GLOBAL CYBER SECURITY INCIDENCE REPORT NOVEMBER 2014

1. Flashpack Exploit Kit Uses Ad Networks to Deliver Cryptowall, Dofoil Malware

Description

Researchers at Trend Micro have spotted a campaign in which attackers abuse advertising networks and the Flashpack exploit kit in an effort to distribute various pieces of malware, including the information-stealing malware Zeus, the Dofoil Trojan, and the Cryptowall ransomware.

Mode and basis of attack

The security firm says Flashpack uses free ads to distribute the threats. Researchers have been monitoring multiple URLs utilized by the exploit kit as landing pages and determined that they have been accessed mostly by users in North America.

When users access a website that serves malicious ads, they are taken via multiple redirects to a Flashpack exploit kit landing page, which is set up to serve a variant of the Dofoil Trojan (TROJ_DOFOIL.WYTU).

The Cryptowall ransomware, which encrypts files found on infected computers and keeps them that way until a ransom is paid, is distributed via SWF files containing exploit code for a Flash Player vulnerability (CVE-2014-0515) which Adobe patched in April following reports that it had been exploited in watering hole attacks.

"Ad-enabled free applications pose a serious threat to users and enterprises as attackers leverage this to distribute threats like Ransomware and DOFOIL. As such, this may lead to system infection and possible information and data theft.

How to handle such attack

End-users are recommended to be cautious with the applications that they install. Similarly, in enterprise setting, employees should be educated on what kind of application can be installed on their desktops. If possible, create IT policies (like Acceptable Usage Policies) that could be drafted by their internal governing bodies, such as their InfoSec department," Trend Micro researchers said in a blog post.

"Aside from this, the combination of ensuring that third party applications like Flash and Java that loaded is by Web browsers is something to note for end-user to enterprise users alike. If possible, use security software with web filtering functionalities that has the capability to block malware-related and ad-related sites," they added.

http://www.securityweek.com/flashpack-exploit-kit-uses-ad-networks-deliver-cryptowall-dofoil-malware

2. Critical Windows Vulnerability is used to spread Sandworm malware

Description

ISIGHT, the company that discovered this virus, says that Sandworm relies on a Windows zero-day vulnerability that is known as CVE-2014-4114. Fortunately, Microsoft patched this vulnerability in October, 2014. It has also been reported that this virus has mostly been used in Russian espionage campaigns targeting such domains as NATO, European Union, Energy Sector firms, Telecommunications United States academic organizations, etc. However, it seems that anyone can become a victim of Sandworm.

Mode and basis of attack.

The main thing that you have to know is how this malware travels around. It seems that it relies on a PowerPoint file that refers to an .INF file. The mostly used method for spreading such files around is with a help of misleading emails. Once a malicious PowerPoint file is downloaded onto the system, it pulls in two files that are known as slides.inf and slide1.gif. Once these files are active, they are used to make specific system modifications and install a virus. Note that malware itself is not hiding in this malicious PowerPoint file. It is downloaded latest without any permission asked.

How to avoid such attack

- If you want to avoid Sandworm virus, make sure you apply Microsoft's MS14-060 patch and fix CVE-2014-4114 vulnerability.
- In addition, installing a reputable security tool would help you to prevent infiltration of this attack and other malwares in the future.
- Always make sure that your anti-virus is up-to-date and that you are using the latest of its version.
- Finally, avoid misleading emails and do NOT download email attachments that came to your inbox from unknown sources.

http://www.2-spyware.com/news/post4871.html

3. Twitter to start snooping at which apps you have installed

Description

Twitter is set to start peeking on users' iPhones, iPads and Androids in order to see which apps they have downloaded.

The company will start collecting the list of apps installed on those smartphones and tablets so that it can, in its own words, "deliver tailored content that you might be interested in."

The additional data collection will allow Twitter to make better recommendations on who to follow, as well as insert content it thinks you will find interesting into your feed.

Mode of operation

The new feature, which Twitter has named "app graph," could tie in with the company's recently announced Instant Timeline feature which takes new users' areas of interest and the people their contacts follow, and serves up a feed created for them in order to better personalize Twitter from day one.

By collecting data about other installed apps, the feature would be better positioned to create a more relevant starting timeline.

The main benefit to Twitter will be the ability to use the collected information to surface more targeted adverts. Or, as Twitter puts it, show you more promoted content it "thinks you'll find especially interesting."

Twitter says it will only record the list of apps you have installed, not how they are used.

