VSPAM.ORG · INDEPENDENT RESEARCH

Trends in Spam, Phishing, Spoofing, Malware & DNS Abuse

A monthly research brief on the email, identity, and DNS threat landscape. June 2026 edition — focused on disruption: what law enforcement removed, and what moved in to replace it.

ISSUE	**Volume 2026, Issue 6**
ISSN	**2026-VSPAM-006**
REPORTING PERIOD	1 – 30 June 2026
RELEASED	July 2026
PUBLISHER	vSpam.org Independent Research
LICENSE	Creative Commons Attribution 4.0 (CC BY 4.0)

ABSTRACT

June 2026 was the most consequential month for anti-cybercrime enforcement in several years. **Operation Endgame** (24 June) removed **326 servers and 142 domains** underpinning SocGholish, Amadey, and StealC — the loader and infostealer layer that feeds much of the ransomware economy — recovering **27 million stolen credentials** and restraining **€41 million** in criminal assets. Two weeks earlier Europol dismantled the **AudiA6** laundering service, which had washed **€336 million** since 2021. Yet ransomware volume **rose 9.4% to 707 victims**, leadership changed hands for the first time in five months, and a previously unseen group debuted at number two. This issue examines what disruption actually buys, reports a single-month loader burst visible in the vSpam.org corpus, and documents the complete reversion of May's novelty-gTLD concentration.

Table of Contents

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

Editorial disclosure. This issue was produced with editorial support from DDMARC (ddmarc.com), a DMARC and anti-spoofing platform that is a vSpam.org research partner. DDMARC had no veto over data, citations, or conclusions; competitor products and services are cited on the basis of the underlying data quality. Readers can verify every numeric claim against the references at the back of this report.

Executive Summary

June 2026 belonged to law enforcement. On 24 June, a multinational operation announced under the Operation Endgame banner took down **326 servers and 142 domains** supporting SocGholish, Amadey, and StealC — three families occupying the initial-access and credential-theft layer of the cybercrime supply chain. The action recovered approximately **27 million stolen credentials** and restrained more than **€41 million (roughly $47 million)** in illicit cryptocurrency. Agencies from the United States, United Kingdom, Germany, the Netherlands, Denmark, and Canada participated alongside Microsoft, IBM X-Force, and Bitdefender, with Europol and Eurojust coordinating.[1]

The scale of what was disrupted is best expressed by Microsoft's own telemetry: the targeted families were linked to more than **140,000 infections globally in the first two weeks of May 2026 alone**.[1] Two weeks earlier, on 10 June, Europol dismantled **AudiA6**, a cryptocurrency laundering service that had processed **€336 million** for ransomware operators and cybercrime networks since 2021.[2] Together the two actions hit the supply chain at its entry point and at its exit point in the same month.

The results are instructive, and they are not what a straightforward deterrence model would predict. Four signals define the month:

1. **Ransomware volume rose despite the enforcement action.** BreachSense recorded **707 victims across 63 leak sites in 87 countries**, up 9.4% from May's 646 and reversing the previous month's dip.[3] Endgame landed on 24 June, so most of the month preceded it — but nothing in the final week suggests a collapse either.
2. **Leadership changed hands for the first time in five months.** TheGentlemen posted **94 victims**, displacing Qilin — which had held first place since January and fell to **71**. More striking, a previously unseen group, **DeadLock, debuted directly at number two with 81 victims**.[3]
3. **Command-and-control infrastructure contracted sharply, and its tooling changed.** Spamhaus recorded botnet C&C servers falling **30% to 14,952** across the first half of 2026, with **Sliver overtaking Cobalt Strike** for the top slot — Cobalt Strike detections fell 68%, its largest decline since tracking began.[4]
4. **Our corpus recorded a loader burst with no history and no successor.** A single family label, `luajit-loader`, accounted for **5,059 indicators in June** — absent from our data before the month and gone from the leading families after it. Meanwhile May's novelty-gTLD concentration reverted completely. Section 6.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

FIGURE 1 *The June action targeted the layer beneath ransomware rather than ransomware itself. SocGholish, Amadey, and StealC supply initial access and stolen credentials to operators who then deploy encryption — a structural choice examined in Section 1.2.*

SocGholish's inclusion deserves particular note for readers of this series. Our April issue identified SocGholish — also tracked as FakeUpdates — as one of three loaders accounting for roughly 80% of attributable initial-access engagements. Nine weeks later it was a named target of the largest coordinated takedown of the year. That is a short interval between a family being identified as systemically important and being acted on, and it reflects a maturing of the intelligence-to-enforcement pipeline that deserves more credit than it typically receives.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

Headline Numbers at a Glance

METRIC	VALUE	SOURCE
Servers seized, Operation Endgame	**326**	Europol
Domains taken down, Operation Endgame	**142**	Europol
Stolen credentials recovered	**≈27 million**	Europol
Illicit crypto assets restrained	**€41M (≈$47M)**	Europol
Infections linked to targeted families	**140,000+ (first half of May)**	Microsoft
AudiA6 laundering volume since 2021	**€336 million**	Europol
Ransomware victims posted to leak sites	**707 (63 groups, 87 countries)**	BreachSense
Month-on-month ransomware change	**+9.4% (from 646)**	BreachSense
Most active group	**TheGentlemen, 94**	BreachSense
Highest-ever debut ranking	**DeadLock, 81 (straight to #2)**	BreachSense
Qilin, after five months at #1	**71 (3rd place)**	BreachSense
US share of ransomware victims	**33% (234) — down from 39.3%**	BreachSense
Most-targeted industry	**Healthcare, 54**	BreachSense
Botnet C&C servers observed, H1 2026	**14,952 (–30%)**	Spamhaus
Sliver C&C detections	**3,008 (+58%, now #1)**	Spamhaus
Cobalt Strike C&C detections	**1,110 (–68%, now #4)**	Spamhaus
Malicious domains detected, H1 2026	**2.15 million**	Spamhaus
Growth in botnet C&C domains	**+289%**	Spamhaus
Growth in `.cn` botnet C&C domains	**+771%**	Spamhaus
Abused registrations, PDR registrar	**+901%**	Spamhaus
Vulnerabilities added to CISA KEV in June	**23**	CISA
M3AAWG 67th General Meeting attendance	**280 from 19 countries**	M3AAWG
vSpam.org collector indicators ingested	**28,287**	vSpam.org
vSpam.org single-family loader burst	**5,059 (`luajit-loader`)**	vSpam.org
vSpam.org fake-update cluster change	**3,387 (–64.8% MoM)**	vSpam.org

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

REFERENCE

Methodology and Data Sources

This report consolidates public, attributable data published during or directly referencing June 2026, and reports directly from the vSpam.org collector corpus. The two are kept in separate sections and separately labelled throughout. Every numeric claim drawn from an external source links to a primary or secondary public reference at the back of this report.

Primary external sources for this issue include Europol and Eurojust operational announcements, Spamhaus botnet and domain-reputation reporting, BreachSense ransomware tracking, CISA, ICANN, M3AAWG, NIST, and vendor telemetry from Microsoft, IBM X-Force, and Bitdefender as cited in the Endgame announcement.

Publication window

This issue reports what was publicly knowable in early July 2026. The Q2 platform-level email telemetry and Q2 incident-response trend reports had not been published at the time of writing, and are deliberately not anticipated here. The forward claims made in our May issue concerning post-takedown displacement remain open, and will be scored in the next issue when the Q2 datasets land.

A caution specific to this issue

Enforcement months invite a particular analytical error: attributing every subsequent movement in the data to the enforcement action. Operation Endgame was announced on **24 June**, leaving six days of the reporting period after it. Monthly aggregates for June are therefore overwhelmingly *pre-action* data, and any June-over-May comparison measures something other than the takedown's effect. Where we discuss the action's consequences we restrict ourselves to the final week and label the analysis as provisional. We flag this because we expect a good deal of published commentary over the coming weeks to make precisely this mistake.

vSpam.org corpus scope and limitations

Section 6 reports the **vSpam.org collector corpus**: indicators ingested, normalised, and scored by our automated collection pipeline from cooperating public feeds (URLhaus, ThreatFox, Feodo Tracker). Figures are counted by *first-seen* timestamp within the calendar month and de-duplicated per source and indicator.

As in the May issue, two limitations apply. **Community submission volume was low through this reporting window**, so no community-derived volume claims are made. Malware-family labels are inherited from upstream feed taxonomies which mix true family names with file architectures and behavioural tags; we identify which is which wherever it affects the analysis. All dates are normalised to UTC.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

SECTION 1

Enforcement — Operation Endgame and AudiA6

1.1 What Was Removed

Operation Endgame's June phase, announced on 24 June 2026, was directed at three malware families: **SocGholish**, **Amadey**, and **StealC**. None of them is ransomware. All three sit one layer beneath it, supplying initial access and stolen credentials to the operators who deploy encryption and extortion.[1]

The material outcomes were **326 servers** and **142 domains** removed, **approximately 27 million stolen credentials** recovered, and more than **€41 million** in illicit cryptocurrency identified and restrained. Law enforcement agencies from the United States, United Kingdom, Germany, the Netherlands, Denmark, and Canada participated, with industry contributions from Microsoft, IBM X-Force, and Bitdefender, and operational coordination from Europol and Eurojust.[1]

The credential recovery figure is the one most likely to matter to individual defenders. Those 27 million credentials were, until June, live inventory in an active market. Their recovery converts them from a tradeable asset into a notification list — which is why the practical follow-through for any organisation is to check exposure against the recovered set as notification channels make it available, and to force rotation where matches appear rather than waiting for the credentials to be used.

1.2 The Loader Layer as a Target

Targeting loaders rather than ransomware brands is a deliberate strategic choice, and it is worth being explicit about the theory behind it.

Ransomware groups are, structurally, the most replaceable component of the cybercrime supply chain. A brand can be retired and relaunched in weeks — as the ecosystem has demonstrated repeatedly — because the brand is little more than a leak site, a negotiation process, and an encryptor. The scarce inputs sit upstream: reliable initial access at scale, and validated credentials. Those are what loaders and infostealers supply, and they require infrastructure that is comparatively expensive to rebuild.

SocGholish is the clearest illustration. It operates through compromised legitimate websites that serve fake browser-update prompts — the same fake-update technique documented in our May issue as the dominant behavioural cluster in our own corpus. Its value to the ecosystem is not any particular payload but a durable, large-scale delivery surface built from other people's web properties. That surface takes time and access to reconstitute.

> **THE STRATEGIC LOGIC**
>
> Disrupting a ransomware brand removes a competitor from a market. Disrupting the loader layer removes an input that every competitor in that market depends on. The second is harder to route around, which is why enforcement has increasingly chosen it — and why the right measure of success is the cost and delay imposed on re-entry, not the number of arrests.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

1.3 The Laundering Layer

Two weeks before Endgame, on **10 June 2026**, Europol coordinated the dismantling of **AudiA6**, a cryptocurrency laundering service that had processed **€336 million** on behalf of ransomware groups and cybercrime networks since 2021.[2]

The AudiA6 action is the less-reported of the two and arguably the more strategically interesting. Extortion economics depend on the ability to convert cryptocurrency proceeds into usable funds; a laundering service with a five-year operating history and third-of-a-billion-euro throughput is a piece of shared infrastructure in exactly the way a loader is. Removing it raises the cost of monetisation for every group that used it, without any of those groups being touched directly.

Taken together, June's two operations bracket the supply chain: Endgame at the entry point where access is acquired, AudiA6 at the exit point where proceeds are realised. This is a recognisable strategy — squeeze the parts of the economy that are shared, capital-intensive, and slow to rebuild, and leave the easily-replaced middle alone.

1.4 What Disruption Buys

The honest answer, on the evidence available, is: time and cost, not elimination. Three observations support that assessment.

- **The March precedent.** The Tycoon2FA takedown, examined in our May issue, removed a platform serving at least 2,000 operators across more than 30,000 domains — and CrowdStrike subsequently reported the service persisting in degraded form rather than ceasing.[5] Degradation, not elimination, is the realistic ceiling.
- **June's ransomware numbers moved the wrong way.** Volume rose 9.4% to 707 victims. Six days of post-action data cannot show a takedown effect, but they also give no indication of one beginning.[3]
- **The ecosystem is structurally absorbent.** Sixty-three active groups posted victims in June, and a previously unseen operation debuted directly at number two. A market with that many participants and that low a barrier to entry redistributes displaced demand rather than losing it.

None of this is an argument against enforcement. Twenty-seven million credentials removed from circulation is a concrete reduction in attacker capability; €41 million restrained and a laundering channel that had processed €336 million taken offline are genuine costs imposed. The argument is against the framing that treats takedowns as terminal events. They are recurring costs levied on an adversary that has proven able to absorb them — and the correct defender posture is to treat the weeks following an action as an opportunity window, not as a resolution.

> **KEY TAKEAWAY**
>
> Measure enforcement by the cost and delay it imposes on re-entry, not by whether the activity stops. On that measure June was a strong month. On the elimination measure — the one most headlines implicitly use — it will look like a failure within a quarter, and that judgement will be wrong.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

1.5 What Defenders Should Do in the Window

The period immediately following a supply-chain disruption has properties worth exploiting. Displaced operators rebuild with unfamiliar tooling, on new infrastructure, often with degraded operational security. Detection that would ordinarily be lost in the noise becomes viable. Four actions are worth prioritising over the next several weeks:

1. **Hunt for the removed families retrospectively.** SocGholish, Amadey, and StealC indicators published alongside the operation cover infrastructure that was live until 24 June. Any historical match in your telemetry is a compromise you did not detect at the time, and the credential consequences persist regardless of whether the infrastructure is now down.
2. **Force rotation against the recovered credential set.** Twenty-seven million credentials were recovered. Where notification reaches you, treat a match as a confirmed exposure rather than as a possible one.
3. **Expect new tooling, and lower detection thresholds accordingly.** Operators rebuilding on unfamiliar frameworks generate atypical traffic. The Sliver displacement documented in Section 3 is precisely this phenomenon at the C2 layer.
4. **Re-baseline fake-update detection specifically.** SocGholish's delivery model depends on compromised legitimate sites. That surface does not disappear when the operator's servers do; it becomes available to whoever rebuilds on it next.

1.6 A Note on Attribution Discipline

One methodological point deserves emphasis before the data sections. In the weeks after a major action, published analysis reliably attributes unrelated movements in threat data to the takedown. June is unusually exposed to this error because the action landed on the 24th, leaving six days in the reporting period.

Any claim that June's aggregate figures show an Endgame effect is arithmetically unsupportable: 80% of the month preceded the action. We restrict our own post-action analysis to the final week, we label it provisional, and we note explicitly in Section 6.4 that the one anomaly we observe in that week is at least as likely to be a collection artefact as a takedown consequence.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

SECTION 2

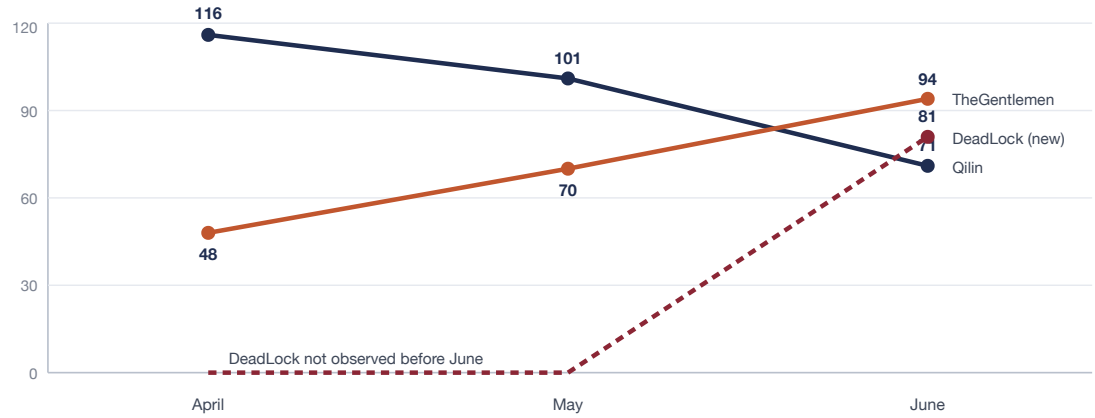
Malware and Ransomware

2.1 Volume Rebound and Leadership Change

BreachSense recorded **707 victims posted across 63 active leak sites** in June 2026, spanning **87 countries** — a **9.4% increase** over May's 646 and a reversal of the previous month's decline.[3] The country count is itself notable: 87 against May's 73, the widest geographic spread of the year so far.

Leadership Change — Top Ransomware Operations, April to June 2026

TheGentlemen overtook Qilin after five months; DeadLock debuted directly at second place



April figures are approximate as published; May and June are exact counts.

Source: BreachSense monthly ransomware reports, April, May and June 2026.

FIGURE 2 *Qilin's five-month run at the top ended in June. The crossing itself is unremarkable; the dashed line is not — an operation with no prior observed activity posting 81 victims in its first month.*

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

2.2 The DeadLock Debut

An operation with no observed prior activity posting **81 victims in its first month** — enough for second place outright — is not a new entrant in any meaningful sense. New operations do not acquire eighty victims from a standing start. What they acquire is a backlog.

Three explanations are consistent with the pattern, and they are not mutually exclusive:

- **Rebrand.** An existing operation relaunching under a new name, publishing accumulated victims to establish immediate credibility. This is the most common explanation historically and generally the correct one.
- **Affiliate migration.** Affiliates displaced from a disrupted or distrusted programme moving en masse and bringing in-progress engagements with them. May's data — three simultaneous first-time entries in the top ten — indicated exactly this kind of movement already underway.
- **Backlog publication.** Victims compromised over preceding months and published in a single batch to maximise the announcement's impact.

The practical consequence is the same under all three: **leak-site postings measure publication events, not compromise events**, and the gap between them can be months. A defender treating monthly victim counts as a proxy for current attack rates is reading a lagging, batch-published indicator as though it were real-time telemetry.

2.3 Geographic Redistribution

June's geographic distribution shifted materially. The United States accounted for **234 victims, 33% of the total**, down from 39.3% in May — while the absolute count fell only from 254 to 234.[3] The share moved primarily because the rest of the world grew, not because US targeting contracted.

COUNTRY	JUNE	MAY	CHANGE
United States	**234**	254	−20
Germany	**38**	29	+9
Italy	**30**	19	+11
Canada	**29**	31	−2
India	**28**	11	+17

India's rise from 11 to 28 is the sharpest proportional move, and Italy's from 19 to 30 the second. Combined with the jump from 73 to 87 countries represented, the picture is of operations widening their target aperture rather than intensifying against existing markets. Healthcare returned to the most-targeted position with 54 victims, with manufacturing second at 49 — an exact inversion of May's ordering.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

2.4 Reading Volume Against Enforcement

It is worth stating plainly what June's ransomware numbers can and cannot tell us about Operation Endgame, because the temptation to connect them will be considerable.

They cannot tell us anything. The action landed on 24 June; the reporting period ends on the 30th. Even setting aside the publication lag documented in Section 2.2 — which places the compromise dates behind many June postings somewhere in April or May — six days is not a sample. The 9.4% rise is a fact about May-to-June activity, and the takedown is a fact about the last week of June. Joining them is a narrative choice, not an inference.

What the numbers do tell us is about the state of the market *into which* the takedown landed: 63 active operations, a new entrant capable of posting 81 victims immediately, a widening geographic aperture, and leadership turnover after five months of stability. That is a liquid, competitive, absorbent market. It is the environment that determines how quickly the removed capacity gets replaced, and it is considerably more informative than the headline count.

> **KEY TAKEAWAY**
>
> Leak-site postings are a publication metric with a lag of weeks to months. They are a poor proxy for current attack rates and a worse one for the short-term effect of an enforcement action. The useful signals in June's data are structural — group count, entry velocity, geographic spread — not volumetric.

We will revisit the Endgame effect in the August issue, when July's full month of post-action data is available and the Q2 incident-response reporting has published. That is the first point at which the question becomes answerable, and we will report the answer whether or not it supports the assessment offered in Section 1.4.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

SECTION 3

Command-and-Control Infrastructure

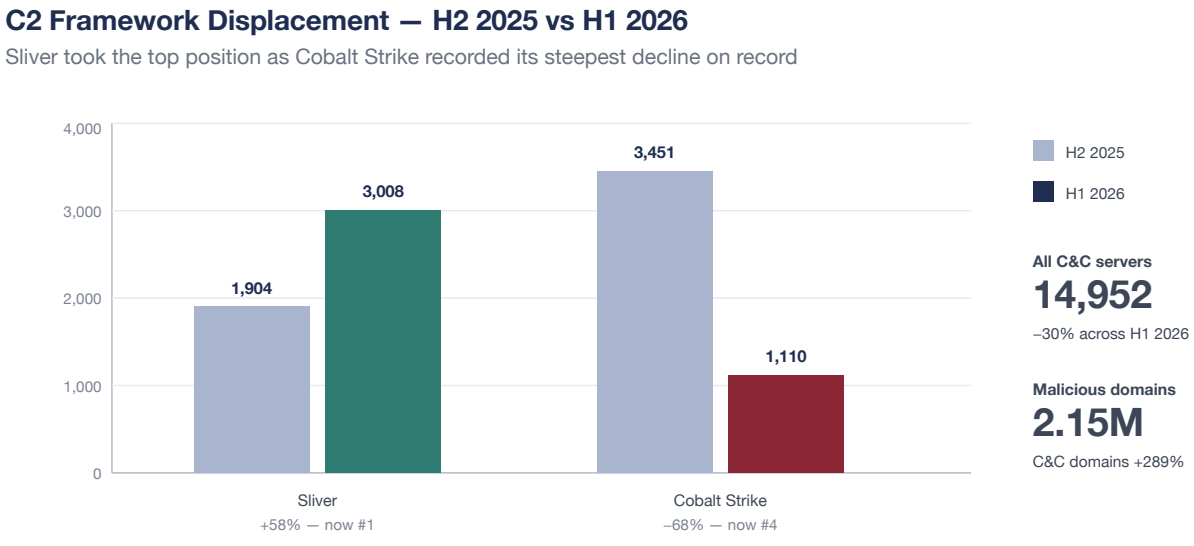
Spamhaus published its half-year botnet threat update on 10 July, covering January to June 2026. It is the most consequential infrastructure dataset of the period, and it documents both a contraction in volume and a change in tooling.[4]

3.1 The Contraction

Botnet command-and-control servers observed fell **30% to 14,952** across the first half of 2026. A drop of that size in six months is unusual, and it is consistent with a period of sustained enforcement pressure — the Tycoon2FA action in March and the Endgame phase in June both removed hosting infrastructure at scale.

