As social networking becomes more a part of our daily lives, individuals find this technology an attractive vehicle to perpetrate cyber crimes. Anonymity provided via social networks allows a person to easily portray another user’s identity. Cyber criminals exploit such vulnerabilities to steal user credentials, which in turn can be used to breach a company’s network infrastructure.

Regarding cyber attacks through social networking platforms, this presentation will focus on the following:

- **Process** – Various steps and methods used to carry out cyber attacks
- **Effect** (or result) – Possible ramifications of a cyber attack to a company/network
- **Safeguard** – Demonstrate methods individuals can use to limit cyber attacks and identify possible threats
Today’s Agenda

- INTRODUCTIONS
- PROCESS
- EFFECTS
- SAFEGUARDS
- QUESTIONS / ANSWERS
Clark Schaefer Consulting:
Serving elite and emerging companies with practical solutions, Clark Schaefer Consulting is a regional consulting firm with practices in accounting, controls, and technology.

Sarah Ackerman, CISSP, CISA, CICP
As the Director of Technology, Sarah Ackerman provides the Firm with extensive experience and knowledge regarding information security, IT audit, and other technology and control related services. Sarah’s work in security operations has resulted in a proven track record of success in identifying system control weaknesses, protecting information assets, and leading clients to successful organizational changes. She is well versed in internal controls and has successfully served in a variety of roles including consulting, risk management, and internal audit.

Kyle Schutte
Kyle is an experienced professional with a strong information technology background. He has experience with information system security, audit, controls, and working with internal and external auditors. Kyle has assisted organizations with the implementation of controls within a wide variety of ERP systems including SAP, Oracle and JDA to identify and correct inefficiencies and control weaknesses.
Process
- Cyber criminal communicates with an individual via social media outlet

- Message contains link to fraudulent website or an attachment which initiates an installation file

- Frequently targeted social media networks:
  - Facebook
  - Twitter
  - LinkedIn
Facebook: “Facebook photo tag notification” scam

- Redirects to a website hosting malicious iFrame script, which takes advantage of the Blackhole exploit kit, potentially resulting in malware; after a few seconds, a META redirect sends the user to the Facebook page of a random user.
Facebook : Other scams

- Facebook has also been affected by “dislike” scam, utilizing bogus Facebook updates posted by third parties, which were the source of malware offering free merchandise to users who participate in (and then forward) a survey
  - Opposite attack is “likejacking”

- Other attacks include rogue applications as well as use of Facebook Chat to spread malware, promote phishing applications, and obtain sensitive information from users using social engineering techniques
Twitter: “Is it you in this photo?” scam

- Clicking the link redirects to an IP address that itself redirects to a .CU.CC domain, to load executable code, ultimately ending up on a .SU domain that contains the Blackhole exploit kit.
Twitter : Other scams

- Attackers use basic spamming techniques, such as creation of short but compelling tweets with links to free vouchers, free merchandise, job posts, etc., which lead unsuspecting users to malicious sites.

- Other attacks have utilized Search Engine Poisoning (aka blackhat SEO), based on Search Engine Optimization (SEO) techniques:
  - Users are attracted to websites, including those that may be similar to more well-known sites, based on search engine results.
  - Users are lured into downloading FAKEAV, backdoor applications, or Trojans, or affected by click-jacking, cross-site scripting, etc.
  - Not unique to Twitter (or social media sites in general).

- KOOBFACE
  - Targeted both Twitter and Facebook
  - Used video-related posts to lead users to a fake YouTube page where they could download malicious files.
LinkedIn: “Confirm that you know” scam

- Redirects to a webpage that installs a variant of the ZBot malware (also known as Zeus)

From: linkedin.com <message-wk881425ffjm55@linkedin.com>
Subject: Mark Andronas at Payroll Processing wants to connect on LinkedIn
Date: June 2, 2011 12:55:01 PM GMT+03:00
To: Mickey Boocaei
Reply-To: message-wk881425ffjm@linkedin.com

LinkedIn

I'd like to add you to my professional network on LinkedIn.

