LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Credential Stuffing

05/09/2019

Report #: 201905091000

Agenda

Credential Stuffing

- Overview
  - Phases
  - Enablers
- Statistics
- Methods and Tools
  - Sentry MBA
  - SNIPR
- Examples:
  - HSBC Bank
  - Health Insurance Company
- Protection / Detection
- Review
- Conclusion

Slides Key:

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

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

Overview – Credential Stuffing

Credential Stuffing Introduction (F5)

What is it?

- **Fueled by data breaches,** attackers amass list of stolen (legitimate) username/password combinations, "stuff" those credentials into a program to automate validity checking
- Exploits password recycling across accounts

Estimated 28 billion credential stuffing attacks in second half of 2018 (H2) (Barracuda)

Who can be attacked?

- *Any organization with a login portal → every sector*
- Healthcare and public health (HPH sector) targeted to steal sensitive information

Impacts (SAGE):

- Application downtime from large spikes in login traffic
- Costs to remediate compromised accounts
- Lost business due to customers switching to competitors
- Damaged brand equity from news stories or social media
- Account takeover (ATO)
- Fraud & financial losses

-Private health information (PHI)
-Health insurance information
-Payment data

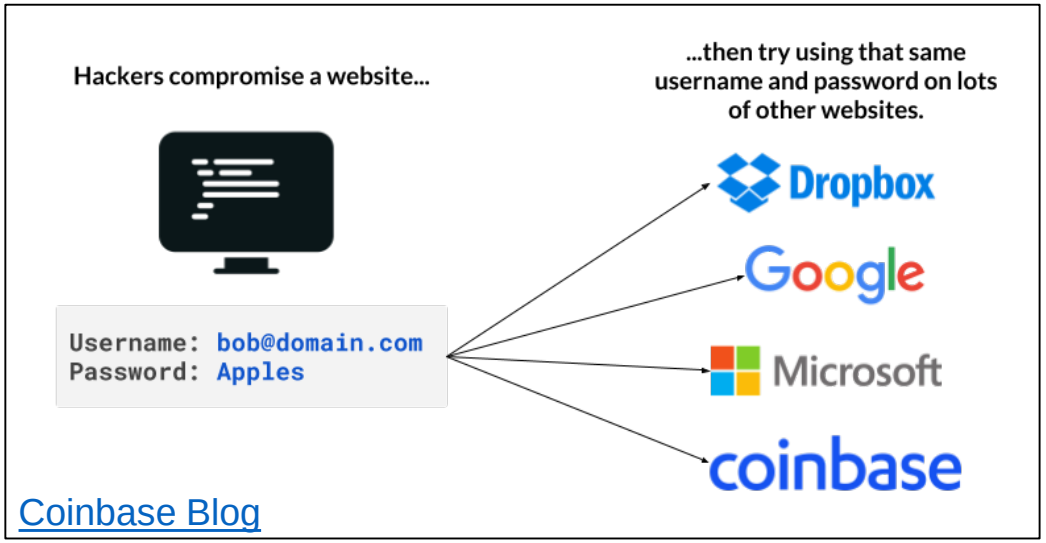
-Attackers take full control of accounts (email, ecommerce, healthcare)
-Hijack email to facilitate fraudulent activity (business email compromise)
-Use account permissions, relationships to spread malware
-Download account information and to abuse and/or sell

Cloud Flare

Overview – Credential Stuffing

Credential Stuffing (F5)

- Leveraging username/password combinations (leaked via data breaches) to gain access on other sites
  - Exploits users' habit of reusing usernames and passwords across multiple online services
    - Nearly 75% of users reuse/recycle their passwords
  - Automated attacks against a website or application's login system
- **Method observed since 2014**
  - **On the rise over last ~6 months**
- Every sector is impacted
  - Attacker groups focused on sectors



Coinbase Blog

Credential Stuffing is NOT Brute Forcing:

In a brute force attack, attackers guess passwords with large lists of common or default username/password combinations

In a credential stuffing attack, attackers use legitimate credentials that have been exposed

Success rate of Credential Stuffing attacks are higher than brute force attacks because the attackers are using legitimate credentials

Cloud Flare

Overview – Credential Stuffing

Credential Stuffing (F5)

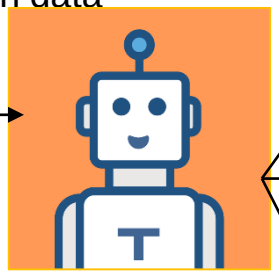
PHASES OF A CREDENTIAL STUFFING ATTACK:

