EMERGING THREATS: INTELLIGENCE MONOPOLIES

HAKIN9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

Vol.5 No.7
Issue 7/2010(32)
1733-7186

SECURING THE CLOUD

SECURING THE CLOUD: IS IT A PARADIGM SHIFT IN INFORMATION SECURITY?

AN INTRODUCTION TO REVERSE ENGINEERING: FLASH, .NET

WEB MALWARE - PART 1

CYBER WARFARE WITH DNSBOTNETS

HACKING TRUST RELATIONSHIPS - PART II

PREY: A NEW HOPE

PLUS

RADIO FREQUENCY-ENABLED IDENTITY THEFT BY JULIAN EVANS

Thinking of advancing your IT Security career?

Get Yourself Trained And Certified As A Penetration Tester... At Your Own Pace!

Penetration testing is big business. As companies and government organizations go increasingly electronic, there is a growing demand for IT professionals who can evaluate the security of these computer systems, networks and suggest safeguards.

Traditionally, training to become a certified "penetration tester" or "ethical hacker" has been a long, drawn-out process. Most certifications assume that candidates already have some form of networking or programming background, which makes it difficult for beginners to get started. Others require the physical attendance of training classes conducted only at certain locations. In all, the time and money spent in obtaining such a certification can be costly.

A new breed of penetration testing courses in the market looks set to change all this. One such course is "Penetration Testing Pro" offered by eLearnSecurity, an Italian IT security firm headed by Armando Romeo, who is also founder of the respected Hackers Center Web Portal.

His real world credentials aside, Armando hopes "Penetration Testing Pro" will change the way such training is conducted in the industry. "We set out to design the most comprehensive training course for IT professionals and anyone who cannot take time off to attend physical lessons. Our course allows them to learn the latest intrusion methods at their own pace, through over 1600 interactive e-learning slides and video lessons. There's no longer a need to sit through hours of boring classes," he says.

A CEH AND LPT KILLER?

Industry experts seem to agree with his methodology, too. Jason Haddix, columnist at EthicalHacker.net, feels the course has great potential.

"I kept thinking – this is what the CEH / LPT should have been – and I am delighted to say that if students can master the topics and techniques in eLearnSecurity's Penetration Testing Pro, they should be well on their way to being an accomplished pentester," he writes.

CEH and LPT refer to *Certified Ethical Hacker* and *Licensed Penetration Tester* respectively, both the gold standards for penetration testing in the industry.

Another veteran industry insider, Timothy Everson from Novell, who holds multiple certifications such as MCNE, CDE, CLE, CCNA on top of the CEH says, "For anyone who is budget constrained, I'd say, with total confidence, that the value of eLearnSecurity training meets or exceeds the value of many of the other programs available. If one truly desires to learn the technical aspects of IT security, it's a certification course well worth the time and investment."

Nathan Suri, an Information Security Architect who holds CISSP, SCJP and CSSLP certifications agrees, "The combination of slides, video, hands-on examples with the lab to practice some of the techniques makes it very effective. I like the balance of theory and practice."

REAL WORLD APPROACH USED BY PENTESTERS

Perhaps it is this real world, raw approach to teaching penetration testing that has made this course so popular. Besides Armando, the other co-authors include Brett Arion, a U.S IT Security specialist, Nitin and Vipin Kumar. Nitin and Vipin, both from India rose to fame after authoring the acclaimed "Windows Vista Bootkit" and "Windows 7 Bootkit" researches at BlackHat.

HOW TO BECOME A HIGHLY SOUGHT AFTER PENTESTER

Armando explains, "Just because someone is certified does not make him a good penetration tester. Penetration testing is part art and science. A tester needs to have experience to know which vulnerabilities to look out for. He also needs to give workable, business-minded suggestions to his clients for countering these exploits."

Given the depth of knowledge required, can someone with no prior experience still be trained to become a good penetration tester?

"Absolutely. The training aspect is key. We start with our e-learning slides and videos which explain every aspect of web application, system and network security testing.

We then follow up with labs and practical exercises. Instead of a multiple choice certification exam, ours is an actual penetration testing exercise. We are not just interested in testing theoretical knowledge. Candidates are required to conduct their own penetration tests on a given target and submit an actual test report for grading."

These rigorous requirements, Armando insists, are needed to ensure that the course is as realistic as possible. "Every student should have the confidence to conduct actual penetration testing in a commercial or mission critical setting."

IS THIS FOR YOU?

If you are looking to further your IT career, or even make a transition to the lucrative field of Penetration testing, these new breed of courses such as "Penetration Testing Pro" may be a great choice. Not only do they cost a mere fraction of what other certifications ask for, it is a great way to get up to speed with the latest penetration testing methods by learning from *actual* hackers and understanding their psychology. Learning at one's own pace without having to set time aside for regular lessons is also a big draw.

At the end of the day, does Armando hope that his course will *replace* the CEH as the de facto certification in the industry?

"Definitely not," he says with a laugh. "We provide the technical training and flexibility that the CEH does not. In fact, students who take our course as a starting point will also acquire most of the knowledge needed to pass other certifications such as CEH and LPT. This means they'll find it much easier later on to pass their certifications as well."

For more information on eLearnSecurity's Penetration Testing Pro course, visit http://www.eLearnSecurity.com .

hakin9
PRACTICAL PROTECTION IT SECURITY MAGAZINE

7/2010 (32)

hakin9 team

Editor in Chief: Karolina Lesińska
karolina.lesinska@hakin9.org
Advisory Editor: Ewa Dudzic
ewa.dudzic@hakin9.org

Editorial Advisory Board: Matt Jonkman, Rebecca Wynn, Steve Lape, Donald Iverson, Michael Munt

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Proofreaders: Henry Henderson aka L4mer, Michael Munt, Jonathan Edwards, Barry McClain

Top Betatesters: Rebecca Wynn, Bob Folden, Carlos Ayala, Steve Hodge, Nick Baronian, Matthew Sabin, Laszlo Acs, Jac van den Goor, Matthew Dumas, Andy Alvarado

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Łozowicka
ewa.lozowicka@software.com.pl

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Marketing Director: Karolina Lesińska
karolina.lesinska@hakin9.org

Subscription: Iwona Brzezik
Email: *iwona.brzezik@software.com.pl*

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokserska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.
All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them.
To create graphs and diagrams we used smartdraw.com program by SmartDraw

The editors use automatic DTP system AUPUS
Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,

It's that time again – summer break! While the Hakin9 team hopes you are enjoying your break, we also want to remind you that your computer does not take breaks and is still vulnerable to various threats and attacks. That's why the Hakin9 team is keeping you up to date with the most recent computer threats and attack vectors.

From the upcoming series about the plague of today's Internet – Web Malware – Rajdeep Chakraborty will explain how a compromised or malicious website can redirect users to a server where malicious code exploit is hosted and how compromised sites infect users redirected from search engines through a browser. In the article "Cyber warfare with DNS botnets", Francisco Alonso will describe the latest techniques being used to deploy malware over the internet. In this issues' defense section you will find an article concerning search engine privacy and security along with our cover topic – Cloud Security.

As usual, Julian Evans, our ID fraud expert, provided a great feature on Radio Frequency enabled "Identity Theft". In the emerging threats section, Matt Jonkman focuses on Intelligence Monopolies.

Enjoy!
Karolina Lesińska
Editor-in-Chief

REGULARS

BASICS

ATTACK

DEFENSE

Security flaw identified in Windows XP

Microsoft revealed earlier this month that there is a critical vulnerability affecting Windows XP and Windows Server 2003. Hackers are using malware to exploit the flaw to distribute malware on Windows machines. The hackers are delivering the malicious payload using fake websites and drive-by downloads. The malware is only targeting Windows XP users at the moment. The flaw allows a remote hacker to execute arbitrary commands. To avoid being affected by this security flaw, ID Theft Protect suggests you use the one-click Fix-It tool to unregister the problematic *hcp:// protocol*.

Source: ID Theft Protect

The Pirate Bay Hacked

The Pirate Bay has been many times on our pages because of the legal case that has brought the Swedish team to be sentenced in 2009 with the cancellation from the DNS's of the ISP from all over the world and a 2,7 million Euros fine to be paid.

The Pirate Bay moreover, served as a search engine and was not hosting any of the copyrighted contents.

The Pirate Bay team, now working on The Video Bay project, has always had the support of the whole hacker community. Gottfrid Svartholm and friends, however, had to face an attack from Argentinian hacker

Ch Russo who managed to break into The Pirate Bay database by means of SQL Injection.

According to a phone interview on Krebsonsecurity, Russo, at least at first, considered selling the database containing names, passwords and IP's of millions of users to RIAA or MPAA, associations that combat The Pirate Bay everyday. In the end the decision was to only make it public *to tell people that their information may not be so well protected*.

Source: Armanod Romeo, www.elearnsecurity.com

Microsoft LNK exploit

A 0-day vulnerability has been found in all Windows versions, including fully patched Windows 7 systems, allowing malicious code to be run without any user interaction. The vulnerability lies in the way *shell32.dll* handles Windows shortcut .lnk files and can be triggered by just having the victim browse a folder containing the malicious shortcut file. The shortcut, pointing to malware on the same folder, will execute the malicious code without the user noticing any suspicious activity. Sophos labs have come up with a proof of concept employing a USB thumb drive with the shortcut file and a rootkit file hiding itself once the external drive Windows Explorer window appears.

The exploit seems to have its origins from highly targeted espionage and attacks against SCADA systems and has come on the wild only recently.

Moreover computer security threat analysts believe that malware has already spread using this technique for a while. On June 17th the first report of malware using this unknown exploit appeared on VirusBlokAda website. SANS has raised the threat level to yellow after years and believes that *large scale exploitation is only a matter of time*.

At the time of writing, Microsoft has confirmed that the issue also affects WebDav and Network shares but since no patch is available, the only option left is to disable shortcuts or avoiding executing files from external or remote drives.

Source: Armanod Romeo, www.elearnsecurity.com

Skype crypto algos now uncovered?

Cryptologist and reverse-engineer Sean O'Neil, probably a fake name, claims he has reverse engineered the encryption algorithms used by Skype for its IM and calls. The same researcher had published some proof of concepts code, earlier this year, that seems to have allowed a wave of spammy instant messages: if you ever got spam messages from people not on your list it's probably due to this code (unless you forgot to adjust your privacy settings). The code released reproduced the same RC4 algorithm that Skype has customized to make it incompatible with other instant messaging services.

Sean O'Neil, in his posts, now pulled and reachable only from Google cache, has attacked Skype for its choice of going Security by obscurity that didn't allow researchers to openly assess its security. According to the researcher he took years to reach his goal and others may have managed to do so but kept it secret in fear legal consequences. The final outcome of the research is still unclear. It is hazardous to conclude that Skype has been hacked, however Sean O'Neill will provide more details in December 2010 at 27c3 conference in Berlin. According to Skype spokesman *the work being done by Sean O'Neil, who we understand was formerly known as Yaroslav Charnovsky, is directly facilitating spamming attacks against Skype and we are considering our legal remedies.*

Source: Armanod Romeo, www.elearnsecurity.com

CoCon Conference

c0c0n – (pronounced cocoon) is an International Information Security and Hacking conference organized annually as part of the Information Security Day. The *Matriux Security Community* (*http://www.matriux.com*) along with the Info Sec Research Association is organizing the 2 day conference from 05 to 06 August 2010 at Cochin, one of the Top 10 locations to appear in the National Geographic Traveler Places of a Lifetime.

A series of technical, non-technical, legal and community activities are organized as part of c0c0n 2010. The events are organized in two different streams covering 24 sessions on four different knowledge domains:

Information Security-Technical, Information Security-Management, Forensics and Investigations, and Legal. The 2 day sessions will be streamed lived and various activities like CTF, Hack The Code challenges are also planned with attractive prizes from sponsors. The event is bringing some of the best security professionals and hackers in the region mixed with activities, ensuring that the conference is addressing the latest and up-to-date security issues.

Source: Armanod Romeo, www.elearnsecurity.com

Vatican victim of Black hat SEO

We had already reported a number of targeted and highly effective Black Hat SEO attacks that manage to alter the natural Google SERP (*Search Engine Raking Position*) bringing a website containing malware on the first position for a very hot keyword search. The most recent being the one during FIFA World Cup in South Africa. Between 16th and 18th July, the Vatican website has undergone a series of similar attacks: a website with url pedofilo.com appeared first for the search term *vatican*. *Pedofilo* in Italian means pedophile and there should be no doubts that this was direct attack to the Holy See for the accuses of pedophilia coming from around the world.

Source: Armanod Romeo, www.elearnsecurity.com

Adobe to embrace sandboxing techniques

In the chart of the most exploited software vendors Adobe is by far the most hit: over 49 different kinds of exploits in 2009. Microsoft, although with a much broader attack surface follows with *only* 41.

Finding exploits in Adobe Acrobat Reader has become a common practice among hackers. Attacks to the end point have become much easier thanks to such kind of vulnerabilities and the use of social networks. At least for its Acrobat PDF Reader, the San Jose corporation was expected to take drastic solutions.

On July 20th, at least one year late, Adobe announced that it will employ sandboxing to mitigate the exploitability of its software. Far from being the solution to the issue, it will definitely mitigate the success rate of the exploits in the wild: other than exploiting the PDF reader engine, jumping out of the sandbox will be required. The techniques used by MSIE8 and Chrome are now being used by Adobe, that admitted that a lot of *advices* had been received by Microsoft and Google in order to implement similar solutions.

The feature will be indeed called Protected mode and according to Brad Arkin, Adobe's director of security and privacy, it has been written from scratch and with security in mind.

This feature is slated for the version 10.0 of Adobe PDF Reader due in Q4 2010.

Source: Armanod Romeo, www.elearnsecurity.com

It's holidays, watch your laptop

You shouldn't bring your corporate laptop on holiday for many reasons. Spoiling your vacation bringing some extra work is not a healthy idea. However stats show that 54% of travelers bring their laptop in hotels, hostels and wherever they go on holiday. Why? Because they fear to leave laptops at home where 35 over 100 laptop theft occur. However hotels and hostels do not shine for wireless security practices.

Connecting your laptop to an insecure wireless connection would be the same as letting someone get their hands on it. Don't turn your holidays in a corporate nightmare. Leave your laptop at home, maybe locked in a safe: you will save yours and your boss's mental sanity.

Source: Armanod Romeo, www.elearnsecurity.com

Rogue Facebook Application Threat

The rogue application redirects to a Facebook profile called *Anne Klien*. The rogue application could be used to deliver malware, adware and spyware payloads. ID Theft Protect cannot confirm at present whether the application delivers any malicious content.

The dubious application is called *I will NEVER text again*, and attracts Facebook users by way of a video. Once the user clicks on the link in the add the app then asks if it can gain access to some of your basic information, this will then be posted on their wall. This certainly sounds a bit scrupulous to me.

Source: ID Theft Protect

Trojan.Sasfis Malware Threat

Security firm Symantec has warned users about the growing menace posed by the Trojan.Sasfis malware. The company said in a blog post that it had seen a recurrence in incidents of the Trojan, and that many businesses are not prepared to deal with the threat.

Trojan.Sasfis arrives as an attachment in an official looking email from Amazon or iTunes, for example, and attempts to convince recipients to open it. Once installed, the malware receives commands from a host server, and attempts to covertly install a number of applications, many of which may consume as much as 94 per cent of CPU power.

Symantec said that the Trojan will often inject itself into common processes, including *iexplore.exe* and *svchost.exe*.

Trojan.Sasfis is essentially a back door Trojan that performs various actions when it receives commands from a malicious host. Downloading and installing misleading applications is the most common of these that we have observed to date, noted the blog post.

Source: ID Theft Protect

Elcomsoft iPhone Password Breaker

Items Tested

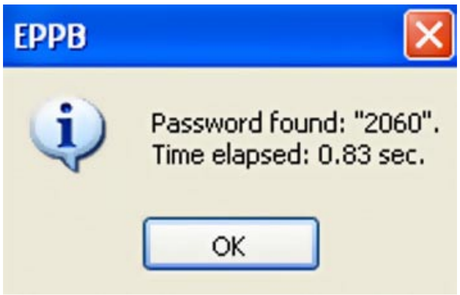
Elcomsoft's new tool iPhone Password Breaker provides a quick reliable and light weight password breaker. It can be purchased and downloaded from *www.crackpassword.com*

Although they do have a free version on the website it does have limitations. It supports password protected backups to iPhone 2G,3G,3GS, and iPod Touch 1st 2nd and 3rd Gen devices.

I recently tested this software on a Windows XP machine on a iPhone 3G encypted backup. The installation process was quick and to the point. Upon startup you will have to browse for the encypted iPhone backup file. In Windows you should be able to find it under C:\Documents and Settings\YourUserName\Application Data\Apple Computer\MobileSync\Backup. If you are unable to find it there I would suggest you do a search for "Manifest.plist".

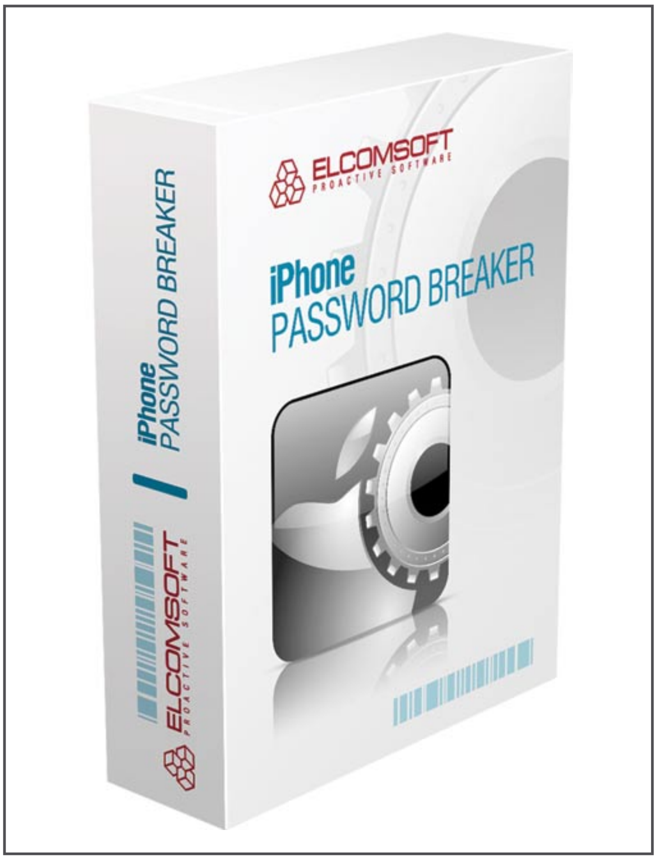
On another note, if you select a file that isn't encrypted then it will not work and you will get an error message that tells you the backup isn't encrypted. Once you have found your encrypted plist file you will then select a password breaking option either a Brute Force attack or a wordlist attack with the ability to specify a text or dictionary file.

When it comes to wordlist it will depend on how good your password list is, however, if you are doing a brute force on a numbered passcode then it will find it within a matter of seconds if not sooner. It found my 4 digit passcode in 0.83 seconds. In the real world an outright brute force attack against anything with upwards of 5 characters including symbols and upper and lower case characters will take substantially longer but with the iPhone password breaker you will be well on your way to finding that encrytped password. Password Breaker also gives you the ability to select multiple processors under the Recovery --> Options Tab. Here you can select multiple processors to work on your job or select only one if you are in need of the resources for something else.



Password found: "2060".
Time elapsed: 0.83 sec.

All in all a great tool and one that I highly recommend adding to your toolkit.



URL: http://www.elcomsoft.com/eppb.html
Cost:
Home Edition 79€
Professional Edition 199€

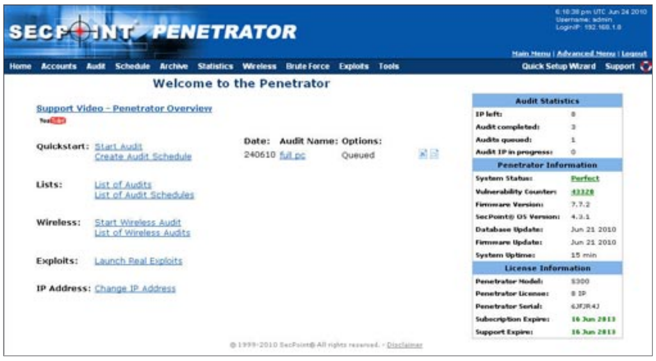
WARDELL MOTLEY JR.

Wardell Motley is a Systems Administrator for a Large clothing Manufactures in Dallas Texas.
He is a member of the ISSA and InfraGard and in his spare time works as freelance IT security researcher.

Secpoint Penetrator

by Michael Munt

The Secpoint Penetrator S300 comes in a small form factor Dell Optiplex unit. All you need to do is plug it in as the operating system and programs etc are already pre-configured for ease of use. Just connect to the system via your local machines' browser and you're ready to go. Once you are logged in you are presented with the following screen;



6:10:38 pm UTC Jun 24 2010
Username: admin
LoginIP: 192.168.1.0

Welcome to the Penetrator

Support Video - Penetrator Overview

Quickstart: Start Audit
Create Audit Schedule

Lists: List of Audits
List of Audit Schedules

Wireless: Start Wireless Audit
List of Wireless Audits

Exploits: Launch Real Exploits

IP Address: Change IP Address

Date:	Audit Name:	Options:
240610	full pc	Queued

Audit Statistics	
IP left:	8
Audit completed:	3
Audits queued:	1
Audit IP in progress:	0
Penetrator Information	
System Status:	Perfect
Vulnerability Counter:	43328
Firmware Version:	7.7.2
SecPoint® OS Version:	4.3.1
Database Update:	Jun 21 2010
Firmware Update:	Jun 21 2010
System Uptime:	15 min
License Information	
Penetrator Model:	S300
Penetrator License:	8 IP
Penetrator Serial:	6JFJR4J
Subscription Expire:	16 Jun 2013
Support Expire:	16 Jun 2013

© 1999-2010 SecPoint® All rights reserved. - Disclaimer

Auditing

There are two options available to use when auditing; a quick audit or a full scan with an option to schedule your scans. Ideal for those who want to put it into the server room and then to perform a monthly audit of the servers or certain parts of the network. This is also an excellent option for those of you that want to be able to offer this as a managed service to your clients. You are also able to see trends on the audits by comparing each scan against the others that have happened in the past.

Quick Audit

This is a small basic audit that scans the known TCP ports and then performs checks against 20 known vulnerabilities to see if your system is susceptible.

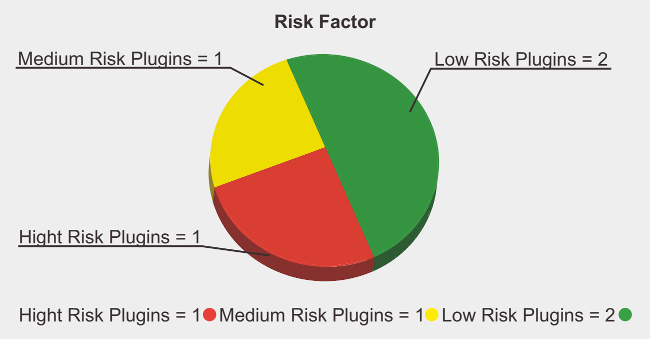
Full Scan

The full scan option will perform an assessment of your requested systems, you have the option to enhance this audit by allowing the system to actually deliver the payload against the machines in question. The Penetrator database of vulnerabilities is currently in excess of 42,000 and is continually growing, as you receive updates throughout the day. Once the audit has completed you are presented with the options on how you would like to view the results.

Reporting

There are two main report options available to you; the Executive summary or the full report (including solutions to the vulnerabilities it has identified). The Executive summary is aimed at the management types and provides enough information concerning the audit, including graphical detail and the amount of vulnerabilities found. The full scan goes into a lot further detail with information on each vulnerability found and a resolution on how to prevent this from being exploited in the future.

An overall risk factor graphic is provided which gives you an immediate indication as to how secure or insecure you are.



You are able to customise and personalise the reporting so that you can insert your own company logo etc which will enable you to sell these to your customers (this is permitted within the licencing of the unit).

Overall Impressions

Whether you are a professional tester or just starting out this unit is a complete solution for testing your own or your customers' networks. Its ease of use is a serious advantage as you wouldn't need to spend time and effort in configuring the system up etc apart from the initial wizards. Once you have scheduled all your audits, you can tuck it away somewhere and forget about it, although you could have it sitting under your desk and would never know it was there, as its almost silent operation had myself checking on more than one occasion to ensure it was turned on.

The sensible clear layout of the menu's makes it so simple to use, that even complete beginners will be using this within 15 minutes. The help documentation provided is of first rate and clear about what you need to do for each section. If you're not the "manual" type each section has a video tutorial attached to it as well.

Finally I have to say something about the support I received when I had some difficulties with my unit. I can some it up in one word. Superb! They were very quick on their initial response and kept me up-to date throughout the issue. Even offering to remote in to the machine to double check that I hadn't made a simple mistake. Once it was all resolved, they still followed up the next day to ensure I was still working properly. This has got to be one of the best levels of support I have received in a very very long time.

URL: *http://www.secpoint.com/penetrator.html*
Product SP-S300-8-1YB
Price (Euro's)949.00

Prey:

A New Hope

Misplaced your laptop or had it stolen? You are not alone.

What you will learn…

- Introduction to Prey
- Scenarios Prey will work in

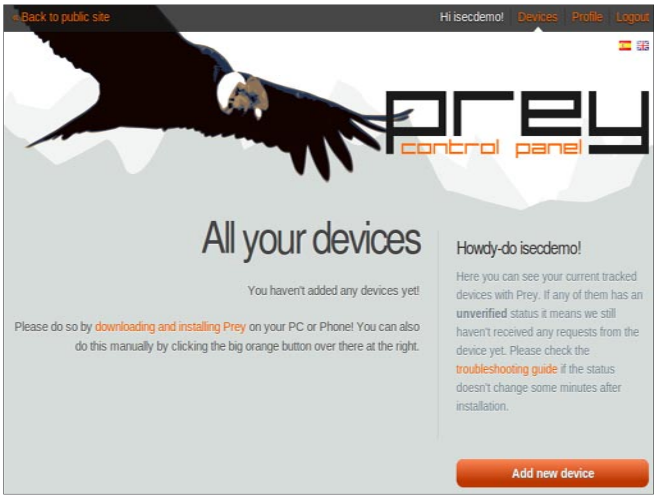
What you should know…

- Fundamentals in networking and system administration
- Network packet analysis
- Basic XML

Dell and the Ponemon Institute collaborated on a study with 106 United States airports as well as over 800 business travelers to ascertain the frequency with which laptops are lost in airports.

The study (*Airport Insecurity: The Case of Missing & Lost Laptops*, 30th June 2008) revealed a few disturbing findings:

- up to 12,000 laptops are lost every week
- 65-70% of lost laptops are never reclaimed
- 53% of business travelers surveyed have sensitive corporate data stored on their laptops



All your devices

You haven't added any devices yet!

Please do so by downloading and installing Prey on your PC or Phone! You can also do this manually by clicking the big orange button over there at the right.

Howdy-do isecdemo!

Here you can see your current tracked devices with Prey. If any of them has an **unverified** status it means we still haven't received any requests from the device yet. Please check the troubleshooting guide if the status doesn't change some minutes after installation.

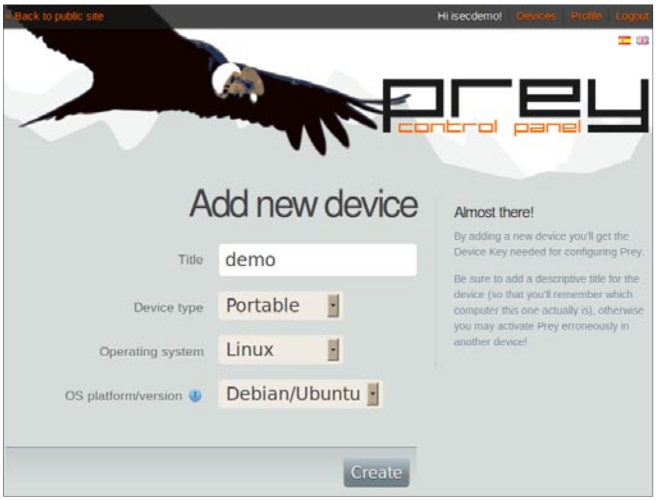
Figure 1. *Adding new device*

Background

Owners resign themselves to the notion that they are a victim of circumstance but there is hope! Prey is a lightweight cross-platform tool that collects information regarding your laptop's whereabouts and status in the event it is disinherited. This application is encompassing as it caters to the majority of people who have Windows installed on their laptops but also empowers Linux and Mac OS X users. The predator now becomes the prey. Let the hunt begin.

Setup

Prey is a simple application to install and configure.



Add new device

Title: demo

Device type: Portable

Operating system: Linux

OS platform/version: Debian/Ubuntu

Almost there!

By adding a new device you'll get the Device Key needed for configuring Prey.

Be sure to add a descriptive title for the device (so that you'll remember which computer this one actually is), otherwise you may activate Prey erroneously in another device!

Figure 2. *New device information*

Note: This article will focus on setting up Prey 0.3.73 on a laptop running Ubuntu 10.04 in *Prey+Control Panel* mode.

- Download the Debian package from the official website (ie. *http://preyproject.com*).
- Install the downloaded package in Ubuntu.
- Register for an account with the Prey website (ie. *http://control.preyproject.com/signup*).
- Upon successful registration, users are able to add devices for future tracking (see Figure 1).
- Fill in the necessary details to obtain the device key needed to activate Prey on your laptop (see Figure 2).
- The device key will be displayed when you register your new device from the Prey Control Panel (ie. *http://control.preyproject.com/*) (see Figure 3).
- Click on *Profile* to access your API key information (see Figure 4).
- Launch the *Prey Configurator* from *Applications>System Tools* menu in Ubuntu. Fill in the API and devices keys (see Figure 5).
- The device status will be displayed as *OK* if the agent successfully contacts the Prey server (see Figure 6)

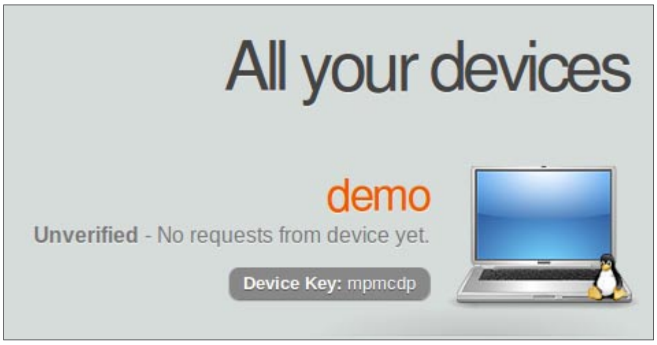
Key features

The Prey Control Panel is intuitive with hints and easy to navigate (see Figure 7).

Prey starts collecting information pertaining to its current state when you flag it as *missing*. The stealth software starts to acquire clues about its location silently in the background depending on what you instruct the agent to harvest. The agent provisions a snapshot of the system, active connections and is even able to take a picture if the device has a webcam. Prey runs in the background as root even though no user has logged into the Mac or Linux laptop.

Wifi cards are prevalent in laptops nowadays. This is a significant advantage as it enables your lost device to determine its Wifi geolocation using Google's Location API without needing to have access to an available hotspot.

Prey will harness any active Internet connection to report its status. If no active connection is available, it will automatically connect to the nearest open Wifi access point available.

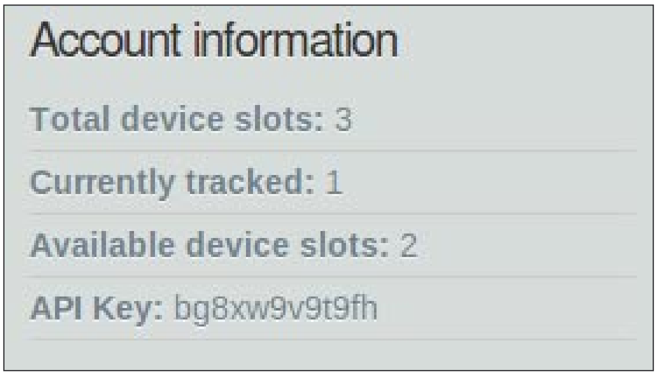

All your devices

demo

Unverified - No requests from device yet.

Device Key: mpmcdp

Figure 3. *Device key*


Account information

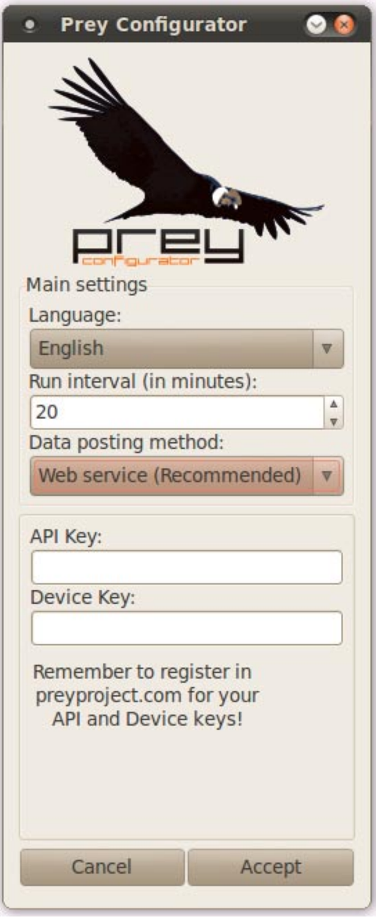
Total device slots: 3

Currently tracked: 1

Available device slots: 2

API Key: bg8xw9v9t9fh

Figure 4. *API key*



Main settings

Language: English

Run interval (in minutes): 20

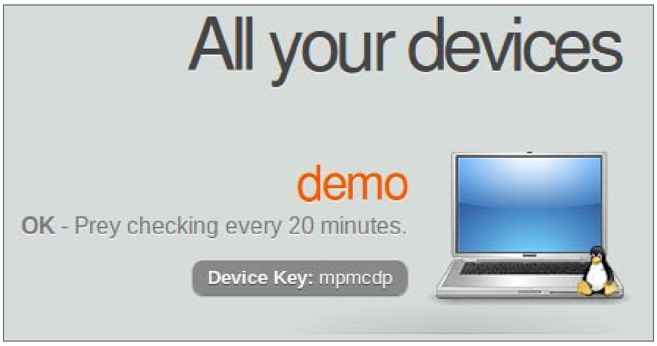
Data posting method: Web service (Recommended)

API Key:

Device Key:

Remember to register in preyproject.com for your API and Device keys!

Figure 5. *Prey Configurator*


All your devices

demo

OK - Prey checking every 20 minutes.

Device Key: mpmcdp

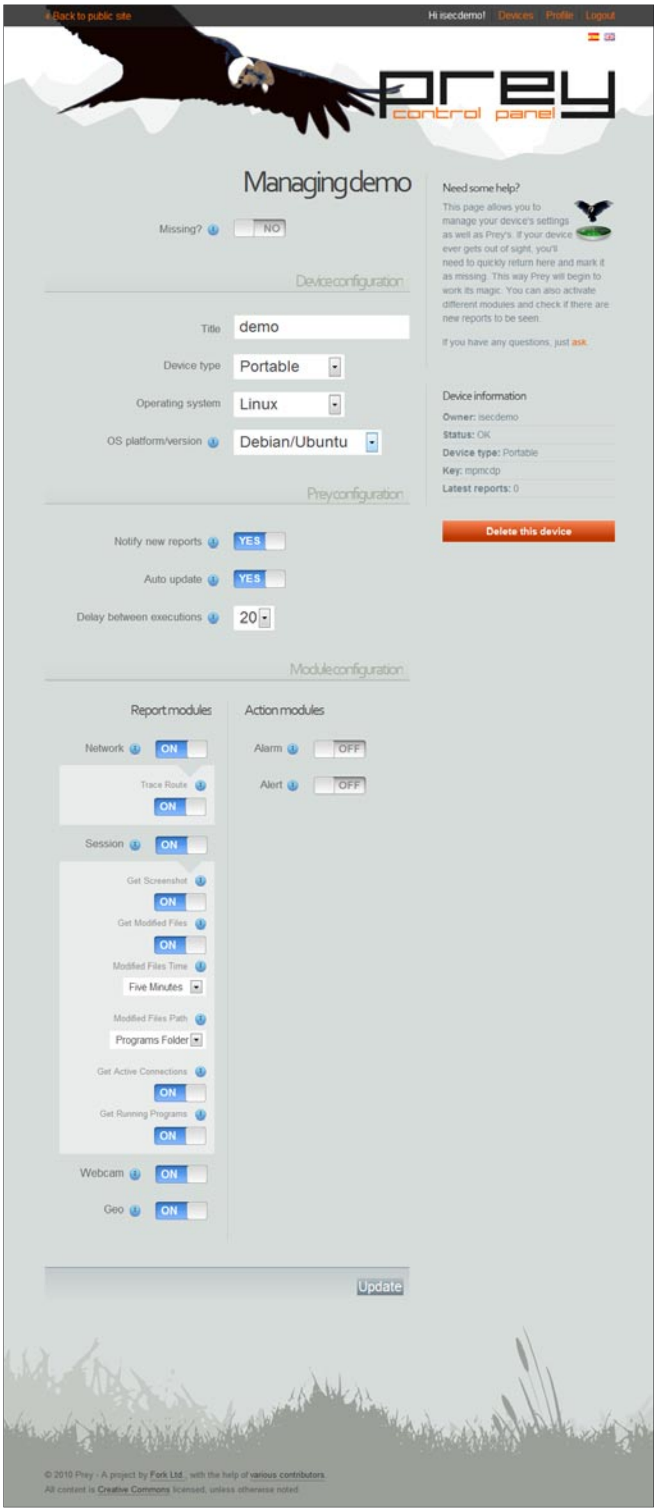
Figure 6. *Device status*

Prey in action

Test case 1

The test laptop was connected to an ADSL router via Ethernet. It was booted up but not logged in.

The laptop was marked as *missing* using another Internet connection. The *lost* laptop successfully reported its status back to the Control Panel. In this scenario, the only useful information collected pertains to the network the device is currently connected to.



Managing demo

Missing? NO

Device configuration

Title: demo
Device type: Portable
Operating system: Linux
OS platform/version: Debian/Ubuntu

Prey configuration

Notify new reports: YES
Auto update: YES
Delay between executions: 20

Module configuration

Report modules

Network: ON
Trace Route: ON
Session: ON
Get Screenshot: ON
Get Modified Files: ON
Modified Files Time: Five Minutes
Modified Files Path: Programs Folder
Get Active Connections: ON
Get Running Programs: ON
Webcam: ON
Geo: ON

Action modules

Alarm: OFF
Alert: OFF

Need some help?

This page allows you to manage your device's settings as well as Prey's. If your device ever gets out of sight, you'll need to quickly return here and mark it as missing. This way Prey will begin to work its magic. You can also activate different modules and check if there are new reports to be seen.

If you have any questions, just ask.

Device information

Owner: isecdemo
Status: OK
Device type: Portable
Key: mpmcdp
Latest reports: 0

© 2010 Prey - A project by Fork Ltd., with the help of various contributors.
All content is Creative Commons licensed, unless otherwise noted.

Figure 7. *Device configuration*

Test case 2

An open Wifi hotspot called *linksys* was set up. The test laptop was booted up and logged in.

The laptop was marked as *missing* using another Internet connection. The *lost* laptop successfully reported its status back to the Control Panel. This situation is the most ideal as the perpetrator is logged in and likely to be present at the machine. Prey will be able to record incriminating as well as concrete evidence of their identity from a screenshot of desktop activity (eg. Facebook profile, Blog, webmail, Instant Chat session) and possibly a picture of the person facing the device's webcam (if available and enabled).

Test case 3

An open Wifi hotspot called *linksys* was set up. The test laptop was booted up but not logged in.

The laptop was marked as *missing* using another Internet connection. After waiting patiently for a duration of time, the agent did not report back.

It was necessary to log into Ubuntu and run Prey check from the Terminal. Prey was unable to connect to the open Wifi hotspot. After researching this issue, it was determined that the *autoconnect* feature is not enabled by default. The *auto_connect* setting was enabled in the Prey configuration file. The *autoconnect* feature still did not function after the test was repeated.

Prey was only able to report its status when I manually established an active connection with the open Wifi hotspot and triggered the Prey script. Wireshark was harnessed to capture how Prey was interacting with the Prey Control Panel over the Internet. The agent accessed the Control Panel to download *mpmcdp.xml* using a HTTP GET command (see Figure 8).

This is the file containing instructions for the agent that was configured in the Control Panel see (Listing 1).

If the value of the *missing* variable within the XML file is *true*, the agent will start to collect data. Cleartext transmission of device information being sent back to the Control Panel is witnessed (see Figure 9).

Caveats

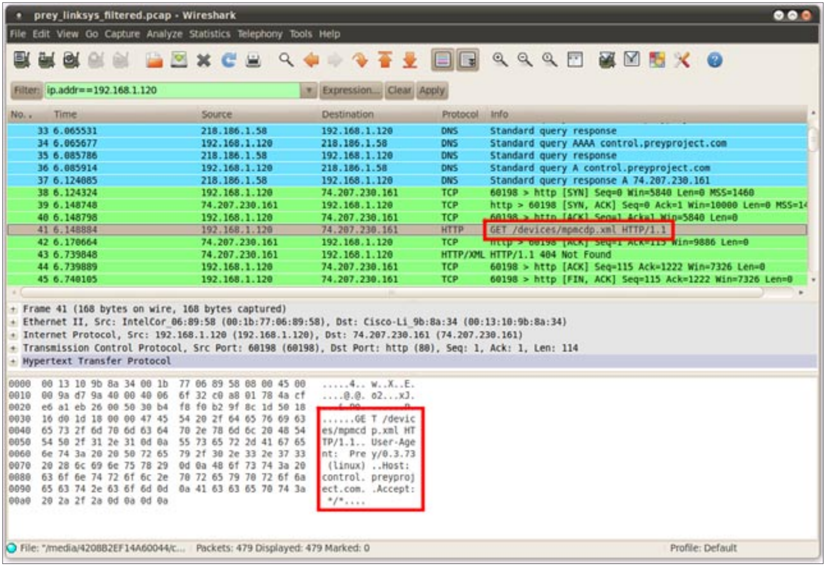
Prey is not an anti-theft solution. Users need to practise due diligence when securing their property, backing up their data regularly as well as protecting their sensitive information.

Prey's ability to *phone home* is dependent upon factors such as:

- the agent installed, configured and functioning properly
- an active Internet connection
- the duration that the laptop is powered on and untampered with
- the perpetrator must be logged in

Listing 1. *Sample device XML file*

```
<device>
  <status>
    <missing>true</missing>
  </status>
  <configuration>
    <current_release>0.3.73</current_release>
    <delay>20</delay>
    <auto_update>true</auto_update>
    <post_url>http://c57361340275c5a7307b.control.preyproject.com/devices/mpmcdp/reports.xml</post_url>
  </configuration>
  <modules>
    <module type="report" active="true" name="network" version="1.1">
      <trace_route>y</trace_route>
    </module>
    <module type="report" active="true" name="session" version="1.1">
      <get_modified_files>y</get_modified_files>
      <get_running_programs>y</get_running_programs>
      <modified_files_path>$programs_path</modified_files_path>
      <get_screenshot>y</get_screenshot>
      <modified_files_time>5</modified_files_time>
      <get_active_connections>y</get_active_connections>
    </module>
    <module type="report" active="true" name="geo" version="1.1"/>
    <module type="report" active="true" name="webcam" version="1.1"/>
  </modules>
</device>
```


prey_linksys_filtered.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply

Filter: ip.addr==192.168.1.120

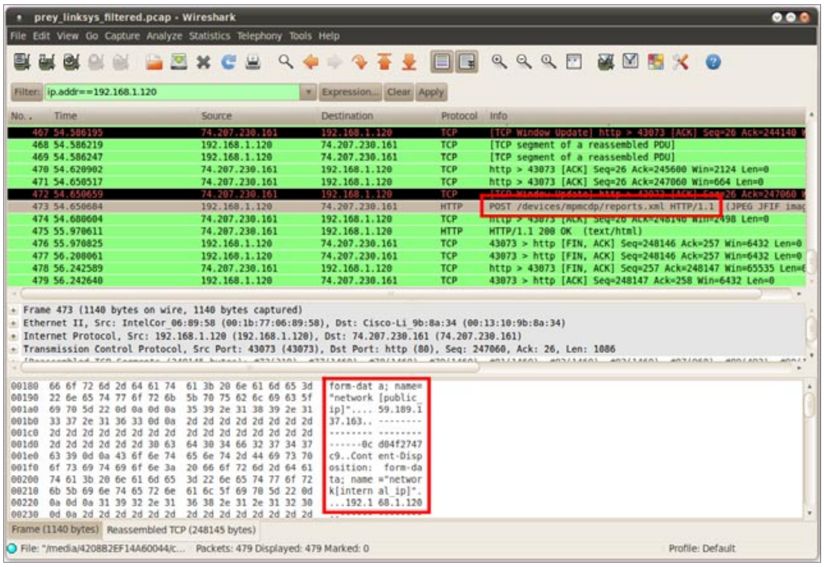
```
No. .  Time        Source           Destination      Protocol  Info
    33 6.065531    218.186.1.58     192.168.1.120    DNS       Standard query response
    34 6.065677    192.168.1.120    218.186.1.58     DNS       Standard query AAAA control.preyproject.com
    35 6.085786    218.186.1.58     192.168.1.120    DNS       Standard query response
    36 6.085914    192.168.1.120    218.186.1.58     DNS       Standard query A control.preyproject.com
    37 6.124085    218.186.1.58     192.168.1.120    DNS       Standard query response A 74.207.230.161
    38 6.124324    192.168.1.120    74.207.230.161   TCP       60198 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460
    39 6.148748    74.207.230.161   192.168.1.120    TCP       http > 60198 [SYN, ACK] Seq=0 Ack=1 Win=10000 Len=0 MSS=14
    40 6.148798    192.168.1.120    74.207.230.161   TCP       60198 > http [ACK] Seq=1 Ack=1 Win=5840 Len=0
    41 6.148884    192.168.1.120    74.207.230.161   HTTP      GET /devices/mpmcdp.xml HTTP/1.1
    42 6.170664    74.207.230.161   192.168.1.120    TCP       http > 60198 [ACK] Seq=1 Ack=115 Win=9886 Len=0
    43 6.739848    74.207.230.161   192.168.1.120    HTTP/XML  HTTP/1.1 404 Not Found
    44 6.739889    192.168.1.120    74.207.230.161   TCP       60198 > http [ACK] Seq=115 Ack=1222 Win=7326 Len=0
    45 6.740105    192.168.1.120    74.207.230.161   TCP       60198 > http [FIN, ACK] Seq=115 Ack=1222 Win=7326 Len=0

+ Frame 41 (168 bytes on wire, 168 bytes captured)
+ Ethernet II, Src: IntelCor_06:89:58 (00:1b:77:06:89:58), Dst: Cisco-Li_9b:8a:34 (00:13:10:9b:8a:34)
+ Internet Protocol, Src: 192.168.1.120 (192.168.1.120), Dst: 74.207.230.161 (74.207.230.161)
+ Transmission Control Protocol, Src Port: 60198 (60198), Dst Port: http (80), Seq: 1, Ack: 1, Len: 114
+ Hypertext Transfer Protocol

0000  00 13 10 9b 8a 34 00 1b  77 06 89 58 08 00 45 00   .....4.. w..X..E.
0010  00 9a d7 9a 40 00 40 06  6f 32 c0 a8 01 78 4a cf   ....@.@. o2...xJ.
0020  e6 a1 eb 26 00 50 30 b4  f8 f0 b2 9f 8c 1d 50 18   ...&.P0. ......P.
0030  16 d0 1d 18 00 00 47 45  54 20 2f 64 65 76 69 63   ......GE T /devic
0040  65 73 2f 6d 70 6d 63 64  70 2e 78 6d 6c 20 48 54   es/mpmcd p.xml HT
0050  54 50 2f 31 2e 31 0d 0a  55 73 65 72 2d 41 67 65   TP/1.1.. User-Age
0060  6e 74 3a 20 20 50 72 65  79 2f 30 2e 33 2e 37 33   nt:  Pre y/0.3.73
0070  20 28 6c 69 6e 75 78 29  0d 0a 48 6f 73 74 3a 20    (linux) ..Host:
0080  63 6f 6e 74 72 6f 6c 2e  70 72 65 79 70 72 6f 6a   control. preyproj
0090  65 63 74 2e 63 6f 6d 0d  0a 41 63 63 65 70 74 3a   ect.com. .Accept:
00a0  20 2a 2f 2a 0d 0a 0d 0a                             */*....
```

File: "/media/4208B2EF14A60044/c... Packets: 479 Displayed: 479 Marked: 0 Profile: Default

Figure 8. *Device XML file*


prey_linksys_filtered.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply
Frame (1140 bytes)
Reassembled TCP (248145 bytes)

Filter: ip.addr==192.168.1.120

```
No. .  Time        Source           Destination      Protocol  Info
   467 54.586195   74.207.230.161   192.168.1.120    TCP       [TCP Window Update] http > 43073 [ACK] Seq=26 Ack=244140 W
   468 54.586219   192.168.1.120    74.207.230.161   TCP       [TCP segment of a reassembled PDU]
   469 54.586247   192.168.1.120    74.207.230.161   TCP       [TCP segment of a reassembled PDU]
   470 54.620902   74.207.230.161   192.168.1.120    TCP       http > 43073 [ACK] Seq=26 Ack=245600 Win=2124 Len=0
   471 54.650517   74.207.230.161   192.168.1.120    TCP       http > 43073 [ACK] Seq=26 Ack=247060 Win=664 Len=0
   472 54.650659   74.207.230.161   192.168.1.120    TCP       [TCP Window Update] http > 43073 [ACK] Seq=26 Ack=247060 W
   473 54.650684   192.168.1.120    74.207.230.161   HTTP      POST /devices/mpmcdp/reports.xml HTTP/1.1 (JPEG JFIF imag
   474 54.680604   74.207.230.161   192.168.1.120    TCP       http > 43073 [ACK] Seq=26 Ack=248146 Win=2498 Len=0
   475 55.970611   74.207.230.161   192.168.1.120    HTTP      HTTP/1.1 200 OK  (text/html)
   476 55.970825   192.168.1.120    74.207.230.161   TCP       43073 > http [FIN, ACK] Seq=248146 Ack=257 Win=6432 Len=0
   477 56.208061   192.168.1.120    74.207.230.161   TCP       43073 > http [FIN, ACK] Seq=248146 Ack=257 Win=6432 Len=0
   478 56.242589   74.207.230.161   192.168.1.120    TCP       http > 43073 [FIN, ACK] Seq=257 Ack=248147 Win=65535 Len=6
   479 56.242640   192.168.1.120    74.207.230.161   TCP       43073 > http [ACK] Seq=248147 Ack=258 Win=6432 Len=0

+ Frame 473 (1140 bytes on wire, 1140 bytes captured)
+ Ethernet II, Src: IntelCor_06:89:58 (00:1b:77:06:89:58), Dst: Cisco-Li_9b:8a:34 (00:13:10:9b:8a:34)
+ Internet Protocol, Src: 192.168.1.120 (192.168.1.120), Dst: 74.207.230.161 (74.207.230.161)
+ Transmission Control Protocol, Src Port: 43073 (43073), Dst Port: http (80), Seq: 247060, Ack: 26, Len: 1086
+ [Reassembled TCP Segments (248145 bytes): [illegible]

00180  66 6f 72 6d 2d 64 61 74  61 3b 20 6e 61 6d 65 3d   form-dat a; name=
00190  22 6e 65 74 77 6f 72 6b  5b 70 75 62 6c 69 63 5f   "network [public_
001a0  69 70 5d 22 0d 0a 0d 0a  35 39 2e 31 38 39 2e 31   ip]".... 59.189.1
001b0  33 37 2e 31 36 33 0d 0a  2d 2d 2d 2d 2d 2d 2d 2d   37.163.. --------
001c0  2d 2d 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   -------- --------
001d0  2d 2d 2d 2d 2d 2d 30 63  64 30 34 66 32 37 34 37   ------0c d04f2747
001e0  63 39 0d 0a 43 6f 6e 74  65 6e 74 2d 44 69 73 70   c9..Cont ent-Disp
001f0  6f 73 69 74 69 6f 6e 3a  20 66 6f 72 6d 2d 64 61   osition:  form-da
00200  74 61 3b 20 6e 61 6d 65  3d 22 6e 65 74 77 6f 72   ta; name ="networ
00210  6b 5b 69 6e 74 65 72 6e  61 6c 5f 69 70 5d 22 0d   k[intern al_ip]".
00220  0a 0d 0a 31 39 32 2e 31  36 38 2e 31 2e 31 32 30   ...192.1 68.1.120
00230  0d 0a 2d 2d 2d 2d 2d 2d  2d 2d 2d 2d 2d 2d 2d 2d   ..------ --------
```

File: "/media/4208B2EF14A60044/c... Packets: 479 Displayed: 479 Marked: 0 Profile: Default

Figure 9. *Device report transmission*

It is ironic that to encourage the finder to leave your OS intact and increase your chances of Prey reporting its status, it is suggested that your device be open. In the case of Windows machines, you would create a guest account with no administrative privileges and null password. For Mac and Linux, you would configure the systems to log in automatically upon boot up.

The application can be removed if the finder has the administrative rights. Setting a BIOS password to prevent the modification of boot sequence will deter most people but will be easily defeated by a knowledgeable party.

Prey is not able to furnish geolocation information if the laptop does not have a wireless card. As stated in the Prey project site's troubleshooting guide, the Geo module is not always reliable and sometimes cannot pinpoint the device's location even with a working wireless card. This was confirmed by testing conducted.

The action modules permit the triggering of an audio alarm or visual cue (ie. alert message or custom wallpaper) and is only advantageous if the device is in close proximity of the owner. The Chinese idiom, *beat the grass and frighten off the snake*, aptly describes this situation. These alerts when enabled will scare parties into disposal or destruction of the laptop instead of promoting the item's return.

Conclusion

Prey is a work-in-progress. The concept behind the tool is laudable and this forms a solid foundation to enhance this utility.

Users are currently only able to access reports from the Prey Control Panel via their browser. It would be useful if the reports could be exported (eg. PDF format) for submission to authorities.

The *autoconnect* feature and the Geo module have proven unreliable. These are key areas that the Prey team should focus on improving.

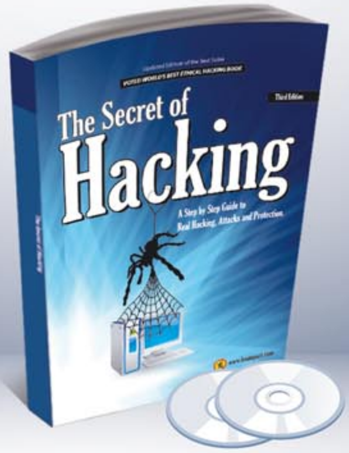
A timestamp of the last contact by the Prey agent would be valuable in informing users of the last time their device checked in.

Prey does not guarantee the recovery of your missing device. There are also a few glitches to be ironed out. However, it is free and requires minimal effort to set up. These factors and the possibility of tracing your property justifies installing it. It offers individuals and enterprises an opportunity to reclaim what is rightfully theirs.

MERVYN HENG

Mervyn Heng, CISSP, is a Security analyst from the sunny shores of Singapore. Information Security is one of his myriad hobbies and his passion motivates him to write articles as his contribution to the community. When he is not busy trying to save the world, he is learning to play the guitar and building his toy collection. If you have any comments or queries, please contact him at commandrine@gmail.com.

LATEST EDITION 2009 YEAR
The SECRET OF HACKING
400+


The Secret of Hacking
Third Edition
A Step by Step Guide to Real Hacking, Attacks and Protection.

An introduction

to Reverse Engineering: Flash, .NET

This article is about the demonstration of Reversing of Flash and .NET applications. This is an introductory article showing basics of decompiling/ disassembling. In the first I have chosen to show reversing of Flash files and .NET files and how to patch them.

What you will learn…

- How to disassemble/decompile files.
- How to change the codes and patch them.
- Tools which are used to disassemble/decompile.

What you should know…

- No specific knowledge required, but familiarity with Flash and .NET technologies desirable.

Reversing Flash

Flash is a popular method of providing interface to the users. Nowadays almost every web application uses Flash to increase interactivity and user-friendliness. Web application like online songs, online videos or online games is very popular amongst the users.

Flash objects are contained within the compiled file that the browser download from the server and executes using a browser plugin. The SWF file contains bytecode that is converted to ActionScript source code using tools like *Flasm*.

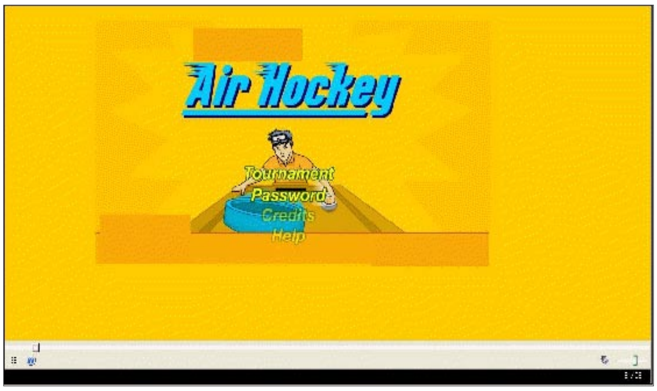
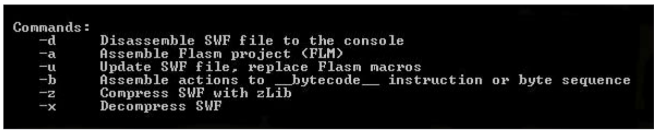


Figure 1. *A flash based game*



```
Commands:
   -d     Disassemble SWF file to the console
   -a     Assemble Flasm project (FLM)
   -u     Update SWF file, replace Flasm macros
   -b     Assemble actions to __bytecode__ instruction or byte sequence
   -z     Compress SWF with zLib
   -x     Decompress SWF
```

Figure 2. *Flasm options*

I shall show you how to disassemble flash file using Flasm and how to change the code and assemble back. The reassembled flash file will have a changed behavior as compared to original flash file.

Download the tool Flasm from *http://www.nowrap.de/flasm.html*.

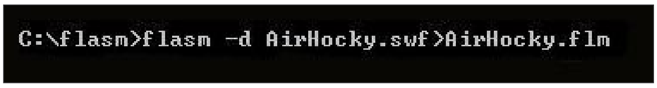
I shall use a simple flash game for this purpose (Figure 1). The following game has a protection. You have to provide valid password in order to get into it.

Now let's disassemble the above file (*AirHockey.swf*).

Place the flash file in the same directory where the Flasm is downloaded. Flasm gives the following options, type flasm `-h` (Figure 2).

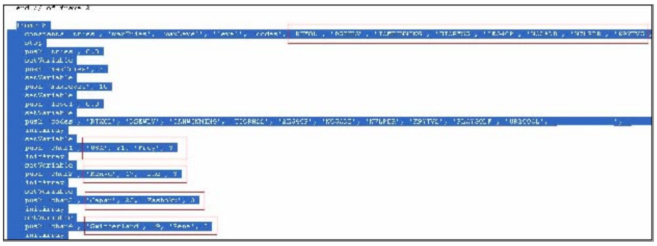
We shall be using `-d` and `-a` options. Now disassemble the SWF file (Figure 3).

The above command tells to disassemble the file and save the output in a file with .flm extension. Now



```
C:\flasm>flasm -d AirHocky.swf>AirHocky.flm
```

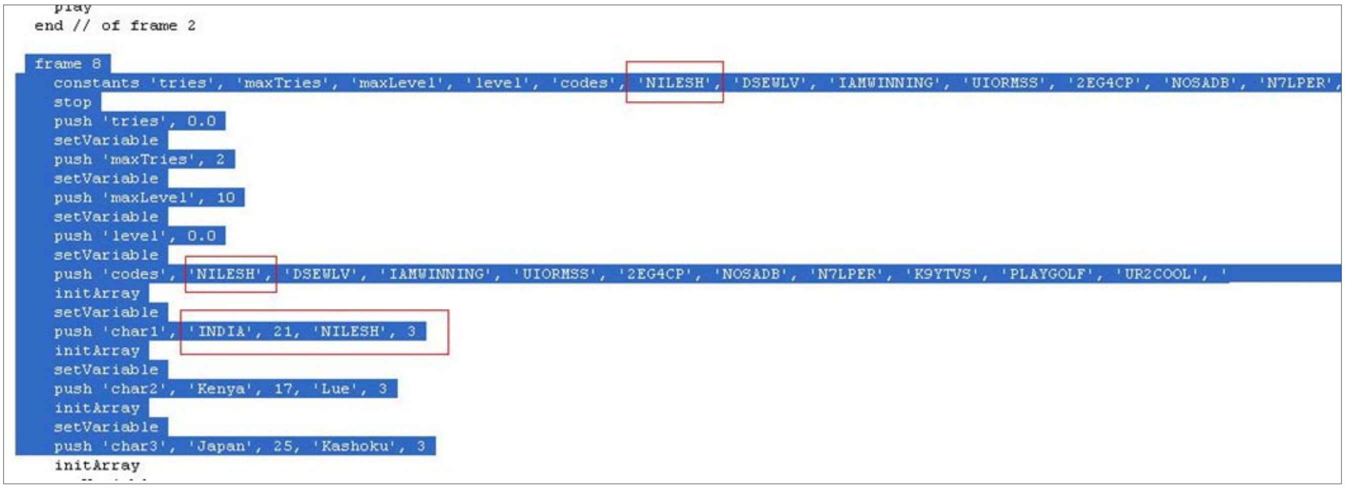
Figure 3. *Disassembling the file*



```
  end // of frame 3

  frame 4
    constants 'tries', 'maxTries', 'maxLevel', 'level', 'codes', [illegible]
    stop
    push 'tries', 0.0
    setVariable
    push 'maxTries', [illegible]
    setVariable
    push 'maxLevel', 10
    setVariable
    push 'level', 0.0
    setVariable
    push 'codes', [illegible]
    initArray
    setVariable
    push [illegible]
    initArray
    setVariable
    push [illegible]
    initArray
    setVariable
    push [illegible]
    initArray
    setVariable
    push [illegible]
    initArray
```

Figure 4. *Disassembled SWF file*



```
    play
  end // of frame 2

  frame 8
    constants 'tries', 'maxTries', 'maxLevel', 'level', 'codes', 'NILESH', 'DSEWLV', 'IAMWINNING', 'UIORMSS', '2EG4CP', 'NOSADB', 'N7LPER',
    stop
    push 'tries', 0.0
    setVariable
    push 'maxTries', 2
    setVariable
    push 'maxLevel', 10
    setVariable
    push 'level', 0.0
    setVariable
    push 'codes', 'NILESH', 'DSEWLV', 'IAMWINNING', 'UIORMSS', '2EG4CP', 'NOSADB', 'N7LPER', 'K9YTVS', 'PLAYGOLF', 'UR2COOL', '
    initArray
    setVariable
    push 'char1', 'INDIA', 21, 'NILESH', 3
    initArray
    setVariable
    push 'char2', 'Kenya', 17, 'Lue', 3
    initArray
    setVariable
    push 'char3', 'Japan', 25, 'Kashoku', 3
    initArray
```

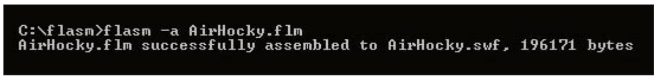
Figure 5. *Make changes in the file*

open the AirHocky.flm file to read the contents. You will find lots of frames in the code starting from frame 0. If you see in Figure 1 above, the password screen is at frame 8. This particular frame might be of our particular interest. Carefully inspect the code and look for frame 8 (Figure 4).

If you see carefully then you can find the player's name, age and country, for example:

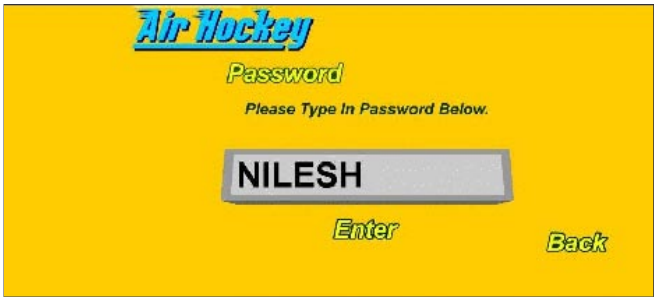
```
USA, 21, Frey.
```

Above are some Player's records, there are corresponding passwords (I tried few of them and it



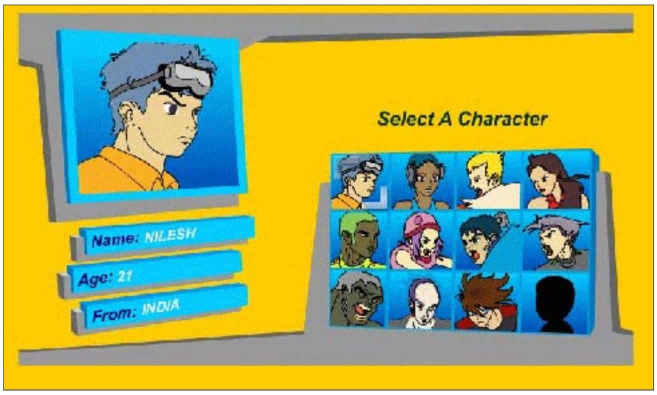
```
C:\flasm>flasm -a AirHocky.flm
AirHocky.flm successfully assembled to AirHocky.swf, 196171 bytes
```

Figure 6. *File ed file converted to SWF file*



NILESH

Figure 7. *Password Nilesh is accepted*



Name: NILESH
Age: 21
From: INDIA

Figure 8. *Profile of the player changed*

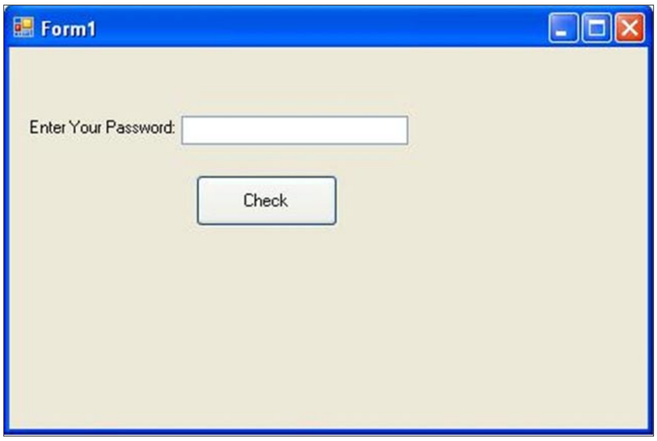
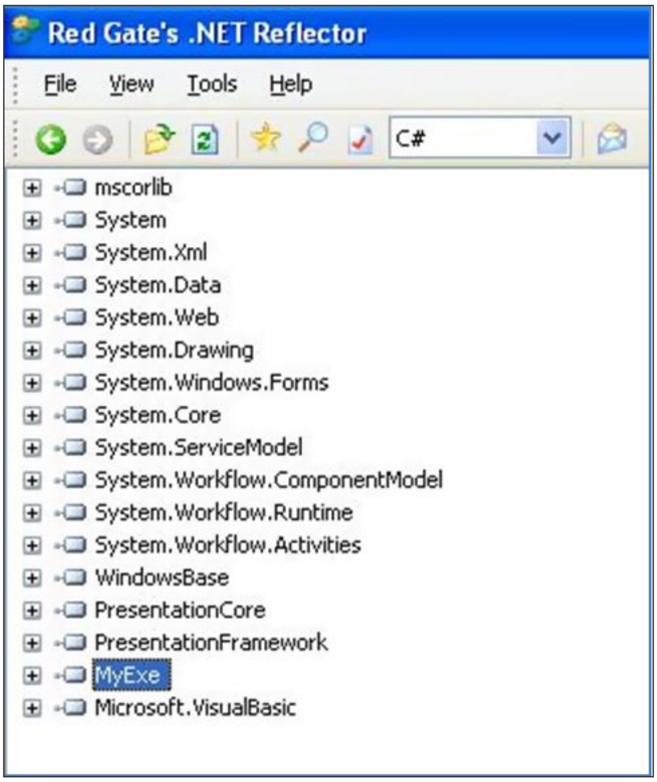
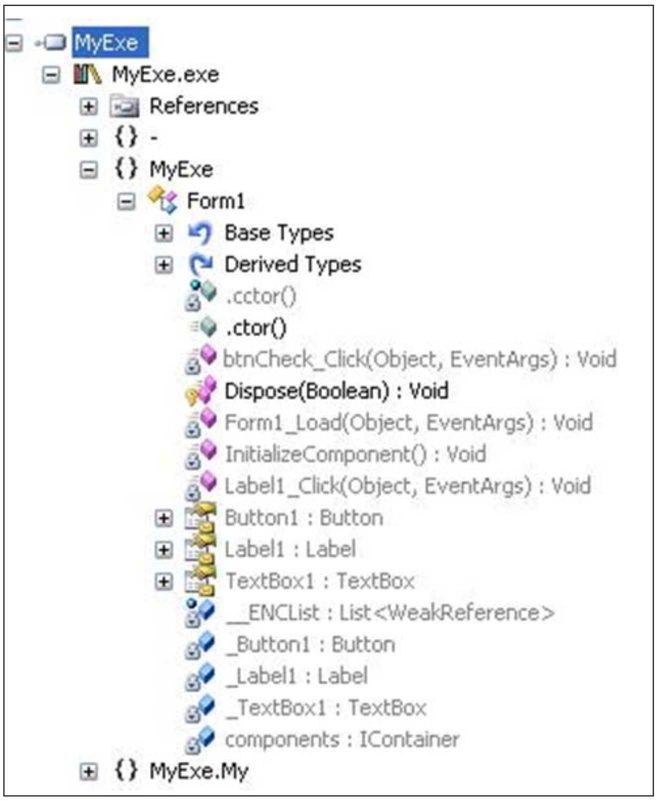


Figure 9. *Exe that checks the password*



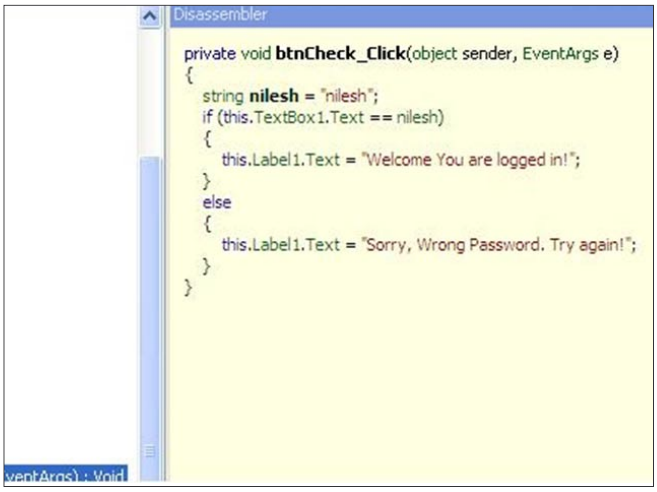
```
mscorlib
System
System.Xml
System.Data
System.Web
System.Drawing
System.Windows.Forms
System.Core
System.ServiceModel
System.Workflow.ComponentModel
System.Workflow.Runtime
System.Workflow.Activities
WindowsBase
PresentationCore
PresentationFramework
MyExe
Microsoft.VisualBasic
```

Figure 10. *Reflector*



```
⊟ MyExe
   ⊟ MyExe.exe
      ⊞ References
      ⊞ {} -
      ⊟ {} MyExe
         ⊟ Form1
            ⊞ Base Types
            ⊞ Derived Types
              .cctor()
              .ctor()
              btnCheck_Click(Object, EventArgs) : Void
              Dispose(Boolean) : Void
              Form1_Load(Object, EventArgs) : Void
              InitializeComponent() : Void
              Label1_Click(Object, EventArgs) : Void
            ⊞ Button1 : Button
            ⊞ Label1 : Label
            ⊞ TextBox1 : TextBox
              __ENCList : List<WeakReference>
              _Button1 : Button
              _Label1 : Label
              _TextBox1 : TextBox
              components : IContainer
      ⊞ {} MyExe.My
```

Figure 11. *MyExe Tree view*

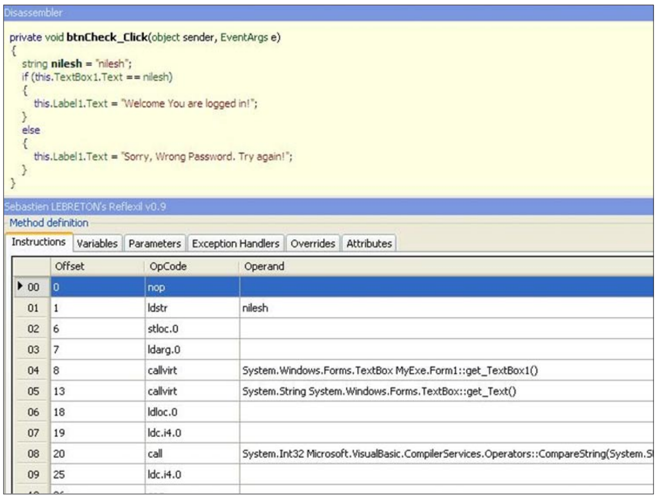


Disassembler

```
private void btnCheck_Click(object sender, EventArgs e)
{
   string nilesh = "nilesh";
   if (this.TextBox1.Text == nilesh)
   {
      this.Label1.Text = "Welcome You are logged in!";
   }
   else
   {
      this.Label1.Text = "Sorry, Wrong Password. Try again!";
   }
}
```

ventArgs) : Void

Figure 12. *Code for checking password*



Disassembler

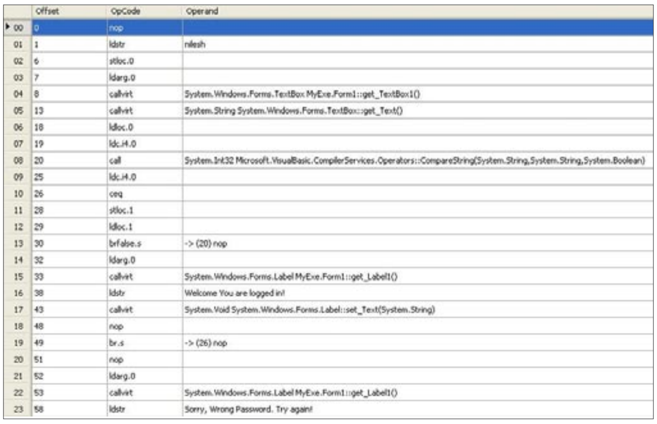
```
private void btnCheck_Click(object sender, EventArgs e)
{
   string nilesh = "nilesh";
   if (this.TextBox1.Text == nilesh)
   {
      this.Label1.Text = "Welcome You are logged in!";
   }
   else
   {
      this.Label1.Text = "Sorry, Wrong Password. Try again!";
   }
}
```

Sebastien LEBRETON's Reflexil v0.9

Method definition

	Offset	OpCode	Operand
▸ 00	0	nop	
01	1	ldstr	nilesh
02	6	stloc.0	
03	7	ldarg.0	
04	8	callvirt	System.Windows.Forms.TextBox MyExe.Form1::get_TextBox1()
05	13	callvirt	System.String System.Windows.Forms.TextBox::get_Text()
06	18	ldloc.0	
07	19	ldc.i4.0	
08	20	call	System.Int32 Microsoft.VisualBasic.CompilerServices.Operators::CompareString(System.S
09	25	ldc.i4.0	

Figure 13. *Reflexil plugin*



	Offset	OpCode	Operand
▸ 00	0	nop	
01	1	ldstr	nilesh
02	6	stloc.0	
03	7	ldarg.0	
04	8	callvirt	System.Windows.Forms.TextBox MyExe.Form1::get_TextBox1()
05	13	callvirt	System.String System.Windows.Forms.TextBox::get_Text()
06	18	ldloc.0	
07	19	ldc.i4.0	
08	20	call	System.Int32 Microsoft.VisualBasic.CompilerServices.Operators::CompareString(System.String,System.String,System.Boolean)
09	25	ldc.i4.0	
10	26	ceq	
11	28	stloc.1	
12	29	ldloc.1	
13	30	brfalse.s	-> (20) nop
14	32	ldarg.0	
15	33	callvirt	System.Windows.Forms.Label MyExe.Form1::get_Label1()
16	38	ldstr	Welcome You are logged in!
17	43	callvirt	System.Void System.Windows.Forms.Label::set_Text(System.String)
18	48	nop	
19	49	br.s	-> (26) nop
20	51	nop	
21	52	ldarg.0	
22	53	callvirt	System.Windows.Forms.Label MyExe.Form1::get_Label1()
23	58	ldstr	Sorry, Wrong Password. Try again!

Figure 14. *The IL in Refelxil*

let me in !). Now you have various options- you can change the records, include your own records or simply steal the passwords. Edit the file as follows (Figure 5).

Save the changes made as *.flm* file. Now we shall reassemble the SWF file: see Figure 6.

We have now the changed copy of AirHocky.swf. Run the file. Enter the password: *NILESH* (Figure 7).

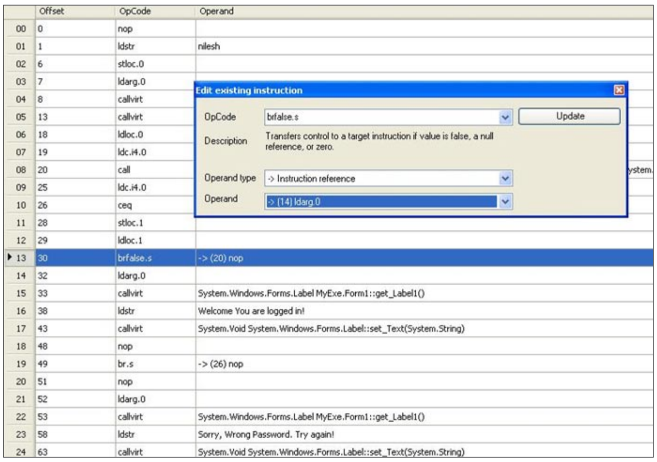
The application will successfully accept the changes. Even we can change Frey's profile to Nilesh (Figure 8).

.NET reversing

Now we shall see how to reverse .NET applications. A program made for the .NET framework is not compiled directly to machine code (as is the case with most traditional languages, e.g. C++), but is instead compiled to an Intermediate Language also called IL. IL is similar to bytecode in Java.

The tool here used is Refelctor, developed by Lutz Roeder, which allows you to load .NET executable and compile it into your language of choice. In addition to that we shall be using a popular plugin for Reflector called *Refelxil*. Reflexil enables you make changes in IL of the program.

I have developed a small program (*MyExe.exe*) for showing some basic concepts on how to reverse engineer a .NET file (Figure 9). The application accepts



	Offset	OpCode	Operand
00	0	nop	
01	1	ldstr	nilesh
02	6	stloc.0	
03	7	ldarg.0	
04	8	callvirt	
05	13	callvirt	
06	18	ldloc.0	
07	19	ldc.i4.0	
08	20	call	ystem.
09	25	ldc.i4.0	
10	26	ceq	
11	28	stloc.1	
12	29	ldloc.1	
▸ 13	30	brfalse.s	-> (20) nop
14	32	ldarg.0	
15	33	callvirt	System.Windows.Forms.Label MyExe.Form1::get_Label1()
16	38	ldstr	Welcome You are logged in!
17	43	callvirt	System.Void System.Windows.Forms.Label::set_Text(System.String)
18	48	nop	
19	49	br.s	-> (26) nop
20	51	nop	
21	52	ldarg.0	
22	53	callvirt	System.Windows.Forms.Label MyExe.Form1::get_Label1()
23	58	ldstr	Sorry, Wrong Password. Try again!
24	63	callvirt	System.Void System.Windows.Forms.Label::set_Text(System.String)

Edit existing instruction

OpCode: brfalse.s

Description: Transfers control to a target instruction if value is false, a null reference, or zero.

Operand type: -> Instruction reference

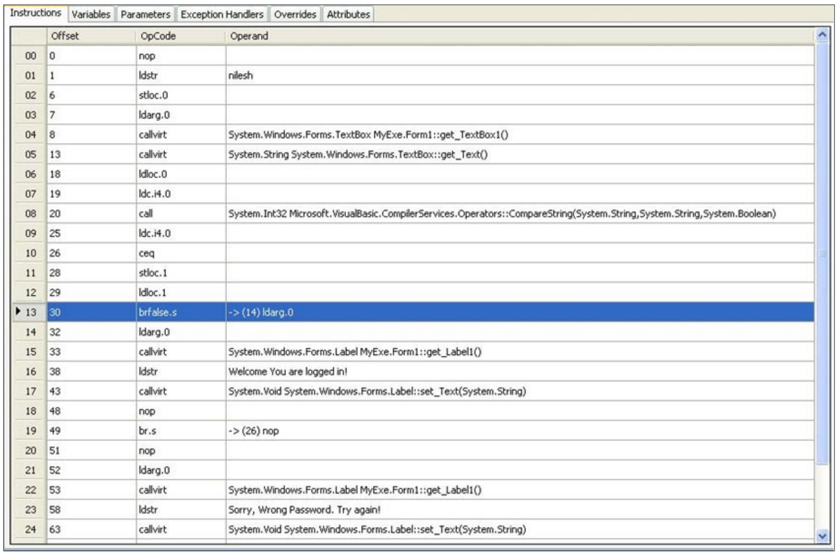
Operand: -> (14) ldarg.0

Figure 15. *Editing the IL*

a preset password and displays Error message or logged in message matching the user.

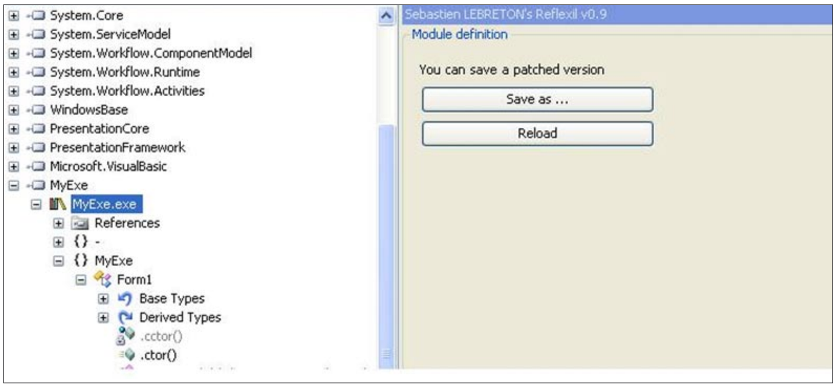
Now let's open the Reflector. Go to *File menu->Open and select MyExe.exe*. Now you can see the attached program like this (Figure 10).

You can select any language from above drop down menu as the main language C#. Other lanagueges available are: Visual Basic, Delphi, IL etc. But C# is a bit easier to understand. When you expand the tree you can see the forms and several GUI elements and functions in it (Figure 11).



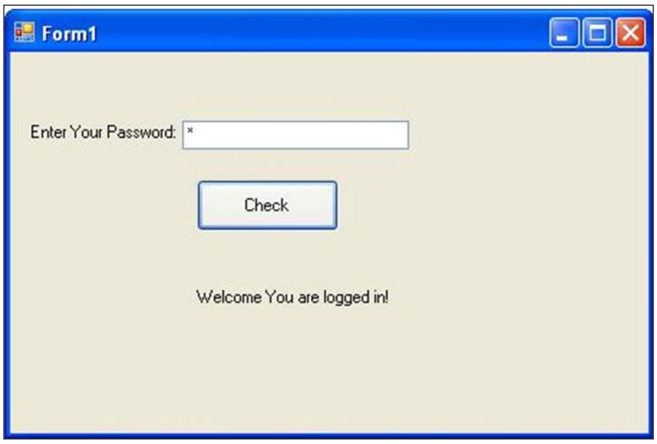
	Offset	OpCode	Operand
00	0	nop	
01	1	ldstr	nilesh
02	6	stloc.0	
03	7	ldarg.0	
04	8	callvirt	System.Windows.Forms.TextBox MyExe.Form1::get_TextBox1()
05	13	callvirt	System.String System.Windows.Forms.TextBox::get_Text()
06	18	ldloc.0	
07	19	ldc.i4.0	
08	20	call	System.Int32 Microsoft.VisualBasic.CompilerServices.Operators::CompareString(System.String,System.String,System.Boolean)
09	25	ldc.i4.0	
10	26	ceq	
11	28	stloc.1	
12	29	ldloc.1	
▸ 13	30	brfalse.s	-> (14) ldarg.0
14	32	ldarg.0	
15	33	callvirt	System.Windows.Forms.Label MyExe.Form1::get_Label1()
16	38	ldstr	Welcome You are logged in!
17	43	callvirt	System.Void System.Windows.Forms.Label::set_Text(System.String)
18	48	nop	
19	49	br.s	-> (26) nop
20	51	nop	
21	52	ldarg.0	
22	53	callvirt	System.Windows.Forms.Label MyExe.Form1::get_Label1()
23	58	ldstr	Sorry, Wrong Password. Try again!
24	63	callvirt	System.Void System.Windows.Forms.Label::set_Text(System.String)

Figure 16. *Updating the IL*



You can save a patched version

Figure 17. *Save the Patched EXE*



Enter Your Password: *

Welcome You are logged in!

Figure 18. *The Patched EXE*

Also we see function like `btnCheck_Click()` which may be our particular interest. Let's examine the code. Double click it and the code will be shown into C# source code in disassemble window (Figure 12).

Here we can see the logic of the program. As you clearly see the password is *nilesh* to login successfully into the application. Now you can directly use the password to login to the application.

Our next step is to patch the application. We can change the flow of the application so that it accepts any password provided! Go to tool menu and select Reflexil for translating the source code above into IL that can be edited (Figure 13).

Now inspect the code in Reflexil closely (Figure 14).

At line 01 the program is loading string *nilesh* with the opcode ldstr. At line 04 and 05 it's accepting inputs from user and then comparing both at line 08. Look at opcode brfalse.s at line 13. Opcode brfalse.s takes decision and if value is false and transfers the control to line 20 which is followed by *Sorry, Wrong Password. Try again!* message. So if we change the flow at line 13 then the application will have no way to tell the program what to do if password doesn't match. So it will execute sequentially and allow anybody with any password to enter the application. Right click on the line 13 and select Edit. You can now edit the OpCode and Operands at that line. In the Operand drop down list, select `->(14)ldarg.0` (Figure 15). Click update, to patch the code. Now you can see the flow of the code has changed at line 13 (Figure 16). Now the application will go to Line 14 in the *False* condition also. So in any condition the application will greet you with *Welcome you are logged in!*

Now time to generate the new patched exe. Navigate to MyExe.exe in the tree list and you can see *Save As* option in right frame (Figure 17). Save the patched exe wherever you want. It will automatically generate a new name like *MyExe.Patched.exe*. Now when you run the new exe and enter any password be it correct or wrong, it will accept (Figure 18).

NILESH KUMAR

Nilesh Kumar is working as an Engineer-Security Analyst with Honeywell Technology Solutions Lab, Bangalore, India. He is mainly focused on Application Security ranging from Code Review to Black Box Testing. Apart from that he shows interest in Network Security and Reverse Engineering.
(Blog: nileshkumar83.blogspot.com)

Web Malware

Part 1

The Internet has been plagued by a variety of Malware that use the Web for propagation and as these threats loom around in the Internet it can infect even the smartest and the most tech savvy computer users.

What you will learn...

- Why the Malware landscape has changed recently
- Why the Web has become a very successful mode for Malware propagation

What you should know...

- Basics about Malwares, AntiViruses, Internet and Web based Applications

These days Malware have become mature enough as they use newer methods and technologies to spread. Gone are the days when these Malware depended on the ignorance of the victims. The success of a Malware depends on one simple factor i.e. maximum number of infected computers in the least possible time. So, for any Malware to succeed, it should find out an effective propagation mechanism and channel that has the maximum reach. From the days of the macro virus to the fast spreading email borne viruses, from network worms to mass USB infectors, we have seen that with the increase in popularity of a technology, the propagation methodology of Malware also change.

There are various write-ups available in the internet that talks about the increasing trend of Web Malware and the statistics involved to justify these facts. But seldom have we come across an article that discusses the various methodologies and ways by which Malware authors use the web for Malware propagation. In this article, we will focus more about the ways by which Malware successfully use the Web as an infection vector. We would also look into the techniques that these Web Malware use to infect and evade detection. However, for the sake of the topic and for information, we would also include relevant and detailed statistics that would show how the Malware landscape has changed and how it has incorporated the Web as a very successful mode of propagation.

Till now we had been using the term *Web Malware*, but what do we mean by this? Before we define what exactly makes a Malware fall under the category of Web Malware, we must stress on the fact that there is no ambiguity with the word Malware as such. A Malware is unwanted software which may or may not carry out malicious activities in the system. The word Malware is a broad classification of various types of threats and unwanted software viz. Trojans, Worms, Viruses, Spywares, Rogue Security Applications etc. Though the word Malware is derived from the term Malicious Software, but a Malware may not always be malicious, at least as far as the meaning of the word malicious is concerned. For example, joke programs, remote administration tools etc may not be as malicious as a Trojan or Worms, but they can also be identified as Malware depending on the purpose of these application. So, it is the intent of the software that determines if it can be classified as a Malware.

Increase in Web Malware Activity

There have been many discussions in various Forums, Blogs and Message Boards that the Web has now become the primary vehicle for the Malware to enter our networks. For more details about such a presentation, please refer to the WebCast *Web Attacks: How Hackers Create and Spread Malware*, presented by *Chris McCormack* (*Web Security Expert – Sophos*) and

Fraser Howard (*Principal Researcher – Sophos*). It is very scary, as pointed out in this WebCast, that there is no such thing as a trusted website. Even the most legal site can become the epicenter of spreading out Malware infections. From the popular social networking sites to private/public discussion boards, web sites and blogs, anything can become the harboring ground of these Web Malware. The table below, taken from Kaspersky Security Bulletin (Statistics 2008), shows the number of Web Malware detected in some of the popular social networking site. This statistics is compiled by comparing the number of malicious programs that attacked users of different social networking sites (Table 1).

Similarly, the below graph shows the sudden increase of Web Malware activity related with some of the popular social networking sites (see Figure 1).

Table 1. *Malwares in Social Networking Sites*

Social Networking Site	Malware Detected (2008)	Registered Users (2008)
Odnoklassniki (*www.odnoklassniki.ru*)	3302 Malware	22000000 Users
Orkut (*www.orkut.com*)	5984 Malware	67000000 Users
Bebo (*www.bebo.com*)	2375 Malware	40000000 Users
Livejournal (*www.livejournal.com*)	846 Malware	18000000 Users
Friendster (*www.friendster.com*)	2835 Malware	90000000 Users
Myspace (*www.myspace.com*)	7487 Malware	253000000 Users
Facebook (*www.facebook.com*)	3620 Malware	140000000 Users
Cyworld (*us.cyworld.com*)	301 Malware	20000000 Users
Skyblog (*www.skyblog.com*)	28 Malware	2200000 Users

Source: Kaspersky Security Bulletin (Statistics 2008)

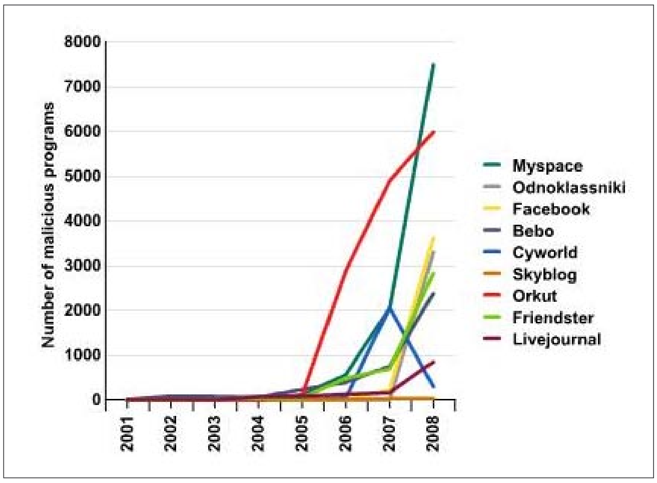


Figure 1. *Targeting the Social Networking Sites(Source: Kaspersky Security Bulletin (Statistics 2008))*

Recently it was discovered that social networking sites were getting used as botnet command control. *Arbor Network Security* reported that, they have identified a *Twitter* account that was being used as part of an update server for infected systems that were part of a botnet. This account was issuing base 64 encoded tweets that pointed to links where the infected computers could receive malware updates from. Almost similar kinds of botnet command control mechanism were also detected in *Tumblr* & *Jaiku* as well. These bots were using *RSS* feed to get the status updates.

It was pointed out by Google that *1% of all search results contained at least one result that point to malicious content and the trend seems to be increasing*. Of the billions of web pages that they *have investigated*, more than 3 million unique URLs on over 180,000 web sites automatically install Malware by drive-by download. Shown below are some of the interesting statistics of Malware activity identified in the Web. These interesting trends were observed by the *Google Security Team*. (see Figure 2).

The above graph shows the percentage of daily queries that contain at least one search result identified as Malicious (see Figure 3).

The above graph shows the number of entries in the *Google Safe Browsing Malware List*. It becomes obvious from these graphs that in the last few years there has been a constant increase of Web related Malware. The Google research paper on this increasing trend of Web Malware activity, as observed by the

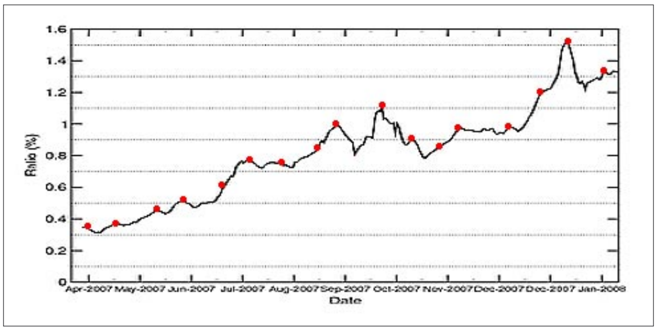


Figure 2. *Web Malware Activity (Source: Google Online Security Blog)*

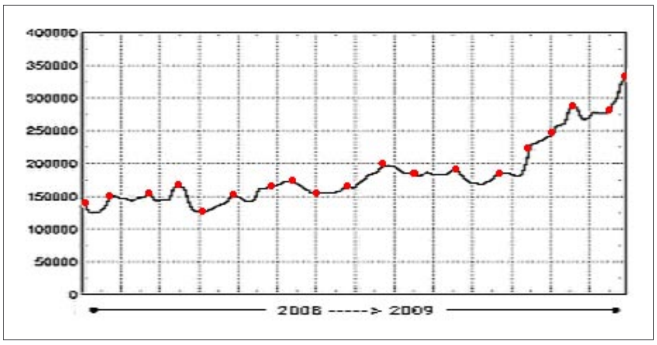


Figure 3. *Malicious Search Result Per Day (Source: Google Online Security Blog)*

Google Security Team, can be referred to from the URL mentioned below in the reference section of this article (*Google Research*).

Taken from *Kaspersky Monthly Malware Statistics*, the below table shows the top twenty Web Malware with new infections detected (highlighted in yellow) and the number of infected web pages (Table 2).

Web Malware have become a major contributor to this growing Malware menace. According to *ScanSafe's Annual Threat Report*, on an analysis of 200 billion web requests they came to a conclussion that web malware infection surged 582 percent last year, with a significant increase visible toward the last quater of 2008. Security researchers at *AVG Technologies* have observed that the number of new infected Web sites has grown by 66 percent, from 100,000 to 200,000 per day to 200,000 to 300,000 per day it is expected that this trend would continue in days to come.

Since 2006, the number of Malware signatures of most of the Antivirus vendors has doubled. But with new variants getting created, newer methods of infection and an increase in the numbers of distribution points, which are mainly compromised websites, this has resulted in a situation where the Antivirus vendors are now finding it difficult to block these threats, hence, resulting in misses in Malware detection. Earlier Antivirus companies were blocking a major portion of these Malware with dedicated and generic signatures. However today, it has become literally impossible to block these Malware with older methodologies. The below statistics (Jan-Jun 2009) shows the misses by some of the major Antivirus engines to detect Malware and this trend has increased off late.

Table 2. *Top 20 Web Malwares*

Position	Malware Name	Infected Web Pages
1	Trojan-Downloader.JS.Gumblar.a	8538
2	Trojan-Clicker.HTML.IFrame.kr	7805
3	Trojan-Downloader.HTML.IFrame.sz	5213
4	Trojan-Downloader.JS.LuckySploit.q	4719
5	Trojan-Downloader.HTML.FraudLoad.a	4626
6	Trojan-Downloader.JS.Major.c	3778
7	Trojan-GameThief.Win32.Magania.biht	2911
8	Trojan-Downloader.JS.ShellCode.i	2652
9	Trojan-Clicker.HTML.IFrame.mq	2576
10	Exploit.JS.DirektShow.o	2476
11	Trojan.JS.Agent.aat	2402
12	Exploit.JS.DirektShow.j	2367
13	Exploit.HTML.CodeBaseExec	2266
14	Exploit.JS.Pdfka.gu	2194
15	Trojan-Downloader.VBS.Psyme.ga	2007
16	Exploit.JS.DirektShow.a	1988
17	Trojan-Downloader.Win32.Agent.cdam	1947
18	Trojan-Downloader.JS.Agent.czm	1815
19	Trojan-Downloader.JS.Iframe.ayt	1810
20	Trojan-Downloader.JS.Iframe.bew	1766

Source: Kaspersky Monthly Malware Statistics

After calculating an average daily detection rate of some of the major Antivirus vendors, it was revealed by *Cyveillance*, a cyber-intelligence gathering company, that none of these Antiviruses were going over the 50% mark as far as successful detection is concerned. The top five scores came from *McAfee* (44 percent), *Sophos* (38 percent), *Dr. Web* (36 percent), *Symantec* (35 percent) and *Trend Micro* (34 percent). The list also had details of *AVG* (31 percent), *F-Secure* (28 percent), *ESET* (27 percent), *Sunbelt* (26 percent), *F-Prot* (23 percent), *Norman* (23 percent), *Kaspersky* (18 percent) and *VirusBuster* (16 percent). *Similarly*, *Panda Security Research* also reported that, out of 1.5 million home computers they looked into, only 37.45 percent were correctly protected with an active anti-malware solution with the latest signature database and out of these protected computers, 22.97 percent had active malware infections which were undetected by the anti-malware solution. This is because; more than 52 percent of the Malware will get reconfigured within 24 hours of its first release so that they can evade signature-based scanners. They also audited a total of 1,206 companies' network. These networks were protected by a variety of different security vendors and in 69.34 percent of the cases they were correctly protected. However they still found that 71.79 percent systems of these networks were actively infected with Malware.

Why is The Web Targeted by Malware

As pointed out in the begening of this article that the success of a Malware depends on one simple factor which is, maximum number of infected computers in the least possible time and with least possible effort.

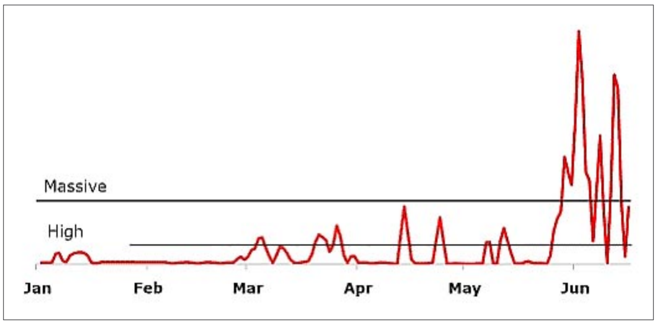


Figure 4. *Misses in Malware Detection (Source: CommTouch Labs)*

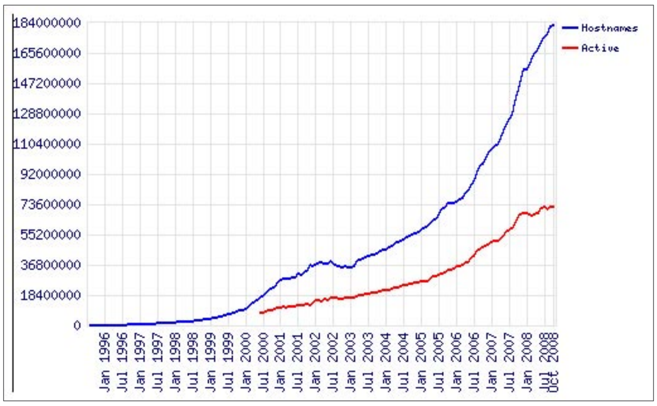


Figure 5. *Total Number of Websites*
(Source: Netcraft October 2008 Web Server Survey)

So, for any Malware to succeed, it should find out an effective propagation mechanism and channel that has the maximum reach. The target for attackers today, is the information residing in the endpoints and not the infrastructure. The web has become a major vector for Malware authors to use it as a very effective medium of Malware propagation and now a day's even a trusted website is no longer safe. To understand why the Malware authors are using the Web as a very effective channel for Malware propagation, let's look into some interesting statistics.

Table 3. *World Internet Usage*

World Internet Usage and Population Statistics				
World Regions	Population	Internet Users	Internet Users	Penetration
	(2009 Est.)	Dec. 31, 2000	Latest Data	(% Population)
Africa	991,002,342	4,514,400	65,903,900	6.70%
Asia	3,808,070,503	114,304,000	704,213,930	18.50%
Europe	803,850,858	105,096,093	402,380,474	50.10%
Middle East	202,687,005	3,284,800	47,964,146	23.70%
North America	340,831,831	108,096,800	251,735,500	73.90%
Latin America/ Caribbean	586,662,468	18,068,919	175,834,439	30.00%
Oceania / Australia	34,700,201	7,620,480	20,838,019	60.10%
World Total	6,767,805,208	360,985,492	1,668,870,408	24.70%

Source: Internet Usage and World Population Statistics 2009

Table 4. *Internet Activity Index*

Category	2003 Avg Time (hours: minutes)	2009 Avg Time (hours: minutes)	Change in Time
Content	3:42	6:58	88%
Communications	5:20	4:54	-8%
Commerce	2:07	2:40	26%
Community	N/A	3:01	N/A
Search	0:27	0:57	111%

Source: OPA Internet Activity Index

Increase in Number of Websites

As per *Netcraft*, an internet research company, the total number of websites on the Internet has exceeded the 182 million mark (see Figure 5).

The above graph shows the total number of websites sites across all domains since August 1995 to October 2008. During their *October 2008 Web Server Survey* they received responses from 182,226,259 sites. This overwhelming response meant a growth of 948 thousand since the September 2008 Survey.

Increase in World Wide Internet Users

As per the *Internet Usage and World Population Statistics* for June 30, 2009, there are approximately 1,668,870,408 Internet users around the world. There has been an increase of 21.6 percent Internet Users as compared to what it was in the year 2000. The internet has penetrated to 24 percent of the world population. Please refer to the chart in Table 3.

Increase in Time Spent Online

According to new reports from *Online Publishers Association* (OPA) based on a six-year analysis of its *Internet Activity Index* (IAI) has shows that percentage of time spent online with websites providing news, information and entertainment (content sites) etc. has grown from 34 percent of total time spent in 2003 to 42 percent in 2009, a significant 24 percent increase. Please refer to the chart in Table 4.

The above statistics definitely shines a light in one fact that the Web has become a popular resort to the growing number of internet users. As more and more internet users are accessing the various Websites and Web related technologies, the more target audience these Malware get. This is a situation from where there is no turning back. In days to come, there will be more Websites and Web related technologies and also the internet which will penetrate into the lives of more people from arround the world. Although this is a good reason for the Malware authors to shift their focus to the Web world but this is obviously not the only reason why Malware have muted to transform themselves into effective Web attacks. There are various other contributing factors for the Malware to choose the Web as an effective propagation channel. To understand this, lets first see what is different in Web Malware that makes it stealthier than a traditional Malware like a regular virus or worm.

The biggest difference between them is the way they infect a system. A typical virus or worm will infest other vulnerable system by exploiting either some underlying OS vulnerability or an application vulnerability. During the exploitation phase it will send out malicious packets containing the exploit code to the remote vulnerable system. Whenever we are talking about sending packets to a remote system, we generally need to establish a socket connection. A socket is a programatic representation of IP, Port and Protocol. Now, a host based firewall in the remote system would usually be configured to block these incoming connection requests on ports untill and unless it's explicitly configured to allow them on those ports. This is when a simple host based firewall can thwat possible infections even when there are vulnerable services in the system. However, the presence of a host based firewall doesn't mean that it would block all infections. As we said, since its blocking all the ports except the ones that it has allowed so vulerable services listening on ports which are allowed in the firewall are very much exposed and prone to exploitation and as a result, getting the system infected. But what if this port is closed? The vulnerable system would not get the exploit code at all thus no further infections. This is where lies the efficiency of Web Malware.

A Web Malware on the other hand will enter a system using the port 80 and as HTTP traffic. The best thing is, the user himself is doing a legitimate activity, for example browsing, downloading etc. and invites the Malware. In majority of the cases he does it unknowingly. In all systems, the incoming request on HTTP port is always open because a closed HTTP port would mean that the user will not be able to browse the internet. This is how Malware authors, by creating Web Malware, completely eradicated the possibility of a closed ports thus ensuring that the Malware would reach the client system for sure. Hence, every endpoint is a potential target for these Malware.

Today the OS is not used by Malware as a target as it was in the past. The attack focus has shifted from the OS to Application layer. The simple truth is that the attack surface of a Web application is technically

On the 'Net

- Microsoft Security Intelligence Report volume 6 (July – December 2008) – *http://www.microsoft.com/downloads/details.aspx?FamilyID=aa6e0660-dc24-4930-affd-e33572ccb91f&displaylang=en*
- Web Attacks: How Hackers Create and Spread Malware – *https://www.techwebonlineevents.com/ars/eventregistration.do?mode=eventreg&F=1001718&K=4ON&cid=well2_webc_*
- Kaspersky Security Bulletin (Statistics 2008) – *http://www.viruslist.com/en/downloads/vlpdfs/kaspersky_security_bulletin_part_2_statistics_en.pdf*
- Kaspersky Monthly Malware Statistics – *http://www.viruslist.com/en/analysis?pubid=204792071*
- Security Response Blog – *http://www.symantec.com/connect/symantec-blogs/security-response*
- Google Online Security Blog – *http://googleonlinesecurity.blogspot.com*
- Google Research – *http://research.google.com/archive/provos-2008a.pdf*
- Arbor Network Security – *http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel*
- Commtouch Q2 2009 Internet Threats Trend Report – *http://blog.commtouch.com/cafe/data-and-research/q2-internet-threats-trend-report-released*
- Panda Security Research – *http://research.pandasecurity.com/archive/tags/stats/default.aspx*
- F-Secure Web Blog – *http://www.f-secure.com/weblog/archives/00001427.html*
- ScanSafe Annual Threat Report – *http://www.scansafe.com/__data/assets/pdf_file/3005/ScanSafe_-_Annual_Global_Threat_Report2.pdf*
- Netcraft October 2008 Web Server Survey – *http://news.netcraft.com/archives/2008/10/29/october_2008_web_server_survey.html*
- Internet Usage and World Population Statistics 2009 – *http://www.internetworldstats.com/stats.htm*
- OPA Internet Activity Index – *http://www.online-publishers.org/newsletter.php?newsId=556&newsType=pr*
- Neil MacDonald – Gartner Blog Network – *http://blogs.gartner.com/neil_macdonald*
- IBM ISS X-Force Lab Malware Report – *http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf*
- Cyveillance Report – *http://www.cyveillance.com/web/docs/WP_CyberIntel_H1_2009.pdf*
- Wikipedia (Rogue security software) – *http://en.wikipedia.org/wiki/Rogue_security_software*
- Google Online Security Blog – *http://googleonlinesecurity.blogspot.com/2009/06/top-10-malware-sites.html*
- *Common Vulnerabilities and Exposures* (CVE) – *http://www.cve.mitre.org/index.html*
- Secunia Advisory – *http://secunia.com/advisories*
- iDefense Security Advisory – *http://labs.idefense.com/intelligence/vulnerabilities*
- Web Browser Plugins Vulnerabilities – *d0ubl3_h3lix*
- Trusteer's Rapport Security Service – *http://www.trusteer.com/solution*
- FireEye Malware Intelligence Labs – *http://blog.fireeye.com/research/2009/07/actionscript_heap_spray.html*
- Umesh Wanve (Zscalar Security Researcher) – *http://research.zscaler.com/2009/09/in-wild-flash-exploit-analysis-part-1.html*
- Brian Krebs (Washington Post) – *http://blog.washingtonpost.com/securityfix/2008/04/hundreds_of_thousands_of_micro_1.html*

broader than the regular desktop applications. It was reported by Neil MacDonald, a member of the *Gartner Blog Network*, that *Microsoft and the other OS vendors are getting better at producing more secure code and we are getting better at patching*. But on the other hand, vulnerable Web Applications on the Internet present a vast scope for Malware authors to target. Experts said that 2008 saw more than 300 percent rise in malicious attacks agaisnt web applications. MXLogic identified 25,000 daily SQL attacks on 2009 summer, but by October the number of attacks was reaching 450,000 a day. It is very interesting that in the second half of 2008, there was a 10 percent increase totaling 2,835 reported vulnerabilities and of those, 80 percent were web application related. As per *IBM ISS X-Force Labs* latest malware report:

- In 2008, 54.9 percent of all disclosed vulnerabilities were Web application vulnerabilities and were one of the primary factors in the overall growth of Vulnerability Disclosures during the year
- SQL injection attacks increased by 30 percent within the last six months
- 74 percent of Web Application vulnerabilities disclosed in 2008 had no patch by year end

How they use the Web to propagate Malware is conceptually very simple. As of now we will not go into the technical details of how these things are done. We will see these technical aspects in the next section. The below points will shows, conceptually, how easy it is for Web Malware to infect a system.

- Malware authors will compromise a Website and inject malicious code in it. Malware authors may even create Websites of their own with Web Malware embedded and entice users to visit the site.
- An Internet User browses these Websites.
- Unknown to the user, the Web Malware will silently sneak through by compromising some vulnerability present in the Web browser.
- User is infected with the Web Malware without his knowledge.

Keeping in mind the statistics and the charecteristics of Web Applications and the associated unpatched vulnerabilities, we can come to a conclussion that the Web is definitely a very effective channel of Malware propagation. Firewalls will generally not block incoming HTTP traffic; also, if the Antivirus/IDS have no information about that particular Web Malware then it will definitely go unnoticed and the endpoint will get infected.

The below details will show the efficiency with which the different categories of Websites are targeted for Malware propagation:

- Pornography – 10 percent
- Business – 10 percent
- Health & Medical – 10 percent
- Computer & Technology – 8 percent
- Search Engines & Portals – 7 percent
- Personal Sites – 7 percent
- Games – 3 percent
- Education – 3 percent
- Real Estate – 3 percent
- Shopping – 3 percent
- Others – 36 percent

Source: CommTouch Labs

For the Malware authors, choosing the Web to propagate Malware fulfills the condition of infecting the maximum number of computers in the least possible time with least possible effort.

Untill now, we were discussing the various aspects of Web Malware. Starting from the statistics that showed us the increase of Web Malware activity in recent times to why the focus of Malware authors have changed from creating havoc in the infrastructure to infecting the endpoints for various other henious purpose, we have seen it all. Once we are aware of these facts and figures, in the next section we will look into the *Technical Details of Web Malware (Part 2)*. We will be talking about *How Malware is designed for using the Web?* How *a Web Malware attacks a system? What are the different forms of Web Malware threats?* etc. These technical details will help us to understand, in a better and deeper way, the threat of Web Malware and also will help us to proactively take precautionary measures to avoid getting infected. As well as carry out identification, removal and remediation incase of a possible infection. Hopefully, this article was insightful and you now understand the various kinds of Web related Malware threats.

Note

A lot of information has also been compiled from various other freely available sources in the internet. Resemblance of any other article with this article is purely co-incidental and unintentional.

RAJDEEP CHAKRABORTY

Microsoft® MVP – Consumer Security (2009, 2010)

http://www.malwareinfo.org

http://in.linkedin.com/in/rajdeepchakraborty

http://mvp.support.microsoft.com/profile=62F27767-F7D0-448F-84C7-F28501B6ECCB

Cyber warfare

with DNSbotnets

Botnets aren't just a fad or items being sold and purchased like items on ebay, but are becoming carefully designed tools used for cyber war. In this article we will discuss what a Botnet is, and the next generation of Botnets over DNS.

What you will learn…

- DNS Botnet, The next Cyberwar, Public DNS

What you should know…

- Some about botnets, DNS protocol, blacklists

Let's start by defining the term *Botnet*. According to Wikipedia, a Botnet is a jargon term for a collection of software agents, or robots, that run autonomously and automatically. The term is most commonly associated with malicious software, but it can also refer to a network of computers using distributed computing software.

While botnets are often named after their malicious software name, there are typically multiple botnets in operation using the same malicious software families, but operated by different criminal entities.§

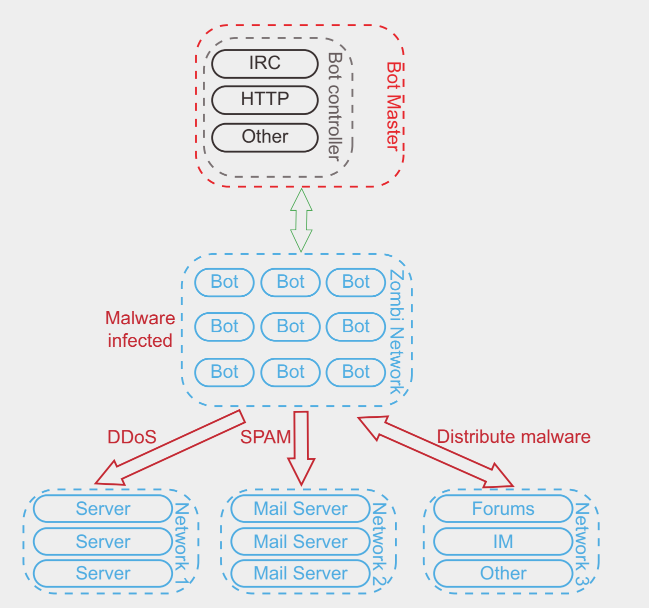


Figure 1. *Basic botnet scheme*

From this common definition we can deduce the basic behavior of a botnet and then start to develop a more complex vision of the problem (Figure 1).

These machines were first developed in the 90's. However, they were not just used for economic gains but instead to distribute attacks and bouncers for new attacks.

It was then the cybernetics mafia began using them in a new business model and to this day they are the most frequently employed for illegal acts on the Internet.

For this purpose they developed a new methodology based on the Malware infection so as to infect the resources of computers. In the beginning the most common way to control these infected computers was

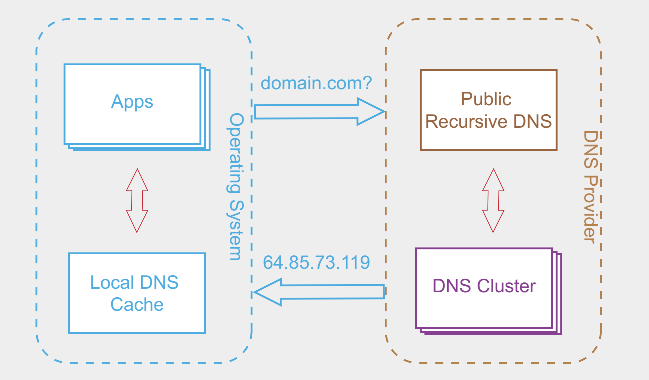


Figure 2. *Basic DNS query scheme*

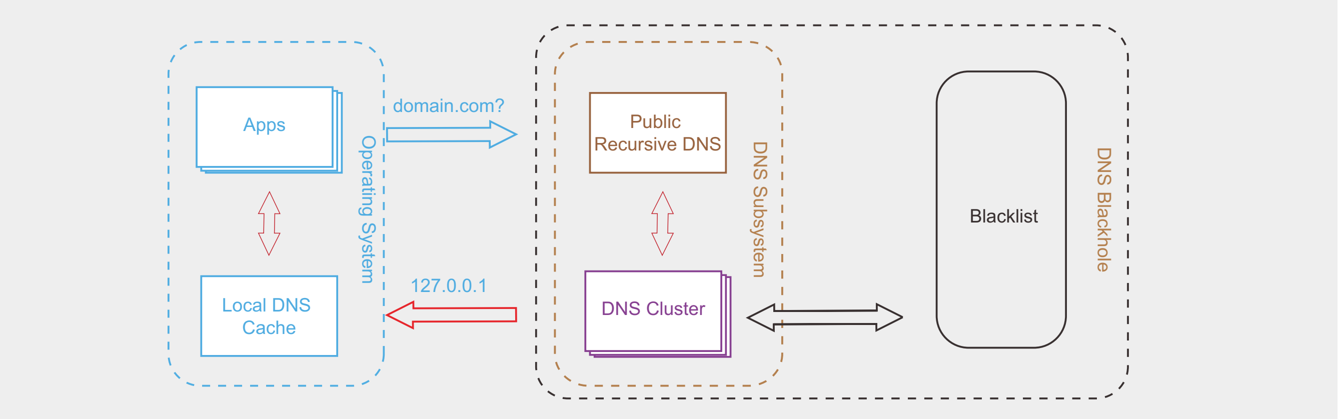


Figure 3. *Basic DNS query scheme with Blacklist*

to use an IRC (*Internet Relay Chat*) channel. Now a new mechanism for controlling has been developed that is becoming increasingly more common, which is based in HTTP (*Hypertext Transfer Protocol*). An example of this instance is being used on Twitter: *http://asert.arbornetworks.com/2009/08/twitter-based-botnet-command-channel/*).

Once the computer is infected with Malware and they start to access the channel control, the computers are in a *zombie-state* waiting for new orders from the Bot's Master side, who is the one frequently responsible for financing the creation of the botnet. The common objective of this payment is to be able to have access to this botnet in order to carry out malicious attacks, such as *DDoS* (*distributed denial-of-service attack*), *SPAM* (*junk-email*) or even to distribute more malware with other different objectives as *Phishing*.

As a solution, some companies offer a new internal security service whose objective is to prevent user access by deploying one of the oldest network protocols on the Internet, the DNS (*Dynamic Name Server* RFC 1034/1035 of 1987) protocol (Figure 2).

Clients request a name resolution for the *domain.com* through a public DNS server and this returns the result to the client 64.85.73.119. To add a new layer of security, companies make a *public DNS* server, available to the client that works in the same way as the standard protocol (Figure 3).

This server will compare *using a blacklist* whether or not the domain that is trying to be resolved, badsite.com, is available within their database of Malware domains. It will then process this information in order to disguise the name's resolution to a different IP, in this case 127.0.0.1. This kind of modification is known as DNS Hijacking. In this way we will be sure that our client is not caching the destiny.

By employing these services we will achieve the following:

- *DNS cache and less latency*: the Web browsing experience will be faster due to the server having most of the cases requested by other users. Most of them have a cluster Geo-located, improving the response time in every request.
- *Content parental control*: blacklist can have sites with pornographic content, violent, etc.
- *Anti-SPAM Filter*: is not necessary an external filter to know the origin of an active spam source. It was the case most frequently to use RBL (*Real-time Blackhole List*), DNSBL (*DNS Blacklists*), DRBL (*Distributed Real-time Block List*), DNSWL (*DNS Whitelist*), RHSBL (*Right Hand Side Blacklist*) or URIBL (*Uniform Resource Identifier Blacklist*). Frequently used from SPAMHAUS (*http://www.spamhaus.org*), SpamCop (*http://www.spamcop.net*).
- *AdSense filter*: apart of the Anti-SPAM filter, this can be exported to other protocols such as to HTTP, in which the filtering of the marketing content is even easier than putting a HTTP proxy with a blacklist.
- To have a *DNS address available and quite easy to remember.*
- *Orthographical correction and auto completion*: if a domain resolution fails, it can try to find out if there is some typographical error, returning the domain information in a good state.

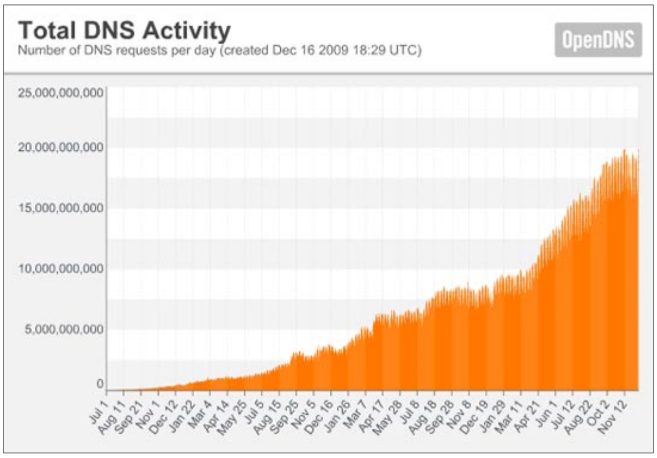
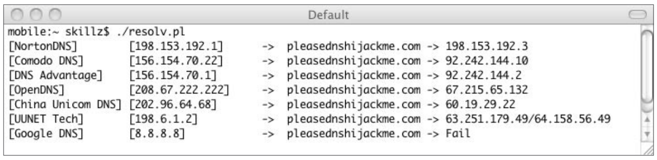


Figure 4. *DNS Activity from OpenDNS req/day*



```
mobile:~ skillz$ ./resolv.pl
[NortonDNS]         [198.153.192.1]      ->  pleasednshijackme.com -> 198.153.192.3
[Comodo DNS]        [156.154.70.22]      ->  pleasednshijackme.com -> 92.242.144.10
[DNS Advantage]     [156.154.70.1]       ->  pleasednshijackme.com -> 92.242.144.2
[OpenDNS]           [208.67.222.222]     ->  pleasednshijackme.com -> 67.215.65.132
[China Unicom DNS]  [202.96.64.68]       ->  pleasednshijackme.com -> 60.19.29.22
[UUNET Tech]        [198.6.1.2]          ->  pleasednshijackme.com -> 63.251.179.49/64.158.56.49
[Google DNS]        [8.8.8.8]            ->  pleasednshijackme.com -> Fail
```

Figure 5. *DNS Hijacking public servers*

We should remember that the purpose of Internet is to create a decentralized and independent network, or at least in definition it should be. But, what has happened with the bigger services operators that are providing public DNS services with the above characterizes mentioned? We can take an example from *OpenDNS*.

Latest statistics of use that are being published in various blogs (*http://blog.opendns.com*) are shedding light on some interesting data to consider (Figure 4).

As we see from the chart, resolving 20 millions of DNS petitions in 24h has doubled the final figure (10 millions), in April of the same year. More than 25.000 schools in the USA are using *OpenDNS*, and several companies are migrating to their services. In the following picture we can see the DNS petition within the public servers (mentioned above) that are being offered (Figure 5).

Maybe we all should take a moment to consider whether this is a good idea or not, or even if would be necessary to stop DNS botnets. We are allowing far too much control of the Internet, to multinational companies with their private interests and own servers. It has been proven that several of them are conducting DNS hijacking to return fake results and in order to redirect users to sites under their control, so as to demonstrate custom publicity through the domain showed, in order to generate stats to sell, etc. At the moment most of them are offering this service without personal benefit as a public service, but should we believe this?

Let's view the latest chart applied to devices that connect to the Internet (Figure 6).

Consider the control features of these devices that these companies can utilize in their clients' name. *As the next generation botnets are being developed we are seeing that they are being built with forethought and intelligent logic schemes* (Figure 7).

It is not necessary to find vulnerabilities to create bots: it is frequently seen that bots are launched through infections.

It is not necessary to develop Malware/Software for management or for updating: applications are continually being developed to deploy Malware. The necessary thing to do is to make an improvement in the protocol that will manage the bot. This is due to the fact that DNS resolutions are dynamic and a DNS server change can take effect immediately.

DNS resolution support overall operating systems: GNU/Linux, MS Windows, Mac OSX, Android, iOS, Bada, *Nix, VxWorks, etc.

Any device can be a Bot: a mobile phone with Internet connection, game console, etc.

Less evidence for forensic analysis: traffic captures, may not contain information of Malware working on

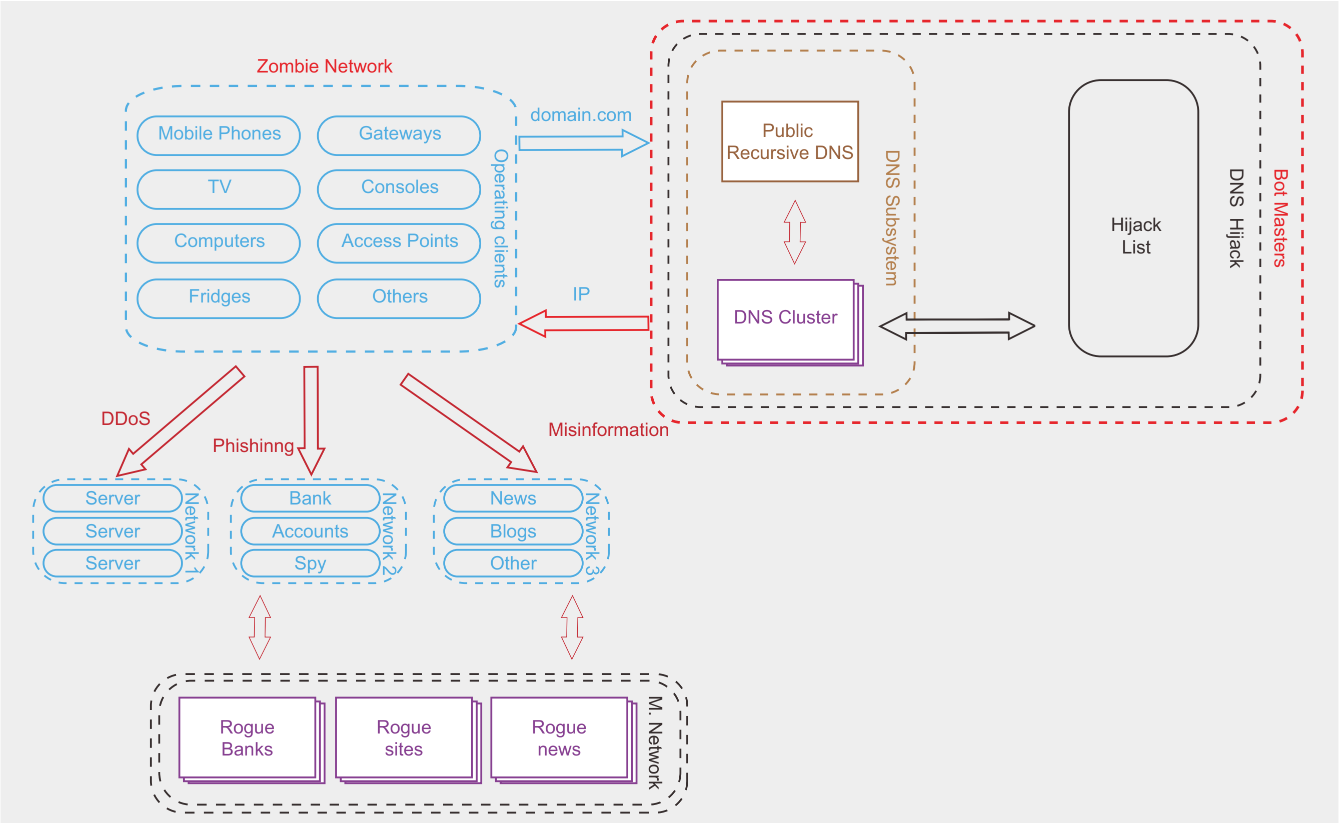


Figure 6. *Basic DNS query scheme with Blacklist updated*

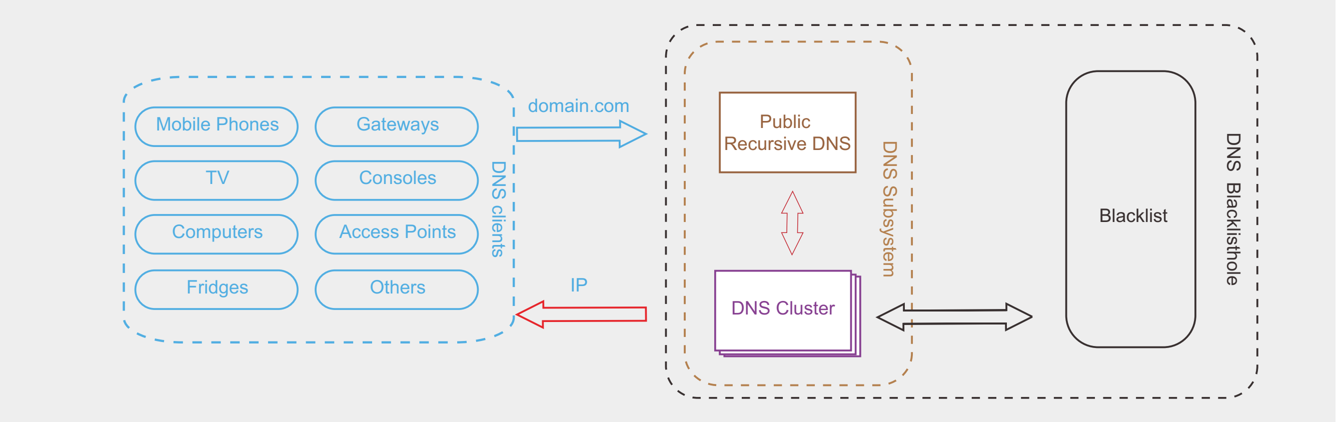


Figure 7. *Next botnet generation*

a system or DNS changes being made, because they are not being registered. Only the local DNS caches could give some evidence, but normally are not helpful because DNS changes can expire in short periods of time.

The infection is based on social engineering: offering a DNS service black hole, cache and an easy DNS address to remember.

The vast majority of firewalls allow DNS traffic: most organizations allow some form of external traffic for name resolution.

Capacity to attack based in Geolocation services: knowing the origin of the IP you can help to figure out the destination of a specific attack. Custom Phishing attacks, DDoS with less latencies in the same country, etc.

It is possible to do these following attacks, but they will become more sophisticated.

- *DDoS*: it is possible to pose as the client in order to forward all the traffic
- generated to IP victim directions. What will happen if we switch the register of *.google.com to critical an IP address?
- *Phishing*: by
- trusting the DNS server, attacks similar to DNS cache poising may occur. Resulting in sensitive information being captured, such as credit card
- numbers, bank information and other user account information.
- *Misinformation*: fake resources will be available, causing confusion to the user or population.
- *Spying*: it will be present in emails, instant messaging conversations or VoIP calls.

Several references are available indicating the presence of patriotic botnets that governments are developing containing their own weapons for future cyber war. Proof of this can be found in the following links: *http://seclists.org/fulldisclosure/2010/Jun/346*.

http://translate.google.es/translate?js=y&prev=_t&hl=es&ie=UTF-8&layout=1&eotf=1&u=http%3A%2F%2Fwww.publico.es%2F323921%2Fataque&sl=es&tl=en

It is evident to see that these companies are present in different locations within the most important countries of the World, and also that these resources are available for countries in conflict. The interest of the country will always override that of human logic, and this new form of weaponry will be used to neutralize the enemy. What will happen when the enemies begin to attack? Is it time for countries to create their own Golden shield project? A project operated by the *Ministry of Public Security* (MSP), a division of China's government, which started in 1998 and began operating fully in November of 2003.

Maybe this *China Firewall* is merely a simple tool to control and censure all their citizens. But ask yourself, is this project just a firewall, or is the real objective of this project just a way to hide Chinas' cyber arsenal at the ready for war?

Without legislation to control all of these mechanisms in a global and open way, within a country engaged in conflict that has the capability to create their own cyber-army, we will merely be pawns confused over the marketing. If we only give these controls under *trust* let us not forgot the words of George Washington: *To be prepared for war is one of the most effectual means of preserving peace*.

FRANCISCO ALONSO
Francisco Alonso. A.k.a. Reverse Skills.
Security researcher from Spain, 26 years old
http://twitter.com/revskills
reverseskills@gmail.com

Search Engine Security and Privacy

It's no secret that search engines like Google, Yahoo, Bing (MSN) retain search data and metadata regarding searches.

What you will learn…

- Search engines record your private information
- Search engines store your private information
- Search engines share your private information

What you should know…

- search engine basics

They are open about doing so. What's unsure, though, is to what extent this creates a long-term threat to information security and privacy. This article briefly reviews what data is retained and stored by these search engines and what readers can do to protect their information.

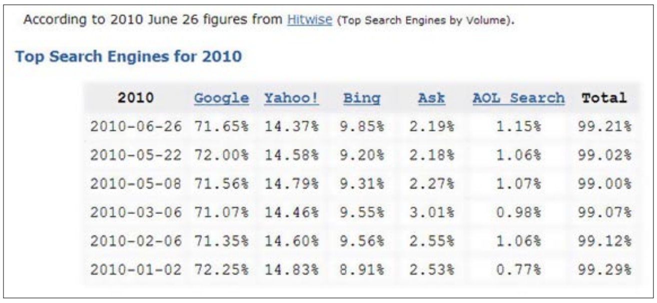
According to Hitwise.com the top 5 USA Search Engines by volume (as of June 26, 2010) are: Google – 71.65%, Yahoo – 14.37%, Bing (formerly MSN Live Search) – 9.85%, Ask (powered by Teoma) – 2.19%, and AOL Search (powered by Google) – 1.15%. *http://www.hitwise.com/us/datacenter/main/dashboard-10133.html* (see Figure 1 and Figure 2)

The leading third tier search engines are (in alphabetical order): AltaVista – Powered by Yahoo!, Fast (AlltheWeb.com) – Powered by Yahoo!, Gigablast, Netscape Search – Powered by Google, and Snap.com – Portions powered by: Gigablast, *Smarter.com*, *SimplyHired.com*, X1 Technologies, Inc. and Enhanced by Ask.com.

All search engines have privacy policies closely resembling Google's policy. For discussion purposes; Google's policy is an excellent baseline for review.

The concern is privacy. The Google search engine gathers many types of information about online activities. All of Google's current products, and likely its future products, will include data gathering and targeting as a primary business goal. All of Google's properties – including Google Search, Gmail, Orkut and Google Desktop – have deeply linked cookies that auto renew every two years. (See Google's response to US Representative Joe Barton 24 privacy questions December 21, 2007, *http://searchengineland.com/pdfs/071222-barton.pdf*) Each of these cookies has a globally unique identifier (GUID) and can store search queries every time you search the Web. Google does not delete any information from these cookies. Therefore, if a list of search terms is given, Google can produce a list of people who searched for that term, which is identified either by IP address or Google cookie value. Conversely, if an IP address or Google cookie value is given, Google can also produce a list of the terms searched by the user of that IP address or cookie value.

Google's Privacy Policy describes how they treat personal information when you use Google's products and services (*http://www.google.com/privacypolicy.html*) Listed below are two examples.



According to 2010 June 26 figures from Hitwise (Top Search Engines by Volume).

Top Search Engines for 2010

2010	Google	Yahoo!	Bing	Ask	AOL Search	Total
2010-06-26	71.65%	14.37%	9.85%	2.19%	1.15%	99.21%
2010-05-22	72.00%	14.58%	9.20%	2.18%	1.06%	99.02%
2010-05-08	71.56%	14.79%	9.31%	2.27%	1.07%	99.00%
2010-03-06	71.07%	14.46%	9.55%	3.01%	0.98%	99.07%
2010-02-06	71.35%	14.60%	9.56%	2.55%	1.06%	99.12%
2010-01-02	72.25%	14.83%	8.91%	2.53%	0.77%	99.29%

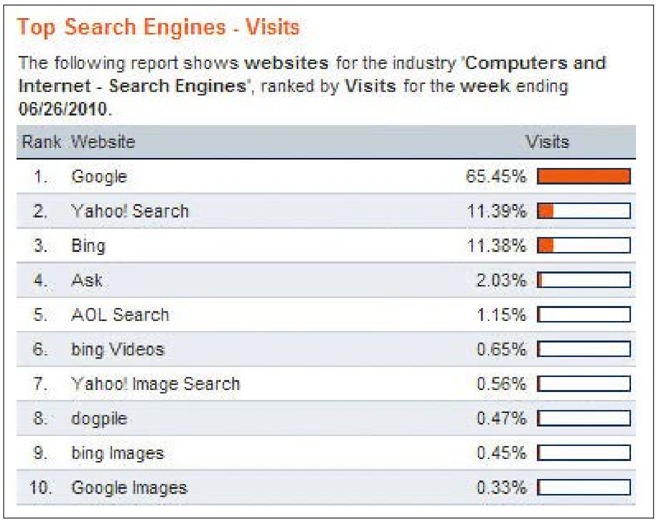
Figure 1. *Top Search Engines by Volume*

Log information – When you access Google services, (their) servers automatically record information that your browser sends whenever you visit a website. These server logs may include information such as your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser.

Location data – Google offers location-enabled services, such as Google Maps for mobile. If you use those services, Google may receive information about your actual location (such as GPS signals sent by a mobile device) or information that can be used to approximate a location (such as a cell ID). (Raj Goel, *Googling Security and Privacy*, InfoSecurity Professional)

Some of (their) services, including Google Toolbar and Google Web Accelerator, send the uniform resource locators (*URLs*) of web pages that you request to Google. When you use these services, Google will receive and store the URL sent by the web sites you visit, including any personal information inserted into those URLs by the web site operator. For example, when you submit information to a web page (such as a user login ID or registration information), the operator of that web site may *embed* that information – including personal information – into its URL (typically, after a question mark (?) in the URL). When the URL is transmitted to Google, (their) servers automatically store the URL, including any personal information that has been embedded after the question mark. Google does not exercise any control over these web sites or whether they embed personal information into URLs.

Remember, Google is not the only search engine that is storing, sharing (paid clients e.g. Google Analytics), and passing onto other third parties information that you might like to keep private. Are they doing this without your consent? No. Anytime you use a search engine you automatically have given them consent. They have information pages the state how they process personal information by referring to the privacy and supplementary privacy notices for particular services. The list below is included for your convenience.



Top Search Engines - Visits

The following report shows **websites** for the industry 'Computers and Internet - Search Engines', ranked by **Visits** for the **week** ending 06/26/2010.

Rank	Website	Visits
1.	Google	65.45%
2.	Yahoo! Search	11.39%
3.	Bing	11.38%
4.	Ask	2.03%
5.	AOL Search	1.15%
6.	bing Videos	0.65%
7.	Yahoo! Image Search	0.56%
8.	dogpile	0.47%
9.	bing Images	0.45%
10.	Google Images	0.33%

Figure 2. *Top Search Engines by Weekly Visits*

- *http://www.google.com/privacypolicy.html* – Privacy Policy
- *http://www.google.com/privacy_faq.html* – FAQ
- *http://www.google.com/privacy_blogs.html* – Blog posts
- *http://www.google.com/intl/en/corporate/privacy_principles.html* – Principles
- *http://www.youtube.com/user/googleprivacy* – Videos
- *https://www.google.com/dashboard* – Dashboard
- *http://www.google.com/ads/preferences/* – Ads Preferences Manager
- *http://tools.google.com/dlpage/gaoptout?hl=en* – Analytics Opt-out
- *http://www.google.com/accounts/TOS* – Terms of Service
- *http://www.google.com/corporate/privacy_principles.html* – Privacy Principles
- *http://www.google.com/privacypolicy.html* – Google's Privacy Policy
- *http://www.google.com/intl/en/sketchup/3dwh/privacy.html* – 3D Warehouse
- *http://www.google.com/privacy_ads.html* – Advertising
- *http://code.google.com/appengine/privacy.html* – App Engine
- *http://www.google.com/a/help/intl/en/users/privacy.html* – Apps
- *http://www.blogger.com/privacy* – Blogger
- *http://books.google.com/googlebooks/privacy.html* – Books
- *http://www.google.com/buzz/help/privacy.html* – Buzz
- *http://www.google.com/googlecalendar/privacy_policy.html*– Calendar
- *https://checkout.google.com/files/privacy.html* – Checkout
- *http://www.google.com/chrome/intl/en/privacy.html* – Chrome
- *http://www.google.com/chromeframe/intl/en/privacy.html* – Chrome Frame
- *http://www.google.com/comparisonads/privacy.html* – Comparison ads
- *http://desktop.google.com/privacypolicy.html* – Desktop
- *http://www.google.com/google-d-s/privacy.html* – Docs
- *http://www.google.com/tools/firefox/extensions_privacy.html* – Firefox Extensions

- *http://gears.google.com/privacy.html* – Gears
- *http://mail.google.com/mail/help/intl/en/privacy.html* – Gmail
- *http://www.google.com/goog411/privacy.html* – GOOG-411
- *http://code.google.com/webtoolkit/privacy.html* – Google Web Toolkit
- *http://groups-beta.google.com/googlegroups/privacy.html* – Groups
- *http://www.google.com/intl/en-US/health/about/privacy.html* – Health
- *http://www.google.com/help/privacy_fusionph.html* – iGoogle
- *http://knol.google.com/k/privacy-policy* – Knol
- *http://www.google.com/privacy-lsf.html* – Location Service in Firefox
- *http://maps.google.com/help/privacy_maps.html* – Maps
- *http://mobile.google.com/privacy.html* – Mobile
- *http://www.google.com/privacy_moderator.html* – Moderator
- *http://tools.google.com/dlpage/res/o3d/en/o3d_privacy_notice.html* – O3D
- *http://www.orkut.com/privacy.aspx* – Orkut
- *http://www.google.com/searchhistory/privacy.html* – Personalized Search
- *http://picasa.google.com/web/privacy.html* – Picasa
- *http://www.google.com/a/help/intl/en/security/terms/new_privacy.html* – Postini
- *http://www.google.com/powermeter/privacy* – PowerMeter
- *http://www.google.com/intl/en_us/privacy_browsing.html* – Safe Browsing
- *http://www.google.com/sites/help/intl/en/privacy_policy.html* – Sites
- *http://www.googlestore.com/shop.axd/PrivacyPolicy* – Store
- *http://www.google.com/talk/privacy.html* – Talk
- *http://www.google.com/mail/help/tasks/privacy.html* – Tasks
- *http://www.google.com/support/toolbar/?quick=privacy* – Toolbar
- *http://www.gstatic.com/marketplace-connect/html/en/privacy-policy.html* – Trader
- *http://translate.google.com/toolkit/TOS.html?hl=en* – Translator Toolkit
- *https://www.google.com/voice/help/privacy* – Voice
- *http://webaccelerator.google.com/privacy.html* – Web Accelerator

Is there anything you can do? Yes, rest assured that some things are still in your control. You can regularly delete most Google cookies when you close your browser or used an application like CCleaner.

To provide website visitors with more choice about how their data is collected by Google Analytics, they have developed the Google Analytics Opt-out Browser Add-on. The add-on communicates with the *Google Analytics JavaScript* (*ga.js*) to indicate that information about the website visit should not be sent to Google Analytics.

If you want to opt out, download and install the add-on for your current web browser. The Google Analytics Opt-out Browser Add-on is available for Internet Explorer (versions 7 and 8), Google Chrome (4.x and higher), and Mozilla Firefox (3.5 and higher). *http://tools.google.com/dlpage/gaoptout?hl=en*

There is still the issue with Gmail and Gmail mobile.

Gmail: The primary risk in using Gmail lies in the fact that most users give their consent to make Gmail more than an email-delivery service and enable features such as searching, storage and shopping. This correlation of search and mail can lead to potential privacy risks. For example, email stored on third-party servers for more than 180 days is no longer protected by the Electronic Communications Privacy Act, which declares email a private means of communication.

Gmail Mobile: Mobile phones are increasingly being sold with Gmail built in, and if not, it can be downloaded. The questions to ask: How uniquely does your mobile phone identify you as the user, and when was the last time you changed your phone and your identifiers? Gmail Patents: Gmail's Patent #20040059712 emphasizes *Serving advertisements using information associated with email*. This allows Google to create profiles based on a variety of information derived from emails related to senders, recipients, address books, subject-line texts, and path name of attachments and so on. (Raj Goel, *Googling Security and Privacy*, InfoSecurity Professional)

The bottom line is that no matter which top search engine you use, they are watching you and tracking you. At the bare minimum, do not use as your search engine the same company that you use for your email e.g. Google Search, Gmail instead Google Search and Yahoo Email or MSN Email.

Best solution? Do not use any of these search engines companies if at all possible. Have an email account that is not associated with any of them. Here are three alternatives but there are many more.

GMX Mail is a reliable email service filtered well of spam and viruses whose 5 GB of online storage you can use not only through a rich web interface but also via POP or IMAP from a desktop email program.

From the Middle East, Gawab.com makes it easy to compose emails in Arabic script even if your operating system and browser do not. It is a speedy, stable and very usable free email service with 10 GB online space, POP and IMAP access as well as many a web-based goodie.

Inbox.com not only gives you 5 GB to store your mail online but also a highly pol ished, fast and functional way to access it via either the web (including speedy search, free-form labels and reading mail by conversation) or through POP in your email program.

There are several recommended search engines that DO NOT track your activities what so ever.

A favorite is the search engine Ixquick (*www.ixquick.com*) which is the world's most private search engine. It focuses on delivering great search results with the best possible privacy. Ixquick is known as Startpage in the United States (*www.startpage.com*). Ixquick has the industry's leading Privacy Policy: No recording of users' IP addresses. No identifying cookies. No collection of personal data. No sharing personal data with third parties. Offers secure encrypted connections (HTTPS/SSL). And a free proxy service that allows anonymous browsing of websites.

No personally identifiable information is ever required by Yippy (*http://clusty.com/*). This means Yippy never seeks any information related to your name, telephone number, address, or even your email address unless you request a Yippy Service where that information is required. Yippy is intended to be an anonymous service.

Proxify (*https://proxify.us/*) is a web-based anonymous proxy service which allows anyone to surf the Web privately and securely. Unlike other proxies, there is no software to install or complicated instructions to follow. Just enter a URL (website address) in the form above. Through Proxify, you can use websites but they cannot uniquely identify or track you. Proxify hides your IP address and our encrypted connection prevents monitoring of your network traffic. Once using Proxify, you can surf normally and forget that it is there, protecting you.

Before you use the standard search engines and their services read through the *terms of service* and *privacy policy* for each of the services you will be using. You may find that using the search engine and those services is not worth the potential cost of losing your privacy.

REBECCA WYNN

Rebecca Wynn, MBA, CISSP, LPT, CIWSA, NSA/CNSS NSTISSI 4011-4016 is a Senior Information Security Analyst with NCI Information Systems, Inc. She has been on the Editorial AdvisoryBoard for Hakin9 magazine since 2008.

Securing the Cloud:

Is it a Paradigm Shift in Information Security?

First let me start by saying No. There's really nothing new in the Cloud except where risk appears to shift. But does it really?

What you will learn…

- The Basics of Cloud Computing
- Holes in the Cloud
- Hardening the Cloud

What you should know…

- Basic Networking
- Scanning for Vulnerabilities
- System Reconfiguration

I would argue that it increases your risk and there can be no shift of blame for a successful *Cloud* attack and breach of confidential data stored in the Cloud. You are ultimately responsible.

Everyone from IT security circles to Corporate Executives in business management are talking about the *Cloud* or *Cloud Computing*. First, does anyone know what the *Cloud* really is? How does it differ from the *Web* or the *Internet* and why is it so important? Once we have a grasp of what the Cloud is, then we can better understand why it is a Hacker Haven and a Malware Magnet.

With this understanding, we will be able to make intelligent judgments about whether this ecosystem is one in which we will shift portions of risk for our own organizations and how to ensure the risk is as minimal as possible.

Rapidly Defining the Cloud

You're in an elevator. Someone walks up to you and says *before I get off on the next floor, tell me, what is the Cloud?* Ok, with twenty seconds to spare, you should tell them that the Cloud is *the concept of offloading data storage, software applications and computing resources to one or more remote locations using various internet protocols*. Yes, I made this one up but it's true. Short, sweet and easy to remember.

The big problem with the Cloud is that you shift risk and lose control to gain flexibility, availability and the cost savings of shared, remote resources. This, of course, opens the doors wide open for hackers, cybercriminals and their malware. I'll give you some ideas on how to deal with this problem later in this article.

The Long Answer: A Formal Definition of Cloud computing

According to the National Institute of Standards and Technology (*NIST.gov*), Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model promotes availability and is composed of:

- Five essential characteristics,
- Three service models, and
- Four deployment models.

Essential Characteristics (see Figure 1):

1) *On-demand self-service*. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

2) *Broad network access*. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

3) *Resource pooling*. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

4) *Rapid elasticity*. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

5) *Measured Service*. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models (see Figure 2):

1) *Cloud Software as a Service* (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

2) *Cloud Platform as a Service* (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

3) *Cloud Infrastructure as a Service* (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems,

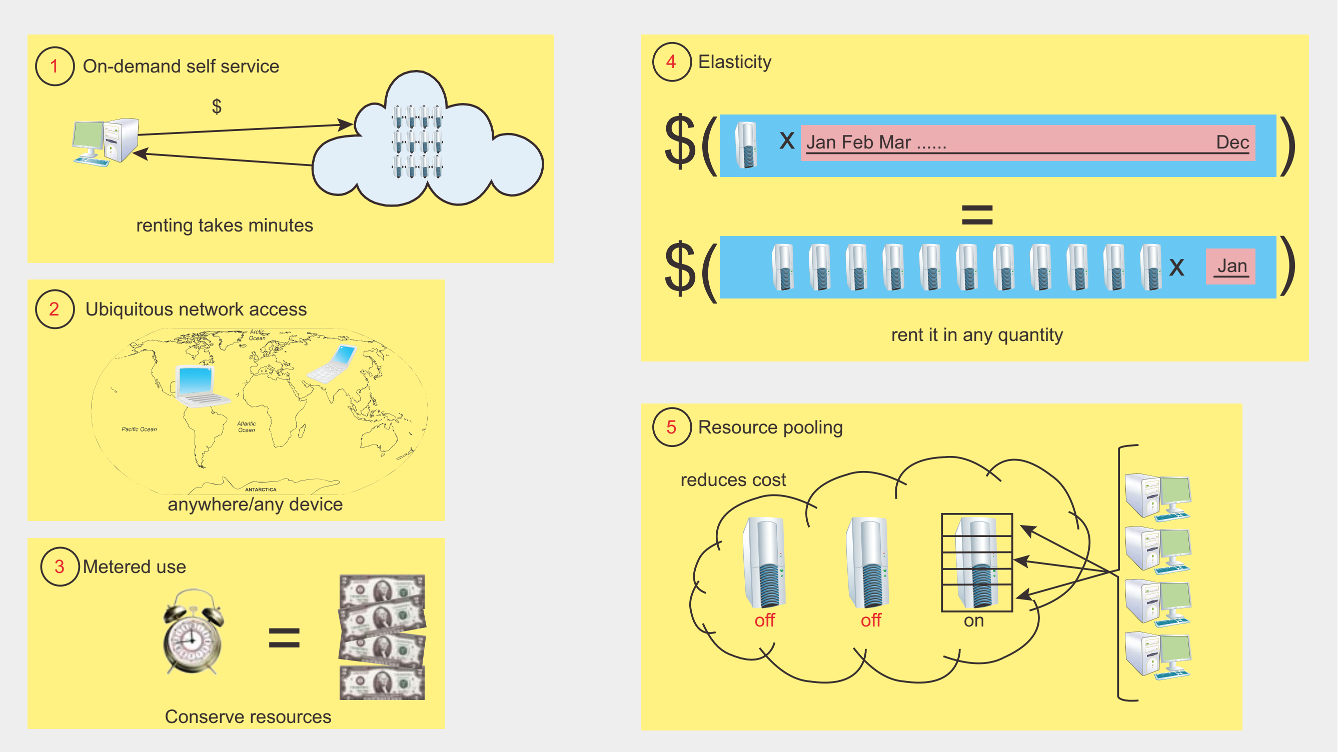


Figure 1. *Essential Characteristics of the Cloud (Source: NIST.gov)*

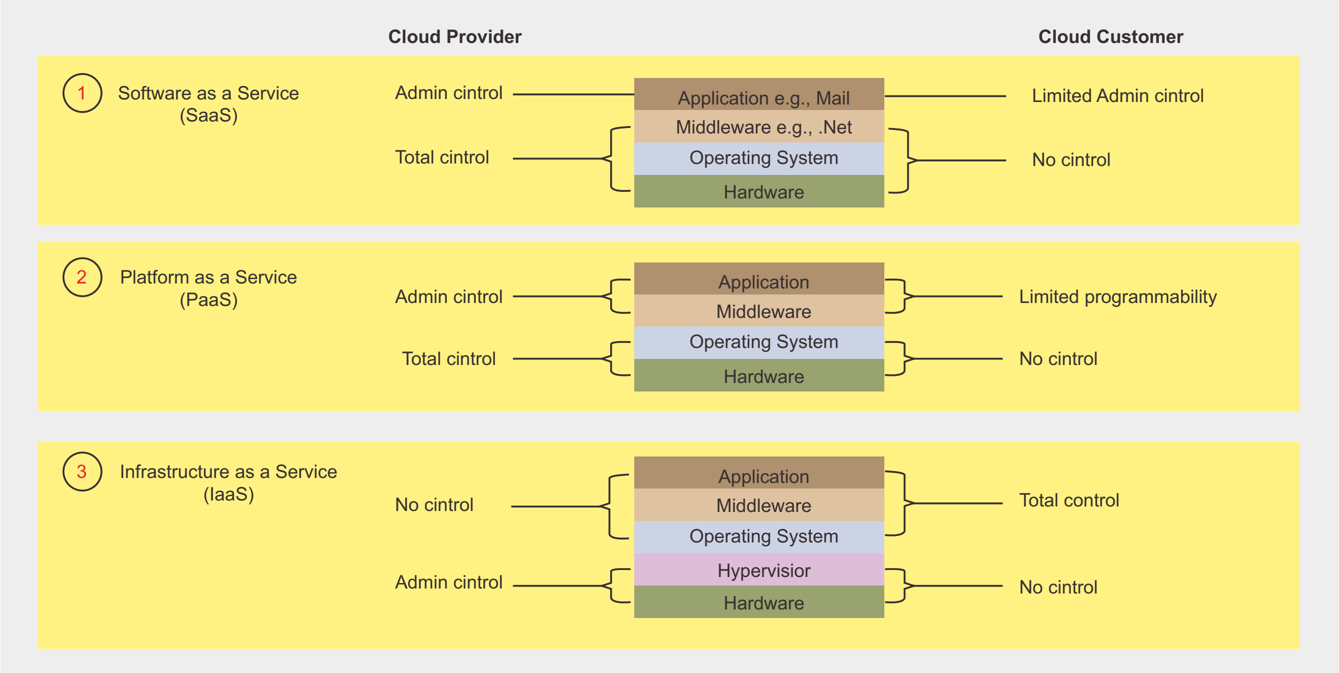


Figure 2. *Service Models of the Cloud (Source: NIST.gov)*

storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models (see Figure 3):

1) *Private cloud*. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

2) *Community cloud*. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

3) *Public cloud*. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

4) *Hybrid cloud*. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

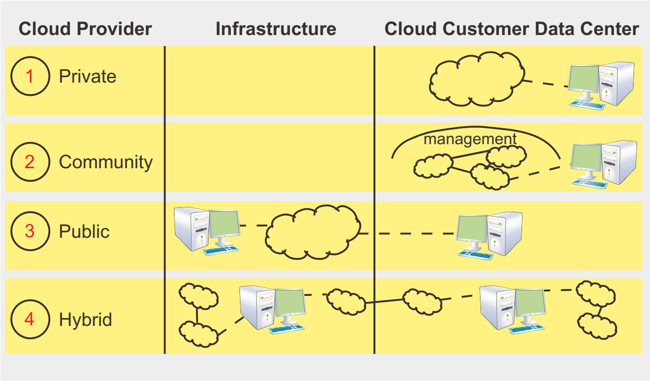


Figure 3. *Deployment Models of the Cloud (Source: NIST.gov)*

Cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

Key Areas of Security Concern

When shifting our risk from locally hosted and managed servers and services to the Cloud, we cannot forget the key areas of security concern for any IT manager or network security officer. Let us remember the CIA formula – *Confidentiality, Integrity and Availability*.

We must make sure that data is not exposed, exploited or leaked (breaching the Confidentiality rule), that the data is correct and attestable and has not been corrupted (breaching the Integrity rule) and finally, that the data is available when needed so that access is not disabled or we are not denied service (breaching the Availability rule).

In the Cloud, we lose local, physical control of the traditional CIA security model. The Cloud can be a dynamic, changing environment and we must have secure access to the Cloud, while the Cloud service provider must protect different users from each other, in the same way a VPN tunnel provides unique, confidential and secure access to various resources for trusted user access.

Therefore, the biggest security issues for the Cloud are very similar to those of VPN access to critical, confidential data:

- Trust
- Multi-tenancy
- Encryption
- Compliance

When becoming a Cloud consumer, there are also security advantages to consider:

- Reducing internal risk exposure to sensitive data because it's no longer in your data center, on your server, in your building, on your network – it's offsite and hosted elsewhere.
- Homogenous Clouds means security audits and vulnerability tests of these Clouds is easier – what works for one private Cloud service for one customer also works for another customer.
- Cloud computing enables automated security management. Auditing, Patch Management, Virus Scanning, Deep packet inspection can all be part of an automated security tools portfolio across the entire Cloud service operation.

In other words, if the Cloud security is strong, multiple users benefit from the common security practices, tools and countermeasures. You also gain the advantage of redundancy and disaster recovery requirements necessary to deploy a more secure and stable data warehouse.

However, one cannot simply assume that the Cloud is secure. Do you trust your Cloud vendor's security model and what are their best practices? Have they been audited? Can you review the results of the audit? How did they respond to audit findings? You will lose physical control over your applications, data, servers and services when you shift them to the Cloud. In addition, if the vendor you choose claims to have a proprietary solution – be it the application or an internal encryption or security methodology, how can you trust the security of their implementation?

Here are some examples of very well known commercial Cloud computing providers and their service offerings:

- Amazon Web Services (AWS), found at *http://aws.amazon.com*
- Google Cloud Services, found at *http://www.Google.com/Apps/Business*
- Microsoft Windows Azure Platform, found at *http://www.microsoft.com/windowsazure/*
- RackSpace, found at *http://www.rackspace cloud.com/*
- SalesForce, found at *http://www.salesforce.com/platform/*

There are so many others, I just don't have the time or room to list them in this article. If you need to find more, visit google and type in any service that is important to you and add the keyword *cloud* or *cloud computing*.

Hacking the Cloud

As many of you already know, Virtual Machines have become a target of hacker attacks and vulnerability exploitation. VMware will become a core component of many of the Cloud offerings. According to VMware, there are many benefits of using their virtual computing environment at the core of Cloud offerings: see Figure 4.

Accordingly, while VMware's vCloud initiative seems to bring to the industry a new platform for cloud computing that addresses the key inhibitors, allowing companies of all sizes to realize the benefits of enterprise-ready private computer clouds, it also opens the door to hackers, cybercriminals and malware.

The industry of the Cloud is hyped with new marketing messages for improved security about reliability, consolidation and isolation. No longer are we bound by hardware or the risk of hardware failure, nor do we need to purchase as much equipment because of the shared computing power of the Cloud and through task isolation, there is less risk to downtime. Right? Not at all. Wrong.

For years, there have been a growing number of VMware or *virtual computing* common vulnerabilities and exposures (see *http://cve.mitre.org* and *http://nvd.nist.gov* – at the time of this writing, over 300 known and exploitable vulnerabilities) or visit VMware directly at their own security advisories page, to see how serious a problem the Cloud is facing, with constant updates, patches and fixes for holes, located at *http://www.vmware.com/security/advisories/*.

Here's a sample security patch from Vmware: see Frame: VMware vCenter Update Manager fix for Jetty Web server addresses important security vulnerabilities.

Which is a reaction to a common vulnerability and exposure (a hole) in VMware: see Frame: Vulnerability Summary for CVE-2009-1523.

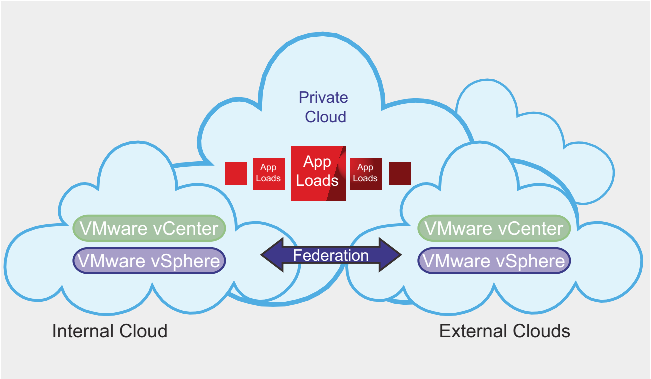


Figure 4. *VMWar's view of Cloud Computing (Source: VMware.com)*

VMSA-2010-0012

VMware vCenter Update Manager fix for Jetty Web server addresses important security vulnerabilities

```
-----------------------------------------------------------------------
              VMware Security Advisory
Advisory ID:     VMSA-2010-0012
Synopsis:        VMware vCenter Update Manager fix for Jetty Web
              server addresses important security vulnerabilities
Issue date:      2010-07-19
Updated on:      2010-07-19 (initial release of advisory)
CVE numbers:     CVE-2009-1523 CVE-2009-1524
-----------------------------------------------------------------------
1. Summary
  VMware vCenter Update Manager fix for Jetty Web server addresses
  important security vulnerabilities.
2. Relevant releases
  VMware vCenter Update Manager 1.0
  VMware vCenter Update Manager 4.0
  VMware vCenter Update Manager 4.1
3. Problem Description
 a. VMware vCenter Update Manager Jetty Web server vulnerabilities
  VMware vCenter Update Manager is an automated patch management
  solution for VMware ESX hosts and Microsoft virtual machines. Update
  Manager embeds the Jetty Web server which is a third party component.
  The default version of the Jetty Web server in Update Manager is
  version 6.1.6 for which the following relevant vulnerabilities are reported.
  A directory traversal vulnerability in Jetty allows for obtaining
  files from the system where Update Manager is installed by a remote,
  unauthenticated attacker. The attacker would need to be on the same
  network as the system where Update Manager is installed.
  A cross-site scripting vulnerability in Jetty allows for running
  JavaScript in the browser of the user who clicks a URL containing a
  malicious request to Update Manager. For an attack to be successful
  the attacker would need to lure the user into clicking the malicious URL.
  The Common Vulnerabilities and Exposures project (cve.mitre.org) has
  assigned the names CVE-2009-1523 and CVE-2009-1524 to these issues.
  VMware would like to thank Claudio Criscione of Secure Network for
  reporting these issues to us.
  Column 4 of the following table lists the action required to
  remediate the vulnerabilities in each release, if a solution is available.
  VMware         Product  Running  Replace with/
  Product        Version  on       Apply Patch
  ============== ======= ======= =================
  Update Manager    1.0  Windows  Update Manager fix for Jetty *
  Update Manager    4.0  Windows  Update Manager fix for Jetty *
  Update Manager    4.1  Windows  Update Manager fix for Jetty *
  * Refer to VMware Knowledge Base article 1023962
4. Solution
  Please review the patch/release notes for your product and version
  and verify the md5sum of your downloaded file.
  VMware vCenter Update Manager
  ----------------------------
  Update Manager fix for Jetty
  http://kb.vmware.com/kb/1023962
5. References
  CVE numbers
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1523
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1524
-----------------------------------------------------------------------
6. Change log
2010-07-19  VMSA-2010-0012
Initial security advisory after release of VMware vCenter Update Manager
security fix for the Jetty Web server on 2010-07-19.
```

The Epiphany: Hacking the Cloud is no different than hacking servers and services running over the internet!

Hackers and cybercriminals will choose to use exploits against common vulnerabilities and exposures to exploit the Cloud. The smarter ones will also use covert channels to bypass cloud security to pass data between multiple *isolated* cloud components so that hacking one might lead to hacking another and collecting data from one *isolated* resource to another.

More sophisticated hackers, for example, will simply use layer two traffic to setup shop for covert channels of communication over *private* and *isolated* members of the Cloud. For example, they could use the IPX communication protocol on Novell or EBTables on Linux (see: *http://ebtables.sourceforge.net/*) and you wouldn't even know it were happening. Once someone has found an exploitable hole and makes it into your Cloud, they will ultimately own the keys to the castle.

In addition, there are numerous networking issues once the Cloud has been attacked. They include the ability to bypass the host firewall – just look at VMware in bridging mode, promiscuous mode, MAC impersonation and IP spoofing. So, one of the biggest problems in Cloud computing is that the Cloud is being developed by software engineers who are isolated from daily attacks and therefore, not security professionals. The world is full of exploiters – cybercriminals and malware who have already figured out how to hack the Hypervisor – the core software for controlling the Cloud. Just follow this link to see how to do it: *http://tinyurl.com/hack-the-cloud*

Proactively Securing the Cloud

To ensure your Cloud is secure, make sure your service provider:

- Utilizes a risk-based information security model that fully addresses the risk formula;

```
R = T x V x A
(R)isk = (T)hreats x (V)ulnerabilities
       x (A)ssets
```

- Maintains and update a detailed set of security controls for risk mitigation;
- Documents a regulatory compliance framework for your industry (GLBA for banking, PCI for e-tail, retail, SOX for public companies, etc.), as compliance requirements extends to service providers.

If you or your Cloud vendors don't already have a well document information security model, there are numerous models to utilize from COBIT, found at *www.isaca.org/*, to the ISO/IEC27001:2005 framework, which can be found at *http://www.iso.org*

You should make no trust assumptions about any Cloud provider. Let's begin with the tools and techniques that are required to secure the Cloud:

Traditional Information Security Countermeasures

Firewalls, Anti-virus, Intrusion Detection Systems, Intrusion Prevention Systems, Multi-factor Authentication, Single-sign on and Tokens are a must for all Cloud services.

Auditing for Common Vulnerabilities and Exposures (CVE®s)

Regularly scheduled Audits of all Cloud touchpoints – from the routers to the managed switches – from the desktops of the IT management staff to the Servers – all network equipment must be audited for CVEs.

System Hardening – Removing CVEs

Most network security features are designed to limit outside access to the protected computing resources. Yet even with these security measures in place, computers are often still vulnerable to outside access. System hardening, also called Operating System hardening, helps minimize these security vulnerabilities. The purpose of system hardening is to eliminate security risks and reduce the chance that a trusted computing resource will be exploited by a malicious outsider or malware. This is done by removing all non-essential software programs and utilities from the Cloud computing server. Not only can you reconfigure a system to remove unnecessary services, you can also find those patches that work without opening new holes. By looking for and removing CVEs, you'll be able to document due care and due diligence for regulatory compliance. With frequently scheduled audits, IT staff can begin to understand where their holes exist, and then they can remove these holes.

If you are going to trust a Cloud vendor, make sure they provide documented evidence of monthly CVE® audits and system hardening. The NSA offers free *Security Technical Implementation Guides* (also known as STIGs) for system hardening. They can be found here: *http://iase.disa.mil/stigs/stig/index.html*. There are also many projects in the Open Source community for system hardening including deploying hardened Linux.

Host-based Intrusion Prevention Systems (HIPS)

Because there are so many holes or CVEs in virtual machine deployments as well as the underlying root operating systems, it is very important that the servers which are being used to host your Cloud service are not only hardened but are running some form of real-time protection against remote exploiters or malicious insiders. A Host-based Intrusion Prevention (HIPS) is usually deployed as an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based, and stateful protocol analysis.

Signature-based Detection: This method of detection utilizes signatures, which are attack patterns that are preconfigured and predetermined. A signature-based intrusion prevention system monitors the network traffic for matches to these signatures. Once a match is found the intrusion prevention system takes the appropriate

Vulnerability Summary for CVE-2009-1523

Original release date:05/05/2009
Last revised:06/10/2009
Source: US-CERT/NIST
Overview
Directory traversal vulnerability in the HTTP server in Mort Bay Jetty 5.1.14, 6.x before 6.1.17, and 7.x through 7.0.0.M2 allows remote attackers to access arbitrary files via directory traversal sequences in the URI.
Impact
CVSS Severity (version 2.0):
CVSS v2 Base Score:7.1 (HIGH) (AV:N/AC:M/Au:N/C:C/I:N/A:N) (legend)
Impact Subscore: 6.9
Exploitability Subscore: 8.6
CVSS Version 2 Metrics:
Access Vector: Network exploitable
Access Complexity: Medium
Authentication: Not required to exploit
Impact Type:Allows unauthorized disclosure of information
References to Advisories, Solutions, and Tools
By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.
US-CERT Vulnerability Note: VU#402580
Name: VU#402580
Hyperlink: http://www.kb.cert.org/vuls/id/402580

action. Signatures can be exploit-based or vulnerability-based. Exploit-based signatures analyze patterns appearing in exploits being protected against, while vulnerability-based signatures analyze vulnerabilities in a program, its execution, and conditions needed to exploit said vulnerability.

Statistical Anomaly-based Detection: This method of detection baselines performance of average network traffic conditions. After a baseline is created, the system intermittently samples network traffic, using statistical analysis to compare the sample to the set baseline. If the activity is outside the baseline parameters, the intrusion prevention system takes the appropriate action.

Stateful Protocol Analysis Detection: This method indentifies deviations of protocol states by comparing observed events with *predetermined profiles of generally accepted definitions of benign activity* (source: *Wikipedia.org*).

The best HIPs solutions are minimally invasive software that monitor ports, protocols, memory, applications and network traffic for anomalous behavior. Heuristic analysis for anomalies as well as stateful packet inspection combined with signature testing is a powerful combination. Look for a HIPS solution that has some form of central control and reporting.

Ask your Cloud service provider what HIPS solution they are using and if they have logging and audit results they can roll up to you on a regular basis to ensure Cloud systems integrity.

Who has Access to the Cloud?

You'll need to ask your Cloud vendor if they have deployed *Physical Access Control* (PAC) and *Network Access Control* (NAC) for their entire Cloud service offering. In physical security, the term access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. *Physical Access Control* is always about *who*, *where*, and *when*. *Network Access Control* is a virtual equivalent of PAC. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Although historically, this was partially accomplished through keys and locks, these systems did not allow restriction of the key holder to specific times or dates. By making sure your Cloud service provider uses an electronic PAC system, credentialed, scheduled access can be better managed and most importantly for compliance, logged. You'll want to know these logs are accessible and auditable, especially forensically, if ever a breach of Confidentiality, Availability or Integrity occurs. Combine this with NAC to control access to the actual services and networking equipment that makes up your Cloud with policies and posture checks and you'll have a much more secure and trustworthy computing environment where you've shifted so much of the risk.

Normally, if someone loses your trust, you'll take away their privileges. When the Cloud is so far away from you, it's harder to know if trustworthy individuals have access to your Cloud resources, are managing these for you and are watching transactions. How hard would it be for a criminal to gain access to your confidential data and cause you to be out of compliance with a regulation that relates to data protection, when the criminal is an employee of your Cloud service provider?

Data Protection in the Cloud

Not only must a Cloud provider deploy constantly updated Information Security Countermeasures, they also should be protecting your data in the Cloud.

This includes Encryption, Backup/Restore services, Database integrity testing as well as a *Business Continuity* and *Disaster Recovery Plan* (BCP/DRP).

Remember, there are numerous free tools out there and open sources in the encryption space – so you can ask your Cloud service provider if they will use an industry standard such as X.509 certifications and *Secure Sockets Layer* (SSL) or *Secure Shell* (SSH) along with encryption algorithms that are well know and well tested for how difficult they are to break and how long it might take a hacker or cybercriminal, in the event they obtained a copy of your encrypted data. One example is the *Advanced Encryption Standard* (AES). This is a symmetric-key encryption standard adopted by the U.S. government. The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. The AES ciphers have been analyzed extensively and are now used worldwide, as was the case with its predecessor, the *Data Encryption Standard* (DES). You can learn even more about open source encryption by visiting *http://www.truecrypt.org* and *http://www.openssl.org*, two of my favorite sites with open sources to try and rich in-depth information on this topic.

As to Backup/Restore services, if your Cloud service provider uses something internal, they should tell you what it is – maybe it's home grown, maybe it's an industry standard from EMC or Veritas – they may even offload this to yet another Cloud service provider – adding yet another layer of depth.

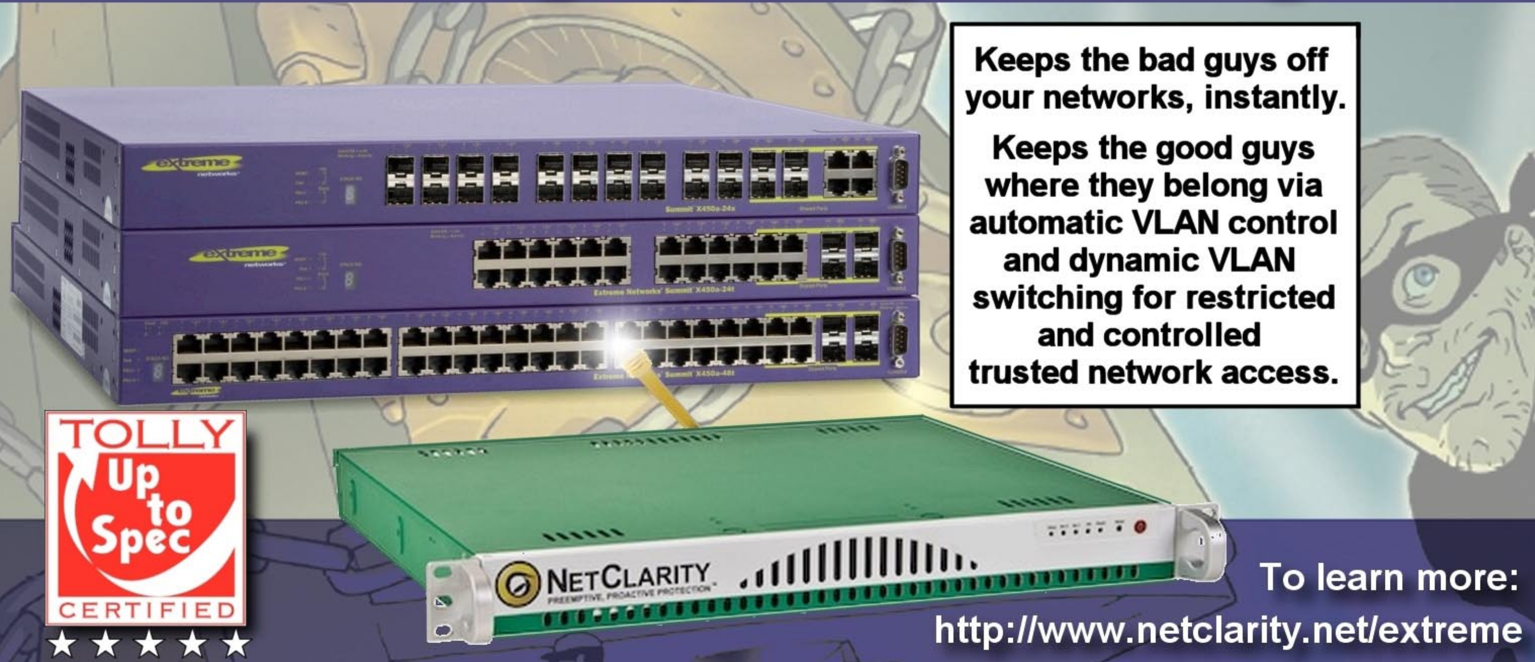
Summary: Securing the Cloud is like Securing Your Own Data Center

In summary, securing the cloud is not much different than securing your own virtual machines and local servers all housed within your own data center. The problem is that you also need to be aware of the fact that you've given all control at mitigating risk to someone else who is far away, maybe in another state or worse yet – another country. Does this shift the blame away from you, if there is a successful breach of confidentiality, availability or integrity and a loss of *personally identifiable information* (PII) or mission critical data? No. In fact, it puts the spotlight on you.

The Cloud has many benefits but like all paradigm shifts, it opens up new doors and new possibilities for both increased rewards and risks. Create and agree upon strong security policies – audit frequently, harden your Cloud service offering, control access and document compliance. By doing so, you will preemptively, proactively stay one step ahead of the hackers, cybercriminals and next wave of malware attacks. Securing the Cloud is not easy, so ask the tough questions before you shift your risk. It's up to you to document the proper steps at securing the Cloud and complying with regulations, no matter who you trust. The Cloud provider is an extension of your own IT service offerings to your own organization, so do not hand over the keys to the castle without knowing who you've given them to and how they will guard your crown jewels.

GARY S. MILIEFSKY, FMDHS, CISSP®

Gary S. Miliefsky is a regular contributor to Hakin9 Magazine. He is the founder and Chief Technology Officer (CTO) of NetClarity, Inc, where he can be found at http://www.netclarity.net. He is a 20+ year information security veteran and computer scientist. He is a member of ISC2.org, CISSP® and Advisory Board of the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. Miliefsky is a Founding Member of the US Department of Homeland Security (http://www.DHS.gov), serves on the advisory board of MITRE on the CVE Program (http://CVE.mitre.org) and is a founding Board member of the National Information Security Group (http://www.NAISG.org).



Radio Frequency-enabled Identity Theft

A discussion on how radio frequency-enabled technology could leave people vulnerable to identity theft and then potential identity fraud.

Identity theft and identity fraud is a growing business. The crime itself is very much still in its infancy in most countries in the world with the exception of the US, where it continues to be a major problem for both the general population and the authorities.

So you will not be surprised to hear that from the US comes yet another type of identity theft called *non-contact identity theft* or what is sometimes referred to as *Wireless identity theft*.

Wireless identity theft is a relatively new type of identity theft that uses radio frequency to gather important personal information from someone's store, access control, credit, debit, passports or identity cards. One particular type of wireless identity theft involves *Radio-frequency identification* or *RFID*.

Radio-frequency Identification

RFID is an object (or TAG) that is incorporated into say a passport or debit/credit card that sends out radio waves for identification and tracking. Most RFID tags can only been read from several meters away – most can also be read from beyond the line of sight of the reader as well.

The RFID tag contains two elements. The first element (circuit) is used for storing and processing information and the other is an antenna for receiving and transmitting the signal.

RFID Tags

RFID tags come in three distinct types. The first type contains a small battery that can transmit signals autonomously; the second type is called passive RFID tags – these have no batter and need an external device to activate a signal handshake. The third type is a battery assisted passive RFID which requires an external device to activate (wake up). The last type has a greater range.

FACT

RFID active tags have been used on more than a million shipping containers that travel outside of the United States. (US Department of Defense) – 2007

RFID technology is developing rapidly, however there are some obvious engineering limitations. RFID technology is miniaturizing as the technology advances, but the advances appear to be currently limited to the radio frequencies available. The antennas themselves are difficult to attach, which in turn limits the reading range. There are new developments in this area which look to overcome these technical difficulties most notably photovoltaic components, but this is some way off.

RFID Technology Use

RFID technology use is without doubt on the increase within industry, in particular the financial industry – where it is used in debit and credit cards. There are several good reasons why business is looking at this technology. One of which is decreased cost of the RFID devices and tags, increased performance and a stable international standard. A number of industries are looking to RFID technology for asset tracking. It is this last point of *tracking* that provokes widespread alarm bells in privacy circles.

With RFID becoming more and more prevalent in everyday life, most people will be unaware of the impact that this technology has on their lives. One particular RFID technology use is with *Biometric Passports*. Most citizens of a country will have one, especially if they want to travel. The Passport is one of the most important *identities* an individual can ever have.

Biometric Passports

The biometric passport is simply a paper document that contains biometric electronic information that can be used to identify travellers. All biometric passports use contactless smart card technology (which uses a computer chip – see Figure 1) and antenna for both computer chip power and hand shaking with a device.

The computer chip (can be seen at the bottom right on the Passport image above) contains exactly the same personal information that is found on the same page as the individual's personal information. Table 1 is an example of the data stored on a UK Biometric Passport.

All biometric passports use a PKI to authenticate the personal data stored on the passport smart card. Authorities claim that the PKI used cannot be broken. The biometrics used for identification includes facial, fingerprint and iris recognition. Each computer chip stores a JPEG or JPEG2000 format image of one of the above identification options. Every time you cross borders a biometric comparison is performed by e-border systems.

Biometric Passport Security Issues

The biometric passport has been designed to have non-traceable computer chip characteristics as well as a number of preventative technologies including *Passive Authentication* (PA) and *Active Authentication* (AA) just to name a few. The real issue with PA is that not all border systems appear to check the cryptographic signature on a passport computer chip. AA also appears to have problems with security, mainly concerning a hacker's ability to alter the anti-cloning mechanism functionality. By altering this functionality it would be possibly to be in two places at once.

In March of this year a security expert in the UK claimed to siphon data off an RFID chip from a passport in a sealed envelope, but the UK Home Office maintains that even if a biometric passport is cloned, airport scanners will pick up a fake chip. However, some experts claim that although British airport scanners have the technology to identify chips which are not genuine, those in other countries do not.

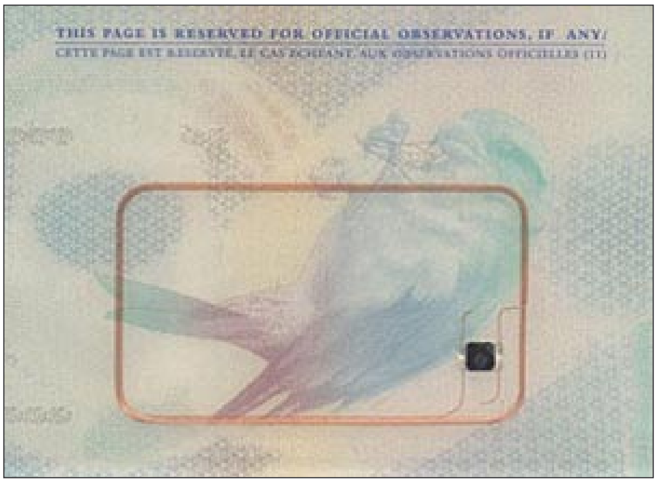

THIS PAGE IS RESERVED FOR OFFICIAL OBSERVATIONS, IF ANY/
CETTE PAGE EST RESERVEE, LE CAS ECHEANT, AUX OBSERVATIONS OFFICIELLES (11)

Figure 1. *Example: UK Biometric Passport with computer chip*

Non-contact Technology

One of the main concerns with non-contact technology is the ability to have your information swiped from your passport or card without you ever knowing. The same problems exist with Bluetooth technology but the Bluetooth security issue has been handled by offering a *passkey*. The Passkey is an encrypted password – normally four digits which allow the user to accept or deny a communication with another Bluetooth enabled device. Unfortunately, this process is likely to never appear on passports or credit or debit cards.

The RF enabled Cards Threat

RF enabled cards (whether they be store, debit or credit cards) allow organisations and retail outlets for example to learn more about their customers. They provide valuable personal data as well as collect profile data on customer behaviour both from what an individual purchases to tracking their every movement.

The RFI chip responds to certain radio frequencies. When an individual's tag comes into contact with these radio frequencies there is a handshake and the data is parsed. There is an opportunity here to harvest the sensitive data in which a hacker or identity thief could program their own cards using already well documented cloning techniques. Websites can easily be found which supply the necessary tools and software to commit *non-contact identity theft*.

RFID Applications

The financial industry has been very active in the RFID market. In the US, most of the debit and credit card providers are migrating away from swipe cards – mainly due to the time it takes to complete a transaction – to the more speedy RFID tagged transaction process. The RFID issuing organisations dispute the RFID identity theft threat. So why have some cards had individuals names and other data removed by some credit card companies? Various white-hat hackers believe RFID is not safe and have produced reports to prove it.

Credit and Debit Card RFID Technology

In the US millions of contactless credit cards have been received – in fact some 250 million Americans have RFID technology. The RFID technology associated with credit and debit cards can never be switched off. The idea behind the RFID is that you don't have to hand over your card. All you do is, wave your card in front of a scanner and that's that. A particularly good method of protecting your RFID privacy is to purchase RFID-blocking sleeves for your contactless cards or use just aluminium foil to block the radio waves.

The continuing RFID threat may well be a problem especially given the cyber security issues that we read about concerning stolen financial records and identity theft. Admittedly there has been no identity theft or cyber crime committed using RFID – not just yet. Most of the threats have been developed in controlled environments using proof-of-concept which demonstrates the supposed RFID vulnerabilities. There does appear a concerted effort to provide high level encryption to RFID contactless technology – but the real question of *has anyone had their data or identity stolen yet*? is something that might happen in the future. Why discount it?

The Malware and DDoS Threat

Consider the number of malware (computer worms and viruses) that are being constantly developed in the online world. Some attempt to steal your personal and financial data; others serve no purpose other than to destroy your PC or data. When computers first appeared it took years for the first virus to appear. If you were to put the clock back – one wonders what foresight would have given us – it wouldn't have given us one of the biggest industries in the world – internet security!

RFID Car Immobilizers

Ever wondered how your car automobile immobilizers work? Well, the car key uses RFID. The immobilizer has a chip in the key which is encrypted which sends an RF wave to the car to open or lock the car including the immobilizer.. As yet there is no real purpose for hacking into a car but given the amount of computer technology that is being built into cars – one day hackers will have a reason to crack into a car (using Bluetooth, RFID or Satellite) maybe to stop your car from working (similar to a DDoS attack).

You can actually purchase a $50 kit from the internet that will read 125-Khz RFID chips. The kit includes; open source software for reading, storing and re-transmitting card data and decoding software. The decoding software decodes the RFID encryption used in car keys for several car models. This would allow a hacker to scan an unsuspecting car-owners' key, decrypt and the data and open the car.

Mitigating the RFID Security Risk

The real security risk for RFID is mainly the opportunity to steal the data as to date no one hacker has admitted to being able to hack an RFID system or crack an RFID card. For individual users of RFID, solid tag and system data security should actually address the privacy concerns while at the same time allowing for greater efficiency and enhanced security. If you want to understand more about RFID technology and the obvious threats, then you only need to visit the *Communications of the Association Machinery* (CAM). Have a read of this

Table 1. *Example of the data stored on a UK Biometric Passport*

Passport Type	Date of Birth
Country Code	Sex type
Passport Number	Place of Birth
Surname	Valid from to dates
First and middle names	Country of Authority
Nationality	Signature

> For successful data retrieval the perpetrator's antenna must catch two different interactions: the forward channel, which is the signal being sent from the RFID reader to the RFID token; and the backward channel, which is the data being sent back from the RFID token to the RFID reader. . . .
>
> . . . the perpetrator would need only an antenna and an amplifier to boost the signal capture, a radio-frequency mixer and filter, and a computer to store the data. The amplifier itself would not even need to be that powerful, since it would need to boost the signal over only a short distance of three to five meters. . . . These RFID "sniffers" can then be plugged into a laptop via a USB port.

The 52-bit encryption key can be easily broken, so one can only be baffled as to why the CAM has made the above statement. Some experts are perplexed as to why 3D barcodes are not used as they can safely store data which is hard to crack.

Last year at DefCon NSA intelligence officers were gathering – what they didn't know what that an RFID scanner was searching for them also using a wireless Bluetooth webcam, which also took their picture. The RFID reader sniffed data from their RFID-enabled ID cards and other documents they were carrying in their backpacks and pockets. Obviously no crime was committed. The project was only to raise awareness.

The Department of Commerce's *National Institute of Standards and Technology* (NIST) in the US is leading the way on RFID security. It understands the risks and has highlighted specific recommendations. Its list of recommended practices for ensuring the security and privacy of RFID systems includes:

- firewalls that separate RFID databases from an organization's other databases and information technology (IT) systems;
- encryption of radio signals when feasible;
- authentication of approved users of RFID systems;
- shielding RFID tags or tag reading areas with metal screens or films to prevent unauthorized access;
- audit procedures, logging and time stamping to help in detecting security breaches; and
- tag disposal and recycling procedures that permanently disable or destroy sensitive data.

NIST will no doubt play a significant role in determining RFID standards for organisations and manufacturers from now and into the future.

Government and Business RFID Strategies

As yet there doesn't appear to be any plans from government or businesses to develop strategies that allow for the future threat that RFID might impose on individuals and organisations. A thorough examination of the threats would be required (see below). This would have to look at existing and new potential threat approaches, malware trends, the value of the data held on RFID cards and how the threats are to be mitigated.

Government and businesses will need to consider both the Privacy and Forging elements. Therefore we can divide RFID security threats into two distinct elements:

Element 1: Privacy

Inventorying – collecting tag data with a suspicious reader

Tracking – Illicit tracking using a tag's serial number

Element 2: Forging

Cloning – Physical replication of an existing tag to introduce to the system

Simulation – Tampering with an RFID system using simulation devices

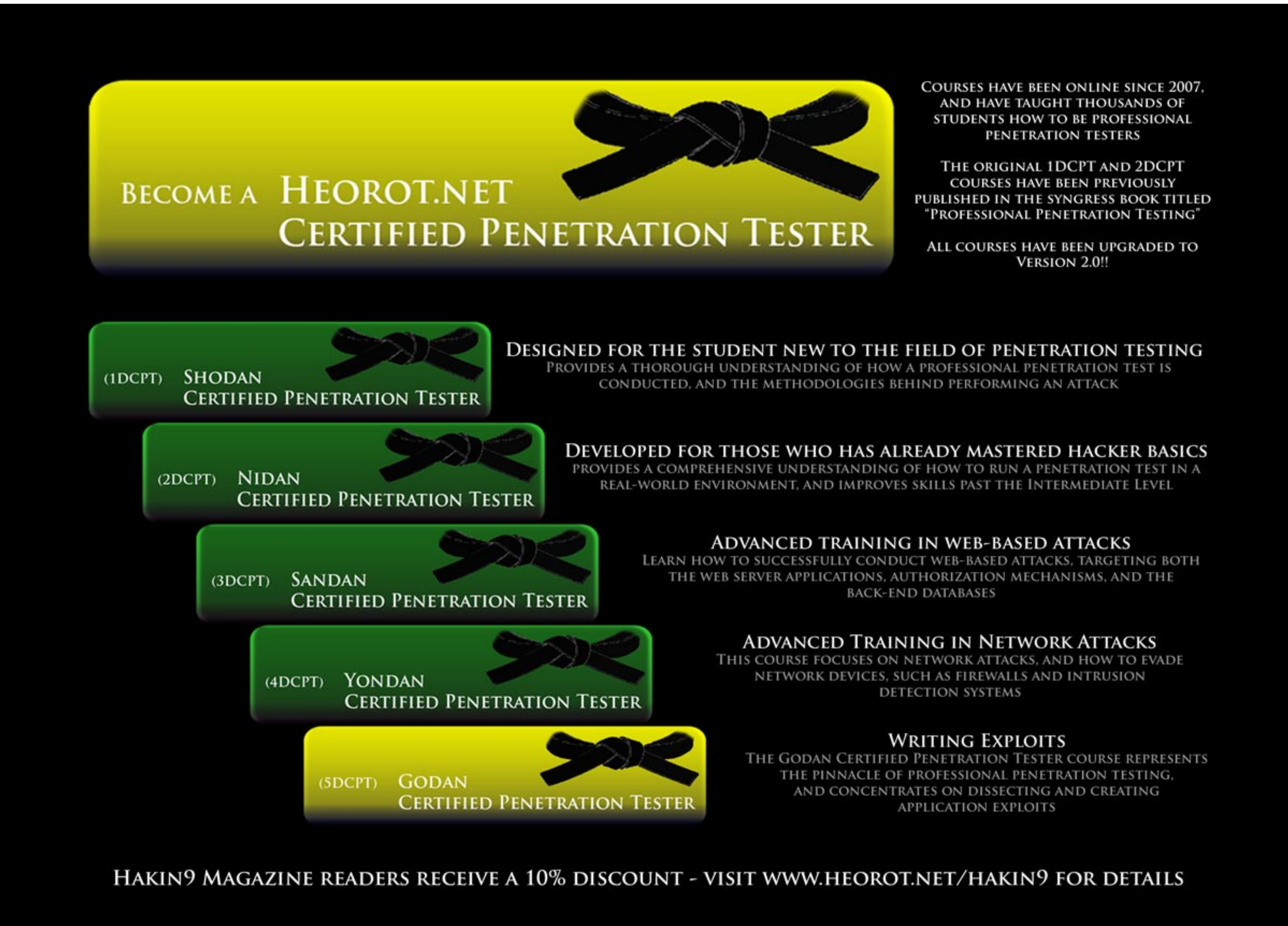
(c) S.Nair, O. Al Ibrahim

Final Thoughts

The technology for analyzing, hacking and cloning RFID tags will only improve over time. The mass production machinery behind the tags cannot keep up with the security threats. This is the same story in the PC world whereby malware is always one step ahead. Will we ever learn from our history? One doubts it. It's only a matter of time before someone or a cybercrime gang finds a method that steals both the personal and business data from the many material objects that will in the future use RFID.

JULIAN EVANS

Julian Evans is an internet security entrepreneur and Managing Director of education and awareness company ID Theft Protect (IDTP). IDTP leads the way in providing identity protection solutions to consumers and also works with large corporate companies on business strategy within the sector on a worldwide basis. Julian is a leading global information security and identity fraud expert who is referenced by many leading industry publications.



Intelligence Monopolies

In general a monopoly is bad for an industry. Prices invariably increase beyond reasonable production costs and innovation stops. It's a natural law that competition brings about new advances and achievement.

Intelligence is of course an industry that relies on innovation. New ideas, new sources, new methods, and new tools are not only useful to the industry but required for it to function. The targets of intelligence gathering will quickly learn how they are being surveilled and find ways to evade. A simple example of this is guerilla and terrorist militias learning that if they went into their tents or caves when the surveillance satellites were overhead the very expensive and sophisticated tools being used against them were much less effective. And a break from the desert sun probably wasn't a bad thing either!

The same tactics that are used in traditional military and diplomatic surveillance apply to us in the computer crime and security world. The bad guys know we are watching, and they know what we are watching for. Guess what they are going to do? They are going to adapt and evade what we're doing today. We must continue to adapt and evolve our tactics and tools or we will become ineffective overnight.

I am an IPS rule writer by trade and by passion. So I'm always looking for better ways to find the intelligence I write rules about. In rule writing we are essentially creating a body of intelligence. I run Emerging Threats which is an open source IPS ruleset. What we strive to do is describe all of the malware, CnC channels, attacks, exploits and general badness that we know of or have learned about over time. These threats change day to day and hour by hour so we have to continue to evolve and expand. If we don't keep ahead of the bad guys they take the advantage quickly.

A disadvantage we have in this regard is that we publish our body of intelligence immediately for the world to see. Of course this is an advantage in that we have thousands of researchers perfecting and contributing to that intelligence. But the bad guys know exactly when they've been busted and figured out, and have a pretty clear clue as to what to change to evade. Its a problem yes, but the advantage of the open community far outweighs the disclosure.

So with that being said, it was pointed out to me by a very smart guy at a recent conference that we all live under intelligence monopolies. The Emerging Threats ruleset is a slight exception because it can be used on any platform, but it's still Snort focused primarily. For the majority of us though, we buy an appliance to protect our networks and organizations. We spend massive amounts of money buying and deploying sensors and correlation engines. We make a very careful choice as to who will manage and handle these devices, and who will respond to the incidents they bring to our attention. We shop appliances, vendors, speeds, taps, failover gear, but we never shop for rulesets. We don't make our vendors disclose how they gather intel, and what they will be feeding us.

I would argue that the ruleset, or the body of intelligence, is absolutely the most critical piece of what we are purchasing and deploying, yet you would be hard pressed to find a salesman from any of the vendors that can tell you much about their ruleset, intel methods, or coverage specifics. Nor could you find someone able to give you a good comparison of the strengths and weaknesses of their ruleset verses the competition.

Why is this? We are not making the vendors do it. We live under a monopoly and we seem to like it. You buy Vendor X and you just have to accept their ruleset because that is all their warranty or support will cover. And you will likely not find a vendor selling intelligence or rules for a competitor's appliance.

So here we are. We live under intelligence monopolies. What does this do for us? We don't get the wide ranging coverage we require. We don't see resource intensive innovations. And I'll be honest, we've done the same thing at Emerging Threats. For years we've been happy to be a complementary ruleset to the VRT or open source Snort rulesets, or imported as a set of add-ons to the commercial appliances running other rules. We've tried to be innovative in what we do, but we haven't had any competition. We weren't competing. We were happy to just coexist.

Well folks, them days are over. With the recent launch of Suricata, the next generation IPS engine from the OISF (*http://openinfosecfoundation.org*) we are officially stepping up to compete. Emerging Threats is stepping up to the plate to provide an intelligence ruleset for many platforms.

This isn't going to be your grandma's ruleset. It is not going to be like your appliance vendors ruleset. This one will innovate. This one will compete. This one will bring you the new threats on an hour by hour basis, day in and day out.

We are launching the ruleset in September of this year. Check out *http://emergingthreatspro.com* for more information very soon. We're blending the best of the open intelligence model, the community, professional research, and extensive malware collection and analysis capabilities. We're harnessing the historical research capabilities of Telus, the folks that have supplied all of your vendors with their intel for years now.

We are also publishing on many platforms in many versions. We are supporting Snort and Suricata immediately, and moving to other formats and tools. One set of research, published to many formats. We are going to compete, and we are going to make your vendors try to keep up.

This isn't going to displace or take advantage of the open Emerging Threats ruleset. All of the innovations we make in the professional ruleset will reflect in the rules at are distributed to and from the community. This is going to improve the open ruleset immensely.

For more information about Suricata hit the Open Information Security Foundation's website, *http://openinfosecfoundation.org*. And watch *http://emergingthreatspro.com* for the launch of your new intel feed.

MATTHEW JONKMAN

Matt is the founder of emergingthreats.net, the only open and community based intrusion detection ruleset, and is also president of the Open Information Security Foundation (OISF). The OISF is building Suricata, an next generation ids funded by the US department of homeland security.

Capturing the New Frontier:

How To Unlock the Power of Cloud Computing

So here's a question: Which IT sector accounts for fully 25% of the industry's year-over-year growth and, if the same growth trajectories continue, will generate about one-third of the IT industry's net new growth by 2013?

The answer is Cloud Services, according to research firm IDC (Worldwide IT Cloud Services Spending, 2008-2012, IDC, October 2008). Cloud computing is garnering its fair share of industry buzz as well. Its promise of revolutionary cost savings and agile, just-in-time capacity has driven IT organizations at enterprises of all sizes to build cloud deployment strategies into their plans.

The Benefits of the Cloud

Cloud computing is immensely popular with companies and government agencies in search of revolutionary cost savings and operational flexibility. According to industry research firm IDC, cloud computing's growth trajectory is, at 27% CAGR, more than five times the growth rate of the traditional, on-premise IT delivery/consumption model (Worldwide IT Cloud Services Spending, 2008-2012, IDC, October 2008). Cloud computing practitioners cite numerous benefits, but most often point to two fundamental benefits:

Adaptability

An enterprise can get computing resources implemented in record time, for a fraction of the cost of an on-premise solution, and then shut them off just as easily. IT departments are free to scale capacity up and down as usage demands at will, with no up-front network, hardware or storage investment required. Users can access information wherever they are, rather than having to remain at their desks.

Cost Reduction

Cloud computing follows a model in which service costs are based on consumption and make use of highly shared infrastructure. Companies pay for only what they use and providers can spread their costs across multiple customers. In addition to deferring additional infrastructure investment, IT can scale its budget spend up and down just as flexibly. This leads to an order of magnitude cost savings that wasn't possible with 100% proprietary infrastructure.

Other benefits of the cloud include collaboration, scaling and availability, but revolutionary cost savings and the almost *instant gratification* offered by the agility of the cloud will be the key contributors to adoption of the cloud.

What is the Cloud?

So much has been written, advertised and discussed about cloud computing, it is appropriate to define the term for common understanding. Cloud computing generally describes a method to supplement, consume and deliver IT services over the Internet. Web-based network resources, software and data services are shared under multi-tenancy and provided on-demand to customers. It is this central tenet of sharing – and the standardization it implies – that is the enabler of cloud computing's core benefits. Cloud computing providers can amortize their costs across many clients and pass these savings on to them. This paradigm shift in computing infrastructure was a logical byproduct and consequence of the ease-of-access to remote and virtual computing sites provided by the Internet. The U.S. *National Institute of Standards & Technology* (NIST) defines four cloud deployment models:

- *Private Cloud*, wherein the cloud infrastructure is owned or leased by a single organization and is operated solely for that organization
- *Community Cloud*, wherein the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns, including security requirements
- *Public Cloud*, wherein the cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group
- *Hybrid Cloud*, wherein the cloud infrastructure is a composition of two or more cloud models that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability

NIST's definition of cloud computing not only defines HOW infrastructure is shared, but also outlines WHAT will be shared. These service models shift the burden of security accordingly between provider and user:

Software-as-a-Service

Software-as-a-Service, or *SaaS*, is the most mature of the cloud services. SaaS offers a *soup to nuts* environment for consumption of a common application on demand via a browser. Typically, the customer controls little or nothing to do with the application, or anything else for that matter, and is only allowed to configure user settings. Security is completely controlled by the vendor. Examples of providers include Salesforce.com, Workday, Mint.com and hundreds of other vendors.

Platform-as-a-Service

Platform-as-a-Service, or *PaaS*, is an emerging cloud service model. The customer is able to develop applications and deploy onto the cloud infrastructure using programming languages and tools supported by the cloud service provider. They are not able to control the actual infrastructure – such as network, OS, servers or storage – the platform itself. Because the customer controls application hosting configurations as well as development, responsibility for software security shifts largely to their hands. Examples include Google App Engine and Amazon Web Services.

Infrastructure-as-a-Service

Infrastructure-as-a-Service, or *IaaS*, is where even more of the infrastructure is exposed to multi-tenant users. The cloud service provider provisions processing, storage, networks and other fundamental computing resources. The customer is able to deploy and run arbitrary software, which can include operating systems and deployed applications. Software security in this deployment model is completely in the customer's hands, including such components as firewalls. Examples include Amazon Elastic Compute Cloud and Rackspace Cloud.

While SaaS gained popularity as an alternative to on-premise software licensing, the models that are driving much of the current interest in cloud computing are the PaaS and IaaS models. Enterprises are especially drawn to the alternative development infrastructure and data center strategies that PaaS and IaaS offer. At this point in time, smaller enterprises seem to have more traction with PaaS, enabling them to rapidly bring websites to market; whereas larger enterprises are more comfortable beginning their cloud deployments with an existing application moved to an IaaS cloud service.

How do we fully realize the benefits of the Cloud?

Realizing the cloud's benefits is greatly determined by the *trustworthiness* of the cloud infrastructure – in particular the software applications that control private data and automate critical processes. Cyber-threats increasingly target these applications, leaving IT organizations forced to sub-optimize the cloud deployments containing this software, limiting flexibility and cost savings. Assuring the inherent security of software, therefore, is a key factor to unlock the power of cloud computing and realize its ultimate flexibility and cost benefits.

Recommended approaches to Cloud software Security

According to the Cloud Security Alliance, a not-for-profit organization promoting security assurance best practices in cloud computing, the ultimate approach to software security in this unique environment must be both tactical and strategic. Some of their detailed recommendations include the following:

- Pay attention to application security architecture, tracking dynamic dependencies to the level of discrete third party service providers and making modifications as necessary
- Use a *software development life cycle* (SDLC) model that integrates the particular challenges of a cloud computing deployment environment throughout its processes
- Understand the ownership of tools and services such as software testing, including the ramifications of who provides, owns, operates, and assumes responsibility
- Track new and emerging vulnerabilities, both with web applications as well as machine-to-machine *Service Oriented Architecture* (SOA) which is increasingly cloud-based

The key to achieving the benefits of the cloud and to putting the above recommendations into practice is *Software Security Assurance*, or *SSA*. Recognized by leading authorities such as CERT and NIST, SSA is is a risk-managed approach to improving the inherent security of software, from the inside. There are three steps to a successful SSA program:

- Find and fix vulnerabilities in existing applications before they are moved into a cloud environment
- Audit new code/applications for resiliency in the target cloud environment
- Establish a remediation/feedback loop with software developers and outside vendors to deal with on-going issues and remediation.

To realize the full benefits of cloud computing, organizations must assess and mitigate the risk posed by application vulnerabilities deployed in the cloud with equal vigor as those within their own data center. It is only then that they will be able to take full advantage of Cloud Computing to save cost and increase the efficiency of their business.

MIKE ARMISTEAD

Mike Armistead, VP Corporate Development, Fortify Software (http://www.fortify.com/)

SMASH THE STACK WARGAMING NETWORK

smashthestack.org

smpCTF Hacker Olympics 2010 is a contest designed by "hackers" and "security enthusiasts" for the like to battle it out against each other over a caffeine and sugar fueled weekend hacking stuff...

In the smpCTF Hacker Olympics qualifications teams and individuals are put up against other teams from around the globe in the same environment with the same objectives and a mission to accomplish. The qualifications are now over. The finals are just around the corner. Check the website for all 8 of the qualifying teams moving into the finals. The winter olympics CTF should be even better!

We have recently teamed up with Smash the Stack War Gaming Network. They provide year around, 24/7 Hacker challenges. Many levels and skill levels to choose from. Bored while waiting for the next smpCTF Hacker Olympics? Smash the Stack is the perfect cure..

OWASP
The Open Web Application Security Project

Application Security Conferences

September 7-10, 2010, Irvine, CA - USA Registration OPEN! http://www.appsecusa.org/register-now.html

September 16-17, 2010, Dublin Ireland

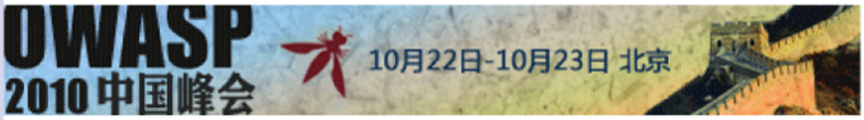
CFP and CFT OPEN – http://www.owasp.org/index.php/OWASP_IRELAND_2010#Call_for_Papers REGISTRATION OPEN - http://www.owasp.org/index.php/OWASP_IRELAND_2010#Registration

October 20-21, 2010, Rochester, NY – USA CFP OPEN - http://www.rochestersecurity.org/call-for-presentations

OWASP AppSec Germany 20.10.2010

October 20, 2010, Nurnberg, Germany

CPF OPEN - http://www.owasp.org/index.php/OWASP_AppSec_Germany_2010_Conference#tab=Call_for_Papers_-_English_Version



October 20-23, 2010, Beijing, China CFP/CFT OPEN - http://www.owasp.org/index.php/OWASP_China_Summit_2010#tab=Call_For_Paper

LASCON 2010

October 29, 2010, Austin, TX - USA

CFP OPEN - http://www.owasp.org/index.php/Lonestar_Application_Security_Conference_2010#tab=Call_for_Papers

M M X

November 8-11, 2010, Washington, DC – USA

CFP/CFT OPEN - http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=CFP

Registration OPEN - http://www.owasp.org/index.php/OWASP_AppSec_DC_2010#tab=Registration

IB WAS '10 IBERO-AMERICAN WEB APPLICATIONS SECURITY CONFERENCE

November 11-12, 2010, Lisbon, Portugal

CFP OPEN - http://www.owasp.org/index.php/IBWAS10#tab=Call_for_Papers

OWASP AppSec Brasil 2010

November 16-19, 2010, Campinas, SP, Brazil

CFP and CFT OPEN - http://www.owasp.org/index.php/AppSec_Brasil_2010#tab=Calls

Hakin9

Apply the discount code:
Hakin9 during registration to receive 10% off of the regular admission.