While entry into the new tracking system is automatic and opt-in by default, Twitter has promised to alert users when the new feature is turned on.

How to opt out

If you don't want your apps to be snapped up by Twitter's data gobblers, here's how to turn it off:

Twitter for Android

1. Tap the **overflow icon** (looks like 3 vertical dots)

2. Choose **Settings**.
3. Select your account
4. Under **other**, turn off **Tailor Twitter based on my apps**.

Twitter for iOS

1. Tap the **Me** tab, and then the gear icon
2. Choose **Settings**
3. Select your account
4. Under **Privacy**, turn off **Tailor Twitter based on my apps**.

Once you opt out, Twitter says it will remove your app graph data from Twitter and stop future collection.

If you don't yet see the option then Twitter won't have started tracking you yet.

If you want to stop the collection before it's started, Twitter says you can turn on **Limit Ad Tracking** on your iOS device by going to **Settings** and **Privacy**.

If you're an Android user, go to **Settings**, tap the **Google** account, choose **Ads** and then turn on **Opt out of interest-based ads**.

https://nakedsecurity.sophos.com/2014/11/27/twitter-to-start-snooping-at-which-apps-you-have-installed-heres-how-to-opt-out/?utm_source=Naked%2520Security%2520-%2520Feed

4. Brute-force Attacks: Crossing the Online-Offline Password Chasm

Description

Passwords are currently, and in the foreseeable future, our main method for online authentication. One of passwords most hated features is the complexity requirement that demands the password to have a minimum size, contain mixed-case letters, digits and special characters.

However, a new research paper from Microsoft Research claims that most of the complexity effort is in vain. Tal Be’ery the VP of Research at Aorato explained Microsofts conclusion and then took a look at two, newly presented solutions, to achieve truer password security.

Mode and nature of attack

Passwords needs to be strong enough to resist a guessing attack, often named a "Brute-force" attack. The brute-force attack comes in two flavors: online and offline. In the online mode of the attack, the attacker must use the same login interface as the user application. In contrast, the offline mode of the attack requires the attacker to steal the password file first, but enables an unconstrained guessing of passwords, free of any application or network related rate limitations. Microsoft researchers had found out that "an enormous gap exists between the effort needed to withstand online and offline attacks, with probable safety occurring when a password can survive 10^6(1M) and 10^{14} (100T) guesses respectively." As a result, having a not-so-complicated password such as "tincan24" that is "1M strong" (i.e. expected to survive a 1M guess attack) is as good as having a "1T strong" password "7Qr&2M". Both are strong enough to survive an online attack, but expected to surrender under an offline attack. However, the latter password is much harder to remember.

Furthermore, by breaking down the use of mixed-cases that necessitates offline guessing protection, the researcher were able to determine that "Offline guessing is a threat when the password file leaks, that fact goes undetected, and the passwords have been properly salted and hashed. In other cases, offline guessing is either unnecessary, not possible, or addressable by resetting system passwords."

Solving the Password File Leakage Problem

In order to prevent the password file from leaking to the outside world, it needs to be bounded to the application environment. The common solution, mentioned in Microsoft paper, is to encrypt each password and store the secret key in a Hardware Security Module (HSM). Since the HSM does not provide access to the stored secret key, password decryption can only take place in the application's environment.

Recently two other innovative solutions to this problem were presented:

1. At Derbycon 2014, Benjamin Donnelly and Tim Tomes presented their "Ball and Chain (BAC)" construction. BAC provides a method to artificially inflate the passwords file size and spread the password data securely across it, to make the exfiltration of it extremely difficult, if not outrightly impossible. For example, it would take an attacker at least a month to send a 2TB

password file over a regular internet connection. Besides taking a long time, the large amounts of data being sent should raise a security flag.

2. Dyadic, a new Israeli start-up company, had revealed its Distributed Security Module. By using the cutting-edge crypto technology of MultiParty Computation (MPC), the DSM splits each password secret across several servers. The attacker needs to breach the security of all involved servers in order to reveal the password. Since the servers can have different access credentials and even operating systems it makes the attacker task much more difficult.

The Take Home Message

Since "passwords are the worst form of authentication except all those other forms that have been tried", understanding their true pros and cons is highly relevant to the security of our systems. Therefore, defeating offline brute-force attacks should be addressed by the application through any of the aforementioned methods, and not to be handled as an extra burden on the users, via "password complexity".

http://www.securityweek.com/brute-force-attacks-crossing-online-offline-password-chasm

5. Regin: Nation-state ownage of GSM networks

Description

Regin is a cyber-attack platform which attackers deploy in the victim networks for ultimate remote control at all possible levels.

