Part of F5

Automating Cybercrime with Sentry MBA

THE MOST COMMONLY USED ATTACK TOOL FOR CREDENTIAL STUFFING

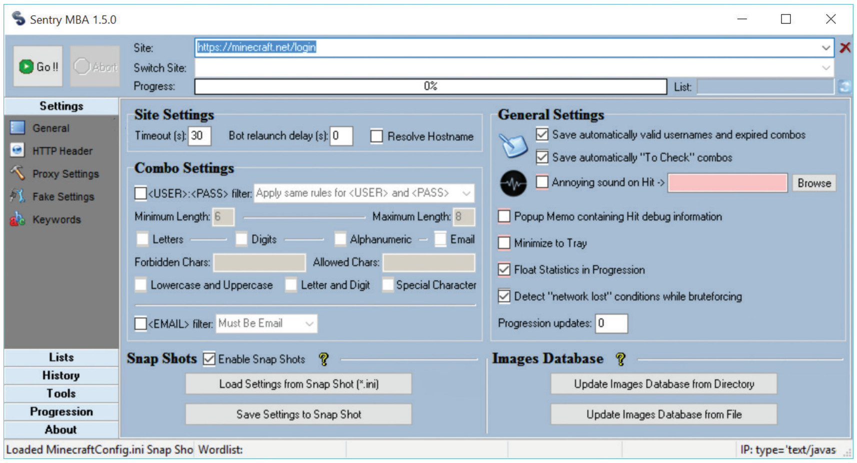
Sentry MBA features advanced capabilities that help attackers elude common web application defenses.

INTRODUCTION

Sentry MBA is an automated attack tool used by cybercriminals to take over user accounts on major websites. With Sentry MBA, criminals can rapidly test millions of usernames and passwords to see which ones are valid on a targeted website. The tool has become incredibly popular — the Shape Security research team sees Sentry MBA attack attempts on nearly every website we protect.

In the past, cybercriminals had to master arcane web technologies to launch online attacks. Sentry MBA has a point-and-click graphical user interface, online help forums, and vibrant underground marketplaces to enable large numbers of individuals to become cybercriminals. These individuals no longer need advanced technical skills, specialized equipment, or insider knowledge to successfully attack major websites.

Sentry MBA features advanced capabilities that help attackers elude common web application defenses. For example, the tool can bypass preventative controls (such as IP blacklists or rate limiting) by using proxies to spread the attack across a large number of IP addresses. Sentry MBA can also bypass detective controls (such as referrer checks that ensure visitors were sent to the login page from another, expected page) by spoofing the “referer” header value.



Sentry MBA 1.5.0

Site: https://minecraft.net/login
Switch Site:
Progress: 0%
List:

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

Combo Settings
□ <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

General Settings
☑ 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

Snap Shots ☑ Enable Snap Shots

Images Database

Loaded MinecraftConfig.ini Snap Sho   Wordlist: IP: type='text/javas

Go !!
Abort
Settings
General
HTTP Header
Proxy Settings
Fake Settings
Keywords
Lists
History
Tools
Progression
About
Browse
Load Settings from Snap Shot (*.ini)
Save Settings to Snap Shot
Update Images Database from Directory
Update Images Database from File

Fig. 1: Sentry MBA General Settings Page, v1.5

USING SENTRY MBA IN CREDENTIAL STUFFING ATTACKS

A list of usernames and passwords is at the heart of every Sentry MBA attack. In Sentry MBA parlance, these are called “combo” lists. If the combo list has credentials that were valid on another website (e.g. via publicized breaches at eBay, Sony, and Ashley Madison or through phishing techniques), the attack is called “credential stuffing.” Credential stuffing works because Internet users routinely reuse passwords across web accounts. Verizon's 2015 data breach report cites the use of stolen credentials as the most common attack action used against web applications today.

Credential stuffing attacks are difficult to stop because they target online user interface elements — like login pages — that are open to all Internet traffic by design. In one such attack, cybercriminals using Sentry MBA targeted the stored-value card program at a large retail corporation. Automation accounted for over 91% of the traffic on the company's login page. Even though the company had implemented established best practices for online security, online fraud losses still exceeded $25M a year.

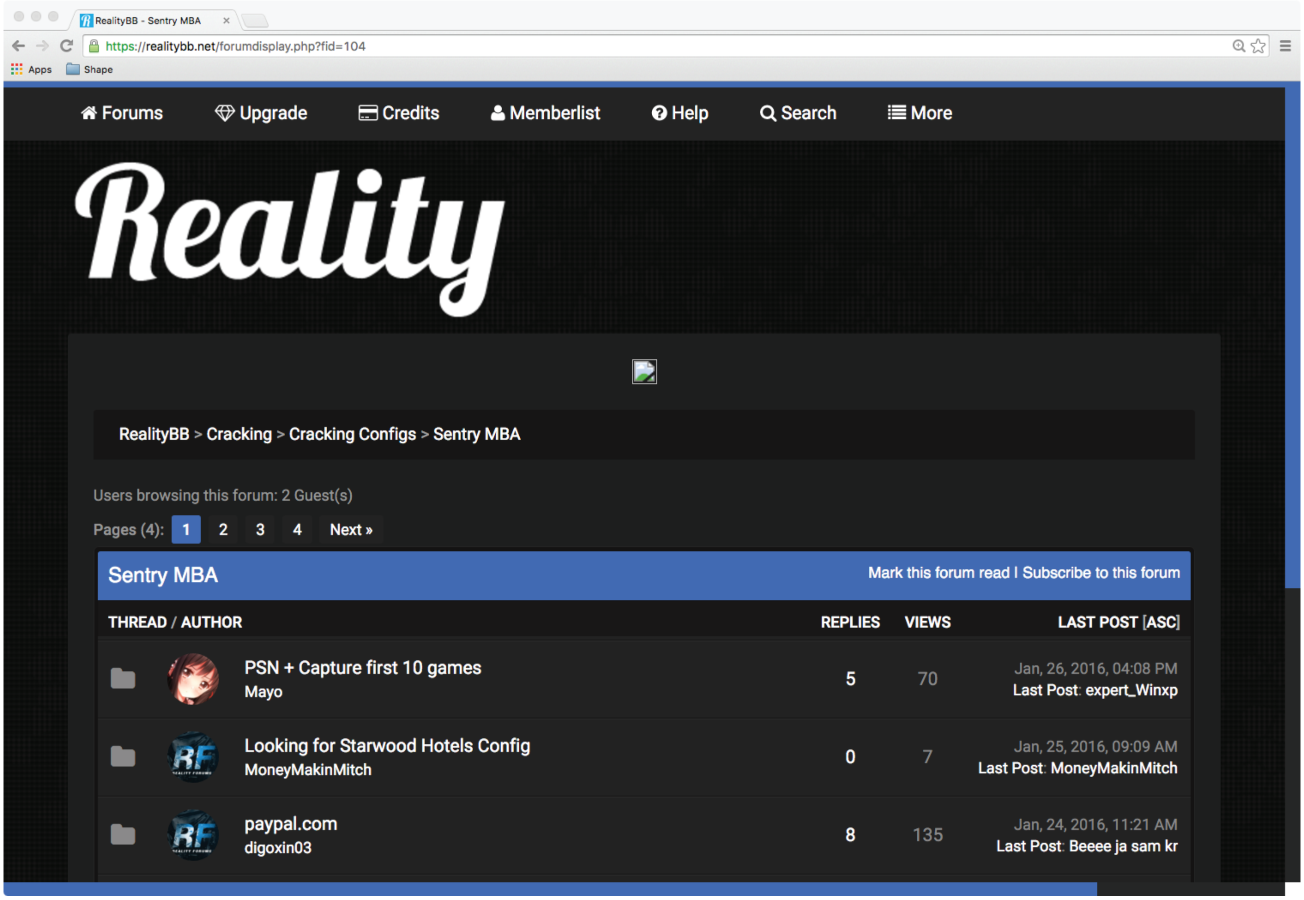
ANATOMY OF A SENTRY MBA ATTACK

An attack using Sentry MBA has three phases:

1. Targeting and attack refinement.
2. Automated account checking.
3. Monetization. Sentry MBA (and the criminal ecosystem that supports it) dramatically improve criminal productivity during the first two phases.

1. Targeting and Attack Refinement

Before it can test account credentials, Sentry MBA must be configured to understand the targeted login page. A Sentry MBA "config" file contains, among other items, the url for the website's login page, field markers to help navigate form elements, and rules for valid password constructions. A number of forums offer a wide variety of working configurations for various websites. Here's a screenshot from one such forum:


RealityBB - Sentry MBA
https://realitybb.net/forumdisplay.php?fid=104
Apps
Shape
Forums
Upgrade
Credits
Memberlist
Help
Search
More
Reality
Pages (4): 1 2 3 4 Next »
Mark this forum read | Subscribe to this forum

RealityBB > Cracking > Cracking Configs > Sentry MBA

Users browsing this forum: 2 Guest(s)

Sentry MBA

THREAD / AUTHOR	REPLIES	VIEWS	LAST POST [ASC]
PSN + Capture first 10 games Mayo	5	70	Jan, 26, 2016, 04:08 PM Last Post: expert_Winxp
Looking for Starwood Hotels Config MoneyMakinMitch	0	7	Jan, 25, 2016, 09:09 AM Last Post: MoneyMakinMitch
paypal.com digoxin03	8	135	Jan, 24, 2016, 11:21 AM Last Post: Beeee ja sam kr

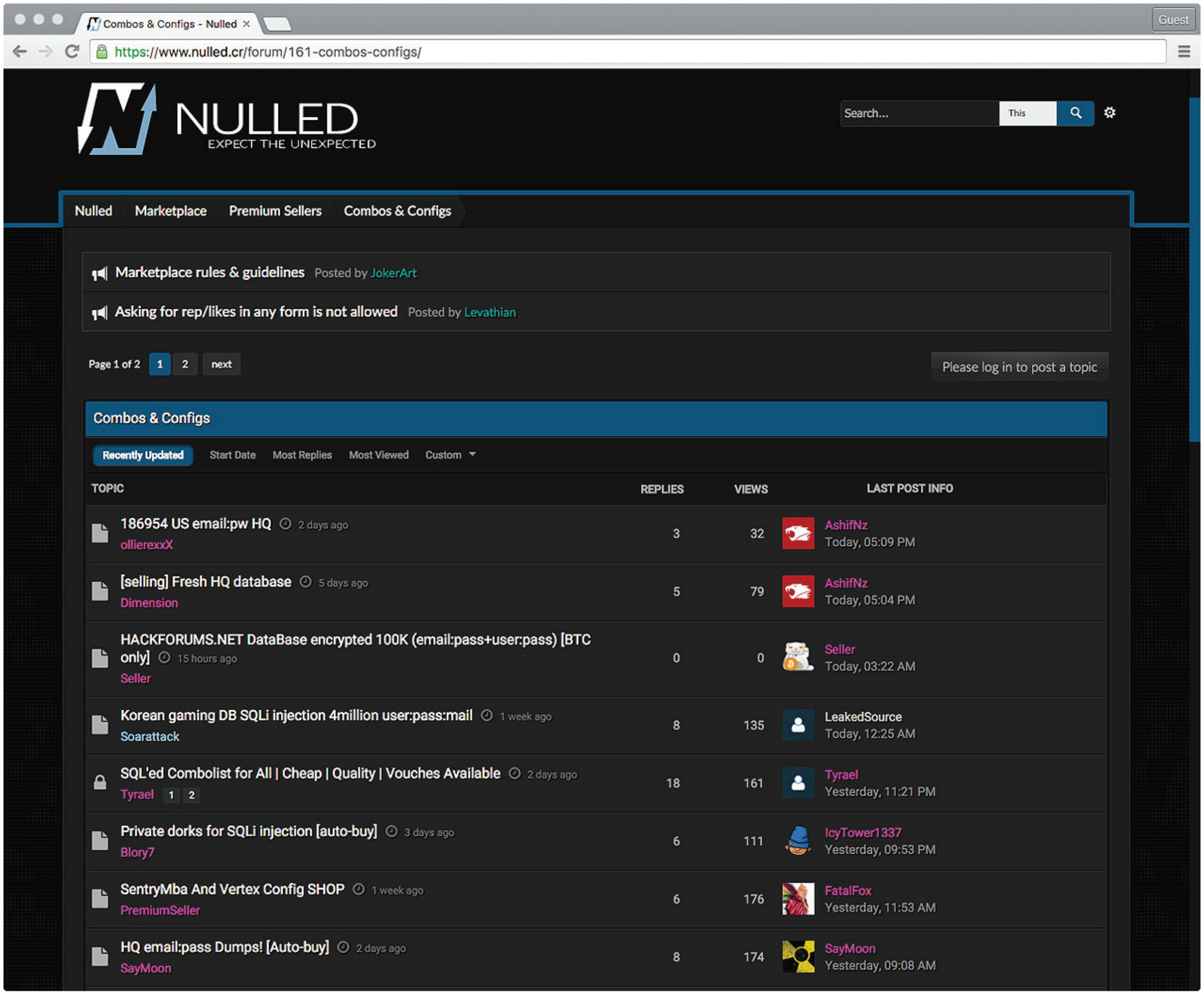
Fig. 2: Underground Site With Sentry MBA Configurations for Playstation, Starwood, Paypal

Once the attacker has a basic working configuration, Sentry MBA offers tools to optimize and test the attack setup against the live target website. For example, the tool can be configured to recognize certain keywords associated with a website's responses to successful and unsuccessful login attempts. If the targeted page includes a CAPTCHA test, Sentry MBA can defeat the CAPTCHA with its optical character recognition module or with an optional database containing thousands of possible CAPTCHA images and answers. This YouTube video demonstrates the process of tuning Sentry MBA to solve CAPTCHA.

2. Automated Account Checking

Once the site configuration is optimized, attackers need only add their "combo" file and a "proxy" file to Sentry MBA to commence their attack.

Combo files are simply lists of usernames and passwords. The Darknet and open web offer many options for acquiring stolen lists of usernames and passwords. Fresh lists are often sold at a premium but other lists can be freely downloaded. Here's a screenshot of combo lists available for sale on a public website:



Marketplace rules & guidelines Posted by JokerArt

Asking for rep/likes in any form is not allowed Posted by Levathian

Combos & Configs

TOPIC	REPLIES	VIEWS	LAST POST INFO
186954 US email:pw HQ 2 days ago ollierexxX	3	32	AshifNz Today, 05:09 PM
[selling] Fresh HQ database 5 days ago Dimension	5	79	AshifNz Today, 05:04 PM
HACKFORUMS.NET DataBase encrypted 100K (email:pass+user:pass) [BTC only] 15 hours ago Seller	0	0	Seller Today, 03:22 AM
Korean gaming DB SQLi injection 4million user:pass:mail 1 week ago Soarattack	8	135	LeakedSource Today, 12:25 AM
SQL'ed Combolist for All | Cheap | Quality | Vouches Available 2 days ago Tyrael 1 2	18	161	Tyrael Yesterday, 11:21 PM
Private dorks for SQLi injection [auto-buy] 3 days ago Blory7	6	111	IcyTower1337 Yesterday, 09:53 PM
SentryMba And Vertex Config SHOP 1 week ago PremiumSeller	6	176	FatalFox Yesterday, 11:53 AM
HQ email:pass Dumps! [Auto-buy] 2 days ago SayMoon	8	174	SayMoon Yesterday, 09:08 AM

Fig. 3: Site Offering Credential Lists for Sentry MBA on the Open Internet

Proxy files are lists of computers used by Sentry MBA to send login attempts to a targeted site. These lists,like combo lists, are readily available on the open web and the Darknet. Proxies make attack detection anddefense far more difficult. Specifically, they undercut two common application defense strategies: IP reputation filtering and rate limiting.

How do proxies defeat IP reputation filtering (also known as “blacklisting”)? Sentry MBA proxies are compromised computers that are typically used without authorization. Cybercriminals constantly work to gain access to fresh proxies that can help evade blacklists. An analysis of a proxy-based attack at one Shape customer revealed that 60% of the proxies used in the attack were new each day. Blacklists can’t be updated quickly enough to detect compromised computers and stop them from joining attacks.

Proxies also help attackers evade defenses that rely on rate limiting. These defenses fail because the attacker’s login attempts appear to come from a large number of different computers. Sentry MBA can be tuned to ensure that no individual proxy sends too many requests, which makes rate limiting ineffective.

With a working configuration, combos, and proxies, the attack can commence. Sentry MBA coordinates proxies and collects information on which credentials successfully open an account. It even checks for what assets are available in an account and notifies the attacker when hits occur. After all the credentials in the combo list have been checked, Sentry MBA’s role in the attack is over.

3. Monetization

Once the cybercriminal has working credentials, they need a way to make money from their victims. Monetization strategies can take many forms. The retailer mentioned earlier was defrauded when cybercriminals transferred stored-value gift card balances out of compromised accounts to cards controlled by the cybercriminal. Sites such as giift.com, giftcardzen.com, and cardpool.com make it easy to liquidate these fraudulent cards for cash or merchandise.

Many other monetization schemes are available to cybercriminals, including extortion, account funds transfers, and acquisition of credit card information, to name a few. As cybercriminals find increasingly creative ways to monetize attacks, more and more websites become attractive targets.

CONCLUSION

The rise of Sentry MBA illustrates the pivotal role automation plays in cybercrime and highlights how cybercrime is increasingly compartmentalized and commoditized. The “script kiddies” have grown up and now have easy access to powerful automation tools. Sentry MBA and the underground marketplaces that have grown up around it are one example of how online attacks have evolved into a mass-market endeavor for legions of cybercriminals across the globe.