- Attackers acquire username/password combinations from a credential dump or purchased via dark web
- Attackers can test the stolen credentials with an account checker against many websites (social media, banking, ecommerce)
- The (sometimes millions) of the collected credentials are loaded into bots or programs to begin *stuffing* various login pages
- The accessed accounts can be used for downloading stored data, including credit card numbers, personally identifiable information (PII) and health data

Attackers obtain large number of credentials

Typically purchased on the dark web or obtained in public data leak

Sometimes millions of username and password combinations are included in credential stuffing attacks



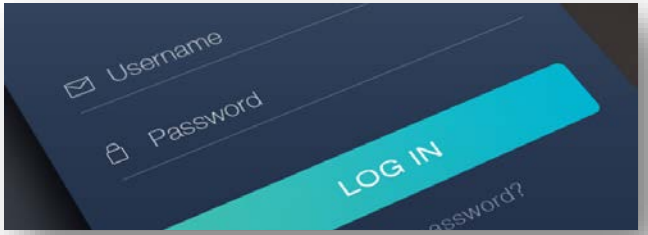
Credentials are loaded into bots/programs to "stuff" various login pages

Password reuse across multiple sites puts banking and health data at risk due to credential stuffing attacks

Akami

Overview – Credential Stuffing

Credential Stuffing (F5)



ENABLERS OF CREDENTIAL STUFFING

- **Single factor username-password authentication**
  - Identity verification process that requires the access-requesting party (can be a person, software or machine) to produce to the authenticating party a single identifier (single factor) that is linked to its identity. [ONLY PASSWORD] (Double Octopus)

- **Compromise and leakage of username / password combinations**
  - Referring to the public unauthorized publication / dumping of sensitive data, especially email addresses, usernames and passwords

- **Password reuse**
  - It is estimated that up to ¾ users are reusing / recycling passwords across multiple accounts

- **Attack tool availability / infrastructure support**
  - Account validity checkers (known as “checkers”), proxy lists, marketplaces

Akami

Credential Stuffing Statistics

Credential Stuffing – By The Numbers (Akami) (F5)

- **75%:** of users recycle their passwords across different accounts
- **1-2%:** The typical success rate of credential stuffing is 1-2%
  - *Cybercriminal with a million stolen credentials can successfully access between **10,000 to 20,000** accounts*
- **28 BILLION:** credential stuffing attempts observed during second half (H2) of 2018 (Bleeping Computer)
  - *Retail was largest with **10 BILLION** attempts*
  - *the United States is also at the top of the list with **22.47 BILLION** credential stuffing attacks observed in H2 2018*
- **773 MILLION:** number of unique email address and associated passwords in “Collection #1” discovered in January 2019 (Bleeping Computer)
  - ***7.73M to 15.46M:** possible number of successful credential stuffing attacks*

Akami

Credential Stuffing Statistics

Credential Stuffing – By The Numbers (Infosecurity-Magazine)

Study of 544 IT professionals with familiarity of credential stuffing attacks on their organization

- **11:** number of credential stuffing attempts observed each month
  - ***1041:*** *number of user accounts targeted in each attack*
- **$4 MILLION:** costs of credential stuffing attacks for organizations each year
  - *1.2 MILLION: downtime*
  - *1.6 MILLION: loss of customers*
  - *1.2 MILLION: extra involvement of IT security and cost of follow-on fraud*
- **26.5:** average number of operational customer-facing websites for cybercriminals to target with credential stuffing attacks
- **88%:** percentage of IT professionals that agreed it's difficult to differentiate between legitimate and fraudulent login attempts

Akami

Overview – Credential Stuffing

CREDENTIAL STUFFING TARGETS MORE THAN JUST PUBLIC WEBSITES

- Although the retail sector is the most targeted in credential stuffing attacks, some cybercriminals are more deliberate in their targeting.