While in most cases, the attackers were focused on extracting sensitive information, such as e-mails and documents, there are cases where the attackers compromised telecom operators to enable the launch of additional sophisticated attacks.

Quick facts:

- The main victims of this actor are: telecom operators, governments, financial institutions, research organizations, multinational political bodies and individuals involved in advanced mathematical/cryptographical research.
- Victims of this actor have been found in Algeria, Afghanistan, Belgium, Brazil, Fiji, Germany, Iran, India, Indonesia, Kiribati, Malaysia, Pakistan, Syria and Russia.

- The Regin platform consists of multiple malicious tools capable of compromising the entire network of an attacked organization. The Regin platform uses an incredibly complex communication method between infected networks and command and control servers, allowing remote control and data transmission by stealth.
- One particular Regin module is capable of monitoring GSM base station controllers, collecting data about GSM cells and the network infrastructure.
- Over the course of a single month in April 2008 the attackers collected administrative credentials that would allow them to manipulate a GSM network in a Middle Eastern country.
- Some of the earliest samples of Regin appear to have been created as early as 2003.

Mode of attack

The exact method of the initial compromise remains a mystery, although several theories exist, which include man-in-the-middle attacks with browser zero-day exploits. The replication modules are copied to remote computers by using Windows administrative shares and then executed. This technique requires administrative privileges inside the victim's network. In several cases, the infected machines were also Windows domain controllers. Targeting of system administrators via web-based exploits is one simple way of achieving immediate administrative access to the entire network.

How to handle such attack:

Kaspersky products detect modules from the Regin platform as: **Trojan.Win32.Regin.gen** and **Rootkit.Win32.Regin**.

If you detect a Regin infection in your network, contact Kaspersky at intelservices@kaspersky.com

http://securelist.com/blog/research/67741/regin-nation-state-ownage-of-gsm-networks/

6. Helpful tips on how to protect your smartphone/tablet

Background

The term “Adware” describes an advertising-supported software, which seeks to make a profit out of commercial advertisements. There is a small line between legitimate advertising, illegal advertising and annoying advertising. Nonetheless, the fact is that the majority of free programs and apps are supported by advertising. That is how developers of such programs are making revenues. However, there is also another term that describes an application for smartphones and tablets that aggressively promotes various products and generates intrusive advertisements. Such programs are labeled as 'Madwares' (adwares that were developed entirely for smartphones/tablets).

Source of Reportage

Juniper Networks (Network Security and Performance) has recently released an interesting report about mobile threats. It looks like smartphones and tablet are becoming the main target for cyber criminals. Drastic increase has been noticed (approximately 615%, from 2012 till 2013) in cyber threats for smartphones/mobiles phones and tablets. Juniper Networks has managed to examine around 1, 85 million mobile apps and spotted more than 276,200 of malicious or hazardous apps.

It was estimated that almost every single person in the world that has a mobile phone, at some point have received a so-called SMS Trojan. This Trojan is a very primitive form of an online scam. Usually, you may get an SMS/MMS with some questionable phone number. Furthermore, if you reply or call the given number, you may get charged an enormous amount of money. That is how this scam works.

As more and more people are starting to use smartphones and tablets, cyber criminals, scammers and hackers are not standing still, and they are also trying to keep up with changing technologies. Thus, keeping that in mind, these security tips should be helpful for people who are using smartphones, mobile phones or tablets.

http://www.2-spyware.com/news/post4435.html

Measures

- Avoid questionable SMS/MMS

This tip should be useful for all mobile phone users, even if you are still using an old phone. Do not reply to questionable messages from unknown numbers. You should also avoid calling such numbers. If you do so, there is a high possibility that by the end of the month, you will receive an enormous phone bill.

- Avoid opening spam emails

  There is a possibility to get a virus, Trojan, potentially unwanted program or malware when opening corrupted spam email attachments. That is why you should be very careful when opening unfamiliar emails.

- Lock your phone

  Use 4 number PIN code in order to protect your SIM card. On top of that, protect your phone with a different code, voice unlock, fingerprint or a similar protection measure.

- Keep your OS updated

  Whether you are using an Android, Apple or a different device, you should keep your OS updated. Older versions of software may have vulnerabilities and flaws that new and updated versions should cover.

- Carefully choose what apps to install.

  As mentioned above, there are many applications that may try to initiate unwanted activities behind your back, such as tracking your online browsing habits, your location, etc. You shouldn’t blindly allow unfamiliar apps to track your location, access your personal information or access your photo profile.

- Online Shopping

  Avoid using questionable free apps for online shopping. There is no telling what information may be recorded if you use an unsafe app. If you are using your smartphone for online shopping, it is better to use a basic internet browser (Internet Explorer, Google Chrome, Apple Safari, Opera, Mozilla Firefox, etc.)

- Social networks

  The same rule applies to social networks as to online shopping. Avoid using unfamiliar apps in order to browse social networks. Your private information may be recorded and even used for various scams.

- Valuable files and documents

You should avoid keeping your credit card numbers, picture of your scanned passport, passwords (in text or as a photo file). It is highly recommended not to keep such information in your phone. No matter if you are keeping your private/valuable information in text files or you have taken a picture of your banking codes. Keep in mind that you may lose your phone, your phone may be stolen in the street by some burglar, or your phone may get hacked by cyber crooks.

- Wi-Fi connection

  If the Wi-Fi connection option is turned on, smartphones, tablets and even laptops are always scanning the nearby areas and looking for new connections. You may accidentally connect to an unsafe Wi-Fi and expose your computer to cyber criminals. If you are not using a Wi-Fi and you are not connected to one, you should switch it off.

- Bluetooth connection.

  The same rule applies to Bluetooth connection as to Wi-Fi connection.

- Browsing history.

  It is recommended to clean your browsing history (at least one time in a month) in order to remove various cookies, tracking beacons and similar files.

- Questionable ads

  Ads can be as dangerous as various Madwares, potentially unwanted programs, dubious apps and even malwares. Some cyber criminals may use ads in order to get your attention and to make you click them. Right after that, you may end up in an unsafe website and expose your device to various cyber threats. Such tricky ads may include promotions, notifications about prizes that you have allegedly won and even fake updates.

- Security Tool

  It is recommended to use a legitimate security tool that should protect your smartphone/tablet. Make a research and find the best tool that suits your needs. However, be careful and try not to download a spyware instead of a legitimate security program. As mentioned before, free programs are usually not the best solution if you are looking for a reliable program.

http://www.2-spyware.com/news/post4435.html

7. Cyberespionage Attacks Against Energy Suppliers

Overview

A cyberespionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims. The attackers, known to Symantec as “Dragonfly” and known by other vendors as “Energetic Bear”, managed to compromise a number of strategically important organizations for spying purposes and, if they had used the sabotage capabilities open to them, could have caused damage or disruption to the energy supply in the affected countries.

Dragonfly has used spam email campaigns and watering hole attacks to infect targeted organizations. The group has used two main malware tools: Trojan.Karagany and

Backdoor.Oldrea. The latter appears to be a custom piece of malware, either written by or for the attackers.

Victims of the Dragonfly group

The current targets of the Dragonfly group, based on compromised websites and hijacked software updates, are the energy sector and industrial control systems, particularly those based in Europe. While the majority of victims are located in the US, these appear to mostly be collateral damage. That is, many of these computers were likely infected either through watering hole attacks or update hijacks and are of no interest to the attacker.

Mode and basis of attack

Dragonfly uses two main pieces of malware in its attacks. Both are Remote Access Tool (RAT) type malware which provide the attackers with access and control of compromised computers. Dragonfly’s favored malware tool is Backdoor.Oldrea, which is also known as Havex or the Energetic Bear RAT. Oldrea acts as a back door for the attackers on to the victim’s computer, allowing them to extract data and install further malware.

Oldrea appears to be custom malware, either written by the group itself or created for it. This provides some indication of the capabilities and resources behind the Dragonfly group. The second main tool used by Dragonfly is Trojan.Karagany. Unlike Oldrea, Karagany was available on the underground market. The source code for version 1 of Karagany was leaked in 2010. Symantec believes that Dragonfly may have taken this source code and modified for its own use.

Symantec found that the majority of computers compromised by the attackers were infected with Oldrea.

Karagany was only used in around 5 percent of infections. The two pieces of malware are similar in functionality and what prompts the attackers to choose one tool over another remains unknown.

Protection

Symantec has the following detections in place that will protect customers running up to date versions of their products from the malware used in these attacks:

Antivirus detections

- Backdoor.Oldrea
- Trojan.Karagany
- Trojan.Karagany!gen1

Intrusion Prevention Signatures

- Web Attack: Lightsout Exploit Kit
- Web Attack: Lightsout Toolkit Website 4

http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat