radware

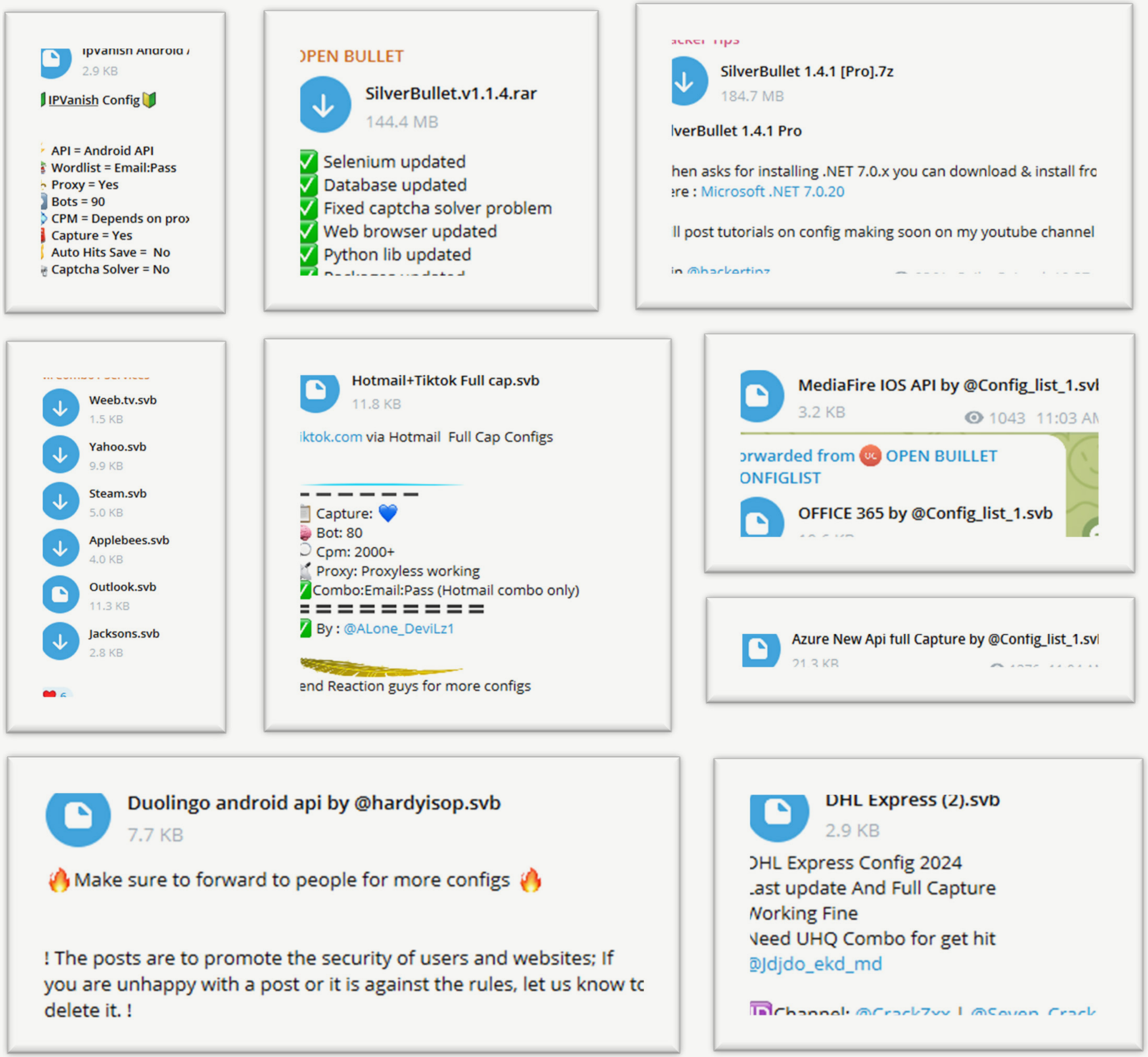
Report

The Invisible Breach: Business Logic Manipulation and API Exploitation in Credential Stuffing Attacks

Contents

Analysis of 100 Advanced Credential Stuffing Scripts Published in Threat Actor Platforms Throughout 2025

Figure 1: SilverBullet Pro cracked version (credential stuffing tool) and Config (attack script) examples, shared across hacker's channels (Source: Telegram)



Ipvanish Android /
2.9 KB
IPVanish Config

API = Android API
Wordlist = Email:Pass
Proxy = Yes
Bots = 90
CPM = Depends on prox
Capture = Yes
Auto Hits Save = No
Captcha Solver = No

OPEN BULLET
SilverBullet.v1.1.4.rar
144.4 MB
✅ Selenium updated
✅ Database updated
✅ Fixed captcha solver problem
✅ Web browser updated
✅ Python lib updated

acker Tips
SilverBullet 1.4.1 [Pro].7z
184.7 MB
lverBullet 1.4.1 Pro

hen asks for installing .NET 7.0.x you can download & install fro
ere : Microsoft .NET 7.0.20

ll post tutorials on config making soon on my youtube channel

in @hackertipz

Weeb.tv.svb
1.5 KB
Yahoo.svb
9.9 KB
Steam.svb
5.0 KB
Applebees.svb
4.0 KB
Outlook.svb
11.3 KB
Jacksons.svb
2.8 KB

Hotmail+Tiktok Full cap.svb
11.8 KB
iktok.com via Hotmail Full Cap Configs

Capture: 💙
Bot: 80
Cpm: 2000+
Proxy: Proxyless working
✅ Combo:Email:Pass (Hotmail combo only)
✅ By : @ALone_DevilLz1

end Reaction guys for more configs

MediaFire IOS API by @Config_list_1.svl
3.2 KB
1043 11:03 AM
orwarded from OPEN BUILLET
ONFIGLIST
OFFICE 365 by @Config_list_1.svb

Azure New Api full Capture by @Config_list_1.svl
21.3 KB

Duolingo android api by @hardyisop.svb
7.7 KB
🔥 Make sure to forward to people for more configs 🔥

! The posts are to promote the security of users and websites; If you are unhappy with a post or it is against the rules, let us know tc delete it. !

DHL Express (2).svb
2.9 KB
DHL Express Config 2024
Last update And Full Capture
Working Fine
Need UHQ Combo for get hit
@Jdjdo_ekd_md
Channel: @Crack7xx | @Seven_Crack

Executive Summary: A Paradigm Shift in Account Takeover Methodologies

Research Overview and Strategic Context

This comprehensive analysis examines 100 advanced credential stuffing configurations deployed through the SilverBullet tool, revealing a fundamental transformation in how threat actors approach account takeover (ATO) automated operations. The research, conducted between December 2024 and May 2025, reveals sophisticated attack methodologies that surpass traditional password-spraying techniques, indicating the emergence of business logic, API and identity exploitation as the primary attack vectors in modern credential stuffing campaigns.

Key Research Findings

Threat Actor Concentration and Specialization

Our analysis reveals a highly centralized threat landscape, where technical expertise poses significant barriers to entry. A total of 51% of all analyzed configurations, which were randomly collected over six months, were written by just three advanced threat actors. Each demonstrates over two years of operational experience and distinct areas of specialization.

- **SVBCONFIGSMAKER:** Specializes in AI platform authentication bypass with advanced CSRF token manipulation (31% implementation rate)
- **t.me/mrcombo1services:** Focuses on mobile API exploitation, particularly Samsung electronics accounts, with sophisticated JWT token handling
- **@Magic_Ckg:** Demonstrates Microsoft cloud services expertise with limited cookie authentication techniques

Strategic Industry Targeting Evolution

Technology/SaaS emerged as the primary target sector (27%), followed by financial services/government (16%) and travel/airline (13%) sectors. However, the most significant finding involves the dramatic shift toward high-value corporate and AI tool targeting:

- AI tools account for 44% of technology/SaaS targeting, with content generation platforms (42%) and design tools (25%) as primary focuses. This might indicate a new type of target audience for config developers: spammers.
- Corporate tools account for 30%, with Microsoft 365, OneDrive and Outlook indicating a new type of target audience for config developers: ransomware groups that seek initial access to organizations' systems.

This targeting evolution aligns with threat actor monetization strategies, as compromised AI tools enable the generation of large-scale phishing content, while corporate accounts provide initial access for ransomware operations.

Technical Innovation in Attack Methodologies

Business Logic Attack Sophistication

The research reveals that 94% of configurations implement four or more business logic attack elements, with 54% demonstrating advanced orchestration using 13+ distinct techniques. These attacks no longer rely on simple authentication attempts but instead:

- Replicate complete user workflows through multi-step authentication sequences
- Implement conditional logic based on application responses (100% distribution)
- Extract valuable post-authentication data in 91% of cases, including account balances, loyalty points and payment methods

Multi-Device Spoofing Emergence

A surprising discovery reveals that 24% of attack scripts alternate between two device types during execution, with 71.1% employing cross-platform transitions (primarily iOS Windows). This technique exploits:

- Inconsistent security policies between mobile and desktop environments
- Reduced scrutiny at authentication boundaries
- Platform-specific API vulnerabilities

API Exploitation Distribution

Research shows that 82.7% of examined configurations contain explicit API-targeting techniques, with significant variation across industries:

- Gaming and AI tools: 100% API targeting
- Travel/airline: 92.31%
- Media: 90%

Notably, 49.4% of API targeting occurs in the post-authentication phase, with a focus on data extraction rather than mere credential validation. Furthermore, 25.61% of API-targeting configurations specifically exploit shadow APIs—legacy or undocumented endpoints with weaker security controls.

