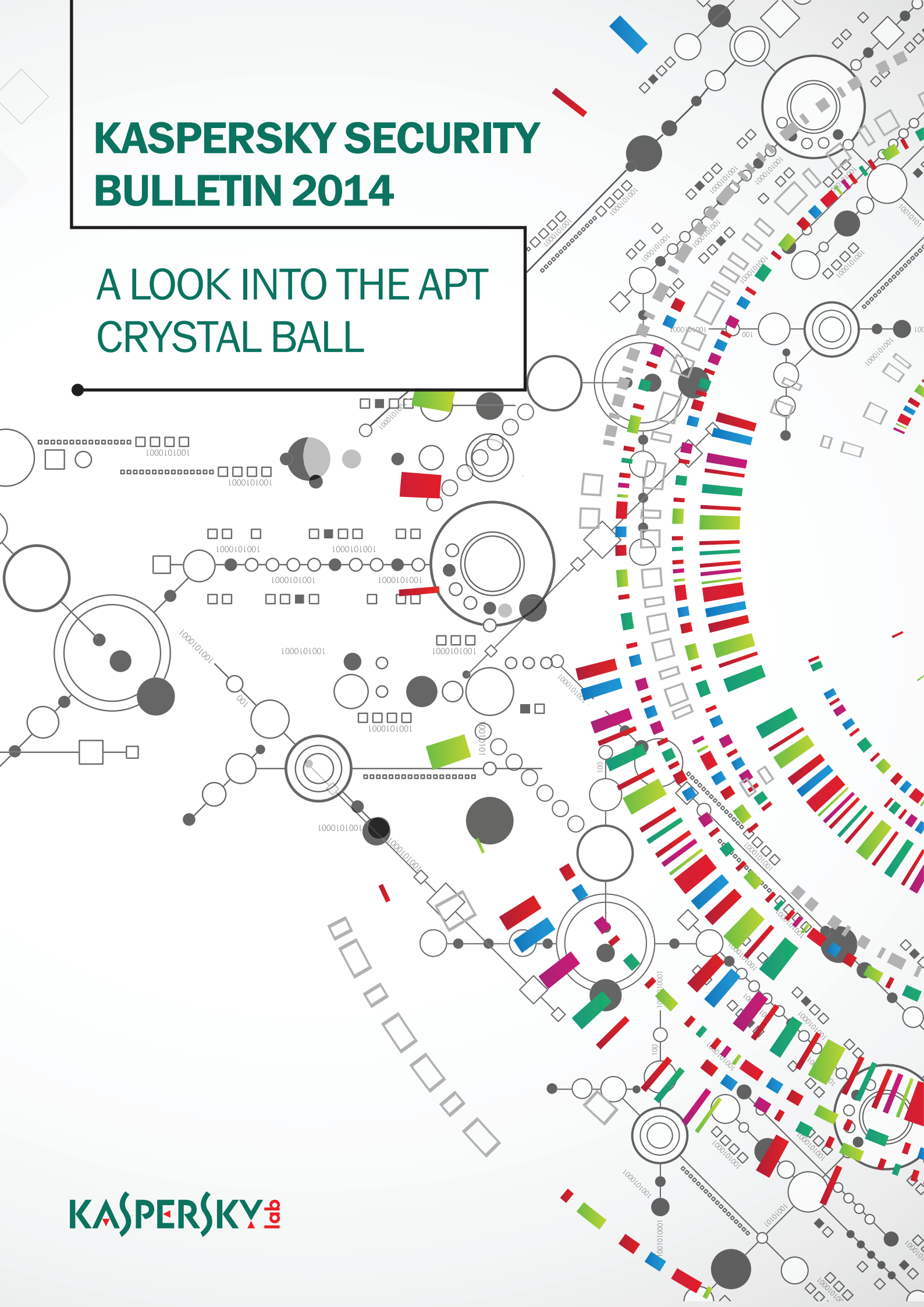
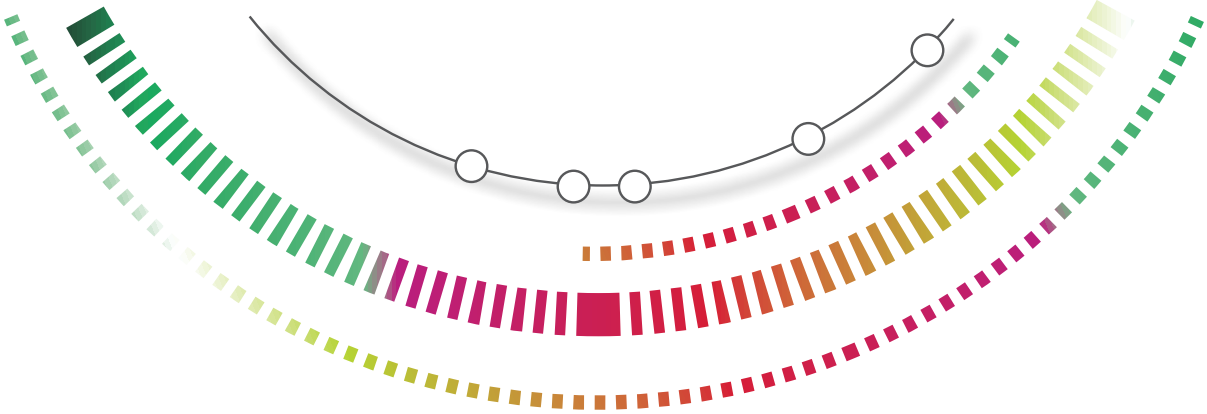
KASPERSKY SECURITY BULLETIN 2014

A LOOK INTO THE APT CRYSTAL BALL



KASPERSKY lab



CONTENT

Costin Raiu

Over the past years, Kaspersky's Global Research and Analysis Team (GReAT) has shed light on some of the biggest APT campaigns, including RedOctober, Flame, NetTraveler, Miniduke, Epic Turla, Careto/Mask and others. While studying these campaigns we have also identified a number of 0-day exploits, including the most recent CVE-2014-0546. We were also among the first to report on emerging trends in the APT world, such as cyber mercenaries who can be contracted to launch lightning attacks or more recently, attacks through unusual vectors such as hotel Wi-Fi. Over the past years, Kaspersky Lab's GReAT team has monitoring more than 60 threat actors responsible for cyber-attacks worldwide, organizations which appear to be fluent in many languages such as Russian, Chinese, German, Spanish, Arabic, Persian and others.

By closely observing these threat actors, we put together a list of what appear to be the emerging threats in the APT world. We think these will play an important role in 2015 and deserve special attention, both from an intelligence point of view but also with technologies designed to stop them.

THE MERGER OF CYBER-CRIME AND APT

For many years, cyber-criminal gangs focused exclusively on stealing money from end users. An explosion of credit card theft, hijacking of electronic payment accounts or online banking connections led to consumer losses in the worth hundreds of millions of dollars. Maybe this market is no longer so lucrative, or maybe the cybercriminal market is simply overcrowded, but it now seems like there is a struggle being waged for 'survival'. And, as usual, that struggle is leading to evolution.

What to expect: In one incident we recently investigated attackers compromised an accountant's computer and used it to initiate a large transfer with their bank. Although it might seem that this is nothing very unusual, we see a more interesting trend: **Targeted attacks directly against banks, not their users**.

In a number of incidents investigated by Kaspersky Lab experts from the Global Research and Analysis Team, several banks were breached using methods straight out of the APT playbook. Once the attackers got into the banks' networks, they collected enough information to enable them to steal money directly from the bank in several ways:

- Remotely commanding ATMs to dispense cash.
- Performing SWIFT transfers from various customer accounts,
- Manipulating online banking systems to perform transfers in the background.

These attacks are an indication of a new trend that is embracing APT style attacks in the cybercriminal world. As usual, cybercriminals prefer to keep it simple: they now attack the banks directly because that's where they money is. We believe this is a noteworthy trend that will become more prominent in 2015.

2

FRAGMENTATION OF BIGGER APT GROUPS

2014 saw various sources expose APT groups to the public eye. Perhaps the best-known case is the FBI indictment of five hackers on various computer crimes:

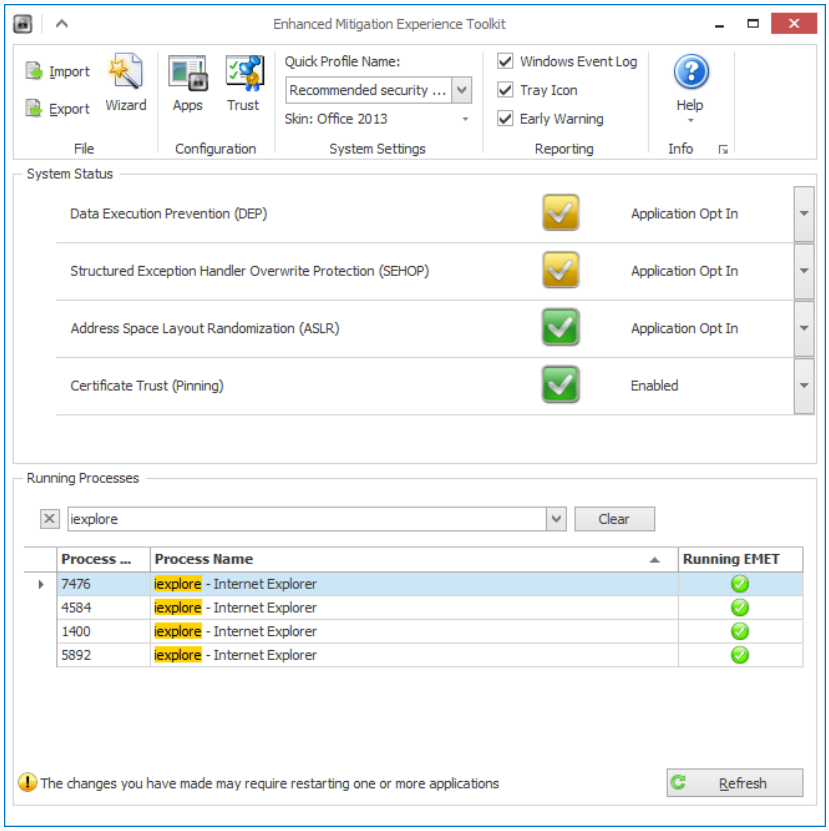
This public "naming and shaming" means we expect some of the bigger and "noisier" APT groups to shatter and break into smaller units, operating INDEPENDENTLY.

What to expect: This will result in a more widespread attack base, meaning more companies will be hit, as smaller groups diversify their attacks. At the same time, it means that bigger companies that were previously compromised by two or three major APT groups (eg. Comments Crew and Wekby) will see more varied attacks from a wider range of sources.

3

EVOLVING MALWARE TECHNIQUES

As computers become more sophisticated and powerful, operating systems also become more complex. Both Apple and Microsoft have spent a lot of time improving the security posture of their respective operating systems. Additionally, special tools such as Microsoft's EMET are now available to help thwart targeted attacks against software vulnerabilities.



With Windows x64 and Apple Yosemite becoming more popular, we expect APT groups to update their toolsets with more powerful backdoors and technologies to evade security solutions.

What to expect: Today, we are already seeing APT groups constantly deploying malware for 64-bit systems, including 64-bit rookits. In 2015, we expect to see more sophisticated malware implants, enhanced evasion techniques and more use of virtual file systems (such as those from Turla and Regin) to conceal precious tools and stolen data.

While we see these increases in advanced techniques, some attackers are moving in the opposite direction. While minimizing the number of exploits and amount of compiled code they introduce to compromised networks alto-

gether, their work continues to require sophisticated code or exploit introduction at a stable entry into the enterprise, script tools and escalation of privilege of all sorts, and stolen access credentials at victim organizations.

As we saw with BlackEnergy 2 (BE2), attackers will actively defend their own presence and identity within victim networks once discovered. Their persistence techniques are becoming more advanced and expansive. These same groups will step up the amount and aggression of destructive last effort components used to cover their tracks, and they include more *nix support, networking equipment, and embedded OS support. We have already seen some expansion from BE2, Yeti, and Winnti actors.

NEW METHODS OF DATA EXFILTRATION

The days when attackers would simply activate a backdoor in a corporate network and start siphoning terabytes of information to FTP servers around the world are long gone. Today, more sophisticated groups use SSL on a regular basis alongside custom communication protocols.

Some of the more advanced groups rely on backdooring networking devices and intercepting traffic directly for commands. Other techniques we have seen include exfiltration of data to cloud services, for instance via the WebDAV protocol (facilitates collaboration between users in editing and managing documents and files stored on web servers).

These in turn have resulted in many corporations banning public cloud services such as Dropbox from their networks. However, this remains an effective method of bypassing intrusion detection systems and DNS blacklists.

What to expect: In 2015, more groups to adopt use of cloud services in order to make exfiltration stealthier and harder to notice.

5

NEW APTS FROM UNUSUAL PLACES AS MORE COUNTRIES JOIN THE CYBER ARMS RACE

In February 2014, we published research into Careto/Mask, an extremely sophisticated threat actor that appears to be fluent in Spanish, a language rarely seen in targeted attacks. In August, we also released a report on Machete, another threat actor using the Spanish language.

Before that, we were accustomed to observing APT actors and operators that are fluent in relatively few languages. Additionally, many professionals do not use their native language, preferring instead to write in perfect English.

In 2014, we observed a lot of nations around the world publicly expressing an interest in developing APT capabilities:


SDA
SECURITY & DEFENCE AGENDA
SECURITY & DEFENCE AGENDA
A NEUTRAL PLATFORM FOR DISCUSSING DEFENCE AND SECURITY POLICIES
HOME POLICY AREAS ACTIVITIES LIBRARY PARTNERS MEMBERSHIP SECURITY JAM CYBER INITIATIVE
SWEDES WANT OFFENSIVE CYBER CAPABILITIES
18/10/2013
The Swedish armed forces want to attack other countries' computer networks, if need be. In a recent report, the armed forces stress the need to go on the offensive as part of its cyber defences.
The report notes that several countries already have or are currently developing a cyber defence that can also to launch cyber strikes. The conclusion of the report is that if Sweden does not keep up with this development, it risks becoming more vulnerable and exposed. In addition, the Swedish Armed forces want to develop capabilities in space and unmanned systems.
The opposing voices to the proposal argue that the armed forces do not have the budget to even carry out their current obligations and that investment should go to making the current system work properly.

What to expect: Although we haven't yet seen APT attacks in Swedish, we do predict that more nations will join the "cyber-arms" race and develop cyber-espionage capabilities.

USE OF FALSE FLAGS IN ATTACKS

Attackers make mistakes. In the vast majority of the cases we analyze, we observe artifacts that provide clues about the language spoken by the attackers. For instance, in the case of RedOctober and Epic Turla, we concluded that the attackers were probably fluent in the Russian language. In the case of NetTraveler we came to the conclusion that attackers were fluent in Chinese.

In some cases, experts observe other meta features that could point toward the attackers. For example, performing file timestamp analysis of the files used in an attack may lead to the conclusion in what part of the world most of the samples were compiled.

However attackers are beginning to react to this situation. In 2014 we observed several "false flag" operations where attackers delivered "inactive" malware commonly used by other APT groups. Imagine a threat actor of Western origin dropping a malware commonly used by a "Comment Crew," a known Chinese threat actor. While everyone is familiar with the "Comment Crew" malware implants, few victims could analyze sophisticated new implants. That can easily mislead people into concluding that the victim was hit by the Chinese threat actor.

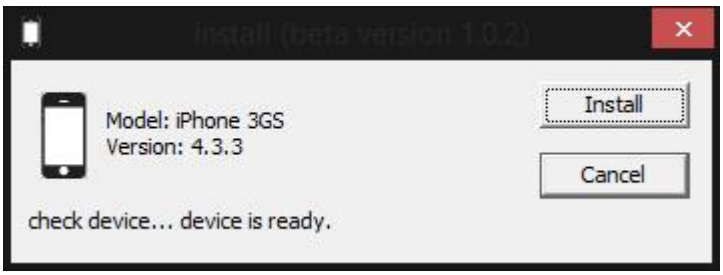
What to expect: In 2015, with governments increasingly keen to "name and shame" attackers, we believe that APT groups will also carefully adjust their operations and throw false flags into the game.

7

THREAT ACTORS ADD MOBILE ATTACKS TO THEIR ARSENAL

Although APT groups have been observed infecting mobile phones, this hasn't yet become a major trend. Perhaps the attackers wish to get data that isn't usually available on mobiles, or maybe not all of them have access to the technologies that can infect Android and iOS devices.

In 2014 we saw several new APT tools designed for infecting mobiles, for instance Hacking Team's Remote Control System mobile modules.



Additionally, during the Hong Kong protests in October 2014, attacks were seen against Android and iOS users which appear to be connected to APT operations.

Although a mobile phone might not have valuable documents and schematics, or geopolitical expansion plans for next 10 years, they can be a valuable source of contacts as well as listening points. We observed this with the RedOctober group, which had the ability to infect mobile phones and turn them into "Zakladka's", mobile bugs.

What to expect: In 2015, we anticipate more mobile-specific malware, with a focus on Android and jailbroken iOS.

APT+BOTNET: PRECISE ATTACK + MASS SURVEILLANCE

In general, APT groups are careful to avoid making too much noise with their operations. This is why the malware used in APT attacks is much less widespread than common crimeware such as Zeus, SpyEye and Cryptolocker.

In 2014 we observed two APT groups (Animal Farm and Darkhotel) using botnets in addition to their regular targeted operations. Of course, botnets can prove to be a vital asset in cyberwar and can be used to DDoS hostile countries; this has happened in the past. We can therefore understand why some APT groups might want to build botnets in addition to their targeted operations.

In addition to DDoS operations, botnets can also offer another advantage - mass surveillance apparatus for a “poor country”. For instance, Flame and Gauss, which we discovered in 2012, were designed to work as a mass surveillance tool, automatically collecting information from tens of thousands of victims. The information would have to be analyzed by a supercomputer, indexed and clustered by keywords and topics; most of it would probably be useless. However, among those hundreds of thousands of exfiltrated documents, perhaps one provides key intelligence details, that could make a difference in tricky situations.

What to expect: In 2015 more APT groups will embrace this trend of using precise attacks along with noisy operations and deploy their own botnets.

9

TARGETING OF HOTEL NETWORKS

The Darkhotel group is one of the APT actors known to have targeted specific visitors during their stay in hotels in some countries. Actually, hotels provide an excellent way of targeting particular categories of people, such as company executives. Targeting hotels is also highly lucrative because it provides intelligence about the movements of high profile individuals around the world.

Compromising a hotel reservation system is an easy way to conduct reconnaissance on a particular target. It also allows the attackers to know the room where the victim is staying, opening up the possibility of physical attacks as well as cyber-attacks.

It isn't always easy to target a hotel. This is why very few groups, the elite APT operators, have done it in the past and will use it as part of their toolset.

What to expect: In 2015, a few other groups might also embrace these techniques, but it will remain beyond the reach of the vast majority of APT players.

COMMERCIALIZATION OF APT AND THE PRIVATE SECTOR

Over the last few years, we published extensive research into malware created by companies such as HackingTeam or Gamma International, two of the best known vendors of "legal spyware". Although these companies claim to sell their software only to "trusted government entities", public reports from various sources, including Citizen Lab, have repeatedly shown that spyware sales cannot be controlled. Eventually, these dangerous software products end up in the hands of less trustworthy individuals or nations, who can use them for cyber-espionage against other countries or their own people.

The fact is that such activities are highly profitable for the companies developing the cyber-espionage software. They are also low risk because – so far – we have not seen a single case where one of these companies was convicted in a cyber-espionage case. The developers of these tools are usually out of the reach of the law, because the responsibility falls with the tool users, not the company that develops and facilitates the spying.

What to expect: It's a high-reward, low risk business that will lead to the creation of more software companies entering the "legal surveillance tools" market. In turn, these tools will be used for nation-on-nation cyber-espionage operations, domestic surveillance and maybe even sabotage.

CONCLUSIONS

In general, 2014 was a rather sophisticated and diverse year for APT incidents. We discovered several zero-days, for instance CVE-2014-0515 which was used by a group we call “Animal Farm”. Another zero-day we discovered was CVE-2014-0487, used by the group known as DarkHotel. In addition to these zero-days, we observed several new persistence and stealth techniques, which in turn resulted in the development and deployment of several new defense mechanisms for our users.

If we can call 2014 “sophisticated”, the word for 2015 will be “elusive”. We believe that more APT groups will become concerned with exposure and they will take more advanced measures to hide from discovery.

Finally, some of them will deploy false flag operations. We anticipate these developments and, as usual, will document them thoroughly in our reports.

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy