

ENTER AT YOUR OWN RISK

January 2012 , Issue 08



Security-Shell
SecManiac Korben The Hacker News Security-FAQs
SECTECHNO



The Hacker News thought the best way to bring you the happiest of New Years was to bring together the best, the brightest, and the most competent of security experts in the field. Our special edition January Magazine does just that and you will find it choc-a-block filled with security news, information, instruction and just plain fun! We extend our most gracious thanks to **Security-Shell**, **SecManiac**, **Korben**, **Security-FAQ's** and **Sectecho** for providing such a comprehensive look at internet security, its issues, its growth and its possibilities.

For The Hacker News, the past year was full of surprises, and many of the accomplishments we made were because of you. We are grateful for our loyal readership and welcome new readers and contributors. The Hacker news has tracked the events of the last year and we are amazed at the talent and finesse of "Techie" people all over the world who can break into the most complicated and sophisticated systems. We love reporting your hacking news and letting the world know what capabilities the hacking world has and what they are doing to affect change in the cyber security world.

As we look back we smile when we think that initially we began as a Cyber-Awareness project (established in November 2010) by a college student. In One year The Hacker News (THN) has become a leading source of providing information and resources to security experts and hackers worldwide. The Hacker News has evolved to work closely with and within the cyber security communities in an effort to make the internet more secure. We have expanded into providing cyber security classes and have helped many corporations and local governments tighten their security systems.

As we end this year and look to the next, we thank you for being such devoted fans of THN and appreciating our efforts and providing us with your Feedback, News Updates and Donations. Many of you been with us through the hard times and the high times, and I have a feeling 2012 will bring tons of great content!

Also this past year we released 7 Issues of The Hacker News Magazine. THN Magazine is a free monthly magazine designed to spread awareness and knowledge about cyber security. Our goal is to provide the most up-to-date information on a wide variety of topics that relate to hackers and security experts worldwide. By sharing our free magazine with your family, friends, co-workers and other security experts, you're helping to promote awareness about global security issues.

The editorial staff at The Hacker News wishes you and your families the happiest of New Years and we look forward to an exciting and ever evolving look at cyber security issues.

We cannot end our New Years message without a special thanks and acknowledgement to ANONYMOUS. We have seen Anonymous grow and refine their understanding of their worth and influence in the political movements taking place throughout the world.

We know now that Anonymous will be a history making identity that will bring corporate greed and government tyranny to its knees. Anonymous will most likely single handedly return government to the people, where it belongs.

Viva La Anonymous and all who work to restore human dignity amongst government and their people.

Mohit Kumar
Founder THN & Chief Editor

Patti Galle
Editor, THN

THN Team
Priyanshu Sahay
Kislay Bhardwaj



Raising your kids to have cyber security awareness

The one thing that is great about the internet is that just like many of the other major media mediums it has content for all different types of age groups. If there are older people who want to be entertained, the internet provides plenty of fun, games and education. If you have younger kids that you have to entertain then you will find something for them as well. But unlike the other major mediums such as TV, you have a more diverse stock from which to pick from. With the internet you are getting content from all around the world and no matter which age group you need to entertain, you will be able to find something for them to watch until their heart is content.

Since the internet does have the ability to entertain children that means that there is a good chance that your child will want to use the computer all of the time. Just like in the 90's when a parent would use the VCR and the TV as a baby sitter, they are now starting to do the same thing with a computer that is connected to the web. Instead of having to try to find activities to do to occupy the child's time they just sit them in front of the computer and let that content entertain them.

But there is an inherent problem with this type of activity. Most parents these days have only been exposed to the internet for a small portion of their lives. This means that they have not grown up around the internet. This means that there is a good chance that they are unaware of the dangers that are on the net for children. Sure, they might have a general idea of what is dangerous on the internet - items such as viruses and other types of malware get the bulk of media attention - but ***what about the other types of dangers that can happen on the internet? How do you help protect your kids from that?***

Protecting your child from cyber danger

If you're going to allow your child to use the computer all of the time then you need to be aware of the dangers that are out there for them to face. You have to educate yourself in order to protect them.

First of all, we will talk about the dangers such as malware that can affect them later in the article. For right now we will focus on the more dangerous threats of meeting strangers on the internet. Some people think that the only way that their child is going to meet up with a stranger is to wander into some adult chat room and talk to the wrong people. That is not true at all. There are more ways than that to meet up with strangers. There are adults who will take the time and stalk kid web sites and act like they are one of them. When they gain the kid's trust they will then try to set up a meeting. We don't even have to express how bad that is. This is why you have to monitor what your kids are doing on the internet all of the time. Don't give the bad guys a chance to strike.

But getting back to malware, yes that is a problem for your kids as well. Having the wrong malware pop up can not only wreck your computer, but it can also cause your child to surf on web sites that are not meant to be for children's eyes. So to keep this from happening you need to make sure that your child's computer has the latest antivirus and other security tools. If your child is going to be on the computer for long periods of time then at least make sure they are safe.

About the Author: Lee Ives is an internet security blogger from London, England. <http://www.security-faqs.com>

"Cyber China"

From Operation Aurora to China Cyber Attacks Syndrome

When we think of China in relation to cyber warfare, we imagine an army of hackers hired by the government in a computer room ready to successfully attack any potential target. China is perceived as a cyber power and ready to march against any insurmountable obstacle using any means. In this connection we read everything and its opposite, and we are ready to blame all sorts of cyber threats to the Country of the Rising Sun.

The truth, however, is quite different, at least in my opinion, and understands that the Chinese people before others have understood the importance of a strategic hegemony in cyber space. However, many doubts are beginning to gather on the real technological capabilities of China. It certainly has a high potential for cyber offensive but its quality is really arguable.

China has the most extensive cyber-warfare capabilities. It began to implement an Information Warfare strategy in 1995 conducting a huge quantity of exercises in which computer viruses have been used to interrupt military and private communications. In 2000, China established a strategic Information Warfare unit, Net Force, which is responsible for “wage combat through computer networks to manipulate enemy information systems spanning spare parts deliveries to fire control and guidance systems.” Today The PLA GSD Third Department and Fourth Departments are considered to be the two largest players in China’s burgeoning cyber-infrastructure.



In November 2011, Desmond Ball, a professor in the Strategic and Defense Studies Centre at Australia's National University argues that the Chinese offensive capabilities today are pretty limited and he has also declared that the internal security has a bunch of vulnerabilities.

Ball says that China's cyber-warfare capabilities are "fairly rudimentary", and is actually able to organize massive attacks (e.g. DDoS attacks) with little sophistication. The technology solutions behind the malware used are really poor and this makes them really simple to detect and remove before any damage has been done or data stolen. The capabilities shown cannot be sufficient to penetrate highly secure networks or covertly steal or falsify critical data.

Are we really sure that behind the attacks are China's hackers?

According to cyber analysts, hackers in China and their attacks have different digital fingerprints, easily recognizable by analyzing the used computer code, and studying the command and control computers that they used to move their malicious software.

No doubt, analysts are convinced that attacks are coming from the Chinese government, because they have tracked enough intrusions to specific locations to be confident they are linked to Beijing cyber structures. Consider that the threat was persistent, spreading malware in target computer networks again and again over the course of several months or even years.

<http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf>

Which are the countries being targeted by China and who are the real targets of these attacks.

Many cyber-intelligence operations have been conducted against numerous countries, including the United States, UK, Australia, New Zealand, Canada, Germany, France, the Netherlands, Portugal, Japan, South Korea, Taiwan, India, Pakistan, Iran, Thailand, the Philippines and Indonesia.

Consider that according to what has been published in the Office of the National Counterintelligence Executive report, prevalent usage of cyber operations is related to attempting to gain business and industrial secrets from companies, in this case from Americans.

Companies are frustrated that the government isn't doing enough to pressure China to stop the attacks which the Chinese government has officially been providing protection and anonymity to those groups of hackers. In the last ten years the attacks have increased dramatically broadened to target defense companies, critical industries, major firms also including critical infrastructure.

China is considered one of the most dangerous players of cyber-espionage operations against world wide business. Forecasts for the next years aren't encouraging because the government of China will maintain an aggressive approach and be capable of collecting sensitive economic, military and industrial information related to foreign nations.

To give you an idea of the huge quantity of attacks reported in 2011 for which China was directly or indirectly considered responsible I submit an interesting table prepared by the security expert Paolo Passeri. The list includes prominent victims such as RSA. Obviously we do not have total certainty on the array of attacks, but the evidence suggests that behind all of these operations there is a single performer, China.

Just last week Julian Assange has declared that Chinese intelligence penetrated into the intelligence system of the Indian government including the Indian equivalent of FBI, the Central Bureau of Investigation. This event brings to the fore the need for governments to have an appropriate cyber strategy so that National Security cannot be affected by such attacks. The economic development of a nation can no longer ignore these cyber attacks regardless of its awareness of the cyber threat.

<http://ibnlive.in.com/news/china-hacked-indias-intel-network-assange/208460-3.html>

Based on the above facts, I believe it is wrong to consider these attacks rudimentary as the effects demonstrate that they are really dangerous and efficient.

Another erroneous belief is that the Chinese government uses a large group of hackers to make the attack. According to a report supplied by the Associated Press the majority of the attacks emanating from China are conducted by a few as a dozen groups of hackers under the control and coordination of the Chinese government.

What is the economic impact of cyber attacks on the U.S.?

Considering a report recently released by the United States Office of the Counterintelligence Executive (ONCIX) several billions of dollars are lost in intellectual property and classified information disclosure every year due cyber espionage.

http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

We are warned that the constant barrage of cyber attacks against economic and critical systems will require a unified effort by government and the private sector to improve security following a well defined cyber strategy addressed by the central Governments. Cyber warfare has just begun, stay sharp.

Written By :

Pierluigi Paganini
Security Specialist
CEH - Certified Ethical Hacker, EC Council
Security Affairs (<http://securityaffairs.co/wordpress>)
pierluigi.paganini@securityaffairs.co

Anatomy of REVOLUTION

When You Have Nothing, You Have Nothing to Loose

American historian Clarence Crane Brinton pointed out very distinctly in his book “Anatomy of a Revolution” the most reliable and common taken path in all societies to revolution. The prerequisite for successful revolution, Brinton maintained; are widespread feelings of entrapment and despair, unfulfilled expectations, a unified solidarity in opposition to a small power elite, discontent that affects nearly all social classes, a refusal by scholars and thinkers to continue to defend the actions of the ruling class, an inability of government to respond to the basic needs of citizens, a steady loss of will within the power elite itself and defections from the inner circle, and a crippling isolation that leaves the power elite without any allies or outside support and, finally, a financial crisis.

Currently, world wide tens of millions of young people are having their hopes and dreams shattered. In larger and larger numbers, the youth of today are becoming progressively more educated to the facts that the economic crisis they are facing has been perpetrated by corrupt governments and politicians and by international banks and corporations, the power elite. The youth of today are facing lower pay, the vilification of worker protective unions resulting fewer safety rights and human rights, than those of previous generations. And the massive and persistent long-term unemployment they are facing has increased competition therefore driving down wages, increasing temporary work and has made it possible for employers to hire and fire at will, because there are hundreds of applicants for every available job. The society that has been passed to today's young people is acutely damaged and in need of a radical overhaul.

It is young people who are bearing the brunt of a failed and greed oriented system. They are angry not only because of the massive unemployment but their seething angry stems from the realization that they are the generation that is the recipients of destroyed hopes, dreams, mistreatment, exploitation and injustice. The blue print for revolution that was laid out so clearly by Clarence Crane Brinton has now come to pass. The power elite of the world think they can contain this boiling pot of youthful rage, but they are mistaken. Their livelihood is dependent on the cycle of consumption of knowledge based technology which is fueled by the masses. Unable to parse or restrict this ubiquitous knowledge, the rabble are increasingly made aware of the injustices and the obvious solutions. There is no need to keep the world hungry and poor; is an idea that universally resonates. Equally, identifiable is the root cause of the dilemma; all that remains is how to resolve matters, who and what price must be paid.

Sated with the fervor of youth and more or less free of responsibilities, the young are customarily the generation most apt to question the status quo and authority. Looking back at the 1960's one can see how the youth oriented activism of the 60's was based on hopefulness and an optimistic conviction that they could really change the world for the better. However the seething youth activism we are witnessing around the world today is completely different and is deeply rooted in the soul destroying high rate of youth unemployment. Societies everywhere are failing to deliver on their promise to their young people. Today's young people were told that if they worked hard, attended school, and kept out of trouble, they could have a comfortable and satisfying life. But now, millions upon millions of young people around the world find themselves in a world that broke those promises. Young people are alienated and are turning their backs on the system that failed them. The collective pain of an unjust system drove young people to stand up and speak out.

Throughout history we have seen young people of conviction and courage stand up and attempt to bring about change that would create more compassionate, empathic and just societies. From civil rights leaders to social reformers of India to African-American abolitionists, feminists, opponents of slavery, political dissidents and suffragists we all stand on their legacy of sacrifice.

In the year 2011 young people of the world exhibited a brave willingness to be at the forefront of the struggle against injustice and the unfair system that failed them. 2011 was the beginning of a massive, widespread worldwide resistance to the brutality of a collective corrupt system that has placed their very lives at risk. The youth of the world owe it to themselves to get involved, stay involved and take their struggle to the next level in 2012. As Chris Hedges, the American journalist, author, and war correspondent, recently wrote, “Welcome to the revolution. Our elites have exposed their hand. They have nothing to offer. They can destroy but they cannot build. They can repress but they cannot lead. They can steal but they cannot share. They can talk but they cannot speak. They have no ideas, no plans and no vision for the future”.

Be warned and be prepared a world-wide clarion call has been sounded for change. The rage of the youth around the world cannot be contained because ~When You Have Nothing, You Have Nothing to loose!

-- Patti Galle,
Editor , THN



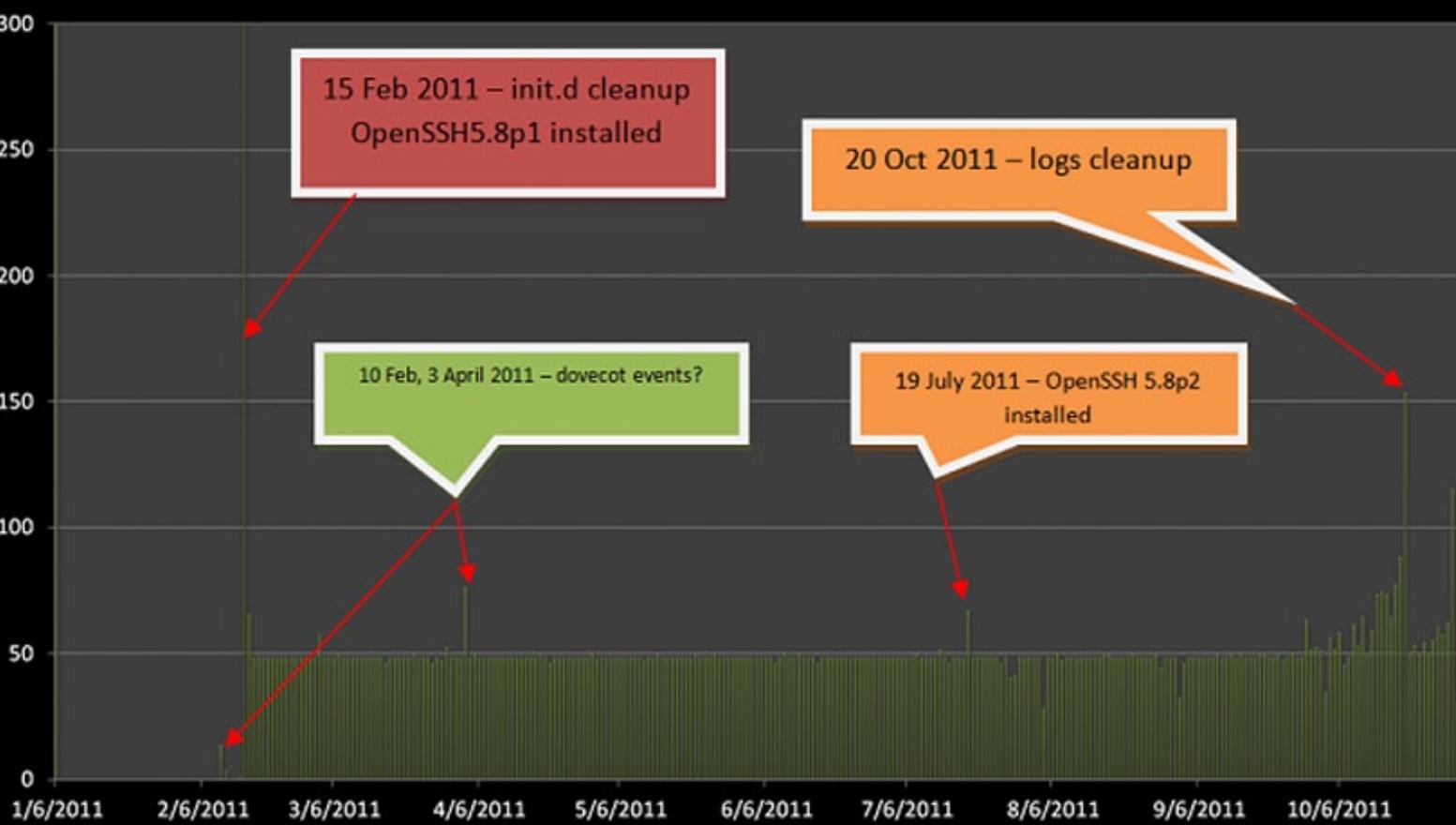
Five Significant Malwares

1) DuQu

This year was really hot for malware discovery and analysis so it is hard to select five malwares that are the most significant. Modern malwares main goal is business wise and their main objective is making money with no real investment. Some of them also have a political objective and are not just broadcasting, but are looking to harm cyber users.

Let's start the list with DuQu which is the first known network modular rootkit. DuQu has flexibility for hackers as it helps to remove and add new features quickly and without special effort. Kaspersky security lab (graph following) followed DuQu and posted a series of articles about their findings. Command and Control servers were hosted in several countries including India, Vietnam, Germany, UK and more.

Some experts have doubts on the relation between the Stuxnet and DuQu creators as they use the same vulnerability that exploit MS08-067 and both aim for stealing and collecting data related to Iranian agencies activities. When analyzed it shows that reversing malwares can lead to discovering new bugs in operating systems. The flexibility in DuQu helps the botnet controller to upgrade their system remotely with the ability to even check the current version. For example, a Viet nam server analysis showed how a hacker with the time frame managed to replace Open SSH 4.3 with version 5.8. This would help to secure communication and add GSSAPI Authentication for stronger encrypted authentication.



Another very interesting analysis about DuQu, conducted by Symantec (following) describes an exploited structure that showed vulnerability in Microsoft word to infect the organization. Analyzing the incident, it was uncovered that DuQu configuration files on some systems contain settings that do not serve in a direct connection to control servers but the program uses a special protocol for sharing files with another compromised system locally that have access to the command & control server. So, it has been as a bridge server between internal network servers and remote command and control servers.

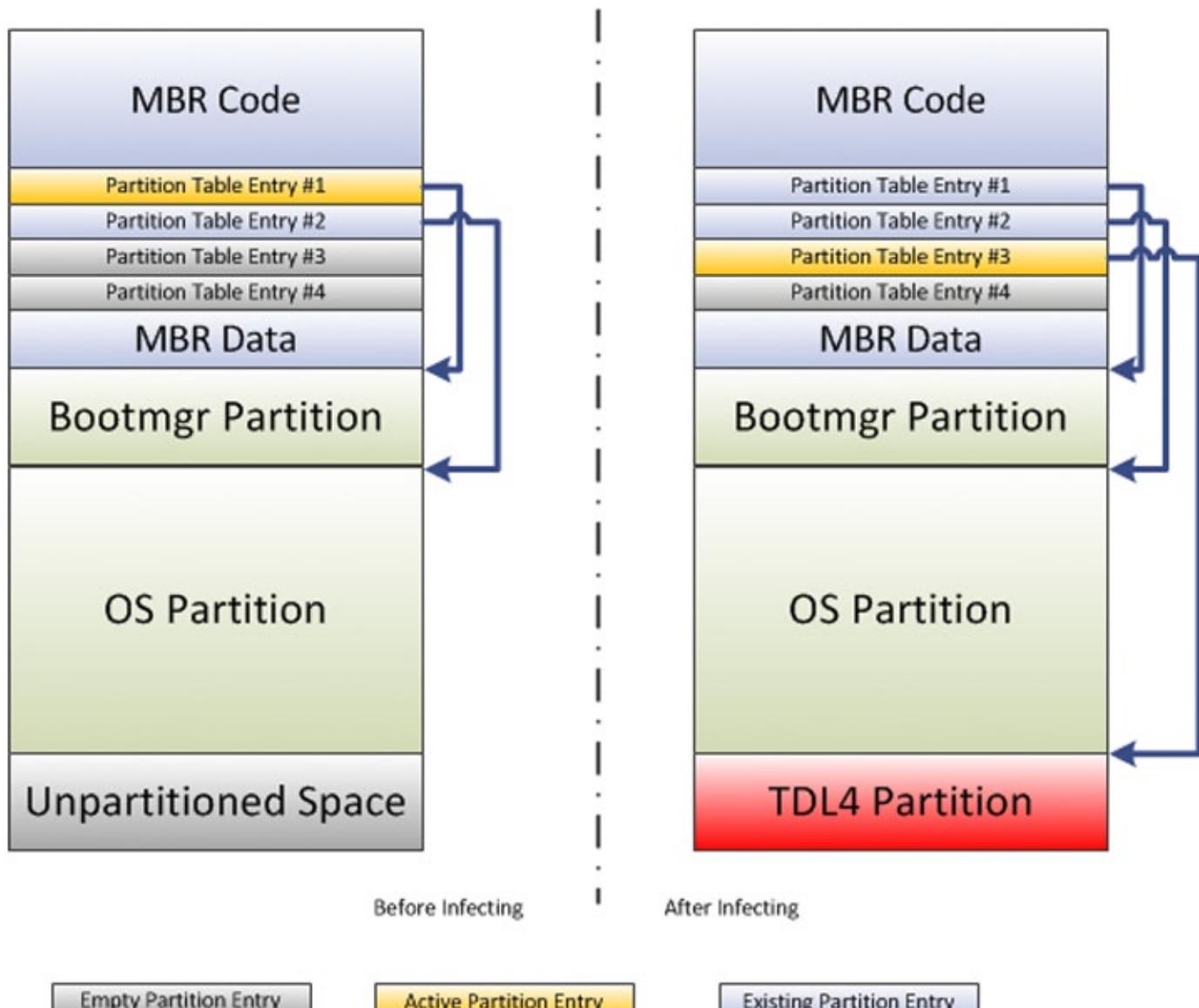


This enables attackers to connect to an infected DuQu system inside the safe zone with the help of remote computers from the internet, and use them as proxy.

After reporting the vulnerability, Microsoft issued advisories and provided a workaround for the zero-day vulnerability. This is another example of how reversing malware helps in finding new vulnerabilities and we can expect how many zero days exist in any environment.

2) TDL4

The second malware is TDL4. We call it a bootkit as it loads directly after the MBR (Master Boot Record). The malware loads before the operating system and it bypasses all OS security measures and makes antivirus hard to detect or removes them as it runs in a separate partition from the operating system. If we execute the malware we will have the following scenario:



- In any windows based operating system during the installation there will be unpartitioned space left at the end of the hard drive.
- By executing the malware it will create a new partition without modifying the MBR (Master Boot Record) which will be booting the same way as MBR but called VBR (Volume Boot Record) and store the malicious program (if there is no such space TDL4 will report to the C&C server and terminate the execution).
- If we scan the operating system we will find no trace of malicious activity.
- Next TDL4 will restart the system and start to hook all OS instructions without being detected or prevented.

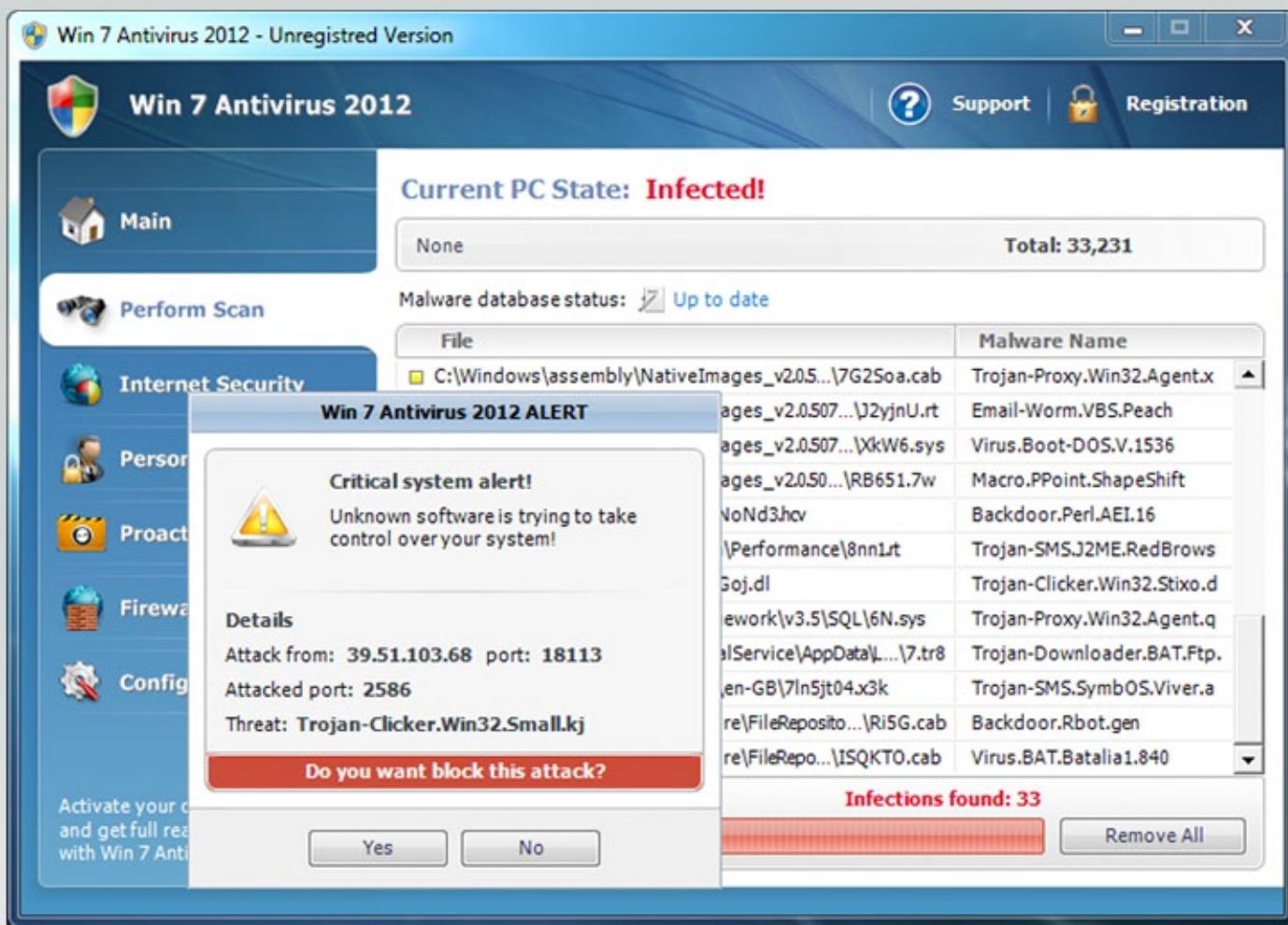
3) ZeuS

The third malware on the list is Zeus. In Today's cyberspace everything can be purchased online, so you just order what you are looking for and make the transaction online directly from the bank. If you have ZeuS installed on your computer or smartphone you can lose all you're sold in a few minutes.

ZeuS aims to grab financial information and uses several forms to infect users, for example it uses Facebook friend requests to invite victims installing java script that contains the malicious code or using spamming messages with social engineering techniques to convince the victim to install the malware.

In 2011 the team behind ZeuS had been very active and modified source code several times to bypass antiviruses and security software. There is a version discovered by Trend micro AV lab (following) ZeuS 2.3.2.0, it updates itself as the AV signatures. But for this version there is a change in encryption from RC4 to new unknown algorithms.

4) Fake antiviruses continue to evolve and today malicious websites are still increasing; the idea behind fake AV is to infect computer and alert victim about an infection that can be removed only by purchasing certain license online. Here the victim will make the transaction directly from the infected computer and criminal can get the bank credentials.



Some new ways have been added to fake antivirus is to have online support to assist users and make the victim more convinced by the criminal services. Here you can find a screenshot for a FakeAV.

So be vigilant with these operations and contact a trusted security expert if you feel that you are in a similar case.

5) Trojan proxies are among the biggest threats as they allow hacker to use the victims computer as a proxy at any time. The malware launches an HTTP proxy server on the TCP-port number XXXX and SOCKS proxy server on TCP-port XXXX. Next the attacker will be tracked on different websites as victim information.

In the end, every year we have new malwares with more complexity in their code and techniques, this is due to the change in technologies and in the way we deal with information. Now we have new security software that is going deep to secure the MBR but this for sure will bring new challenges and different ways to bypass this protection.

Reference:

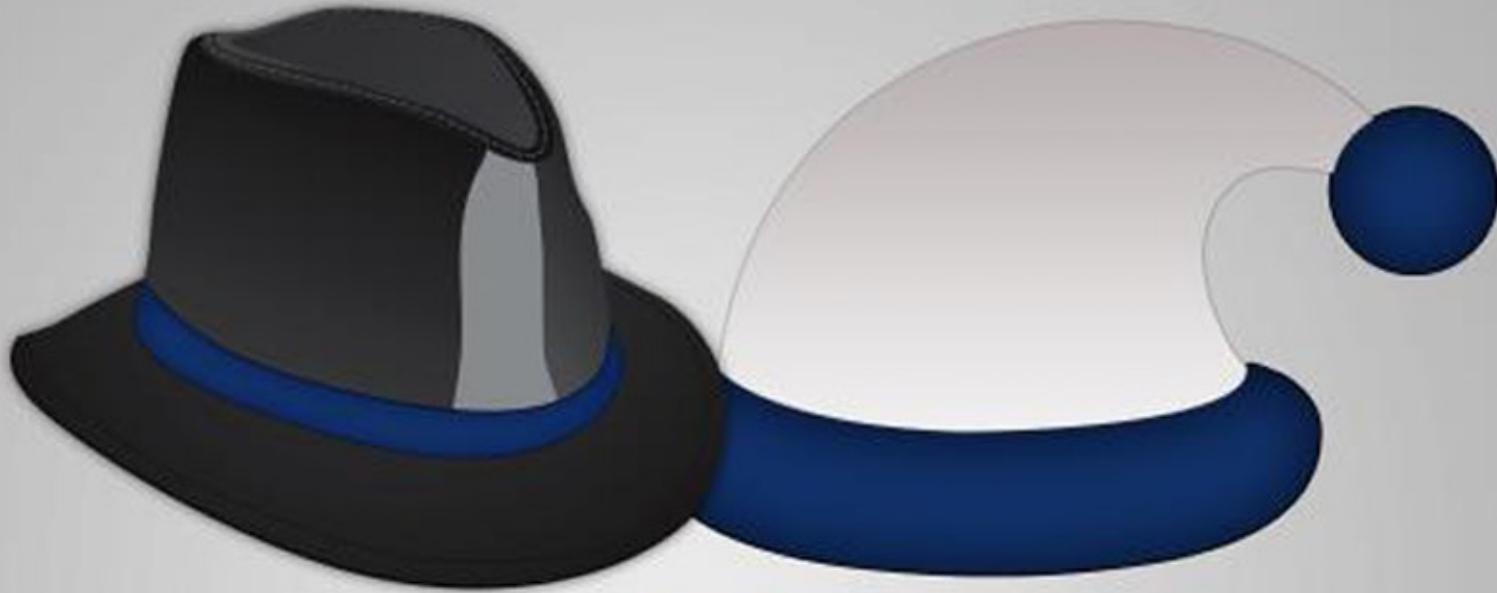
(1) Figure 1: updating openSSH Server ‘A’ – Vietnam
<http://www.securelist.com/en/blog?topic=199380362>

(2) Figure 2: Countries with reported Duqu infections. Red represents confirmed infections, orange represents unconfirmed reports
http://www.symantec.com/connect/w32-duqu_status-updates_installer-zero-day-exploit

(3) Figure 3: Hard disk partitions before and after TDL4 execution
<http://blog.eset.com/2011/10/18/tdl4-rebooted>

(4) ZeuS Gets Another Update <http://blog.trendmicro.com/zeus-gets-another-update/>

Written By : Mourad Ben Lakhouda is an Information Security practitioner. Admin at www.sectechno.com | info@sectechno.com



DefCamp

Where Hacking & Security Collide

DefCamp is a national initiative that tries to develop people's skills about computer security by creating a stimulating environment which allows offline and online exchanges of knowledge between underground security specialists, academics and corporations in Romania. DefCamp is focused on presenting technical information related to the security and insecurity of virtual and real environments. DefCamp emerged from a desire to unite for the first time in Romania providing cyber security experts an informal environment to enable them to know and participate in competitions with each other. Also, to make friends and allow them to investigate the near future from which to develop and grow.

History

The idea came in a virtual environment and joining several discussions that I had with several people. In linking all these discussions it was concluded that Romania lacks an offline "framework" that would bring together and encourage sharing of vulnerabilities, exploits and 0-days. Thus, in Spring the first discussion using the term "DefCamp" began to appear.

DefCamp @Bran, the first national cyber-security conference in Romania, was held in Bran between 30 September - 2 October. Almost 70 hackers gathered to talk, share experience and have fun. The event gathered people from all over the country who wanted to know, who wanted to see what was really happening in this area, who wanted to feel comfortable with other people with same interests and passions. Many left there with new friends that, finally, will link new strong projects and start to put points on Romania when someone refers to Eastern Europe.

The event was for some a 72 hour marathon. The three-day event was supported by numerous presentations from some of the most popular young people that have security information in their blood. The second day of the event has been characterized by a competition of over 8 hours of forensics.

DefCamp Forensic Contest 2011. Between official activities, there were some that played different games while others where sharing or trying to pentest different services randomly chosen. Pushed forward by the success of the first edition and by the feedback from participants, we are soaring this time in promoting the event in the main regions of Romania. The first of three was Moldova through its historic center, Iasi. The “Gheorghe Asachi” Technical University in Iasi, Romania, hosted first regional edition of the hacking and INFOSEC conference DefCamp on December 17, where underground, academic and enterprise security specialists shared their insight on some of the hot topics that currently affect both individuals and companies. At this event we raised the bar on the number of participants and quality of presentations. It was an event of nearly 10 hours loaded with numerous presentations of specialists coming both from the corporate environment as well as independent security experts. A number of presentations from Iasi were appreciated by the international press. Among the presentations there were theoretical, POC's, o-day and last but not least, mistakes from some who work with complex network infrastructures. This time, there were over 170 attendees.

Follow-up

The event will not stop here and long-term want to touch participants and speakers from all over Eastern Europe at an event with an international impact. Year 2012 will be very important for the conference future and surprises are all ready to emerge.

submitted By:

Avram Marius Gabriel, who works under the pseudonym "d3v1l", is a well-known figure in the international security community. He has identified several vulnerabilities in commonly used applications, helping to improve the security of those applications for millions of users.

<http://security-sh3ll.blogspot.com>



SOPA

The Hacker News say “NO WAY”

The Stop Online Piracy Act (SOPA), or H.R. 3261, is a bill that was introduced on October 26, 2011 in the United States House of Representatives, by right-wing Texas Republican, Representative Lamar Smith and twelve initial co-sponsors. The Stop Online Piracy Act dramatically broadens the capacity of United States law enforcement and copyright holders to fight online trafficking in copyrighted intellectual property and counterfeit goods. Proponents of bill H.R. 3261 state SOPA protects the intellectual property market and related industry, jobs and revenue, and is essential to reinforce and strengthen enforcement of copyright laws particularly against foreign websites. Opponents of the bill forcefully deem that the bill infringes on First Amendment rights, is effectively Internet censorship, and in fact will completely and effectively hobble the Internet. And more importantly, opponents strongly believe SOPA will significantly intimidate, threaten and frighten all potential whistle-blowers and adversely effect many important aspects of free speech.

To date, a large portion of the most important and innovative Internet industries and a very significant percentage of Internet users have shown robust public opposition to Internet-related legislation and SOPA is no exception. Publicly argued by top Internet innovators such as Craig Newmark founder of Craigslist List, Sergey Brin, co-founder of Google, Reid Hoffman, co-founder of LinkedIn and many other principal Internet industry leaders that SOPA puts the United States on a plane with the majority of tyrannical and oppressive nations in the world, They also firmly believe that SOPA will give the Feds excessive and unacceptable power and authority to censor the Web. (Check out the growing and updated list of impressive opponents.
<http://goo.gl/iSkQh>

Attempting to make their concerns known on November 15, 2011 a letter of "grave concern" was sent to principal members of the United States Senate and the United States Congress and signed by, eBay, Mozilla, Yahoo, AOL Twitter, Zynga, LinkedIn, Google, and Facebook stating how they strongly believe SOPA would establish "a serious risk to our industry's continued track record of innovation and job creation, as well as to our nation's cyber security." It is yet to be seen if their concerns will be taken into consideration or not. But one thing is crystal clear, the Internet's most well-liked sites such as Facebook, Twitter, eBay, and Google, regard the "Hollywood" sponsored copyright legislation as a real and dangerous threat.

Around the world opposition is growing to what is viewed a United States repressive corporate lead attack on the freedom of the internet. The European Parliament (the directly elected parliamentary institution of the European Union) recently adopted a resolution strongly worded and stressing "the need to protect the integrity of the global Internet and freedom of communication by refraining from unilateral measures to revoke IP addresses or domain names." This body is composed of 736 Members of the European Parliament, who serve the second largest democratic electorate in the world (after India) and the largest trans-national democratic electorate in the world which is well over 375 million eligible voters. Forty-one global Human Rights Organizations have joined together expressing their concern with SOPA and Protect IP Act, stating "Through SOPA, the United States is attempting to dominate a shared global resource. Building a nationwide firewall and creating barriers for international website and service operators makes a powerful statement that the United States is not interested in participating in a global information infrastructure.

Also, an importantly, an ever increasing number of Law professors are voicing their apprehension and are beginning to advance numerous legal concerns as well as prominent Harvard law professor and author of American Constitutional Law, Laurence Tribe. Tribe is maintaining that SOPA is unconstitutional because, if enacted, "an entire Web site containing tens of thousands of pages could be targeted; if only a single page were accused of infringement."

Tribe also stated in his written criticism to the US Congress “But proclaiming the bill to be constitutional does not make it so – any more than reminding everyone of a proposed law’s good intentions renders that law immune to First Amendment scrutiny. There is now a loudly growing critical chorus from within and without the US of negative reactions to the Stop Online Piracy Act (H.R. 3261) as well as its Senate counterpart, the Protect IP Act (S. 968).

The power and considerable wrath of opponents of SOPA was recently leveled against Internet domain registrar and Web hosting company Go Daddy. Go Daddy is currently the largest ICANN-accredited registrar in the world. The protest started from a single thread appearing on the social news website Reddit on December 22, 2011. The thread discussed the identity of supporters of the United States Stop Online Piracy Act (SOPA) and identified Go Daddy as an ardent SOPA supporter. Getting word of the internet dust-up Go Daddy doubled down and soon after released additional statements verifying their support of SOPA, causing many companies to immediately close their GO Daddy accounts. The word of Go Daddy SOPA support quickly spread across the internet and was rapidly followed by a proposed Go Daddy Boycott day on December 29, 2011. Soon a boycott and transfer of domains was proposed and quickly caught fire.

The strongest and most vocal supporter of this action was CEO Ben Huh, of Cheezburger Nation. Huh immediately pledged that his company would remove over 1,000 domains from GO Daddy if the company continued their support of SOPA. Huh’s threat was followed quickly by Jimmy Wales, Wikipedia founder announcing that all Wikipedia domains would be removed from Go Daddy as their position on SOPA was “unacceptable”. Soon the action of Huh and Wales was followed with action by Alan Schaaf, Imgur owner transferring his website as well. In solidarity the collective hacker group Anonymous released a video, containing an ominous warning to Go Daddy “Together, we will strategically remove Go Daddy from the internet.” And on December 25, 2011 as a result of the boycott and internet actions Go Daddy lost 16,191 domains.

On December 26, 2011, a Google bomb was started against Go Daddy to remove them from the number one place on Google for the term "Domain Registration" in reprisal for supporting SOPA.



On December 23, 2011 go Daddy CEO; Warren Adelman claimed to have pulled Go Daddy support for SOPA. Go Daddy officially released a statement saying "Go Daddy will support SOPA when and if the Internet community supports it. Adelman stated he felt that the public statement removing Go Daddy support would be enough for now. It is yet to be seen if Go Daddy is sincere in disavowing their support of SOPA. It may be worth noting that while many Internet sites would be subject to shut downs under SOPA, Texas Republican Lamar S. Smith, SOPA sponsor, specifically named Go Daddy in an amendment to the bill as being excluded from penalties from the act.

Although there is a large and fiery storm of protest against SOPA unfortunately where it matters most there is only a small but growing opposition in the US Congress and the Senate to SOPA. A recent letter signed by California congressional Democrats Zoe Lofgren, and Anna Eshoo, along with Ron Paul, the Texas Republican and current presidential candidate tenaciously predicting the passage of SOPA will invite "an explosion of innovation-killing lawsuits and litigation." And Nancy Pelosi, the House Democratic leader recently tweeted that "A better solution than SOPA needs to be found."

But even as the opposition to SOPA grows the support for Protect IP is surprisingly broad in the United States Senate, and for SOPA support is slightly less so. So far, SOPA has only 24 cosponsors, but it hasn't been around quite as long. A study funded by the Recording Industry Association of America (RIAA) a main supporter and lobbyist for Protect IP and SOPA states that of 1,900 bills introduced in the Senate, only 18 other bills boast the same number of bipartisan cosponsors as Protect IP. It appears that this study, places SOPA in the top 1 percent of most-popular bills ever, at least by this measurement of congressional enthusiasm. Of Protect IP's sponsors in the Senate, and surprisingly over 60 percent are Democrats.

There are three very powerful organizations that have been broadly outspoken in their support of SOPA, The Motion Picture Association of America, Inc. (MPAA), the Recording Industry Association of America, (RIAA) and the U.S. Chamber of Commerce. Recently released documents show that "Hollywood Coalition" has outspent the Silicon Valley Technology sector more than ten times on lobbyists in the past two years and the US Chamber of Commerce has placed its considerable corporate weight and money behind SOPA. In a letter to the editor of The New York Times, The U.S. Chamber of Commerce voiced their whole hearted and enthusiastic support of SOFA with the rationale that rogue web sites that steal America's innovative and creative products attract more than 53 billion visits a year and threaten more than 19 million American jobs. It has been reported that Yahoo has cancelled its membership with the U.S. Chamber of Commerce because of the Chambers fervent support for SOPA and has ask others to do the same.

The outlook for those that want to Stop Net Neutrality and Keep the Internet Free is looking rather glum The US Senate Judiciary Committee after a two day debate wasted little time in passing the Protect IP. It is apparently clear that support of SOPA has an unassailable majority on the Senate Judiciary Committee. Sopa is expected to be approved when Congress reconvenes in 2012. As far as Protect IP, it has already been approved by the US Senate Judiciary Committee and is in queue for a January 24 floor vote.

Unfortunately, at this time, there are no indications that would signal any further hearings.

Public Knowledge, one of the many groups that has voiced criticism and has difficulty with the SOPA called it “overbroad, ripe for abuse and bad international precedent”. Even though Public Knowledge, like most of SOPA detractors supports combating online piracy, they also believe this particular bill is definitely not the way to confront the problem. "Therefore the question must be asked, is this inept bill worth the risk of permanently damaging aspects of free speech and forever damage the function of the Internet? **To SOPA The Hacker News says “NO WAY”**

Please go to this site and do as many of the actions as you can. This bill has strong corporations behind it, but together we are stronger

<http://american censorship.org/>

Stop American Censorship

This week, a bill that would create America's first Internet censorship system is going to a full committee for a vote, and is likely to pass. This week, millions of us will protest censorship, censoring our own posts and asking you to call Congress. We need your help - please make a call right now.

RIGHT NOW, SENATORS ARE CONSIDERING A BILL TO CENSOR THE WEB.

SITES YOU USE EVERY DAY COULD BE BLOCKED IF IT PASSES

NOT IN THE US? PETITION THE STATE DEPARTMENT

The State Department constantly speaks out about internet censorship in other countries.

Pressure them to speak out about America's new domestic censorship system.

Email

SIGN THE PETITION

Written By :

Patti Galle

Editor - The Hacker News [THN]

Treasure of Firefox Addons

Firefox has been the developer's favorite browser for a long time, thanks to its amazing collection of addons. This also made it the aware users and pentester browsers. That's the reason why I've picked you up a selection of security tools to test your Web site and protect yourself when surfing.



To audit your Web site security:

- If you're doing your tests through proxies, give FoxyProxy a try. FoxyProxy allows you to switch easily between proxies : <http://goo.gl/8Szrw>
- RefSpoof as says its name allows you to spoof your referrer URL. It's pretty handy to bypass Referrer based security checking or make a Webmaster believe anything you want : <http://goo.gl/WnRFH>
- If you need to encrypt or hash some content, FireEncrypter is a very handy tool to get everywhere with you. : <http://goo.gl/yRE9T>
- Domain Checker allows you to learn almost everything about the server and the domain name you're pentesting : <http://goo.gl/qxcqj>
- If you're testing XSS flaws and SQL injection, HackBar is a highly recommended all in one tool to audit your Web site security : <http://goo.gl/kKEhE>
- GroundSpeed will help you to change any form you're accessing on any Web site : <http://goo.gl/ZMt1I>
- If you're looking for XSS samples, XSSed Search will add every single XSS search engine around in your Firefox search bar : <http://goo.gl/g4I3l>

-- In the same vein, SecurityFocus Search allows you to directly dig into SecurityFocus database for existing software vulnerabilities.
<http://goo.gl/6FjuH>

-- Chickenfoot is a very handy extension that allows you to run JavaScript macros in Firefox so you can automate some tasks, or make some sites you're visiting do them for you : <http://goo.gl/IUIMi>

-- Cryptofox is an amazing tool helping you to break md5 encrypted string using rainbow tables like databases : <http://goo.gl/6Gi3t>

-- SQLInjectMe allows you to easily test SQL injection :
<http://goo.gl/uNMV1>

-- XSS-Me works the same way as SQLInjectMe but on XSS vulnerabilities : <http://goo.gl/ZMt1I>

-- Tamper data allows you to read and update HTTP / HTTPS headers and test your application security by updating POST data :
<http://goo.gl/1AES9>

-- URL Flipper allows you to do URL sequence prediction when browsing doing params incrimination : <http://goo.gl/YDdzX>

-- Firesheep turns your Firefox in a sniffer. You will know when someone tries to connect on a Web site without using HTTPS and eventually gets his credential : <http://codebutler.github.com/firesheep/>

-- User Agent Proxy Switcher allows you to easily change your "user agent", that's to say your browser fingerprint. This allows you to make a server you're surfing from an iPhone or are GoogleBot :
<http://goo.gl/CEtm>

-- ShowIP is a small Firefox Addon that allows to locate the server where the site you're browsing is : <http://goo.gl/42o5e>

- JavaScript Deobfuscator is obviously a JavaScript deobfuscator. And it's quite useful too : <http://goo.gl/u8oVa>
 - Do I really need to introduce Firebug? This addon allows you to analyze Web pages source code, including CSS and JavaScript : <http://goo.gl/ht3co>
 - Modify Headers allows you to change or block HTTP headers sent to the server hosting the Web site you're surfing : <http://goo.gl/MLVoR>
 - Cookie Manager Plus allows you to modify, delete or forge any cookie : <http://goo.gl/oPMc8>
 - FlashBug is a Flash debugger, and is pretty handy when it comes to look for Flash based vulnerabilities : <http://goo.gl/q1NEL>
- Protect yourself:**
- Noscript automatically blocks Javascripts, Java applets, Flash and other potentially malicious or harmful plugins : <http://goo.gl/1VbNM>
 - HTTPS Everywhere is a plugin created by the Electronic Frontier Foundation that allows you to force HTTPS on every Web site you're visiting : <http://goo.gl/1VbNM>
 - Search engines such as Google can create a very precise profile of your browsing habits just by analyzing your searches. TrackMeNot is the perfect extension to lure this profiling sending false queries : <http://goo.gl/aekfW>
 - FoxTor and TorButton allows you to use Tor encrypted network with Firefox for anonymous surfing.<https://addons.mozilla.org/en-US/firefox/addon/foxtor/> or <https://www.torproject.org/torbutton/>
 - Perspectives prevents man in the middle attacks using self signed or hacked certificates when accessing a Web page through HTTPS : <http://goo.gl/1VbNM>

- Gmail S/MIME makes Gmail emails encryption easy :
<http://goo.gl/eOAdW>
- If you want to avoid keyloggers, use KeyScrambler in its free version encrypts everything you type on your keyboard in Firefox. It is very handy to avoid password stealing : <http://goo.gl/G6X73>
- Firekeeper is IDS (Intrusion Detection System) and a security tool for Firefox. It detects, blocks, and warns the user about malicious, harmful and infectious Web sites : <http://firekeeper.mozdev.org/>
- Trashmailnet is a 1 click temporary email creator Firefox addon :
<http://goo.gl/OLTTv>
- SSL Blacklist detects expire and weak SSL certificates, like certificates using vulnerable MD5 cipher : <http://goo.gl/l1kB5>
- WOT is a community based addon that allows to give a trust rank to visited Web sites. If the site is considered as malicious, you'll be warned before accessing it. A must have! <http://goo.gl/rLhf>
- Ghostery offers to block any tracking script, including Analytics, Facebook or advertisement : <http://goo.gl/l5BeI>



Written by :

Manuel Dorne,
Admin - <http://korben.info>

Confusing Attackers with Artillery

<-- By Dave Kennedy (ReL1K) -->

I've traditionally been on the offensive side of security through my career. With tools that I've developed like Fast-Track and The Social-Engineer Toolkit (SET), it's primarily focused on the attack front. Awhile back I had an idea of creating a more defensive tool around both Windows and *nix systems and keep things open-source as usual. I started Artillery about three months ago with the intent of developing an open-source project that does a bit of everything.

The name “Artillery” spawns from one of my favorite techno bands Infected Mushroom and enhances the overall security of whatever touches it. Artillery supports both Linux and Windows and is a purely open-source/free toolset. The concept is relatively simple; combine multiple avenues to harden an overall platform. Artillery has multiple modules, the first is the active honeypot technique which sets up a number of ports (configurable) on the given server. If a stable TCP connection is established with the remote port, the opposing IP address is blocked. The second portion is the file-integrity monitoring which monitors configured directories to see if changes occurred (similar to OSSEC HIDS). The last portion monitors certain files for configuration flaws, for example default SSH ports, insecure PHP configurations and other aspects.

Installing Artillery

Artillery is programmed purely in python and has native support for Linux and Windows. Thus far, there are no external dependencies required. Some features are not fully functional within the Windows platform however Artillery is still in alpha mode. In order to install Artillery, simply run `python install.py install`. This will install a service within `/etc/init.d/`. On Windows, it's the same install however need to manually start Artillery. A service that runs each time is in development and should be finished shortly.

```

root@bt: ~/Desktop/artillery
File Edit View Terminal Help
root@bt:~/Desktop/artillery# ls
artillery.py artillery_server.py config database install.py readme README remove_ban.py restart_server.py src
root@bt:~/Desktop/artillery# python install.py

Welcome to the Artillery installer. Artillery is a honeypot, file monitoring, and overall security
tool used to protect your nix systems.

Written by: Dave Kennedy (ReL1K)

Do you want to install Artillery and have it automatically run when you restart [y/n]: y
[*] Checking to see if Artillery is currently running...
[*] Beginning installation. This should only take a moment.
[*] Adding artillery into startup through init scripts..
Do you want to keep Artillery updated? (requires internet) [y/n]: y
[*] Checking out Artillery through subversion to /var/artillery
[*] Doing some housecleaning..
A   /var/artillery/restart_server.py
A   /var/artillery/database
A   /var/artillery/remove_ban.py
A   /var/artillery/config
A   /var/artillery/src
A   /var/artillery/src/core.py
A   /var/artillery/src/service
A   /var/artillery/src/_init_.py
A   /var/artillery/src/anti_dos.py
A   /var/artillery/src/harden.py
A   /var/artillery/src/smtp.py
A   /var/artillery/src/email_handler.py
A   /var/artillery/src/ssh_monitor.py
A   /var/artillery/src/honeypot.py
A   /var/artillery/src/monitor.py
A   /var/artillery/src/program_junk
A   /var/artillery/README
A   /var/artillery/install.py
A   /var/artillery/readme
A   /var/artillery/readme/LICENSE
A   /var/artillery/readme/CHANGELOG
A   /var/artillery/readme/CREDITS
A   /var/artillery/readme/README
A   /var/artillery/artillery.py
Checked out revision 1129.
[*] Finished. If you want to update Artillery go to /var/artillery and type 'svn update'
Would you like to start Artillery now? [y/n]: y
[*] Installation complete. Edit /var/artillery/config in order to config artillery to your liking..
root@bt:~/Desktop/artillery# 
```

Active Honeypot

Once Artillery is launched, you can configure the ports in the Artillery config file. You can add as many ports as you want. Artillery comes with a select set of default (and commonly attacked) ports on which it listens on. Doing a simple netstat -antp | grep LISTEN shows the ports actively running:

```
root@bt:~/Desktop/artillery# netstat -antp | grep LISTEN
```

tcp	0	0.0.0.0:135	0.0.0.0:*	LISTEN	20319/python
tcp	0	0.0.0.0:5800	0.0.0.0:*	LISTEN	20319/python
tcp	0	0.0.0.0:3306	0.0.0.0:*	LISTEN	20319/python
tcp	0	127.0.0.1:587	0.0.0.0:*	LISTEN	916/sendmail: MTA:
tcp	0	0.0.0.0:5900	0.0.0.0:*	LISTEN	20319/python
tcp	0	0.0.0.0:110	0.0.0.0:*	LISTEN	20319/python
tcp	0	0.0.0.0:10000	0.0.0.0:*	LISTEN	20319/python

```

tcp    0  0.0.0.0:8080      0.0.0.0:*
      LISTEN   20319/python
tcp    0  0.0.0.0:53        0.0.0.0:*
      LISTEN   20319/python
tcp    0  0.0.0.0:21        0.0.0.0:*
      LISTEN   20319/python
tcp    0  0.0.0.0:22        0.0.0.0:*
      LISTEN   20319/python
tcp    0  0.127.0.0.1:631    0.0.0.0:*
      LISTEN   1225/cupsd
tcp    0  0.0.0.0:1337      0.0.0.0:*
      LISTEN   20319/python
tcp    0  0.0.0.0:1433      0.0.0.0:*
      LISTEN   20319/python
tcp    0  0.127.0.0.1:25    0.0.0.0:*
      LISTEN   916/sendmail: MTA:
tcp    0  0.0.0.0:44443     0.0.0.0:*
      LISTEN   20319/python
tcp    0  0.0.0.0:1723      0.0.0.0:*
      LISTEN   20319/python
tcp    0  0.0.0.0:3389      0.0.0.0:*
      LISTEN   20319/python
tcp    0  0.0.0.0:445       0.0.0.0:*
      LISTEN   20319/python
tcp6   0  0.::1:631        :::*
      LISTEN   1225/cupsd
root@bt:~/Desktop/artillery#

```

Anything labeled with python would be Artillery running. When an attacker attempts to connect to the port, a random set of data is sent back to the attacker (to make it look like a funky protocol) and then the connection is terminated and the attacker banned.

```

attacker-macine:~ relik$ nc 192.168.235.129 135
s??m|??Й□??5????????VK@)?+?7?[V
s * ? D ? ? ? 6 ? ? ? ? > , ? ? b & ? . ? x ? ? □ ? o □
?w???Bo??]+?7p?qxZ???G?k?>#?Sv???Y??b???S?IU5?<??9?5?`Ї?3?□
G?E"?g?l}l=2??????7?=^fYdw??6l?y+zK?A??l?6??4?D??}\?2?@S?Y
□?`??g?:??j?O6?O~?Z???wj&??i??j?-<snip>

```

Looking back at the Artillery machine, you can now see the system is blocked and can no longer connect with the machine:

```

root@bt:~/Desktop/artillery# iptables -L
Chain INPUT (policy ACCEPT)
target  prot opt source          destination
ARTILLERY all -- anywhere       anywhere

```

```

Chain FORWARD (policy ACCEPT)
target  prot opt source          destination

```

```

Chain OUTPUT (policy ACCEPT)
target  prot opt source          destination

```

```

Chain ARTILLERY (1 references)
target  prot opt source          destination
DROP    all -- 192.168.235.1    anywhere

```

Configuration Changes

Artillery can detect changes in files on the operating system and specific directories that are defined in the config. In order to edit the config, head over to the default install path over at /var/artillery. Edit the config, and there are options you can configure for monitoring:

```
# DETERMINE IF YOU WANT TO MONITOR OR NOT
MONITOR=NO
#
# THESE ARE THE FOLDERS TO MONITOR, TO ADD MORE, JUST DO
"/root","/var/", etc.
MONITOR_FOLDERS="/var/www","/etc/"
#
# BASED ON SECONDS, 2 = 2 seconds.
MONITOR_FREQUENCY=60
#
# EXCLUSE CERTAIN DIRECTORIES OR FILES. USE FOR EXAMPLE:
/etc/passwd,/etc/hosts.allow
EXCLUDE=
```

You can exclude directories or files that often change and don't want to monitor. You can also include different directories. By default, Artillery will monitor /var/www and /etc/ for major configuration changes. The monitor_frequency is also set to a default every 60 minutes. The way SET performs the configuration changes is it generates hash values using SHA-512 and stores them in a local database. If changes occur to the file-system, the signatures mismatch and trigger an alert. If active notifications are sent, an email will be delivered to the individual, otherwise it will store it locally on a local log.



Artillery can detFeatures

Artillery is still heavily under development. Currently, it supports being able to send GMAIL alerts to whomever when an IP address is blocked, configurations have changed, SSH brute force attacks, or insecure configurations have been detected. There is also anti-dos protection built into Artillery by limited the amount of active connections per IP as well as alert on specific DOS attacks. Artillery is still a work in progress and still in an early alpha release. The overall goal with Artillery was to develop an open-source platform that combined active responses, lead in attackers with false data, and ultimately monitor the overall health of the system.

Things to come

Artillery is a side project I started along with the Social-Engineer Toolkit. It's a work in progress and a number of features are already in development. A few of these are a full-fledged windows service for monitoring/starting Artillery for Windows based systems. The ability to use other email providers or your own email server versus only being able to use GMAIL. Move off diff and use the native python difflib libraries for doing the file comparisons. Add more integrity checks into Linux and Windows based systems looking for insecure configurations.



Written by :

Dave Kennedy (ReL1K)
A security ninja & penetration tester



Listen to your instincts when it comes to the web

When you are on the web the best thing that you can do is to go with your instincts. In real life, when we walk around, we usually go with our gut to make sure that we stay out of danger. If something does not seem right we usually “sense” it for lack of a better term. This is not something that is new. This is how we survived in the wilderness all of those many years ago. We made sure that we stayed safe by following our instincts and doing the right thing. All of these years later and that same advice still hold up to be true.

But like we said in the previous paragraph, you have to worry about following your instincts when you are on the web as well. There are many different kinds of pitfalls that you can encounter when you are on the web. It doesn’t matter whether it is meeting the wrong type of person or it is downloading the wrong type of file. The dangers that you face on the web can go beyond virtual and can easily become something that you deal with in real life.

What your instincts can help you avoid

There are several different types of malware that float around the internet on a daily basis. They just sit out there waiting for either you to discover them or for you to make a mistake and get caught downloading them. But do not make the mistake and think that all of the malwares out there are the same. No, they are all different. The ones that you can really avoid with the help of your gut are the ones that are delivered through social manipulation.

People think that hackers are people who do not like to interact with others. That is only a stereotype and is not true at all. Most of the attacks that you see on the web are initiated by social interaction. While yes, most of the social interaction of these attacks is through the web it does not always stay that way. Some of these attacks are schemes to try and get you to give up money or information. This means that they will try and actually talk to you through the use of web cams or through the use of talk software such as Skype. If you are in the same area they will actually try to meet with you. This is called social hacking and it is something that is practiced all of the time. As a matter of fact, one of the most well known hackers of all time, Kevin Mitnick, biggest strength was his ability to social hack.

But social hacks are not the only ones that you can avoid through the use of your gut. You can also avoid tech based hacks as well. You can do this by listening to your inner self when it comes to what links to click on and what files to download. If you are unsure about a click, then most of the time you should not do it. This is especially true if you are on a web site that you have never visited before. But even well known web sites can give you this feeling as well. If you are on a site like Facebook and the link that you see seems weird then do not click it. Listen to your gut and avoid all of the problems that not listening can bring.

You do not have to be a computer genius to do a little computer security. Most of the problems that you run across can be avoided entirely by just doing a simple little thing like following your instincts.

About the Author:

Lee Ives is an internet security blogger from London, England. He started his web site a couple of years ago as a means of communicating security topics to the average internet user in a way that they would understand. Contrary to some people's expectations he works in retail and not the security industry which goes to show how just about anyone can accumulate a great deal of knowledge about how to protect themselves online if they are prepared to look for the answers. For those who are too busy to look, many answers can be found on his site at :
<http://www.security-faqs.com>

No Turning Back 2012

Rebellions are most always rooted in a call for justice, decency and morality. World history is full of countless rebellions against despots and others who did not conform to the will of the people. And as inequality grows to absurd new heights around the world and institutions of power are considered fundamentally dishonest, corrupt, and leaders no longer command the respect and confidence of the people then you have societies where social upheaval is inevitable. Rebellions spring up against fraudulent power and authority, and it is grounded in real outrage against mass murder (neo-imperialism, neo-colonialism), violation of human rights (torture, war crimes), widespread lying and hypocrisy, endemic political corruption, unrestrained thirst for money and power, and unprecedented greed, which all lead to economic chaos. Therefore, when critical masses of people feel profoundly aggrieved, they rise up in anger and demand “Change”.

The vehicle by which a people’s rebellion originally manifests itself is most always material in nature. It may appear that the Arab Spring was about rising food prices or the Occupy Wall Street protests, the London riots, the rioting in Greece, Spain and Chile are about money and jobs, but these causes are merely the sparks that have ignited a bonfire globally, a bonfire that has been years in creation. If we look closer it is simple to uncover the core reason for the simmering discontent that is now engulfing the globe. It is that the youth of the world cannot envision or recognize a future in the existing corrupted world system.

The world wide economic crisis has produced untold legions of unemployed youth worldwide. Ever since the beginning of the economic crisis, 2007 to 2009, youth unemployment increased by 7.8 million on a global level (1.1 million in 2007-2008 and 6.6 million in 2008-2009).

Putting these figures into perspective; over the course of the ten-year period prior to the current crisis (1996-1997 to 2006-2007), the number of unemployed youth increased, on average, by 192,000 per year. But by 2009 there were 80.7 million beleaguered young people struggling to find work. Recent studies have projected that a mere 1 percentage point increase in unemployment in the United States results in a 6 to 7 per cent decrease in the wages of college graduates. And while the wage cost lessens with time, it still remains statistically significant 15 years later. And the length time it takes to find a job is increasing as more than one in five unemployed youth in Germany, Spain and the United Kingdom have been unemployed for longer than one year.

And we are witnessing more and more young people in every country of the world become increasingly discouraged and are leaving the labor market for good. In addition, young people around the world are witness to their own parents being laid off, causing families to collapse financially. The youth of the world are now seeing that they have been robbed of a viable future. We are witnessing, on an unprecedented global scale, a grassroots rebellion lead and inspired by the youth of the world; a rebellion birthed spontaneously out of many heartrending cries for justice and equality; but I believe that this “spontaneous” rebellion has been decades in the making, and has wide-ranging and a deep intellectual foundation and that the final chapter is still extremely uncertain and many developments good and bad can take place before a final chapter is written and a new era emerges.

Change happens when a sufficient amount of people arrive at the belief that the materialistic, greedy elite and corporations have taken complete control of their societies and their governments. They are also annihilating and devastating the whole world and everyone’s future in the process making a recipe for more than “Passionate Protests.” Now you have “Rebellion.” We live in a volatile time when our entire planet finds itself in the throes of an ongoing protest that is teetering on the brink of full scale Rebellion. This revolution will last out the decade and revolutionize the world and will have a transformative impact socially, politically and economically world wide as we face a new era.

I hope with all my heart, at this point in world history, that young people all over the world are wakening, and in large numbers are preparing themselves to rise to the immense challenge facing us and all citizens of the world. And to everyone the world over To the young and to the old, to men and to women and to each and every child ~ “Inaction is not an option”.

Considering the alternatives, other than servitude, what do we have to lose?



-- Patti Galle