Inside the Infostealer Economy: How Threat Actors Turn Stolen Credentials into Enterprise Breaches

Marcelle Lee

ISSA Central Maryland

28 October 2026



Marcelle Lee | Fractal Security Group. All Rights Reserved.

About Marcelle

- Founder & Principal Advisor, Fractal Security Group
- Security researcher, consultant, and threat intelligence practitioner
- Adjunct Professor
- Cyberjutsu BoD President
- Four degrees and many certifications



linktr.ee/marcellelee

mylee@fractalsecuritygroup.com

Marcelle Lee | Fractal Security Group. All Rights Reserved.

Agenda

- Why info stealers matter
- The info stealer economy
- Infection vectors
- Vercel case study
- Mitigation and detection



Marcelle Lee | Fractal Security Group. All Rights Reserved.

Why Info Stealers Matter



Marcelle Lee | Fractal Security Group. All Rights Reserved.

DATA BREACHES

Dozens of Major Data Breaches Linked to Single Threat Actor

The initial access broker (IAB) relies on credentials exfiltrated using information stealers to hack organizations.



By Ionut Arghire | January 6, 2026 (7:29 AM ET)

Anthropic Users Hit by Infostealer Attacks, Session Thefts

A threat actor used a variety of infostealers to collect session information and access Claude accounts belonging to an unknown number of users.



Jai Vijayan, Contributing Writer
August 31, 2026

3 Min Read

Featured

Iranian Hackers Likely Used Malware-Stolen Credentials in Stryker Breach

The medtech giant has been working on restoring systems affected by the cyberattack conducted by the Handala hackers.



By Eduard Kovacs | March 18, 2026 (8:47 AM ET)

BLOG POST

Infostealers Are Actively Hunting AI Agents and Developer Keys – Warden Infostealer

InfoStealers OCT 7, 2026 7 MIN READ

Vercel confirms breach as hackers claim to be selling stolen data

By **Lawrence Abrams**

World Cup grudge attackers may have scored Argentine FA access via year-old infostealer infection

Footie fans? Overreacting? There's a first time for everything

Connor Jones CYBERSECURITY REPORTER

4

State of the Info Stealer Threat Landscape



Close to **2 billion credentials** were stolen from **7.5 million devices** in the first half of 2026 alone.

A single compromised host can yield close to **100 credential pairs**.

Up to **80% of MFA-bypass incidents** trace back to stolen session tokens and cookie replay.

Over **54% of ransomware victims** had domain credentials listed for sale on dark web stealer-log marketplaces.

Stolen credentials and identity abuse are tied to close to **40% of all enterprise breaches**.

Marcelle Lee | Fractal Security Group. All Rights Reserved.

Review: Top Initial Access Vectors



SOCIAL ENGINEERING



CREDENTIAL ABUSE



VULNERABILITY EXPLOITATION

Info stealers bridge these two vectors

Marcelle Lee | Fractal Security Group. All Rights Reserved.

The Info Stealer Economy



Marcelle Lee | Fractal Security Group. All Rights Reserved.

INFO STEALER LIFECYCLE



MALWARE CREATION AND MAAS BUILDER

DISTRIBUTION VIA MALVERTISING

LOG EXFILTRATION TO C2

DARK WEB SALES VIA INITIAL ACCESS BROKERS

ENTERPRISE COMPROMISE

Malware as a Service (MaaS)

- Affordable monthly subscriptions allow low-skilled actors to deploy enterprise-grade malware.
- Payloads are continuously updated to outpace EDR behavioral signatures.
- Platforms offer user documentation, 24/7 technical support, feature requests, and escrow services.



Marcelle Lee | Fractal Security Group. All Rights Reserved.

ANY RUN

Malware Trends Tracker

Malware and phishing trends powered by a community of 700,000+ security professionals: rankings, IOCs, and analysis sessions, updated in real time.

Search by malware name...

