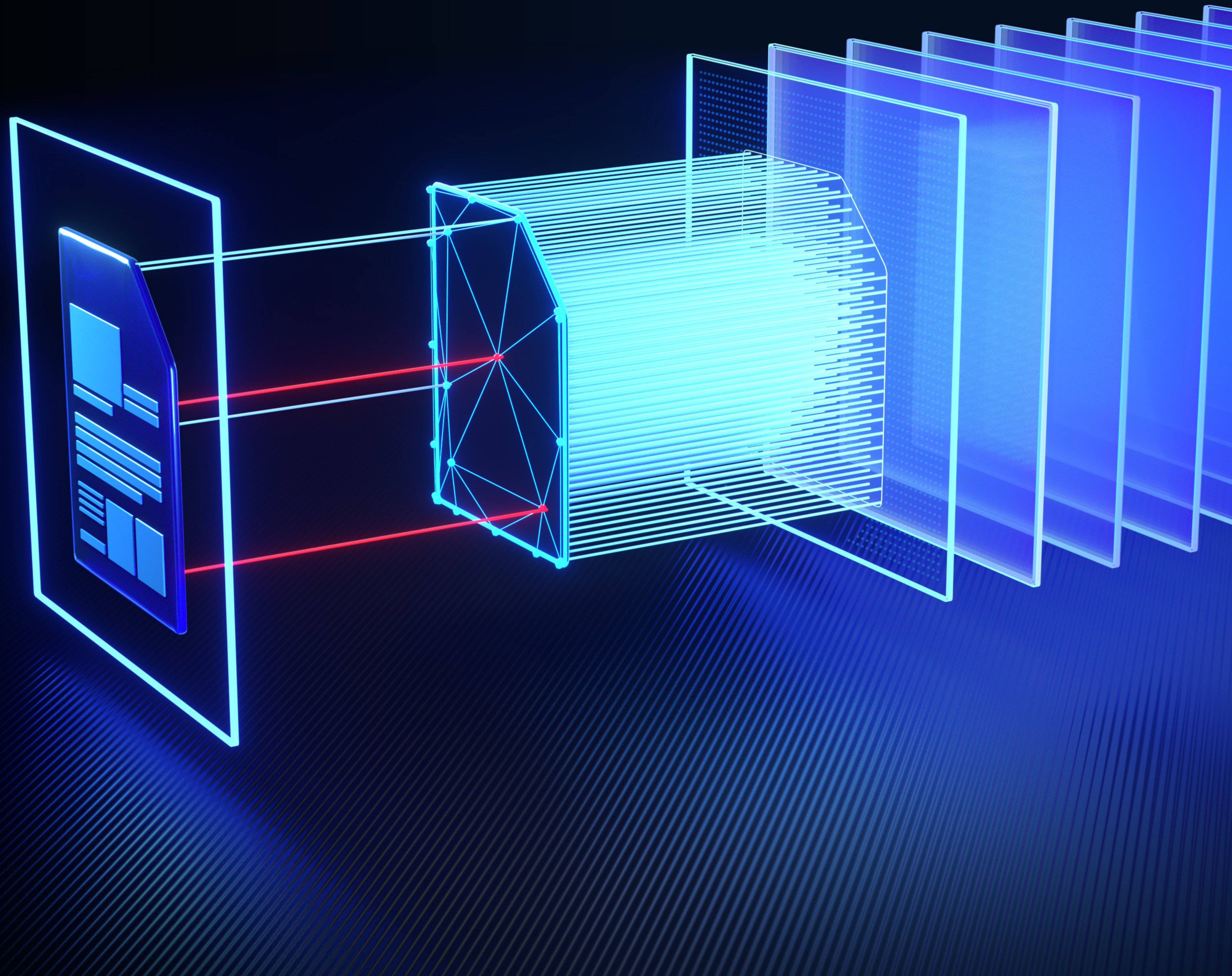
OPSWAT.

2025 OPSWAT Threat Landscape Report

Global Cyberattack Trends Require Actionable Intelligence for Better Protection

Protecting the World’s Critical Infrastructure

Table of Contents



01

Executive Summary

The accelerating complexity of cyber threats is outpacing traditional detection methods, leaving critical infrastructure, government systems, and enterprise environments exposed to increasingly evasive and modular malware.

OPSWAT's inaugural Threat Landscape Report, based on telemetry from nearly one million sandbox scans conducted via Filescan.io over the last 12 months, reveals that adversaries are innovating faster than static defenses can adapt.

Key insights from the data include a 127% increase in attack chain complexity over the past 6 months—measured through multi-stage execution chains and obfuscation tactics designed to mislead traditional security tools. Notably, 7.3% of files undetected by public OSINT feeds were reclassified as malicious by the emulation-based sandbox 24 hours earlier than conventional sources on average. This gap highlights the growing limitations of signature- and reputation-based tools in the face of zero-day and fileless threats.

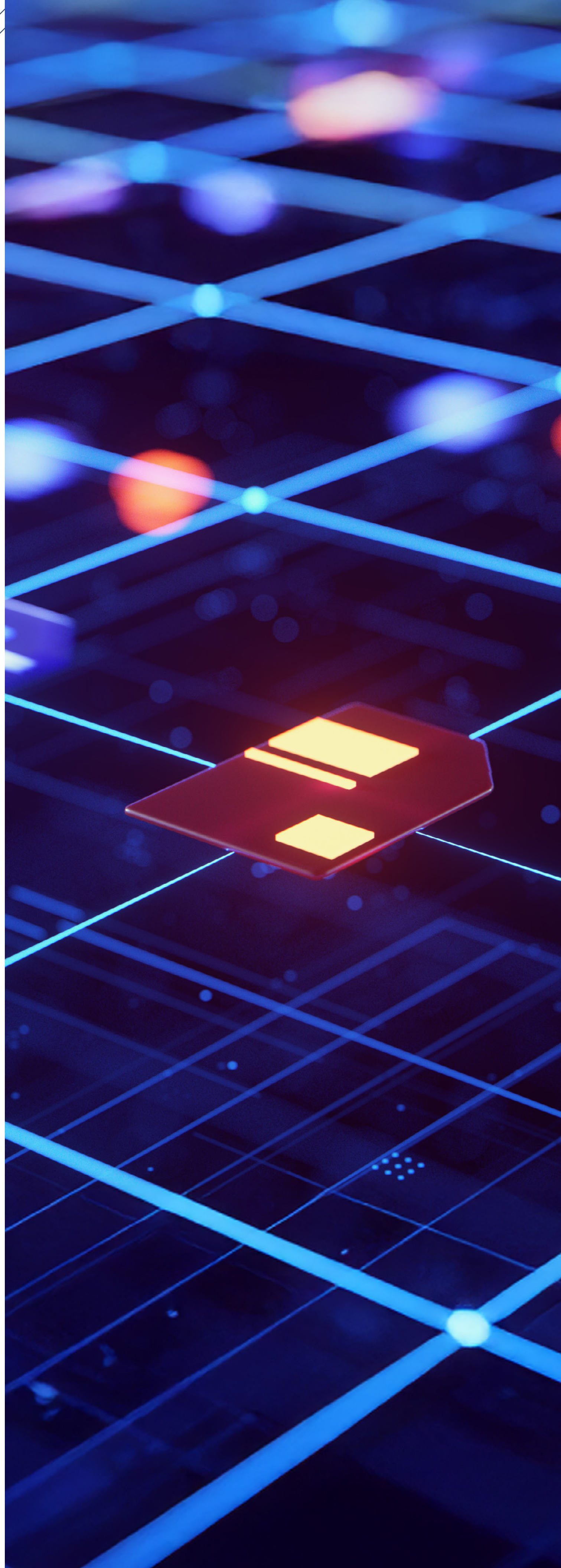
Attackers continue to favor stealth and adaptability: malware families now commonly embed payloads in benign-seeming formats such as .NET Bitmaps, steganographic images, and even Google services abused for covert command-and-control. Emerging techniques like ClickFix, a clipboard-based social engineering tactic, are gaining ground among both criminal and nation-state actors.

