# INSIDER THREAT DEFENSE

**Protecting Against Insider Threats Requires Thinking Outside The Box**

**Data And Information Exfiltration Made Easy**

- Malicious Insiders attempting to commit data or information theft against the government or business will in most cases exploit an organizations weakest links, that give them the greatest chance of success, without being caught.
- User Activity Monitoring (UAM) tools are important for visibility of employee actions and the detection of Insider Threats, but UAM tools **will not detect all techniques** that could be used by a Malicious Insider. Identifying other potential security threats is critical.

**Malicious Insider Playbook Of Options**

How Could A Malicious Insider Try To Remove Or Disclose Classified, IP, Trade Secrets, Business Sensitive, Information From Your Organization?

- ☐ By Taking / Copying Documents Of Importance (IP, Business Sensitive, Trade Secrets. Etc.) That Are Stored On Employees Desks Unprotected, That Should Not Be There? (3M Visual Hacking Experiment)
- ☐ By Smartphone (Verbally, Pictures, Audio / Video Recording)
- ☐ By Use Of USB Storage Devices (Thumb Drives, Smart Phones, MP3 Players, Etc.)
- ☐ By Using Fax Machines Without Authentication
- ☐ By Using A Multi-Function Devices (Print, Fax, Scan, E-Mail) Without Authentication (Scan Sensitive Or Classified Documents To An Internet Connected Scanner With E-Mail Capabilities, Then E-Mail To Personal E-Mail Account Or Other Individual
- ☐ By Portable Hand Held Document With Wifi Or Wireless Mouse Scanner
- ☐ By Installing Cell Phone Spy Software On An Employees Smartphone
- ☐ By Using Keyboard / Keystroke Capture Devices (Records Keystrokes / Passwords (Undetectable)
- ☐ By Use Of Removable, Writeable Media (Floppy Disk, DVD-CD) (Burning Software May Not Need To Be Installed To Burn DVD-CD Disks. Download Self Running Executable Burning Software)
- ☐ By Printing To Local Printer Attached To Employees Computer. Bypass Network Print Monitoring
- ☐ By Using Remote Access Tools (No Install Required-Self Running Executable) Or Chrome Remote Desktop Extension
- ☐ By Using Webcams Or Computer Screen Sharing Software To Share Information / Screen On Internet (No Install Required-Self Running Executable) (Screenleap, Join Me, Etc.)
- ☐ By Using Steganography Tools (Hidden Data Techniques) (No Install Required-Self Running Executable) (Steganography Tool Demo)
- ☐ By Using A Computers Microphone To Dictate Sensitive Information To A Sound File, Then E-Mailing The Sound File To Personal E-Mail Account Or Other Individual (Plug Mic Port)
- ☐ By Sending Sensitive Files Using Web Based Personal E-Mail From Work (HTTPS Blind Spot To Network Monitoring Tools)
- ☐ By Using Web Based Applications To Send Large Files, To Bypass Corporate Content Filters / File Size Limits (Drop Send, Drop Send Demo)
- ☐ By Exporting An E-Mail Inbox And Subfolders Using An Outlook PST File, Then Uploading To Web Based Personal E-Mail Or Cloud Storage (Turn Off Export Feature In Outlook)
- ☐ By Using Facebook Instant Messenger / Chat Software To Upload Sensitive Files

- Using A Smartphone's Hot Spot Capability To Connect A Wifi Enabled Desktop Computer To The Internet, Then Upload The Sensitive Files Via Webmail, Cloud Storage, FTP, Etc., Bypassing Network Security Monitoring Tools
- By Downloading The Sensitive Files From A Network Share, To A Local Hard Drive (HD). Then Disconnect The Computer From The Network, Install 2nd HD, Boot From USB Thumb Drive / DVD-CD, And Clone To 2nd Hard Drive. Then Walk Out Door With HD.
- Is An Employee Booting From A Live CD / USB? (Boot Into Live Operating System Without Installing Anything) Connecting To Network, Locating Sensitive Files And Sending Via Web, Bypassing Network Security Monitoring Tools)
- By Walking Out The Front Door (No Bag Checks / Security Guard Inspections)
- By mailing classified, sensitive information or intellectual property to another source outside the organization. Does the company inspect packages before they are sealed and shipped via USPS, FEDEX, UPS?

**Services Available For Malicious Purposes**

**Web Cam / Screen Sharing (No Software Installation Required)**

**Threat Example**: Access classified documents of interest. If smart, remove security classification markings. Print documents. Scan classified documents using unclassified document scanner connected to the network, save to network, or local storage. Share screen or documents to Smartpone, Computer or Tablet.

**SpoofCard - Caller ID Spoofing With Voice Spoofing**

**Social Engineering**

**Call Helpdesk And Reset Password**

**Access Smart Phone Voice Mail Without Passwords**

www.spoofcard.com

**Spoof Card Demo / Spoof Card In The News**

www.youtube.com/watch?v=cKY7SdHpUyg

www.youtube.com/watch?v=QoNlxNnThLQ

**Key Me - 3D Printing Of Keys**

**Take Picture Of Keys Using Smartphone App And Have Them Made And Mailed To You**

Contacted KeyMe Regarding Ordering A Key And Having It Shipped. Received Instruction Listed Below.

1) Download The FREE KeyMe App.
2) Create An Account.
3) Using The KeyMe App Scan A Physical Copy Of A Key, Which Will Be Added To Your KeyMe Key Chain.
4) Select The Key You Want To Order From Your KeyMe Key Chain.
5) Place The Mail Order Via The KeyMe App. Pay By Credit Card.
6) Once Te Mail Order Ships, Expect To Receive It Within 5 Business Days Via USPS.

www.key.me

**Key Me Demo / Key Me In The News**

www.youtube.com/watch?v=4Mzd5E7DqGA

www.cbsnews.com/news/how-tech-savvy-thieves-can-steal-your-house-keys/

**Contact Information**
**Jim Henderson, CISSP, CCISO**
**Founder / Chairman Of The National Insider Threat Special Interest Group**
**CEO Insider Threat Defense, Inc.**
**Insider Threat Program Development / Management Training Course Instructor**
**Insider Threat Vulnerability Assessor & Mitigation Specialist**
**888-363-7241 / 561-809-6800**
jimhenderson@nationalinsiderthreatsig.org
www.nationalinsiderthreatsig.org
www.insiderthreatdefense.us
james.henderson@insiderthreatdefense.us