Number One Risk: Not Knowing your Asset Inventory

Presented by Aaron Sanderson, CISSP, CEH

June 7, 2023

Agenda

- Who am I
- Security Requirements
- Why is Asset Management Important
- Breaches Caused by Insufficient Asset Inventories
- Holistic Visibility of Attack Surface

Who Am I?

Aaron Sanderson

Senior Penetration Tester / Threat Analyst
CISSP, C|EH

Subject Matter Expert

- Penetration Testing
- Cyber Forensics
- Website Scanning and Exploitation Tools
- Vulnerability Scanning
- Incident Response and Reporting
- Network/Endpoint/Information Security
- Computer Network Defense

Red Team Operator/Penetration Tester/Threat Analyst

Navy Red Team (one of nine NSA Certified DoD Red Teams) providing on-board Cyber Threat Emulation during Fleet, Command, and Joint Exercises during pre-deployment training, acquisition program assessments, and operational readiness assessments.

Clearance

Active Top Secret/SCI with current SSBI

30 Years in IT
Focused on Security since 2004
Penetration Tester since 2018

Aarons@JanusAssociates.com
@SecurityAaron

Top Security Controls

CIS Critical Security Control 1: Inventory and Control of Enterprise Assets support identifying unauthorized and unmanaged assets to remove or remediate; and **CIS Critical Security Control 2: Inventory and Control of Software Assets** ensures authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution

The Payment Card Industry Data Security Standard (PCI DSS) requires that an inventory of system components (PCI Req. 2.4: Complete Inventory List) is maintained.

NIST 800-53 Revision 5 CM-8 System Component Inventory requires an organization to develop and document an inventory of system components, and review and update the system component inventory regularly

NIST Cybersecurity Framework ID.AM-1: Physical devices and systems within the organization are inventoried; ID.AM-2: Software platforms and applications within the organization are inventoried; and ID.AM-4: External information systems are catalogued

ISO 27001 A.8.1.1 Inventory of Assets: Any assets associated with information and information processing facilities need to be identified and managed over the lifecycle, always up to date

Why is Asset Management Important

Internet-accessible assets have grown exponentially increasing the attack surface

Malicious actors scan the Internet searching for vulnerabilities and/or weaknesses on assets that are not properly managed

Mismanaged assets become hard to track and determine what needs protection

Unknown assets can include Shadow IT, test and deployment servers, login portals, temporary services, etc.

Data leakage due to vulnerable and publicly accessible information systems hosting an internal system

Which Assets?

- Known
- 3rd Party
- Shadow IT
- Rogue

Shadow IT

- Companies or organizations may not know of information technology
- Employees are using information technology without company approval
- Shadow IT can be an application, cloud-based services, or hardware
- Examples of Shadow IT are unapproved communication and collaboration tools (Slack, Dropbox, WhatsApp, etc.)

Rogue Assets

- An unauthorized node on a network
- Can include a list of discovered assets not currently present in the asset inventory
- Can be hardware or software
- Best detection method is regular network discovery scans and/or vulnerability scanning across the network

Apache Struts

- CVE-2017-05638
- Published March 6
- Scanning started March 9
- Initial Breaches March 14

