KnowBe4
Human error. Conquered.

Top 5 Cloud Security Hacks and How You Can Avoid Them

Roger A. Grimes
Data-Driven Security Evangelist
rogerg@knowbe4.com

Roger A. Grimes
Data-Driven Defense Evangelist
KnowBe4, Inc.

e: rogerg@knowbe4.com
Twitter: @RogerAGrimes
LinkedIn: https://www.linkedin.com/in/rogeragrimes/

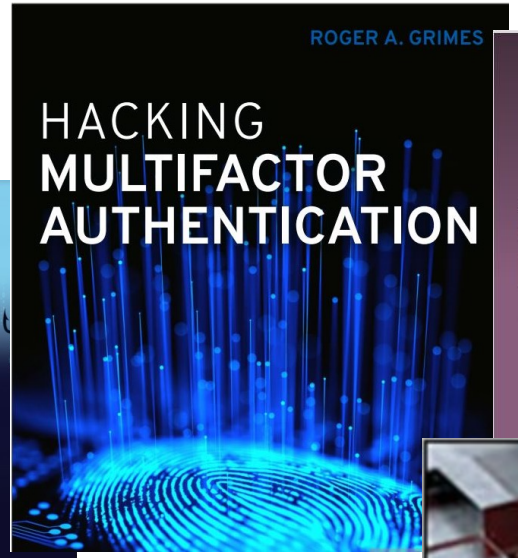
About Roger

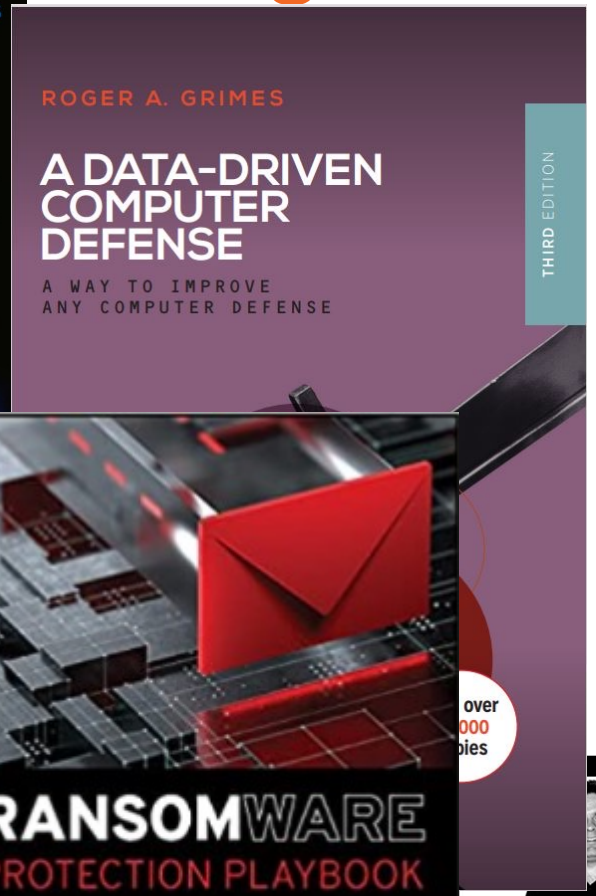
- 35 years plus in computer security, 20 years pen testing
- Expertise in host and network security, IdM, crypto, PKI, APT, honeypot, cloud security
- Consultant to world's largest companies and militaries for decades
- Previous worked for Foundstone, McAfee, Microsoft
- Written 14 books and over 1,300 magazine articles
- *InfoWorld* and *CSO* weekly security columnist 2005 - 2019
- Frequently interviewed by magazines (e.g. Newsweek) and radio shows (e.g. NPR's All Things Considered)

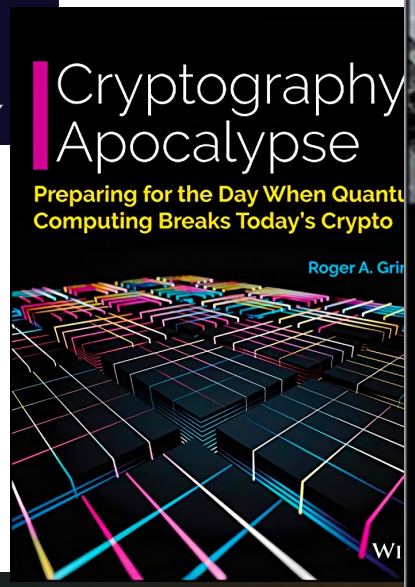
Certification exams passed include:

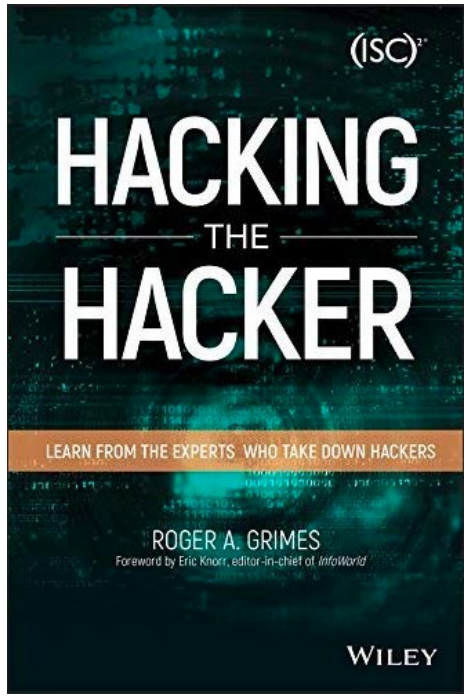
- CPA
- CISSP
- CISM, CISA
- MCSE: Security, MCP, MVP
- CEH, TISCA, Security+, CHFI
- yada, yada

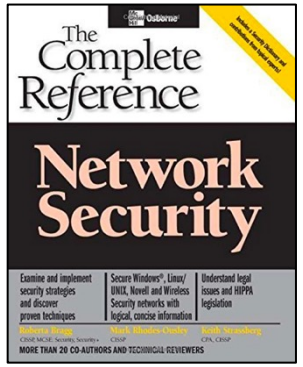
Roger's Books

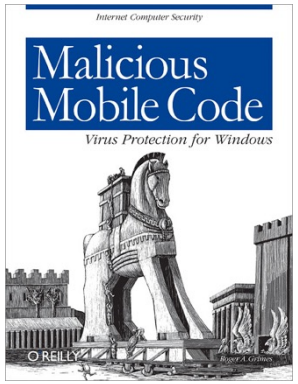


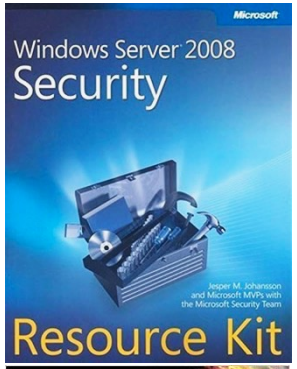


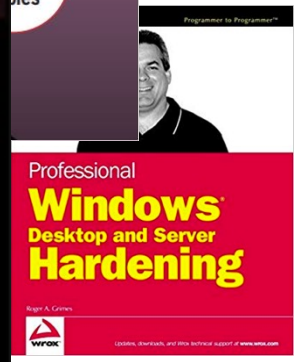


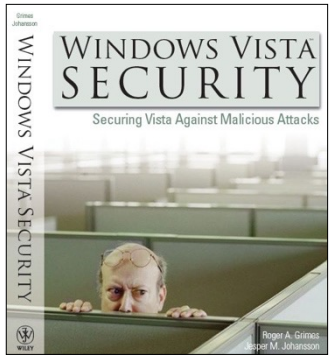


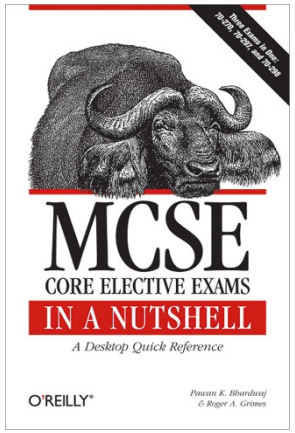


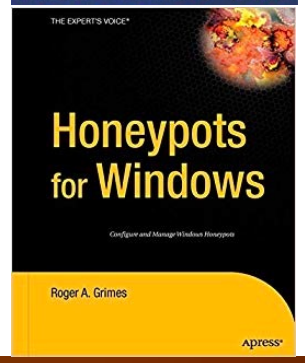








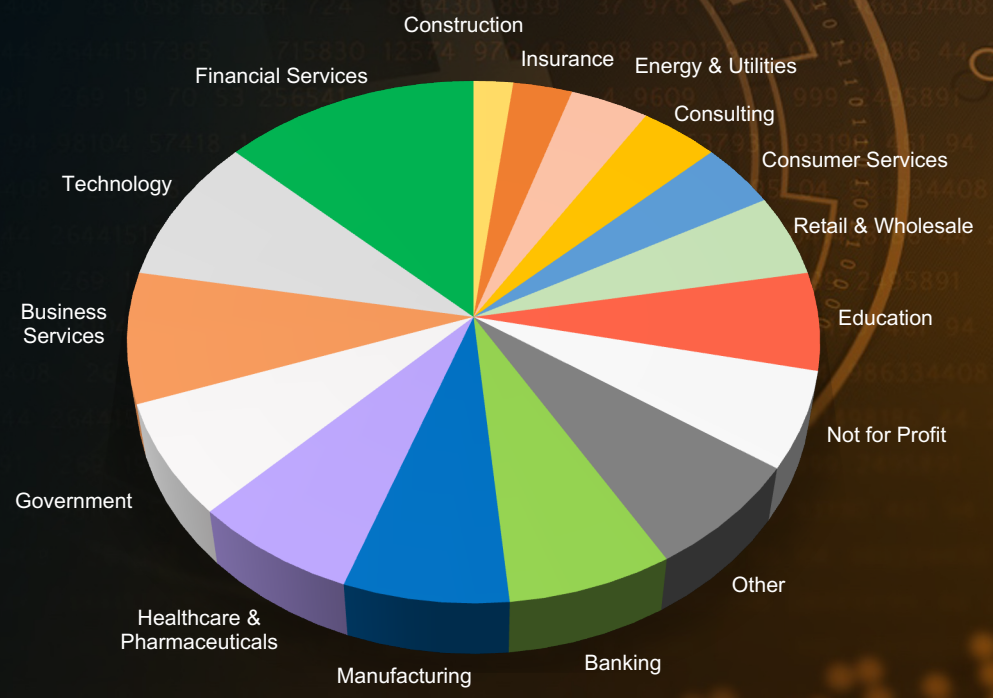




Over

60,000

Customers



About Us

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

FORRESTER® WAVE LEADER 2022 Security Awareness And Training Solutions

AMERICA'S FASTEST-GROWING Inc. 500 PRIVATE COMPANIES

Gartner peerinsights customers' choice 2021 ™

Today's Presentation

- Cloud Security Alliance Top 11
- Better Way of Thinking About Cloud Security Threats
- Top Cloud Security Threats

Agenda

- Cloud Security Alliance Top 11 Threats
- Better Way of Thinking About Cloud Security Threats
- Top Cloud Security Threats

CSA Top 11

Cloud Security Alliance (CSA)

- https://cloudsecurityalliance.org
- Formed in 2008, most respected cloud security organization
- 35 active working groups
- Chapters around the world

CSA Top 11

Cloud Security Alliance (CSA)

Top Threats to Cloud Computing: Pandemic 11 Deep Dive report

- https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven-deep-dive/
- Considered one of the best reports on the state of cloud security
- Different report with a different “cool” name each year

CSA Top 11

Top Cloud Threats Coverage

In the 2022 "*Top Threats* to Cloud Computing - Pandemic Eleven" report, we surveyed over 700 industry experts on security issues in the cloud industry. Our respondents identified eleven important security issues to their cloud environment (ranked in order of concern indicated by the survey:

PE1. Insufficient Identity, Credentials, Access, and Key Management	PE7. System Vulnerabilities
PE2. Insecure Interfaces and APIs	PE8. Accidental Cloud Data Disclosure
PE3. Misconfiguration and Inadequate Change Control	PE9. Misconfiguration and Exploitation of Serverless and Container Workloads
PE4. Lack of Cloud Security Architecture and Strategy	PE10. Organized Crime/Hackers/APT
PE5. Insecure Software Development	PE11. Cloud Storage Data Exfiltration
PE6. Unsecured Third-Party Resources	

CSA Top 11

CSA Top 11 Report Weaknesses

I love the CSA and the education they provide, but…

- It's a survey of gut feelings, not actual data
  - The world is full of experts fearing lots of non-critical critical threats
- Doesn't include some types of attacks, DDoS, etc.
- Seems a bit vendor-driven at times
- Relevance rankings not backed by hard data
- It's a hodge-podge mix of threats and causes of threats
  - Data exfiltrations are outcomes of threats and risks, not a threat
  - Data exfiltrations occur because of everything else
- Still a great report that should be read by all cloud users and providers

Agenda

- Cloud Security Alliance Top 11
- Better Way of Thinking About Cloud Security Threats
- Top Cloud Security Threats

Data-Driven Defense

Better Way of Thinking About Cloud Security

- Real Data Should Drive Risk Relevance
- Focus on Root Causes of Initial Exploits
- Mitigate Top Root Causes First and Best
- Communicate Top Root Causes and Planned Defenses Across Teams and Organization

If you are interested in more on this subject:

- https://info.knowbe4.com/webinar-grimes-computer-security-defenses
- https://www.amazon.com/Data-Driven-Computer-Defense-Should-Using/dp/B0BR9KS3ZF
- http://aka.ms/datadrivendefense

Focus on Root Causes

You should care most about root causes of initial breaches

Ransomware isn't the problem. Pass-the-hash-attacks aren't the problem

Focusing on individual threats and only what they did after they got in is like worrying about your brakes after your car is stolen

When you've adjusted your thinking, adware is as worrisome as a malicious backdoor remote access Trojan or ransomware

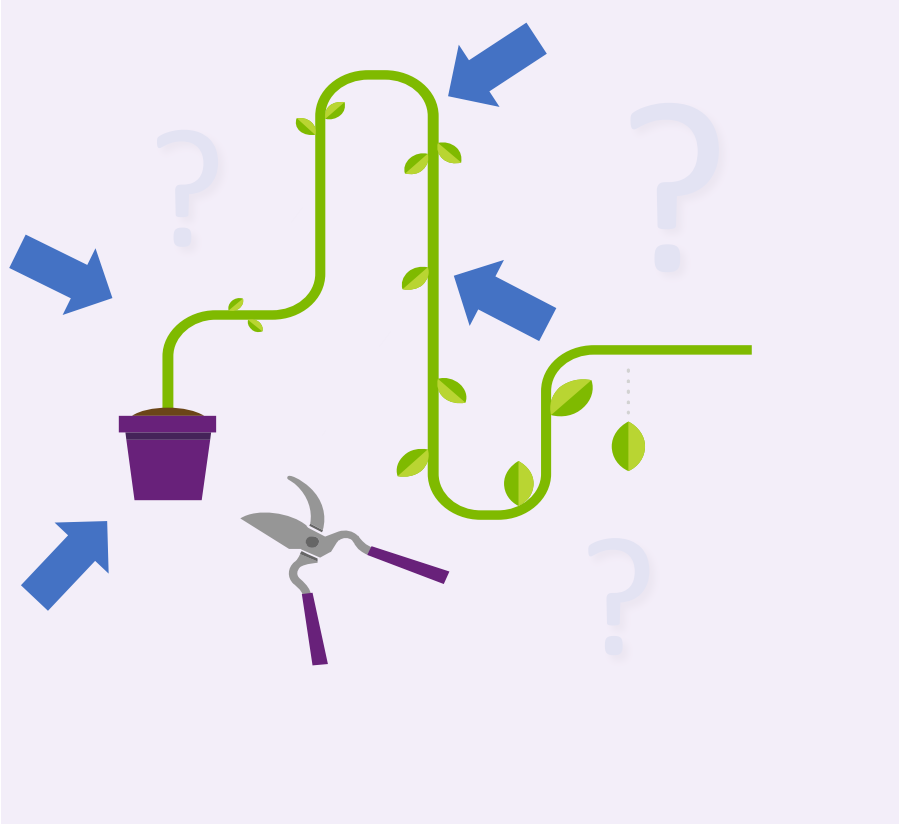
<u>Both took the same effort to get into your environment</u> and is revealing defensive gaps

Focus on Root Causes

How attackers/malware break in

What's the number one initial root exploit in your environment?

- Social Engineering
- Programming Bug (patch available or not available)
- Authentication Attack
- Malicious Instructions/Scripting
- Data Malformation
- Human Error/Misconfiguration
- Eavesdropping/MitM
- Side Channel/Information Leak
- Brute Force/Computational
- Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue (supply chain/vendor/partner/etc.)
- Physical Attack

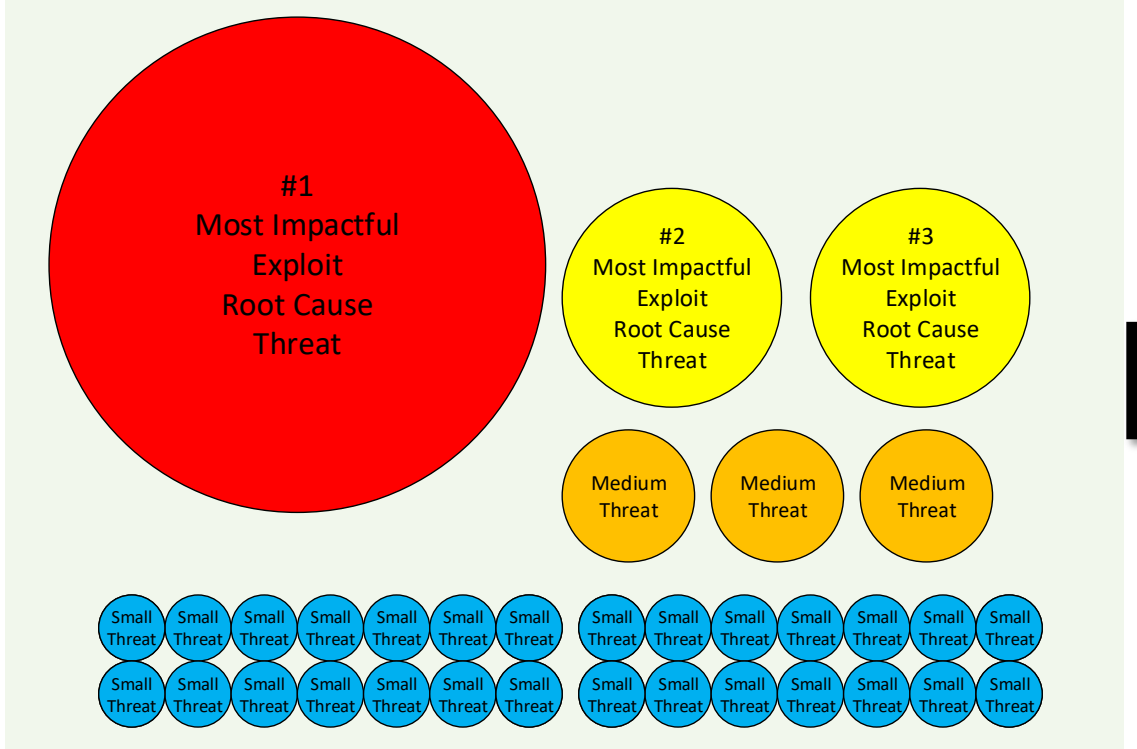


Ask Yourself 3 Key Questions:

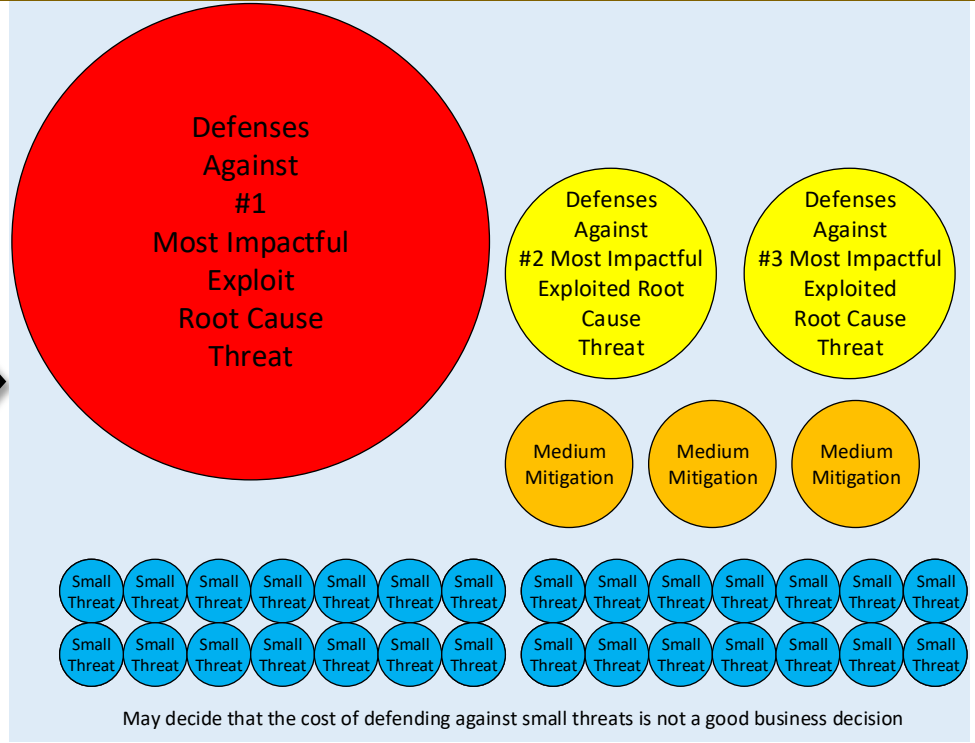
1. Can your team correctly answer what is the top initial exploit cause?
2. Is the answer consistent across all stakeholders?
3. Do you have data to back up the right answer?

The Data-Driven Defenders Approach

The Data-Driven Threat Perception



Data-Driven Defense Application



Risk Ranked Threat Perceptions:

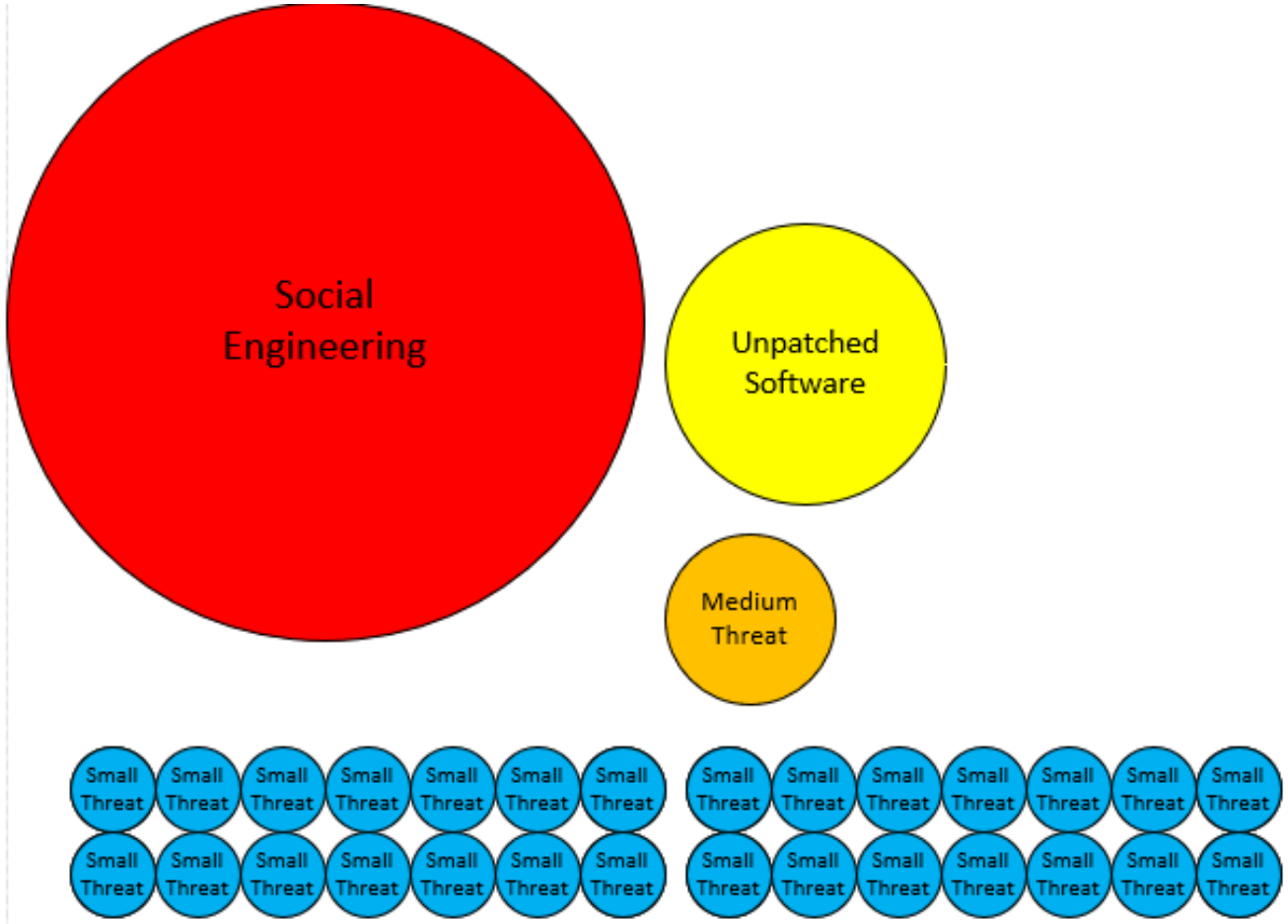
- Focuses on root causes
- Local experience and data is highly valued
- Relevance is a big deciding factor

Risk Ranked Defenses:

- Mitigates root causes, not individual threats
- More efficient resource utilization
- Allows clearer cost/benefit considerations

Biggest Initial Breach Root Causes for Most Companies

- Social Engineering
- Unpatched Software



Preventative Controls

- Technical
- Training

Social engineering is responsible for 70% - 90% of all malicious data breaches

Agenda

- Cloud Security Alliance Top 11
- Better Way of Thinking About Cloud Security Threats
- Top Cloud Security Threats

It’s Not These, As Previously Expected

Cloud Security Issues We Were Always Worried About But You Don’t See (Much of if any) In The Real-World (Yet)

- Tenant co-mingling/collisions
- Cloud-based malware
- Virtual machine client-to-client or host-to-client or client-to-host attacks
- Malicious undeletion
- Data Ownership issues

- Real issues that are causing problems aren’t as “sexy”…

Top Cloud Security Threats

Summary

- Social Engineering (is the top threat)
- Logon/Authentication Issues
- Overly Permissive Permissions
- Unpatched Software (and Firmware)
- Insecure APIs

Social Engineering

- Examples

Dropbox | 2022

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal: Dropbox developers were successfully targeted with phishing	*Phishing via email and website*	*Insufficient phishing training* *3rd- and 4th-party process management and authentication risks* **PE1** Insufficient Identity, Credentials, Access, Key Management	**PE11** *Cloud Storage Data Exfiltration* Company's code leaked, inclusive of in-code secrets Additionally, PII of Dropbox employees was leaked	**Financial** - Dropbox stock lost 6% but quickly recovered **Operational** - Incident response - Forensics analysis - Revoking the stolen GitHub credentials and rotating relevant keys **Compliance** - Possible violations of some SOC and ISO controls **Reputational** - Comprehensive coverage of media breach	**Preventive** - CEK-21 - CEK-11 - IAM-11 - IAM-14 - STA-02 - HRS-11 **Detective** - LOG-01 - LOG-05 **Corrective** - AIS-04 - CEK-19 - STA-07
External: Unidentified threat actors		**PE5** *Insecure Software Development* Credentials and secrets were found in stolen code repositories			

"Attackers targeted…with a phishing campaign, resulting in this October 2022 breach. Some employees clicked the malicious links and authenticated in the fake CircleCI website using their GitHub credentials and OTP mechanism. That enabled the attacker's privileged access to Dropbox's GitHub repositories.

Social Engineering

- More Examples

Portuguese & Brazilian Embassies - APT29 | 2022

Threat actor	Threat	Vulnerabilities	Technical impacts	Business Impacts	Controls
Internal *Unaware embassy workers* Opening links or attachments from a malicious sender, resulting in an infection of the user's computer	*Malicious files installed using HTML smuggling* techniques to deliver an image or ISO file	*Lacking staff cyber awareness.* Exploiting the human factor and the trust between similar diplomatic entities	**PE11** *Cloud Storage Data Exfiltration* After gaining a foothold,sensitive data is exfiltrated to C2 servers or third-party cloud services	**Financial** None reported **Operational** Incident Response & Breach Notification to other government intelligence agencies	**Preventive** - HRS-11 - HRS-12 - UEM-09 - UEM-10 - UEM-11
External **PE10** *Organized Crime/ Hackers/APT* Spear phishing, targeting large lists of recipients that were suspected to be primarily publicly listed points of contact of embassy personnel	*Social Engineering* Utilizing compromised email addresses, fabricated embassy administrative updates were sent, complete with malicious attachments, to embassy employees	**PE6** *Unsecure Third-Party Resources:* Using legitimate email addresses from other compromised organizations for phishing access credentials	APT29 exploits and *misuses cloud services* like Dropbox and Trello to extract stolen data for cyber espionage	**Compliance** None reported. Possible fines or penalties levied by regulators if personal data is exposed (GDPR or LGPD, for example) **Reputational** None reported. -Attacks can undermine diplomatic relationships, erode trust, and create national tensions. -The affected embassies may be perceived as vulnerable or unable to protect sensitive information - Potential damage to credibility and diplomatic standing	**Detective** - TVM-02 - TVM-04 - LOG-01 - LOG-03 - LOG-13 **Corrective** - SEF-01 - SEF-03

"The attackers obtained initial access to various victim mailboxes using malicious attachments to spear phishing emails. This access established persistence on target endpoints and enabled lateral movement from the endpoints to adjacent systems"

Logon/Auth Issues

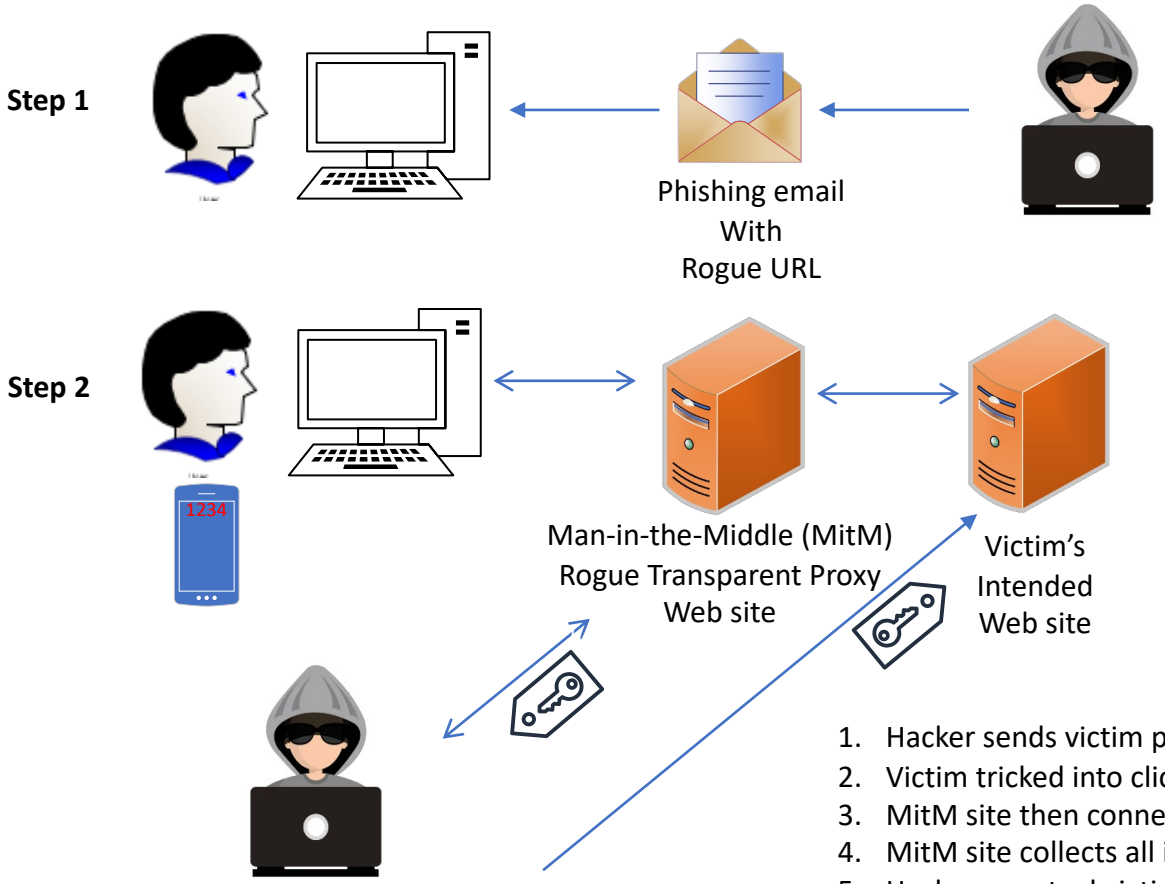
Methods

- Phishing/Social Engineering
- Password Guessing
- Hard Code Credentials
- Ex-Employee
- Hacking MFA

Adversary-in-the-Middle Attack

Network Session Hijacking

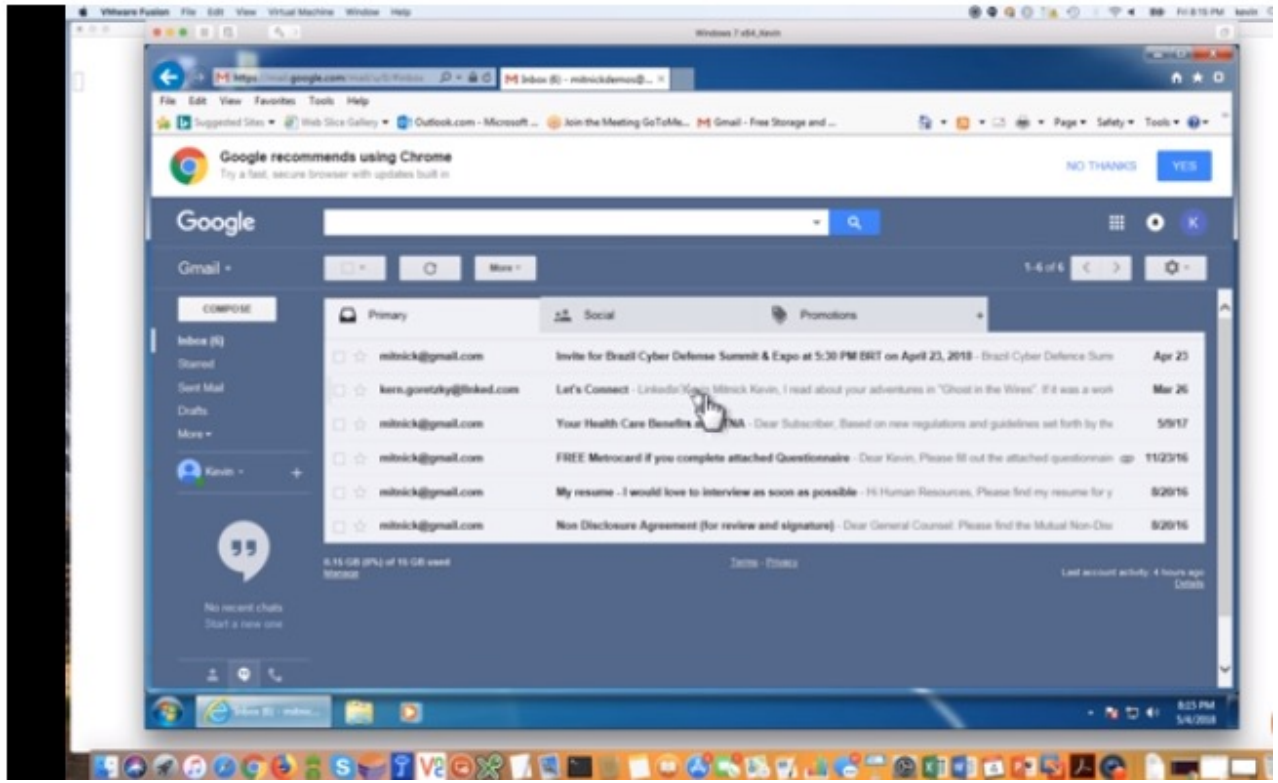
Network Session Hijacking Proxy Theft Logical Diagram



1. Hacker sends victim phishing email with rogue URL
2. Victim tricked into clicking on rogue URL, taking victim to rogue MitM site
3. MitM site then connects to victim's intended legitimate, real, web site
4. MitM site collects all info/data sent between victim and real web site; and vice-versa
5. Hacker can steal victim's logon creds, MFA, access control token cookie, etc.
6. Hacker uses victim's access control token cookie to logon

MFA Hack Example Demo

AitM Hack Demo



https://blog.knowbe4.com/heads-up-new-exploit-hacks-linkedin-2-factor-auth.-see-this-kevin-mitnick-video

VMware Fusion File Edit View Virtual Machine Window Help

Windows 7 x64_Kevin

https://mail.google.com/mail/u/0/#inbox

Inbox (6) - mitnickdemos@...

File Edit View Favorites Tools Help

Suggested Sites | Web Slice Gallery | Outlook.com - Microsoft ... | Join the Meeting GoToMe... | Gmail - Free Storage and ...

Page | Safety | Tools

Google recommends using Chrome
Try a fast, secure browser with updates built in

NO THANKS | YES

Google

Gmail

More

1–6 of 6

COMPOSE

Inbox (6)
Starred
Sent Mail
Drafts
More

Kevin

No recent chats
Start a new one

Primary | Social | Promotions

mitnick@gmail.com	**Invite for Brazil Cyber Defense Summit & Expo at 5:30 PM BRT on April 23, 2018** - Brazil Cyber Defence Sum	Apr 23
kern.goretzky@linked.com	**Let's Connect** - LinkedIn Kevin Mitnick Kevin, I read about your adventures in "Ghost in the Wires". If it was a work	Mar 26
mitnick@gmail.com	**Your Health Care Benefits at AETNA** - Dear Subscriber, Based on new regulations and guidelines set forth by the	5/9/17
mitnick@gmail.com	**FREE Metrocard if you complete attached Questionnaire** - Dear Kevin, Please fill out the attached questionnain	11/23/16
mitnick@gmail.com	**My resume - I would love to interview as soon as possible** - Hi Human Resources, Please find my resume for y	8/20/16
mitnick@gmail.com	**Non Disclosure Agreement (for review and signature)** - Dear General Counsel: Please find the Mutual Non-Disc	8/20/16

0.15 GB (0%) of 15 GB used
Manage

Terms - Privacy

Last account activity: 4 hours ago
Details

Inbox (6) - mitnic...

8:14 PM
5/4/2018

Logon/Auth Issues

- Examples – Adversary-in-the-Middle Attacks

July 12, 2022 • 13 min read

From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud

Microsoft 365 Defender Research Team

Microsoft Threat Intelligence Center (MSTIC)

A large-scale phishing campaign that used adversary-in-the-middle (AiTM) phishing sites stole passwords, hijacked a user's sign-in session, and skipped the authentication process even if the user had enabled multifactor authentication (MFA). The attackers then used the stolen credentials and session cookies to access affected users' mailboxes and perform follow-on business email compromise (BEC) campaigns against other targets. Based on our threat data, the AiTM phishing campaign attempted to target more than 10,000 organizations since September 2021.

Logon/Auth Issues

- Examples

What Caused the Uber Data Breach in 2022?

Edward Kost
updated Mar 02, 2023

The Uber data breach began with a hacker purchasing stolen credentials belonging to an Uber employee from a dark web marketplace. An initial attempt to connect to Uber's network with these credentials failed because the account was protected with MFA. To overcome this security obstacle, the hacker contacted the Uber employee via What's App and, while pretending to be a member of Uber's security, asked the employee to approve the MFA notifications being sent to their phone. The hacker then sent a flood of MFA notifications to the employee's phone to pressure them into succumbing to this request. To finally put an end to this notification storm, the Uber employee approved an MFA request, granting the hacker network access, which ultimately led to the data breach.

How did hacker get stolen credentials to begin with? Hmm. Hmm.

Logon/Auth Issues

- Examples – Hard Coded Passwords

Uber's massive hack

2017 Attack

What happened

Uber CEO Dara Khosrowshahi said two hackers broke into the company in late 2016 and stole personal data, including phone numbers, email addresses, and names, of 57 million Uber users. Among those, the hackers stole 600,000 driver's license numbers of drivers for the company.

Related: Uber paid hackers $100,000 after they stole data on 57 million users

Khosrowshahi says hackers accessed the data through a third-party, cloud-based service. According to Bloomberg, they got into Uber's GitHub account, a site many engineers and companies use to store code and track projects. There, hackers found the username and password to access Uber user data stored in an Amazon server.

Jeremiah Grossman, chief of security strategy at security firm SentinelOne, says this was not a sophisticated hack. Companies frequently accidentally keep credentials in source code that is uploaded to GitHub, he said.

Logon/Auth Issues

- Examples – Hard Coded Passwords

Contractor for Universal Music Group exposes internal credentials

Kromtech Security Center experts discovered that Agilisium (a cloud data storage contractor for Universal Music Group) exposed UMGs internal FTP credentials, AWS configuration details (secret access key and password), along with internal source code details (SQL passwords) via two unprotected instances of Apache Airflow server.

```
def ftp_file():
    ftp_host='[redacted]
    ftp_user='[redacted]
    ftp_passwo[redacted]
    ftp_destination='/Test/test/'
    source_file_name='/home/airflow/airflow/dags/ftpupload/weeklyrefresh.txt'

    with ftputil.FTPHost(ftp_host, ftp_user, ftp_password) as ftp_host:
```

Logon/Auth Issues

Defenses

- Education
- Require phishing-resistant MFA
  - https://www.linkedin.com/pulse/dont-use-easily-phishable-mfa-thats-most-roger-grimes
    https://www.linkedin.com/pulse/my-list-good-strong-mfa-roger-grimes
- Require unique, non-common, complex, not-shared-with-any-other-site passwords, that are get changed at least once a year
  - https://blog.knowbe4.com/password-policy-e-book
- Enable account lockout
- Lock logons to predefined IP addresses, digital certs, or devices
- Prevent and scan for hard-coded credentials

Logon/Auth Issues

Password Policy
Practical Implementation

Use MFA wherever you can
Multifactor Authentication where you can to protect valuable things

Whenever possible use phishing-resistant MFA

https://blog.knowbe4.com/u.s.-government-says-to-use-phishing-resistant-mfa

Use MFA and/or long passwords/passphrases to logon to your devices

All passwords should be changed at least annually

For Passwords

If you can, use a Password Manager
. Protect password manager with MFA and/or long password/passphrase

12-character perfectly random passwords defeat all known guessing/cracking attacks

Perfectly Random Password Examples
R#Yv&ZCAojrX
ELv!2MibAb>RC?ru
a!#=dH)vvLykiJhu

If you must create a password
Create a unique, different, long password/passphrase for all sites and services

Human-created passwords
8-characters – weak
12-characters – better
20-characters – strong

Examples of Good Passphrases
I went to 7-11 earlier today.
rogerjumpedoverthepurplefox
2belivingtherockandrolllifeforever

*Hackers are routinely cracking 18-character human-created Windows passwords if they get the hashes

Optimally:
MFA +
Password Manager +
Strong individual passwords where needed

For more detail: https://info.knowbe4.com/wp-password-policy-should-be

Overly Permissive Permissions

- One of the most common security issues
- Misconfigured permissions, allowing too many people to view non-public data
- Usually due to human error

Overly Permissive Permissions

- Examples

Sensitive US military emails spill online

A government cloud email server was connected to the internet without a password

Zack Whittaker @zackwhittaker / 9:40 AM EST • February 21, 2023

Comment

The U.S. Department of Defense secured an exposed server on Monday that was spilling internal U.S. military emails to the open internet for the past two weeks.

The exposed server was hosted on Microsoft's Azure government cloud for Department of Defense customers, which uses servers that are physically separated from other commercial customers and as such can be used to share sensitive but unclassified government data. The exposed server was part of an internal mailbox system storing about three terabytes of internal military emails, many pertaining to U.S. Special Operations Command, or USSOCOM, the U.S. military unit tasked with conducting special military operations.

But a misconfiguration left the server without a password, allowing anyone on the internet access to the sensitive mailbox data inside using only a web browser, just by knowing its IP address.

Overly Permissive Permissions

- More Examples

The Discovery

On September 17th, 2017, UpGuard Director of Cyber Risk Research Chris Vickery discovered four Amazon Web Services S3 storage buckets configured for public access, downloadable to anyone who entered the buckets' web addresses into their internet browser. A cursory analysis on September 18th of the four buckets - titled with the AWS subdomains "acp-deployment," "acpcollector," "acp-software," and "acp-ssl" - revealed significant internal Accenture data, including cloud platform credentials and configurations, prompted Vickery to notify the corporation; the four AWS buckets were secured the next day.

Overly Permissive Permissions

- More Examples

120 Million American Households Exposed In 'Massive' ConsumerView Database Leak

Whilst there were no names exposed, Chris Vickery, a cybersecurity researcher from UpGuard, told *Forbes* it was simple to determine who the data was linked to, either by looking at the details or by crosschecking with previous leaks. He found the data was sitting in an Amazon Web Services storage "bucket," left open to anyone with an account, which are free to obtain.

As long as they knew the right URL to visit, an Amazon Web Services user could retrieve all the data, which was left online by marketing analytics company Alteryx. It was apparent that the firm had purchased the information from Experian, as part of a dataset called ConsumerView, on top of which Alteryx provides marketing and analytics services.

Overly Permissive Permissions

- More Examples

Personal data of over 50,000 Honda Connect App leaked

Researchers at Kromtech Security Center discovered a trove of data belonging to Honda Connect App which was exposed online. The data was stored in two unsecured Amazon AWS S3 Buckets available for public access without any protection

Overly Permissive Permissions

Defenses

- Education
- Practice Least Privilege Permissions
- Periodically Audit/Verify Permissions
- Alert on unauthorized permission changes
- Change/Configuration Control
- Lock logons to IP addresses, digital cert, technology, behind VPN, etc.
- “Wrap” data in encrypted container

Unpatched Software

- How Big of a Problem?

23 May

[Hands-On Defense] Unpatched Software Causes 33% of Successful Attacks

Stu Sjouwerman

Unpatched software is responsible for 33% of successful attacks

Well, this article (https://www.action1.com/patching-insights-from-kevin-mandia-of-mandiant/) states that Kevin Mandia (who created Mandiant, which sold to Google recently) says unpatched software is responsible for 33% of successful attacks. Mandia is a true veteran, and we greatly trust anything he says. Social engineering is likely involved in 70% to

https://blog.knowbe4.com/hands-on-defense-unpatched-software-causes-33-of-successful-attacks

Unpatched Software

- 33% of all malicious data breaches are due to unpatched software

<u>Hacker Steps</u>

- 1. Find unpatched software or firmware
  - Nmap, Shodan, Nikto2
- 2. Locate related exploit
  - Exploitdb (https://www.exploit-db.com/)
- 3. Execute exploit against target victim

Unpatched Software

EXPLOIT DATABASE

GET CERTIFI

Verified Has App

Filters Reset All

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2019-12-12			✗	ManageEngine Desktop Central - 'FileStorage getChartImage' Deserialization / Unauthenticated Remote Code Execution	WebApps	Multiple	mr_me
2020-03-06			✗	Deep Instinct Windows Agent 1.2.29.0 - 'DeepMgmtService' Unquoted Service Path	Local	Windows	Oscar Flores
2020-03-06			✗	ASUS GiftBox Desktop 1.1.1.127 - 'ASUSGiftBoxDesktop' Unquoted Service Path	Local	Windows	Oscar Flores
2020-03-06			✗	SpyHunter 4 - 'SpyHunter 4 Service' Unquoted Service Path	Local	Windows	Alejandro Reyes
2020-03-06			✗	Iskysoft Application Framework Service 2.4.3.241 - 'IsAppService' Unquoted Service Path	Local	Windows	Alejandro Reyes
2020-03-02			✗	netkit-telnet-0.17 telnetd (Fedora 31) - 'BraveStarr' Remote Code Execution	Remote	Linux	Immunity
2020-03-05			✓	EyesOfNetwork - AutoDiscovery Target Command Execution (Metasploit)	Remote	Multiple	Metasploit
2020-03-05			✓	Exchange Control Panel - Viewstate Deserialization (Metasploit)	Remote	Windows	Metasploit
2020-03-04			✗	UniSharp Laravel File Manager 2.0.0 - Arbitrary File Read	WebApps	PHP	NgoAnhDuc
2020-03-03			✗	RICOH Aficio SP 5210SF Printer - 'entryNameIn' HTML Injection	WebApps	Hardware	Olga Villagran
2020-03-03			✗	GUnet OpenEclass 1.7.3 E-learning platform - 'month' SQL Injection	WebApps	PHP	emaragkos
2020-03-03			✗	Alfresco 5.2.4 - Persistent Cross-Site Scripting	WebApps	PHP	Alexandre ZANNI
2020-03-03			✗	RICOH Aficio SP 5200S Printer - 'entryNameIn' HTML Injection	WebApps	Hardware	Paulina Girón
2020-03-02			✗	Wing FTP Server 6.2.3 - Privilege Escalation	Local	Windows	Cary Hooper
2020-03-02			✗	Cacti v1.2.8 - Unauthenticated Remote Code Execution (Metasploit)	WebApps	PHP	Lucas Amorim

Showing 1 to 15 of 42,441 entries

FIRST PREVIOUS 1 2 3 4 5 ... 2830 NEXT LAST

PWK

AWAE

WIFU

Unpatched Software

DATABASE

Verified | Has App

Filters | Reset All

Show 15

Search: windows 10

Date	D	A	V	Title	Type	Platform	Author
2020-02-17			✗	MSI Packages Symbolic Links Processing - Windows 10 Privilege Escalation	Local	Windows	nu11secur1ty
2020-01-29			✗	Microsoft Windows 10 - Theme API 'ThemePack' File Parsing	Local	Windows	Eduardo Braun Prado
2020-01-07			✗	Microsoft Windows 10 (19H1 1901 x64) - 'ws2ifsl.sys' Use After Free Local Privilege Escalation (kASLR kCFG SMEP)	Local	Windows_x86-64	bluefrostsec
2020-01-13			✗	Microsoft Windows 10 build 1809 - Local Privilege Escalation (UAC Bypass)	Local	Windows	Nassim Asrir
2019-12-20			✗	Microsoft Windows 10 BasicRender.sys - Denial of Service (PoC)	DoS	Windows	vportal
2019-09-20			✗	Microsoft Windows 10 - 'WSReset' UAC Protection Bypass (propsys.dll)	Local	Windows	valen
2019-12-07			✗	Mozilla FireFox (Windows 10 x64) - Full Chain Client Side Attack	Local	Windows_x86-64	Axel Souchet
2019-11-14			✗	Microsoft Windows 10 Build 1803 < 1903 - 'COMahawk' Local Privilege Escalation	Local	Windows	TomahawkAPT69
2019-09-10			✓	Windows 10 - UAC Protection Bypass Via Windows Store (WSReset.exe) and Registry (Metasploit)	Local	Windows	Metasploit
2019-09-10			✓	Windows 10 - UAC Protection Bypass Via Windows Store (WSReset.exe) (Metasploit)	Local	Windows	Metasploit
2019-08-26			✓	Windows 10 - SET_REPARSE_POINT_EX Mount Point Security Feature Bypass	Local	Windows	Google Security Research
2019-08-14			✗	Microsoft Windows 10 AppXSvc Deployment Service - Arbitrary File Deletion	Local	Windows	Abdelhamid Naceri
2019-07-18			✓	Microsoft Windows 10 1903/1809 - RPCSS Activation Kernel Security Callback Privilege Escalation	Local	Windows	Google Security Research
2019-07-16			✓	Microsoft Windows 10 < build 17763 - AppXSvc Hard Link Privilege Escalation (Metasploit)	Local	Windows	Metasploit
2019-07-16			✗	R 3.4.4 (Windows 10 x64) - Buffer Overflow SEH (DEP/ASLR Bypass)	Local	Windows	blackleitus

Showing 1 to 15 of 414 entries (filtered from 42,441 total entries)

FIRST PREVIOUS 1 2 3 4 5 ... 28 NEXT LAST

PWK AWAE WIFU

EXPLOIT DATABASE

Microsoft Windows - BlueKeep RDP Remote Windows Kernel Use After Free (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47416	2019-0708	METASPLOIT	REMOTE	WINDOWS	2019-09-24

EDB Verified: ✓ Exploit: / {} Vulnerable App:


```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

#  Exploitation and Caveats from zerosum0x0:
#
#    1. Register with channel MS_T120 (and others such as RDPDR/RDPSND) nominally.
#    2. Perform a full RDP handshake, I like to wait for RDPDR handshake too (code in the .py)
#    3. Free MS_T120 with the DisconnectProviderIndication message to MS_T120.
#    4. RDP has chunked messages, so we use this to groom.
#       a. Chunked messaging ONLY works properly when sent to RDPSND/MS_T120.
#       b. However, on 7+, MS_T120 will not work and you have to use RDPSND.
#           i. RDPSND only works when
#              HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Winstations\RDP-Tcp\fDisableCam = 0
#           ii. This registry key is not a default setting for server 2008 R2.
#              We should use alternate groom channels or at least detect the
#              channel in advance.
```

Unpatched Software

- Examples

LastPass Hack Due to Unpatched Software

Articles, Information Assurance | 8 March, 2023 | ♥ 0

LastPass suffered two large-scale and public data breaches last year, the first in August to steal source code, and the second in November where partially encrypted password vault data and customer information was stolen. Information from the first breach was used to carry out the second attack, and a keylogger was installed on a senior DevOp's engineer's home computer, which was key to the success of the November attack.

Gaining Credentials

New details have been revealed about how the keylogger was installed on a senior employee's computer, including that the point of failure was a vulnerability in Plex Media Server software running on the employee's home network. This software vulnerability was patched in May 2020, with a spokesperson for the company explaining "The version that addressed this exploit was roughly 75 versions ago".

Unpatched Software

- Examples

A publicly available database belonging to VOIPO which was not properly secured has exposed everything from call logs to internal system credentials to the public.

This month, Director of Trust & Safety at Cloudflare Justin Paine, who is also the creator of the Rainbow Tabl.es security blog, said that an improperly secured ElasticSearch database belonging to the Californian voice over IP services provider was found via the Shodan search engine, which can be used to find Internet-connected devices and systems online.

https://www.shodan.io/

Unpatched Software

- More Examples

Equifax blames open-source software for its record-breaking security breach: Report

The credit rating giant claims an Apache Struts security hole was the real cause of its security breach of 143 million records. ZDNet examines the claim.

Open Source Cloud Storage Firm Finds Unsettling Number of Unpatched Instances Online

NO PATCH TAX —

Unpatched VPN makes Travelex latest victim of "REvil" ransomware

Unpatched PulseSecure VPN appears to have let cybercriminals in to steal, encrypt data.

SEAN GALLAGHER - 1/8/2020, 11:03 AM

Unpatched Software

Defenses

- Patch your software in a timely manner
- If it's on the **CISA Known Exploited Vulnerabilities Catalog** list, get it patched ASAP!!
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Clearly define who has patching responsibility for assets
- If you can't patch quickly, use application-level firewall/proxy

CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Known to be Used in Ransomware Campaigns	Notes
CVE-2023-22515	Atlassian	Confluence Data Center and Server	Atlassian Confluence Data Center and Server Broken Access Control Vulnerability	2023-10-05	Atlassian Confluence Data Center and Server contains a broken access control vulnerability that allows an attacker to create unauthorized Confluence administrator accounts and access Confluence.	mitigations are unavailable. Check all affected Confluence instances for evidence	2023-10-13	Unknown	https://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html

Insecure APIs

Application Programming Interfaces

- Many organizations and services have them
- They are online portals/connection points that allow external people and systems to interact with them to do programmatic inquiries and actions
- Sadly, often not secured or monitored
- APIs are a common entry point for hackers and abuse

```
GET https://api.pwnedpasswords.com/range/{first 5 hash chars}
```

Insecure APIs

Examples

- 2023 T-Mobile API attack exposed PII of 37M customers
- 2023 Honda API attack allowed an attacker to reset anyone's password

```
n.prototype.resetUserPassword = function(e, n, l) {
    return this.__post("api/v1/user/resetpassword?", {
        dealerNo: e,
        zipCode: n,
        email: l
    })
}
```

Unsecured cloud interface of crypto-ATM manufacturer abused in a hack to steal $1.5M, leading to discontinuation of the cloud service and temporary shutdown of thousands of ATMs across the US (GeneralBytes, 2023).[1]

Insecure APIs

Examples

- API security company FireTail states more than half a billion records have already been exposed via vulnerable APIs this year so far
- Enterprise Strategy Group says 92% of surveyed orgs experienced a breach due to an API attack
- Akamai said 75% of 61B password spray attacks it tracked used APIs
  - https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-financial-services-hostile-takeover-attempts-report-2020.pdf

Defenses

Summary

- Inventory your APIs
- Secure Your APIs
  - At the very least, make sure normal security hygiene is applied to APIs
  - Maybe used an application-level firewall/gateway/proxy to protect it/them
- Monitor Your APIs and alert on anomalous behavior

Defenses

Summary

- Pay attention to the top cloud hacks, according to the CSA
- Pay the most attention against the most-likely real-world attacks against your cloud sites and services

Defenses

Summary

Secure your cloud sites and services, especially against:

- Social engineering
- Unpatched software and firmware
- Use Phishing-Resistant MFA where you can to protect valuable data and systems
  - Don’t Use Easily Phishable MFA and That’s Most MFA!
  - https://www.linkedin.com/pulse/dont-use-easily-phishable-mfa-thats-most-roger-grimes
  - My List of Good, Strong MFA
  - https://www.linkedin.com/pulse/my-list-good-strong-mfa-roger-grimes
- Get rid of overly permissive permissions
- Secure your APIs

Platform for Awareness Training and Testing

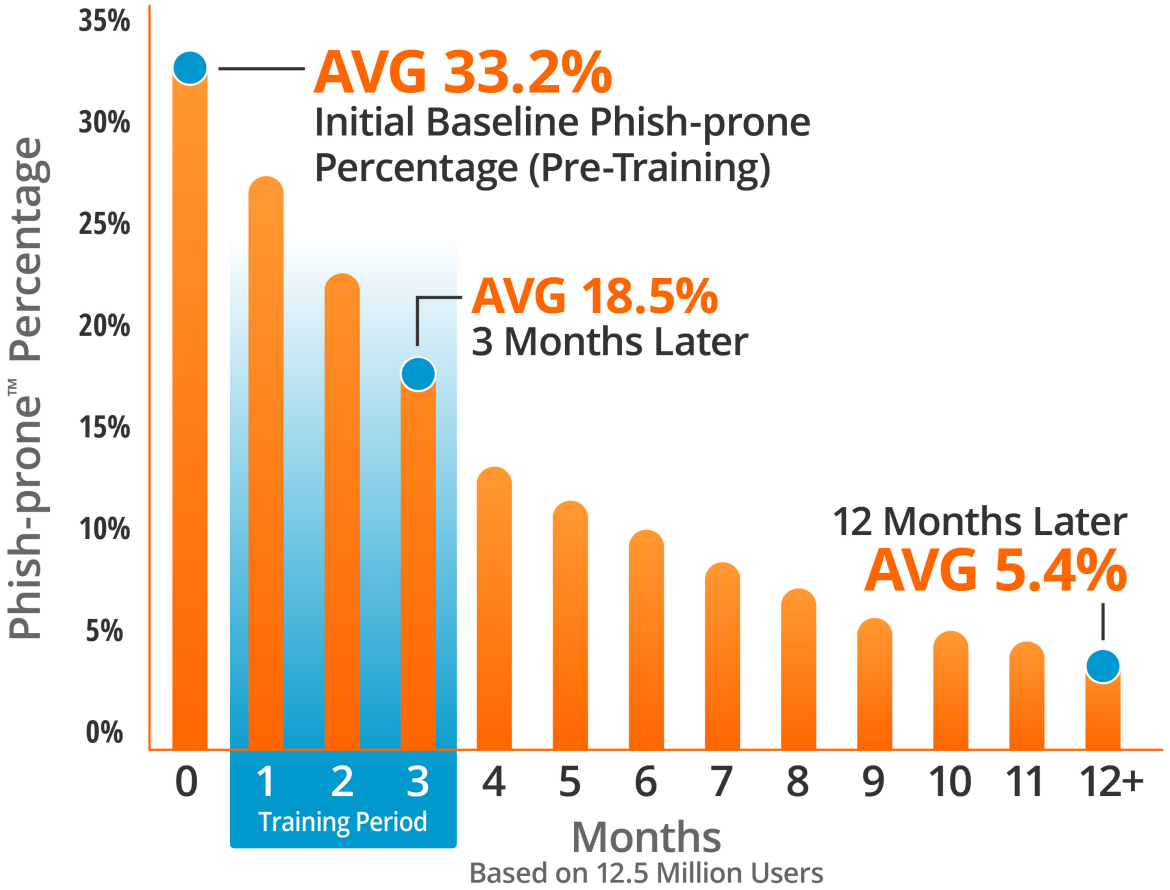
1. Train Your Users
2. Phish Your Users
3. See the Results

Generating Industry-Leading Results and ROI

- Reduced Malware and Ransomware Infections
- Reduced Data Loss
- Reduced Potential Cyber-theft
- Increased User Productivity
- Users Have Security Top of Mind

82% Average Improvement

Across all industries and sizes from baseline testing to one year or more of ongoing training and testing



Source: 2023 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Questions?

Roger A. Grimes– Data-Driven Defense Evangelist, KnowBe4
rogerg@knowbe4.com
Twitter: @rogeragrimes
https://www.linkedin.com/in/rogeragrimes/