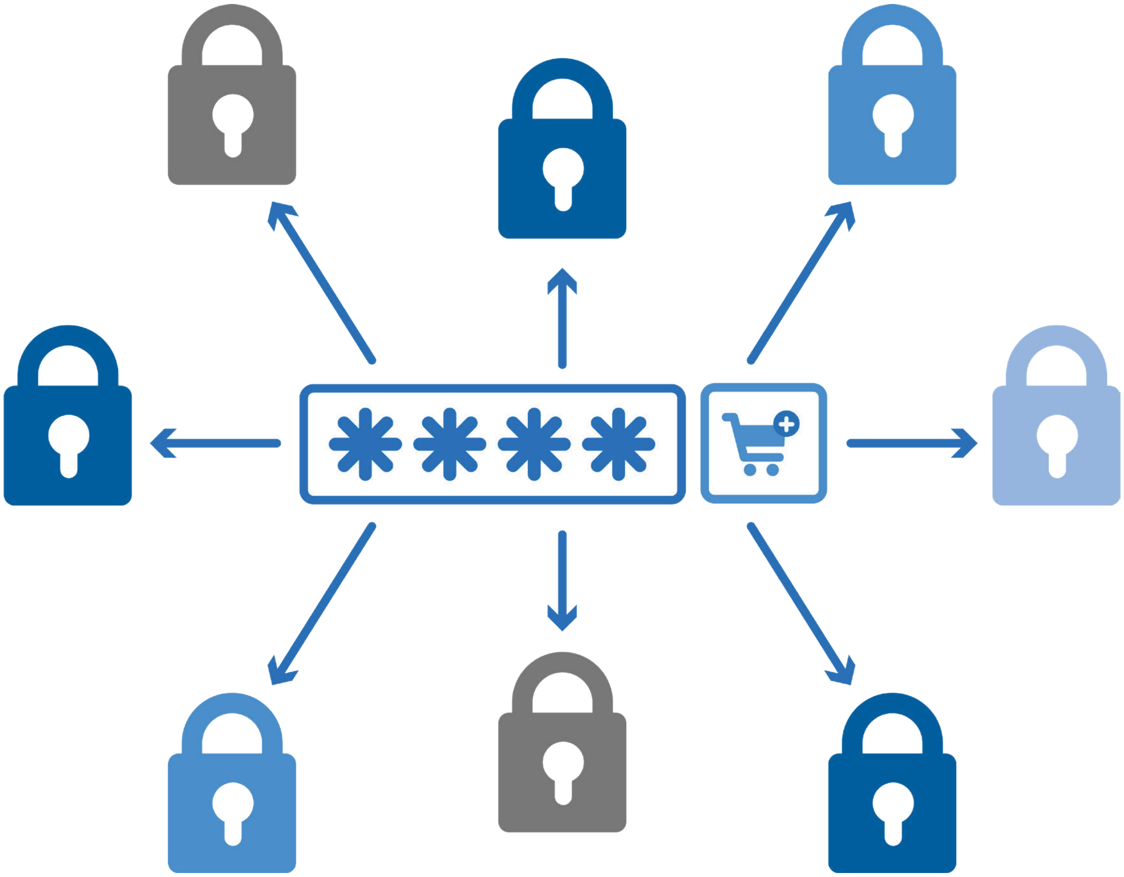
Recorded Future

CYBER THREAT ANALYSIS

The Economy of Credential Stuffing Attacks

By Insikt Group



CTA-2019-0425

This report covers the current threat landscape of credential stuffing attacks. It reviews the most popular tools used by cybercriminals to initiate credential stuffing and describes some of the most popular marketplaces that sell compromised credentials. This report contains information gathered using the Recorded Future® Platform, as well as additional open source, dark web, and underground forum research, and will be of most interest to analysts protecting e-commerce, telecommunications, and financial organizations from credential stuffing attacks, as well as those looking for investigative leads on threat actors performing such attacks.

Executive Summary

The rapid proliferation of automated marketplaces on the dark web, fueled by the widespread availability of support infrastructure such as account-checking software, email and password combo lists, and proxy service providers, has created the perfect attack landscape for the abuse of thousands of popular web services such as e-commerce, financial services, travel websites, and telecommunications companies. It is safe to assume that almost every large organization with an online retail presence has had their users exposed to credential stuffing attacks in the past few years, with some companies having upwards of millions of exposed login credentials available for purchase on the dark web at any given moment.

Key Judgments

- The first widespread credential stuffing attacks were observed in late 2014, coinciding with the proliferation of automated underground marketplaces. When selling accounts, attackers offered the quick and easy monetization of compromised account credentials. Some actors who engaged in credential stuffing attacks remain active today.
- With an investment of as little as $550, criminals could expect to earn at least 20 times the profit on the sale of compromised login credentials.
- The overall supply of compromised login credentials across several large marketplaces exceeds tens of millions of accounts.
- Insikt Group identified at least six popular variants of account-checking software used by cybercriminals; however, dozens of lesser-known variants can be found on the dark web.

- While some companies may choose to implement multi-factor authentication (MFA), which blocks the credential stuffing attack vector, organizations may not be prepared to choose security over convenience.

Background

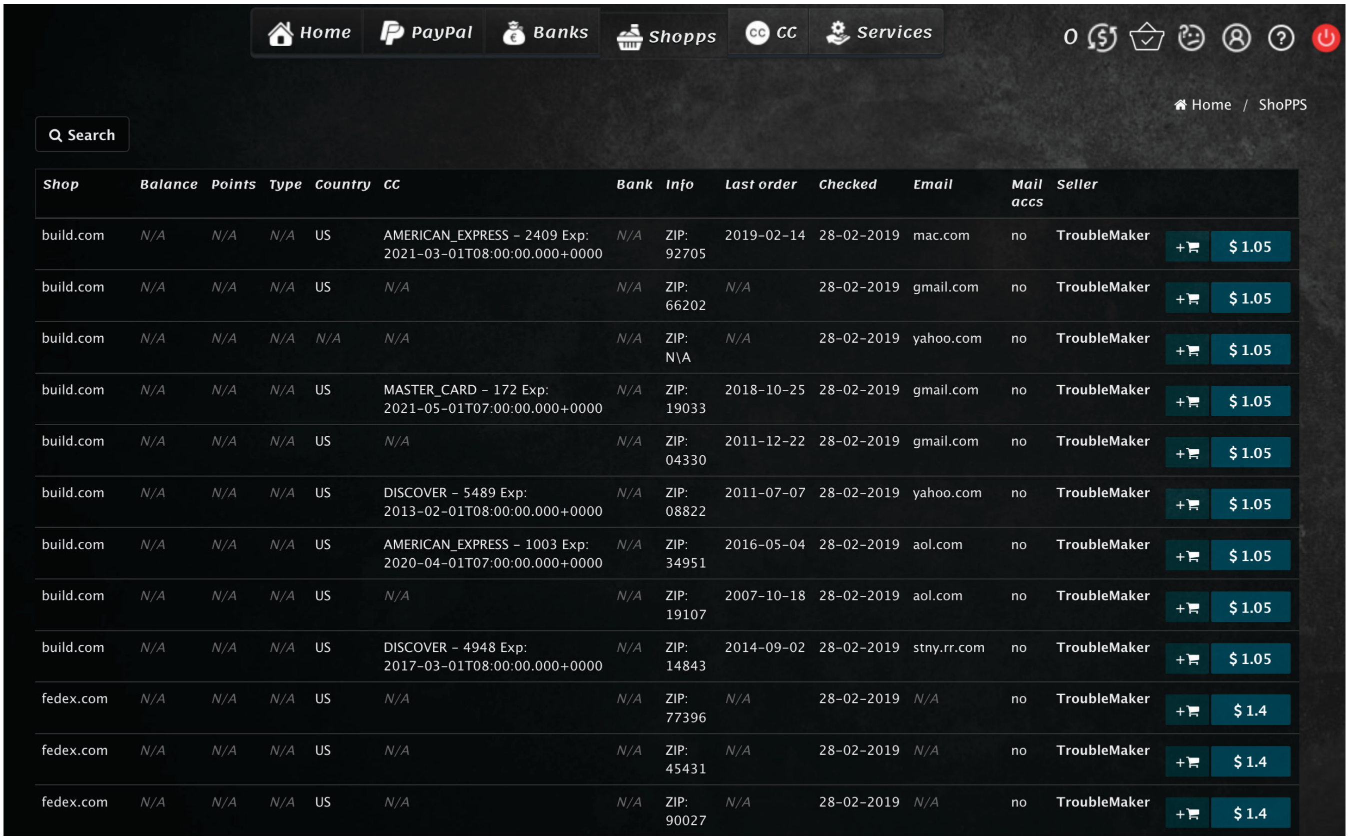
Around late 2014 and in the beginning of 2015, we observed the widespread adoption of new dark web business models specifically tailored to facilitate a high volume of trades in a fully automated manner. Designed to emulate legitimate retail platforms such as eBay and Amazon, these so-called "automated shops" allow even low-level criminals to become vendors of stolen data, such as compromised login credentials, without having to worry about maintaining their own infrastructure or marketing campaigns. By and large, the adoption of account marketplaces was made possible primarily by the proliferation of account-checking software, or simply "checkers," used as the main tool in credential stuffing attacks.

Threat Analysis

Compromised account credentials were always a valuable commodity in the dark web — the number of transactions was relatively small, and they were primarily conducted either on a peer-to-peer basis or via semi-automated markets such as AlphaBay, Silk Road, and Hansa Market. In older models, buyers received their wares only after the seller manually approved the deal and delivered the purchased data. Moreover, sellers had to maintain the listings and communicate with the buyers personally.

However, with the advent of automated shops, the need for manual engagement was eliminated and the business of compromised accounts fully transitioned from peer-to-peer dealings to a much more democratized, open-to-everyone enterprise.

For a nominal 10 to 15 percent commission deducted from the amount of each sale, members can upload any number of validated compromised accounts, which in addition to email and password, often include data such as the account holder's city or state of residency, transaction history, and/or account balance. All of this is valuable data to fraudsters seeking to buy accounts tailored to their specific needs. The vendor's main focus is replenishing the stock, while all customer support, remittances, and dispute resolutions are handled by the shop's support team.

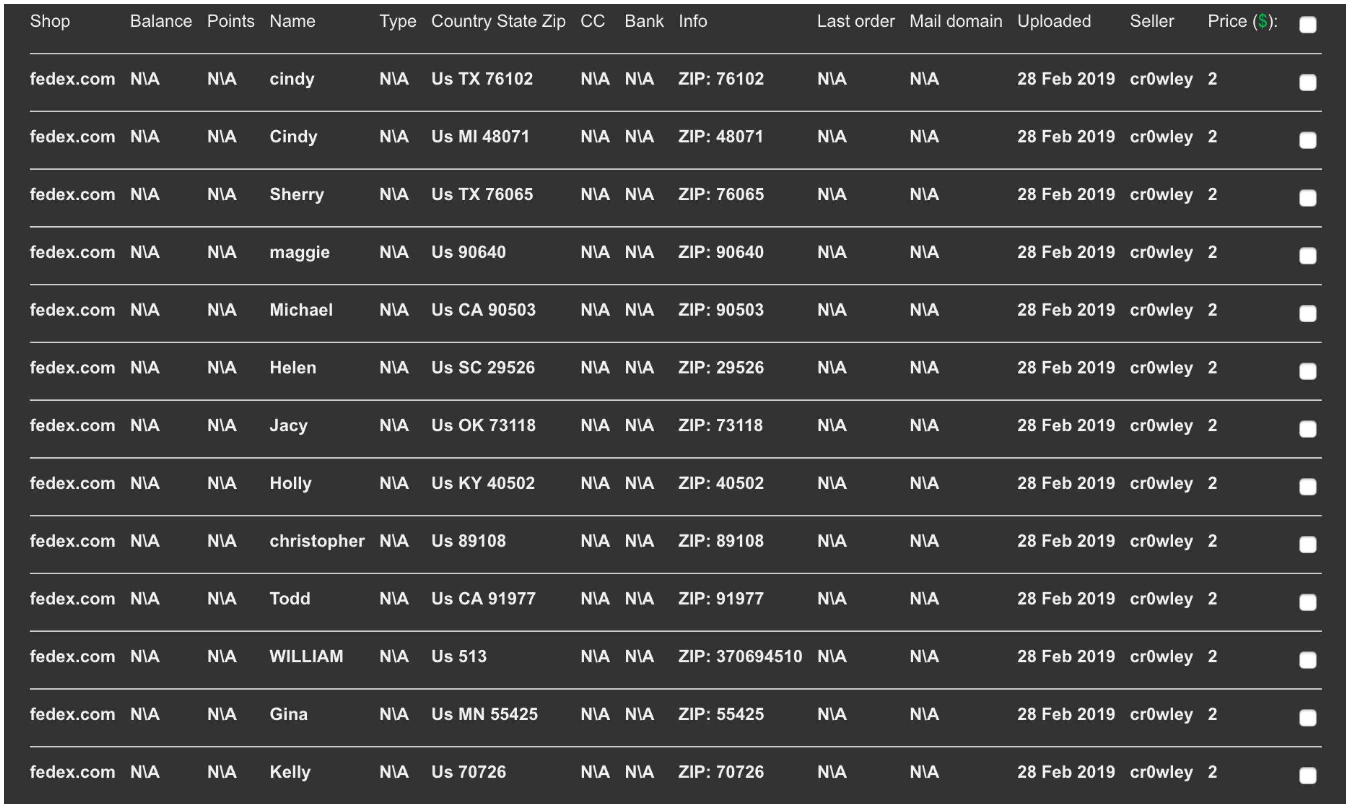


Shop	Balance	Points	Type	Country	CC	Bank	Info	Last order	Checked	Email	Mail accs	Seller		
build.com	N/A	N/A	N/A	US	AMERICAN_EXPRESS - 2409 Exp: 2021-03-01T08:00:00.000+0000	N/A	ZIP: 92705	2019-02-14	28-02-2019	mac.com	no	TroubleMaker	+🛒	$ 1.05
build.com	N/A	N/A	N/A	US	N/A	N/A	ZIP: 66202	N/A	28-02-2019	gmail.com	no	TroubleMaker	+🛒	$ 1.05
build.com	N/A	N/A	N/A	N/A	N/A	N/A	ZIP: N\A	N/A	28-02-2019	yahoo.com	no	TroubleMaker	+🛒	$ 1.05
build.com	N/A	N/A	N/A	US	MASTER_CARD - 172 Exp: 2021-05-01T07:00:00.000+0000	N/A	ZIP: 19033	2018-10-25	28-02-2019	gmail.com	no	TroubleMaker	+🛒	$ 1.05
build.com	N/A	N/A	N/A	US	N/A	N/A	ZIP: 04330	2011-12-22	28-02-2019	gmail.com	no	TroubleMaker	+🛒	$ 1.05
build.com	N/A	N/A	N/A	US	DISCOVER - 5489 Exp: 2013-02-01T08:00:00.000+0000	N/A	ZIP: 08822	2011-07-07	28-02-2019	yahoo.com	no	TroubleMaker	+🛒	$ 1.05
build.com	N/A	N/A	N/A	US	AMERICAN_EXPRESS - 1003 Exp: 2020-04-01T07:00:00.000+0000	N/A	ZIP: 34951	2016-05-04	28-02-2019	aol.com	no	TroubleMaker	+🛒	$ 1.05
build.com	N/A	N/A	N/A	US	N/A	N/A	ZIP: 19107	2007-10-18	28-02-2019	aol.com	no	TroubleMaker	+🛒	$ 1.05
build.com	N/A	N/A	N/A	US	DISCOVER - 4948 Exp: 2017-03-01T08:00:00.000+0000	N/A	ZIP: 14843	2014-09-02	28-02-2019	stny.rr.com	no	TroubleMaker	+🛒	$ 1.05
fedex.com	N/A	N/A	N/A	US	N/A	N/A	ZIP: 77396	N/A	28-02-2019	N/A	no	TroubleMaker	+🛒	$ 1.4
fedex.com	N/A	N/A	N/A	US	N/A	N/A	ZIP: 45431	N/A	28-02-2019	N/A	no	TroubleMaker	+🛒	$ 1.4
fedex.com	N/A	N/A	N/A	US	N/A	N/A	ZIP: 90027	N/A	28-02-2019	N/A	no	TroubleMaker	+🛒	$ 1.4

Automatic shop listings. Alongside the compromised company name, buyers can see the available balance or loyalty points, the account holder's place of residency, associated payment cards, the date of the last transaction, and a hostname of the account holder's login email.

At first, only a handful of select vendors became the primary suppliers of stolen data, but as the tradecraft was shared among members of the criminal underground, the business of stolen credentials has grown exponentially.

Since regular internet users tend to reuse the same passwords across multiple websites, threat actors quickly learned that instead of attempting to obtain access to an individual account, which may take a very long time, they should instead focus on hacking multiple random accounts, reducing their efforts.



Shop	Balance	Points	Name	Type	Country State Zip	CC	Bank	Info	Last order	Mail domain	Uploaded	Seller	Price ($):	☐
fedex.com	N\A	N\A	cindy	N\A	Us TX 76102	N\A	N\A	ZIP: 76102	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	Cindy	N\A	Us MI 48071	N\A	N\A	ZIP: 48071	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	Sherry	N\A	Us TX 76065	N\A	N\A	ZIP: 76065	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	maggie	N\A	Us 90640	N\A	N\A	ZIP: 90640	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	Michael	N\A	Us CA 90503	N\A	N\A	ZIP: 90503	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	Helen	N\A	Us SC 29526	N\A	N\A	ZIP: 29526	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	Jacy	N\A	Us OK 73118	N\A	N\A	ZIP: 73118	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	Holly	N\A	Us KY 40502	N\A	N\A	ZIP: 40502	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	christopher	N\A	Us 89108	N\A	N\A	ZIP: 89108	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	Todd	N\A	Us CA 91977	N\A	N\A	ZIP: 91977	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	WILLIAM	N\A	Us 513	N\A	N\A	ZIP: 370694510	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	Gina	N\A	Us MN 55425	N\A	N\A	ZIP: 55425	N\A	N\A	28 Feb 2019	cr0wley	2	☐
fedex.com	N\A	N\A	Kelly	N\A	Us 70726	N\A	N\A	ZIP: 70726	N\A	N\A	28 Feb 2019	cr0wley	2	☐

Slilpp automatic shop listings.

A combination of several elements made the hacking of various online services accounts not just effortless, but also incredibly lucrative. To launch account brute-forcing, also known as credential stuffing attacks, an attacker only needed brute-forcing software, a database of random email and password combinations, and access to a pool of proxies.

The Economics

Early versions of checkers were made to target a single company and were sold for between $50 and $250, depending on the tool's capabilities. These tools 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 valid logins, more expensive and complex checkers would also collect additional information from the compromised account, such as linked banking and payment card information, account balances, the owner's address, and even transaction history. Until this day, the ingenuity of the method truly lies in the economy of scale, allowing criminals to process hundreds of thousands of combinations in a very short period of time.

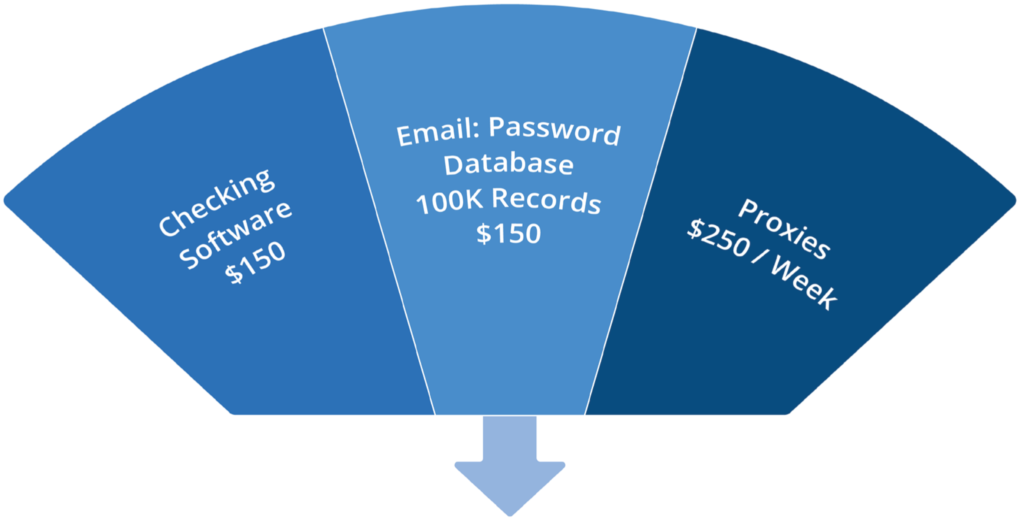
Eventually, several dominant players such as STORM, Black Bullet, and Sentry MBA entered the market with more robust tools, supporting an unlimited number of custom plugins, also called "configs," which essentially offered hackers the capability to target almost any company with an online retail presence.

What had initially started as several hundred or several thousand compromised accounts quickly ballooned to hundreds of thousands, or even millions, of accounts. Some of the most prominent account shops have tens of millions of compromised accounts for sale at any given moment.

Although the competition quickly brought the average price of a single compromised account from over $10 down to a mere $1 to $2, the overall profitability of credential stuffing attacks increased significantly through sheer volume.

According to underground chatter observed over time, the average success rate for credential stuffing is anywhere between one to three percent. Hence, for every one million random combinations of emails and passwords, attackers can potentially compromise between 10,000 and 30,000 accounts. Moreover, the same database could then be reused over and over again to hack dozens of different websites, yielding even higher profits.

Credential Stuffing Economics



Checking Software $150

Email: Password Database 100K Records $150

Proxies $250 / Week

Victim	Average Price	Max. Potential Profit
Amazon	$2.00	$2,000
PayPal	$1.00	$1,000
eBay	$3.50	$3,500
Expedia	$0.50	$500
Airbnb	$1.50	$1,500
FedEx	$1.50	$1,500
Credit Karma	$2.00	$2,000
Online Video Service	$1.40	$1,400
Xfinity	$3.50	$3,500

Gross Profit Margin	97.5%	Gross Profit $19,150
	2.5%	Direct Cost $550

← Max. Selling Price $19,700

← Gross Price $550

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.

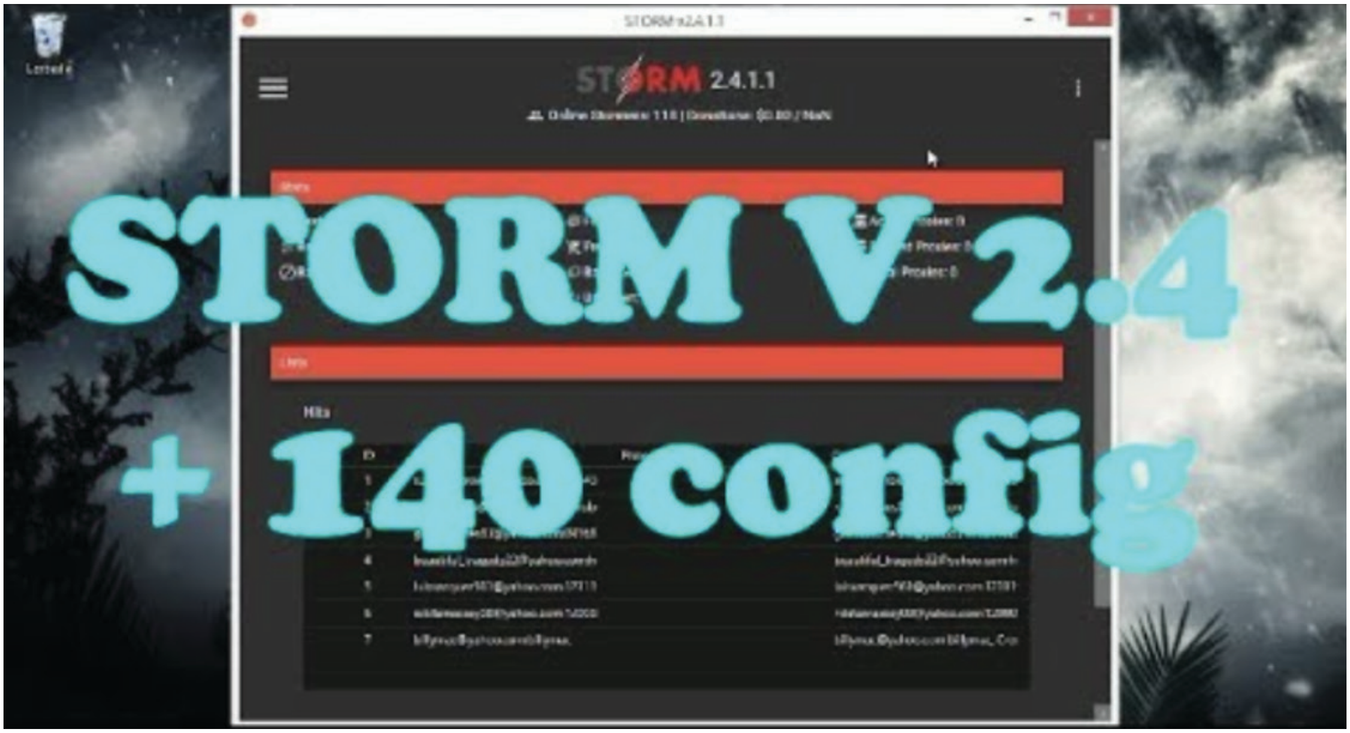
Technical Analysis

Below are the most prominent variants of account-checking software used by cybercriminals in credential stuffing campaigns. It is important to note that lesser-known solutions, which are often built to target a single company, are also available for purchase. However, such one-off tools rarely gain significant market presence and tend to disappear quickly, as the developers cease product support due to slow adoption.

STORM

STORM is marketed across several English-speaking forums, and unlike other account-checking tools, is available free of charge. However, users are encouraged to make donations. The exact identity of the developer is unknown; however, according to underground forum chatter, the software was allegedly created by the actor mrviper. STORM was first launched in January 2018, and according to the description found on dark web advertisements, it is characterized as a free "cracking" program designed to perform website security testing. STORM is written in C language and was developed in close cooperation with members of the Cracked forum. The tool has the following technical features:

- Supports FTP cracking
- Simultaneous FTP and HTTP attacks
- Concurrent sessions
- Debug functionality for activity analysis
- Supports combo lists of up to 20 million email:password records
- Supports HTTP/HTTPS
- Supports SOCKS4 and SOCKS5
- Proxy auto update with automated harvesting from public sources
- Keywords capture (collection of premium account details)
- JavaScript redirect



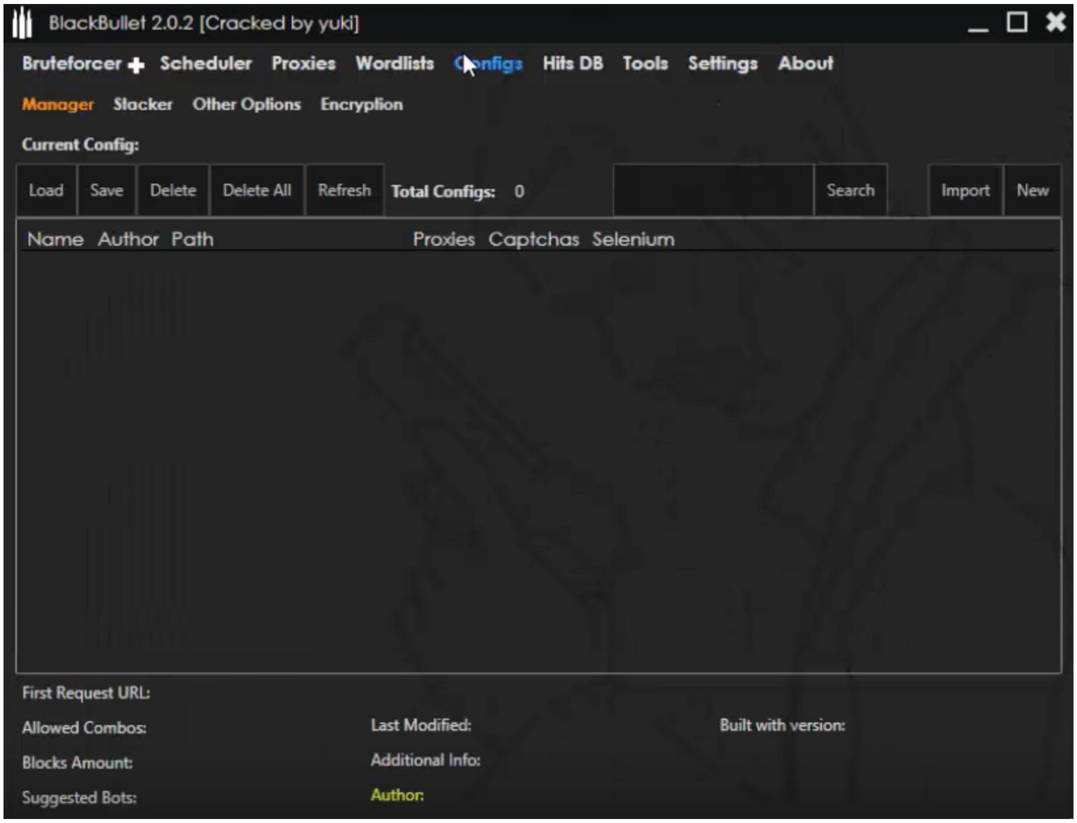
STORM account cracker advertisement on the dark web.

Black Bullet

Black Bullet first appeared on the dark web in early 2018 and likely was created by the actor Ruri, who operates the official www.bullet[.]black website; however, according to the information found on the main page, the community no longer accepts new members. Several members of the dark web, including daltonbean8 and Doberman, were observed distributing the tool.

In contrast to other account-checking tools, BlackBullet does not offer multi-threaded capabilities, and only allows a single company at a time to be attacked. The tool also comes with a brute-forcing feature that can perform dictionary attacks when run against specific accounts.

- Captchas bypass
- Configuration files: ~ 530; however, users have an option to modify and create new configurations themselves
- Selenium Webdriver support
- Price: Between $30 and $50



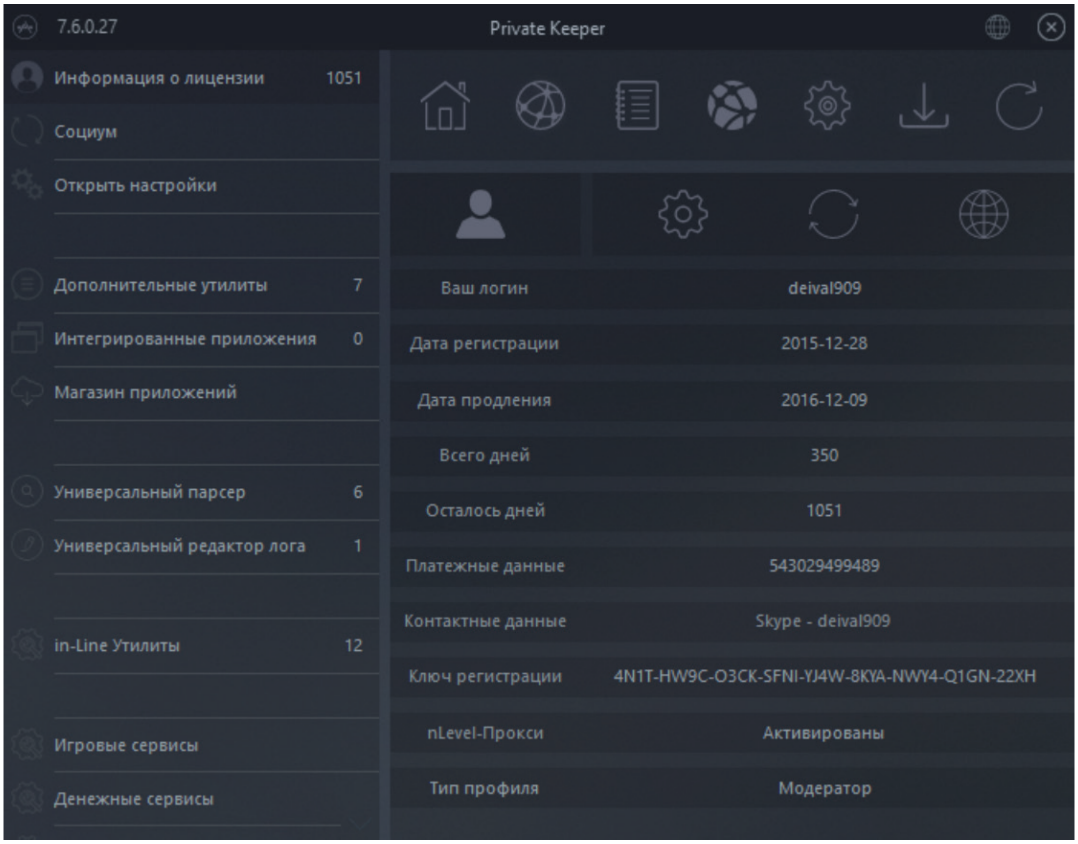
Total Configs: 0

BlackBullet V.2.0.2 control panel interface.

Private Keeper

Private Keeper was developed by the actor deival909. According to the description provided by the actor, the tool is based on in-line technology. Private Keeper is by far the most popular account-checking software in the Russian-speaking underground.

- Price: From 49 Russian rubles (approximately $0.80)
- Concurrent sessions
- Utility software to aid in automated connection to the private or publicly available proxy services
- Official online store: www.deival909[.]ru
- Latest version: 7.9.3.34



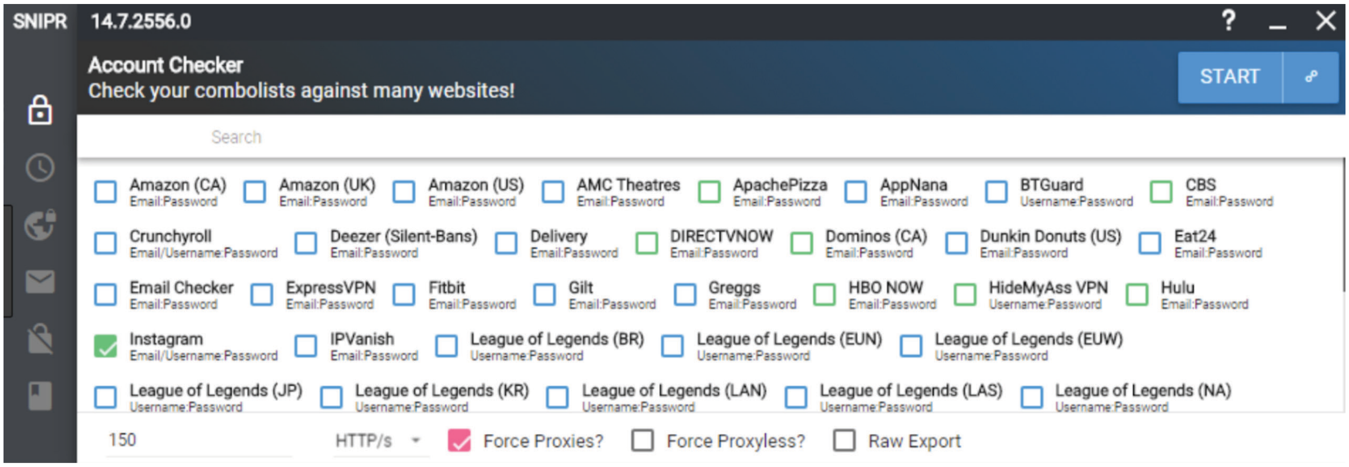
Ваш логин	deival909
Дата регистрации	2015-12-28
Дата продления	2016-12-09
Всего дней	350
Осталось дней	1051
Платежные данные	543029499489
Контактные данные	Skype - deival909
Ключ регистрации	4N1T-HW9C-O3CK-SFNI-YJ4W-8KYA-NWY4-Q1GN-22XH
nLevel-Прокси	Активированы
Тип профиля	Модератор

Private Keeper control panel interface.

SNIPR

SNIPR was sold and publicly shared on multiple underground forums. The threat actor PRAGMA is the developer of the malware. SNIPR is a configurable account-checking software, written in C language that supports both online credential stuffing and offline brute-forcing dictionary attacks. Although the tool was advertised by multiple threat actors, this account checker 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



Account Checker
Check your combolists against many websites!

□ Amazon (CA) Email:Password □ Amazon (UK) Email:Password □ Amazon (US) Email:Password □ AMC Theatres Email:Password □ ApachePizza Email:Password □ AppNana Email:Password □ BTGuard Username:Password □ CBS Email:Password

□ Crunchyroll Email/Username:Password □ Deezer (Silent-Bans) Email:Password □ Delivery Email:Password □ DIRECTVNOW Email:Password □ Dominos (CA) Email:Password □ Dunkin Donuts (US) Email:Password □ Eat24 Email:Password

□ Email Checker Email:Password □ ExpressVPN Email:Password □ Fitbit Email:Password □ Gilt Email:Password □ Greggs Email:Password □ HBO NOW Email:Password □ HideMyAss VPN Username:Password □ Hulu Email:Password

☑ Instagram Email/Username:Password □ IPVanish Email:Password □ League of Legends (BR) Username:Password □ League of Legends (EUN) Username:Password □ League of Legends (EUW) Username:Password

□ League of Legends (JP) Username:Password □ League of Legends (KR) Username:Password □ League of Legends (LAN) Username:Password □ League of Legends (LAS) Username:Password □ League of Legends (NA) Username:Password

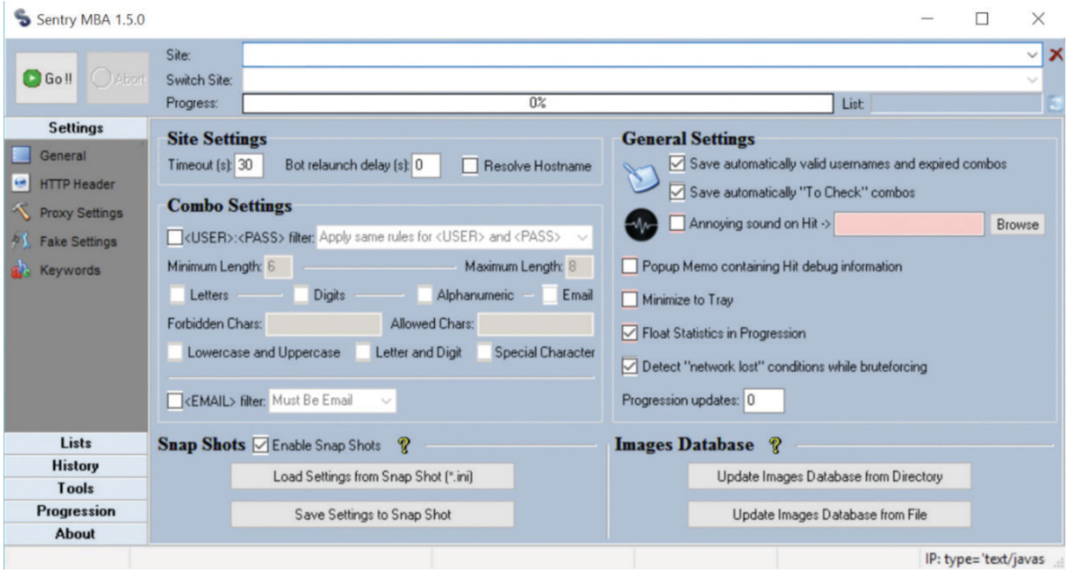
150 HTTP/s ☑ Force Proxies? □ Force Proxyless? □ Raw Export

Over 100 config files are included in the SNIPR account checker by default.

Sentry MBA

Sentry MBA, with over 1,000 configuration files available, is one of the most prominent and readily available examples of account-checking software on the dark web. Several criminal forums maintain ongoing discussion threads dedicated to Sentry MBA. As of December 2018, the registration at https://sentry[.]mba, the official Sentry MBA marketplace and discussion board, is closed and available by invitation only. Insikt Group identified that the tool has been actively advertised on the dark web since late 2014. However, the official Twitter account was launched in July 2013. The tool was allegedly developed by an actor using the alias "Sentinel" and later modified by another actor, "Astaris." Sentry MBA uses OCR (optical character recognition) functionality to bypass captcha. However, Sentry MBA doesn't support Javascript anti-bot challenges. Sentry MBA 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 configuration file
- Supports HTTP/HTTPS
- Supports SOCKS4 and SOCKS5



Site:
Switch Site:
Progress: 0%
List:

Timeout (s): 30
Bot relaunch delay (s): 0
□ Resolve Hostname

□ <USER>:<PASS> filter: Apply same rules for <USER> and <PASS>
Minimum Length: 6
Maximum Length: 8
□ Letters
□ Digits
□ Alphanumeric
□ Email
Forbidden Chars:
Allowed Chars:
□ Lowercase and Uppercase
□ Letter and Digit
□ Special Character
□ <EMAIL> filter: Must Be Email

☑ Save automatically valid usernames and expired combos
☑ Save automatically "To Check" combos
□ Annoying sound on Hit ->
□ Popup Memo containing Hit debug information
□ Minimize to Tray
☑ Float Statistics in Progression
☑ Detect "network lost" conditions while bruteforcing
Progression updates: 0

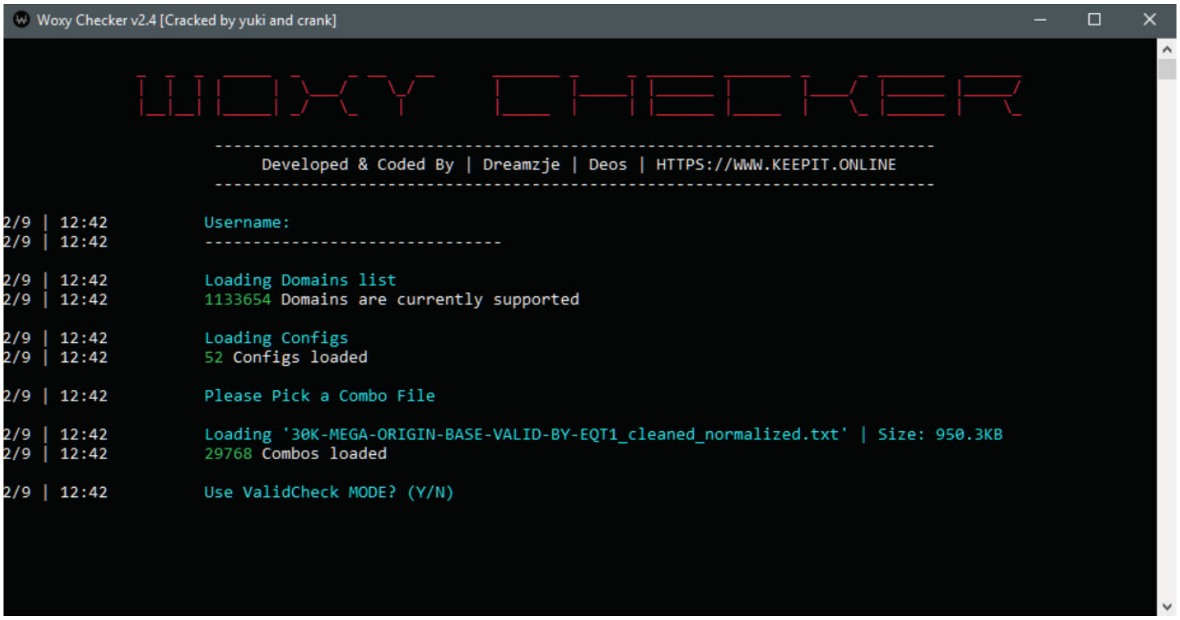
☑ Enable Snap Shots

IP: type='text/javas

Sentry MBA control panel.

WOXY

Unlike a typical account-checking software, the WOXY email checker allows criminals to verify the validity of email accounts, scan email content for valuable information (like gift card codes or online subscriptions to streaming services, travel websites, and financial institutions), and hijack valid accounts by resetting login passwords automatically. According to the conducted analysis, WOXY was developed by the actors Dreamzje and Deos, who operated the currently defunct website www.keepit[.]online. The original price of the WOXY checker was $40; however, in September 2018, actors Crank and Yuki shared the cracked version of WOXY on the dark web, which now can be easily obtained free of charge.



```
          ---------------------------------------------------------------------------
               Developed & Coded By | Dreamzje | Deos | HTTPS://WWW.KEEPIT.ONLINE
          ---------------------------------------------------------------------------

2/9 | 12:42         Username:
2/9 | 12:42         ------------------------------

2/9 | 12:42         Loading Domains list
2/9 | 12:42         1133654 Domains are currently supported

2/9 | 12:42         Loading Configs
2/9 | 12:42         52 Configs loaded

2/9 | 12:42         Please Pick a Combo File

2/9 | 12:42         Loading '30K-MEGA-ORIGIN-BASE-VALID-BY-EQT1_cleaned_normalized.txt' | Size: 950.3KB
2/9 | 12:42         29768 Combos loaded

2/9 | 12:42         Use ValidCheck MODE? (Y/N)
```

WOXY email checker V3.4 info.

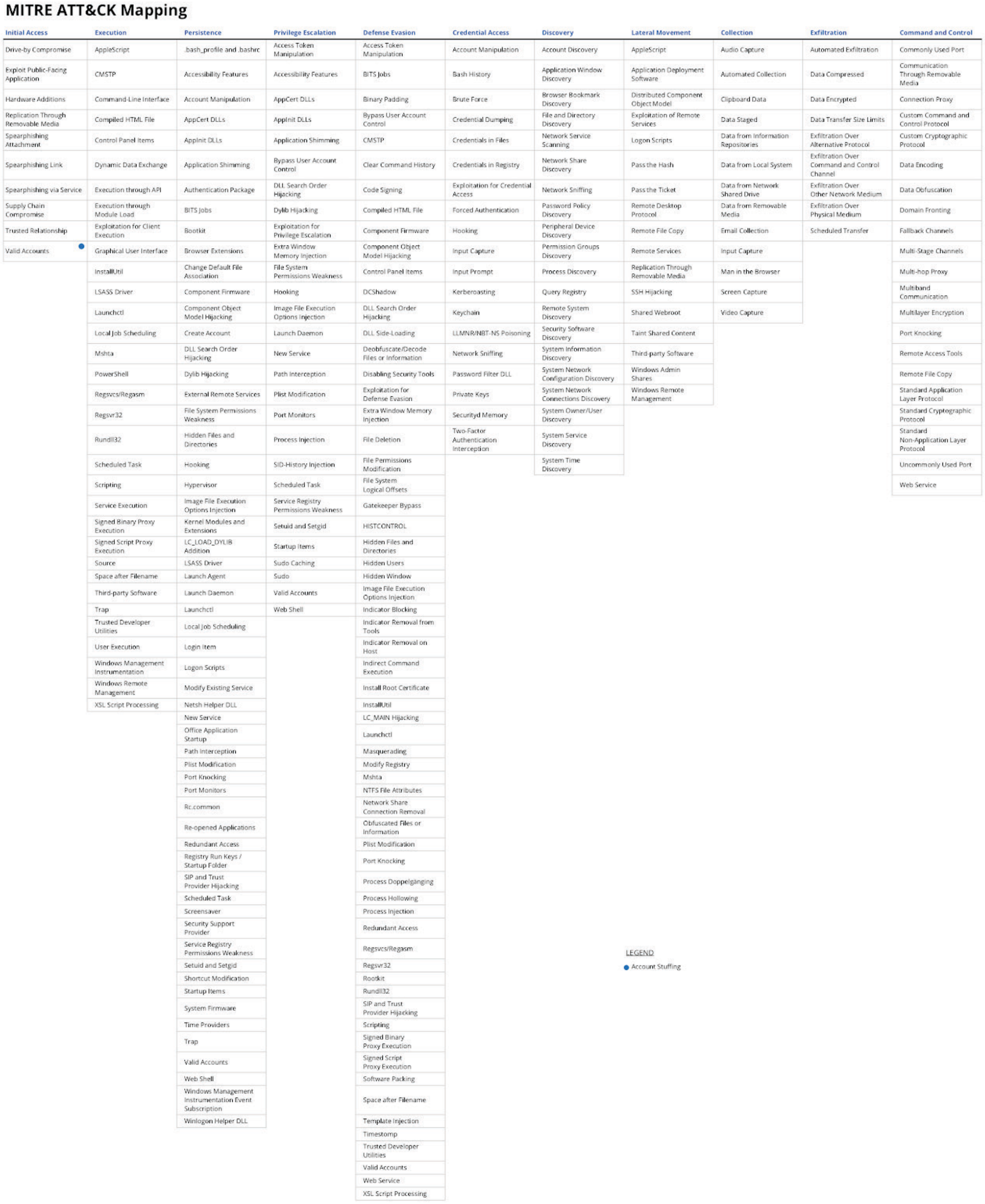
Mitigation

- Criminals will often use paid proxy services aside from using publicly available free proxies to further obfuscate attacks. However, our analysis shows that such services often use geo-spoofing techniques to create a wide pool of IPs. Such domains will have the same IP addresses, but they will use different subnets. Monitoring for web traffic activity from such IPs offers additional mitigation capabilities.
- The introduction of multi-factor authentication has proven to be a highly effective mitigation practice for many organizations that historically experienced a high level of credential stuffing attacks.
- Monitoring criminal underground communities for the availability of new configuration files targeting your organization, acquisition, and the thorough analysis of such files for additional attack indicators.
- End users can reduce the risk of being victimized by a credential stuffing attack by using a password manager and setting a unique strong password for each online account.

Appendix A — Most Targeted Industries

- Financial
- E-commerce
- Social Media and Entertainment
- Information Technology and Telecommunications
- Restaurants and Retail
- Transportation

Appendix B — MITRE ATT&CK Techniques



MITRE ATT&CK Mapping

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts ●	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Local Job Scheduling	Create Account	Launch Daemon	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	SID-History Injection	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Scheduled Task	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	HISTCONTROL						
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Hidden Files and Directories						
	Source	LSASS Driver	Sudo Caching	Hidden Users						
	Space after Filename	Launch Agent	Sudo	Hidden Window						
	Third-party Software	Launch Daemon	Valid Accounts	Image File Execution Options Injection						
	Trap	Launchctl	Web Shell	Indicator Blocking						
	Trusted Developer Utilities	Local Job Scheduling		Indicator Removal from Tools						
	User Execution	Login Item		Indicator Removal on Host						
	Windows Management Instrumentation	Logon Scripts		Indirect Command Execution						
	Windows Remote Management	Modify Existing Service		Install Root Certificate						
	XSL Script Processing	Netsh Helper DLL		InstallUtil						
		New Service		LC_MAIN Hijacking						
		Office Application Startup		Launchctl						
		Path Interception		Masquerading						
		Plist Modification		Modify Registry						
		Port Knocking		Mshta						
		Port Monitors		NTFS File Attributes						
		Rc.common		Network Share Connection Removal						
		Re-opened Applications		Obfuscated Files or Information						
		Redundant Access		Plist Modification						
		Registry Run Keys / Startup Folder		Port Knocking						
		SIP and Trust Provider Hijacking		Process Doppelgänging						
		Scheduled Task		Process Hollowing						
		Screensaver		Process Injection						
		Security Support Provider		Redundant Access						
		Service Registry Permissions Weakness		Regsvcs/Regasm						
		Setuid and Setgid		Regsvr32						
		Shortcut Modification		Rootkit						
		Startup Items		Rundll32						
		System Firmware		SIP and Trust Provider Hijacking						
		Time Providers		Scripting						
		Trap		Signed Binary Proxy Execution						
		Valid Accounts		Signed Script Proxy Execution						
		Web Shell		Software Packing						
		Windows Management Instrumentation Event Subscription		Space after Filename						
		Winlogon Helper DLL		Template Injection						
				Timestomp						
				Trusted Developer Utilities						
				Valid Accounts						
				Web Service						
				XSL Script Processing						

LEGEND

● Account Stuffing

About Recorded Future

Recorded Future arms security teams with the only complete threat intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.