



SECTOR
BRIEFINGS
October 1-2, 2025
METRO TORONTO CONVENTION CENTRE

The Once and Future Rules of Cybersecurity

Hello!

- 🍁 Creator/Lead of the Metasploit Project (2003-2015)
- 🍁 Found & exploited hundreds of vulnerabilities
- 🍁 Previously a system admin, consultant, and CSO
- 🍁 I ❤️ building tools, products, and companies
- 🍁 I ❤️ security research & open source

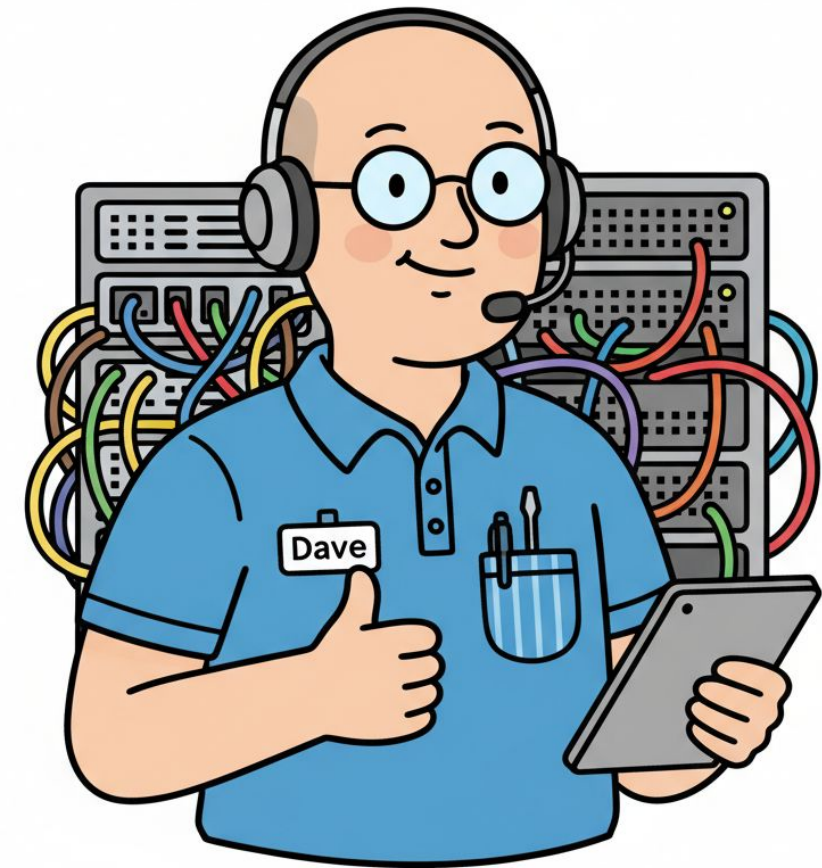


HD MOORE
Founder & CEO



Dave the IT Manager

- 🍁 Worked his way up from mailroom clerk
- 🍁 Friendly and knew everyone by name
- 🍁 Recently rolled out new security policies
- 🍁 Super excited about the assessment!



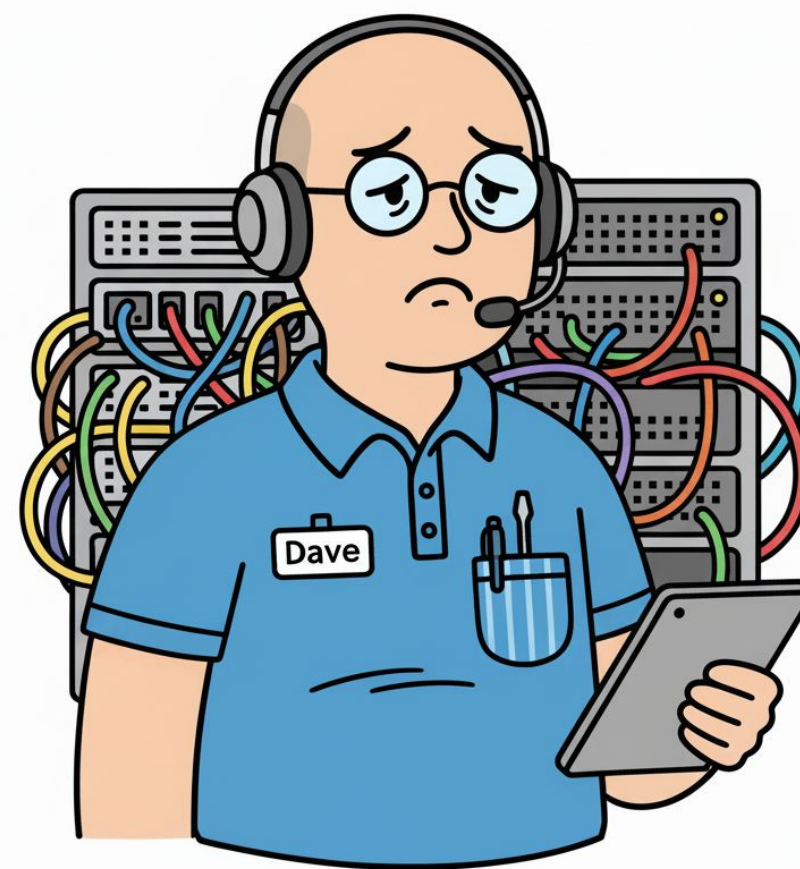
L0phtCrack

- 🍁 Dumped and cracked ~3,000 user accounts
- 🍁 Long passwords, but generally weak
- 🍁 Typical to see org-specific trends
- 🍁 “Dolphins\$2004” & “Summer2003!”
- 🍁 Policies drive password choices



