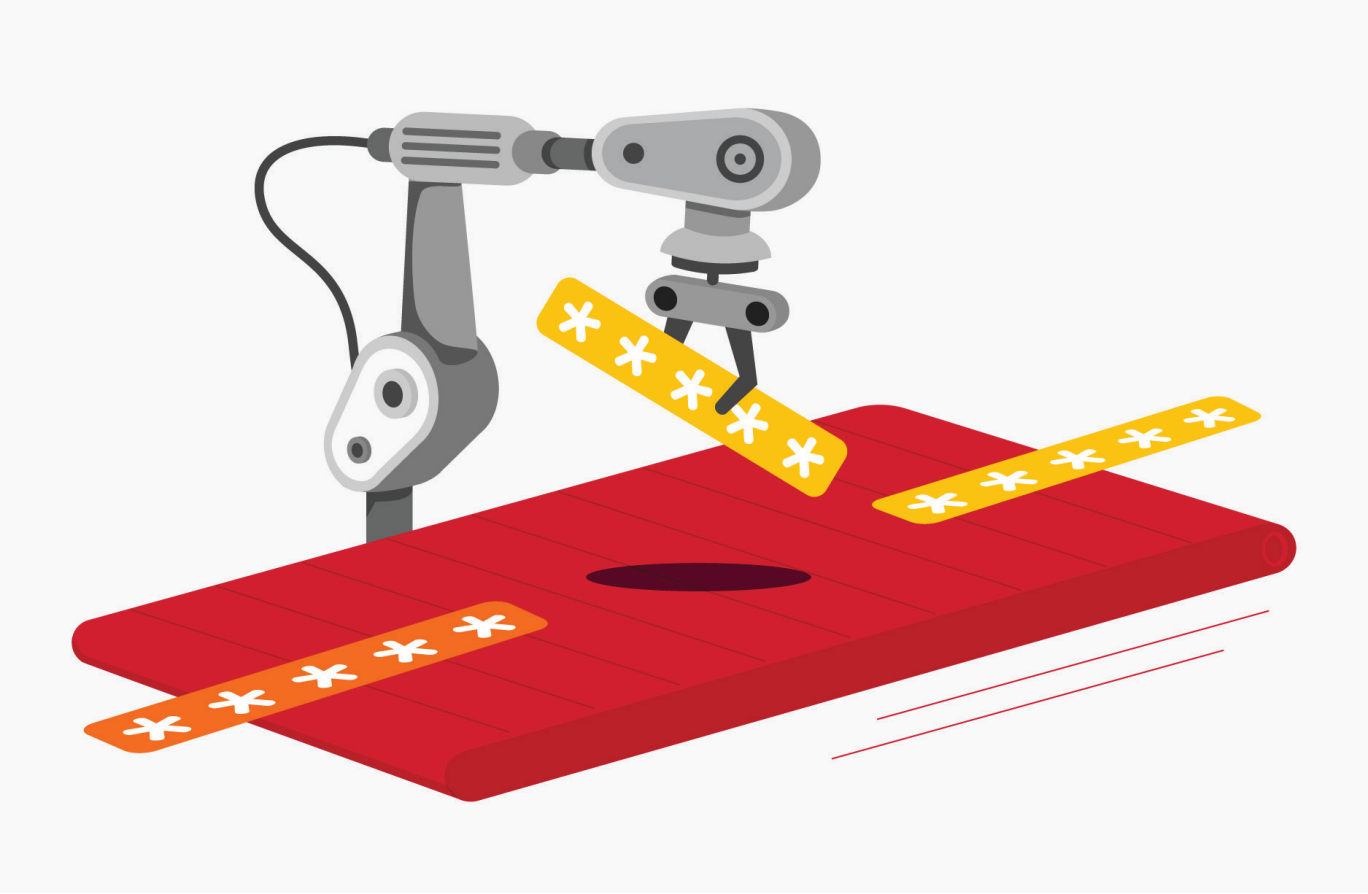
Recorded Future®

CYBER THREAT ANALYSIS

Checkers and Brute Forcers Highlight Dangers of Poor Password Management

By Insikt Group®



CTA-2020-0616

Recorded Future analyzed current data from the Recorded Future® Platform, information security reporting, and other open source intelligence (OSINT) sources to identify checkers and brute forcers that facilitate threat actor campaigns. This report expands upon findings addressed in the report "Combating the Underground Economy's Automation Revolution," following the first report in this series, "Database Breaches Remains Top Cyber Threat for Organizations." This report will be of most interest to network defenders, security researchers, and executives charged with security risk management and mitigation.

Executive Summary

Checkers and brute forcers are popular tools sold and shared on the criminal underground. Some are all-in-one, credential-stuffing attack platforms, while others are company-specific. These tools help unskilled cybercriminals launch an array of automated brute-forcing attacks against organizations' sites, which they profit from by stealing financial and personal data, installing webshells and sniffers, or simply reselling access on the dark web.

One such tool, a new checker and brute forcer identified by Insikt Group, is profiled as "Big Brute Forcer" in this report. This tool is designed to target websites, web servers, website builders, e-commerce platforms, customer relationship management (CRM) systems, and other network protocols, such as File Transfer Protocol (FTP). Its ease of use and developer support enables cybercriminals who may lack necessary skills or intrusion infrastructure to gain access to e-commerce websites and platforms to steal customer data.

We also offer some mitigation strategies at the end of this report, such as suggestions for better password hygiene; as long as these strategies are not followed, cybercriminals will continue to find that checkers and brute forcers provide an easy way to steal data and turn a profit.

Key Judgments

- The industries most affected by cybercriminals using checkers and brute forcers are software, media and entertainment, e-commerce, finance, and telecommunications.
- Threat actors use automated checkers and brute forcers available on the criminal underground with the goal of validating accounts and gaining access to them.