The domain-side picture runs the other way, and the contrast matters. **2.15 million malicious domains** were detected over the same period, with domains associated with botnet C&C up **289%** and malware-associated domains up **206%.**[4] Fewer servers, far more domains: operators are fronting a contracting server estate with a rapidly expanding domain layer, which is exactly the behaviour one expects when the servers are the scarce, targeted asset and the domains are cheap and disposable. It also corroborates, from an independent corpus, the bulk-registration pattern we documented in our May issue.

3.2 Sliver Displaces Cobalt Strike



Source: Spamhaus Botnet Threat Update, January to June 2026 (published 10 July 2026).

FIGURE 3 *Cobalt Strike's 68% fall is the largest percentage decline Spamhaus has recorded for it since tracking began. The server estate contracted 30% overall while the malicious domain layer expanded sharply.*

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

Cobalt Strike has been the default post-exploitation framework in criminal use for the better part of a decade. Its detections falling from 3,451 to 1,110 — a **68% decline**, dropping it from first place to fourth — is the most significant change in the C2 landscape in years, and it has a straightforward explanation: sustained pressure on cracked-licence distribution combined with detection coverage so mature that using Cobalt Strike is now a liability rather than an advantage.

Sliver, an open-source adversary-emulation framework, absorbed the displaced demand, rising 58% from 1,904 to **3,008 detections** and taking the top position.[4] The migration is entirely rational from the attacker's side: Sliver is free, actively maintained, cross-platform, and — critically — carries substantially less mature detection coverage in most defensive estates precisely because it has been less common.

> **DETECTION IMPLICATION**
>
> Estates whose C2 detection was tuned primarily against Cobalt Strike beaconing are now optimised against the fourth-most-common framework. Sliver detection coverage — session establishment patterns, mTLS and WireGuard transport behaviour, its distinctive HTTP implant traffic — is the highest-leverage detection-engineering investment available this quarter.

3.3 Registrar and ccTLD Concentration

The domain-layer figures show extreme concentration in where abuse is registered, and both the increases and the decrease are informative:

LOCUS	CHANGE, H1 2026	READING
`.cn` botnet C&C domains	+771%	Concentration into a single ccTLD at scale
PDR (India) abused registrations	+901%	A single registrar absorbing bulk abuse volume
REGRU abused registrations	–90%	Demonstrates the problem is tractable when addressed
Botnet C&C domains, all	+289%	Domain layer expanding as server estate contracts
Malware-associated domains	+206%	Same pattern in the distribution layer

The REGRU figure is the most important number in this table and the least likely to be quoted. A **90% reduction** at a single registrar, over six months, in the same period that two other loci grew by several hundred per cent, establishes that registrar-level abuse volume is a policy variable rather than an environmental constant. Registrars that invest in verification at registration reduce their abuse burden dramatically. Those that do not become concentration points. There is no third outcome visible in this data.

This connects directly to ICANN's tightened contractual regime discussed in our May issue. The 2026 registry agreements mandate automated abuse detection and contractual response windows. Spamhaus's data suggests the mandate is well-founded — and that the gap between best and worst performers is measured in orders of magnitude, not percentages.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

SECTION 4

Email Authentication and Spoofing

4.1 The Mid-Year Position

No major new adoption dataset published in June; the benchmark remains EasyDMARC's 2026 report covering 1.8 million domains, treated in detail in our May issue. Continuous-measurement sources tracking a wider corpus give a consistent, and slightly bleaker, mid-year picture: of approximately **5.5 million domains** measured, **12.8% — about 702,000 — publish an enforcing policy**, split roughly evenly between `p=reject` (6.0%) and `p=quarantine` (6.8%).[6]

The difference from the EasyDMARC figures is a corpus effect, not a contradiction. EasyDMARC measures the top 1.8 million domains — a population skewed toward organisations with the resources to run a messaging programme. Widening the corpus to 5.5 million pulls in the long tail, where enforcement rates are far lower. Both numbers are correct about their respective populations, and the gap between them *is* the finding: DMARC enforcement correlates strongly with organisational scale.

4.2 What June's Enforcement Actions Change

The 27 million credentials recovered in Operation Endgame have a direct bearing on authentication posture, and the connection is worth drawing out explicitly.

Every one of those credentials, while circulating, was a potential route to an *authenticated* sending position — a real mailbox, on a real domain, capable of passing SPF, DKIM, and DMARC cleanly. This is the mechanism behind supplier email compromise constituting 61% of BEC, documented in our May issue. Credential theft and email authentication are not separate problem domains; the first is the standard method of defeating the second.

> **KEY TAKEAWAY**
>
> A perfectly configured `p=reject` policy provides no protection whatsoever against mail sent from a genuine account whose credentials were stolen. Email authentication and credential hygiene are the same control surface viewed from two directions, and an organisation strong on one and weak on the other is not defended.

4.3 Practical Guidance

- **Pair DMARC enforcement with mandatory phishing-resistant MFA on every sending identity.** Enforcement stops forgery; only device-bound authentication stops the authenticated-compromise case.
- **Monitor aggregate reports for legitimate-but-unexpected sources.** A sending source that authenticates correctly but has no business reason to exist is the signature of a compromised account or an unsanctioned integration, and it is visible in RUA data before it is visible anywhere else.
- **Treat the recovered-credential notifications as an authentication event.** A match means a sending identity you own may have been operable by a third party. Rotate, then review what was sent.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

SECTION 5

Major Incidents — June 2026

DATE	ORGANISATION	NATURE	REPORTED SCALE
15 Jun	**AssuranceAmerica**	Insurance data compromise; file review completed	6,998,886 individuals
17–23 Jun	**KDDI**	Email platform breach serving six Japanese ISPs	Up to 14.22M addresses and passwords
18 Jun	**Texas Parks & Wildlife**	Third-party licensing vendor compromise	3M+ licence customers
15 Jun	**Kodak**	Data theft claimed by ShinyHunters	2.2M customer and corporate records *(actor claim)*
Jun	**DentaQuest**	Dental benefits data published by ShinyHunters	234 GB archive *(actor claim)*

5.1 KDDI — the Highest-Consequence Incident of the Month

KDDI detected unauthorised access on **17 June** and disclosed on **23 June**. The affected system was an email platform KDDI provides to **six Japanese internet service providers**, with up to **14.22 million email addresses and passwords** exposed.[7]

This is the month's most consequential incident and it received a fraction of the attention given to larger nominal record counts. The reason is structural. The exposure is not a customer list; it is **credential pairs for consumer mailboxes** — and a consumer mailbox is the recovery address for that person's banking, government, and commercial accounts. An email address plus password is not a data point about someone. It is, for as long as it remains valid, operational control of their online identity.