> If there's any way a hacker or a fraudster could abuse a user's account, then that company will likely face a credential stuffing attack at one point or another. -ZDNet

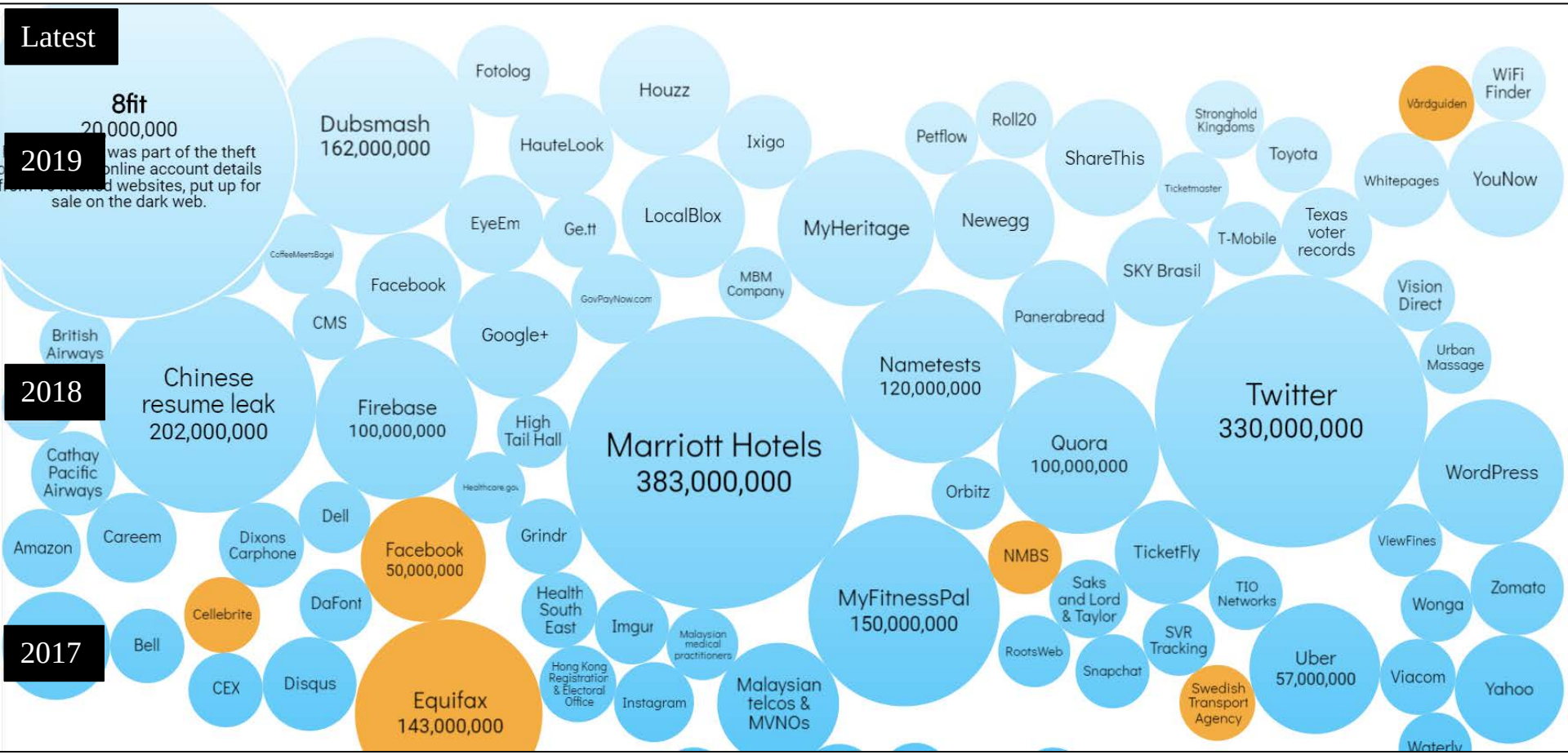
What else can credential stuffing be used to target?

- **Admin credentials, websites without user registration:**
  - Credential stuffing can be used in attempt to access private websites **that don't even have huge userbases**
  - For example: WordPress sites to take over the site and use it in other malware distribution campaigns
- **RDP, Telnet, and SSH endpoints:** servers and normal workstations can be targeted just as well as websites.
- **Corporate intranets, or other enterprise applications** are also vulnerable to credential stuffing attacks

ZDNet

Prevalence of Data Dumps

Data Dumps Fuel Credential Stuffing



[Information is Beautiful]

Prevalence of Data Dumps

Data Dump Fuel Credential Stuffing (HIBP)

Notable Data Dumps concerning the HPH sector:

8fit → health and fitness service

- 15M unique email addresses alongside names, genders, IP addresses and passwords (bcrypt hashes)

Acne[.]org

- 430k forum members' dates of birth (DOB), email addresses, IP addresses, passwords, usernames

Anti Public Combo List

- 458 million unique email addresses, many with multiple different passwords hacked from various online systems

Collection #1-5 → "breach of breaches" (WIRED)

- **2.2 billion** unique username and password combinations, all available to download in plaintext—for free

Quarter 1 (Q1) 2019: (@riskbased Twitter)

- Over **1,900 data breaches** were reported in the first 3 months of 2019, a new Q1 record
- Three breaches exposing **100 million or more records**

What can be done with all this exposed data?

