Chrysler, get operation privilege of car key functions

BMW
allow unauthorized
attacker to open door of car

Dodge Ram（2013–2014 type ）
Dodge Viper，Jeep
Control infected cars remotely

financial and payment security

Fingerprint payment vulnerability
bypass fingerprint recognition to unlock screen
install applications and even transfer payment
Android mobilephones
fingerprint recognition framework vulnerability

Pos device vulnerability
spend money in other peoples' banks

data breach Hacking Team
APT Naikon APT
APT Black Vine
DDoS ProtonMail
APT Oil Tanker
APT Tibetan Uprising Day
DDoS Bank of China Tower
APT Duqu2.0
DDoS Qunar
DDoS 1&1
APT HAMMERTOSS
APT Tropic Trooper
APT APT-TOCS
APT Rocket Kitten
APT Thamar Reservoir
DDoS Bank of East Asia
APT Equation
APT Blue Termitex
DDoS dnsmadeeasy
data breach Live platform Twitch
APT The Anthem Hack
DDoS GitHub
data breach Gfan
DDoS Tuniu
data breach Damai
APT Morpho
APT volatile-cedar
APT Operation Lotus Bloom

Quoted from “2015 network security annual report of Antiy Labs ”

ANTIY

Prospect of 2016

Prediction of 2016 network security situation

The speed of advanced threats changing to common threats will increasingly accelerate. Any subtle idea of APT attacks once being exposed, it will quickly be learned and imitated by other attackers. And the techniques of attackers that base on national and political groups can be more coupled with that of underground industry. As the commercial platform and commercial Trojan are figured by development cost saving, interference of tracking, etc, a growing number of attack organizations will adopt molding or half-molding business platforms, business Trojans and black industry big data infrastructure as the combined weapon of network attack. “Nuclear deterrence” needs considering, but the proliferation of weapons will bring more concerns.

Ransomware will become the most direct threat to worldwide individuals and even corporate customers. In addition to encrypting user files, blackmailing coins, ransoming attackers is likely to make more targeted attacks, such as combination of network penetration. There are some other delivery modes except mail. When after more email service provider open default fully encryption, it is difficult to effectively discover and block in traffic side. Thus, apart from the mail service providers having the responsibility to filter blackmailers, the terminal security vendors also have the responsibility.

The simple beacon sharing level of threat information will meet challenge, and the hidden traces of attack techniques that use scripts, memory-resident, no entity files, etc. will be more popular. For instance, the PowerShell used in APT - TOCS as file carrier to load malware. The simple file HASH share will not be able to effectively cope with it. In addition, as more attackers occupying a variety of network equipment resources, more covert communications will gradually render more attackers to get rid of the dependence on fixed domain of C&C. The communication beacon detection based on file HASH and address will take a dominate role in the fight against APT attacks. At the same time, we need to remind our colleagues, the threat information sharing system also has the possibility of contamination.

“Upstream manufacturers” will suffer from more attacks, which will lead to the increased vulnerability of entire supply chain and tool chain. Attackers will target at third party suppliers with weak protection ability and attack enterprises with strengthened capability of protection by its trusted identity as the springboard, which will result in a more widespread impact. For example, the attack on analysis tools and safety tools can affect reverse enthusiasts and malwares analysts; the attacks on development scenarios can affect large amount of high sensitive users and the users will determine it as a trusted application or software; pre-installation of malware on factory equipment can directly affect the users. Therefore, both the upstream manufacturers and developers need to take effective protection responsibility. At the same time, OEM, OEM behavior, piracy tool chain, etc. also makes the threat map more complex and the call for transparency of supply chain needs to take action.

What we need to pay attention to is that the promotion of Internet leads to the development of traditional industries by many countries, including China, and network security threats will also approach to traditional industrial and infrastructure.

We are on the road

In 2015, Antiy has changed from anti-virus detection engine vendor to an advanced threat detection ability manufacturer, the initially formed “Antiy Labs” as the base with two wings of “enterprise security” and “mobile security (AVL TEAM)”. We hope to depend on effectively detection and analysis ability and data reserve, rely on long-term attempts and accumulation against malware and APT, in order to create more effective and immediate security for users.