Compounding this, the platform was operated *on behalf of six other providers*. The subscribers affected had no relationship with KDDI and no reason to associate a KDDI breach notice with their own accounts. Platform concentration in consumer email means a single operational failure propagates across provider boundaries into populations that cannot reasonably self-identify as affected.

> READ THIS AGAINST SECTION 1
>
> In the same month that Operation Endgame recovered 27 million stolen credentials from circulation, a single platform incident placed up to 14.22 million credential pairs into it. The two figures are the same order of magnitude. Enforcement removes inventory; operational failures replenish it — and the replenishment requires no criminal infrastructure at all.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

5.2 AssuranceAmerica — the Detection-to-Notification Gap

AssuranceAmerica, an auto and renters insurance provider, detected suspicious activity on **17 March 2026** and completed its file review on **15 June**, disclosing that **6,998,886 individuals** were affected. Exposed data included names, contact information, policy details, and **driver's licence numbers**.[8]

The interval between detection and notification is approximately **ninety days**. That is not negligence — determining precisely which records were accessed in an unstructured document store genuinely takes months — but it means seven million people were exposed for a quarter of a year without the information needed to protect themselves. Driver's licence numbers are particularly consequential because, unlike a password, they cannot be rotated.

5.3 The Third-Party Pattern, Again

The Texas Parks & Wildlife incident, disclosed **18 June** after Texas Cyber Command detected unauthorised access, involved a **third-party licensing vendor** rather than the agency's own systems. More than **3 million** licence customers may have been affected, with exposed data including driver's licence information, passport numbers, email addresses, phone numbers, and residential addresses.[9]

This is the fourth consecutive month in which the largest incidents traced to a party other than the named victim: April's headline breaches ran through contractors and OAuth-connected applications, May's through a platform provider, and June's through a licensing vendor and a white-label email platform. The pattern is now sufficiently consistent that it should be treated as the base case rather than as a recurring observation.

> **THE COMMON THREAD**
>
> Four months, and in each one the organisation that was compromised was not the organisation whose customers were exposed. Third-party risk assessment that stops at contract signature is measuring the wrong thing at the wrong time; what matters is which suppliers hold credential-grade data about your users, and what their detection-to-notification interval actually looks like in practice.

One reporting note. The Kodak and DentaQuest figures in the table above originate with ShinyHunters, not with the affected organisations, and are marked as actor claims accordingly. As set out in our May issue, actor-supplied record counts are systematically inflated and should not be aggregated into industry statistics as though they were measurements.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

SECTION 6

vSpam Researcher Team Analysis

6.1 Corpus and Scope

28,287
INDICATORS FIRST SEEN IN JUNE

514
DISTINCT FAMILY / TAG LABELS

5,059
SINGLE-FAMILY BURST, ONE MONTH ONLY

–64.8%
FAKE-UPDATE CLUSTER, MONTH ON MONTH

The vSpam.org collector ingested **28,287 indicators** by first-seen timestamp in June — 28,073 from URLhaus and 214 from ThreatFox — a 5.8% decline from May's 30,039.[13] The label diversity moved the other way: **514 distinct family and tag labels** against May's 450, the widest of the year.

That combination — slightly less volume spread across meaningfully more labels — is the quantitative signature of a fragmenting ecosystem, and it echoes what Section 2 observed in the ransomware leak-site data over exactly the same period. Two unrelated corpora, measuring different layers of the criminal economy, showing the same structural movement in the same month is worth flagging as a genuine convergence rather than a coincidence.

INDICATOR TYPE	CLASSIFICATION	JUNE 2026	MAY 2026
URL	Malware distribution	**21,837**	20,801
Domain	Malware distribution	**6,236**	9,055
IP	Botnet command & control	**155**	155
Domain	Payload delivery	**34**	9
URL	Botnet command & control	**12**	8
Domain	Botnet command & control	**11**	11

The composition shift is the notable part. URL-type malware distribution rose 5.0% while **domain-type fell 31.1%**, taking the URL-to-domain ratio from roughly 2.3:1 in May to **3.5:1 in June**. Command-and-control indicators held almost exactly constant at 178 against May's 174 — the stability of that baseline across two months, against substantial movement everywhere else, is itself informative.

> **SCOPE STATEMENT**
>
> As in the May issue: community submission volume was low through this window, so nothing here derives from community reporting. Family labels are inherited from upstream feed taxonomies which mix true family names with file architectures and behavioural tags. Where a label below is an architecture or behavioural tag rather than a family attribution, we say so.

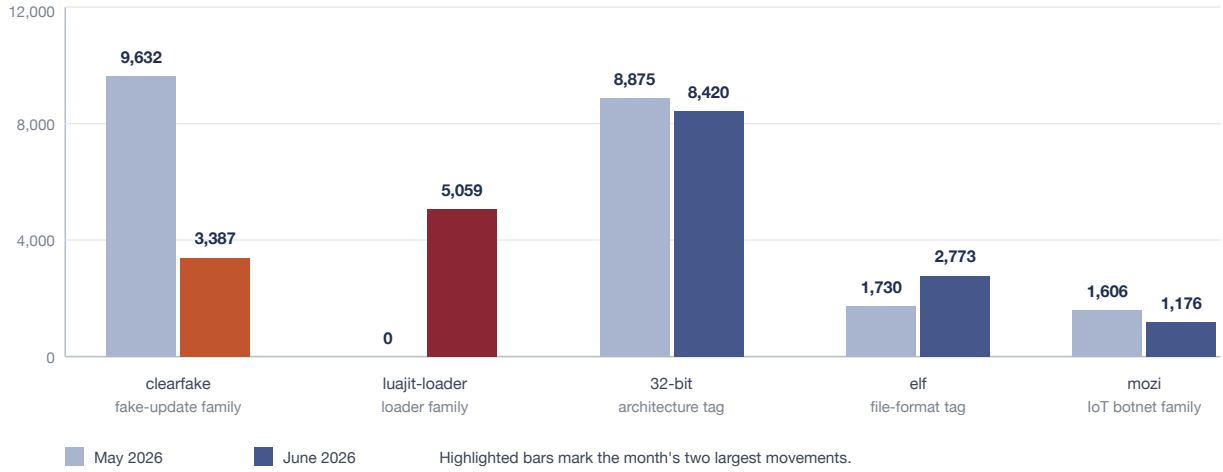
ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

6.2 The Single-Month Loader Burst

June's family distribution contains the most abrupt single-label movement we have recorded. A loader label, `luajit-loader`, accounted for **5,059 indicators** — 17.9% of the entire month's corpus and its second-largest label overall. It does not appear in May's leading families at all, and it is absent from July's.

Family Label Composition — May vs June 2026

vSpam.org collector; a loader burst arrives as the fake-update cluster contracts



Source: vSpam.org collector corpus, indicators by upstream family label, first-seen timestamp, May and June 2026.

FIGURE 4 *Two large movements in opposite directions. The fake-update cluster fell 64.8% while a loader label absent from the previous month arrived at 5,059 indicators. Architecture and file-format tags — included for scale — barely moved.*

The magnitude is worth restating: a label that did not exist in our corpus one month earlier became its second-largest the next, then vanished again. Nothing in the surrounding data — total volume, indicator-type mix, or the command-and-control baseline — moved comparably. The corpus absorbed a campaign roughly the size of a fifth of its monthly output without otherwise changing shape.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

Figure 4 deliberately includes `32-bit` and `elf` alongside the true family labels. Those are architecture and file-format tags, not families, and their near-stability across the two months — 8,875 to 8,420, and 1,730 to 2,773 — provides the control against which the family-label movements should be read. The corpus itself did not change character; two specific operations within it did.

A label reaching 17.9% of a month's corpus with nothing before it and nothing after it describes a discrete campaign, not a trend. Our reading is that a single operator ran a concentrated distribution push through June using a distinctive loader, and either ceased or changed tooling at the month's end. That is worth stating carefully: we observe the distribution infrastructure, not the operator, and we make no attribution claim.

The simultaneity with the fake-update contraction is the more interesting question. ClearFake fell 64.8% in the same month a new loader took 17.9% of the corpus. That is consistent with operators rotating delivery tooling — but it is equally consistent with two unrelated operations whose schedules happened to coincide. We do not have the evidence to distinguish these, and we note the alternative because the first reading is the more attractive one and attractiveness is not evidence.

6.3 The gTLD Reversion

Our May issue[14] documented **3,459 domain indicators — 38.1% of that month's domain corpus — concentrated in four novelty gTLDs**: `.lat`, `.surf`, `.pics`, and `.garden`. We characterised it as a bulk-registration event rather than organic distribution, and predicted it would not persist.

June's data settles the question.

MAY 2026 — TOP TLDS	INDICATORS	JUNE 2026 — TOP TLDS	INDICATORS
`.lat`	**1,718**	`.com`	**685**
`.surf`	**847**	`.xyz`	**443**
`.pics`	**600**	`.bet`	**148**
`.garden`	**294**	`.shop`	**116**
`.hu`	**213**	`.app`	**82**
`.com`	**172**	`.casino`	**78**

The four-TLD cluster vanished entirely from the leading positions. `.com` moved from sixth place with 172 indicators to first with 685, and the remainder of the distribution flattened into a conventional mix — legacy generics, `.xyz`, and a gambling-adjacent tail (`.bet`, `.casino`) that also appears in July.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

FORECAST SCORED

Our May issue predicted the novelty-gTLD concentration would prove to be a discrete bulk-registration event rather than a durable shift. June's data confirms it: the four-TLD cluster is gone and `.com` leads with four times May's count. We record this as a correct call, and note the more useful implication — that a defender who had built TLD-based blocking rules from May's data would have spent June blocking a distribution that no longer existed.

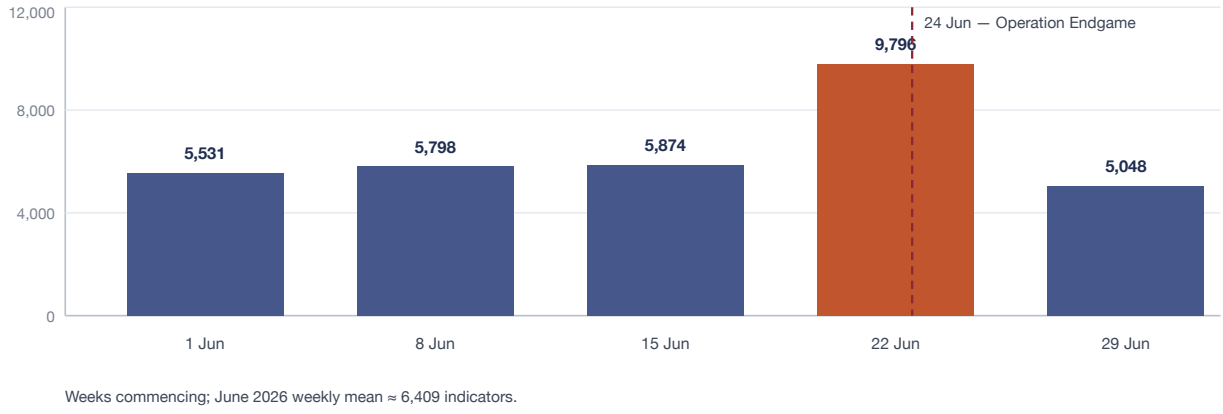
That last point generalises beyond this case. Reputation systems keyed to TLD are keyed to the most volatile attribute in the domain namespace, because TLD choice is a pure cost decision that operators revisit whenever pricing or scrutiny changes. Registration *behaviour* — velocity, registrant fingerprinting, nameserver assignment patterns — is durable in a way that TLD is not, which is why Section 3.3's REGRU result matters: verification at registration addressed the behaviour, and the abuse fell 90%.

6.4 Reading the Endgame Week

One anomaly in June's weekly data requires careful handling. The week commencing **22 June** — which contains the Operation Endgame announcement on the 24th — recorded **9,796 indicators** — **76% above the mean of June's other four weeks** (5,563), which ranged only from 5,048 to 5,874. It is also the week in which the fake-update cluster fell to its lowest point of the month, 335.

Weekly Ingestion — June 2026

Total indicators ingested, with the Operation Endgame announcement marked



Source: vSpam.org collector corpus, total indicators by first-seen timestamp, weeks commencing 1–29 June 2026.

FIGURE 5 *A 76% excursion above the month's other weeks, coinciding with the Endgame announcement. The correlation is real; the causal reading is not established, for the reasons set out opposite.*

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

It would be easy, and probably well received, to present Figure 5 as our corpus detecting the takedown. We are not going to do that, because at least three explanations fit the data and we cannot distinguish between them:

1. **Disclosure cascade.** Coordinated actions are accompanied by indicator publication from the participating parties. Upstream feeds ingest those indicators, and our collector ingests the feeds. On this reading the spike is *reporting* about infrastructure, much of which had been live for months.
2. **Operator flight.** Operators sensing exposure rotate infrastructure rapidly, generating genuinely new indicators in a compressed window. This would be a real behavioural signal.
3. **Coincidence.** Our weekly series shows a comparable excursion in the week commencing 4 May, with no corresponding enforcement event. Bursts of this magnitude occur in this corpus without external cause.

Explanation one is the most probable on prior grounds, and it is the least interesting. The honest position is that **a single week is not evidence**, and that the correlation is reported here because concealing it would be worse than reporting it with appropriate caveats.

> **RESEARCHER TEAM ASSESSMENT**
>
> June's corpus shows a fragmenting ecosystem — more labels across slightly less volume — with campaign-scale movement in individual families and a stable command-and-control baseline. The domain layer continues to churn: May's novelty-gTLD event reverted completely within a month. Our overall reading is that the infrastructure layer is becoming more disposable and more diverse simultaneously, which degrades every defensive approach that depends on the durability of a specific indicator.

6.5 What We Will Be Watching

Three questions carry into July, and we commit to reporting on each regardless of what the data shows:

- Whether `luajit-loader` reappears, which would reclassify June's burst from a discrete campaign to an intermittent operation.
- Whether the fake-update cluster continues declining or recovers — the direct test of whether SocGholish's removal displaced the technique or merely one operator of it.
- Whether the URL-to-domain ratio continues rising past 3.5:1, which would confirm the domain layer's decline as the meaningful unit of malicious infrastructure.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

SECTION 7

Cross-Cutting Analysis — The Economics of Disruption

June offers an unusually clean opportunity to think about what disruption does, because two major actions landed in the same month and because a third — Tycoon2FA in March — is now far enough behind us to have generated observable aftermath.

