Democratising Cybersecurity
www.falconfeeds.io

The Evolving Stealer Threat Landscape:

A One-Month Deep Dive

(Aug 20 – Sept 19, 2025)

Rapid commoditisation, new high-value targets, and living-off-the-land TTPs — what every security leader must act on now.

The Deepest Watch on the Darkest Web

FalconFeeds.io delivers the largest real-time monitoring of deep and dark web activity—from ransomware gangs to Telegram dumps and access marketplaces.

Executive Summary

The Evolving Stealer Threat

What this means

Attackers are buying turnkey tools and hiding in legitimate traffic — so "known bad" signatures aren't enough.

The stealer threat landscape is changing fast. Over the one-month window (August 20 – September 19, 2025) our telemetry shows a sharp rise in activity, a strategic re-orientation to novel target vectors, and adoption of more advanced TTPs. The environment has become commoditized: malware is now routinely offered as complete, scalable packages with builder panels, enabling faster proliferation and easier evasion of signature-based defences.

Top families by IOC volume are **FormBook, MassLogger, and XWorm.** New entrants such as Trap Stealer 2025 and the **Phoenix Android Botnet** are growing explosively, pointing to a pivot toward social and mobile platforms. Three cross-cutting themes dominate the period: (1) an As-a-Service economy for malware, (2) extensive abuse of legitimate, trusted services and living-off-the-land techniques for C2 and exfiltration, and (3) intensified monetization of high-value assets (cryptocurrency, 2FA, sensitive corporate and government data). This report profiles these threats, their operational methods, and provides actionable mitigation steps.

The Stealer Threat Landscape:
A Quantitative Analysis

Think Box

Do you maintain a prioritized IOC watchlist of new variants? How frequently do you run hunts for unknown hashes?

At Falcon Feeds we analysed **1,847+ IOCs** related to stealer activity from **August 20 – September 19, 2025** — hashes, URLs, domains, and IPs — producing a granular picture of operational scale.

Overall Threat Statistics

- **28 distinct malware families** identified.
- **19 active threat actor groups.**
- **156 new variants** (previously unknown samples) — a metric that underscores rapid development and iteration.
- **243 active C2 servers** identified, plus multiple sellers/operators advertising on underground forums — clear evidence of horizontal scaling and commoditisation.

Signature-only defences are increasingly ineffective against this continuously changing fingerprint landscape.

Temporal Analysis

The Pulsating Attack Cycle

What this means

Attackers schedule for victim business hours — detection windows must map to attacker schedules, not attacker local time.

Activity was not steady — it pulsed and spiked: Week 1 (Aug 20–26) baseline **287 IOCs;** Week 2 **354 IOCs** (+23%); Week 3 (Sep 3–9) **498 IOCs** (coinciding with a major RazStealer campaign); Week 4 peaked at **523 IOCs** (driven by the Phoenix Android Botnet).

Two consistent daily windows of peak activity emerged: **02:00–06:00 UTC** and **08:00–11:00 UTC**. These windows align with mid-day hours in Asia-Pacific and morning/mid-day in Europe/Americas respectively — suggesting coordinated, professionalized global operations timed to target business hours for maximum impact.

Geographic Analysis

Regional Hotbeds

IOC counts by region show concentration and tailored threats:

Think Box

Where are your critical assets and user bases located? Are you monitoring region-specific threat families?

Asia-Pacific:
743 IOCs (40.2% of total), +23% activity; primary threats: Mozi, Vidar, FormBook.

Europe:
554 IOCs (30.0%), +15% activity; primary threats: RedLine, XWorm, Agent Tesla.

North America:
369 IOCs (20.0%), stable trend.

South America:
experienced an 8% increase.

This regional concentration implies campaign tailoring — e.g., organizations with heavy European exposure must be especially vigilant against RedLine and XWorm.

Detailed Profiling of Top Stealer Families

Think Box

Which of these families present the highest business risk to your vertical? Do you have tailored detections for crypto-theft and browser data exfiltration?

The most prevalent families by IOC volume are profiled below (counts, targets, TTPs). All figures and IOCs follow our month-long telemetry.

Rank	Stealer Family	IOCs Count	% of Total	Primary Targets
1	FormBook	287	15.5%	Business credentials, emails
2	MassLogger	234	12.7%	FTP, email, browser data
3	XWorm	198	10.7%	System info, keystrokes
4	Agent Tesla	176	9.5%	Corporate credentials
5	Vidar	154	8.3%	Crypto wallets, 2FA
6	RedLine	143	7.7%	Browser data, crypto
7	SalatStealer	98	5.3%	Generic credentials
8	StrelaStealer	87	4.7%	Email clients
9	PureCrypter	76	4.1%	Loader/crypter
10	Valley RAT	65	3.5%	Remote access + stealing

FormBook

The Workhorse of Crimeware-as-a-Service

FormBook emerged as the most active stealer, representing 15.5% of all IOCs observed in the past month. Its reach spans everything from basic corporate logins to highly sensitive patient records, making it one of the most versatile CaaS offerings on the market.

Strategic Takeaway

Attackers are diversifying beyond finance into **healthcare and academia.** Organizations in these sectors must treat data like research and patient records with the same urgency as financial systems.

Prevalence:

287 IOCs (largest share).

Targets:

Business credentials, emails, and healthcare data.

Tactics:

Distributed in bulk through large-scale campaigns.

CaaS footprint:

Widely bought, sold, and reused by numerous actors.

Key IOC:
SHA256 Payload:
1a5bb7485c201a19270ff12961ea08e21ed03ed8d9a9714808909532935d442f

MassLogger

Academia Under Siege

Accounting for **12.7% of IOCs,** MassLogger sets itself apart by going after the education sector. Beyond FTP, browser, and email data, its operators are specifically targeting **research data and student credentials** — a sign that IP theft is expanding into new verticals.

Prevalence:

234 IOCs.

Targets:

FTP, email, browser data, research info.

Sector focus:

Universities and research institutions.

Value driver:

Monetization through stolen intellectual property.

Key IOCs:

- SHA256: da3f6cf27a03bd8e7463774e60dceea1aef6f1001e6450e66c2732c7bed3d092
- MD5: fc8dcd2ca78742d6ba6c9030b53ce7b2
- MD5: cefc4ee7d09b3b98d086064abf2cf84e

XWorm

A Swiss Army Knife for Attackers

Strategic Takeaway

Both XWorm and Agent Tesla highlight that attackers aren't just stealing credentials — they're going after developer pipelines and state-linked data, signalling higher stakes for enterprises and governments.

With **198 IOCs** identified, XWorm is a multifunctional threat designed to harvest **system information, keystrokes, and developer assets like API keys and source code.** Its infrastructure spans multiple countries, making takedowns harder.

Prevalence:

10.7% of total IOCs.

Targets:

Developer systems, APIs, code repositories.

C2 network:

IPs in the US, Netherlands, Germany.

Evasion:

Uses raw paste sites (dpaste) as droppers to mimic legitimate traffic.

Key IOCs:

- IPs: 193[.]124[.]205[.]25:9896, 23[.]227[.]202[.]222:7031, 178[.]16[.]53[.]106:2323, 191[.]101[.]30[.]34:7000
- Dropper URL: https://dpaste[.]org/BNCvw/raw

Agent Tesla

The Persistent Veteran

A long-standing name, **Agent Tesla** remains the fourth most active stealer with **176 IOCs**. It's favoured for corporate credential theft and is increasingly tied to **government employee compromises**. Its longevity shows its developers' commitment to regular updates and evasive delivery.

Prevalence:

9.5% of IOCs.

Targets:

Corporate accounts and government logins.

TTPs:

Consistent updates, mature evasion techniques.

Role:

Trusted tool in both espionage and criminal campaigns.

Key IOC:
SHA256 Main Payload:
a6bd76580c2b907fa0b7dac1abfaeaf4c4e97930bcc8518338de2160cdf10dc2

Vidar
The Crypto Hunter

Strategic Takeaway

The shift toward **crypto and financial theft** is undeniable. RedLine's affordability and Vidar's precision show that both low-level criminals and targeted campaigns now converge on the same prize: your money and digital assets.

Vidar takes aim at **cryptocurrency wallets and 2FA** codes, making up **8.3% of IOCs (154 total).** Its campaigns show global reach, with heavy activity in APAC despite its **EU-based C2 infrastructure.**

Prevalence:

154 IOCs.

Targets:

Crypto wallets, 2FA tokens, banking data.

Infrastructure:

C2 server in Germany; domain ext[.]aztu[.]edu[.]az.

Campaign:

Tagged op74rh.

Key IOCs:
C2 URL: https://ext[.]aztu[.]edu[.]az
C2 IP: 78[.]46[.]230[.]162:443
Campaign: op74rh

RedLine

The Consistent Player

Ranking sixth, **RedLine** remains a staple with **143 IOCs.** Its focus: **browser-stored credentials, cryptocurrency wallets, and banking details**. Underground chatter confirms active developer support, with variants sold for **$150–$500.**

Prevalence:

7.7% of IOCs.

Targets:

Browser credentials, crypto, financial logins.

Marketplace presence:

Regular updates, affordable pricing.

CaaS model:

Maintained like a subscription product.

