Automation & Hacking: Potential Impacts on Healthcare

December 08, 2022

TLP:CLEAR, ID# *202212081300*

Agenda

- Overview
- History of Automation
- Why Use Automation?
- Artificial Intelligence Hacking
- Common Uses
- Automation and the Cyber Kill Chain
- Automation in Cybersecurity

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Disclaimer

- The activities and information presented in this brief are for presentation and awareness purposes only. Using these resources and tools can result in criminal action and should not be attempted without the proper training, knowledge, and consultation with your organization.

- These tools and methods are not endorsed by HC3 or the HHS.

Overview

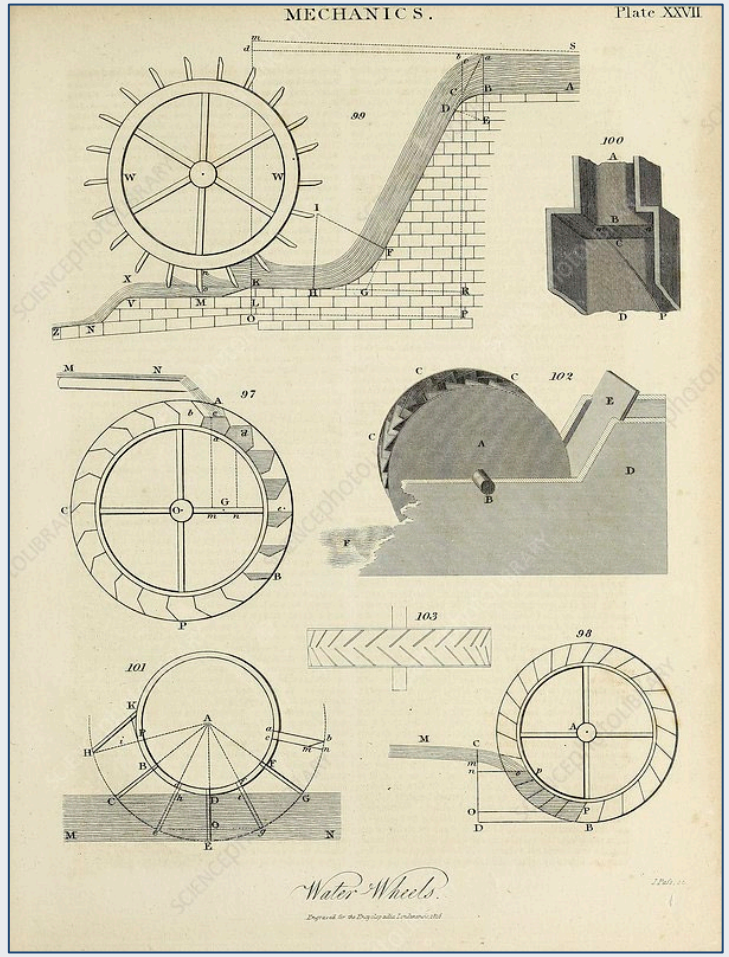
What is Automation?

- **Automation:** The use of largely automatic equipment in a system of manufacturing, or other production process
- Integration of technology
- Can be done with software or hardware
- Reduces the manual involvement of humans
- Automation in Cybersecurity
  - Penetration testing/hacking
  - Defensive measures
  - Machine learning and Artificial Intelligence
  - Automated Intelligence Collection

History of Automation

Timeline

- 27,000 BCE: Weighted fishing nets
- 1500 BCE: Use of sundials in Egypt
- 4th Century BCE: Use of water wheels in Mesopotamia
- 1436: Gutenberg's moveable printing press
- 1645: Pascal's mechanical calculator
- 1764: Watt's rotary-motion steam engine
- 1801: Jacquard's power loom
- 1830: Babbage's Analytical Engine
- 1913: Ford's moving assembly line
  - 1946: The term "automation" was officially coined
- 1943: Colossus, the first programmable computer
- 1971: Invention of microprocessors – The Digital Age



Source: SciencePhoto

Why Use Automation?

Why Use Automation?

- Lowers operating costs
- Increases production
- Increases competitive capabilities
- Consistent production and quality
  - Enables 24/7 operations
- Decreases hands-on requirements
- Reduces the need for outsourcing
  - Creation of in-house products
- Increases human efficiency
- Increases operational capabilities
- Decreases human labor

Source: Bicentennial Man *(1999)*

People Trust Robots

Artificial Intelligence is becoming more popular, and some studies have shown that people are more willing to trust robots over human judgement.

- Artificial Intelligence (AI) is becoming more common
  - 50% of people report using some type of AI
- 64% of people trust robots more than people
- 2016 Georgia Research Tech Institute Study
  - Tested to see if people would trust a robot during an emergency
  - Belief that robots know more
  - Robot made intentional mistakes early on
  - Humans still trusted the robot, despite errors

Popular Tools

There are many open-source tools available that are not only easily accessible, but also have strong support documentation on using them.

Tools

- Nmap
- Wireshark
- Legion
- Jok3r
- Zed Proxy Attack
- Nikto2
- OpenSCAP
- SqImap
- Scapy
- CrackStation