Hundreds of similar passwords

- 🍁 *“****YouDave!”*
- 🍁 *“Dave****ingSucks!”*
- 🍁 *“F***ThisSh*Dave”*
- 🍁 *“DavesBullSh*t”*



More than a policy failure

- 🍁 Bad rules alienate people, create resentment, and make us less secure
- 🍁 Security is a team sport, compliance isn't enough to succeed
- 🍁 You need organization-wide buy-in and belief
- 🍁 Buy-in requires elevating the “why”
- 🍁 Good rules build mutual trust
- 🍁 Let's explore these rules



Passwords

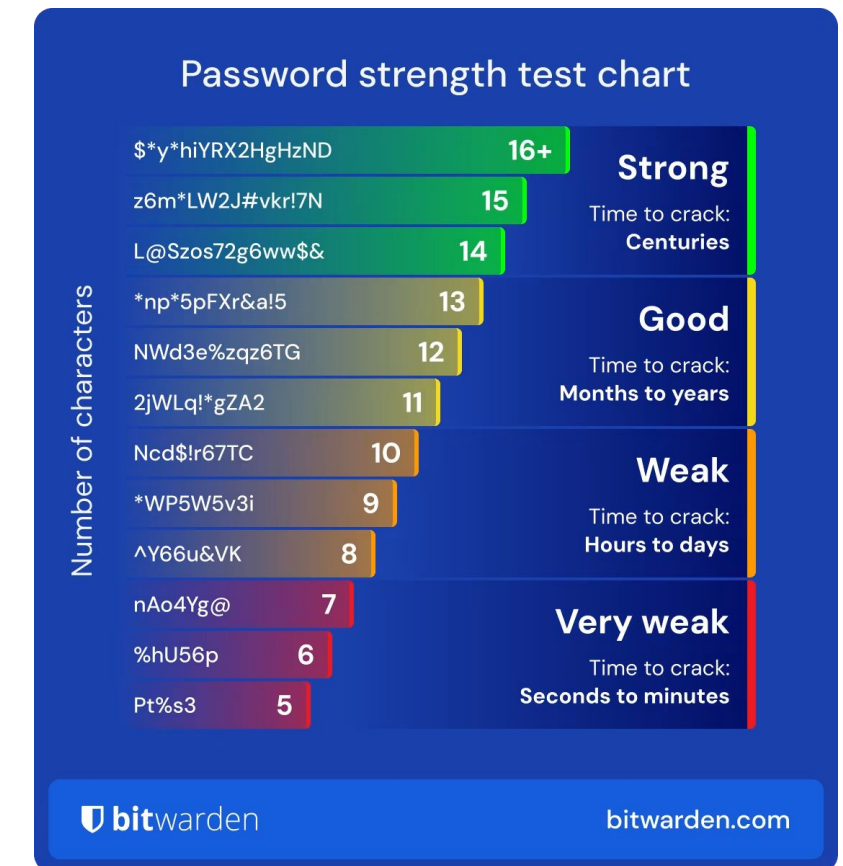
Passwords

“Passwords must be long, complex, unique, frequently changed, and never written down.”

Old Rule

Why it failed

- 🍁 Tried to solve multiple security challenges at once
 - Discourage password sharing between users
 - Prevent physical exposure to observers
 - Reduce success of online brute-forcing
 - Slow down offline cracking
- 🍁 Best practices went against human nature
- 🍁 Technical requirements made things worse
- 🍁 A bit of cargo culting and junk science



<https://bitwarden.com>

Technology limits drove password rules

- 🍁 Unix: Ignores everything after the 8th character
- 🍁 Windows: Splits passwords into two 7-character sequences
- 🍁 Legacy Systems: Can't handle special characters in input
- 🍁 Modern Systems: Can't handle more than 72 characters
- 🍁 Mobile Devices: Limited CPU & restricted keyboards
- 🍁 Web Applications: A laundry list of buggy behaviors

The future is short PINs within enclaves

- 🍁 A convenient PIN unlocks a complex encryption key, safely
- 🍁 Workstations using BitLocker, FileVault, or LUKS, with pins in TPM
- 🍁 Passkeys managed by an application or operating system
- 🍁 Webauthn / FIDO2 keys with presence and/or PINs
- 🍁 Mobile phones with dedicated security hardware
- 🍁 Hard drives that self-encrypt by default

Passwords

“Passwords must be unique, stored in a password manager, expensive to guess, used with MFA, without SMS.”

New Rule

Passwords

“Avoid passwords entirely. Use one-time codes to email with MFA and passkeys or hardware tokens.”