Data Dumps – Credential Stuffing

Data Dump Fuel Credential Stuffing

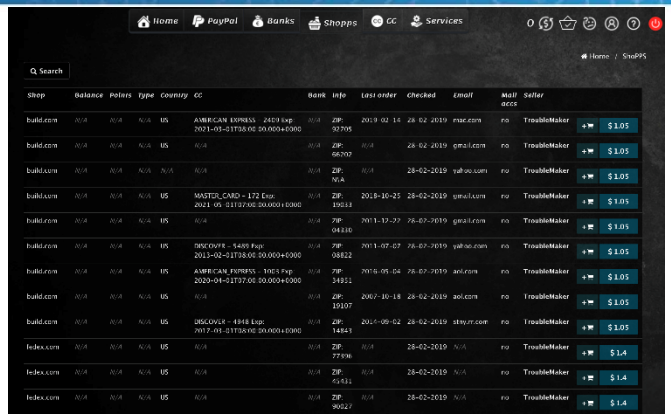
- **COLLECT:** Attackers collect the leaked records (purchased or otherwise acquired)
- **CHECK:** Attackers check the validity of the credentials with a tool (WIRED)
  - Most people don't change their passwords regularly, so even older credential dumps can be used with relative success
  - Because password reuse is rampant, cybercriminals will generally test a set of credentials against numerous different websites
- **AUTOMATE:** Attackers use credential stuffing tools to…
  - Incorporate “proxy lists” to bounce the requests around the web and make them look like they're coming from all different IP addresses.
  - Manipulate properties of login requests so the attempts appear to come from different types of browsers (avoid suspicion)
  - Defeat Captchas

WIRED

Data Dumps – Credential Stuffing

Credential Stuffing Methods and Tools

- Automated marketplaces on the dark web
- Support infrastructure
  - Username/email and password combination lists
  - Proxy service providers
  - Account checking software



To launch a credential stuffing attack, an attacker basically only needs an account checking software, a database of random email [or username] and password combinations, and access to a pool of proxies.

Recorded Future

X- Killer YouTube

Methods/Tools – ‘CHECKERS’

Credential Stuffing Methods and Tools

How Checkers Work

- Checkers (early versions) were made to target a single company
  - The cost would typically be between $50 and $250, depending on the tool’s capabilities.
  - These checkers would attempt to log in to a website using an email and password combination obtained from a random database often obtained on the dark web.
  - If a combination worked, it would be marked as valid (If not, the software would simply pick another combination from the list and attempt to log in again)
  - For successful logins, some checkers would also collect additional information from the compromised account, such as linked banking and payment card information, account balances, the victim’s address, and even transaction history
- Today, there are several cybercriminals that dominant the credential stuffing marketplace
  - Examples: STORM, Black Bullet, SNIPR, Sentry MBA
  - These were more robust tools that supported an unlimited number of custom plugins (“configs”)
  - These offered the cybercriminals (customers) the capability to target almost any company with an online login portal presence.

Recorded Future

Methods/Tools – 'CHECKERS'

Credential Stuffing Methods and Tools

Economics of Credential Stuffing

- Some of the most prominent account shops have tens of millions of compromised accounts for sale at any given moment.

- Despite the low average sale price of compromised credentials, the overall profitability of credential stuffing attacks increased significantly through sheer volume.

- According to Recorded Future, (based on a conservative success rate of one percent per 100,000 compromised emails and passwords) the economics behind credential stuffing attacks reveals at least 20 times higher profit levels.

Recorded Future

Credential Stuffing Tool

Sentry MBA → Credential Stuffing Tool (Shape Security)

- One of the more prominent and readily available examples of account-checking software available
- Sentry MBA has been actively advertised on the dark web since late 2014
  - The official Sentry MBA Twitter account was launched in July 2013.
- Sentry MBA uses OCR (optical character recognition) functionality to bypass captcha
- Can be configured to recognize specific keywords associated with a website's responses to successful and unsuccessful login attempts.