The Other Top Families

Modular & Multi-Purpose Threats

Strategic Takeaway

Stealers are no longer single-purpose tools. The rise of **multi-function loaders and RATs** means defenders must watch the **entire attack chain**, not just the final payload

Not all threats are simple stealers — some act as **stepping stones for bigger payloads.**

SalatStealer (98 IOCs):

Generic credential theft. SHA256: 6f99cc9a335d32f1ac7e75627df25bf7efda71ce923a48911aa480617b6fe2bd

StrelaStealer (87 IOCs):

Email-specific credentials. SHA256: 3050a5206d0847d5cfa16e79944ce348db688294e311db4d7b6045ffbe337450

PureCrypter (76 IOCs):

Loader/crypter, bypassing defenses to deploy final payloads.

Valley RAT (65 IOCs):

Combines remote access with credential theft. MD5: 2bc7ae7f3215fadffddcefbbb340ce69

These families highlight the **modular evolution** of stealers — initial loaders now pave the way for final payloads, complicating detection and response.

Analysis of Emerging and Trending Threats

Simplified Summary

- **What this means:** Attack surface now includes social/gaming and mobile endpoints — asset inventory must expand.
- **Point to Ponder:** Are social and gaming accounts part of your brand protection posture? Do you have mobile threat defence for employees?
- **Strategic takeaway:** Extend threat intel to consumer platforms and mobile threat defence; include social account protection in security budgets.

New and rising families show a pivot toward social, gaming and mobile targets with faster growth rates:

Stealer	Growth Rate	First Seen	Notes
Trap Stealer 2025	+340%	Sep 18, 2025	WhatsApp, Discord, Steam targeting
Doofi Stealer v2.2	+280%	Sep 14, 2025	Chrome v20 compatible
Phoenix Android Botnet	+420%	Sep 13, 2025	Mobile-focused, 500+ injections
Nexoria Panel	+190%	Sep 10, 2025	Android SMS stealer
RazStealer 2	+150%	Sep 8, 2025	Email/FTP exfiltration

Emerging Stealer Campaigns

Trap Stealer 2025

Social & Gaming in the Crosshairs

With a +340% surge in days, Trap Stealer 2025 shifts focus to WhatsApp, Discord, and Steam — platforms rich in trust, digital assets, and social reach.

Growth:

+340% in less than a week

Targets:

WhatsApp, Discord, Steam

Risks:

Social engineering, brand abuse, virtual asset theft

Phoenix Android Botnet & Nexoria Panel

The Mobile Takeover

The Phoenix Android Botnet (+420%) and Nexoria Panel (+190%) confirm mobile as a prime attack surface. Phoenix's 500+ injections show how attackers exploit phones as the single point of failure for finance and identity.

Phoenix:

+420% growth, 500+ injections

Nexoria:

+190% growth, SMS stealer

Risk driver:

Banking, crypto, and MFA concentrated on mobile

ClearFake Campaign

Fileless & Evasive

Strategic Takeaway

The shift toward crypto and financial theft is undeniable. RedLine's affordability and Vidar's precision show that both low-level criminals and targeted campaigns now converge on the same prize: your money and digital assets.

ClearFake, a JavaScript-based stealer, hides code in images (steganography) and rotates across fast-flux domains — designed to slip past static defences.

Delivery:

Fileless JavaScript

Evasion:

Steganography in images

Infrastructure:

Fast-flux domains (e.g., eg.z-99-l[.]ru)

Detection:

Requires behavioural analysis

Cross-Cutting TTP Analysis and Strategic Insights

Several TTPs recur across families and campaigns:

What this means:

Trusted consumer services and AI obfuscation are now core parts of attacker toolchains.

Strategic takeaway:

Block/monitor high-risk consumer channels from sensitive segments; prioritize behavioral ML that flags abnormal use of trusted services.

The Commoditization of Malware

- **As-a-Service model** dominates: **72% of new stealers** are sold with a panel or builder. Vendors sell "full packages" and FUD variants, lowering the bar for entry and enabling wide distribution. Examples: Paijopulupulu selling Trap Stealer full package for **$500–$1,500**; aviana selling a FUD Doofi Stealer variant for **$300–$800**. Cracked versions of older stealers (e.g., Prynt Stealer) create a secondary market.

Evasion and Anti-Detection

- **FUD variants** are proliferating; **AI-enhanced obfuscation** detected in **12%** of samples. Living-off-the-land uses (PowerShell, WMI) and abuse of legitimate cloud services (GitHub, Pastebin, Discord, ConnectWise, TeamViewer) blend malicious traffic with benign traffic.

Exfiltration and Infrastructure

- **68% of new stealers** use **Telegram** for data transfer — attackers exploit its API and encryption to exfiltrate through trusted consumer channels. This complicates network detection and forensic visibility.

Threat Actor and Underground Market Activity

What this means:

Trusted consumer services and AI obfuscation are now core parts of attacker toolchains.