- Mark Andronas

Neal Collins
Vice President, Strategy & Corporate Development at Payroll Processing
Greater Chicago Area

Confirm that you know Neal

© 2011, LinkedIn Corporation
Pornspace:
- MySpace attack utilizing flaw in security mailing list, resulting in password-stealing worm that hijacked user profiles and sent porn-based spam

My Webcam Thingy:
- Malware attacked over 700 Twitter accounts and tweeted the followers to check out a webcam performance
- Led viewers to a portal which stole passwords and credit card details

Fire Foxed:
- Firefox was affected by click-jacking intrusion which redirected users to porn sites which activated a worm resulting in access to passwords
Cyber attackers use malware payloads to infect a user’s computer or network
   – Types of malware: Trojan Horse, BotNet or Fake AV

In the past, pop up ads and attachments containing viruses were the primary methods of delivering malware

Sophisticated techniques now used to compromise legitimate websites in order to spread malware through holes in user’s OS
Web Exploit Kits

- Common Procedure of Web Exploit Kit

Diagram showing the flow of traffic from a user visiting a legitimate site, to a compromised web server, and finally to an exploit kit server.
Web Exploit Kits

- Malicious toolkit used to exploit security holes found in software applications for the purpose of spreading malware
- The life span of these programs are short in nature and constantly changing and updated
- Kits vary in their traffic (how much traffic is redirected to exploit kit), detection evasion (use of obfuscation, polymorphism, integrated AV scanning), and business model (license vs. rental)

- Examples of Popular Web Exploit Kits:
  - Black Hole
  - Phoenix
  - Nuclear Pack
  - Sweet Orange
Phoenix

- How it works:
  - Designed to booby-trap hacked and malicious websites so that they impose drive-by downloads on visitors
  - Probes visitor’s browser for presence of outdated and insecure versions of browser plug-ins like Java and Adobe Flash and Reader
  - Exploit kit will then silently install malware of the attacker’s choosing on the victim’s PC
    - Phoenix targets only Microsoft Windows computers
Popular Web Exploit Kits (cont.)

Black Hole

- **How it works:**
  - Potential victims load a compromised web page or open a malicious link in a spammed email
    - Compromised sites injected with JavaScript or use simple HTML iframe elements
  - Compromised web page or malicious link in the spammed email sends the user to Black Hole exploit kit server's landing page
    - Injected redirects sometimes reference remote server that then bounces the request (HTTP 30x) to the exploit site, rather than directly to the Black Hole host
Black Hole

How it works (cont.):

– Landing page contains obfuscated JavaScript that determines what is on the victim's machine and loads all exploits to which the host is vulnerable
  
  • Recent prevalent payloads include:
    – Fake AV
    – Zeus
    – ZeroAccess rootkit
    – Ransomware

28% of all cyber threats detected by Sophos and 91% detected by AVG are due to this exploit kit
Popular Web Exploit Kits (cont.)

Black Hole: General characteristics

- Multiple versions available
  - v1.0.0 released in 2010, v1.2.2 released in February 2012
  - Significant overlap between various kits available

- Emphasis on vulnerabilities in Oracle Java and Adobe Reader/Flash

- Configuration options for query parameters, file paths, redirect URLs, credentials, etc.
Black Hole: General characteristics (cont.)

- MySQL backend
- Ability to blacklist IPs, ranges, referring URL, etc.
- Provides management console with statistics to track successful exploits, country, OS, browser, landing page, etc.
- “Rental” option available, such that users pay to use kit for period of time
  - License for 3 months: $700, 6 months: $1000, 1 year: $1500
  - Rent and run on hosted server for 1 week: $200, 1 month: $500
The infected machine, commonly defined as a “zombie” contacts a public server that the attacker has set up as a control plane to issue commands.

The infected machine will first be controlled to recruit other machines using the same process of scanning for vulnerabilities.

The collection of zombies controlled by one individual is referred to as a BotNet.
A typical BotNet with zombies
Collection of Internet-connected programs communicating with other similar programs in order to perform tasks

- Hard to detect because highly dynamic, adapting their behavior to evade the most common security defenses
- Infected computers can remain dormant and undetected until commands are directed

Common technique is to use public IRC servers

- Hijacked servers can also issue instructions using HTTPS, SMTP, TCP, and UDP strings
BotNet (cont.)

- Control planes not static and frequently moved to evade detection
  - Run on machines (and by proxies) that are never owned by the botmaster

- Using control plane, botmaster can periodically push out new exploit code to the bots
  - Can also be used to modify bot code itself in order to evade signature-based detection or to accommodate new commands and attack vectors
  - Botnet masters can also modify their code to avoid other antivirus techniques such as behavioral monitoring, static analysis, and heuristics.
## BotNet (cont.)

<table>
<thead>
<tr>
<th></th>
<th>File checksums</th>
<th>RedEx Signatures</th>
<th>File Heuristics</th>
<th>Behavioral Analysis</th>
<th>Debugger Analysis</th>
<th>Static File Analysis</th>
<th>Reverse Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Code Metamorphism</strong></td>
<td>✓✓✓</td>
<td>✓✓✓</td>
<td>✓✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Noise Insertion</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(code)</td>
<td>✓✓✓</td>
<td>✓✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Compiler Settings</strong></td>
<td>✓✓</td>
<td>✓✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Noise Insertion</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(binary)</td>
<td>✓✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Crypters</strong></td>
<td>✓✓</td>
<td>✓✓</td>
<td>✓✓</td>
<td>✓</td>
<td>✓✓</td>
<td>✓✓</td>
<td>✓✓</td>
</tr>
<tr>
<td><strong>Protectors</strong></td>
<td>✓✓</td>
<td>✓✓</td>
<td>✓</td>
<td>✓</td>
<td>✓✓</td>
<td>✓✓</td>
<td>✓✓</td>
</tr>
<tr>
<td><strong>Packers</strong></td>
<td>✓✓</td>
<td>✓✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td><strong>Binders</strong></td>
<td>✓✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

✓ = Relative effectiveness in bypassing the detection/analysis technique
Armed with a network of “zombie” machines, perpetrators can attack on an enormous scale or target specific individual.

Attacks can hypothetically be carried out on any individual, corporate office, government or online retailer connected to the Internet.

Attacks can persist for long duration as proxy connections and IPs are constantly changing by the attacker.
Types of BotNet Attacks

- **Distributed Denial of Service (DDoS)**
  - With thousands of zombies distributed around the world, a botnet may launch a massive, coordinated attack to impair or bring down high-profile sites and services by flooding the connection bandwidth or resources of the targeted system.

- **Phishing**
  - Zombies can help scan for and identify vulnerable servers that can be hijacked to host phishing sites, which impersonate legitimate services (e.g., PayPal, banking websites) in order to steal passwords and other identity data.
Types of BotNet Attacks (cont.)

- **Identity Theft**
  - Botnets often deployed to steal personal identity information, financial data, or passwords from a user's PC and then either sell it or use it directly for profit

- **Spyware**
  - Zombies monitor and report user web activity for profit, without knowledge or consent of the user (and at times for blackmail and extortion)
  - May also install keylogger to harvest system vulnerability information for sale to third parties
Effects
Effects of Cyber Crime

- Anyone can fall victim to cyber crime – individuals, companies, and organizations are all susceptible.
- Attacks are becoming increasingly more prevalent and risks to individuals and companies are significant.
  - Specific effects vary for individuals vs. businesses.
- Some of the most prevalent effects are:
  - **Financial losses**: Monetary losses which are the direct result of cyber crime (e.g. financial account compromised).
  - **Recovery costs**: Costs of actions taken to remedy a breach and prevent further attacks.
  - **Penalties**: Financial penalties imposed by regulators or compensatory payments to customers for losses resulting from cyber crimes.
Effects of Cyber Crime (cont.)

- **Intellectual property/confidential information**: For businesses, loss of proprietary strategies/plans, trade secrets, financial data, and customer personal information (e.g. social security numbers, driver’s license IDs, bank information)

- **Opportunity Costs**: Service disruption or loss of transactional business for period of time

  ▪ **Reputational damage/Fear**: Adverse views and opinions of a company formed as a result of cyber crimes

- Other effects across the Internet at large include abuse of dynamic DNS and domain registration services, as well as hosting on compromised web servers (unbeknownst to the organization)
Symantec’s 2013 Norton Report details significant financial losses across countries:
Norton Report details significant average losses per victim:

**The Global Price Tag of Consumer Cybercrime**

$113 BN

Enough to host the 2012 London Olympics nearly 10 times over.

83% of direct financial costs are a result of fraud, repairs, theft and loss.

USD $298

Average cost per victim represents a 50 percent increase over 2012.
Statistics

- Approximately one third of enterprise breaches resulted from social media vulnerabilities
  - Resulted in average loss of $5.4 million per attack
- Approximately 12% of users reported an account being compromised in the previous year
- However, users continue to show weak security awareness:
  - 39% of users do not log out after each social media session
  - 25% share social media credentials
  - 31% connect with unknown parties
Many recent examples of high-profile businesses attacked through cyber crime

In 2014, Target and Home Depot were hacked, resulting in loss of customer credit card information
  – Demonstrates loss of confidential information and significant reputational damage

Sony was also hacked, resulting in exposure of information about employees, film leaks, and other data
  – Shows an instance where all of the common effects of cyber crime were evidenced.
  – Most prevalently, attack resulted in loss of intellectual property/ confidential information
Recent Examples of Cyber Crime (cont.)

- In recent years, social media accounts for many businesses and organizations have been attacked:
  - **April 2013**: The Associated Press Twitter account was hacked, resulting in false reports of explosions at the White House.
    - Caused a $136 billion drop in value on the stock market
  - **October 2013**: The Syrian Electronic Army hijacked a link from President Obama’s Twitter account and redirected it to a video of terror incidents
Recent Examples of Cyber Crime (cont.)

- **2013-2014**: Malicious code developed by the Carbanak hacker group infected systems for banks in more than 30 countries. This resulted in the theft of approximately $1 billion over two years.
  - Infection began through three spear phishing emails.
- **January 2015**: Social media accounts for U.S. Central Command were hacked, resulting in purported threats to American soldiers
- **January 2015**: Twitter accounts for the New York Post and United Press International were hacked, resulting in publication of erroneous news stories
In 2014, ISIGHT Partners, a security firm, found evidence that a group of Iranian hackers were targeting U.S. officials through social engineering in an attempt to gather intelligence information.

- Threat was dubbed Newscaster

Hackers used more than a dozen fake identities, and impersonated legitimate people, on sites like Facebook, Twitter, LinkedIn, Google+, YouTube, and Blogger.

- More than 2,000 targets were connected
Case Study: Newscaster Threat – How it Worked

- Campaign targeted U.S. military, diplomatic, and congressional personnel as well as Washington journalists, U.S. think tanks, defense contractors, and others who supported Israel
  - Additional victims in Saudi Arabia, the U.K. and Iraq were targeted

- Fake personas claim to work in journalism, government, defense contracting
  - Accounts are elaborate and created credibility using many means, most notably newsonair.org, which plagiarized news content

- The personas connected, linked, followed, and “friended” target victims, giving them access to information from updates and content
Accounts were targeted with spear-phishing messages
  – Seemingly legitimate links were sent asking recipients to log onto false pages, thereby capturing credential information which could be leveraged in further exploitation

The campaign was also linked to malware
  – While not sophisticated, it included the capability to perform data extraction

This example of cyber crime is elaborate; the amount of data extracted is unclear
Safeguards
Top 10 Safeguards

1. Employee Awareness and Risk Management
2. Social Media Privacy Settings
3. Access Control
4. Vulnerability Management
5. Patch Management
6. Data Inventory/Protection
7. Data Loss Prevention
8. Monitor System Configuration Changes
9. Leverage Threat Feeds
10. Anti-Malware and Anti-Virus Protection
#1. Employee Awareness/Risk Management

- Social media security training
  - Comprehensive, on-going employee training and awareness programs
    - New employee training and periodic security education and awareness programs
    - Periodically check/validate security awareness (e.g., internal email campaign to determine if users continue to click bad links, attempts to tailgate into secure areas, determine if PCs are left unlocked)
  - Organizations that do not have security awareness programs report significantly higher average financial losses from cybersecurity incidents

Only 36% of companies have instituted bare minimum of social media training for employees and even fewer have active Social Risk Management programs
Social Risk Management Programs

- Enable security leaders to:
  - Articulate the criticality and goals of cybersecurity (specifically focusing on social cyber attacks)
  - Set agenda for prioritizing and validating investments based on risk management strategies

- Provide a framework for:
  - Periodic risk assessments
  - Objective third party to assess the security program
  - Risk-based approach to prioritize protection of high-value information across the enterprise and allocate resources in correlation with the greatest risks
#2. Social Media Privacy Settings

- Block profiles from public searches
- Restrict who can find you via online search
- Limit what people can learn about you (or your company) through searching

Other tips…
- Log out after each session
- Don’t share social media credentials
- Don’t accept requests from unknowns
- Don’t click suspicious links
#3. Access Control

**Account/Password Management Policies**

- Ensure that password length/complexity/reset/history requirements are defined and configured

**Identity Management**

- Ensure there is comprehensive, continuous process to understand which users should have access to which resources
- Validate each user has appropriate access entitlements on a regular basis
Two-Factor Authentication (aka multi-factor authentication)

- Two or more of the following:
  - Something you have (e.g., ATM card)
  - Something you know (e.g., password)
  - Something you are (e.g., biometrics)
  - Somewhere you are (e.g., location-based coordinates)

Intrusion Prevention System (IPS)

- Critical layer of defense to protect network from harmful traffic such as a cyber-threat that has passed through or bypassed firewall
Organizations that have detected attacks are considerably more likely to employ security capabilities such as vulnerability management.

Automate threat and vulnerability remediation
- By automating remediation of vulnerabilities, cyber attacks can be detected and contained more quickly through tool self-analysis.

Correlate data gathered from vulnerability scanning with its business criticality or risk to the organization
- This allows for prioritization and more efficient mitigation of vulnerabilities.
#5. Patch Management

- Create system/process to ensure that security patches are applied in timely manner to all systems and applications, whether at infrastructure or end-user level

- Implement policy-based approach
  - Drives patch-management responsibility to the client end-point, which uses agent to constantly self-check to see if it has the pre-defined policy or desired state
  - Any device whose state differs from the desired state (e.g., does not have the most current security patch) automatically receives update without any intervention from IT
Support remote and mobile users

- Unique needs of remote and mobile users make patch management difficult
  - Mobile users typically connect only intermittently and often through unstable, low-bandwidth connections

- Given remote users' varying connections and time availability, allow a user to defer non-critical installation for certain number of days.
  - Conversely, critical patch might come through mandatory forced install
#6. Data Inventory/Protection

- Inventory data and understand who has access to it
  - Understand where confidential and/or PII data is within the environment
  - The first step in protecting data is knowing where it is and who has access to it

- Protect confidential data
  - Once you know where the confidential data is, build controls around it
  - Encrypt data at rest and/or in transmission
#7. Data Loss Prevention

- DLP products monitor, detect and block sensitive data while
  - **in-use** (endpoint actions)
  - **in-motion** (network traffic)
  - **at-rest** (data storage)

- Implement controls to detect data exfiltration
  - When data is being abnormally transferred out of the organization

- Many DLP products cover the most common actions taken to steal sensitive information
#8. Monitor System Configuration Changes

- Deploy system configuration change monitoring

- Many cyber attacks can be easily detected by watching key indicators on systems

- Provides visibility and assurance of system configurations and the compliance impact of configuration changes
#9. Leverage Threat Feeds

Use feeds of threat data that identify IP addresses and domain names used to control botnets

Match this data against firewall or proxy logs

This can help accelerate detection and thus containment
#10. Anti-Malware/Anti-Virus Protection

- Install anti-malware and anti-virus protection
  - Regardless of platform, use secure passwords and encryption on every device that touches the business (phones, tablets, laptops, desktops)
  - If devices support third-party anti-malware apps like those from McAfee, Symantec, or Trend Micro, install one
  - Implement business-class security suites that offer multi-device protection
For More Information

If you wish to discuss any aspects of this presentation in more detail, please feel free to contact us:

Clark Schaefer Consulting, LLC.
120 East Fourth Street, Suite 1100
Cincinnati, Ohio 45202
513-768-7100
www.clarkschaefer.com

Or send an e-mail to either of us directly:
Sarah - sackerman@clarkschaefer.com
Kyle - kschutte@clarkschaefer.com