Strategic Implications and Recommendations Immediate Security Priorities

Research shows that 82.7% of examined configurations contain explicit API-targeting techniques, with significant variation across industries:

1. **Implement Comprehensive Process Validation:** Organizations must move beyond credential-centric controls to validate entire user workflows, correlating cross-request behavior patterns.
2. **Deploy Cross-Platform Session Binding:** With 71.1% of device-spoofing attacks using cross-platform transitions, session validation must span device types and authentication stages.
3. **Discover and Remediate Shadow APIs:** Conduct thorough API inventory audits, particularly in media (66.67% shadow API distribution) and gaming (50%) sectors.

Long-term Strategic Considerations

- **Threat Intelligence Integration:** Take advantage of the concentration of expertise among few threat actors to create opportunities for targeted disruption and attribution.
- **Business Logic Security Framework:** Develop security strategies that validate application logic flows rather than individual requests.
- **API Lifecycle Management:** Implement strict deprecation policies and continuous monitoring for legacy endpoints.

Conclusion: The New Credential Stuffing Paradigm

This research demonstrates that credential stuffing has evolved from a volume-based attack to a sophisticated, multi-stage infiltration technique. Modern attacks leverage business logic manipulation, cross-platform device spoofing, and strategic API exploitation to bypass traditional defenses. The shift toward high-value targets (AI tools and corporate applications) combined with advanced post-authentication data harvesting capabilities represents a fundamental change in the threat landscape.

Security teams must adapt their defensive strategies to address these workflow-centric attacks, implementing controls that validate entire user journeys rather than isolated authentication events. As threat actors continue to demonstrate increasing sophistication in their attack methodologies, organizations must evolve their security postures to match this new reality of business logic exploitation and API-focused credential stuffing campaigns.

Background

Within the realm of credential stuffing (CS) attacks, SilverBullet has emerged over the last five years as one of the most prominent and feature-rich account takeover tools. It can generate thousands of bots that mimic real users and breach accounts using breached passwords.

This background chapter reviews SilverBullet's origins, the evolution of its codebase, notable recent attack cases, its primary differentiators relative to other credential stuffing suites, and the specific technical capabilities that make it a go-to choice for many threat actors. Understanding these fundamentals sets the stage for a deeper analysis of how SilverBullet scripts, often referred to as ".svb configs," work.

SilverBullet's Origin and Evolution

SilverBullet can be traced back to the open-source tool OpenBullet, a successor to earlier cracking tools such as Sentry MBA and BlackBullet [1]. In 2019, OpenBullet was released publicly under an MIT license, enabling rapid forking and community-driven modifications[2]. Among these derivatives, SilverBullet gained traction:

- **Foundational Code:** SilverBullet retained OpenBullet's modular "LoliScript" approach but introduced its configuration format (.svb). It also retained backward compatibility with some .loli or .anom scripts[3].
- **Emergence and Adoption:** Originally published by a developer using the handle "mohamm4dx," SilverBullet added new blocks and user interface improvements that appealed to cybercriminal communities [3]. Over time, a paid "pro" variant also appeared (often leaked), introducing extended protocol support (e.g., FTP, IMAP, SSH) and a refined graphical user interface[4].
- **Forks and Modifications:** The main lineage is OpenBullet → OB Anomaly → SilverBullet → SilverBullet Pro[2]. Other spinoffs (e.g., CyberBullet, AirBullet) also exist, but SilverBullet remains one of the best-known forks in underground forums[1].

Through continuous updates, community-driven scripts, and an easy-to-use interface, SilverBullet solidified its position as a highly adaptable credential stuffing framework [1][2][3].

SilverBullet's Pro Crack and Leak

SilverBullet Pro is a paid, advanced credential stuffing tool (an enhanced variant of the OpenBullet platform) that was sold privately. From 2022, every paid version has been cracked and leaked online:

- **June 2022 (v1.0.0) –** The paid tool SilverBullet Pro (initial version) appears in crackingx[.]com forums.
- **Mid–2023 (v1.4.1) –** Another major version is leaked (v1.4.1), cracked copies spread widely, often reposted on multiple cracking sites such as drcrypter[.]ru
- **Mid–2024 (v1.5.5) –** Subsequent versions (1.5. x series) are similarly cracked soon after release, with posts in demonforums[.]net citing June 2024 for v1.5.5.
- **Late 2024 – 2025 (v1.5.8+) –** Further updates (like v1.5.8) continue to be cracked and distributed through 2025 in cracked[.]miami, indicating an ongoing pattern of leaks for newly released versions.

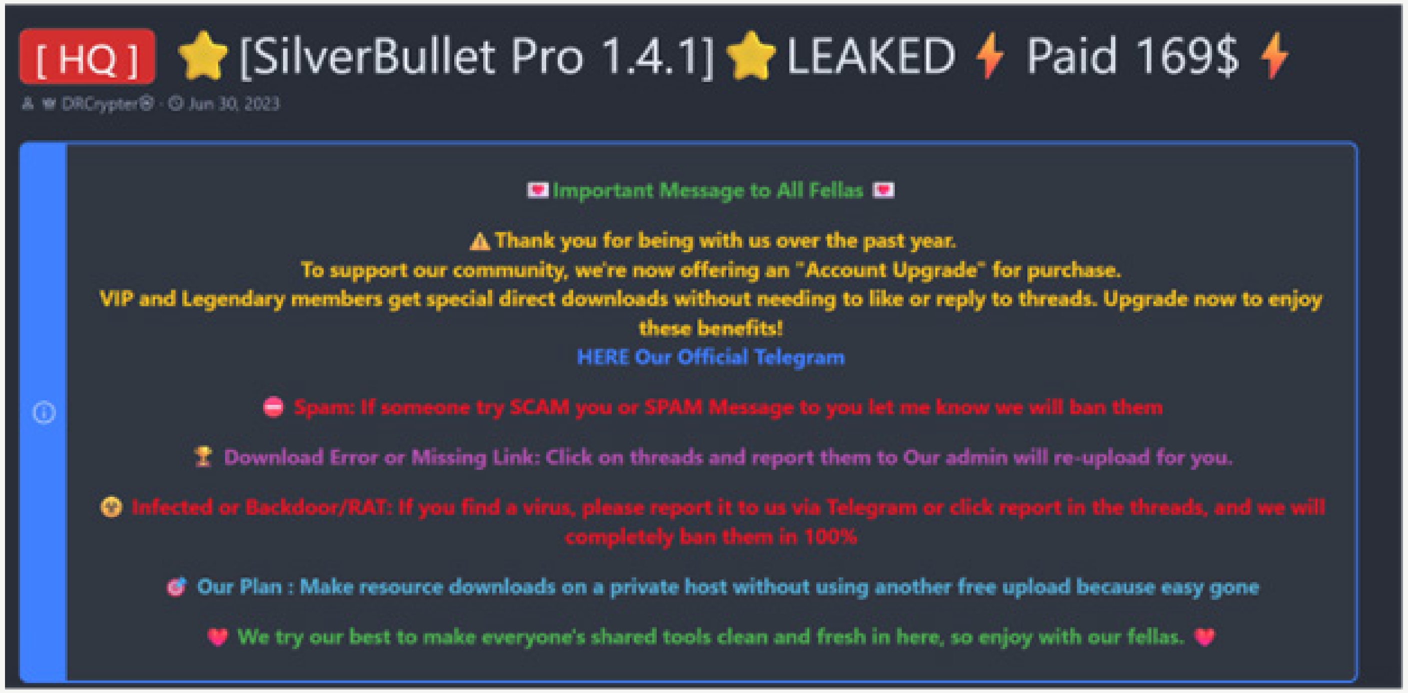
Notable Attack Cases

Multiple high-profile incidents underscore SilverBullet's role in large-scale account takeover (ATO) campaigns. Below are select examples from the last five years:

- **Roku Accounts Breach (2023–2024):** Attackers reportedly compromised hundreds of thousands of Roku accounts by testing stolen credentials with automated tools, including OpenBullet 2 and SilverBullet[5].
- **DraftKings Sports Betting Hack (2022):** An accused hacker allegedly gained unauthorized access to around 60,000 user accounts using OpenBullet variants such as SilverBullet[4]. The attackers monetized successful logins by adding payment methods and withdrawing funds.

These cases demonstrate SilverBullet's utility for automated credential testing at scale, resulting in account takeovers across various online platforms, including streaming and betting services[5][6].

Figure 2: SilverBullet Pro leak thread (Source: drcrypter[.]ru)



[HQ] ⭐ [SilverBullet Pro 1.4.1] ⭐ LEAKED ⚡ Paid 169$ ⚡

DRCrypter · Jun 30, 2023

💌 Important Message to All Fellas 💌

⚠ Thank you for being with us over the past year.
To support our community, we're now offering an "Account Upgrade" for purchase.
VIP and Legendary members get special direct downloads without needing to like or reply to threads. Upgrade now to enjoy these benefits!
HERE Our Official Telegram

⛔ Spam: If someone try SCAM you or SPAM Message to you let me know we will ban them

🏆 Download Error or Missing Link: Click on threads and report them to Our admin will re-upload for you.

☣ Infected or Backdoor/RAT: If you find a virus, please report it to us via Telegram or click report in the threads, and we will completely ban them in 100%

🎯 Our Plan : Make resource downloads on a private host without using another free upload because easy gone

💗 We try our best to make everyone's shared tools clean and fresh in here, so enjoy with our fellas. 💗

Technical Capabilities

SilverBullet's effectiveness stems from various features supporting large-scale credential testing and evasion of traditional defenses. These capabilities also facilitate seamless integration with third-party services, making it an all-in-one solution for attackers.

Features Driving Popularity

- **Open-Source and Customizable:** Like OpenBullet, SilverBullet is (or has been) freely available under permissive licensing, with forkable code and plugin support [3].
- **User-friendly GUI:** A tabbed interface allows non-technical users to load wordlists, manage proxies, and run attacks with minimal scripting knowledge [2][3].
- **Community Ecosystem:** Thousands of configurations targeting popular sites circulate on forums, making "plug-and-play" attacks routine [1][7].
- **Continuous Development:** Regular updates or forks (such as SilverBullet Pro) introduce new request blocks, enhanced configuration management, and advanced protocol support [4].

Bypassing Traditional Defenses

- **Proxy Rotation and Throttling:** Attackers can load extensive proxy lists (HTTP/SOCKS) and cycle them to evade IP-based rate limiting [1].
- **CAPTCHA Solving Integration:** APIs for services like 2Captcha or Anti-Captcha are seamlessly embedded, automating reCAPTCHA and other challenges [3][7].
- **Cloudflare/Anti-Bot Evasion:** Scripts handle JavaScript-based challenges by simulating browsers or using built-in solver libraries [2][4].
- **Multithreading and Configuration Logic:** Parallel runners test credentials at scale, while custom "blocks" parse dynamic login flows and handle advanced checks [1][2].

Third-party Integrations and Extensibility

- **Plugin Framework:** External .DLL plugins enable tasks like real-time Telegram alerts, advanced solvers, or calling external scripts [3].
- **Support for Multiple Protocols:** Beyond standard HTTP-based login, variants of SilverBullet integrate checks for IMAP, SMTP, FTP, and SSHI-MAP, SMTP, FTP, and SSH checks, expanding its scope [4].
- **Breach Data and Combo Lists:** Attackers commonly feed SilverBullet with credentials sourced from large breach compilations, systematically "testing" their validity across multiple platforms [1][7].

By combining easy configuration, extensive evasion techniques, and integrations that automate CAPTCHA solving (bot challenges) and manage proxy IPs SilverBullet offers attackers a comprehensive toolkit for high-volume credential stuffing [2][3][7]. Its open-source nature and active community ensure that new bypasses and improvements continually arise, significantly burdening defensive countermeasures.

Credential Stuffing Script (Config) Lifecycle

Phase 1: Testing and Writing – The config developer chooses the target site/application and asks their followers for credentials for an active user account. They use this account to test the application logic, API endpoints, third-party security vendors, and target detections.

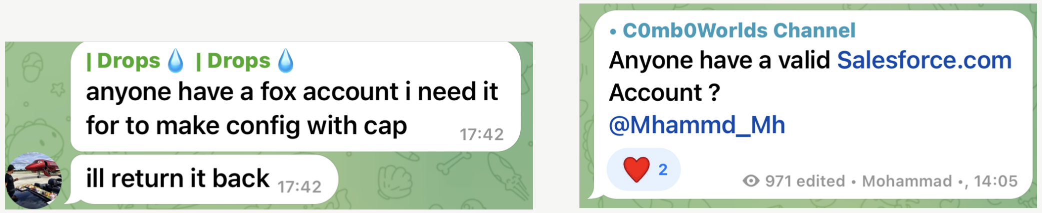
Phase 2: Underground – As soon as the configuration is created, it is sold for $50-150 per target for 3-4 weeks. Only 5-15 copies will be sold to minimize the attack's visibility and ensure it remains unpatched for as long as possible.

In this screenshot, you can see how the config developer is offering a new SVB config for sale and providing a "hit sample" of breached accounts as proof of concept.

Phase 3: Public – The configuration is shared for free on the developer's social media channels to enhance their reputation among potential clients. This step only occurs after the effectiveness of the configuration has been demonstrated. Although the attack still works, it typically has a lower success rate at this stage.

This is the stage at which we have collected all the configurations of the research sample, comprising 100 individuals overall.

Figure 3: Config developers asking followers for valid personal-use accounts (Source: Telegram)



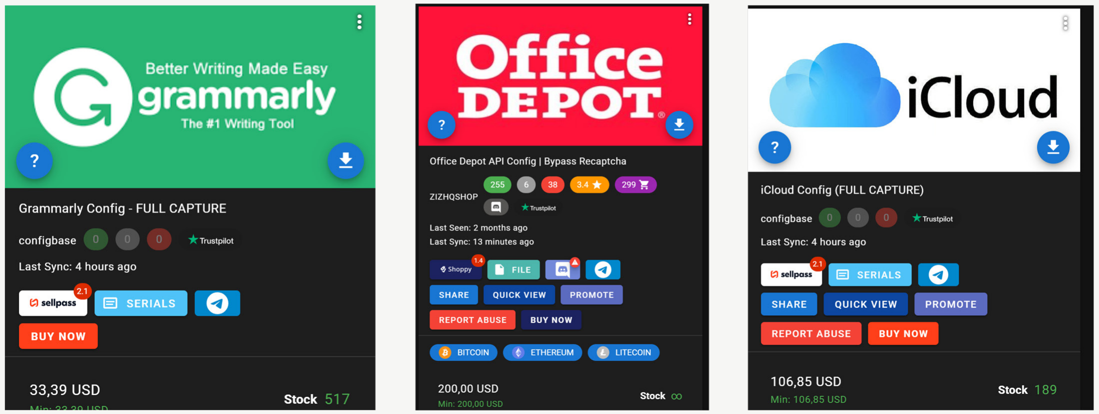
| Drops 💧 | Drops 💧
anyone have a fox account i need it for to make config with cap 17:42

ill return it back 17:42

• C0mb0Worlds Channel
Anyone have a valid Salesforce.com Account ?
@Mhammd_Mh

❤️ 2 971 edited • Mohammad •, 14:05

Figure 4: Configs (Credential stuffing script) offered for sale (Source: Shellix)



Grammarly Config - FULL CAPTURE
configbase 0 0 0 Trustpilot
Last Sync: 4 hours ago

33,39 USD
Min: 33,39 USD
Stock 517

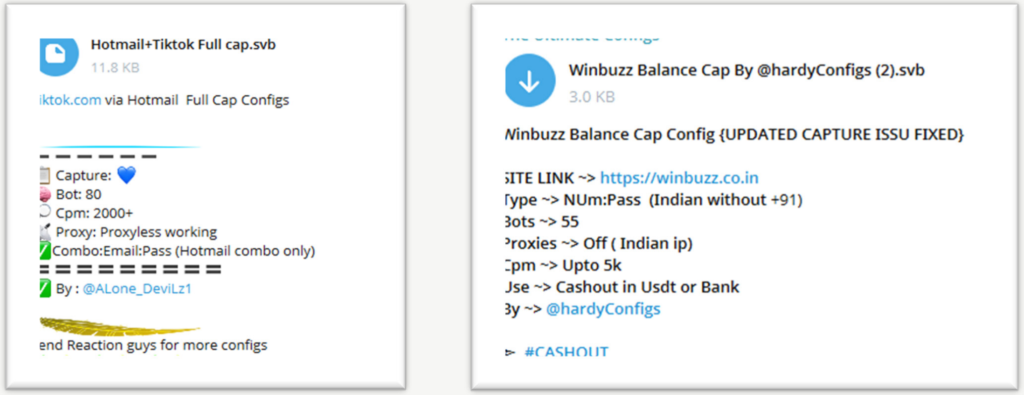
Office Depot API Config | Bypass Recaptcha
ZIZHQSHOP 255 6 38 3.4 ★ 299
Trustpilot
Last Seen: 2 months ago
Last Sync: 13 minutes ago

200,00 USD
Min: 200,00 USD
Stock ∞

iCloud Config (FULL CAPTURE)
configbase 0 0 0 Trustpilot
Last Sync: 4 hours ago

106,85 USD
Min: 106,85 USD
Stock 189

Figure 5: Config shared for free (Source: Telegram)



Hotmail+Tiktok Full cap.svb
11.8 KB
iktok.com via Hotmail Full Cap Configs

— — — — — — —
Capture: 💙
Bot: 80
Cpm: 2000+
Proxy: Proxyless working
✅Combo:Email:Pass (Hotmail combo only)
= = = = = = = = =
✅ By : @ALone_DeviLz1

end Reaction guys for more configs

Winbuzz Balance Cap By @hardyConfigs (2).svb
3.0 KB
Winbuzz Balance Cap Config {UPDATED CAPTURE ISSU FIXED}

SITE LINK ~> https://winbuzz.co.in
Type ~> NUm:Pass (Indian without +91)
Bots ~> 55
Proxies ~> Off (Indian ip)
Cpm ~> Upto 5k
Use ~> Cashout in Usdt or Bank
By ~> @hardyConfigs

#CASHOUT

Research Methodology

This research analyzes 100 SilverBullet credential stuffing attack scripts (configs) to identify emerging trends, techniques, and tactics in modern account takeover (ATO) campaigns.

Research Sample

Each of the 100 scripts collected from Telegram channels of threat actors met all four of the following criteria:

- Published between December 2024 and May 2025
- Written and designed for SilverBullet 1.1.4 (credential stuffing tool)
- Written by threat actors with at least one year of online presence

The analysis focuses on the following significant aspects:

1. **Threat Landscape and Targeted Industries**
   - Who are the top threat actors that wrote the 100-script research sample?
   - What makes them different?
   - What are the most targeted industries?
2. **Business Logic Attacks**
   - Exploration and exploitation of mobile, web, and API authentication endpoints
   - How threat actors manipulate a target's legitimate business logic to bypass its defenses
3. **API Targeting**
   - How and why threat actors target API authentication endpoints, especially older "shadow" APIs

Analytical Methodology

The research methodology employed forensic analysis of configuration scripts to identify and categorize attack patterns:

1. **Configuration Parsing:** Each SilverBullet configuration was analyzed to extract key attack components, workflow sequences, and target applications.
2. **Pattern Identification:** Statistical analysis was performed to identify prevalent attack methodologies and categorize them into taxonomies.
3. **Sophistication Scoring:** To assess relative sophistication, configurations were evaluated across multiple dimensions, including device manipulation, token exploitation, and business logic elements.
4. **Case Study Selection:** Representative configurations demonstrating advanced techniques were selected for in-depth analysis to illustrate emerging attack patterns.

This analysis focuses on the script's attack methods rather than the core features of the SilverBullet platform, allowing for the recognition of techniques employed by attackers through a standardized toolset.

Chapter 1: Threat Landscape and Targeted Industries

Threat Actors

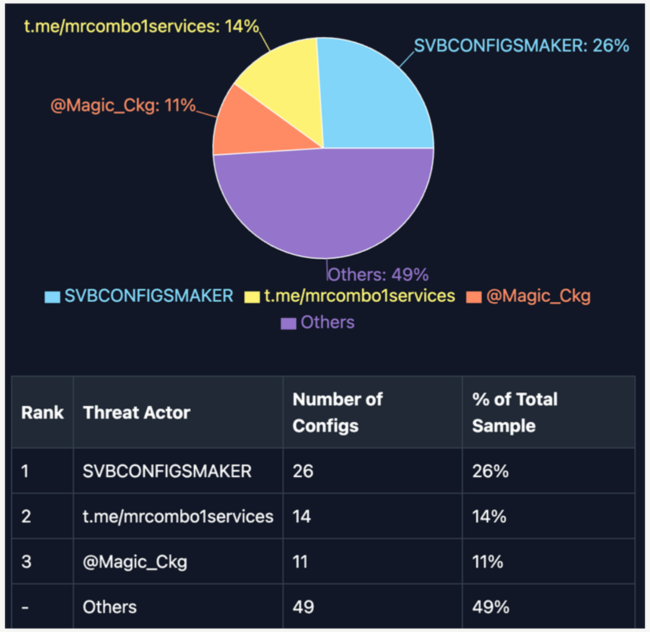
Our analysis of 100 SilverBullet credential stuffing configurations collected over the past six months reveals a concentrated landscape of threat actors actively developing and distributing attack scripts. Fifty-one of these configurations were written by only three threat actors (configuration authors).

Distinctive TTPs and Areas of Expertise

Each threat actor demonstrates identifiable patterns in their attack methodologies, revealing specialized competencies and preferred tactics:

	Areas of Expertise	Key TTPs
SVBCONFIGSMAKER	**AI platform auth bypass specialist** ↗ Auth token handling with CSRF (31%) ↗ Bypasses server redirects ↗ Advanced CAPTCHA handling	↗ User-agent spoofing (88%) ↗ API targeting (50%) ↗ JSON/form parsing (50%) ↗ Token exploitation (38%)
t.me/ mrcombo1services	**Mobile API specialist (Samsung)** ↗ Targets electronics accounts ↗ Sophisticated reCAPTCHA handling ↗ JWT token manipulation ↗ Multi-step auth bypass techniques	↗ User-agent spoofing (71%) ↗ Header injection (64%) ↗ Form parsing (57%) ↗ Referrer manipulation (57%)
@Magic_Ckg	**Microsoft cloud services specialist** ↗ Limited cookie auth (18%) ↗ No CSRF manipulation ↗ Enterprise auth bypass expertise ↗ OAuth flow specialist	↗ Form parsing (55%) ↗ User-agent spoofing (45%) ↗ JSON parsing (45%) ↗ API targeting (27%)

Figure 6: Distribution of attack script authors (configuration developers) across the research sample (Source: Radware)



Rank	Threat Actor	Number of Configs	% of Total Sample
1	SVBCONFIGSMAKER	26	26%
2	t.me/mrcombo1services	14	14%
3	@Magic_Ckg	11	11%
-	Others	49	49%

Key Findings:

- The author distribution across the research sample reveals a skill-centralized SilverBullet landscape dominated by a few experienced threat actors: **3 config developers are responsible for 51/100 configs.**
- All of these top 3 threat actors have been developing configs and selling them for more than two years
- Each threat actor demonstrates distinctive TTPs and areas of expertise (e.g., SVBCONFIGSMAKER specializes in AI platform auth bypass)

Creating an effective credential stuffing script demands specialized knowledge and skills. Due to this technical barrier, the three experienced configuration developers dominated the research sample, which included 28 threat actors.

Targeted Industries Distribution

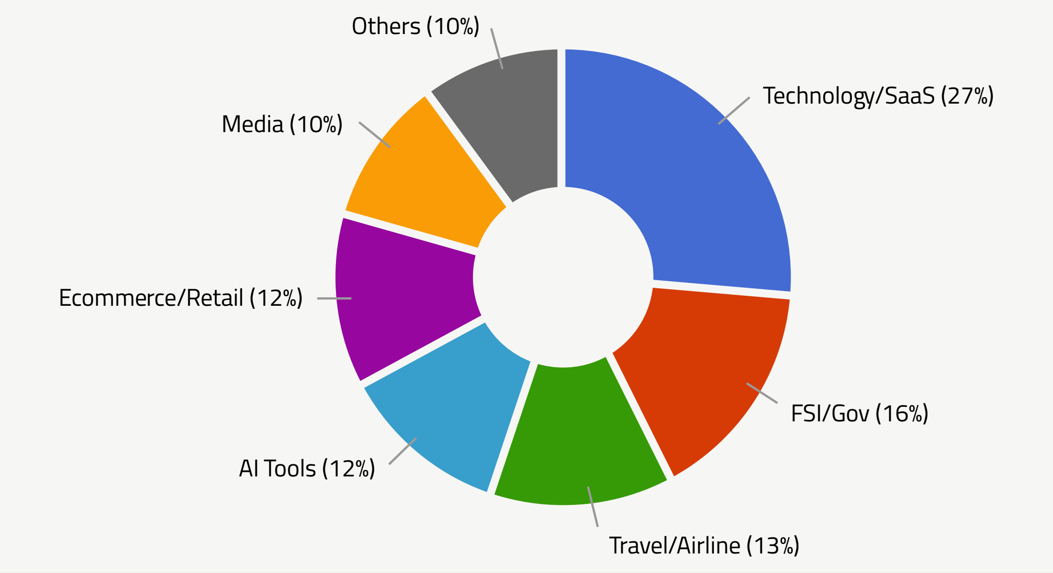
Each config is designed to attack specific applications or websites. By tagging the targeted application into industries we can learn about the threat actor's focus, driven by their buyer's (account cracker's) demand.

Our analysis reveals significant patterns in industry targeting, highlighting sectors most vulnerable to these attacks.

Key Statistics:

- Technology/SaaS (27%) is the most targeted industry, representing over a quarter of all credential stuffing attacks
- Financial services/government (16%) and travel/airline (13%) together account for 29% of attacks
- AI tools (12%) and e-commerce/retail (12%) each represent significant targeting percentages
- Media (10%) platforms continue to be a consistent target for account takeover
- Others (10%) include social media (7%), gaming (2%), and uncategorized (1%) targets

Figure 7: Total configs by industry across the entire research period (Source: Radware)



Total Sample Size:

100 SilverBullet credential stuffing configurations collected from Dec 2024 to May 2025

Industry Targeting Trends Over Time

The breakdown of targeted industries across the entire dataset reveals the following distribution:

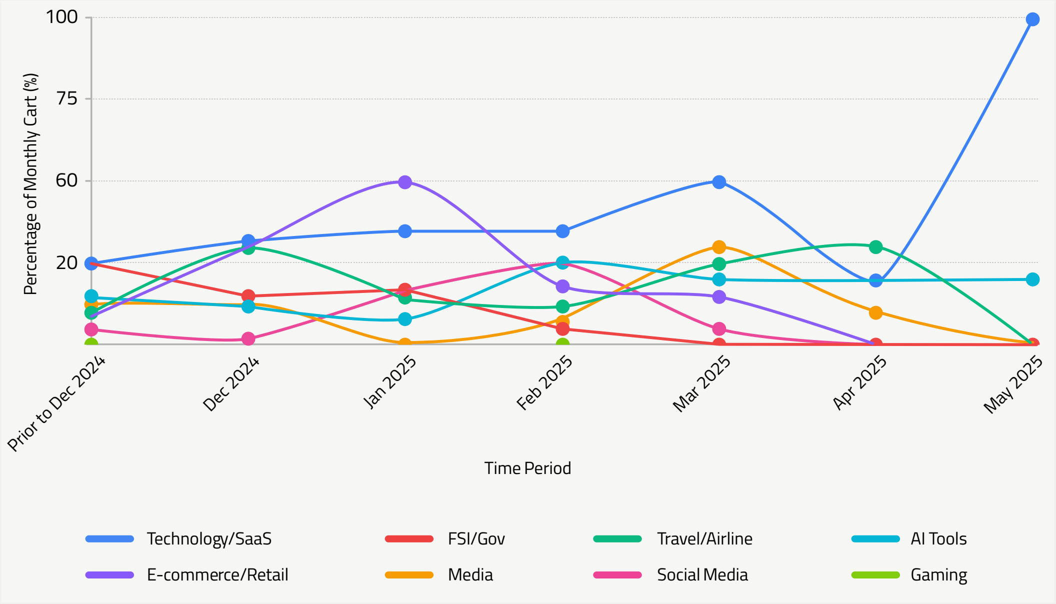
Key Findings:

- Technology/SaaS targeting varies significantly, with 100% focus in May 2025 as a result of two new sub-categories: corporate application and AI SaaS services (See "Highly Targeted Tools").
- E-commerce/retail shows a significant spike in January 2025 (50%)
- AI tools emerge strongly in February 2025 (27%)
- Travel/airline and media peak in April 2025 (30% each)
- Financial services shows sporadic but consistent targeting

Temporal Patterns:

- Clear shift from broad to focused targeting over time
- Cyclical patterns in industry focus by different threat actors
- Emerging targets (AI tools, gaming) appear primarily in 2025
- Concentration of attacks tends to correlate with industry events
- Recent months show more specialized, targeted campaigns

Figure 8: Industry targeting trend over time (Source: Radware)



Insights:

Focusing on the spike in e-commerce configs in January 2025 aligns with the 2024 holiday season:

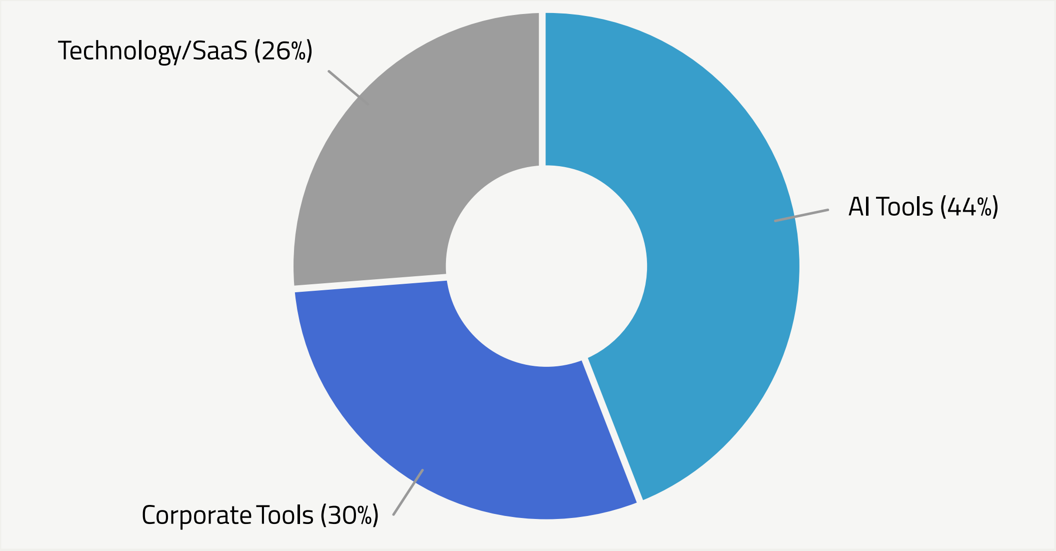
1. The holiday season takes place annually from November to December, featuring three significant online sales: Singles' Day, Black Friday, and Cyber Monday. This is a profitable period for e-commerce retailers, as shoppers are highly active, exchanging gift cards and updating their payment methods.
2. Account crackers are seeking new configs that will allow them to take over user accounts, which are now worth more than ever.
3. Config developers reacted to this growing demand by focusing on e-commerce and retail industries, reverse engineering their detections and expanding their target base.
4. As discussed in the previous "Credential Stuffing Script (Config) Lifecycle" section, each config is shared publicly only a few weeks after its creation. Thus, the configs we collected for the research were mainly written and sold in limited copies a month before. Therefore, the spike we see for the e-commerce industry in January 2025 makes sense.

Highly Targeted Tools

As shown in Figure 7, in May 2025, the technology/SaaS category spiked significantly, indicating that the config developers were heavily focused on this specific industry. Why?

The following is a breakdown of credential stuffing configurations targeting the technology/SaaS sector:

Figure 9: Application types within the "Tech" cluster (Source: Radware)



Key Stats:

- AI tools represent nearly half (44%) of technology/SaaS targeting
- Corporate tools account for 30%, demonstrating a growing focus on enterprise environments
- Combined, these emerging subcategories account for 74% of technology/SaaS campaigns

Insights:

This shift indicates a strategic evolution toward higher-value credential targets that are in demand by spammers and APT groups:

1. AI tools are in demand from spammers and social engineering threat actors.
2. Corporate applications are in high demand from ransomware groups and advanced persistent threats (APTs) seeking to gain initial access to organizations' and companies' networks.

AI Tool Target Breakdown

The distribution of AI tools targeted by credential stuffing attacks, followed by their exploitation potential, reveals how threat actors might use them for cyber activity.

Exploitation Potential:

- **Content Generation (42%):** Exploited to create convincing phishing messages at scale
- **Design & Creation (25%):** Enables fake branded content and spoofed materials
- **Research Platforms (17%):** Provides computational resources that can be diverted for malicious purposes
- **Text-to-Speech (8%):** Enables creation of voice deepfakes for vishing attacks
- **Website Builders (8%):** Rapidly create convincing phishing sites that mimic legitimate services

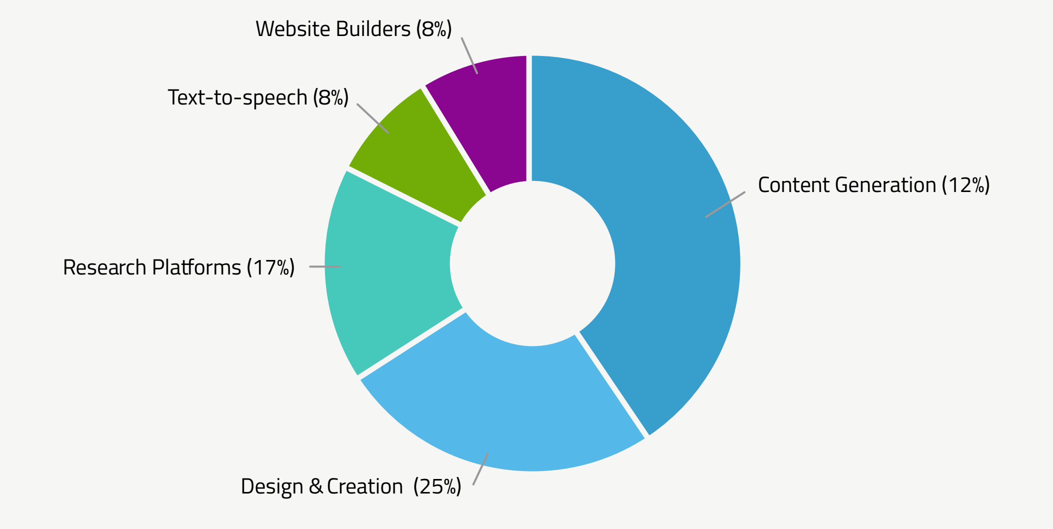


Figure 10: Application types within the "AI tools" cluster (Source: Radware)

Corporate Tool Target Breakdown

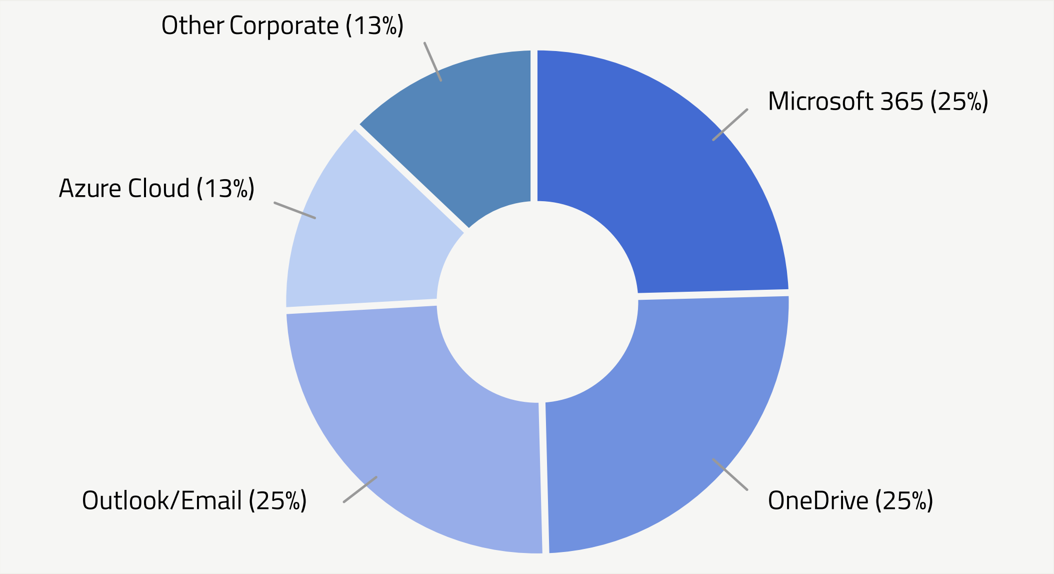
Distribution of AI tools targeted by credential stuffing attacks:

Security Impact:

- **Microsoft 365 (25%):** Provides access to corporate documents, communication, and potential for lateral movement
- **OneDrive (25%):** Enables data exfiltration and malware distribution via trusted channels
- **Outlook/Email (25%):** Facilitates business email compromise (BEC) attacks from legitimate addresses
- **Azure Cloud (13%):** Grants access to enterprise infrastructure and potentially sensitive data
- **Other Corporate (13%):** Offers various enterprise authentication systems with potential for privilege escalation

This subcategory represents a concerning trend: the shift from targeting consumer accounts to corporate authentication systems that potentially provide access to sensitive organizational data and resources. These techniques suggest increased sophistication in bypassing enterprise-grade security measures, with threat actors demonstrating detailed knowledge of corporate authentication workflows.

Figure 11: Application types within the "corporate tools" cluster (Source: Radware)



Chapter 2: Business Logic Attack (BLA) and Identity Manipulation

Definition and Significance

BLA Technical Definition: Business logic attacks exploit the design and implementation flaws in application workflows, session handling, transaction processing, and authorization controls by manipulating the expected sequence of steps, application states, or logical flows without triggering conventional security controls.

In simple terms, instead of breaking into an application by exploiting code vulnerabilities, business logic attacks essentially walk through the front door by following legitimate paths in unexpected ways, similar to how a con artist might exploit social norms rather than breaking physical locks to gain unauthorized access.

Business logic attacks are particularly challenging to defend against because they:

- Use legitimate application functions and API endpoints
- Generate traffic patterns that closely mimic normal user behavior
- Often bypass traditional security controls like WAFs and rate limiting
- Exploit flaws in business processes rather than technical implementation
- Leverage the application's own rules and logic against itself

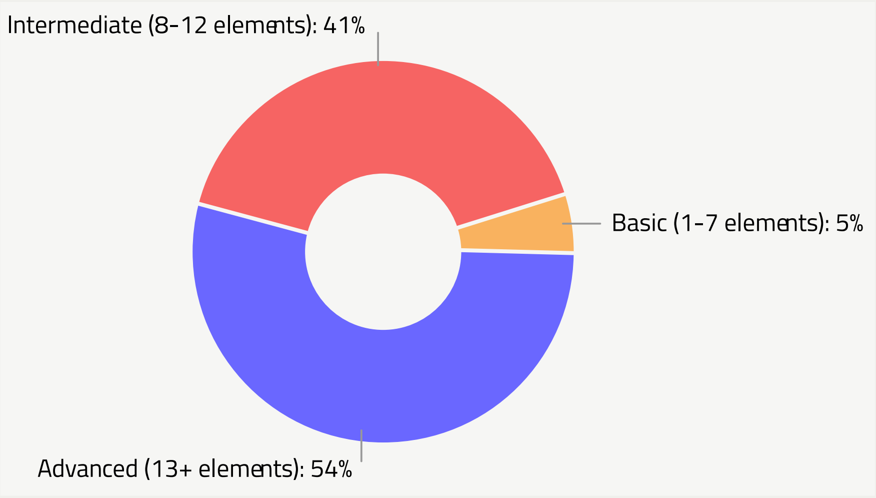
Business Logic Attack Distribution

Our findings suggest that business logic exploitation has become a fundamental component of credential stuffing, having evolved far beyond simple authentication attempts. The following section reveals the different levels of business logic sophistication:

Business Logic Attack Sophistication Levels:

- **Basic (1-7 elements):** Only 5% of configurations implement basic business logic attacks, typically limited to simple authentication attempts with minimal workflow manipulation.

Figure 12: Distribution of BLA level within the "BLA configs" cluster (Source: Radware)



- **Intermediate (8-12 elements):** 41% of configurations employ moderate sophistication, implementing multiple business logic techniques such as API sequencing, error message analysis, and session management.
- **Advanced (13+ elements):** The majority (54%) of configurations demonstrate highly sophisticated business logic orchestration, combining numerous attack techniques into complex workflows that closely mimic legitimate user behavior.

This BLA analysis shows that credential stuffing has evolved from basic password guessing into orchestrated **business logic exploitation**. Rather than simple repeated login attempts, attackers now:

- **Replicate entire user workflows:** following multi-step or multi-redirect sequences, handling conditional authentication paths, and analyzing errors to adjust.
- **Mimic regular traffic:** adopting genuine user-agent strings, re-using session tokens, and splitting requests logically.
- **Focus on post-auth data:** enumerating account details, subscription information, linked services, and privileges far beyond mere credential checks.

The near-universal (94%+) use of four or more elements indicates a fundamental shift in the threat landscape. Defending organizations must move beyond credential-centric controls to adopt security strategies that validate entire user processes, correlate cross-request behavior, and detect suspicious patterns in business logic flows.

These findings underscore that credential stuffing should be viewed as a multi-stage infiltration rather than merely a series of repeated password attempts. By recognizing the complexity of modern business logic attacks, security teams can implement defenses that effectively address these evolving, workflow-centric threats.

While device spoofing is a known tactic that bot operators have used for years, the Radware CTI team was surprised to find that 24% of the attack scripts alternated between two types of devices during the attack.

Distribution

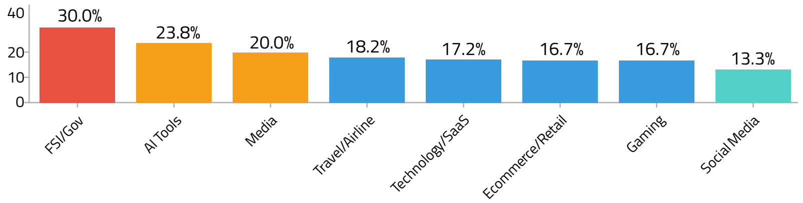


Figure 13: Distribution of ALL 24 device-transitioning configs across industries (Source: Radware)

Fingerprint Component Manipulation

Analysis of browser fingerprint components reveals selective manipulation. These are the most frequently manipulated headers:

Detection Opportunity: While all configs change User-Agent headers (100%), only ~60% also modify platform-specific headers (sec-ch-ua-*). This inconsistency creates a significant opportunity for detection systems to identify spoofing attempts by checking for mismatched device signals.

Platform Transition Distribution

- **Cross-platform transitions:** 32 out of 45 (71.1%)
- **Most common pattern:** iOS ↔ Windows bidirectional switching (62.3% of transitions)
- **Multi-OS targeting:** 16.7% of configs target 3+ operating systems

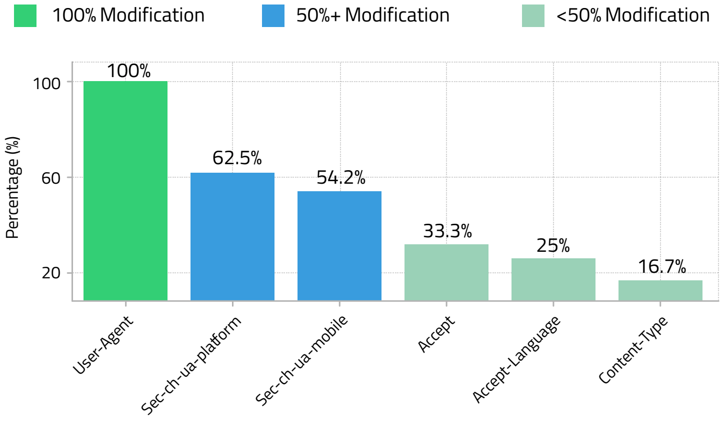


Figure 14: Percentage of configs that change each component between requests (Source: Radware)

Cross-Platform Switching Analysis

Examples

Case Study 1: PAYPAL BUG (FSI/Gov)

Devices: Windows, iOS

Transition Pattern: Windows → iOS

Strategic placement analysis:

1. **Pre-authentication (Windows):** Initial page load and CSRF token retrieval
2. **Authentication (Windows → iOS)**: Device switch occurs during login submission
3. **Post-authentication (iOS):** Account access and data extraction

Actual User-Agent Transition:

- **Windows:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36...
- **iOS:** Mozilla/5.0 (iPhone; CPU iPhone OS 16_6 like Mac OS X)

Case Study 2: Facebook Full Capture (Social Media)

Devices: Android, Windows

Transition Pattern: Android → Windows

Transition occurs at functional boundary:

1. **Mobile API authentication (Android):** Initial login via mobile endpoint
2. **Web session establishment (Windows):** Switch to desktop for full account access

Case Study 3: Samsung (E-commerce/Retail)

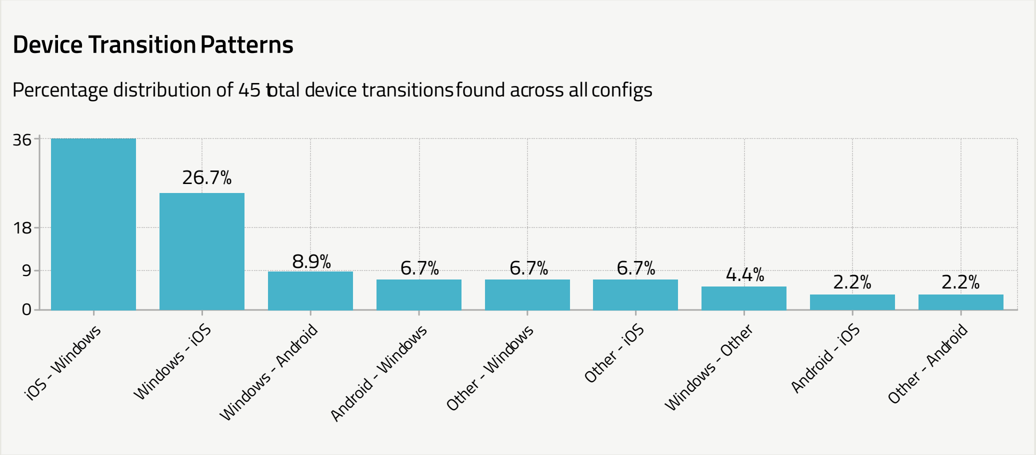
Devices: iOS, Windows

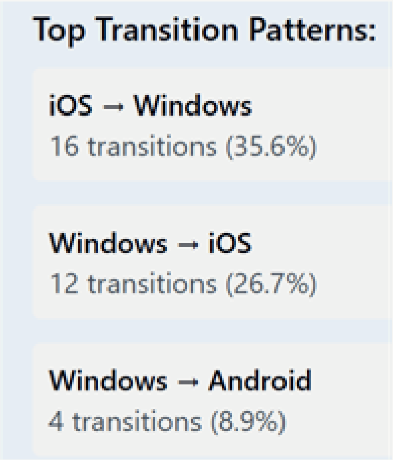
Multiple Transitions: iOS → Windows → iOS

Complex pattern targeting different security zones:

1. **Mobile app simulation (iOS):** Initial authentication
2. **Desktop checkout (Windows):** Payment processing
3. **Mobile verification (iOS):** Order confirmation

Figure 15: Percentage distribution of 45 total device transitions found across all configs (Source: Radware)





Top Transition Patterns:

iOS → Windows
16 transitions (35.6%)

Windows → iOS
12 transitions (26.7%)

Windows → Android
4 transitions (8.9%)

Security Implications and Recommendations

Key Findings

1. **71.1% of transitions are cross-platform**, indicating deliberate exploitation of inconsistent security policies between mobile and desktop environments. Bots are collecting authentication tokens with one device and replaying these tokens on another device as part of the same attack.
2. **FSI/Gov sector shows highest sophistication** with 20% of configs using 3+ device types, suggesting targeted attacks on high-value accounts.
3. **Strategic placement at authentication boundaries -** 87% of transitions occur during or immediately after authentication, exploiting reduced scrutiny post-login.

Defensive Recommendations

1. **Implement cross-platform session binding** that validates device consistency throughout authentication flows.
2. **Deploy behavioral analytics** that specifically monitor for rapid device-type transitions within single sessions.
3. **Strengthen security at functional boundaries** where attackers commonly place transitions (login API, mobile desktop).
4. **Institute industry-specific controls:**
   - **FSI/Gov:** Enhanced monitoring for 3+ device patterns
   - **Technology/AI:** Focus on iOS Windows transition detection
   - **E-commerce:** Monitor checkout flow device consistency

Conclusion

This analysis reveals sophisticated multi-device spoofing as a prevalent tactic in 25% of credential stuffing attacks, with attackers strategically placing device transitions to exploit gaps in security controls. The high percentage of cross-platform transitions (71.1%) and concentration in high-value industries demonstrates the evolving sophistication of credential stuffing attacks. Organizations must implement comprehensive device fingerprinting and behavioral analytics that span across platforms and authentication stages to combat these threats effectively.

Chapter 3: API Exploitations in Credential Stuffing Attacks

Our comprehensive analysis of 100 SilverBullet credential stuffing configurations reveals that APIs have become a significant target for threat actors. Using strict identification criteria that include explicit API paths, versioned endpoints, GraphQL endpoints, and API-specific headers, we found that 82.7% of examined configs contained API targeting techniques, demonstrating the distribution of API-based attacks in modern credential stuffing campaigns.

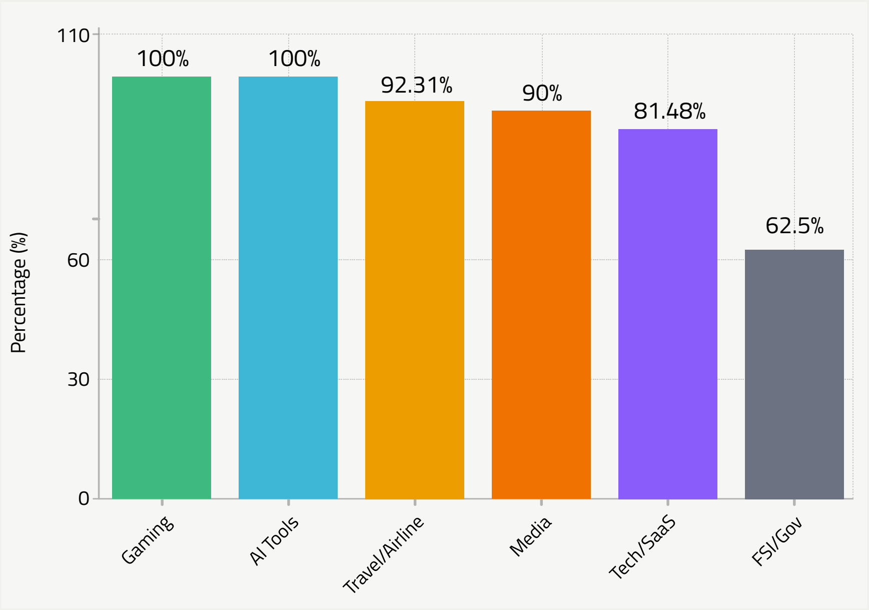
Industry Distribution

The distribution of API-based credential stuffing attacks varies across industries:

How many API targeting script were found per industry?

- **Gaming & AI tools (100%):** All configurations exclusively target API endpoints
- **Travel/airline (92.31%):** Heavy reliance on mobile app APIs for booking systems
- **Media (90%):** Focus on streaming APIs and content delivery endpoints
- **Technology/SaaS (81.48%):** 4/5 credential stuffing attack target API endpoint
- **FSI/gov (62.50%):** 2/3 credential stuffing attack targets the API endpoint

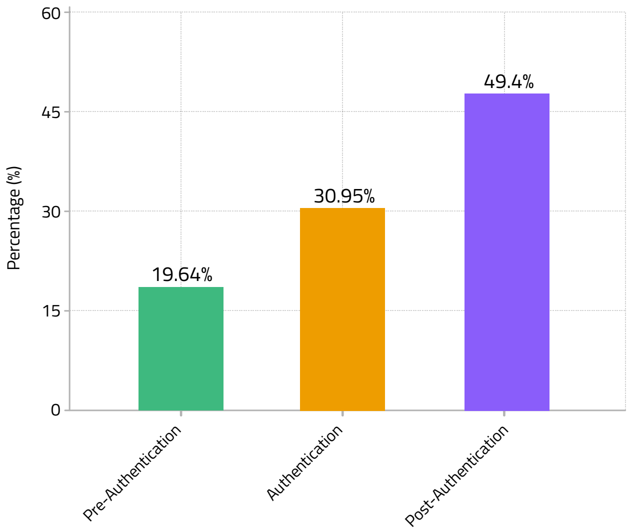
Figure 16: Distribution of API targeting per industry (Source: Radware)



Distribution of API Targeting Throughout the Attack Steps

Our analysis of the 168 API endpoints identified in the research sample reveals a clear pattern in how API targeting is distributed across the credential stuffing attack lifecycle:

Figure 17: Distribution of API targeting throughout the attack steps (Source: Radware)



1. **Pre-Authentication Phase (19.64%)**: These API calls typically involve gathering initial metadata, CSRF tokens, or session identifiers needed for subsequent authentication requests. This phase sets up the attack framework.
2. **Authentication Phase (30.95%):** Nearly a third of API targeting occurs during authentication, where credentials are validated, and the initial session context is established.
3. **Post-Authentication Phase (49.40%):** The majority of API targeting occurs after successful authentication, focusing on data extraction and validation of successful compromise. This reflects the ultimate goal of threat actors: to extract valuable information from compromised accounts so it can be used to accurately price the breached accounts.

The significant weight toward post-authentication activities (nearly 50% of all API targeting) reveals that credential stuffing attacks are not merely interested in validating credentials but are systematically designed to extract valuable data and fully exploit compromised accounts.

API Targeting Strategy Across Attack Phases

The analysis reveals distinct patterns in how APIs are targeted across phases:

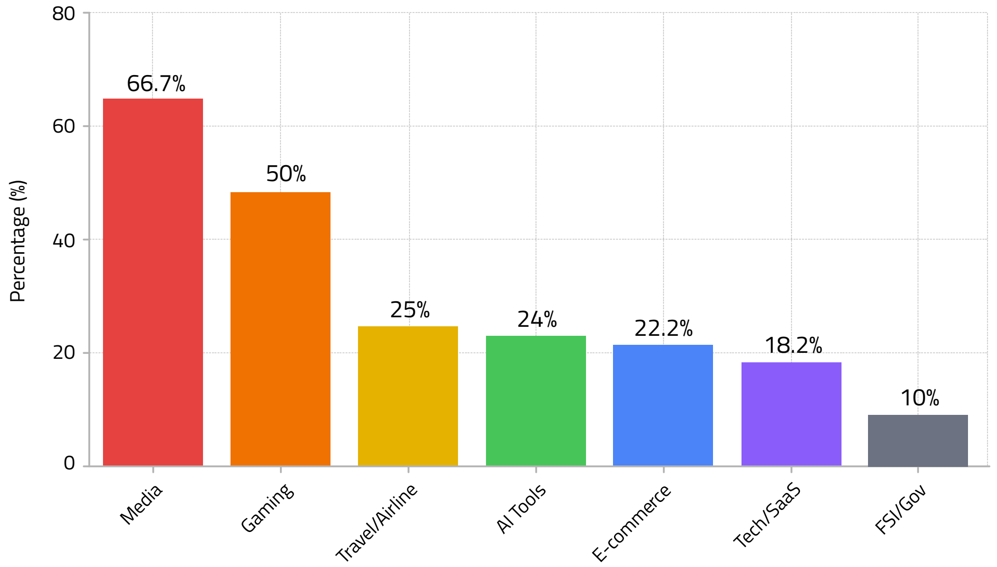
1. **Pre-Authentication Phase:**
   - Target metadata APIs for initial reconnaissance
   - Request CSRF tokens and session identifiers
   - Retrieve site structure and authentication requirements
2. **Authentication Phase:**
   - Submit credentials to the authentication APIs
   - Process multi-factor authentication challenges
   - Exchange initial tokens for session tokens
3. **Post-Authentication Phase:**
   - Query user profile and account information
   - Access financial data and transaction history
   - Retrieve loyalty points and program benefits
   - Gather subscription details and entitlements

This progressive targeting strategy illustrates how threat actors develop sophisticated, multi-stage API-based attack chains that follow the natural progression of application workflows: prepare, authenticate, and extract.

Shadow API Exploitation

Shadow APIs represent legacy, deprecated, or undocumented API endpoints that remain accessible but are often less monitored and may have weaker security controls. Using strict identification criteria that focus on genuine legacy indicators, we found that 21 API-targeting configs (25.61%) specifically exploit shadow APIs.

Figure 18: Distribution of Shadow-API targeting across industries (Source: Radware)



Distribution of shadow-API attack scripts across each targeted industry:

The media sector exhibits the highest distribution of shadow API targeting (66.67%), followed by the gaming sector (50.00%). This suggests that these industries may maintain more legacy API endpoints for compatibility with older systems or mobile applications.

Shadow API Targeting Techniques

Our analysis identifies several genuine techniques that attackers use to target shadow APIs:

1. **Explicit Legacy Terminology:** Some configurations target endpoints that explicitly include “legacy” or “deprecated” in their paths or documentation, indicating older functionality that may remain accessible but receive less security attention.
2. **Legacy OAuth Implementations:** A subset of attacks target OAuth 1.0 endpoints, which are considered legacy compared to the more secure OAuth 2.0 protocol widely used today.
3. **Version Fallback Logic:** More sophisticated attacks include logic to try different API versions, falling back to older versions if newer ones fail, potentially exploiting different validation rules.
4. **Multiple Version Indicators:** Configurations that exhibit multiple indicators of targeting older versions, such as combining v1 paths with legacy headers or comments referencing older compatibility.

Summary and Insights

Chapter 1: Threat Landscape

Key Threat Actor Findings:

- Analysis of 100 credential stuffing configurations reveals a skill-centralized SilverBullet landscape dominated by a few prolific threat actors. Three config developers are responsible for 51/100 configs.
- Each of these top three threat actors have been developing configs and selling them for more than two years.
- Each threat actor demonstrates distinctive TTPs and areas of expertise (e.g., SVBCONFIGSMAKER specializes in AI platform auth bypass).

Creating an effective credential stuffing script demands specialized knowledge and skills. Due to this technical barrier, three experienced configuration developers dominated the research sample.

Industry Targeting Statistics:

- **E-commerce:** Experienced a notable spike in January 2025 (aligned with post-holiday season)
- **Technology/SaaS subcategories:**
  - AI tools - (44%)
  - Corporate tools (30%)
  - Traditional SaaS (26%)

AI Tool Targeting Breakdown:

- Content generation platforms (42%)
- Design tools (25%)
- Research platforms (17%)
- Text-to-speech and website builders (8% each)

Chapter 2 - Business Logic Attack

Attack Sophistication Levels:

- **Advanced (13+ elements):** 54% of configurations
- **Intermediate (8-12 elements):** 41% of configurations
- **Basic (1-7 elements):** Only 5% of configurations

Most Common Business Logic Attack Elements:

- Error message analysis/response differentiation (100%)
- Conditional logic based on responses (100%)
- Header manipulation (98%)
- Parameter manipulation/injection (97%)
- Multi-step authentication sequence manipulation (77%)
- API sequencing/request order manipulation (90%of API-targeting Configs)

Post-Authentication Activities:

Data harvesting (91% extract valuable account data) – also known as “Capture” – this information usually includes:

  - Account balance
  - Miles/royalty points/credits/gift cards
  - Payment methods and the last four numbers of the user’s credit card

Entity relationship mapping:

- 23% of configurations map account relationships – identify linked services or subscriptions
- Implementation focuses on understanding the complete account ecosystem

These behaviors indicate that modern credential stuffing extends beyond merely validating credentials and involves thorough account profiling and data extraction. Developers catering to account crackers require Config to gather this data because it is essential for them to determine the value and price of the compromised account.

Chapter 3: API Exploitations

82% of examined configurations contain explicit API targeting techniques

API Targeting by Industry:

- AI tools and gaming (100%)
- Travel/airline (92.31%), media (90%)
- Technology/SaaS (81.48%), e-commerce/retail (75%), social media (71.43%)
- Financial services/government (62.50%)

API Endpoint Type Distribution:

- Authentication endpoints (71.95%)*
- User/profile endpoints (30.49%)*
- Data retrieval endpoints (2.44%)*
- Payment/billing endpoints (1.22%)*

Attack Phase Distribution:

- Pre-authentication phase (19.64% of API endpoints)
- Authentication phase (30.95% of API endpoints)
- Post-authentication phase (49.40% of API endpoints)

Shadow API Exploitation:

- API-targeting configurations exploit shadow APIs (25.61%)
- **Highest Distribution:** Media sector (66.67%), gaming (50%)
- **Medium Distribution:** AI tools (25%), travel/airline (25%), e-commerce/retail (22.22%)
- **Lower Distribution:** Technology/SaaS (18.18%), FSI/Gov (10%)
- **No observed targeting:** Social media (0%)

*Authentication endpoints 71.95 % + User/profile endpoints 30.49 % + Data retrieval endpoints 2.44 % + Payment/billing endpoints 1.22 % = 106.1 %. Configs can hit multiple endpoint types, therefore the percentage exceeds 100%

Resources List

1. https://www.trendmicro.com/en_us/research/21/d/how-cybercriminals-abuse-openbullet-for-credential-stuffing-.html
2. https://www.wired.com/story/roku-breach-hits-567000-users/
3. https://github.com/mohamm4dx/SilverBullet
4. Leaked "SilverBullet Pro" Documentation (2022) – Details on extended protocols, improved UI, and code forks. (Deep Web classified resource) /
5. https://minutodaseguranca.blog.br/
6. https://www.kasada.io/fraudsters-silver-bullet-for-credential-stuffing/

Author

Arik Atar | Senior Cyber Threat Intelligence Researcher

Editors

Pascal Geenens | Director of Cyber Threat Intelligence

Executive Sponsors

Ron Meyran | VP Strategic Alliances Marketing & Cyber Threat Intelligence
Deborah Myers | Senior Director of Corporate Marketing

Production

Jeffrey Komanetsky | Content Development Manager
Kimberly Burzynski | Senior Marketing Communication Manager

Table of Figures

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILABILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT USER'S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY RELATED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE.

© 2025 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this report are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see https://www.radware.com/LegalNotice. All other trademarks and names are the property of their respective owners.