Current Trends in Cybersecurity

Wednesday, October 17
10:35-11:50 a.m.

Steve Gemperle, Senior Special Agent,
US Secret Service

Sit in on this discussion of cybersecurity trends led by one of the U.S. Secret Service’s top network intrusion investigators in the nation operate a traditional accounting system.
Steve Gemperle is a senior special agent with the United States Secret Service who specializes in cybercrime. Steve joined the Secret Service in 1999 and is currently assigned to the San Antonio field office. For the last several years he has focused on computer crimes and network intrusion investigations including numerous high level hacks. Gemperle also provides cyber protection advances for the President and Vice President when they travel. Gemperle has been recognized as the Secret Service’s top network intrusion investigator for 2014, 2015 and 2016. He was also named one of the top five forensic investigators in the Secret Service. He teaches computer crime and network intrusion investigations both domestically and internationally. Gemperle has held a number of other positions within the Secret Service. He was assigned to the Presidential Protection Division for President George W. Bush and was an instructor at the Secret Service training academy where he served as the lead instructor for the combatives and tactics unit.
UNITED STATES SECRET SERVICE

Current Trends in Cyber Crime

October 17, 2018

What most people think we do....
**Integrated Mission: Part I**

**Protection**
- President
- Vice-President
- Former Presidents
- President Elect
- Foreign Dignitaries
- Others

---

**Integrated Mission: Part II**

**Investigations**

**Electronic Crimes**
- Computer / Internet Fraud
- Network Intrusions/Data Breach
- Critical Systems Protection

**Financial Crimes**
- Identity Crime
- Check Fraud
- Access Device Fraud
- Bank Fraud
- Mortgage Fraud
- Wire Fraud

**Counterfeit**
- Currency
CRYPTOCURRENCY

WHAT WE THINK OF

- bitcoin
- ripple
- Ethereum
- Litecoin
- Megacoin
WHAT IS CRYPTOCURRENCY?

CRYPTOCURRENCIES

- Digital Currency or Virtual Currency
  - Electronic
  - Global
  - Community Specific
  - Unregulated

[Images of Delta SkyMiles and Points Travelers]
WHAT IS CRYPTOCURRENCY?

<table>
<thead>
<tr>
<th>Month</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2017</td>
<td>$863</td>
</tr>
<tr>
<td>December 2017</td>
<td>$20,000</td>
</tr>
<tr>
<td>January 2018</td>
<td>$10,000</td>
</tr>
<tr>
<td>March 2018</td>
<td>$11,000</td>
</tr>
<tr>
<td>April 2018</td>
<td>$8,900</td>
</tr>
<tr>
<td>May 30 2018</td>
<td>$7,518</td>
</tr>
</tbody>
</table>
WHAT IS CRYPTOCURRENCY?
ANONYMOUS
Which is Why Criminals Love it!

WHAT IS CRYPTOCURRENCY
ANONYMOUS

WORLD OF WARCRAFT
PlayStation.
WHAT IS CRYPTOCURRENCY?
PSEUDO-ANONYMOUS

HOW IT WORKS
HOW IT WORKS

Bitcoin Address

Bitcoin is stored on an address
Ex: 1UM09GDndX94FffJRKSx84XX5

The address is stored in a Bitcoin Wallet

HOW IT WORKS

Bitcoin Address

- Bitcoin address:
  - Between 26-36 random characters long or a QR code
  - Is a public key
  - Represents the user
  - Pathway for the sender and receiver
  - Must be known to make a transaction

Bitcoin Address = Email Address/Bank Routing #
HOW IT WORKS
Private Key
- Private Key:
  - The Wallet is unlocked with a passcode/private key
    - The user must have the passcode or private key to gain access to the wallet to initiate a transaction
    - Similar to an Email Password or ATM PIN#

TWO TYPES OF WALLETS
Cold Wallet
- No Internet/Web Access
- No Recovery
- No Remote Access*
- No Vault/Host
- Physical Device/Hardware/Paper
  - USB/Trezor

Hot Wallet
- Internet/Web Access
- Recovery Options
- Remote Access
- Mobile Device Wallet
- Software Wallet
  - Server
TRANSACTION

Network
- In order to complete a transaction a user must be connected to a network
- A network is established by Bitcoin users connecting to other Bitcoin users
- Most wallets will automatically connect to an established or embedded network or node
- This network or connection of users is often called a NODE
**TRANSACTION**

Miner Comes in

1.) Verify Transaction
2.) Record Transaction on Ledger

**MINERS**

- Every time a Miner verifies/records a transaction, they are placed in a lottery to receive Bitcoin as payment
- 12 bitcoin every 10 min – or $90k every 10 min.
- In addition to being an incentive for Miners to verify and record transactions, mining is also the only way for NEW bitcoin to be introduced into circulation
- Currently, almost 78% of Bitcoin has been released into circulation - Around 18 Million
- It is anticipated that all 21 million Bitcoins will be released by 2025
From pranks to cyber warfare

- Dec 16 2016
  - Hackers cut off power to the Ukraine
  - Lasted 4 days
  - Simultaneous attacks on transportation, treasury and Pension funds
  - Used BlackEnergy and KillDisk malware
At home…

- Presidential Inauguration - 2017
  - DC Metro camera system
    - Crypto mining
- North Carolina 911 - 2017
  - Valid user credentials found
    - Unpatched system
- Atlanta - 2018
  - Ransomware event
- Baltimore MD - 2018
  - Ransomware

Avenue of Attack

- Number of the these were compromised through 3\textsuperscript{rd} party vendors
- 3\textsuperscript{rd} party vendors compromised through email.
- 90\% of all cyber attacks begin with an infected email message
More common than you think
Why they do what they do…

- Organized Criminal Groups
  - The US is seen as weak on security
  - Punishment is seen as weak
  - Extradition is difficult
  - Profit potential is high
  - Business are willing to absorb “acceptable levels” of fraud loss
  - Seen a “victimless” because “evil corporations” take loss not individuals

Vladimir Drinkman
Drinkman

- Kitco.com (1999)
- FiServ (2003)
- CardEx (2006)
- Best Buy (2007)
- Subway (2007)
- Carrefour (2008)
- 7-11 (2008)
- JC Penny (2008)
- Hanneford (2008)
- Nasdaq (2010)
- Dow Jones (2010)
- Euronet (2011)
- Global Payments (2011)

- Baiduri.com (2001)
- Banamex (2005)
- Metro Cash & Carry (2008)
- Visa Jordan (2009)
- JetBlue
- Wet Seal

Drinkman

- Dave and Busters
- TJ Maxx
- Heartland Payment Systems
- JC Penny
- TARGET (malware attributed to Drinkman)
Between 1999 and 2012 Drinkman stole 160+ million credit card numbers and pocketed $189+ million

Feb 15, 2018

Vladimir Drinkman was sentenced to 144 months in prison
Motivation

- Curiosity and challenge
- Challenges from other hackers on IRC channels
- Bragging rights
- Challenges keep getting harder as you go
- Contract work
- Financial Gain

Hacking Rules

- **NO RUSSIAN TARGETS**
  - Get in but don’t disrupt operations
  - **NO DDOS**
  - Will not go after targets where loss of life could occur
  - Remain Anonymous
Daily Grind

- Wake up and get to work
- Research potential breaches – recent news headlines / Securityfocus.com / bugtrack
- Typically had 5 to 6 “projects” at any given time
- Check security bulletins
- Look for new exploits / vulnerabilities – Loves Microsoft’s Patch Tuesday
- Marijuana use to encourage creativity

His Malware

- Can’t clean everything but he tried to erase footsteps
- Malware would beacon once a day
- Malware may sleep for a couple of weeks
- ALWAYS installs additional backdoors
  - Usually adds 3
- Main folder attached - Windows/System32
- Will change Date Created on malware
- Will change name of malware to match name of files on system (Whitelist hiding)
**Method**

- Find the IP range of a company
- Use port scanners to find openings
- Find servers exposed to the web
- **Steal a backup**
- Load the backup in VM and build a mock system
- Attack the system to test proof of concept
- Test where and how the exploits will affect system, so your cleaning tools can erase the evidence

**Attack Vectors**

- Webserver – SQL injections
- SpearPhishing
- Botnet
- Insider – Banamex (2005)
- Router – provided shell access and are trusted devices
- Unicode – old code, but still used in lots of banks. If found will give access to any file on the server.
Attacks continued

- External webservers that have a common / shared domain with the data server are a huge risk
- External Webserver MUST be in a DMZ
- Links between dataserver and the DMZ should be controlled and filtered.
- Are you staging servers exposed to the outside (hint: *Everyone* says no)
Current Trends

- Ransomware
- Business Email Compromise
  - Romance Scams / Work from home
- Skimming
- Mobile Malware
- Microsoft Tech Support

Ransomware

- Ransomware is a type of malware which restricts access to the computer until user pays a ransom.

- This one is ugly – once your infected there is only a slight chance that you can be helped.

- www.nomoreransom.org
Business Email Compromise

- Employee receives an email
- May be from a person of authority (CEO) or a simple invoice
- Employee answers the email
- Employee is instructed to conduct a wire transfer
- Wire transfer is quickly initiated

BEC – What just happened?

- Email received has been spoofed
- Invoices can be made to look legitimate
- Employee often thinks this is a chance to make a good impression / honored to be part of something important
- Because the employee initiated the transfer most banks won’t take the loss
What do we do?!?!?

- Contact the Bank – attempt to recall the wire
- Contact Law Enforcement
- Both should be done quickly – time is of the essence!!!
- DON’T TRY to cover it up.....
- By the way...your computers may be infected and the bad guy possibly has access to all your email

Romance Scams / Work from Home

- Seems legitimate
- Asks you to set up a bank account
- Will send you checks or wire transfers
- Asks that you send the money to them
- BEC tie in / Illegal money remitter / money laundering
May 24th Skimming Roundup
- 7 law enforcement agencies
- PSI and McConn technicians

- 407 pumps inspected
- 37 stations
- 2 Skimmers recovered
Gas Pump Skimming

- Common Skimming Locations
  - Gas Stations (affixed to pumps)
  - ATMs (affixed to machine)

- Why are these locations so popular?
  - Heavy customer volume
  - Credit card is common payment method
  - Pumps not required to be updated until 2020
  - Multiple employees (difficult to identify suspect)
  - Employee turnover (co-conspirators easy to recruit)
  - Covertly placed (gas pumps and ATMs)
Mobile Malware

- Huge increases in Mobile malware
- Monkey Run malware
  - In Feb. 120 games in Google Play were actually banking malware
- Free Flashlight app
  - Turned on your camera and microphone
  - Steals banking information
- Avoid all Fortnite apps on Android
- Differences between Android and IOS
- Run a mobile antivirus program
Microsoft Tech Support

- Scam where you give control of your device

- 2 out of 3 people have experienced

- 1 in 10 people lost money in a tech support scam in the last year.

Microsoft Tech Support

- Of those that were victimized
  - 17% were older than 55
  - 33% were between 35 and 54

- **50% were millennials between 18 and 34**
Cyber Tips - personal

1. Disable Macros
2. Protect your computer from cyber attacks
   • Update your computers operating system
   • Have latest security software patches & antivirus
3. Use 2 form authentication for banking credentials
4. Back up important information regularly
5. Change default passwords on devices
Cyber Tips - Professionally

- DON’T unplug machines – remove from network but leave powered on.
- Ransomware – isolate machines from network
- BEC – quick action or the $$$ is gone / run headers for IPs if you can get email
- Skimming – limited data on some skimming devices / DNA and fingerprints
- Mobile malware – pay attention to downloads / run antivirus

Advice from a Hacker

- Backup files – Big issue
  - Where are they located?
  - How good is their security?
  - Infect the backup first or just take the whole thing
  - Destroy backup before attack
Advice from a Hacker

- Google your own company
  - yoursitem.com + " .asp"
- Google will find unprotected areas for you!
- Google will show you folders and scripts which are vulnerable.
- This will show mapped areas of servers which are unprotected.
- He used this to find SQL injection vulnerabilities

Advice from a Hacker

- Afterhours can you shut down Internet access – most hackers will attack at night (day time over there)
- Firewalls almost never detect lateral movement
- Monitor outbound and encrypted outbound traffic
  - Will your firewall prevent reverse SSH to a C&C server
- Patch installation and updates
Advice from a Hacker

- Implement IDS
- Establish a baseline for activity on your system
- Red Team your systems
- Implement regular system discovery
- Flag geolocation lookup sites in your weblogs
- Can you authenticate every device on your network?

Advice from a Hacker

- Should have a honeypot on every subnet and it should alert immediately
- Webserver backdoors – fix them
  - .asp and .jsp allow backdoors
- Webserver default error page – Change the output
- Utilize PCI, ISO27001 and NIST framework
We have seen a marked increase in the quality, quantity, and complexity of cyber crimes targeting both private industry and critical infrastructure.

Don’t ask the question “Will we be breached?”

Ask the question: “When we become a victim, do we have a plan?”
People may *think* the cost of protecting data is high, but doing nothing can be far more expensive.

Cyber security is usually an afterthought until there is an incident, then it becomes the only thought.

UNITED STATES SECRET SERVICE

Questions?
Ten CyberSecurity Tips for Small Businesses

Broadband and information technology are powerful factors in small businesses reaching new markets and increasing productivity and efficiency. However, businesses need a cybersecurity strategy to protect their own business, their customers, and their data from growing cybersecurity threats. Here are ten key cybersecurity tips for businesses to protect themselves:

1. **Train employees in security principles**
   Establish basic security practices and policies for employees, such as requiring strong passwords, and establish appropriate Internet use guidelines that detail penalties for violating company cybersecurity policies. Establish rules of behavior describing how to handle and protect customer information and other vital data.

2. **Protect information, computers and networks from cyber attacks**
   Keep clean machines: having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats. Set antivirus software to run a scan after each update. Install other key software updates as soon as they are available.

3. **Provide firewall security for your Internet connection**
   A firewall is a set of related programs that prevent outsiders from accessing data on a private network. Make sure the operating system’s firewall is enabled or install free firewall software available online. If employees work from home, ensure that their home system(s) are protected by a firewall.

4. **Create a mobile device action plan**
   Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network. Require users to password protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information while the phone is on public networks. Be sure to set reporting procedures for lost or stolen equipment.

5. **Make backup copies of important business data and information**
   Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Backup data automatically if possible, or at least weekly and store the copies either offsite or in the cloud.
6. Control physical access to your computers and create user accounts for each employee
Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

7. Secure your Wi-Fi networks
If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password protect access to the router.

8. Employ best practices on payment cards
Work with banks or processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations pursuant to agreements with your bank or processor. Isolate payment systems from other, less secure programs and don’t use the same computer to process payments and surf the Internet.

9. Limit employee access to data and information, limit authority to install software
Do not provide any one employee with access to all data systems. Employees should only be given access to the specific data systems that they need for their jobs, and should not be able to install any software without permission.

10. Passwords and authentication
Require employees to use unique passwords and change passwords every three months. Consider implementing multi-factor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multi-factor authentication for your account.