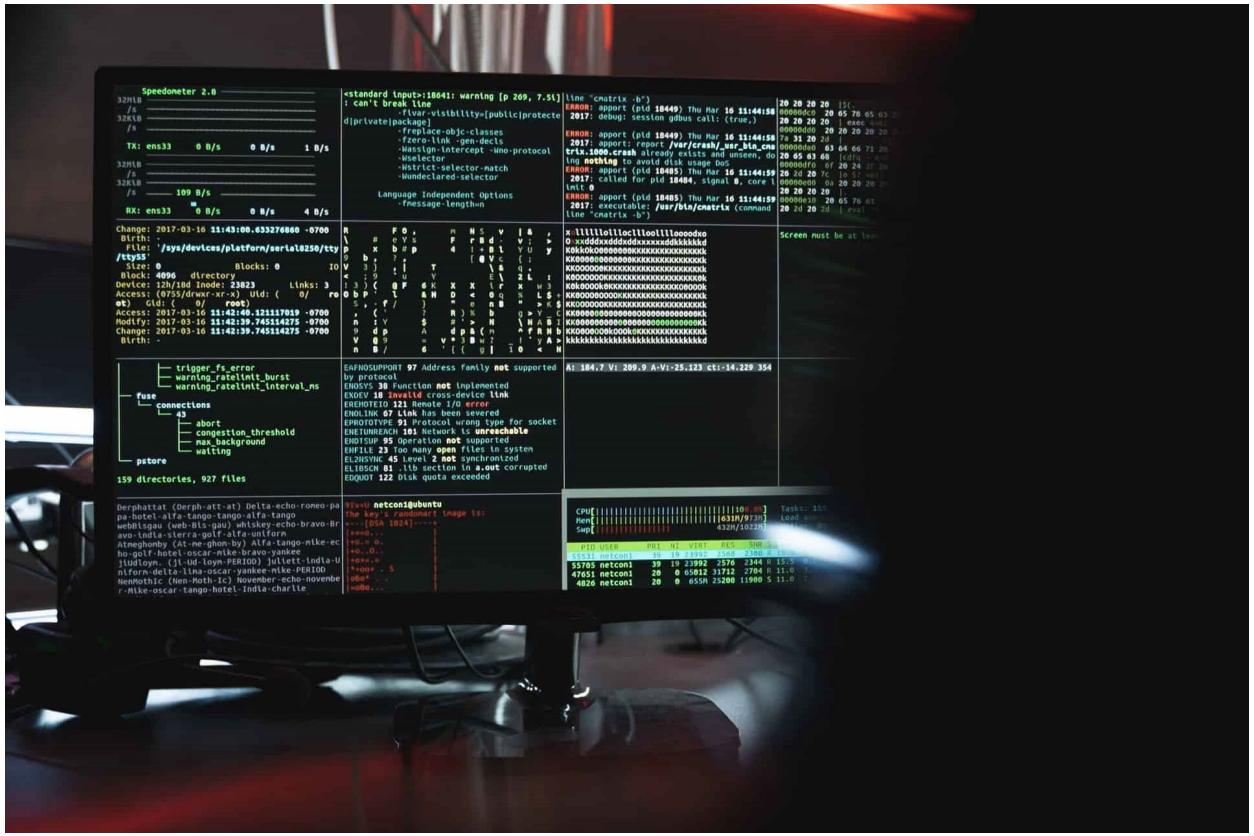
- Equifax was breached two months later

Other Breaches

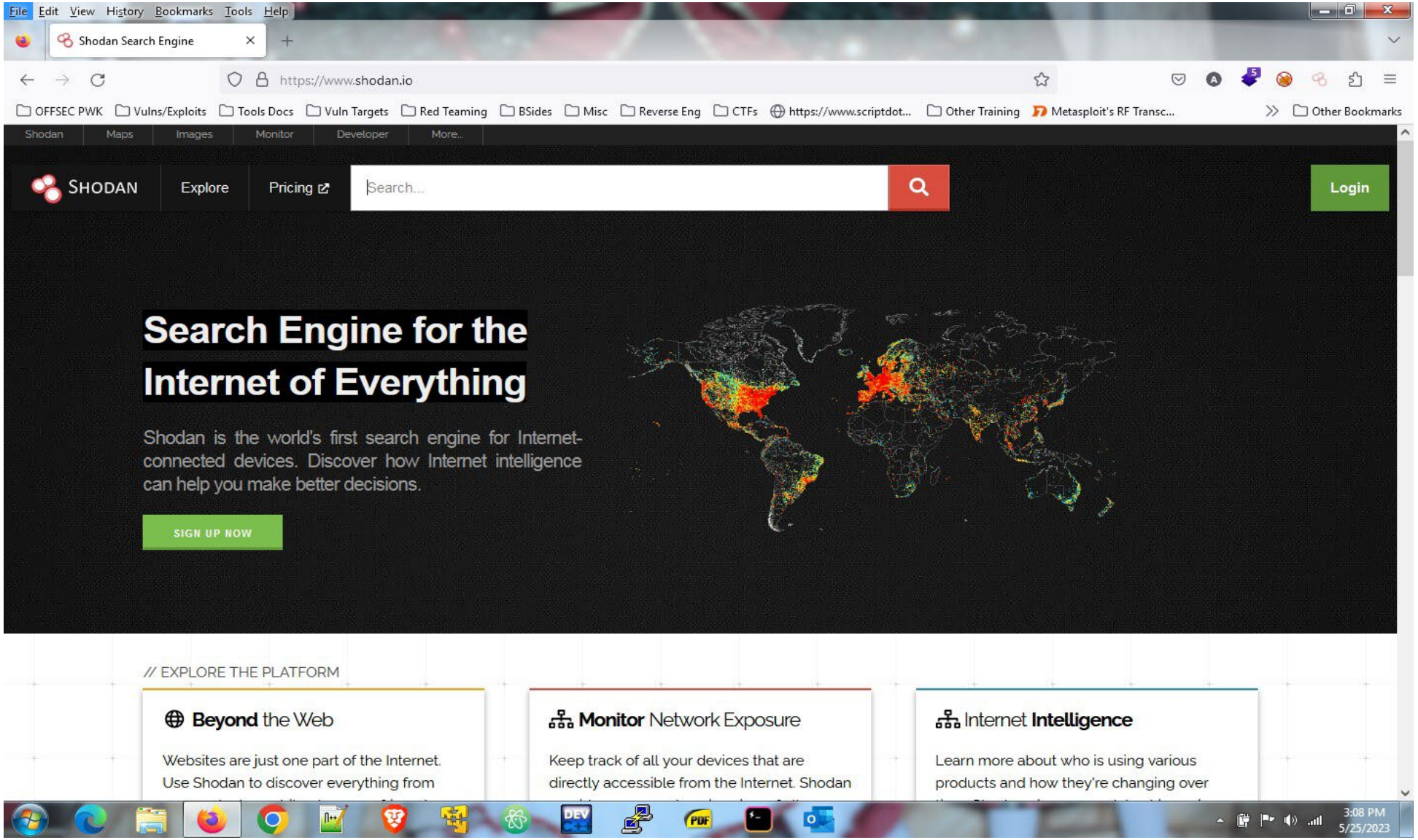
- Target (Unsegmented HVAC Controls. 40 million credit and debit card numbers and 70 million records of personal information were stolen)
- OPM (Shared Network Infrastructure with another Agency. PHI Breach = 22.1 million people)
- WeWork (Inputing WeWork name into Resonance platform resulted in source code & credentials.
  PII spill of over 40,000 data sets)
- Global Big 4 Consulting Firm (Leakage of PII, Client Names, Project Names, Partner Details, Storage System credentials including sheets and documents, System logs, and operations)