New Rule

Recovery is critical

- 🍁 Authentication is only as strong as your recovery process
- 🍁 Password managers put all your eggs in one basket
- 🍁 Physically print out backup MFA codes for accounts
- 🍁 Roots of recovery are often email & SMS
- 🍁 Secure these first
- 🍁 Test!



Perimeters

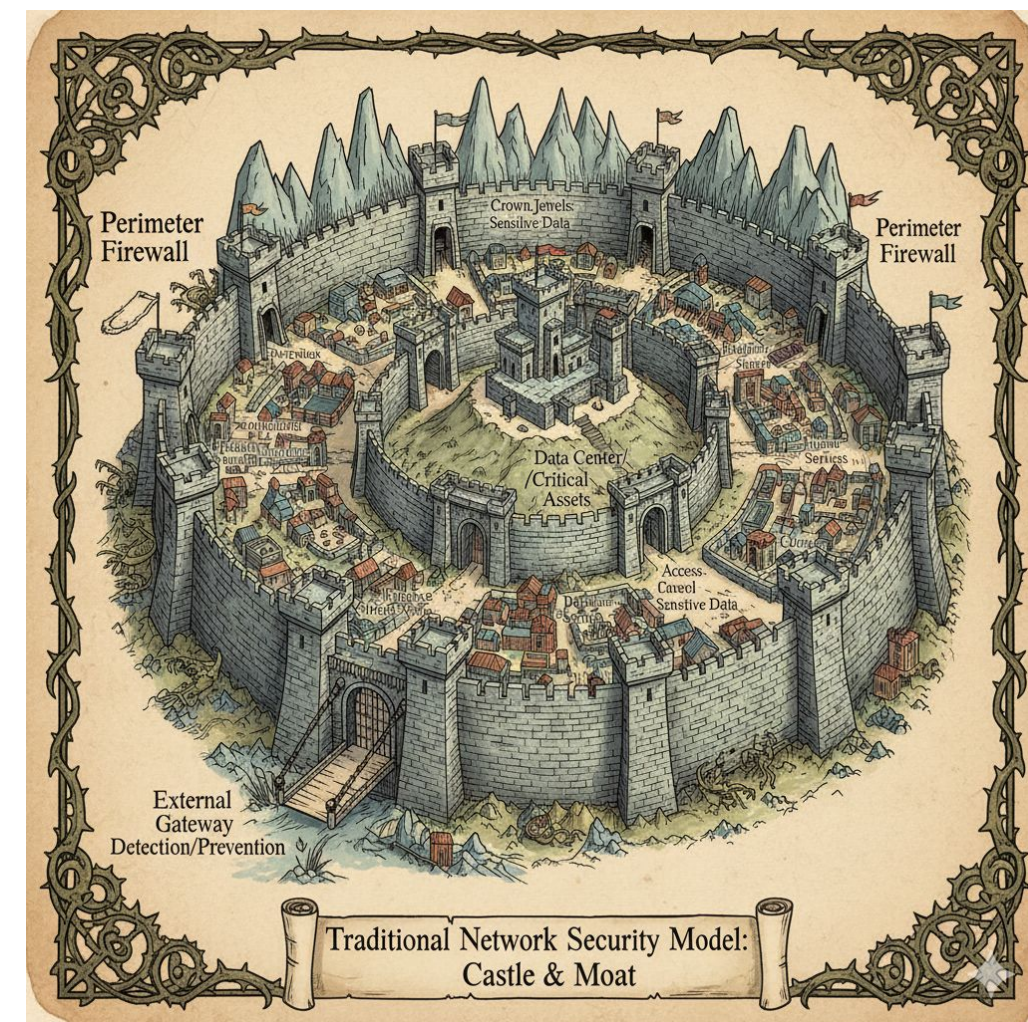
Perimeters

“A hard outer shell and a soft center.”