7 d | 14 d | 30 d | 365 d | All time

Filters

Stealer

#	Family	Type	Trend changes	World rank	Tasks overall
1	SalatStealer	Stealer		3 ↑	1 210
2	ACR Stealer	Stealer		5 ↑	971
3	LokiBot	Stealer		22 ↓	202
4	Stealc	Stealer		29 ↓	135
5	Lumma	Stealer		35 ↓	109
6	RedLine	Stealer		45 ↓	73
7	Remus Stealer	Stealer		50 ↓	62
8	Blank Grabber	Stealer		52 ↑	60
9	Rhadamanthys	Stealer		54 ↑	55
10	Raccoon	Stealer		70 ↑	27

Marcelle Lee | Fractal Security Group. All Rights Reserved.

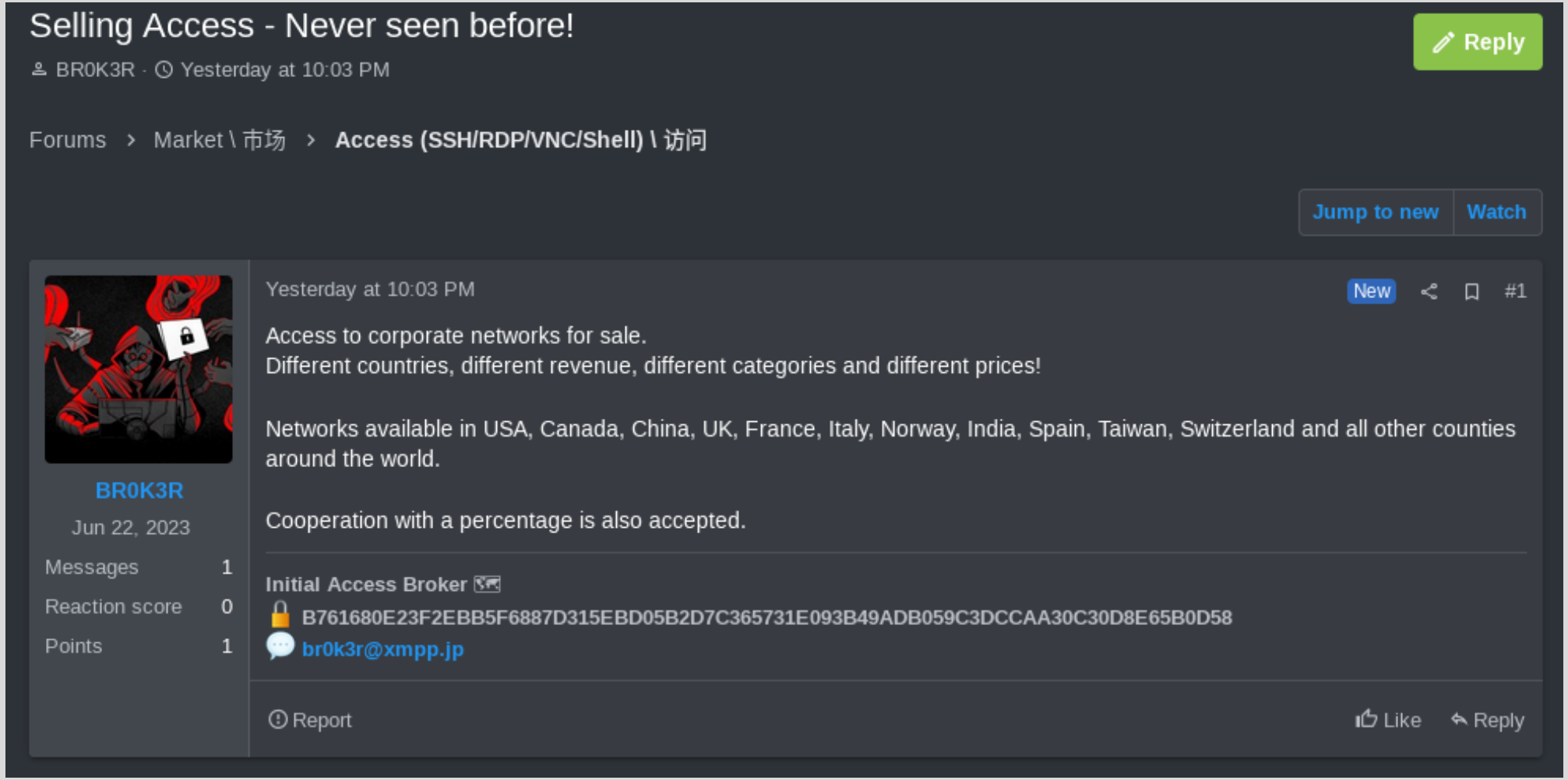
Initial Access Brokers (IABs)

- IABs are the wholesale distribution layer of cybercrime.
- Gain initial access only versus executing full end-to-end attacks.
- Rely on high-volume, automated attacks.
  - Purchase bulk info stealer logs
  - Run automated scans to identify vulnerable infrastructure
- Research targets to determine the price tag of access
  - Company revenue
  - Access level and type
  - Organizational defenses



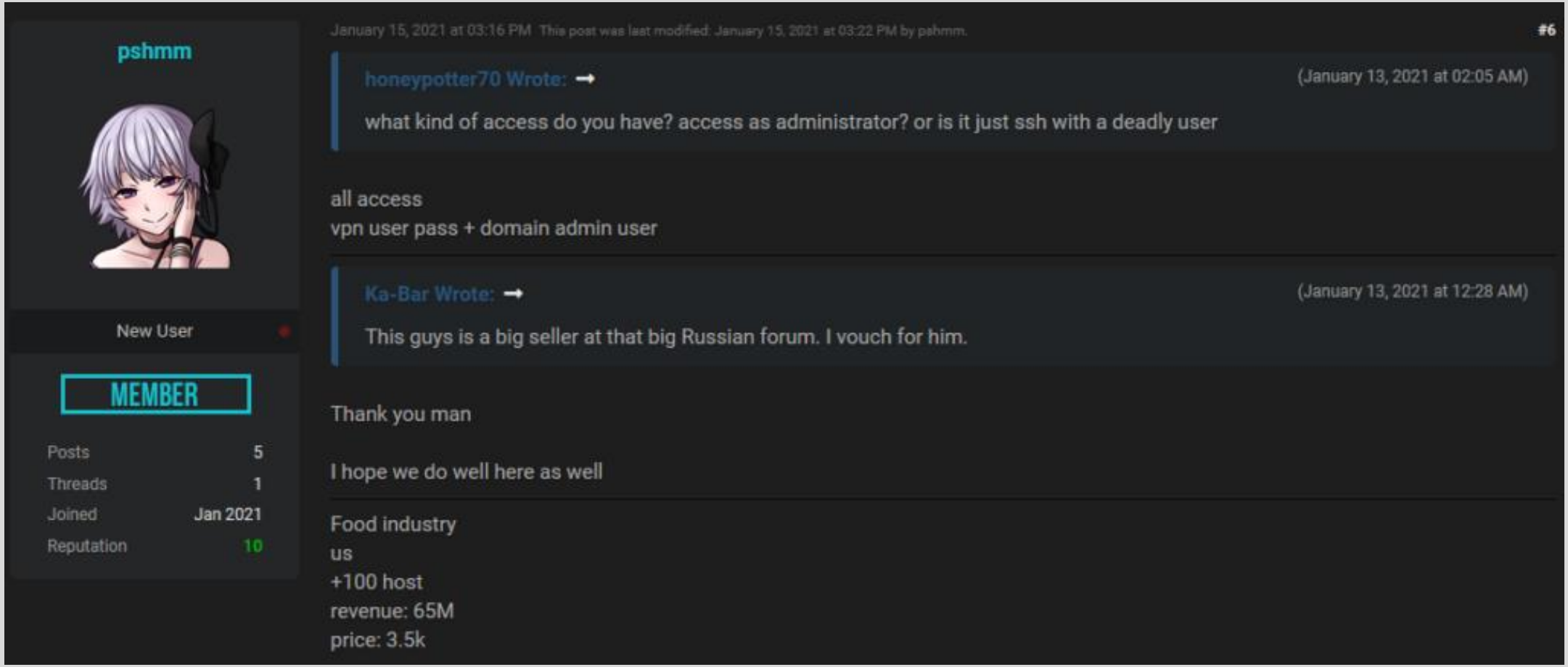
Marcelle Lee | Fractal Security Group. All Rights Reserved.

IAB Marketplace Post



Marcelle Lee | Fractal Security Group. All Rights Reserved.

