Ensuring the Continued Security of the United States Critical Electric Infrastructure

86 FR 21309

SpyCloud Inc.
Douglas Lingenfelter
doug.lingenfelter@spycloud.com
202-265-7931

spycloud.com/solutions/government/

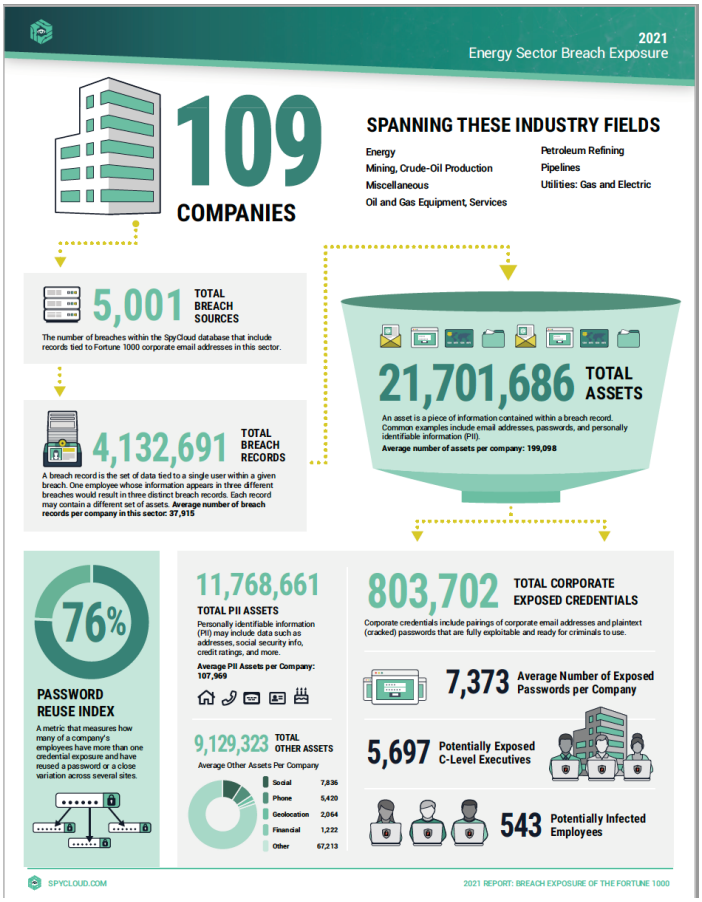
Ensuring the Continued Security of the United States Critical Electric Infrastructure

86 FR 21309

Closing A "BIG" Door on Ransomware:

Ransomware has been growing steadily since 2016 – and 2021 is no different including the high-profile attack on Colonial Pipeline. More than doubling its frequency from 2019, **ransomware as an action was present in 10% of breaches** last year. Bad actors look for easy access and prefer the use of stolen credentials or brute force as a tactic; in Verizon's annual 'Data Breach Investigation Report for 2020'*, 60% of the ransomware cases Verizon observed involved direct install or installation through desktop sharing applications.

SpyCloud Applied Research analyzed breach data tied to employees of Fortune 1000 companies. For this analysis, we examined over 107 million Fortune 1000 employee breach records containing more than 543 million assets, all of which are available to cybercriminals and can be used for malicious purposes. The extent of exposed credentials and infections of 'credential stealing' malware is illustrated in this graphic for the 109 Energy Sector companies in the Fortune 1000.



With an estimated 4,000+ companies in the nation's electric infrastructure, and many small companies with little resources for cybersecurity, the 'easy' path for criminals to use stolen credentials to penetrate networks and install ransomware is frightening. Early detection and continuous visibility of exposed credentials and 'credential stealing' malware infected user machine records for the electric infrastructure employees, c-suite and their suppliers' is a needed and obvious first line of defense against the use of the stolen credentials in brute force, credential stuffing, password phishing and social engineering attacks. Closing a "big' door on criminals.

DOE and CISA can get fast and encompassing visibility into stolen credentials and 'credential stealing' malware infections with SpyCloud. With no implementation required, within days DOE and CISA can begin reporting and sharing these critical cyber risks to the electric critical infrastructure companies.

SpyCloud is the largest source of collected and curated breach data assets: 120 billion breach data assets, 29 million email addresses, 26 billion plaintext passwords and the only source for 200+ million 'credential stealing' malware infected user machines records from 14 families of malware.

What makes SpyCloud different from other breach data sources:

- 90% of data is collected using our HUMINT tradecraft from covert and private sources, days if not hours from when a breach happens. Our competitors are limited to using dark web scanning that cannot access these sources and the result is SpyCloud on average obtains breach data 180+ days prior to publication on the dark web.
- 90% of found passwords are cracked into plaintext. SpyCloud has built our own password passing platform to crack passwords at scale. No other source has this volume of crack passwords for exact and fuzzy matching to access the true risk of exposed credentials
- 50+ billion assets are from foreign domains including Chinese, Russian and Iranian domains. SpyCloud Investigations enable attribution to help de-anonymize the threat actors, their organizations and infrastructure.
- 250+ million 'credential stealing' malware infected user machines records collected by our HUMINT tradecraft directly from criminal sources. Approximately 10 million are monthly. The high risk, high fidelity, and data rich records include the infected machine id, IP address, infection timestamp, infected install path, and visited URLs. SpyCloud is the only known source for records from 14 families of malware.

SpyCloud's go-to market solutions help proactively protect employees, consumers, and employees of suppliers of Federal Agencies from cyber threats using stolen credentials and malware infected user machines and to de-anonymize the threat actors and organizations from their historical exposed digital footprint. SpyCloud solutions include:

- **SpyCloud Employee Protection (EAP).** Monitoring, dashboard reporting and automated alerts of all exposed credentials and infected user machines records for multiple company domains, IP addresses, or VIP email addresses, and all infected user machine records for visitors to domains or IP addresses.
- **SpyCloud Active Directory Guardian (ADG).** Automates the matching, alerts and remediation of exposed credentials and infected user machine records to your active employee. ADG initiates a change to the password used and enforces password strengthening in compliance with NIST 800-63B.
- **SpyCloud Third Party Insights (3PI).** Monitoring, dashboard risk ranking and reporting, and alerts of exposed 'plaintext' credentials and infected user machines records for employee's and c-c-suite for third party suppliers or sub organizations such as a DOE Laboratory. Actionable data for remediation of the risk can be shared with the third party with tracking of the remediation in the 3PI dashboard.

Ensuring the Continued Security of the United States Critical Electric Infrastructure

1. **What Technical Assistance would States, Indian Tribes or units of local government need to enhance their security efforts relative to the electric system?**
   - The lowest and easiest path for criminals is using exposed credentials to launch attacks. With the explosion of work from home, personal devices and remote access has only complicated the attack surface. Early detection of exposed credentials, knowing the plaintext passwords and knowledge of any 'credential stealing' malware infected user records is an easy and highly effective way for governments to close the most used and easiest path for criminals.

     - **SpyCloud Employee Protection (EAP)/Active Directory Guardian (ADG):** Automate the monitoring of Government active directories to detect exposed 'exact match or closely matching' credentials and any infected user machine. Remove the exposures and strengthen new passwords in compliance with NIST 800-63b guidelines. SpyCloud is the largest source of breach data, earliest collection, largest source of cracked passwords and the only source of infected user machine records. SpyCloud has had States inquire if DHS CISA could make this service available to Government organizations to help the States, Indian Tribes and local governments to detect and remediate the most used source of attacks, exposed credentials. Cloud hosted by SpyCloud in AWS, EAP requires no implementation other than entering the domains, IP addresses and VIP emails to monitor and report. ADG does require loading of a module onto the active directory server and adds the automation to initiate a change to the password.

About SpyCloud

SpyCloud is a small emerging technology company with headquarters in Austin TX. SpyCloud is doing business with the US Federal Government with customers in both Civilian and DoD Agencies. Gov@spycloud.com

References:

Verizon 2020 Data Breach Investigation Report.
https://www.verizon.com/business/solutions/secure-your-business/business-security-tips/?cmp=knc:ggl:ac:ent:security:8003162844&utm_term=verizon%20dbir%202020&utm_medium=knc&utm_source=ggl&utm_campaign=security&utm_content=ac:ent:8003162844&utm_term=verizon%20dbir%202020&gclid=Cj0KCQjwnueFBhChARIsAPu3YkTGtcW1dA748L8B2OCqD6b3VZ5jZ4vRaygmkkULxN0yBfMLXe10kEAaAvjIEALw_wcB&gclsrc=aw.ds