Old Rule

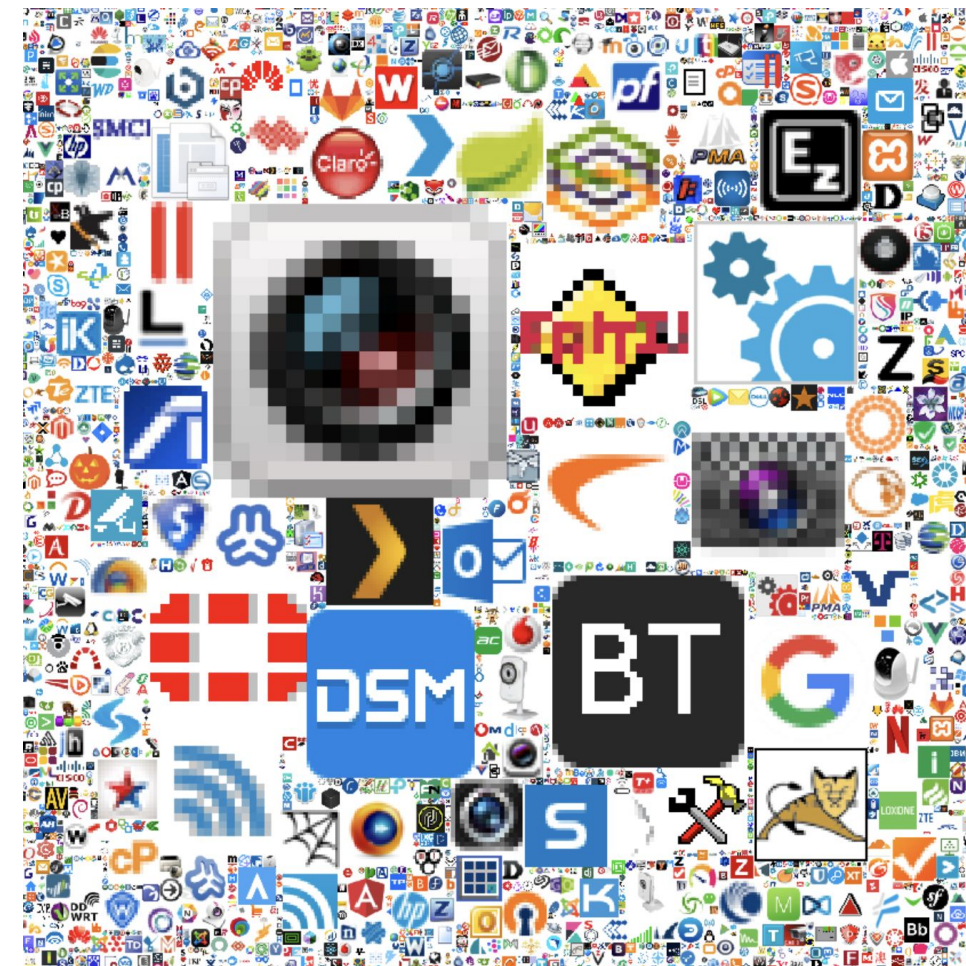
Perimeters

- 🍁 The classic model looks like a medieval city
- 🍁 High security on the outside
- 🍁 Limited defenses inside



Automated device exposure via UPnP

- 🍁 Popular ISP-provided routers enable UPnP
- 🍁 Many devices automatically port-forward
- 🍁 Massive unintentional exposure
 - IP Cameras
 - DVRs
 - File Servers
 - Media Servers



<https://faviconmap.shodan.io/>

Firewalls that spray credentials

- 🍁 Internet-wide scan in 2014 resulted in a flood of inbound credentials
 - ~5,000 PAN firewalls with User-ID misconfigured (R7-2014-16) **404?**
- 🍁 Internet-wide scan in 2025 still found a few more
 - Handful of PAN along with WatchGuard (SSO Agent)
- 🍁 Still a widespread issue within **internal** networks
 - Vulnerability scanners and IT tools too!

```
SMB Administrator::BIDCON:a459...  
SMB watchguard_sso::BANKOFNNN:6dbf...  
SMB WGAdmin::BIGMFG:a412...  
SMB _SSOWatchguard::GNRTRANSP:9c93...  
SMB PA_Agent::MYAIRNATIONAL:0c18...
```


Firewalls and VPNs are rich targets

- 🍁 Firewalls and VPNs are one of the most common entry points
- 🍁 Top-four initial access vectors* in 2024 were security appliances
- 🍁 2025 is not looking any better
 - See Matthew Flanagan’s “**Panning for Gold**”
 - Often the same ~5 vendors

* **Mandiant M-TRENDS 2025**

Most Frequently Exploited Vulnerabilities

Among the Mandiant incident response investigations performed in 2024, the most frequently exploited vulnerabilities affected security devices, which are, due to their function, typically placed at the edge of the network. Three of the four vulnerabilities were first exploited as zero-days. While a broad selection of threat actors have recently targeted edge devices, Mandiant also specifically noted an increase³ in targeting from Russian⁴ and Chinese⁵ cyber espionage actors.

Most Frequently Exploited Vulnerabilities



Why it failed

- 🍁 Cloud, mobile, WFH, wireless, hyperscale, and BYOD broke the model
- 🍁 Endpoints turned to agents for EDR and zero-trust security models
- 🍁 Wireless networking became ubiquitous for mobile endpoints
- 🍁 Unmanaged devices were often left behind

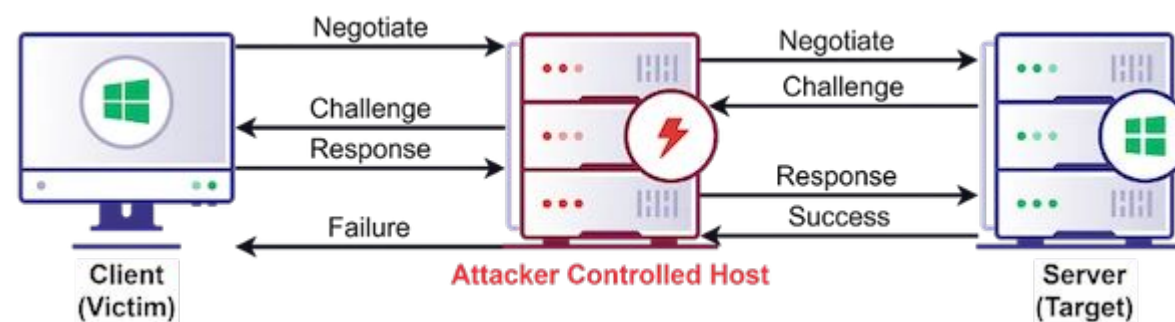
Everything is a WAP if you squint

- 🍁 All multi-homed wireless-enabled devices can be access points
- 🍁 Laptops, printers, media servers, and IoT gateways
 - Printer with WiFi or BT can become a WAP
 - Printers are often stuffed with credentials