Strategic takeaway:

Block/monitor high-risk consumer channels from sensitive segments; prioritize behavioral ML that flags abnormal use of trusted services.

The underground market is mature and segmented:

Key vendors:

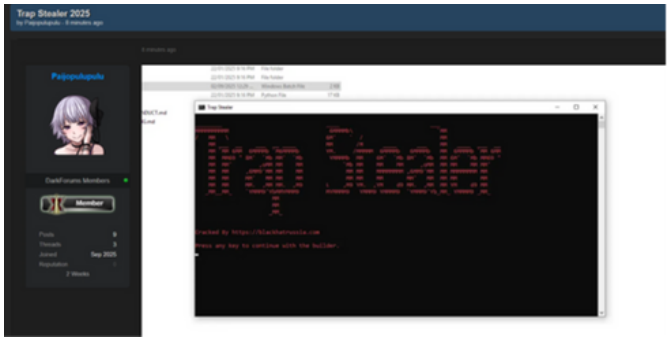
Paijopulupulu (Trap Stealer full package, DarkForums), aviana (Doofi v2.2, DemonForums).

Pricing:

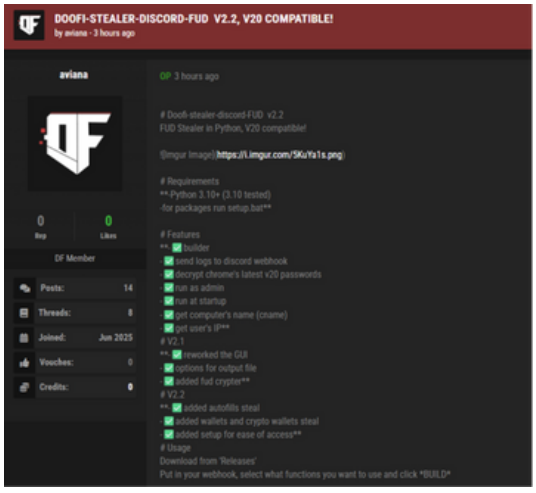
Tools range from **$200 to $2,000+** depending on features, with full packages and FUD versions commanding premiums.

Modes:

Cracked versions and secondary markets broaden access.



Screenshot from dark forums



Screenshot from demon forums

Mitigation and Defensive Recommendations

What this means

A multi-layered approach is mandatory — no single control will stop commoditized stealers.

The landscape demands a strategic shift from reactive to proactive defence:

Implement Behavioural-Based Detection:

Move beyond static signatures to behavioural and ML-driven anomaly detection that can identify stealer behaviours even when static fingerprints change.

Strengthen Application and Network Controls:

Enforce strict application whitelisting; monitor anomalous traffic from trusted services (ConnectWise, GitHub, Discord, cloud tunnels). Adopt zero-trust network policies and audit remote management tools frequently.

Proactive Threat Hunting:

Actively hunt for the IOCs provided (hashes, C2 URLs, IPs) within endpoint and network logs. Maintain a proactive IOC ingestion and hunting cadence.

Enhance Mobile Endpoint Security:

Deploy mobile threat defence that detects mobile-specific malicious behaviour, prevents app injections, and stops unauthorized data exfiltration.

Employee Education:

Expand training to cover social/gaming platform risks and modern social engineering techniques; emphasize credential hygiene across all platforms.

Conclusion

From **August 20 to September 19, 2025,** stealer threats escalated in sophistication and scope. Attackers have moved beyond credential harvesting into a modular, commoditized ecosystem that targets desktop, mobile, and social platforms. New variants like **Trap Stealer 2025** and the **Phoenix Android Botnet** — together with persistent families such as **FormBook, MassLogger, and XWorm** — demonstrate both innovation and resilience in attacker tactics.

Three strategic shifts define the period: the dominance of the As-a-Service model; widespread abuse of legitimate cloud and communication platforms for C2/exfiltration; and a pivot to monetizing non-traditional assets (cryptocurrency wallets, 2FA codes, social accounts). The stealer ecosystem is a critical cybercrime frontier — defeating it requires continuous intelligence sharing, rapid adoption of adaptive defences, and coordinated efforts to disrupt the marketplaces that enable these threats


FalconFeeds
Stay Ahead of Cyber Threats with FalconFeeds.io
FalconFeeds.io delivers real-time intelligence, automates monitoring, and reduces manual effort—helping organizations stay proactive against evolving cyber threats. With seamless integrations and an efficient alerting system, we empower teams to detect, analyze, and respond faster.
Don't just react—stay ahead. Strengthen your defenses with FalconFeeds.io.
Start Your Free 14-Day Trial Today
support@falconfeeds.io
Democratising Cybersecurity
www.falconfeeds.io