IAB Forum Discussion



Marcelle Lee | Fractal Security Group. All Rights Reserved.

FINANCIAL IMPACT OF THE INFOSTEALER ECONOMY:

From Dark Web Markets to Enterprise Damages

DIRECT DARK WEB MARKET SIZE

$3 BILLION

Estimated revenue from infostealer sales (malware-as-a-service, credentials, data logs) within underground forums



Stolen credentials

SOVEREIGN COUNTRY GDP COMPARISON

BELIZE

Est. GDP:
~$3.2 BILLION
(or a similar recent number)

BHUTAN

Est. GDP:
~$2.8 BILLION
(or a similar recent number)

*Annual figures for context (approx.)

DOWNSTREAM ENTERPRISE IMPACT

OVER $100 BILLION+

DATA BREACH COSTS
- INCIDENT RESPONSE
- LEGAL FEES
- REGULATORY FINES

INTELLECTUAL PROPERTY THEFT
- LOST R&D
- COMPETITIVE DISADVANTAGE

RANSOMWARE PAYMENTS
- SYSTEM LOCKOUTS
- EXTORTION DEMANDS

CREDENTIAL STUFFING ATTACKS
- ACCOUNT TAKEOVERS
- FRAUD LOSSES

OPERATIONAL DISRUPTION
- DOWNTIME COSTS
- PRODUCTIVITY LOSS

Infection Vectors



Marcelle Lee | Fractal Security Group. All Rights Reserved.

Infection Vectors

Attack	Mechanism	Lure / Trick	Payload
ClickFix & Fake CAPTCHA Prompts	Users visiting compromised or malicious websites encounter a fake system error, verification check, or "CAPTCHA" prompt.	The page instructs the victim to "prove they are human" or fix a display issue by copying a provided code snippet and pasting it into the Windows Run dialog (Win + R) or PowerShell terminal.	The pasted string silently executes a fileless PowerShell command that downloads and runs the infostealer in memory before the user realizes what happened.
Malvertising & Brand Spoofing	Cybercriminals purchase sponsored ad slots at the top of legitimate search engines (e.g., Google Ads, Bing Ads) targeting common enterprise queries.	Spoofing popular corporate tools, remote desktop clients, utility apps, or developer frameworks (e.g., Notepad++, PuTTY, Teams, Zoom, Slack, or AI tools like Claude Code / Gemini CLI).	Users clicking the ad are sent to a cloned brand website that serves a Trojanized installer bundled with an infostealer payload.
Search Engine Optimization (SEO) Poisoning	Attackers manipulate search engine algorithms using black-hat SEO techniques (keyword stuffing, backlink networks) or by compromising established, high-authority websites.	High-ranking search results offering technical documentation, niche software fixes, or utility installers.	Clicking the search result directs the user through traffic distribution networks (TDS) that selectively serve malicious downloads disguised as legitimate installers or setup files.
Fake Software & Browser Updates (Drive-By Downloads)	Compromised legitimate websites (e.g., hacked WordPress instances) are injected with malicious scripts that overlay urgent pop-ups.	Warnings stating that the user's browser (Chrome, Firefox, Edge) or software plugin is out of date and must be updated to view the content.	Clicking "Update Now" downloads a disguised executable package that drops the stealer binary directly onto the endpoint.
Phishing	Direct communication targeting specific roles (developers, IT admins, executive assistants) via email, LinkedIn, GitHub, or Telegram.	Fake job offers, "work samples," code review requests, or vendor invoice attachments.	Password-protected ZIP or ISO archives containing shortcut files (.lnk), compiled C# binaries, or obfuscated scripts designed to bypass perimeter email gateways.



Marcelle Lee | Fractal Security Group. All Rights Reserved.

Vercel Case Study



Marcelle Lee | Fractal Security Group. All Rights Reserved.

Vercel Security Incident



In February 2026, an employee at Context.ai (a third-party AI startup) downloaded a malicious file that delivered Lumma Stealer.



Lumma Stealer harvested saved browser data, session tokens, and credentials from the Context.ai employee's machine.



Separately, a Vercel corporate employee had previously signed up for and used Context.ai, granting the app broad, persistent OAuth permissions over their Vercel corporate Google Workspace account.