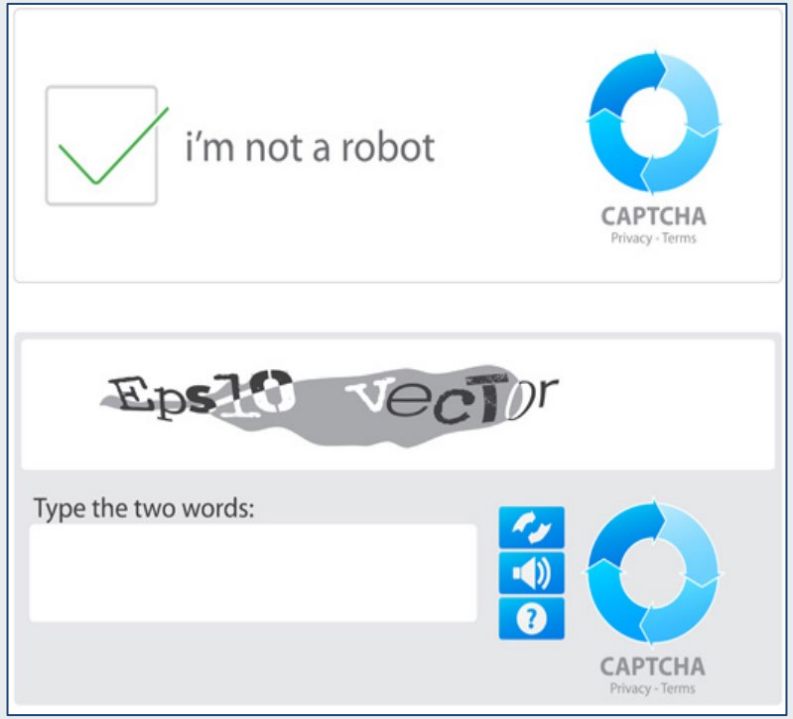
Accessibility

- Ease of implementation
- Level of automation
- Configurable to tune out false positives
- Compatibility with existing tools
- Clarity and comprehensiveness of results and reports
- Good support and technical documentation

Artificial Intelligence Hacking

Artificial Intelligence Hacking

- Considered speculative technology
- Deep Learning
- Building better malware
- Creating deepfake data
  - Impersonation on social networking platforms
- AI-supported password guessing
  - Password Generative Adversarial Network (PassGANS)
  - Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)
- Machine Learning-enabled penetration testing tools



Source: Futuretimeline

Mayhem

- Winner of The Defense Advanced Research Projects Agency (DARPA) Cyber Grand Challenge
  - Crashed 40 rounds in with 55 rounds remaining
- First machine to enter The Defense Readiness Condition (DEFCON) Capture the Flag
  - 96-round, time-based competitive hacking event
- Can automatically:
  - Detect
  - Exploit
  - Patch
- Accomplished this through “fuzzing” and “symbolic” execution
  - Intelligent guesses and formally finding exploits

Source: blog.rittal

Uses of Automation

Uses of Automation

- **Data Breaches and Sales**
- Large number of data breaches
- Historically, data has strong value on the dark web
- Time consuming for attackers for manually go through everything
- Use of automated software to identify valuable information
  - Emails
  - Passwords
  - Credit cards
  - Personal/sensitive information

Uses of Automation, Part 2

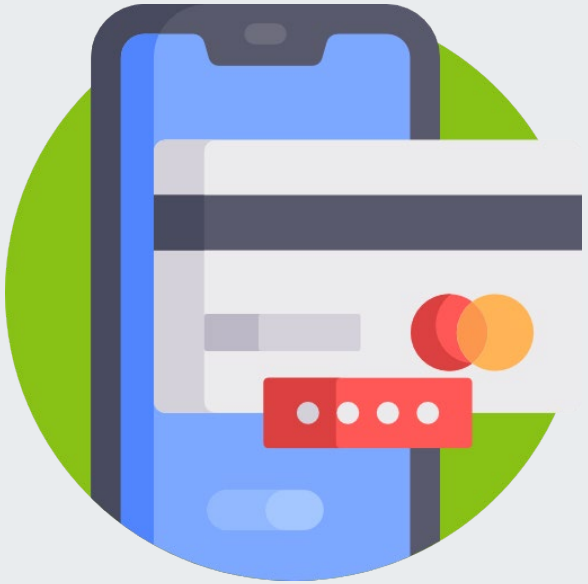
- **Credential Stuffing and Brute Force Attacks**
- One of the most common types of automated attacks
- Using stolen or commonly used passwords
  - Software can fully automate this attack
- Fully automated password cracking tools

- **Loaders and Cryptors**
- Enables obfuscation and delivery of payloads
- Premade software allows for use by lower skill levels

Uses of Automation, Part 3

- **Keyloggers**
- Preconfigured tools for harvesting credentials
- Monitors user activity

- **Banking Injects**
- Modules combined with Trojans
- Redirects you from a legitimate site
- Steals credentials
- Has gone for four figures on the dark web



Autosploit and Easysploit

- **Autosploit**
  - Combines Shodan and Metasploit
  - Uses Shodan to find targets
  - Uses Metasploit to automate exploits
  - Available on GitHub

- **Easysploit**
  - Runs Metasploit through an automated tool
  - Attacks systems with different operating systems
  - Can download files
  - Can monitor keystrokes
  - Available on GitHub

Spam/Phishing

- Spam: Unsolicited emails, instant messages, phone calls, or other messages
  - Typically, easy to recognize
  - Solicitation of goods or services
  - Sent to a bulk number of email addresses
- Phishing: An email sent from a cybercriminal that is intended to look legitimate
  - Malicious in nature
  - Wants to reveal sensitive information
  - Deploys malware
- One of the easiest types of cyber crime
  - Automated software can generate email addresses

Blackeye

- Open-source tool
- Phishing templates
- Harvests credentials
- Can be downloaded from GitHub
- Free tutorials and literature online
- Stopped being supported due to abuse

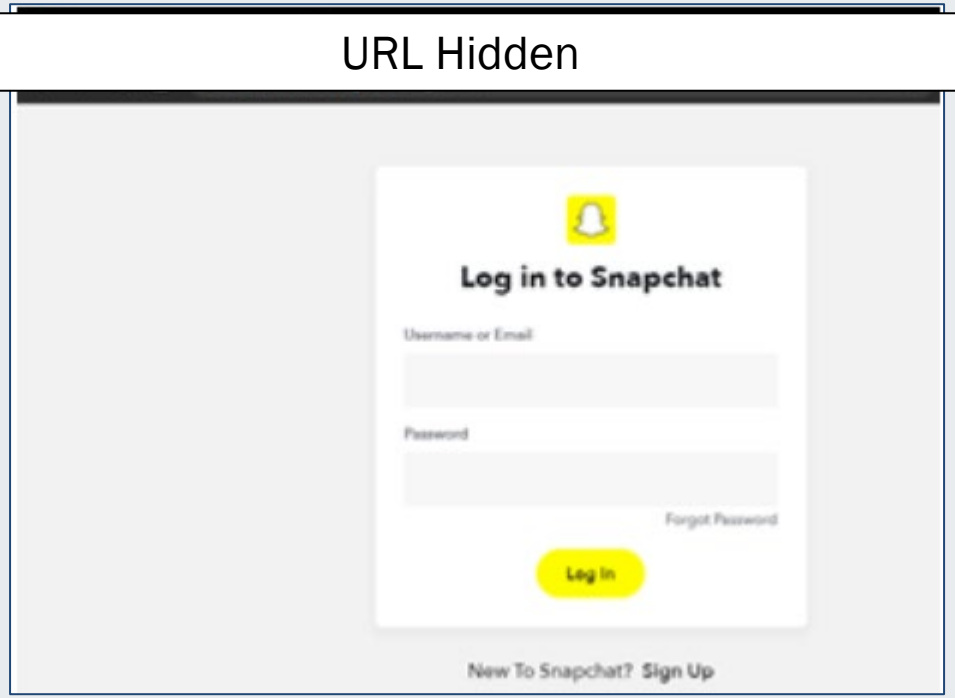
Blackeye

```
:: Disclaimer: Developers assume no liability and are not   ::
:: responsible for any misuse or damage caused by BlackEye. ::
:: Only use for educational purporses!!                     ::

:: Attacking targets without mutual consent is illegal!     ::

01] Instagram      [17] IGFollowers   [33] Custom     BLACKEYE  v1.1
02] Facebook       [18] eBay
03] Snapchat       [19] Pinterest
04] Twitter        [20] CryptoCurrency
05] Github         [21] Verizon
06] Google         [22] DropBox
07] Spotify        [23] Adobe ID
08] Netflix        [24] Shopify
09] PayPal         [25] Messenger
10] Origin         [26] GitLab
11] Steam          [27] Twitch
12] Yahoo          [28] MySpace
13] Linkedin       [29] Badoo
14] Protonmail     [30] VK
15] Wordpress      [31] Yandex
16] Microsoft      [32] devianART

CODED BY:  @thelinuxchoice
UPGRADED BY: @suljot_gjoka

*] Choose an option: 2
*] Put your local IP (Default 192.168.1.19):
*] Starting php server...
*] Send this link to the Victim: 192.168.1.19
*] Waiting victim open the link ...
```

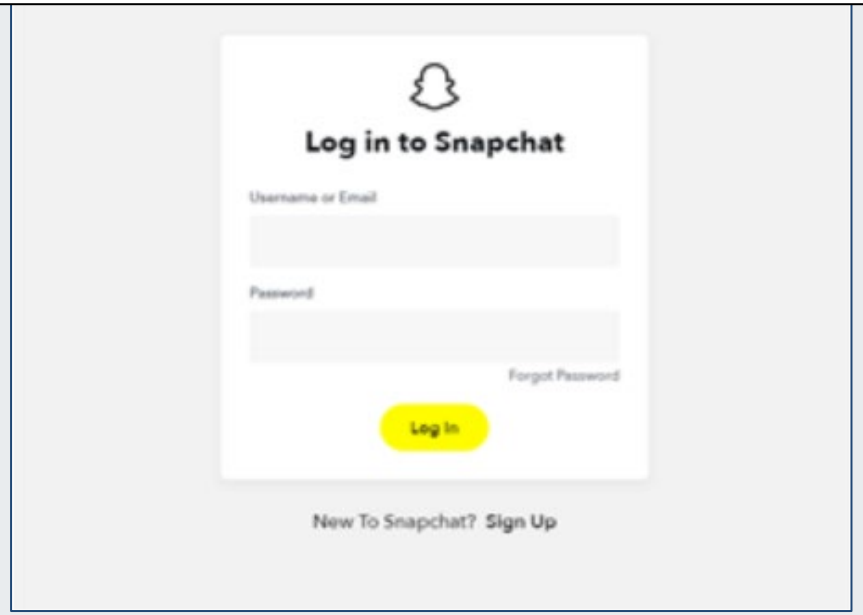
Source: Kalitut

Blackeye Template: SnapChat

URL Hidden



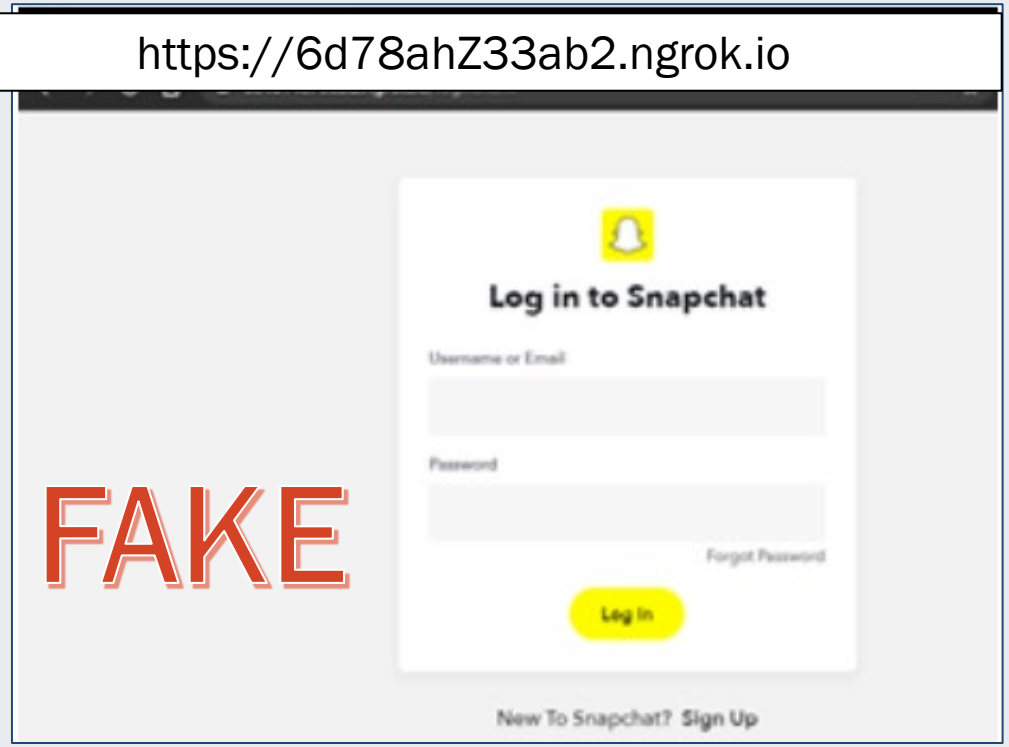
URL Hidden



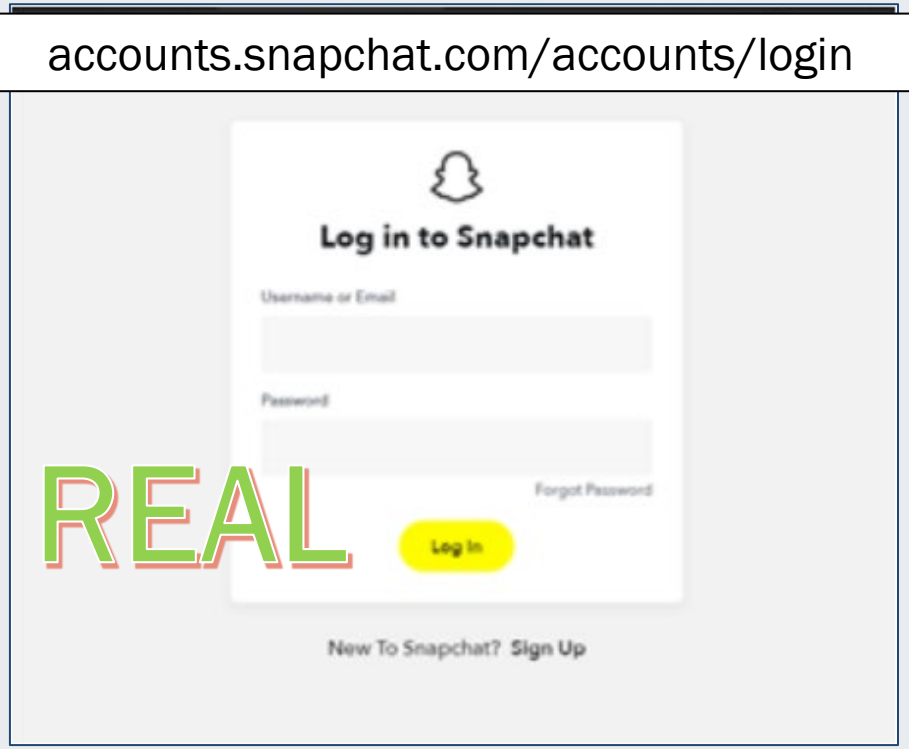
Source: ritsec.wordpress

Blackeye Template: SnapChat, Part 2

https://6d78ahZ33ab2.ngrok.io



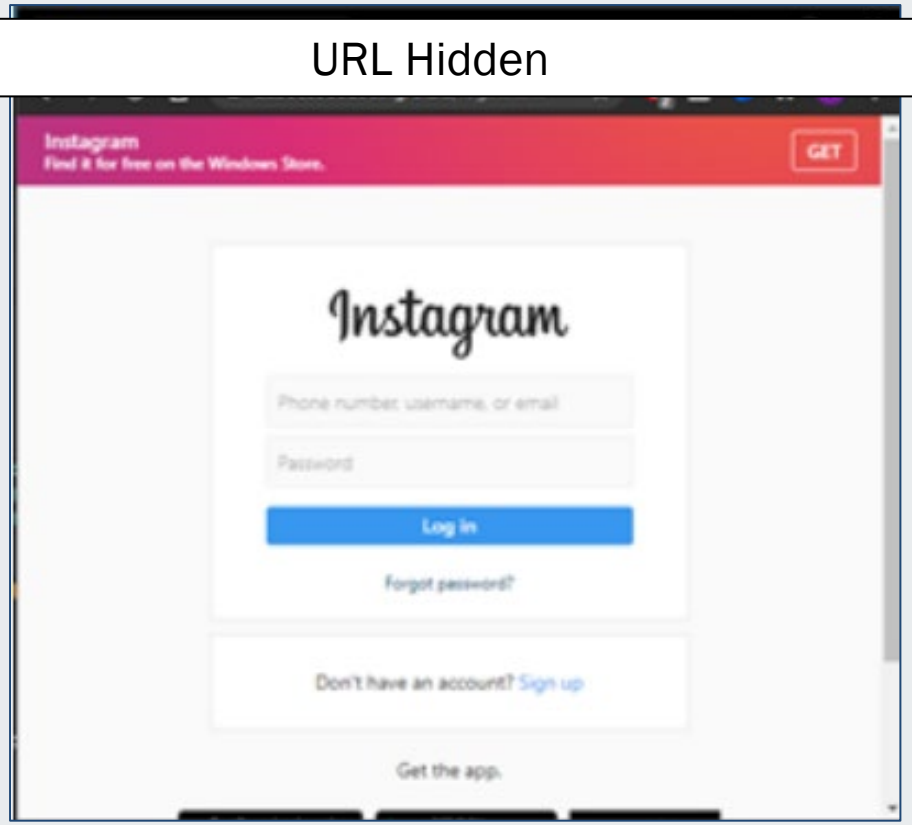
accounts.snapchat.com/accounts/login



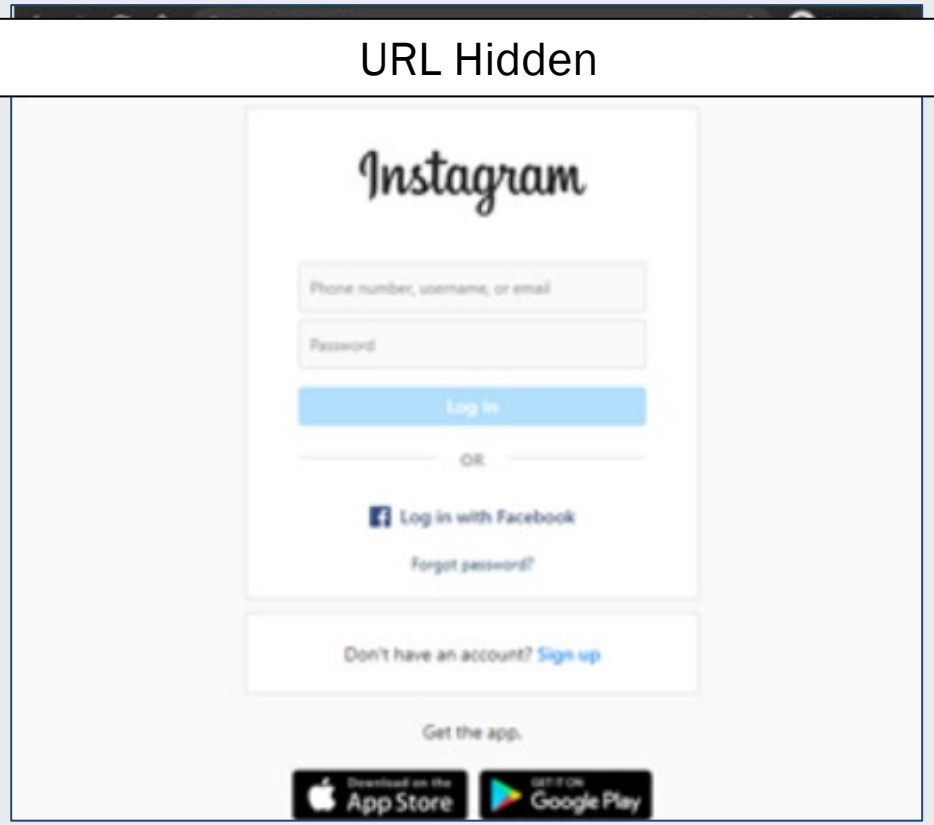
Source: ritsec.wordpress

Blackeye Template: Instagram

URL Hidden



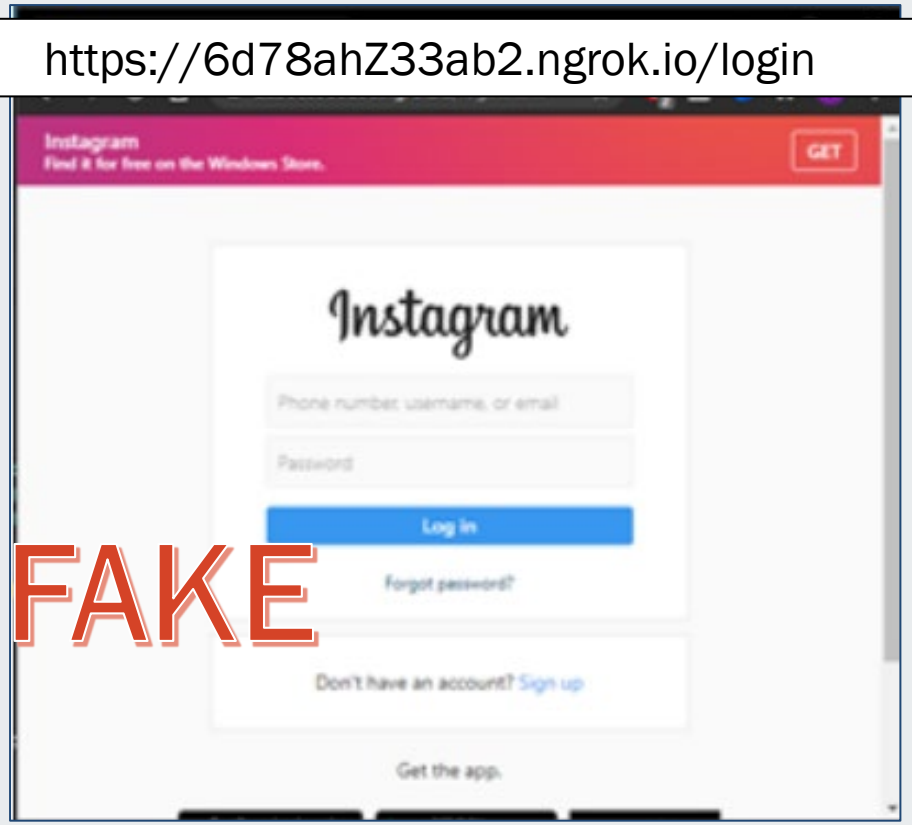
URL Hidden



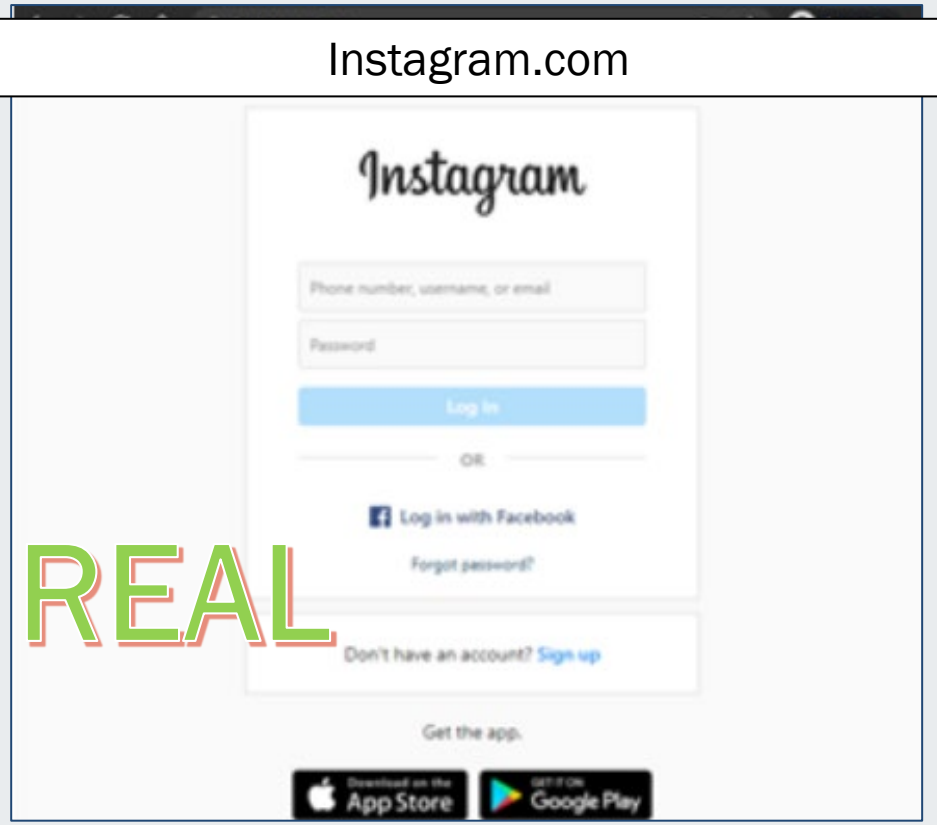
Source: ritsec.wordpress

Blackeye Template: Instagram, Part 2

https://6d78ahZ33ab2.ngrok.io/login



Instagram.com



Source: ritsec.wordpress

Network Mapper (Nmap)

- Free and open-source tool
- Created in 1997
- Can be used on multiple operating systems (OS)
- Still popular today
- Can be used for:
  - Vulnerability scanning
  - Port scanning
  - Network mapping
- Powerful reconnaissance tool
- Originally required advanced programming skills
  - Easier to use today

Source: rafed.github

Vulnerability Scanning

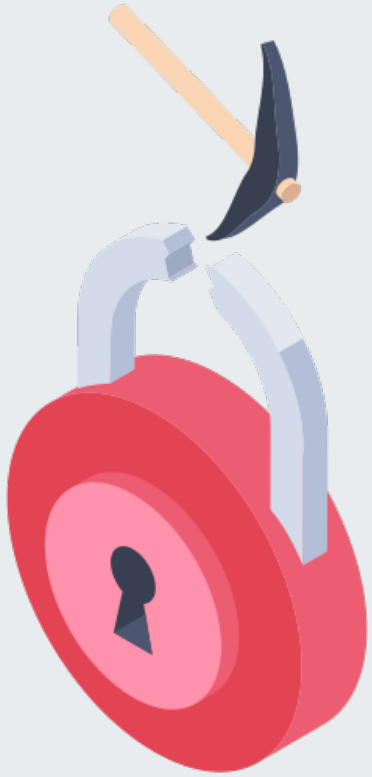
- nmap -sV –script=vulscan/vulscan.nse 192.167.1.105
- Nmap scan report for 192.167.1.105 Host is up
- Not shown: 999 closed ports
- PORT STATE SERVICE VERSION
- 53/tcp open domain

- [CVE-2013-0198] (description)
- [CVE-2012-3411] (description)
- [CVE-2009-2958] (description)

Automation and the Cyber Kill Chain

The Cyber Kill Chain

- The Cyber Kill Chain was developed by Lockheed Martin in 2011
  - An evolved form of the kill chain for cyber attacks
- Originally a military concept for identifying the structure of an attack
  - Step-by-step approach for stopping enemy activity
- Typically used as a defense tool against advanced threat actors
- Consists of seven phases:
  - Phase 1: Reconnaissance
  - Phase 2: Weaponization
  - Phase 3: Delivery
  - Phase 4: Exploitation
  - Phase 5: Installation
  - Phase 6: Command and Control
  - Phase 7: Actions on Objective



Reconnaissance

During the Reconnaissance phase, a malicious attack will search for information and weaknesses on a target. By incorporating automation, an attacker can advance to the phase quicker.

Adversary

- Harvest email addresses
- Identify employees
- Collect other media information
- Discover Internet-facing servers

Defender

- Collect website visitor logs/alerts
- Collaborate with web administrators
- Build detections for browsing behaviors
- Prioritize defense around recon activity
  - Technology and people

Tool: Nmap

Weaponization

In the Weaponization phase, the adversaries are in a preparation phase for their operation. Malware creation is more than likely not made from scratch, and automation-based tools will be used.

Adversary

- Obtain a weapon, either made or acquired
- For file-based exploits, select a “decoy” document
- Select backdoor implant and C2
- Designate “mission ID” and embed the malware
- Compile backdoor and weaponize the payload

Defender

- Conduct malware analysis
- Build detections, observe new campaigns
- Analyze timeline of when malware was created versus when it was used
- Collect files and metadata
- Determine which artifacts are relevant to which APTs

Tool: Metasploit, Luckystrike

Delivery

In the Delivery phase, the adversary will be launching their operations. This is an important phase where defenders will want to prevent the operation from happening.

Adversary

- Adversary-controlled delivery:
  - Direct against web servers
- Adversary-released delivery:
  - Malicious email
  - Malicious USB stick
  - Social media contact
  - Watering holes

Tool: Blackeye

Defender

- Analyze the delivery method
- Understand why the target was chosen
  - Targeted server or individual roles
- Infer intent based of targeting
- Leverage weapon artifacts to detect payloads
- Consider the time of day that the operation started
- Collect web logs and emails to conduct forensics

Exploitation

At this phase, the attacker needs to exploit a vulnerability to gain access.

Adversary

- Software, hardware, or human vulnerability
- Acquire or develop a zero-day exploit
- Trigger server-based vulnerabilities
- Trigger human-based exploits
  - Clicking malicious emails

Defender

- User awareness training
- Secure code training
- Vulnerability scanning /penetration testing
- Endpoint hardening
- Endpoint process auditing

Installation

Typically, an attacker will install a backdoor or some type of implant in the victim's environment to maintain access to it.

Adversary

- Install web shell on web server
- Install backdoor/implants
- Create persistence
  - Add services, auto-run keys, etc.
- May "time stomp" a file
  - Helps a malware appear normal

Tools: The Backdoor Factory, backdoorme

Defender

- Block common installation paths
- Understand what privileges a malware needs
- Endpoint auditing to detect abnormal files
- Understand malware compile time

Command and Control (C2)

In this phase, the malware will open a communications channel so that the adversary can remotely manipulate a victim's environment.

Adversary

- Open a two-way communication channel
- Usually C2 is done through web, DNS, and email protocols
- C2 infrastructure can be the adversaries or another victim network

Defender

- Discover C2
  - Malware analysis
- Harden network
- Customize blocks on C2 protocols
- Conduct open-source research to discover C2 infrastructure

Tools: Cobalt Strike, PoshC2, Merlin

Actions on Objective

At the final phase, the adversary will attempt to accomplish whatever their objectives are.

Adversary

- Collect credentials
- Privilege escalation
- Internal reconnaissance
- Lateral movement
- Collect and exfiltrate data
- Destroy systems
- Corrupt or modify data

Defender

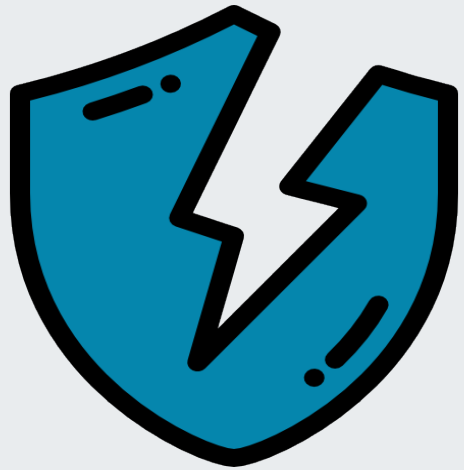
- Establish incident response actions
- Detect data exfiltration
- Detect lateral movement
- Detect unauthorized credential use
- Deploy forensic agents
- Capture network packet activity
- Conduct triage/damage assessments

Automated Cybersecurity

Blue Team Uses

Many tools were created with ethical intent to help make a system more secure, but plenty of them have a history of being misused.

- Many of these tools are also used defensively
- Security Information & Event Management tools
- Automated Cyber Intelligence Tools
  - Threat Intelligence feeds
- Automated Mitigation
  - Can suggest recommended actions
- Expected to be more sophisticated in the future



Cybersecurity Automation Tools

- Security Monitoring and Alerting Tool (SMAAT)
  - Tool that can help conduct surveillance on a system
  - Will alert to potential security incidents
- Vulnerability Management Tools
  - Tools that can scan for vulnerabilities
- Network Intrusion Detection Systems (NIDS)
  - Helps monitor traffic to detect potentially malicious activity
- Network Intrusion Prevention Systems (NIPS)
  - Helps monitor traffic to block potentially malicious activity

Reference Materials

References

- Arazi, Eyai. “Cybercriminals Use Automation, Here is Why You Should Too”. Radware. Nov 4, 2021. https://blog.radware.com/cloud-security-3/2021/11/cybercriminals-use-automation-here-is-why-you-should-too/
- “Artificial Intelligence”. NIST. https://www.nist.gov/artificial-intelligence
- “Autosploit: Automated Mass Exploiter”. Cyberpunk. https://www.cyberpunk.rs/autosploit-automated-mass-exploiter
- Admin. “Network Reconnaissance Using Nmap - One STOP Solution”. Golinuxcloud. https://www.golinuxcloud.com/network-reconnaissance-using-nmap/#Overview_on_Network_Reconnaissance
- Buchanan, Ben. Bansemer, John. Cary, Dakota. Lucas, Jack. Musser, Micah. “Automating Cyber Attacks”. CSET. Nov 2020. https://cset.georgetown.edu/publication/automating-cyber-attacks/
- Bong, Nathan. “The Evolution of Automation”. Progressiveautomations. Aug 26, 2022. https://www.progressiveautomations.com/blogs/news/the-evolution-of-automation

References

- Borges, Esteban. “How to Detect CVEs Using Nmap Vulnerability Scan Scripts”. Securitytrails. May 26, 2020. https://securitytrails.com/blog/nmap-vulnerability-scan
- Cobb, Michael. “11 open source automated penetration testing tools”. Techtarget. https://www.techtarget.com/searchsecurity/tip/11-open-source-automated-penetration-testing-tools
- Coberly, Cohen. “Mayhem is a machine that can automatically detect, exploit, and patch cybersecurity vulnerabilities” techspot. Jan 30, 2019. https://www.techspot.com/news/78494-mayhem-machine-can-automatically-detect-exploit-patch-cybersecurity.html
- Crowdstrike. “WHAT IS THE **CYBER KILL CHAIN?** PROCESS & MODE”. Oct 14, 2022. https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/
- Donahole, Stephanie. “A New Tool for Hackers – AI in Cybersecurity”. GlobalSign. Aug 28, 2019. https://www.globalsign.com/en/blog/new-tool-for-hackers-ai-cybersecurity
- “EasySploit: MetaSploit Automation Tool”. Cyberpunk. https://www.cyberpunk.rs/easysploit-metasploit-automation-tool

References

- Griffin, Mathew. “BREAKTHROUGH AI HACKING TOOL CRACKS MILLIONS OF USER PASSWORDS IN MINUTES”. 311institute. Jan 12, 2019. https://www.311institute.com/breakthrough-ai-hacking-tool-cracks-millions-of-user-passwords-in-minutes/
- Georgia Institute of Technology. “In emergencies, should you trust a robot?”. Sciencedaily. Feb 29, 2016. https://www.sciencedaily.com/releases/2016/02/160229095951.htm
- Groover, Mikell. “automation”. Britannica. https://www.britannica.com/technology/automation
- Kaufman, Mitch. “A Brief History of Automation” Excela. July 23, 2020. https://www.exelatech.com/blog/brief-history-automation?language_content_entity=en
- Künzli, Pascal. “The History of Automation”. Prautomation. The History of Automation - PR Automation
- Krenn, Robert. “Editorial: Automated Hacking”. Cybersprint. Dec 21, 2021. https://www.cybersprint.com/blog/editorial-automated-hacking
- Cybersecurity-automation. “Examples of Cyber Security Automation Tools”. https://www.cybersecurity-automation.com/examples-of-cyber-security-automation-tools/

References

- Ramakrishnan, Vishnu. “Analysis of Current Machine Learning and AI Techniques to Perform Automated Hacking” Fall 2020-Winter 2021. https://era.library.ualberta.ca/items/7f13e223-fef8-4b28-b643-a53e7f8b59cf
- Palmer, Danny. “Cybersecurity warning: 10 ways hackers are using automation to boost their attacks”. Zdnet. Mar 25, 2020. https://www.zdnet.com/article/cybersecurity-warning-10-ways-hackers-are-using-automation-to-boost-their-attacks/
- Krenn, Robert. “The Rise of Automated Hacking”. Infosecurity. Jun 13, 2019. https://www.infosecurity-magazine.com/infosec/the-rise-of-automated-hacking-1-1-1/
- Townsend, Kevin. “AutoSploit: Automated Hacking Tool Set to Wreak Havoc or a Tempest in a Teapot?” securityweek. Feb 01, 2018. https://www.securityweek.com/autosploit-automated-hacking-tool-set-wreak-havoc-or-tempest-teapot
- Korolov, Maria. “9 ways hackers will use machine learning to launch attacks” csoonline. Jun 13, 2022. https://www.csoonline.com/article/3250144/6-ways-hackers-will-use-machine-learning-to-launch-attacks.html
- Schneier, Bruce. “The Coming AI Hacker”. Belfercenter. April 2021. https://www.belfercenter.org/sites/default/files/2021-04/HackingAI.pdf

References

- Meah, John. “AI in Cybersecurity: The Future of Hacking is Here”. Techopedia. Aug 26, 2022. https://www.techopedia.com/ai-in-cybersecurity-the-future-of-hacking-is-here/2/34520
- Schneier, Bruce. “The Coming AI Hackers”. Schneier. https://www.schneier.com/academic/archives/2021/04/the-coming-ai-hackers.html
- Zaware, Trupti. “CYBERSECURITY AUTOMATION USING CYBER KILL CHAIN”. Irjmets. https://www.irjmets.com/uploadedfiles/paper/issue_9_september_2022/29648/final/fin_irjmets1662317451.pdf
- Hsu, Jeremy. “Should Humans Trust Robots?”. Discovermagazine. Mar 01, 2016. https://www.discovermagazine.com/technology/should-humans-trust-robots
- “Gaining the Advantage Applying Cyber Kill Chain”. Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

References

- Shuttleworth, Martyn. “Heron’s Inventions”. Explorable. https://explorable.com/heron-inventions
- Freiberger, Paul. “Pascaline”. Britannica. https://www.britannica.com/technology/Pascaline
- Hatch, Nicolas. “James Watt’s Steam Engine and the Start of the Industrial Revolution”. https://stmuscholars.org/james-watts-steam-engine-and-the-start-of-the-industrial-revolution/
- Brownlee, Jason. “What is Deep Learning”. Machinelearningmastery. August 19, 2019. https://machinelearningmastery.com/what-is-deep-learning/
- Blondale, Aaron. “Using Blackeye to Deploy False Login Pages for Phishing Attacks”. Ritcsec.wordpress. May 09. 2021. https://ritcsec.wordpress.com/2021/05/09/using-blackeye-to-deploy-false-login-pages-for-phishing-attacks/
- Prokopets, Marie. “The Ultimate Manual for For Nmap Vulnerability Scanning”. Nira. https://nira.com/nmap-vulnerability-scanning/
- “Benefits of Automation”. Productivity. https://www.productivity.com/benefits-of-automation/

Questions

FAQ

Upcoming Briefing

- January 12, 2023 – 2022 Healthcare Cybersecurity Year in Review and 2023 Look-Ahead

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

CPE Credits

This 1-hour presentation by HHS HC3 provides you with 1 hour of CPE credits based on your Certification needs.

The areas that qualify for CPE credits are Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security.

Typically, you will earn 1 CPE credit per 1 hour time spent in an activity. You can report CPE credits in 0.25, 0.50 and 0.75 increments.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

HHS.GOV/HC3

HC3@HHS.GOV