Meanwhile in the past year, we have improved our products to obtain more effective cache and backtracking ability. We improved the sandbox technology that can trigger malicious behavior more effectively and the deepening revealing ability of PE samples; we make the antivirus engine become a knowledge system rather than simply act as an identification device; we also continue to improve the security of research and investment related to mobile areas. We also got a detection rate of full marks in two tests of AV – C, which is only one vendor worldwide. Through the improvement, Antiy have formed with PTD (persistent threat detection system) (Antiy VDS network virus detection system) as the lateral traffic probe, IEP (intelligent endpoint protection system) as the terminal defense, PTA (persistent threat analysis) ability as the advanced threat detection protection scheme, and met the needs of industry users and departments by combining situational awareness and early warning reports.

We focus on threat information sharing mechanism and big data. We also believe that threat intelligence is not only a simple beacon mining and swaps, but needs reliable security threat detection ability. At the same time, to be alert that sharing system can be upstream polluted, which will result in information value descending or even an opposite effect.

The transformation of forwarding products can provide better service for customers, but we are still focus on against-APT and against malware. We will neither swing with the new concept, nor being tempted by a “perfect” solution.

Besides our responsibility of the user, Antiy will cherish the interaction with brother companies and act as antivirus engine vendors.

We support the threat information through reliable detection, output ecological security by detection ability.

This is the responsibility of Antiy at present and in future.

Retrospect of 2015

In the 15 years of Antiy when early Antiy CERT analysists almost at the age of forties, we have to recognize that we have hesitated and moved.

Security workers and security threats are in a never ending competition, competing not only for power, but also spirit and volition. Whether the underground economy practitioners’ pursuit of interests, or the determination of APT attack sponsors are driving them.

What we need to insist on is not only the diligence and determinacy, but our integrity. We insist on the defender's position, insist on the mission of safeguarding user value, insist on the empathy feelings of security threat to victims and adhere to principles and rules, which is the basis and prerequisite of our company. Because only in this way, can we achieve our efforts and progress!

Appendix 1: References

[1] A Trojan That Can Modify the Hard Disk Firmware——*A Discovery to the Attack Components of the EQUATION Group*

http://www.antiy.net/p/a-trojan-that-can-modify-the-hard-disk-firmware/

[2] Analysis on the Encryption Techniques of EQUATION Components

http://www.antiy.net/p/analysis-on-the-encryption-techniques-of-equation-components/

[3] Analysis on APT-to-be Attack That Focusing on China’s Government Agency

http://www.antiy.net/p/analysis-on-apt-to-be-attack-that-focusing-on-chinas-government-agency/

[4] An Analysis on Targeted Trojan Attack with “Interview” as a Social Engineering Tool

http://www.antiy.net/p/an-analysis-on-targeted-trojan-attack-with-interview-as-a-social-engineering-tool/

[5] Analysis and Review of Xcode Unofficial Supply Chain Pollution Incident (XcodeGhost)

http://www.antiy.net/p/analysis-and-review-of-xcode-unofficial-supply-chain-pollution-incident-xcodeghost/

[6] Comprehensive Analysis Report on TROJAN/ANDROID.EMIAL.AS[RMT,PRV,EXP], “PHOTO ALBUM”

http://www.antiy.net/p/comprehensive-analysis-report-on-trojanandroid-emial-asrmtprvexp-photo-album/

[7] Uncovering the Face of Ransomware

http://www.antiy.net/p/uncovering-the-face-of-ransomware/

[8] An Analysis Report of Blackmailer Trojan Spread by Emailing JS Script

http://www.antiy.net/p/an-analysis-report-of-blackmailer-trojan-spread-by-emailing-js-script/

Appendix 2: About Antiy

Starting from antivirus engine research and development team, Antiy now has developed into an advanced security product supplier with four research and development centers, nationwide detection and monitoring ability as well as products and services covering multiple countries. With a fifteen-year continual accumulation, Antiy has formed massive security knowledge and promoted advanced products and solutions against APT with integrated application of network detection, host defense, unknown threat identification, data analysis and security visual experiences. With the recognition of technical capacity by industry regulators, customers and partners, Antiy has consecutively awarded qualification of national security emergency support unit four times and one of the six of CNNVD first-level support units. Antiy detection engine for mobile is the first Chinese product that obtained the first AV - TEST (2013) annual awards and more than ten of the world’s famous security vendors choose Antiy as their detection partner.

More information about antivirus engine: http://www.antiy.net