Because the attackers now controlled Context.ai's backend infrastructure, they extracted the active OAuth tokens granted by that Vercel employee. These tokens allowed the attackers to authenticate as the Vercel employee, bypassing MFA entirely.



The threat actor used this compromised employee session to log directly into Vercel's internal environments and bulk-extract customer secrets and environment variables.



Marcelle Lee | Fractal Security Group. All Rights Reserved.

Mitigation and Detection



Marcelle Lee | Fractal Security Group. All Rights Reserved.

Mitigations

- Application allow-listing
- Browser isolation/managed profiles
- Network-level DNS filtering
- Enterprise ad blockers
- Phish-resistant MFA, e.g. hardware keys
- Session revocation policies
- Device compliance rules
- Continuous dark web monitoring
- Continuous credential exposure monitoring
- User education
- Leverage threat intelligence



Marcelle Lee | Fractal Security Group. All Rights Reserved.

Using Threat Intelligence to Combat Infostealers

- Track Emerging Infostealer Campaigns
  - Monitor malware families such as Lumma, RedLine, StealC, and Vidar
  - Understand evolving delivery methods including ClickFix, phishing, and fake software updates
- Improve Detection & Detection Engineering
  - Identify indicators associated with active campaigns
  - Develop detections for browser credential theft, cookie theft, and token abuse
- Prioritize Defensive Investments
  - Focus on the techniques most commonly used by infostealer operators
  - Align security controls to current attacker tradecraft
- Support Incident Response
  - Determine whether stolen credentials have appeared in criminal marketplaces
  - Assess exposure from leaked session tokens and browser artifacts
- Provide Strategic Risk Awareness
  - Understand how compromised credentials are fueling ransomware and extortion operations
  - Communicate emerging risks to leadership using real-world intelligence



Marcelle Lee | Fractal Security Group. All Rights Reserved.

