Dissecting the Attack: How Hackers Target and Compromise Products and Systems Just Like Yours

Valerie Thomas, Securicon
Introduction

• Technical Director for Securicon
• 15+ years in Infosec
• Coauthor of *Building An Information Security Awareness Program*
• Social Engineering Trainer
• Physical Security enthusiast
Agenda

• Why this topic
• Who are we defending against?
• Walkthrough of attack phases
  • Information gathering
  • Attack creation
  • Attack execution
  • Post attack
• Prevention and Mitigation
Many cyber defenses can be bypassed with physical access

Attackers want to gain physical access to attack cyber assets

The ultimate goal is to obtain access and stay there unnoticed

One of the best methods to achieve this is to target physical security personnel, vendors, and integrators
Now that blended cyber and physical attacks are becoming more mainstream, physical security technology and the companies that create and deploy it are high value targets for hackers.
Misconceptions

• Attacks or "hacks" only take one step or happen quickly
• Hacking is always performed remotely
• Hacking always involves computers
• Information only comes from one source
Who Are We Defending Against?
Where Do Hackers Get Information?

Common starting areas:
- The target’s website
- Social media (Facebook, Twitter, Instagram)
- LinkedIn
- The Dark Web
- Shodan
- Wikileaks
- Openleaks
- Pastebin
Be great at what you do

Get started - it's free.

First name

Last name

Email

Password (6 or more characters)

By clicking Join now, you agree to the LinkedIn User Agreement, Privacy Policy, and Cookie Policy.

Join now
LinkedIn: The Phone Book for Social Engineers

Groups Directory

Browse by name  # ABCDEFGHIJKLMNOPQRSTUVWXYZ

Featured Groups

Software & Technology Professionals: Managers I HR I Recruiters I Blockchain I Investors

Harvard Business Review
Finance Club

#1 Project Manager (PM) Network I Business & Software I BlockChain & Crypto Consulting I FinTech

On Startups - The Community For Entrepreneurs
Marketing Communication
Engineering Career Opportunities (Jobs & Employment)

Social Media Marketing
Linked:HR (#1 Human Resources Group)
Digital Marketing
The Recruiter.com Network -#1 Recruiting, Career, Jobs, HR Social Media & Recruitment Business Group
Fórum VAGAS.com - RH, carreiras e profissões
Marketing I CMO I Social Media I Education I Digital
Dubai Recruitment
Pete Asmus' Real Estate Networking Group (Investor Strategies)
Telecoms Professionals: IoT, LTE, M2M, OTT, Internet of Things, Mobile, Telecom
Physical Security Professional (PSP)

Standard group

19,491 members

Request to join

About this group

The PSP group on LinkedIn is comprised of Physical Security Professionals certified by ASIS International. If you are a PSP or have the ambition to become one you are welcome to join. Information regarding the PSP-certification is available through the group administrator.
Security Clearance Jobs
35,665 members

ADMINs

Eric Pecinovsky • Group Owner
Director of Marketing at ClearanceJobs

Evan Lesser • Manager
President and Founder, ClearanceJobs

Lindy Kyzer • Manager
Senior Editor, ClearanceJobs.com

Ashley LaGanga • Moderator
Writer/Editor

ABOUT THIS GROUP

ClearanceJobs.com, the largest security-cleared career network. Search thousands of jobs from pre-screened, registered defense industry employers. Specializes in defense jobs for professionals with security clearances. Defense industry news, security clearance jobs, security clearance issues and career advice.
Military & Defense Logistics
4,747 members

All Cleared - Recruiter-Candidate Connection
6,291 members

Defense & Aerospace
135,445 members
<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Company</th>
<th>Location</th>
<th>Current Job</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkedIn Member</td>
<td>VP - Unix Engineering at ilNautix Tech (I) Pvt. Ltd, Chennai Area, India - Information Technology and Services</td>
<td></td>
<td></td>
<td>Current: Team Lead Unix Administrator at Cap Gemini Ernst &amp; Young</td>
<td></td>
</tr>
</tbody>
</table>
• Installation & Configuration of Windows 2003 Server remotely through DRAC & iLO, troubleshooting server 2003 Active Directory and network infrastructure DNS, DHCP, IIS etc.
• Allocating DHCP Scope, DNS Entry Creation.
• Planning and Scheduling Monthly Patch deployment in all Middle East Servers.
• Provides Application and Operating system support.
• Installation and configuration of Anti-Virus Software (Symantec Antivirus), also working on anti-virus update issue.
• Resolving the Server related issues.
• Server Preparation as per requirement
• Managing WSUS (Windows System update Services) Server for patch deployment
• Monitoring the Servers using HP Operations Manager, HP Sitescope
• Lotus Domino Monthly Maintenance in all Middle East Offices.
• Managing the Intra Mail Service (Lotus Notes)
• Maintaining the local VLAN based Networking
Armed security at [redacted] 275 &
[eBook] Power Grid Convergence: The Path to Cyber-Physical Resilience

The integration of cyber and physical technologies is fundamental for the evolution of the digitally enabled grid.

Without this data, a network cannot achieve the potential efficiency and effectiveness of a converged network, and the ability to offer ... Show more

Power Grid Convergence eBook: The Path to Cyber-Physical Resilience

This exclusive eBook gives an insight into the integration of cyber and physical technologies. Specifically, this focuses in on the top...

HTTP://BIT.LY/2S1CQ3D
HTTPS://GOO.GL/G2F9KE
<table>
<thead>
<tr>
<th>Domain</th>
<th>Original Price</th>
<th>Reduced Price</th>
<th>Add to Cart</th>
</tr>
</thead>
<tbody>
<tr>
<td>ics-security.org</td>
<td>$19.99*</td>
<td>$7.99*</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>icssecurities.com</td>
<td>$14.99*</td>
<td>$11.99*</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>ics-security.online</td>
<td>$49.99*</td>
<td>$0.99*</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>ics-security.info</td>
<td>$19.99*</td>
<td>$2.99*</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>Domain</td>
<td>Original Price</td>
<td>Discounted Price</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>physicalsecurityprofessionals.com</td>
<td>$14.99*</td>
<td>$11.99*</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>physicalsecurityprofessional.org</td>
<td>$19.99*</td>
<td>$11.99*</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>physicalsecurityprofessional.pro</td>
<td>$21.99*</td>
<td>$6.99*</td>
<td>Add to Cart</td>
</tr>
<tr>
<td>physicalsecurityprofessional.net</td>
<td>$18.99*</td>
<td></td>
<td>Add to Cart</td>
</tr>
</tbody>
</table>
Why did you need another one ? Me: "I needed a duty gun for work so......" 😏 #glock #glock17 #g17 G17 #securityofficer
WINNER!!

Keep your coffee hot with our Dunkin warmer
How do we protect ourselves?

- Review your resume (and LinkedIn)
- Consider using burner phone numbers or Google Voice for documents such as resumes and your social media presence
- Remove metadata from documents that you share/upload
Safer Browsing

• Remember, not all phishing uses email
• Dedicated workstations for access control environment
• Dedicated laptops for client equipment maintenance
• Educate staff on dangers of USB device attacks
Don’t Forget About File-Based attacks

Kathleen Schmidt
Registered Representative at New York Life Insurance Company, NYLIAC

SEP 29

Kathleen Schmidt • 1:28 PM
Hi Patrick. Thank you for connecting with me. There's an upcoming seminar that I know you'll find informative. If you can attend, please let me know and I'll save you a seat(s).

PDF
Finke Oct 3rd Invitation
552 KB

Write a message or attach a file
Email addresses

• Never underestimate the importance of your official email address
• Avoid using your professional email address for:
  • Social media registration
  • Job searching
  • Conference registration
What Can Be Done (Corporate)

Eliminate default passwords in equipment and software

California’s new "Information Privacy: Connected Devices" bill

• Comes into effect on January 1, 2020
• Applies to devices manufactured or sold in California
• Bans pre-installed and hard-coded default passwords on devices that are capable of connecting to the Internet
• Mandates device manufacturers to either create a unique password for each device at the time of production or require the user to create one when they interact with the device for the first time
What Can Be Done (Corporate)

• Test (and retest) your products internally and by an outside organization
  • New products
  • Existing products before major release

• Establish a vulnerability tracking and reporting program
  • How can individuals outside of the organization report a potential vulnerability?
  • Create a severity rating and tracking system
  • Remember that vulnerabilities exist on every system or piece of equipment—there is no shame in reporting them
What Can Be Done (Corporate)

• Know your hardware’s software
  • Create a master list of what third-party software is utilized in each device
  • Establish a procedure for monitoring publicly announced vulnerabilities of the third-party software components and integrating these findings into the vulnerability tracking system

• Create a security resource center for your integrators and end users
  • Create a process for alerting integrators and users of security issues and solutions
  • Include implementation and lockdown guides for your components and solutions
What Can Be Done (Corporate)

• Update your internal security awareness training programs
  • Remember, as a vendor, you are a prime target for attackers
  • Educate your employees on position-specific risks (field technician, customer service representative)
  • Take phishing attempts seriously and create an easy process for employees to report them

• Include cyber security in the development process—don’t try to add it later

• Remember that an effective security program is an on-going process
Valerie Thomas
@hacktress09
@securiconLLC