Attackers can become the network

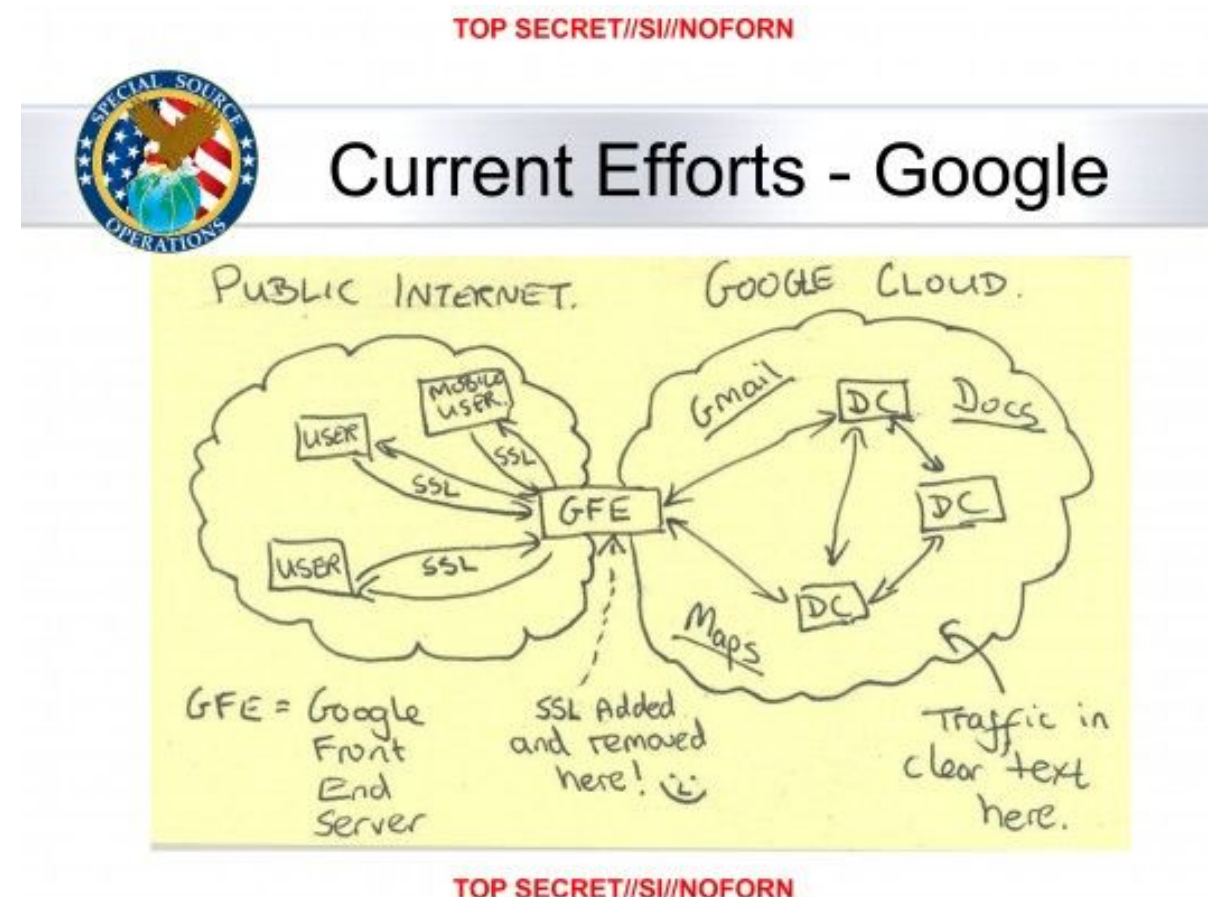
- 🍁 Wireless attacks can force a device to join a malicious network
- 🍁 This leads to immediate credential leaks and often much more
- 🍁 VPN connections get confused, SMB continues anyways
- 🍁 Still working variants today



<https://www.helpnetsecurity.com/2025/07/04/ntlm-relay-attacks/>

Containers and clouds are not immune

- 🍁 VPCs and pods reintroduce the classic perimeter challenges
- 🍁 TLS terminated and routing is clear-text
- 🍁 Weak passwords for sidecar containers
- 🍁 IP forwarding on by default



Perimeters

“Adopt zero-trust, retire SSL-VPNs, restrict firewall management interfaces, disable wireless, harden containers and VPCs.”

New Rule



User Behavior

User Behavior

“Users are your weakest link. Train and test them accordingly.”

Old Rule

Month of Browser Bugs

- 🍁 A new zero-day browser vulnerability, every day, for a month straight
- 🍁 Still had hundreds left when it was all done
- 🍁 Kick-started major security improvements
- 🍁 Helped finally kill ActiveX & Java GUIs



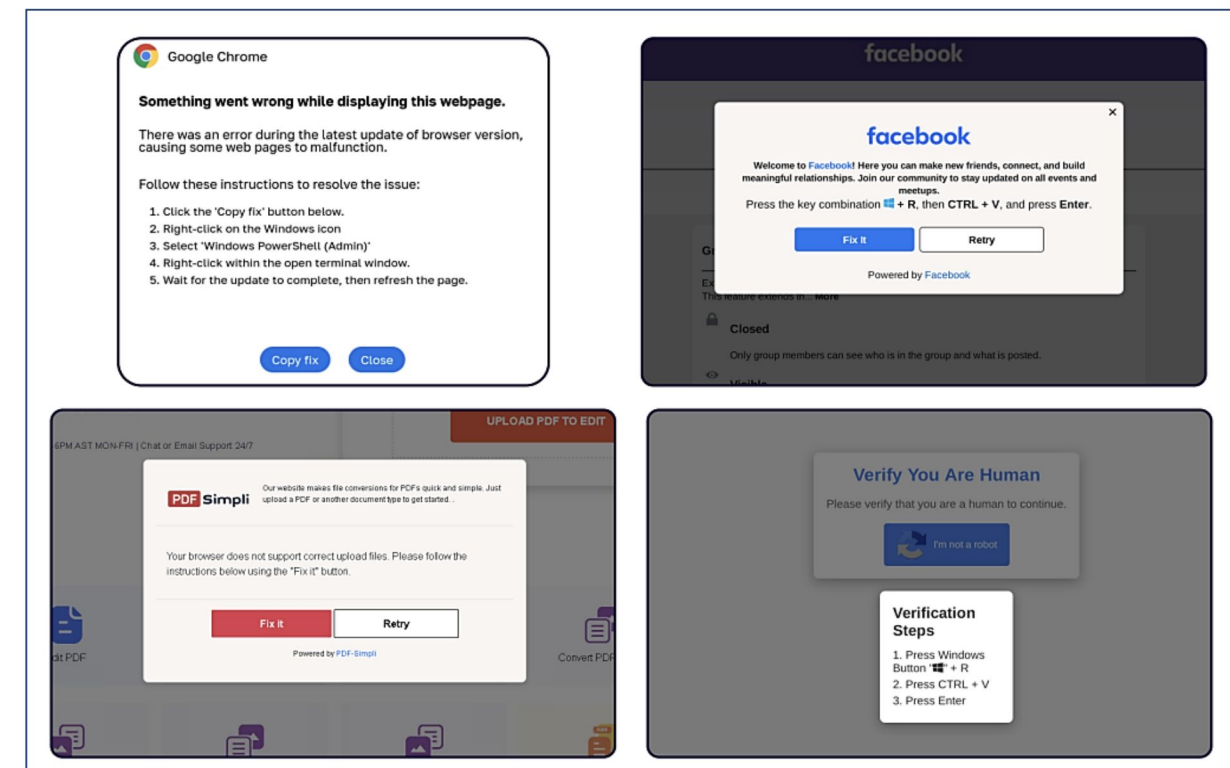
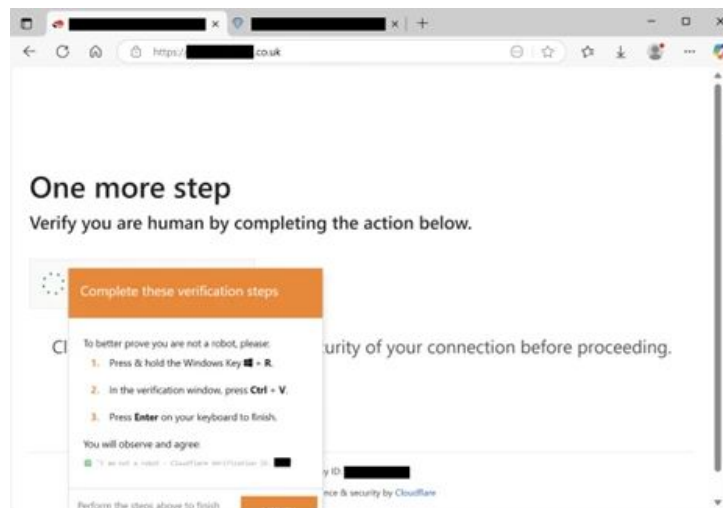
Why it failed

- 🍁 Web browser security is now ridiculously good compared to other software
- 🍁 Tasteless phishing tests burned goodwill without real benefit
- 🍁 We still tell people not to click things, they still click things
- 🍁 Security has improved, but so have attackers
- 🍁 August 2025: Month of AI Bugs!

<https://monthofaibugs.com/>

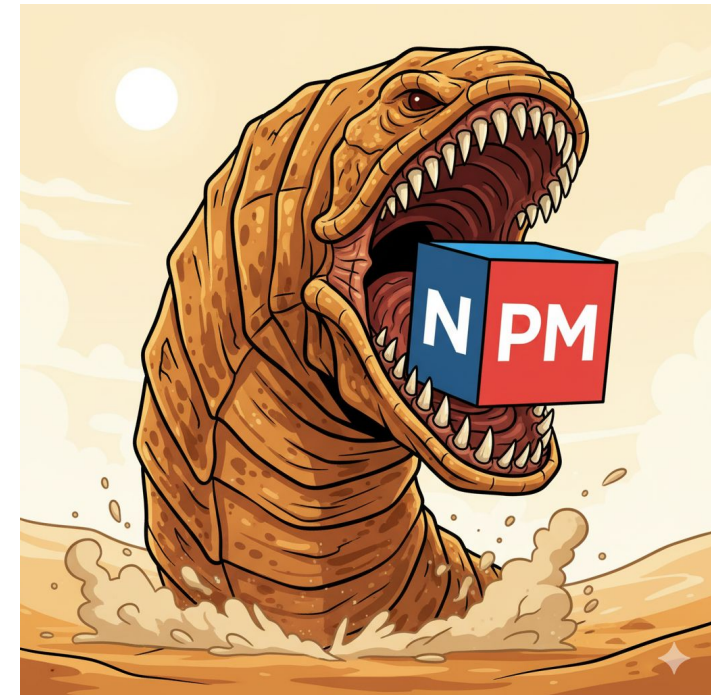
Attackers adapted

- 🍁 Relay phishing and malware through trusted third-party services
- 🍁 Calendar invites, DocuSign requests, cloud provider hostnames
- 🍁 ClickFix and variants are actually working



Technical users are (great) targets

- 🍁 Supply chain attacks often start with phishing against developers
- 🍁 New attacks via internal package name squatting & CI actions
- 🍁 Chrome extensions are still being bought and backdoored
- 🍁 Even rock-solid SDLC can't stop a `npm install new-shiny`
- 🍁 See Cory Doctorow's "How I Got Scammed" article



User Behavior

“Users are always fallible, including your technical users & leadership; plan for it and practice rapid response.”

New Rule




Attacker Behavior

Attacker Behavior

*“Prioritize remediation based on
real-world attacks and
exploitability data”*

Old Rule

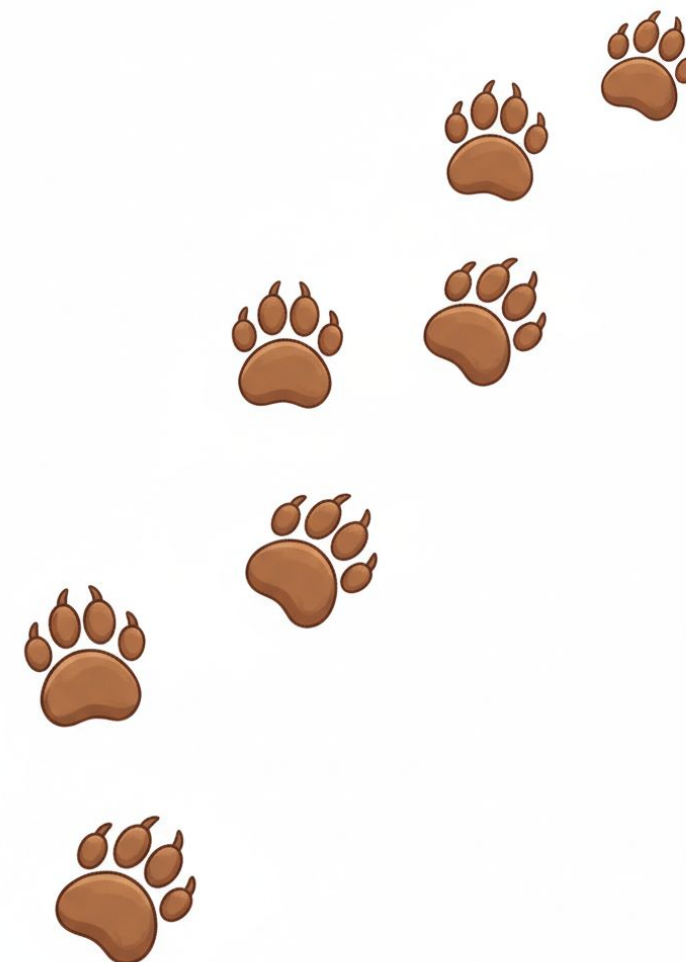
The bear test

 Are you sure that you want to go hiking with your marathoner friend?



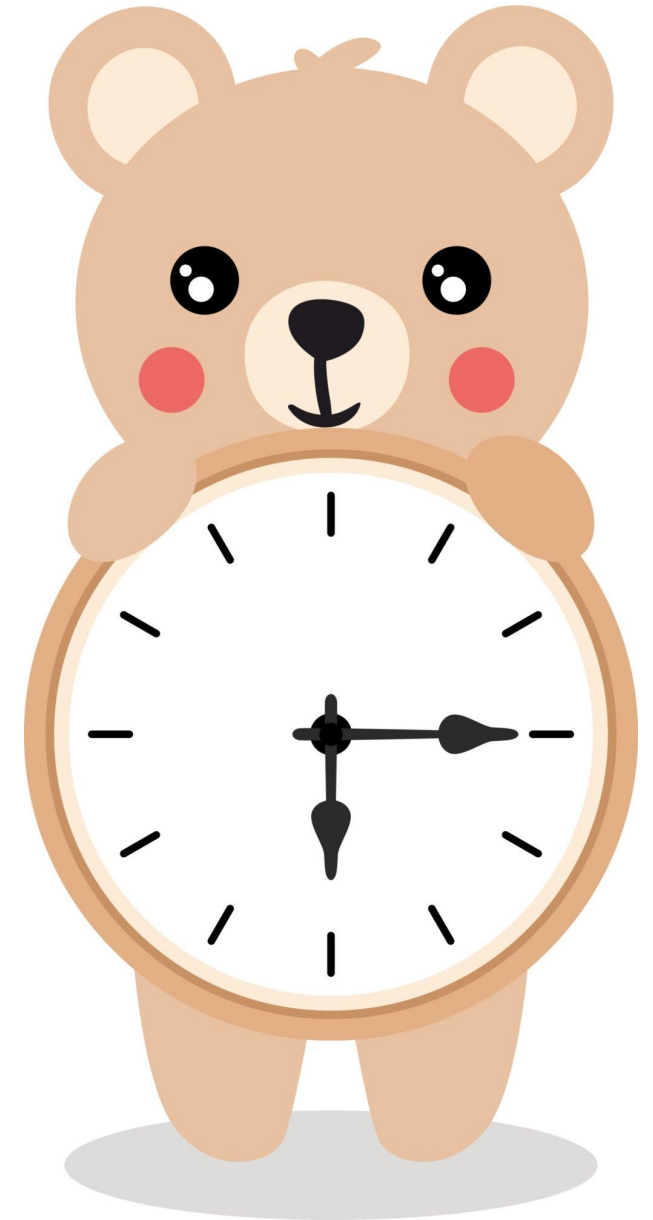
Evidence of exploitation

- 🍁 Watch the CISA Known Exploited Vulnerabilities list
- 🍁 Read news articles describing successful attacks
- 🍁 Look around for public tools and exploits
- 🍁 These all assume time you don't have



CISA KEV timelines

- 🍁 CISA KEV requires a CVE to be allocated
- 🍁 CVEs often lag discovery by three weeks
- 🍁 CISA generally waits for verified attacks
- 🍁 Typically lags behavior by two weeks
- 🍁 Waiting for the KEV?
- 🍁 You are the KEV



The internet used to be a big place

- 🍁 A deep and barely-explored global ocean of technology
- 🍁 Plenty of empty space and often relatively quiet
- 🍁 Chances of being directly targeted were low
- 🍁 Why go after your organization?



The internet got crowded and small

- 🍁 Ping any valid IPv4 address – 17% chance of getting a reply
- 🍁 20 minutes and \$5 dollars to exploit all of IPv4
- 🍁 SHODAN and Censys know your applications
- 🍁 Targeting is now a search query



Attackers racing each other to exploit

Surge in networks scans targeting Cisco ASA devices raise concerns

By **Bill Toulas**

September 8, 2025 05:44 PM 0



September 8th, 2025

EMERGENCY DIRECTIVES

ED 25-03: Identify and Mitigate Potential Compromise of Cisco Devices

September 25, 2025

RELATED TOPICS: [CYBERSECURITY BEST PRACTICES](#)



September 25th, 2025

Attacker Behavior

“Assume your assets are already cataloged and that attackers are waiting. Respond faster. Attackers are cheap and the internet is small.”

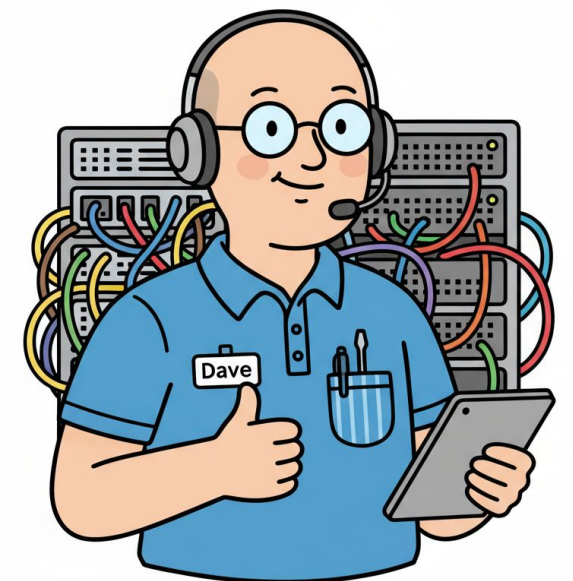
New Rule



Summary

Your challenge

- 🍁 Fundamentals still matter across every aspect of security
- 🍁 Focus on preparedness, resiliency, and response speed
- 🍁 It's always worth questioning our assumptions
- 🍁 Is this rule having the intended outcome?
- 🍁 Can you break it? Can you redefine it?



Thank you!

Contact information at
[HDM.io](https://hdm.io)



**For Q&A head to
Booth 734!**