An Attacker's Visibility

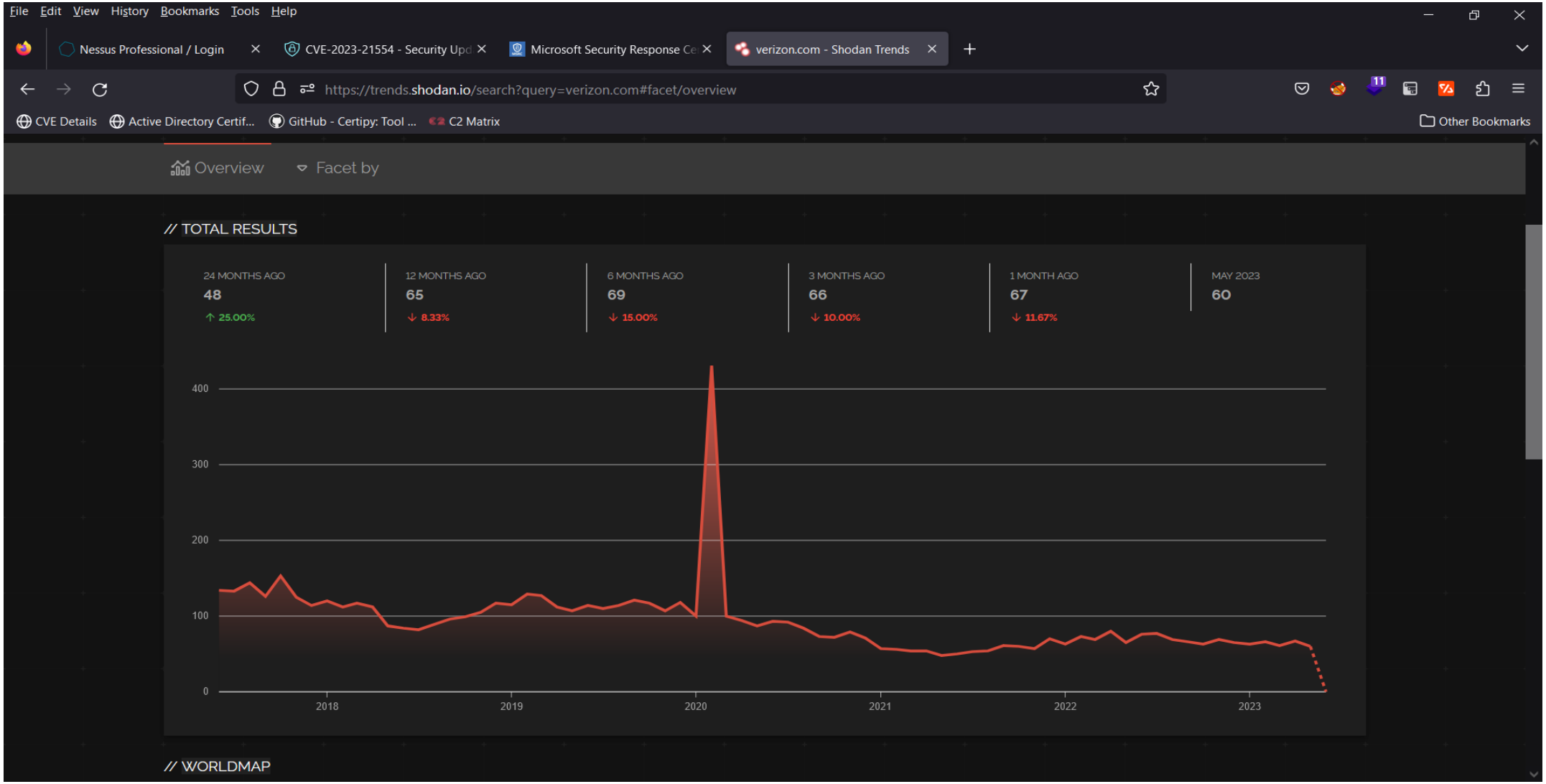
- Shodan.io / Masscan
- Builtwith
- Wappalyzer