7.1 Three Actions, One Pattern

ACTION	DATE	LAYER TARGETED	OBSERVED AFTERMATH
Tycoon2FA	March 2026	Phishing-as-a-service platform	Platform persists in degraded form; 330 domains seized
AudiA6	10 June 2026	Cryptocurrency laundering	€336M service dismantled; too recent to assess
Operation Endgame	24 June 2026	Loaders and infostealers	Too recent to assess; six days of in-period data

The pattern across all three is a shift away from targeting the visible, brand-bearing end of the criminal economy and toward the shared infrastructure it depends on. None of these actions targeted a ransomware group. All three targeted something that ransomware groups *buy*: credential-phishing capability, laundering capacity, initial access.

7.2 Why Shared Infrastructure Is the Right Target

The economic argument is straightforward. Criminal markets exhibit specialisation, and specialised suppliers serve many customers. Removing one ransomware brand removes one buyer from that market; removing a loader operation removes a supplier that many buyers depend on, forcing all of them to pay switching costs simultaneously.

Two properties of shared infrastructure make it attractive as a target. It is **capital-intensive** — SocGholish's compromised-website estate took time and access to assemble — and it is **trust-dependent**, since criminal customers must believe a service will not defraud or expose them. Seizure damages the first directly; the publicity around seizure damages the second, sometimes more durably. A laundering service whose operators have been arrested is not merely offline; it is a service no rational customer will return to.

7.3 The Limits, Stated Plainly

Against that, the evidence for absorption is strong. Tycoon2FA persists post-takedown. Ransomware volume rose 9.4% in the month of Endgame. A previously unseen group posted 81 victims. Sixty-three operations remain active. And the KDDI incident placed up to 14.22 million credential pairs into circulation in the same month that enforcement removed 27 million — replenishment through ordinary operational failure, requiring no criminal infrastructure at all.

> **THE SYNTHESIS**
>
> Disruption is a recurring tax on criminal operations, not a terminal event. It raises costs, imposes delay, destroys accumulated trust, and — in Endgame's case — removes 27 million credentials from circulation. It does not reduce the number of organisations attacked next month. Both halves of that statement need to be held simultaneously, and most published commentary holds only one.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

7.4 What Displacement Looks Like in the Data

Three displacement signals are visible this month, at three different layers, and together they describe the mechanism by which an ecosystem absorbs pressure.

- **At the tooling layer:** Cobalt Strike detections fell 68% while Sliver rose 58% to take the top position.[4] Operators did not stop using C2 frameworks; they moved to one with less mature detection coverage.
- **At the infrastructure layer:** C&C servers fell 30% while malicious domains reached 2.15 million with C&C domains up 289%.[4] The expensive, targetable asset contracted; the cheap, disposable one expanded to compensate.
- **At the operator layer:** Qilin fell from 116 to 71 victims across three months while TheGentlemen rose from 48 to 94 and DeadLock arrived at 81.[3] Capacity redistributed between operations rather than leaving the market.

In each case the aggregate activity level is roughly preserved while its composition changes completely. This is what a resilient system looks like under pressure, and it explains why volumetric metrics are such poor measures of enforcement success. The right question is not "did activity fall" but "what did it cost them to keep it constant" — and the answer to that is visible in the composition changes above, not in the totals.

7.5 Implications for Defenders

1. **Detection coverage should follow displacement, not volume.** The Sliver migration is the clearest actionable finding of the month. Coverage tuned against Cobalt Strike is now aimed at the fourth-most-common framework.
2. **Expect composition change, not volume change, after enforcement.** Plan for new tooling on new infrastructure rather than for a lull.
3. **Exploit the transition window.** Operators rebuilding on unfamiliar tooling make mistakes that are detectable for a limited period. The weeks following a major action are the cheapest detection opportunity available.
4. **Fix the replenishment side.** Enforcement removed 27 million credentials in June; one platform incident supplied up to 14.22 million. Credential hygiene, MFA coverage, and platform concentration risk determine how fast the removed inventory is replaced — and those are defender-side variables, not law-enforcement ones.

SECTION 8

Standards and Regulatory Developments

8.1 M3AAWG 67th General Meeting — Montréal, 8–11 June

M3AAWG held its 67th General Meeting in Montréal from 8 to 11 June 2026, drawing **280 attendees from 19 countries**, of whom **58 were attending for the first time**. The meeting produced **eight proposed outcomes** through its Outcomes and Recommendations Track, with all four Priority Committees convening in person to set roadmaps against the abuse challenges ahead.[10]

The new-attendee proportion — better than one in five — is the number worth noting. An anti-abuse community that is one-fifth new arrivals at a given meeting is one that is recruiting faster than it is losing people, which has not consistently been true of this field. M3AAWG's own summary characterises the week as marked by urgency across AI-driven messaging abuse, identity, and online safety.

For messaging operators the practical significance of M3AAWG lies in its best-practice documents, which materially shape what large mailbox providers require of senders. Operators should track the eight proposed outcomes as they are formalised; historically, M3AAWG recommendations precede mailbox-provider policy changes by roughly two to four quarters.

8.2 CISA

CISA added **23 vulnerabilities** to the Known Exploited Vulnerabilities catalogue during June 2026, with CVSS scores ranging from 5.8 to 10.0 and the majority above 7.5.[11] Affected products spanned remote-access, network-management, and enterprise-application software — including SimpleHelp, Cisco Unified Communications Manager and Catalyst SD-WAN Manager, Ubiquiti UniFi OS, Splunk Enterprise, Oracle PeopleSoft, Ivanti Sentry, Google Chrome, Check Point Security Gateway, SolarWinds Serv-U, and the Linux kernel.

Federal remediation obligations follow from Binding Operational Directive 26-04. The concentration in remote-access and management tooling is consistent with the initial-access economy described throughout this issue: the products being exploited are the ones that grant broad administrative reach once compromised.

8.3 ICANN

No new ICANN policy milestone fell in June. The contractual regime described in our May issue — two years of DNS Abuse enforcement, nearly 530 investigations with roughly two-thirds resulting in remedial action, and the tightened 2026 gTLD round obligations — remains the operative framework.[12] Spamhaus's registrar-level findings in Section 3.3 provide the first substantial independent evidence of how unevenly that framework is being applied in practice.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

SECTION 9

Outlook and Recommendations

9.1 Forecast (July – September 2026)

1. **Ransomware volume will continue rising through Q3, not fall.** Endgame targeted the access layer, and access-layer disruption takes one to two quarters to propagate into extortion volume — if it propagates at all. We expect July and August above 700 victims.
2. **Sliver's share will keep growing.** The framework migration is early and self-reinforcing: as detection coverage remains weaker than Cobalt Strike's, the incentive to switch strengthens. We expect Sliver to hold first position through H2 2026.
3. **A SocGholish successor will emerge within one to two quarters.** The fake-update delivery surface — compromised legitimate websites — was not removed by the takedown; only the operator's infrastructure was. That surface remains available to whoever rebuilds on it.
4. **Q2 telemetry will show a large Tycoon2FA step change with partial recovery.** We restate the forecast made in our May issue so that it can be scored against the Q2 datasets due later this month.
5. **Credential-exposure incidents will continue outpacing credential recovery.** June's arithmetic — 27 million recovered, up to 14.22 million exposed in a single incident — is not favourable, and nothing in the current trajectory changes it.

