ERT Threat Alert
Credential Stuffing Campaign
October 19, 2018

Abstract

Over the last few weeks, Radware has been tracking a credential stuffing campaign targeting the financial industry in the United States and Europe. Credential stuffing is an emerging threat in 2018 that has continued to accelerate over the past month as more breaches occur. Today, a breach doesn't just impact the compromised organization and its users, but it also affects every other website that the users may use.

Additionally, resetting passwords for a compromised application will only solve the problem locally; criminals are still able to leverage those credentials externally against other applications due to poor user credential hygiene.

Credential stuffing is a subset of Brute Force attacks but is different from credential cracking. These campaigns do not involve the process of brute forcing password combinations and leverage leaked username and passwords in an automated fashion against numerous websites to hyjack user accounts due to credential reuse.

Criminals collect and data mine leaked databases and breached accounts for several reasons. Typically cybercriminals will keep this information for future targeted attacks, sell it for profit or exploit it in fraudulent ways.

The current campaign Radware is witnessing is motivated by fraud. Criminals are using credentials from prior data breaches to gain access to a users' bank accounts. These attackers have been seen targeting financial organizations in both the United States and Europe. When significant breaches occur, the compromised emails and passwords are quickly leveraged by cybercriminals. Armed with tens of millions of credentials from recently breached websites, attackers will use these credentials, along with scripts and proxies, to distribute their attack against the financial institution in an attempt to take over banking accounts. These login attempts can happen in such volumes that they resemble a distributed denial-of-service (DDoS) attack.

Attack Methods

Credential Stuffing

Credential stuffing is one of the most commonly used attack vectors by cybercriminals today. It's an automated web injection attack where criminals use a list of breached credentials in an attempt to gain access and take over accounts across different platforms due to poor credential hygiene. Attackers will route their login request through proxy servers to avoid blacklisting their IP address.

Attackers automate the logins of millions of previously discovered credentials with automation tools like cURL and PhantomJS or tools designed specifically for the attack, like Sentry MBA and SNIPR.

This threat is dangerous to both the consumer and organizations due to the ripple effect caused by data breaches. When a company is breached, compromised credentials will either be used by the attacker or sold to other cybercriminals. Once credentials reach a final destination, a for-profit criminal will use the data or credentials obtained from a leaked site to take over user accounts on multiple websites like social media, banking, and marketplaces. In addition to the threat of fraud and identity theft to the consumer, organizations have to mitigate credential stuffing campaigns that generate high volumes of login requests, consuming resources and bandwidth in the process.

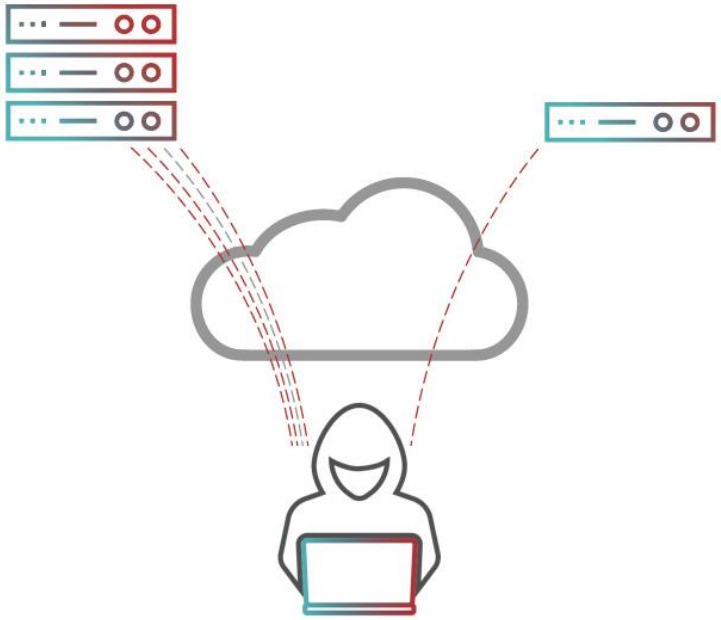

Figure 1: Credential stuffing attack

Credential Cracking
Credential cracking attacks are an automated web attack where criminals attempt to crack users' passwords or PIN numbers by processing all possible combinations of characters in a specific sequence. These attacks are only possible when applications do not have a lockout policy for failed login attempts.

Attackers will use a list of common words or recently leaked passwords in an automated fashion to take over a specific account. Software for this attack will attempt to crack the user's password by mutating or brute forcing values until authentication.

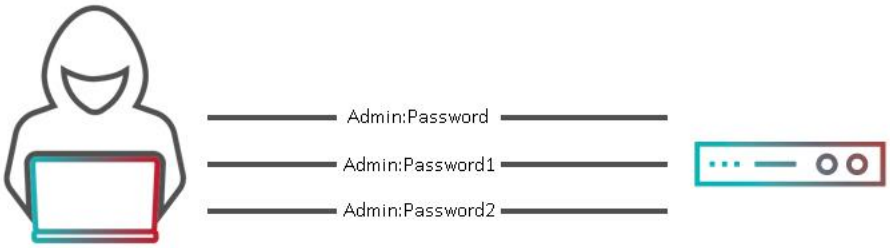

Figure 2: Credential cracking

Targets
In recent campaigns, Radware has seen financial institutions targeted in both the United States and Europe by credential stuffing campaigns.

Crimeware

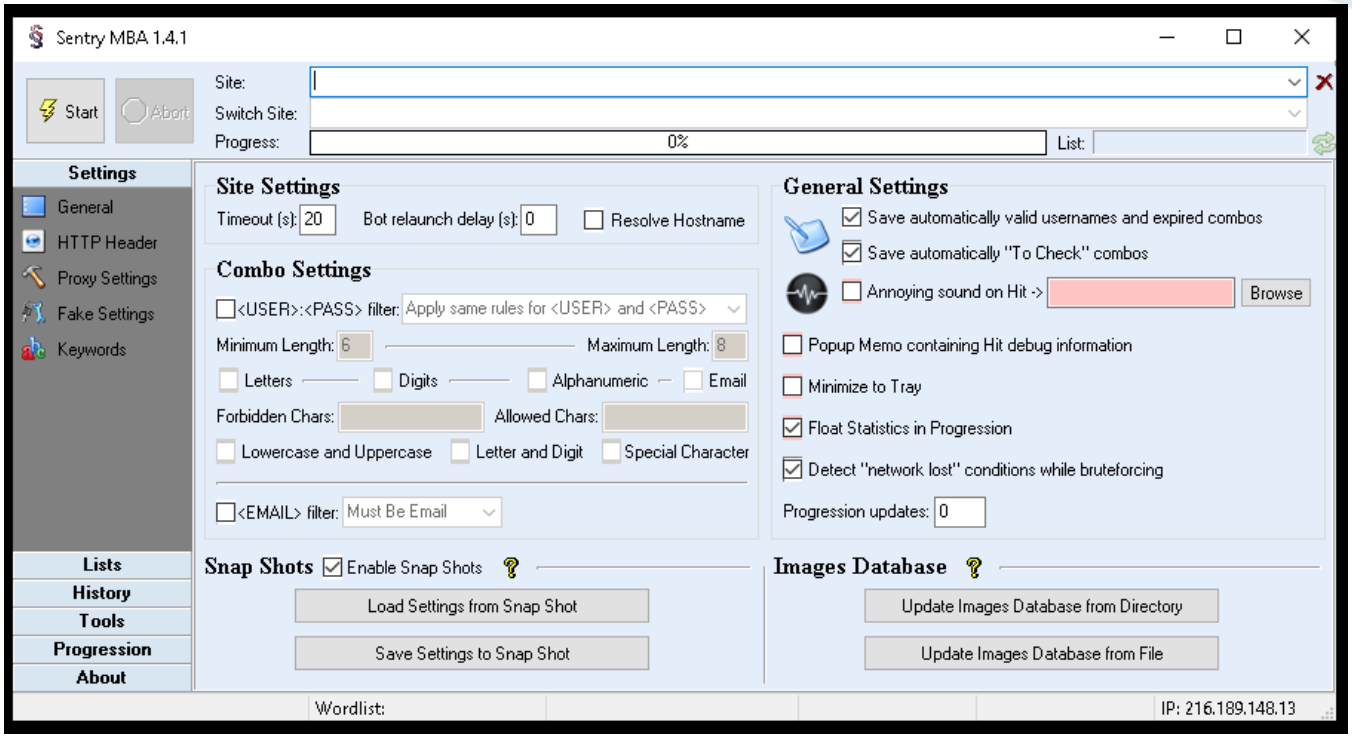

Figure 3: Sentry MBA – Password stuffing toolkit

Sentry MBA is one of the most popular credential stuffing toolkits used by cybercriminals today. This tool is hosted on the Sentry MBA crackers forum. The tool simplifies and automates the process of checking credentials across multiple websites and allows the attackers to configure a proxy list so they can anonymize their login requests.

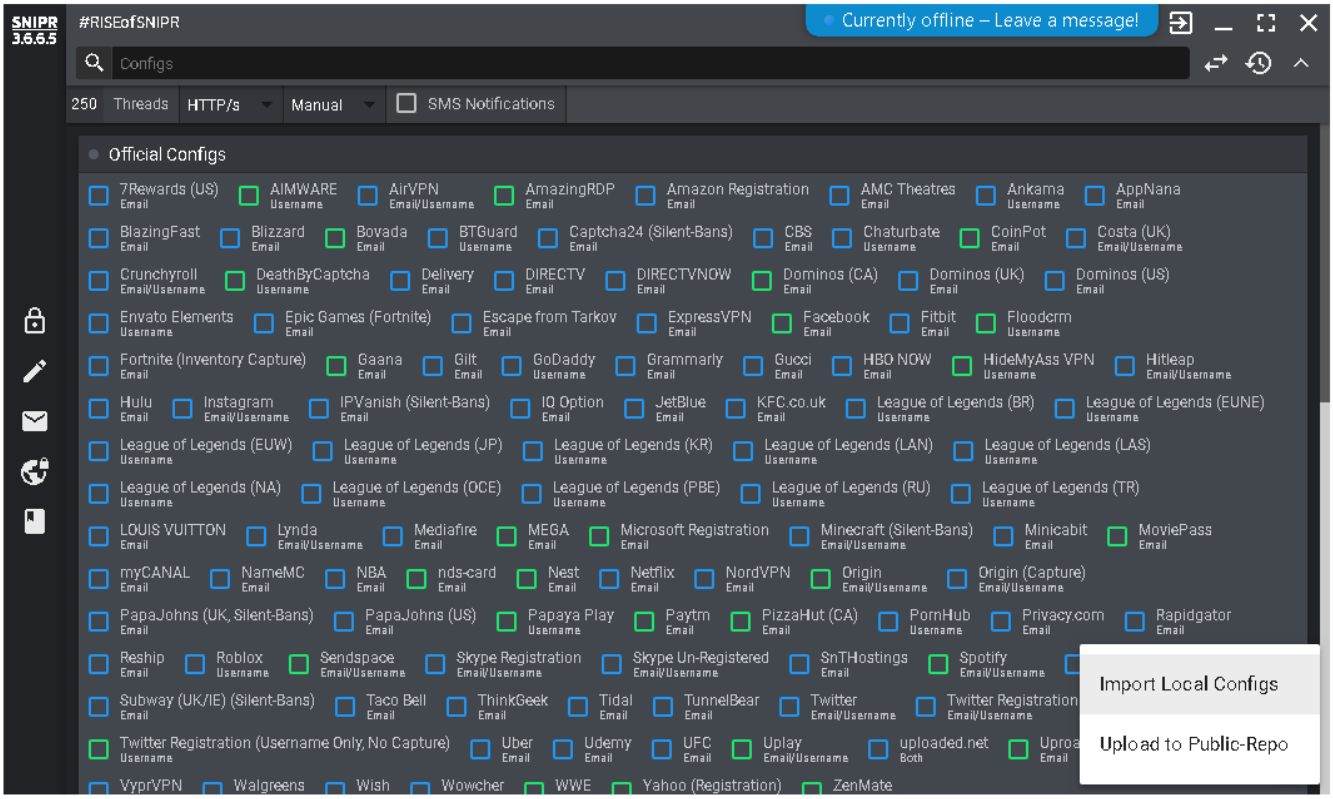

Figure 4: SNIPR – credential stuffing toolkit

SNIPR is a popular credential stuffing toolkit used by cybercriminals and is found hosted on the SNIPR crackers forums. SNIPR comes with over 100 config files preloaded and the ability to upload personal config files to the public repository.

Reasons for Concern

Recent breaches over the last few years have exposed hundreds of millions of users' credentials. One of the main reason for concern of a credential stuffing campaign is due to the impact that it has on the user. Users who reuse credentials across multiple websites are exposing themselves to an increased risk of fraud and identity theft.

The second concern is for organizations who have to mitigate high volumes of fruadulate login attempts that can saturate a network. This saturation can be a cause for concern as it will appear to be a DDoS attack, originating from random IP addresses coming from a variety of sources, including from behind proxies. These requests will look like legitimate attempts since the attacker is not running a Brute Force attack. If the user for that account does not exist or authenticate on the targeted application, the program will move to the next set of credentials.

Mitigation

To defend against a credential stuffing campaigns organizations need to deploy a WAF that can properly fingerprint and identify malicious bot traffic as well as automated login attacks directed at your web application. Radware's AppWall addresses the multiples challenges faced by credential stuffing campaigns by introducing additional layers of mitigation including activity tracking and source blocking.

Radware's AppWall is a WAF capable of securing web applications as well as enabling PCI compliance by mitigating web application security threats and vulnerabilities. Radware's WAF prevents data from leaking or being manipulated which is critically important in regard to sensitive corporate data and/or information about its customers.

The AppWall security filter also detects such attempts to hack into the system by checking the replies sent from the Web server for Bad/OK replies in a specific timeframe. In the event of a Brute Force attack, the number of negative replies from the web server (due to bad username, incorrect password, etc.) triggers the Brute Force security filter to monitor and take action against that specific attacker. This blocking method prevents a hacker from using automated tools to carry out an attack against web application login pages.

In addition to these steps, network operators should apply two-factor authentication where eligible and monitor dump credentials for potential leaks or threats.

Effective Web Application Security Essentials

- **Full OWASP Top-10** coverage against defacements, injections, etc.
- **Low false positive rate –** using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources
- **Flexible deployment options -** on-premise, out-of-path, virtual or cloud-based

Under Attack and in Need of Emergency Assistance? Radware Can Help

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, Contact us with the code "Red Button."

Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit DDoSWarriors.com. Created by Radware's Emergency Response Team (ERT), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cybersecurity.