WHITE PAPER

IMPERVA®

The Industrialization of Hacking

Summary

Cybercrime has evolved into an industry whose value in fraud and stolen property exceeded one trillion dollars in 2009.[1] By contrast, in 2007, professional hacking represented a multibillion-dollar industry.[2] What explains this rapid growth? Industrialization. Just as the Industrial Revolution advanced methods and accelerated assembly from single to mass production in the 19th century, today's cybercrime industry has similarly transformed and automated itself to improve efficiency, scalability, and profitability.

The industrialization of hacking coincides with a critical shift in focus. Previously, hackers concentrated attacks on breaking perimeter defences. But today, the goal has changed. The objective is no longer perimeter penetration and defence. To paraphrase a popular political slogan, "it's the data, stupid." Today's hacker is intent on seizing control of data and the applications that move this data. This is why attacks against Web applications constitute more than 60 percent of total attack attempts observed on the Internet.[3]

Industry Overview

Today's complex hacking operation now utilizes teamwork, global coordination, and sophisticated criminal techniques designed to elude detection. In recent years, a clear definition of roles and responsibilities has developed within the hacking community forming a supply chain that resembles that of a drug cartel.[4] Additionally, the machine of choice is the botnet—armies of unknowingly enlisted computers controlled by hackers. Modern botnets scan and probe the Web seeking to exploit vulnerabilities and extract valuable data, conduct brute force password attacks,[5] disseminate spam, distribute malware, and manipulate search engine results. These botnets operate with the same comprehensiveness and efficiency used by Google spiders to index websites. Researchers estimate that some 14 million computers have already been enslaved by botnets. This number is expected to grow quarterly at double-digit rates.[6]

[1] Fatal System Error, Joseph Menn, January 2010, page x

[2] http://www.wallstreetandtech.com/blog/archives/2007/06/the_multibillio.html;jsessionid=TI4NAAE14S0UNQE1GHPSKH4ATMY32JVN#more

[3] http://www.sans.org/top-cyber-security-risks/

[4] http://www.pbs.org/wgbh/pages/frontline/shows/drugs/business/inside/colombian.html

[5] http://www.nytimes.com/2010/01/21/technology/21password.html

[6] McAfee Security Journal: Security Beyond the Desktop published summer 2011

Improvements in automated and formalized attack tools and services have introduced a new set of security problems for businesses. With data as the primary target, no Web application is safe from attack. Of the top 10 data breaches in 2009, half involved stolen laptops, while the other half involved Web and database assaults.[7] Attack campaigns are equal opportunity offenders; they do not discriminate between well-known and unknown sites or enterprise-level and non-profit organizations.[8] An application may be a target for attack, based on the value of the information it stores or as a means to increase the army of "zombie" computers controlled by a botnet.

With advances in hacking, come new technological vulnerabilities and security threats. Researchers estimate 92 percent of Web applications have vulnerabilities, primarily SQL injections—which enable data theft—and cross-site scripting which enables fraud.[9] In the past few years, SQL injection vulnerabilities have experienced the most dramatic growth, averaging 250,000 attacks per day.[10] Further, Imperva research found nearly 30 percent of current hacker chat forum discussions focus on SQL injection.

In order to protect personal data and avoid becoming part of a botnet army, today's consumer must learn to rely on automatic operating system updates and anti-malware software. Government and corporate enterprises must also adapt to the evolving threatscape by adjusting Data security strategies to effectively deal with high volume automated attacks.

Definition of Roles

Over the years, a clear definition of roles and responsibilities within the hacking community has developed to form a supply chain that resembles a drug cartel. The division of labor in today's industrialized hacking industry includes:

- **Researchers**: Vulnerability researchers and exploit developers who remain distant from the actual exploitation of systems. A researcher's sole responsibility is to hunt for vulnerabilities in applications, frameworks, and products and sell their knowledge to malicious organizations for profit.