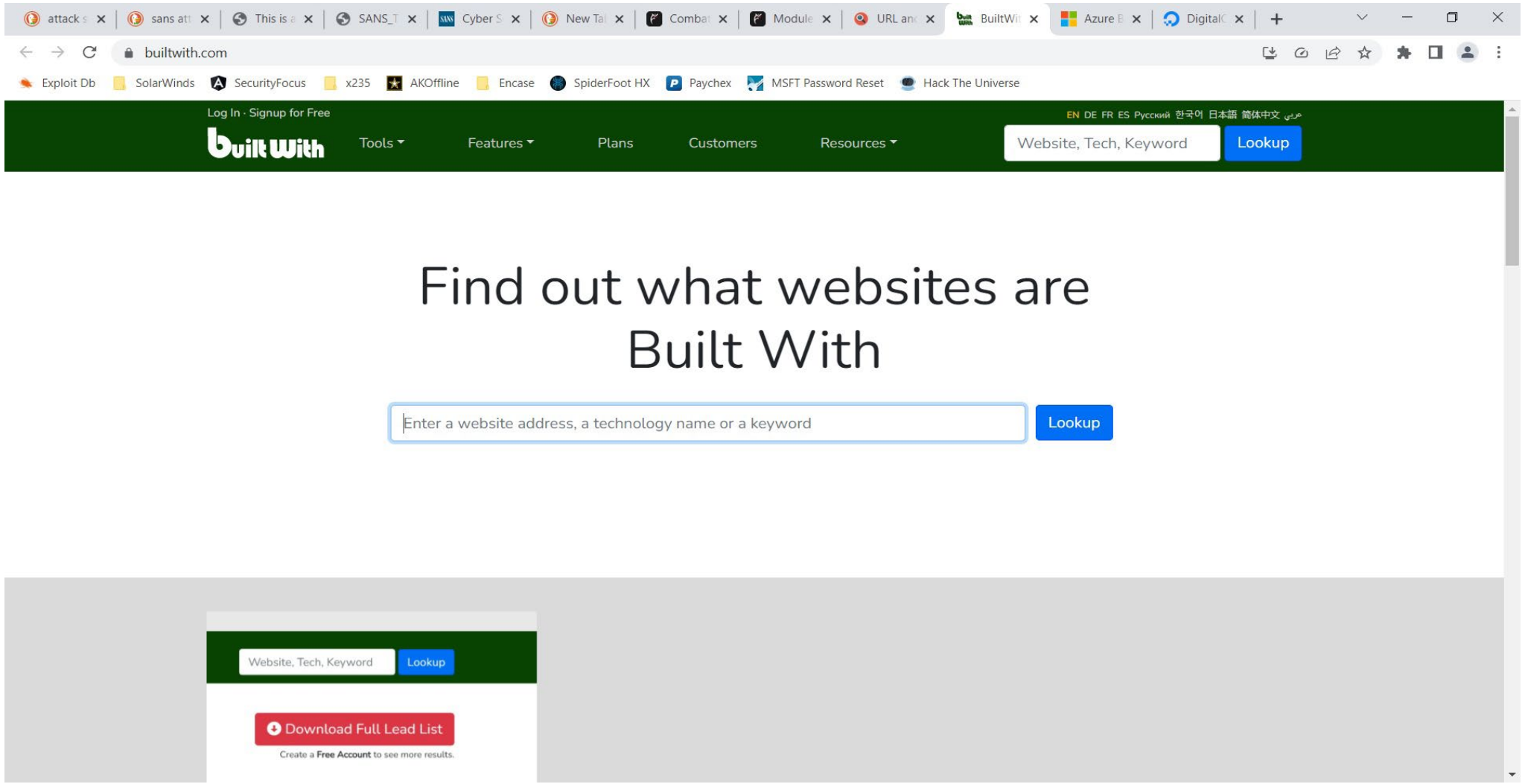
Shodan.io



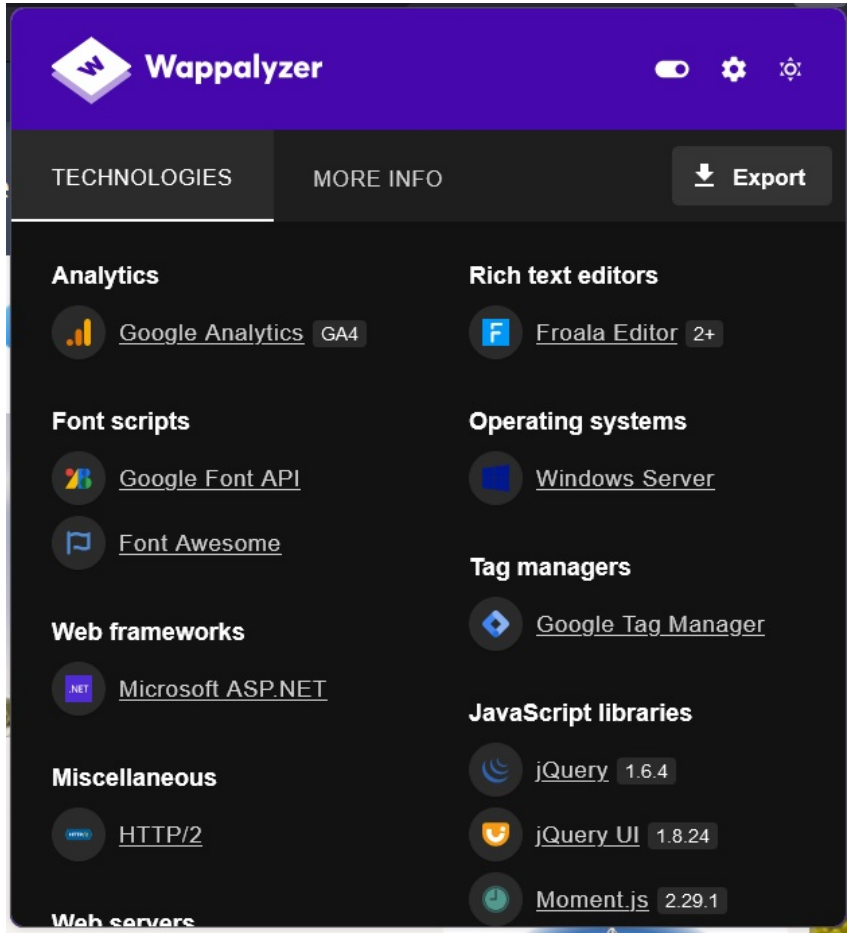
Shodan Historical Data

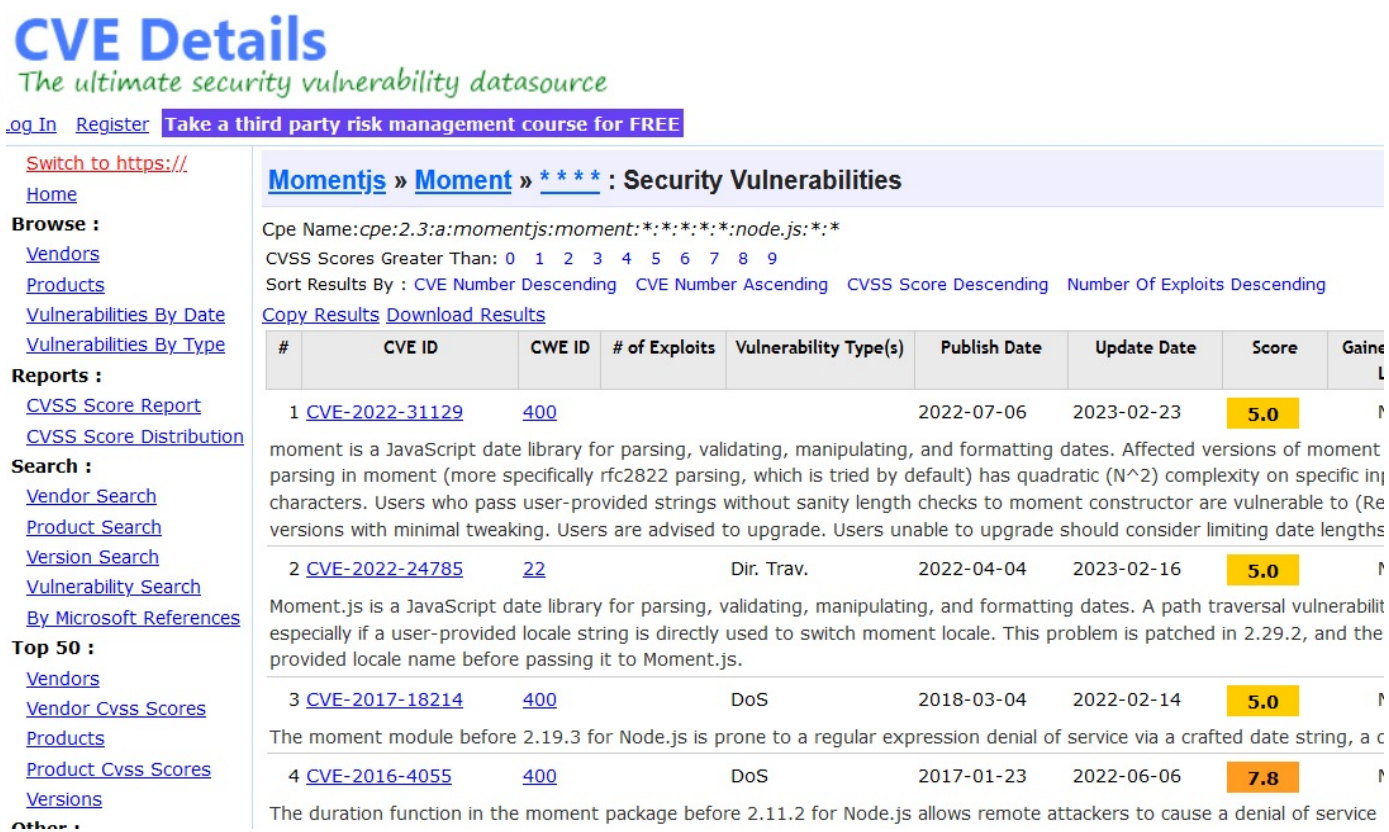


Builtwith



Wappalyzer





We are JANUS Associates

Trusted NYS Information Security Consultants

- Vendor-neutral, Cyber security specialists
- Founded 1988, the longest continuously operating IT Security specialty consultancy in US.
- Industry Certified, Senior Level Subject Matter Experts – only
- 34+ years serving government, business, and non-profits
- Privately held, WBE (woman-owned business)
- GSA Multiple Award Schedule (MAS) Contract: GS-35F-471BA
- **NYS PBITS Contract #PB028AA**

JANUS Corporate Headquarters
2 Omega Drive
Stamford, CT 06907
(203) 251-0200
www.janusassociates.com

Aaron Sanderson CISSP, CEH, Sr. Penetration Tester
Aarons@janusassocaites.com
O: (203) 251-0222
C: (503) 780-8268

Philip Massa, Director
phillipm@janusassociates.com
O:(203) 251-0234
C: (203) 999-3324

CELEBRATING 30+ YEARS
PROTECTING client data since 1988
JANUS ASSOCIATES