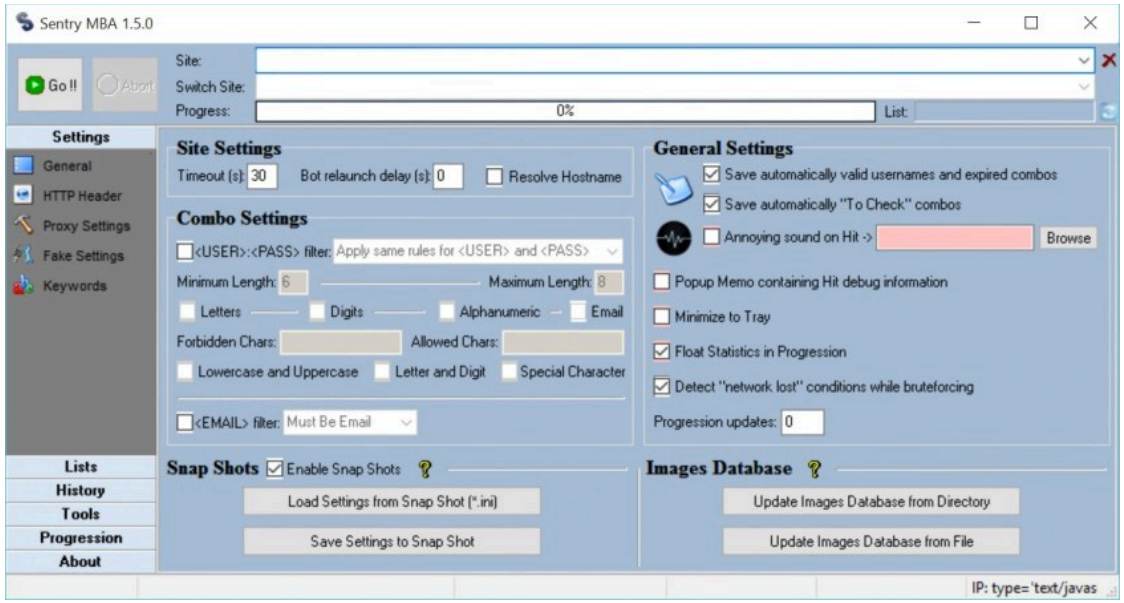
Available Configs: More than 1000

Official Website: https://sentry[.]mba

Price: Between $5 and $20 per config file

Supports HTTP/HTTPS

Supports SOCKS4 and SOCKS5



Sentry MBA Control Panel

Recorded Future

Credential Stuffing Tool

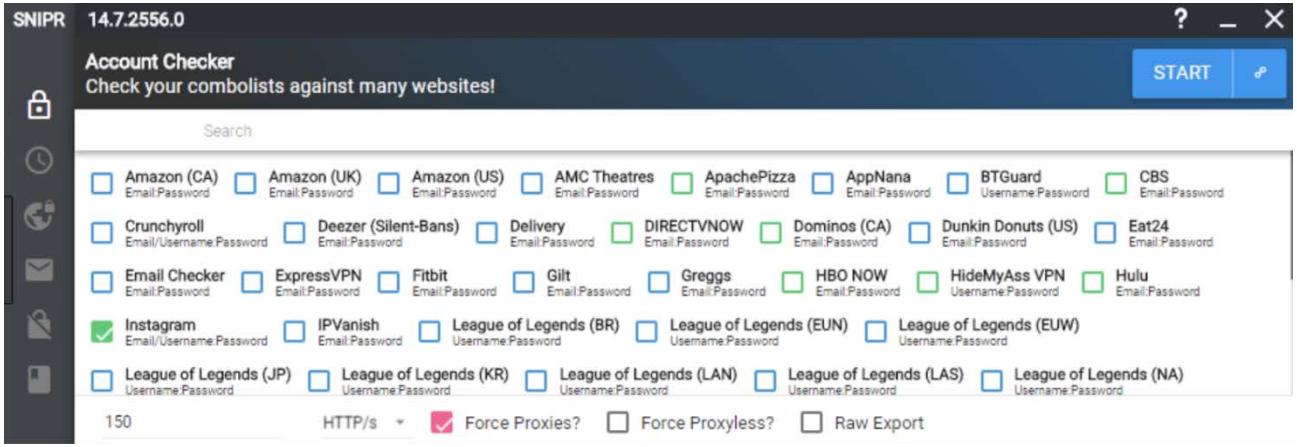
SNIPR → Credential Stuffing Tool (Shape Security)

- SNIPR is sold and publicly shared on multiple underground forums.
- Described as a configurable account-checking software, written in C language that supports both online credential stuffing and offline brute-forcing dictionary attacks.
- SNIPR has its own website with a forum and a marketplace www.snipr[.]gg.
  - The website allows third party developers to share custom-made configuration files.

Configuration files: More than 100 are part of the official package

Concurrent attacks: Up to four targets

Price: $20



SNIPR Control Panel

Recorded Future

Credential Stuffing Example

Large Financial Organization – 2018 (Double Octopus)

- Credential stuffing attack enabled unauthorized access to data of up to 14,000 customers, including….
  - Names, mailing addresses, phone numbers, email addresses
  - Account data → account numbers, balances, and transaction histories
- The unauthorized access lasted from October 4th through October 14, 2018

Tax Preparation Company – 2015 (Big Law Business)

- Credential stuffing attack enabled unauthorized access to 9,000 TaxSlayer customers' accounts, including…
  - details about customers ranging from their SSNs, bank account and credit card numbers, marital status, dependents, financial assets, and health insurance.
  - Attackers filed an unknown number of fraudulent returns, directing refunds to themselves instead of to the actual taxpayers.
- The unauthorized access lasted from October through December, 2015

Double Octopus

Credential Stuffing Example

Health Insurance Company – 2018

- Unknown, unauthorized actor obtained system credentials for employees of a health insurance company, and gained access to websites where people can log in to apply for healthcare policies
- The intruder had access to the data from May 30 through September 13, 2018
- Breach affected consumer insurance applications and data within them, including…
  - Birthdates
  - Addresses
  - Last four digits of Social Security numbers (SSN)
  - Insurance-related data (policy or application numbers, type and cost of coverage)

According to the chief privacy officer's observations….

- The volume of attacks indicated a "large and broad-based automated attack"
- The attacker had a large amount of user IDs and passwords, and was attempting to see which combinations were valid.
- The amount of failures shows the ID/password combos didn't come from [the Health Insurance company]

DARKReading

Protection / Detection

Protections options against credential stuffing (SAGE)

Don't use the same passwords at multiple sites → *especially* where protected and / or sensitive information is exchanged

- It is difficult to manage multiple passwords, but very necessary
- Consider using a password manager tool to securely generate, encrypt, and store your passwords.

Always turn on multifactor / two-factor (MFA/2FA) authentication

- Two-factor authentication provides an extra layer of security because it requires at least two things to access an account
  - Something you know (a password)
  - Something you have (an authentication code generated by an authenticator app on your phone or a One-Time-PIN texted to your phone),
  - Something you are (a fingerprint).
  - List of websites that support 2FA: https://twofactorauth.org

Change your passwords regularly

- If credentials have already been compromised, a credential stuffing attack can be thwarted by changing your passwords.
- Criminals are opportunistic, and a failed login attempt with invalid credentials might discourage them

Protection / Detection

Mitigating Credential Stuffing Attacks (JASK)

Recommended authentication policy:

- Password change period (Default 90 days)
- Account lock after a number of failed attempts
- Enforce complex passwords
- Rate limit logins per IPs and accounts (Must include APIs as well)
- Enforce Multi Factor Authentication (MFA)

Additional Reading / Recommended Policies:

The Open Web Application Security Project (OWASP) offers cheat sheets for IT and security professionals to implement within their enterprise security policies:

- Apply OWASP credential stuffing prevention cheat (Available Here)
- Apply OWASP Brute Force prevention measures (Available Here)

Protection / Detection

Sentry MBA Detection (Shape Security)

Sentry MBA default User Agent strings

By default, Sentry MBA uses the following five User Agent strings:

- Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
- Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
- Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
- Mozilla/5.0 (Windows; U; Windows NT 5.1; en) AppleWebKit/522.11.3 (KHTML, like Gecko) Version/3.0 Safari/522.11.3
- Opera/9.80 (Windows NT 6.0; U; en) Presto/2.2.0 Version/10.00

If you find these User Agent strings in your web logs, you should also be able to find some characteristics of credential stuffing.

Reference Materials

References

- Abcd
  - Abcdefg.com

Questions

Questions

Upcoming Briefs

- Triton/Trisis/HatMan Malware
- Software Subversion

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

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

Threat Briefings & Webinar

Briefing document and presentation that provides 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.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV