Automatic Vulnerability Assessment

in the
Year 2013
Myth or Reality

Noam Rathaus
CTO & Co-founder

www.BeyondSecurity.com
www.SecuriTeam.com

Back to the Future

- Before we begin, let me take you into the not so far future

Back to the Future - contd

- 2008 – due to a flood of worms that slow the Internet to a crawl, exploiting various vulnerabilities in now popular Windows Vista, Microsoft announces release of new OS in 2010

- 2013 – After 3 years of delays, Microsoft releases “Most Secure OS ever – Windows Horizon”

Back to the Future - contd

- 2015 – 20% of end users embrace new OS
- At the same time hackers get a hold of a commercial grade fuzzer called beSTORM and find a large set of 0-Days – it looks like storm clouds are converging on Windows' Horizon

- One of these 0-Days is in WinFS, and also allows for the first time the installation of malware that resides inside a database

Back to the Future - contd

- Using this 0-Day hackers install an advanced P2P Trojan horse on over 100 Million computers
- Unlike previous OSes WinFS – an SQL based file system – allows the hackers to quickly retrieve sensitive information such as credit card numbers, usernames and passwords no matter where they are stored on the hard drive

Back to the Future - contd

- It appears that no information is secure, and that now hackers can gather information – considered the most lucrative commodity – from practically million of unsuspecting people

Back to the Future - contd

- With such a vast network of P2P, hackers have in their hands:
  - Unprecedented computing power for cracking encryptions, hashes,...
  - Ability to move data around including placeholders for storing various malware such as Trojan horses and Viruses
  - One of the largest anonymous networks on the Internet – by simply implementing the standard TOR package

Back to the Future - contd

- The business is not just for fun, since the group offers a “rent-a-computer” service to spammers, phishers and malware exchange groups. Thus becoming one of the largest revenue generating scheme ever, establishing itself as one of the Fortune 100 companies

(in USD)	Amount
Revenues	$25,000,000,000
R&D Expenses	-$1,000,000,000
Marketing Expenses	-$1,000,000,000
Operational Costs	-$100,000,000
Mafia Protection Tax	-$5,000,000,000
Net Profit	**$17,900,000,000**

Back to the Present

- Sounds imaginary, so lets go back to reality for a second and see how close are we to this “near future”

ANI Vulnerability

- Just 2 weeks ago a Chinese group of hackers unleashed an exploit for a previously undisclosed vulnerability which attacks Internet Explorer browsers infecting them with malware

ANI Vulnerability Explained

- The vulnerability was located in an Animated Icon (ANI for short). The vulnerability overflowed an internal buffer in LoadAnih function. This vulnerability was not completely new, it was patched by Microsoft MS05-002, but apparently Microsoft didn't do a good job

ANI Vulnerability Similarities

- Not too surprisingly, this vulnerability affects Windows Vista, considered by Microsoft as their “Most Secure OS ever”
- Can you spot the similarity yet? If not, here is another interesting point, the hackers installed a Trojan horse whose sole purpose was to gather passwords stored in your computer, as well as look for keywords such as Credit Card and PINs, and send them back to what is referred to as Control Centers

Malware Spreading Grounds

- Further, the Chinese hackers used the best spreading ground for their malware, the NFL superbowl web site
- These were hacked not on the day of the release of the new exploit, but rather months back, more specifically a few weeks before the last Superbowl

Malware Spreading Grounds - contd

- Unlike “regular” sites, these sites are high volume and have a large percentage of non-technical visitors. This makes it a prime candidate for spreading the hacker's malware and exploiting the visitors' vulnerabilities – with little threat of them noticing it
- Some additional web sites that were hacked include asus.com, windrivers.com and others (any sites you visit?)

Malware Spreading Grounds - contd

- Most web site operators have not noticed the hack done to their web site as the attackers inserted only a minor Javascript change into the pages, this change allowed the hackers to alter dynamically the content shown to the user, and when the time comes insert a browser attacking script

Malware Spreading Grounds - contd

- In an attempt to contain the damage, the web sites that contained the malicious malware and the Javascript code were taken down
- Instead of fixing the problem (the Javascript code) the web sites the Javascript code pointed to was taken down, this made the problem appeared to have been “solved”, where in fact it wasn't

Malware Spreading Grounds - contd

- The good news was that the malware was taken down, the bad news was that the Indianapolis colts won the Superbowl :)

Malware Spreading Grounds - contd

- The Javascript was reused on the first of April by the Chinese hackers to spread the newly discovered ANI vulnerability very simply by bringing up the previously shutdown web site
- It is estimated that thousands of users were infected with malwares due to this vulnerability

Malware Roadmap

- This illustrates that the Chinese group, unlike most other hacker groups, is well organized, have a “development plan”, roadmap and access to 0-Day vulnerabilities
- Further they are more than willing to buy new vulnerabilities. As this email on the Fuzzing mailing list shows "... we buy 0Day vulnerabilities ..." if I had to guess I would say this came from the Asia Pacific Region

0Day Buyouts

- How the market for purchasing 0-Days currently looks like:
  - Good guys - 3Com and Versign that pay thousands of dollars on previously undisclosed exploits showing us that there are enough people out there that are willing to sell them
  - Bad guys - Foreign governments and Organized crime can easily afford those thousands of dollars as part of their “R&D” expenses
  - The rest of us – we live in the dark, believing that what we don't hear or see doesn't happen

So how will the future look like?

- Faster detection
- Quicker and automated patching
- Vendors finding problems before product shipment
- Networks of honeynets will catch attacks as they emerge and provide warning

Is it such a far future?

- This is what we have today:
  - ZERT – provide quick vulnerability to patch solutions
  - AVDS – allows detection of vulnerabilities and implement patches
  - beSTORM – provides vendors with the ability to find vulnerabilities in their products
  - WebHoneyNet – gives an early warning on new and emerging vulnerabilities

ZERT

- ZERT
  - Get your hold on patches as quickly as possible, even if they are not from the vendor
  - The Zeroday Emergency Response Team routinely releases patches days, weeks or even months before official vendors release them
  - ZERT concentrates mainly on high-risk vulnerabilities and creates quality patches for them
  - Missing:
    - Adoption by large corporates
    - More research on how to write better patches, make them “cross-platform” and how to get them distributed

AVDS

- AVDS
  - Automated Vulnerability Detection systems are vulnerability management systems that scans your network on a occurring basis for the latest security holes
  - Whenever they are found, close integration with Patch Management solutions provides you with fast deployment of security patches
  - This of course, minimizes your corporate exposure time
  - Missing:
    - People's faith in automation rather than in manual labor
    - More research on how to detect vulnerabilities without having access to the machine's registry or files

beSTORM

- beSTORM
  - Is no fiction, it is the first commercial grade fuzzer, it has been already used to find over 30 previously undiscovered vulnerabilities in network protocols and file formats
  - Fuzzing tools as such as beSTORM find 0-Days in vendor products and enable you to test third-party applications for unknown security holes
  - These are what your adversaries are using right now! and some vendors have already started to endorse the usage of fuzzing tools

  Missing:
  - Vendors understanding the importance of finding security issues in their products
  - Research that will improve fuzzing technologies and algorithms – find more quickly

WebHoneynet

- WebHoneynet
  - We operate a large group of volunteers that go over their web site logs looking for previously unknown attacks as well as monitoring changes in behavior of incoming users
  - This allows us to detect new trends in vulnerabilities as well as keep an eye for new 0-Days
  - Missing:
    - More honeynets being placed on the Internet, improving the current coverage of on-going-attacks
    - Research on how to better capture, and what to do with what is captured – with automation as a direction to explore

Lets Summarize

- So are we far from a completely automatic vulnerability assessment systems? in one word **NO**
- The ANI vulnerability proved it, the WebHoneynet caught the early signs of attack. ZERT built a patch within the first 24 hours of discovery. An AVDS test made it possible to detect the problem and implement the patch
- From problem to a non-issue within less than 48hours
- What is do missing, is more research that will assist us in making the time window of exposure smaller

Questions?