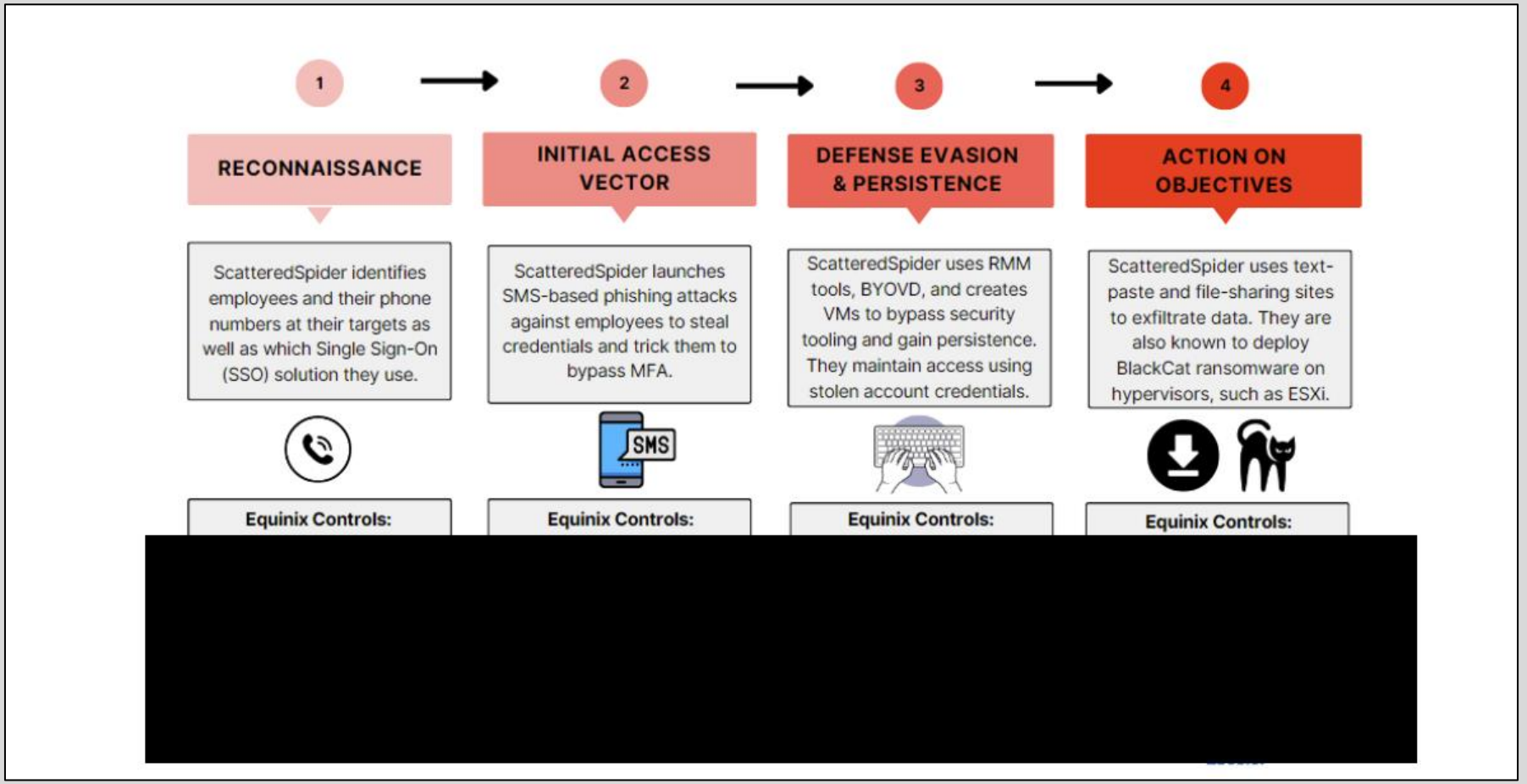
ATT&CK Mapping

Tactical Phase	Technique ID	Technique / Sub-Technique	Observed Infostealer Behavior / Telemetry
Initial Access	T1189	Drive-by Compromise	Malvertising campaigns, poisoned Google/Bing ads redirecting to fake software download sites.
	T1566.002	Phishing: Spearphishing Link	Phishing emails containing links to malicious ISO/ZIP archives or "Fake CAPTCHA" pages.
Execution	T1204.002	User Execution: Malicious File	User opening an executable disguised as utility software (e.g., Notepad++, PDF reader, game mods).
	T1059.001	Command Scripting: PowerShell	"ClickFix" fake CAPTCHA tricks users into pasting PowerShell command strings into Win + R Run dialogs.
Credential Access	T1555.003	Credentials from Web Browsers	Extracting SQLite databases (Login Data, Cookies, Web Data) across Chromium and Gecko browsers.
	T1539	Steal Web Session Cookie	Extracting pre-authenticated session tokens to facilitate subsequent Multi-Factor Authentication (MFA) bypass.
Discovery	T1082	System Information Discovery	Gathering OS version, hostname, installed antivirus, GPU drivers, and public IP to fingerprint the target.
Collection	T1005	Data from Local System	Bundling browser profiles, VPN configs, crypto wallets, desktop files, and screenshots into a .zip log archive.
Command & Control	T1071.001	Web Protocols	Exfiltrating zip logs to C2 servers via HTTPS POST requests, or leveraging legitimate APIs (Telegram Bot API, Discord Webhooks).
Initial Access (Pivot)	T1078.004	Valid Accounts: Cloud Accounts	Adversaries perform session replay / token theft to log directly into Microsoft 365, Okta, or AWS without MFA prompts.



Marcelle Lee | Fractal Security Group. All Rights Reserved.

Assessing Security Control Gaps



Marcelle Lee | Fractal Security Group. All Rights Reserved.

Operationalizing Intelligence

Threat Hunting: develop hypotheses and hunt across systems

Detection Engineering: use mapping to create or tune detection rules

Incident Response: create playbooks and investigation workflows

Control Validation: test controls and remediate gaps

Leadership: prioritize investments and communicate risk



Marcelle Lee | Fractal Security Group. All Rights Reserved.

Conclusion



Every stolen login represents a potential entry point.

Treat identity as your new perimeter.

Marcelle Lee | Fractal Security Group. All Rights Reserved.

MARCELLE LEE

Fractal Security Group

mylee@fractalsecuritygroup.com

linktr.ee/marcellelee

SCAN TO CONNECT

Marcelle Lee | Fractal Security Group. All Rights Reserved.