- Password reuse and poor password-management hygiene remain among top issues enabling successful credential-stuffing attacks.

Background

Equipped with credentials obtained from database breaches, attackers can use checkers and brute forcers to conduct credential-stuffing attacks, where they direct large-scale, automated login requests against websites to determine the validity of victim accounts and gain unauthorized access. With an investment of as little as $550, criminals can earn at least 20 times the profit on the sale of compromised login credentials. In 2019, Akamai reported that it detected over 3.5 billion credential-stuffing requests aimed at financial institutions over 18 months.

The majority of the checkers and brute forcers that Recorded Future analyzed in a 2019 report are still widely sold and used by criminals, with some that have been around since as far back as 2016. The continued effectiveness of these tools is in part due to poor password hygiene that allows threat actors to capitalize on password reuse.

There is no honor among thieves, and some of these checkers and brute forcers have been cracked, allowing any interested cybercriminal to use these tools at a cheaper price than offered by the original seller or completely free.

Checkers

Checkers are automated tools (scripts or software) used by cybercriminals to check the validity of user login credential combinations in bulk. Checkers may use the website's main page, mobile app, or an application program interface (API) function to identify valid accounts.

In a credential-stuffing attack, a threat actor will use a database of usernames and passwords frequently obtained from data breaches. For example, an attacker could have obtained credentials from the LinkedIn data breach of 170 million accounts compromised in 2012 and leaked on the dark web in 2016 (1,135,936 of those LinkedIn accounts used the password "123456"). An attacker would take the email and password combination from that LinkedIn database breach, and see if the same credentials can be used to gain unauthorized access to other victim accounts, such as an email or a bank account, because threat actors know that users frequently reuse the same passwords across multiple websites and platforms. Checkers automate and commoditize credential-stuffing attacks for easier and faster ways of gaining access to user accounts and personally identifiable information (PII). In fact, checkers may outnumber legitimate login attempts by a factor of greater than four to one.

Brute Forcers

Brute forcers are automated password cracking tools used to gain access to user accounts through automated server requests. These tools attempt to guess and crack passwords or usernames using a trial and error method or via a dictionary attack, which helps attackers expedite guessing a password for a particular user or website. Partial information, such as a username obtained from a data dump, also makes it easier for an attacker to use a brute forcer to get the password.

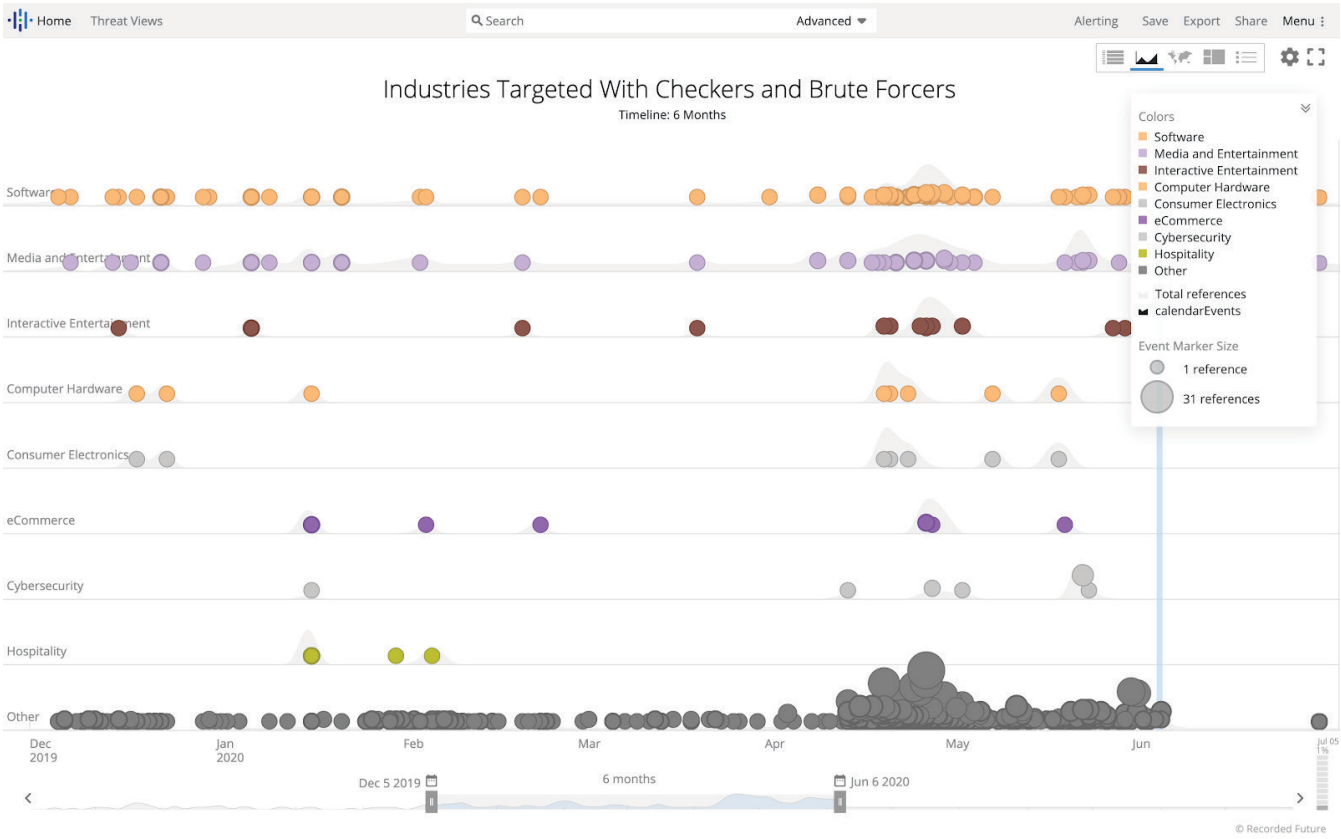
Threat Analysis

Below are some notable breaches that emerged from successful credential-stuffing attacks:

- In July 2019, U.S. banking and insurance company State Farm said it suffered a credential-stuffing attack during which "a bad actor" was able to confirm valid usernames and passwords for State Farm online accounts.
- In January 2020, the Amazon-owned smart camera maker Ring faced a lawsuit from a family whose camera in the children's bedroom was hacked. Allegedly, criminals used a list of common passwords to brute-force their way into the family's Ring camera account.
- On January 30, 2020, TechCrunch reported about a breach at Indian airline SpiceJet that affected 1.2 million passengers. Reportedly, the access to SpiceJet internal systems was gained by brute-forcing the system's easily guessable password.

These types of attacks are even more likely to succeed if victims reuse the same login information (username and password) across multiple online platforms. According to University of Southern California research, "password reuse is rampant and indiscriminate; 98% of users reuse their passwords verbatim and 84% reuse an important password at a non-important, and likely less secure site; main causes for password reuse are poor understanding of risk and preference for memorability over security."

The most affected industries targeted by cybercriminals using checkers and brute forcers are software, media and entertainment, e-commerce, finance, and telecommunications. The image below shows the impacted sectors over a six-month timeline based on dark web source collections.



Industries targeted by checkers and brute forcers. (Recorded Future)

Cybercriminals will commonly use lists containing thousands of credentials with automated custom and "off-the-shelf" tools available on the dark web. Many tools support an unlimited number of custom plugins, known as "configs," which allow cybercriminals to target almost any company with an online presence and conduct account takeovers. There are also lesser-known tools built to target single high-profile companies (like Netflix, Facebook, Instagram, and Spotify). If an organization sees a checker advertised for their particular brand or entity, it may be a precursor to an increase in credential-stuffing attacks against them.

These automated tools help attackers use compromised usernames and passwords against a range of accounts, including banking, e-commerce, loyalty or rewards programs, social media, and online cryptocurrency wallets. Once the attackers obtain access to an account, they try to drain available funds and rewards points, steal personal and financial details (such as credit card data), or commit fraud and identity theft. For automated brute-forcing tools, attackers will often use a list of common passwords with the most common combinations first.

Many forums on the criminal underground have sections specifically devoted to the sale and discussion of brute forcers and checkers. One such forum we observe has thousands of threads dedicated to credential-stuffing attacks and sales of checker software, and it's no wonder why: According to forum discussions, it only takes one checker tool 90 seconds to check a database of 5,400 email addresses and return successful login and password combinations to the attacker. That tool is sold on the criminal underground for only $12.

Without tools like these, threat actors would have to create their own tools or configure existing ones, create or rent a botnet to launch attacks from, and rent bulletproof servers to host their attack infrastructure.

A Closer Look at 1 Brute Forcer

One example tool we found on the criminal underground, which we will call "Big Brute Forcer," comes in two versions: the "Basic" for $1,000, and the "Pro" for $2,500. The more expensive "Pro" version provides the buyer with an entire toolset and infrastructure for account checking and brute forcing. We chose this specific tool because of its novelty, impact on businesses, and automation capabilities.

Big Brute Forcer employs a botnet to perform brute-force attacks, which distributes the computational workload across multiple machines and allows login attempts from multiple IPs. The use of multiple IPs in mass brute forcing allows cybercriminals to mask any single origin of attack by attempting to access victim accounts from

hundreds of different IP addresses. Big Brute Forcer has features that make it particularly easy, even for unskilled cybercriminals, to launch an array of brute-force attacks against websites and online resources in an automated fashion:

- Big Brute Forcer is a web-based application, providing the buyer with various options to launch brute-force attacks without a need to open a command line or any specialized technical knowledge.
- Big Brute Forcer comes with technical support for installation and configuration.
- The buyer can either use their own list of domains for the control panel or use one supplied by the developer of Big Brute Forcer to control their attacks.
- Big Brute Forcer comes with preloaded dictionaries of password combinations from various breaches to use in attacks.
- Cybercriminals can create their own Big Brute Forcer botnet, or rent a premade one from its developer.
- The developer offers and operates bulletproof hosting services that can be purchased directly.

In the past, threat actors would have needed multiple manual steps to launch a successful brute-force attack. They would have to gather or purchase compromised credentials, compile the lists of domains and subdomains to attack, configure their tool of choice — often requiring a certain level of technical skill — create a botnet to launch attacks from, and finally, rent servers from bulletproof hosters to host their control panel. In addition, many tools used in credential-stuffing attacks require configuration files that define a target's parameters, all of which Big Brute Forcer can also provide.

The tool's graphical user interface is also simple and easy for inexperienced users. It allows viewing the progress of brute forcing, the speed of compromises, and statistics of successful and failed access attempts. Furthermore, the user can pivot directly to the lists of thousands of usernames and passwords along with the links to the login portals of breached accounts. With administrative access to these websites, cybercriminals can then steal customer PII and payment card data. Big Brute Forcer even offers to install webshells and backdoors to infect and steal directly from the compromised websites.

The developer also provides detailed YouTube videos on how to configure Big Brute Forcer functionality to expedite the client's setup process. One video, for example, gives step-by-step instructions of how to breach websites, showing dozens of breached websites in the process. As the threat actor uploads the lists of domains and subdomains, in less than half an hour, Big Brute Forcer returns lists of cracked login and password details, which the developer uses to log in to those websites in real time.

Among victimized companies shown in the video are e-commerce and entertainment websites, as well as travel agencies with customer PII and financial data. Big Brute Forcer indiscriminately breaches websites and online resources based in various regions, including Europe, the United States, Asia, and Brazil. In one instance, the developer of Big Brute Forcer shows how they access the website of a New Zealand-based security company that emphasizes the need for good security and highlights its own commitment to protecting their clients' security. Notably, this company's admin panel login was easily guessable, with "admin" as a username and the company's name as a password.

Mitigation Strategies

- Increase awareness among the users within your organization to use unique passwords for each of their accounts. A password manager would help end-users generate, store, and retrieve unique and complex passwords.
- Require additional details (for example, CAPTCHA, or user's last name) during the login process to break the attacker's programmed logic in automated credential-stuffing attacks.
- Use multi-factor authentication (MFA) if possible. While MFA will not prevent brute-forcing or checking attacks from occurring, it provides an extra layer of security such that any attempt to login by a malicious threat actor will be hindered by that extra layer of authentication.
- Establish customized web application firewall rules, with special attention to unusual header orders and user-agents, as well as checking for valid referrers.
- Intentionally slow down and rate limit login traffic to discourage attackers. For example, lock out accounts after a certain number of failed login attempts or introduce a delay in server responses to login requests.
- Remove unused public-facing login paths and tighten controls on mobile and API login paths.
- Baseline traffic and network requests to monitor web service for unexpected traffic, including volume and request type.
- Use Recorded Future to monitor criminal underground communities for the availability of new configuration files targeting your organization, acquisition, and for a thorough analysis of such files for additional attack indicators.

- Use Recorded Future to surface compromised credentials from database breaches, and once identified, take appropriate action to address the threat.
- Always store client passwords in a hashed format. Never leave them in plaintext. As part of the hashing algorithm, incorporate a salt value that cannot be easily derived by an attacker. While hashes are irreversible, failure to incorporate a salt value makes it possible for attackers to compare hashes against publicly available databases of hashes for common passwords.

Outlook

Cybercriminals will continue to use checkers and brute forcers because of the success they have had with gaining unauthorized access to user accounts and the profits they make from selling cracked accounts on the underground economy. This practice will continue to threaten companies and individual users until better password hygiene practices and security measures are implemented. Recorded Future continually monitors checkers and brute forcers advertised and discussed on the dark web to inform the clients on ways to enhance their mitigation strategies. Using the Recorded Future platform, clients can identify tools targeting their brand or entity, which may indicate that there will be an increase in attacks against them.

About Recorded Future

Recorded Future arms security teams with the only complete security 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.