- **Farmers**: A farmer's primary responsibility is to maintain and increase the presence of botnets in cyberspace. Farmers write botnet software and attempt to infect as many systems worldwide as possible by:

  – Probing Web application vulnerabilities to extract valuable data
  – Executing brute force password attacks
  – Disseminating spam
  – Distributing other types of malware

- **Dealers**: Dealers are tasked with the distribution of malicious payloads. The dealers rent botnets to conduct attacks aimed at extracting sensitive information and other more specialized tasks. The rental agreement ranges from targeted one-time attacks to multiple, persistent, and coordinated assaults. The 2009 attack against United States government agencies, purportedly by North Korean attackers, was likely executed by botnets for hire.[11] This group also includes cybercriminals, who acquire sensitive information for the sole purpose of committing fraudulent transactions.

[7] http://blog.imperva.com/2009/11/2009-the-year-of-the-mega-security-breach.html
[8] http://www.mis-asia.com/technology_centre/security/cyber-attacks-charities-can-fight-back
[9] Imperva's Application Defense Center.
[10] The IBM 2009 X-Force Trend and Risk Report, published March 2010
[11] http://www.publictechnology.net/sector/government-computers-found-be-part-massive-cybercrime-botnet-network (Note this April 23, 2009 article requires registration)

Two-Stage Industrialized Attack Process

Hacking techniques once considered cutting-edge and executed only by savvy experts are now bundled into software tools available for download. Today, the hacking community typically deploys a two-stage process designed to proliferate botnets and perform mass attacks.

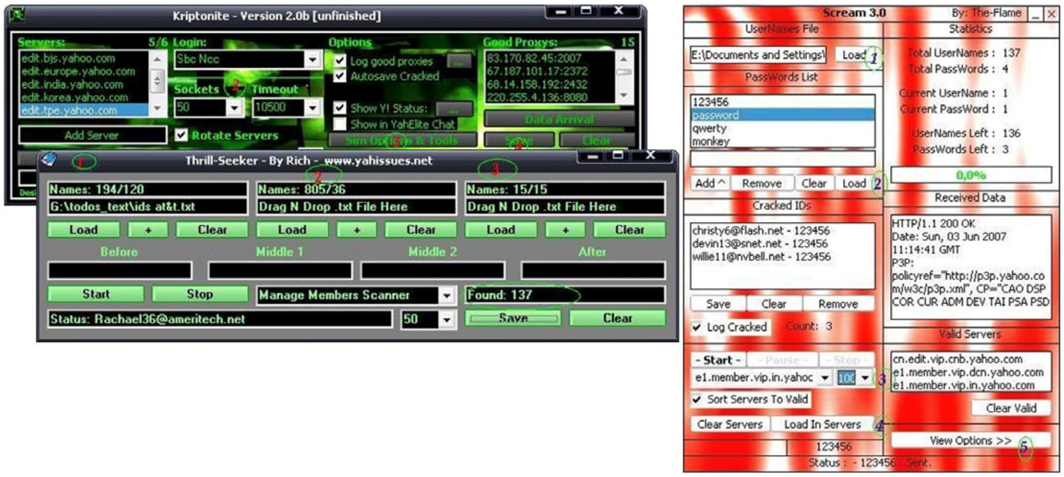
Stage One: Farmers Spread Botnets Via

- **Search engine manipulation**. This technique is the most prevalent method used to spread bots, yet it remains virtually unknown to the general public. Essentially, attackers promote Web-link references to infected pages by leaving comment spam in online forums and by infecting legitimate sites with hidden references to infected pages. For example, a hacker may infect unsuspecting Web pages with invisible references to popular search terms, such as "Britney Spears" or "Tiger Woods." Search engines then scour the websites reading the invisible references. As a result, these malicious websites now top search engine results. In turn, consumers unknowingly visit these sites and consequently infected their computers with the botnet software.

- **Email attachments and spam campaigns**. This technique is more commonly known to the general public.

Stage Two: Dealers Execute Mass Attacks Through Automated Software

To gain unauthorized access into applications, dealers input email addresses and usernames as well as upload lists of anonymous proxy addresses into specialized software, the same way consumers upload addresses to distribute holiday cards. Automated attack software then performs a password attack by entering commonly used passwords. In addition, today's industrialized hackers can also input a range of URLs and obtain inadequately protected sensitive data.



Servers: 5/6
edit.bjs.yahoo.com
edit.europe.yahoo.com
edit.india.yahoo.com
edit.korea.yahoo.com
edit.tpe.yahoo.com

Login: Sbc Ncc

Sockets: 50

Timeout: 10500

☑ Log good proxies
☑ Autosave Cracked
☑ Show Y! Status:
□ Show in YahElite Chat
☑ Rotate Servers

Good Proxys: 15
83.170.82.45:2007
67.187.101.17:2372
68.14.158.192:2432
220.255.4.136:8080

Names: 194/120
G:\todos_text\ids at&t.txt

Names: 805/36
Drag N Drop .txt File Here

Names: 15/15
Drag N Drop .txt File Here

Manage Members Scanner

Found: 137

Status: Rachael36@ameritech.net

50

E:\Documents and Settings\

123456
password
qwerty
monkey

christy6@flash.net - 123456
devin13@snet.net - 123456
willie11@nvbell.net - 123456

☑ Log Cracked Count: 3

e1.member.vip.in.yahoc 100

☑ Sort Servers To Valid

123456

Status : - 123456 Sent.

Total UserNames : 137
Total PassWords : 4
Current UserName : 1
Current PassWord : 1
UserNames Left : 136
PassWords Left : 3

0,0%

HTTP/1.1 200 OK
Date: Sun, 03 Jun 2007
11:14:41 GMT
P3P:
policyref="http://p3p.yahoo.co
m/w3c/p3p.xml", CP="CAO DSP
COR CUR ADM DEV TAI PSA PSD

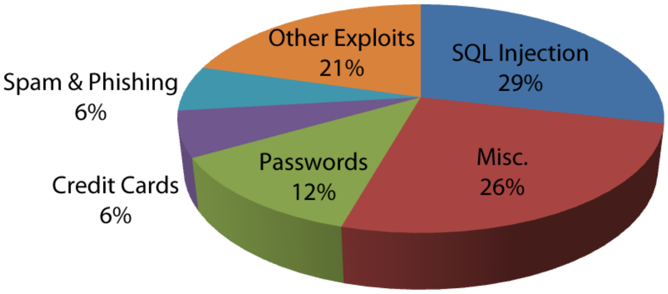
cn.edit.vip.cnb.yahoo.com
e1.member.vip.dcn.yahoo.com
e1.member.vip.in.yahoo.com

The screenshots above illustrate commonly used automated attack software

Common Attack Techniques in an Industrialized Era

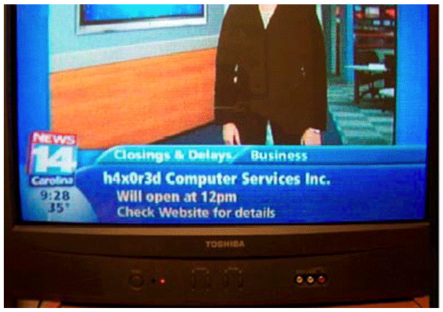
The recent shift in focus from personal information and credit card numbers to application credentials has given rise to three main types of attacks:

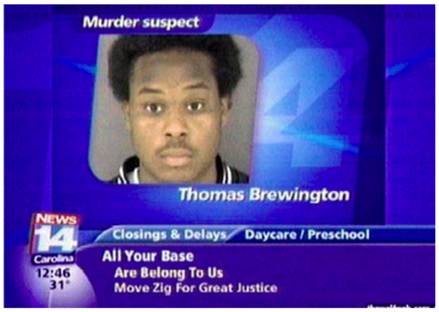
1. **Data theft or SQL injections**: Considered the number one vulnerability in Web applications, data theft is commonly administered through a technique called SQL injection. Between January and June of 2009, IBM reported nearly 250,000 daily SQL injection attacks on websites around the world. Imperva researchers reported the use and deployment of SQL injections as the top chat topic on hacker forums. Further, the 2009 assault against Heartland Payment Systems, which resulted in 130 million dollars of lost records, was attributed to SQL injection.



2. **Business logic attacks**: Web application hackers have developed attacks that target vulnerabilities in the business logic, rather than in the application code. Business logic attacks often remain undetected. In fact, most business logic vulnerabilities are hard to anticipate and detect using automated test tools, such as static code analyzers and vulnerability scanners. Often, attack traffic resembles normal application traffic. Attacks are usually not apparent from code and are too diverse to be expressed through generic vulnerability scanner tests.

   Further, in some cases, the vulnerability is not in the implementation, but rather in the business process itself. For example, a website for North Carolina's Cable News 14 allowed registered users to submit weather related announcements to alert local residents of school and business closures. The submissions were posted to the onscreen crawl during the daily newscast. In this particular attack, a malicious user submitted an informative message to the news station and then waited for the moderator to approve the blurb for airing. Once obtaining approval, the attacker edited the original message with a new bogus message. Subsequently, the content aired.





   The system did not require edited messages to undergo further moderator scrutiny. By the time Cable News 14 noticed the loophole in the submission-editing feature of the system, the malicious user had already shared the discovery with other hackers on a public message board.[12]

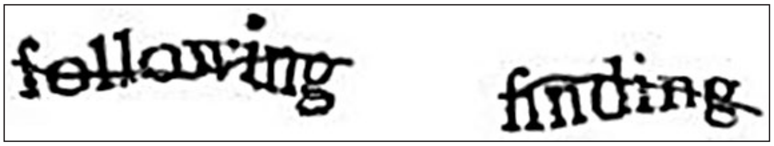
3. **Denial of service attacks**: This type of attack is usually executed as part of a blackmail scheme in which application owners are forced to pay a ransom to free their application from the invasion of useless traffic. For instance, attackers will threaten to shut-down online gambling sites for a particular ransom.[13]

[12] http://www.whitehatsec.com/home/assets/WP_bizlogic092407.pdf
[13] http://fserror.com/excerpt.html

How To Mitigate Industrialized Hacking

Today's consumer must learn to rely on automatic operating system updates and anti-malware software to protect personal data and avoid becoming part of the botnet army. The real burden, however, falls on enterprises, which must protect sensitive data and shield applications from malicious attacks. These organizations must follow traditional data and application security best practices. In addition, government and corporate enterprises must also adapt to the evolving threatscape by adjusting security strategies to deal with the growing number of automated and high-volume attacks by:

- **Fighting automated attacks with**:
  - CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). This technique attempts to distinguish humans from bots by presenting a distorted picture that users must correctly identify before admittance into the application.[14]

    An example of CAPTCHA

  - Adaptive authentication: This technique mitigates several automated attacks, including password and cross-site request forgery attacks. When dealing with highly sensitive transactions and when automation is suspected, applications must be armed with additional authentication dialogs throughout a user session. These additional authentication steps rely on previously supplied personal information from the user, such as a pet's name, favorite movie star, or a mother's maiden name.
  - Access and click rate controls: This technique monitors and detects the difference between a human browsing the Web versus faster, automated, botnet-controlled Web browsing.
- **Quickly identifying and blocking the source of malicious activity**: Knowing the IP address of commonly used attack platforms can quickly reduce attack volume.
- **Strategically enhancing defences with forensics from recent attacks and introducing reputation based controls**: Leveraging unique and identifiable characteristics from third party attacks to better help filter Web traffic. Essential forensic information includes anonymous proxies, TOR relays (The Onion Router),[15] active bots, or references from compromised servers.

[14] http://en.wikipedia.org/wiki/CAPTCHA

[15] Onion routing is a technique for anonymous communication over a computer network. Messages are repeatedly encrypted and then sent through several network nodes called onion routers. Each onion router removes a layer of encryption to uncover routing instructions, and sends the message to the next router where this is repeated. This prevents these intermediary nodes from knowing the origin, destination, and contents of the message.

Conclusion

Generals are notorious for their tendency to "fight the war" by using the strategies and tactics of the past to achieve victory in the present. However, today's cyber warriors cannot use yesterday's technology to fight tomorrow's cyber war. Organizations must realize this growing trend leaves no Web application out of reach. Attack campaigns are constantly launched not only against high profile applications but against any available target. An application may be attacked for the value of the information it stores or for the purpose of turning it into yet another attack platform. Protecting data using database and application level security solutions is a must for any organization to succeed against a strengthening foe.

About Imperva

Imperva, pioneering the third pillar of enterprise security, fills the gaps in endpoint and network security by directly protecting high-value applications and data assets in physical and virtual data centers. With an integrated security platform built specifically for modern threats, Imperva data center security provides the visibility and control needed to neutralize attack, theft, and fraud from inside and outside the organization, mitigate risk, and streamline compliance.

www.imperva.com