9.2 Recommendations — Messaging Operators and ISPs

- **Treat platform concentration as systemic risk.** KDDI's breach propagated across six ISPs whose subscribers had no relationship with KDDI. Operators reselling or white-labelling mail platforms should ensure their incident-communication path reaches end subscribers directly, because those subscribers will not connect a supplier's breach notice to their own account.
- **Force rotation against recovered credential sets.** Twenty-seven million credentials re-entered defender hands in June. Where notification reaches you, treat a match as confirmed exposure.
- **Score registrar reputation, not just domain reputation.** Spamhaus's data shows a 901% abuse increase at one registrar and a 90% decrease at another over the same six months. Registrar-level signal is stable in a way TLD-level signal demonstrably is not.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

9.3 Recommendations — Enterprise Defenders

— **Build Sliver detection coverage now.** This is the highest-leverage detection-engineering investment of the quarter. Session establishment patterns, mTLS and WireGuard transport behaviour, and implant HTTP traffic characteristics are the places to start.

— **Hunt retrospectively for SocGholish, Amadey, and StealC.** Indicators published alongside Operation Endgame cover infrastructure live until 24 June. Historical matches represent compromises that went undetected, and their credential consequences persist after the infrastructure is gone.

— **Audit third parties for credential-grade data holdings.** Four consecutive months of major incidents originating with a party other than the named victim makes this the base case. The question is not whether a supplier has a security programme but which of them hold credentials, licence numbers, or identity documents relating to your users.

— **Assume a ninety-day detection-to-notification interval.** AssuranceAmerica — a competently run response — took from 17 March to 15 June. Plan monitoring on the assumption that you will learn about a supplier compromise a quarter after it happens.

— **Re-baseline fake-update detection.** Whether the technique migrates to a successor operation is one of the open questions this issue commits to tracking. Coverage should not depend on which operator is running it.

9.4 Recommendations — Registrars and Registries

— **REGRU's 90% reduction is the proof of concept.** Registrar-level abuse volume is a policy variable. A 90% reduction over six months, achieved while other registrars grew several hundred per cent, establishes that verification at registration works.

— **Detect on registration behaviour, not on TLD.** Section 6.3 shows a TLD concentration disappearing entirely within one month. Velocity, registrant fingerprinting, and nameserver assignment patterns are durable; TLD choice is a pure cost decision that changes whenever pricing does.

— **Prepare for the domain-layer expansion to continue.** With C&C domains up 289% while server counts fell 30%, the domain layer is absorbing the pressure applied to hosting. Registry abuse teams should expect volume to grow regardless of enforcement success elsewhere.

> **WHERE WE MAY BE WRONG**
>
> The forecasts above are falsifiable and we intend them to be scored. The claim most likely to prove wrong is 9.1(1): if Endgame's access-layer disruption propagates faster than we expect, Q3 ransomware volume could fall rather than rise, and we would have mistaken a structural effect for market absorption. We will report that outcome plainly if it occurs.

ISSN 2026-VSPAM-006 · VOL. 2026 · ISSUE 6

APPENDIX A

Tools and Suppliers Referenced

This report mentions multiple commercial suppliers as illustrative examples of categories of tooling. Inclusion is not an endorsement, and the list is non-exhaustive. Capability, pricing, and regional availability vary substantially; readers should evaluate against their own requirements.

CATEGORY	EXAMPLES CITED IN THIS ISSUE
Managed DMARC and email authentication	DDMARC (research partner — see editorial disclosure), Valimail, dmarcian, EasyDMARC, PowerDMARC
Enforcement and coordination bodies	Europol, Eurojust, CISA, ICANN, M3AAWG
Industry partners to Operation Endgame	Microsoft, IBM X-Force, Bitdefender
Threat intelligence and incident response	Cisco Talos, CrowdStrike, Trend Micro
Botnet and domain reputation	Spamhaus, SURBL, URIBL, vSpam.org
Breach and ransomware tracking	BreachSense, PKWARE, UpGuard, SharkStriker
Open threat-intelligence feeds	URLhaus, ThreatFox, Feodo Tracker (abuse.ch)
C2 frameworks referenced	Sliver, Cobalt Strike — cited as detection targets, not recommendations

Data availability

The vSpam.org figures reported in Section 6 are derived from the public collector corpus. Aggregate statistics are available through the vSpam.org public API, and researchers seeking the underlying per-indicator data for replication may request access at **research@vspam.org**. We will supply the exact queries used to produce every figure in Section 6 on request.

Forecast scoring

This series records its forecasts explicitly so they can be checked. The May issue's prediction that the novelty-gTLD concentration would not persist is scored as **correct** in Section 6.3. The May issue's Tycoon2FA displacement forecast remains **open** and will be scored in the next issue against the Q2 platform telemetry.

REFERENCES

References

1. Europol (24 June 2026). *Operation Endgame — coordinated action against SocGholish, Amadey and StealC.* europol.europa.eu; see also associated reporting by Cybersecurity Dive, *Western governments disrupt trifecta of cybercrime tools.*
2. The Hacker News (June 2026). *Europol Disrupts AudiA6 Crypto Laundering Service Used by Ransomware Gangs.* thehackernews.com/2026/06/europol-disrupts-audia6-crypto.html
3. BreachSense (July 2026). *June 2026 Ransomware Report: 707 Victims, 63 Groups.* breachsense.com/ransomware-reports/june-2026/
4. Spamhaus (10 July 2026). *Botnet Threat Update, January to June 2026.* spamhaus.org/resource-hub/botnet-c-c/botnet-threat-update-january-to-june-2026/
5. CrowdStrike (2026). *Tycoon2FA Phishing-as-a-Service Platform Persists Following Takedown.* crowdstrike.com
6. DmarcDkim.com (2026). *DMARC Adoption Statistics — live global data;* DMARCguard, *Email authentication research.* Continuous-measurement corpora, approximately 5.5M domains.
7. KDDI corporate disclosure (23 June 2026), as compiled in contemporaneous breach reporting; see SharkStriker, *June 2026 Data Breaches.* sharkstriker.com/blog/june-2026-data-breaches/
8. AssuranceAmerica breach notification (15 June 2026), as compiled by BrightDefense, *List of Recent Data Breaches in 2026.* brightdefense.com/resources/recent-data-breaches/
9. Texas Parks & Wildlife Department disclosure (18 June 2026); Texas Cyber Command. See CM-Alliance, *June 2026: Biggest Cyber Attacks, Data Breaches, Ransomware Attacks.*
10. M3AAWG (June 2026). *M3AAWG's 67th General Meeting Brings Clarity, Connections in High-Stakes Time for Online Safety.* m3aawg.org/blog/M3AAWG67MontrealRecap
11. CISA (June 2026). *Known Exploited Vulnerabilities Catalog* additions; Binding Operational Directive 26-04. cisa.gov/news-events/alerts
12. ICANN (6 February 2026). *Two Years of Enforcing DNS Abuse Mitigation Requirements: Progress & Next Steps.* icann.org/en/blogs
13. vSpam.org collector corpus, 1–30 June 2026. Aggregate figures reproducible via the vSpam.org public API; per-indicator data available on request to research@vspam.org.
14. vSpam.org Independent Research (June 2026). *Trends in Spam, Phishing, Spoofing, Malware and DNS Abuse — May 2026.* ISSN 2026-VSPAM-005.

This report is published by vSpam.org as part of the ongoing independent research series on email and DNS abuse. ISSN 2026-VSPAM-006. Volume 2026, Issue 6. Released under the Creative Commons Attribution 4.0 International License (CC BY 4.0). Citation: vSpam.org Independent Research. (July 2026). "Trends in Spam, Phishing, Spoofing, Malware, and DNS Abuse — June 2026." Volume 2026, Issue 6. ISSN 2026-VSPAM-006. Corrections, additional data, or feedback: research@vspam.org