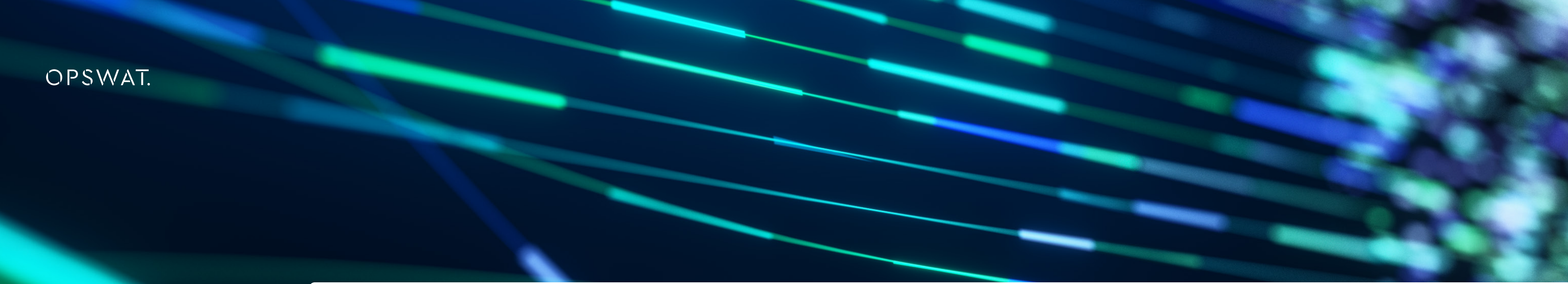
The data shows malware is built to evade, not overwhelm—making behavioral analysis, backed by sophisticated anti-evasion technology, essential. With 99.97% detection efficacy across scripts, executables, and documents, the report shows that dynamic pipelines rooted in emulation and behavioral correlation can reveal campaigns that remain invisible to legacy AV and EDR stacks.

Key Insights:

- Malware complexity jumped 127% in six months, driven by multi-stage execution chains and heavy obfuscation.
- 7.3% of files missed by public OSINT feeds were flagged as malicious by Filescan.io—on average 24 hours earlier, exposing a widening gap in reputation-based tools.
- Adversaries favor stealth over scale: payloads hide in formats like .NET bitmaps and steganographic images, with Google services repurposed for covert C2.
- Social engineering is adapting too—tactics such as "ClickFix" (clipboard hijacking) are spreading across criminal and nation-state campaigns.

Ultimately, this Threat Landscape Report is a call to action: defenders must transition from reactive controls and outdated defenses to **adaptive, behavior-first detection strategies and multi-layered solutions.** Understanding the evolving playbook of cyber adversaries demands continuous emulation, campaign correlation, and faster reclassification to close the threat window—before the next breach.





OPSWAT.

02

The Broadening Cyber Threat Landscape

Surge in Critical Infrastructure Attacks

Attacks on operational technology (OT) and critical infrastructure have continued their upward trajectory in 2025. Sectors such as manufacturing, energy, and utilities remain at the forefront of threat actor targeting, with financial and espionage motivations both in play.

Verizon's 2025 Data Breach Investigations Report (DBIR)[1] analyzed over 12,000 confirmed data breaches, revealing that manufacturing experienced 1,607 confirmed breaches, a significant increase over prior years. External actors were responsible for 86% of these cases, while nearly 20% involved espionage motives—pointing to a growing focus on intellectual property theft and operational disruption.

Ransomware remains one of the most prominent threats, featuring in 44% of all breaches across sectors and accounting for 75% of breaches within the System Intrusion pattern. In parallel, vulnerability exploitation has risen sharply as an initial access vector, with attackers particularly focusing on edge devices, firewalls, and VPN services—a trend seen in both espionage campaigns and financially motivated ransomware operations.

The global cost of cybercrime is projected to reach $1.2 trillion in 2025, with business downtime and lost productivity accounting for up to $1 trillion of that figure[2]. Regulatory scrutiny is intensifying, particularly in the EU (NIS2, Cyber Resilience Act) and North America, driving mandatory reporting and resilience requirements for critical infrastructure[2,3]. The cybersecurity market itself is projected to grow at a 12.6% CAGR, reaching $301.9 billion in 2025[3].

Verizon's data also highlights a doubling of breaches associated with third-party infrastructure, indicating increasing systemic risk via cloud and SaaS interdependencies. Notably, credential abuse accounted for 22% of initial access vectors.

> "Manufacturing breaches doubled in a year—espionage and ransomware dominate critical infrastructure risk."
>
> **Verizon 2025 DBIR**

File-Based Attack Vectors Remain Pervasive

File-based malware remains a pervasive and adaptable threat in 2025. Adversaries continue to rely on common document formats—including PDFs, archives (ZIP/RAR), and HTML files—to deliver payloads that evade detection by blending into expected workflows. These file types continue to dominate threat telemetry, while DOCX and XLSX usage has declined.[4,6,8] HTML smuggling techniques, which use embedded JavaScript in .html attachments to load malware from external servers, have surged in effectiveness.

> “Archives and PDFs are today’s malware workhorses—file-based attacks adapt faster than defenses.”
> **Hornetsecurity**

> “Credential phishing up 703%—your inbox is now the frontline of cyber risk.”
> **SlashNext**

Explosive Growth in Credential Phishing and Social Engineering

Phishing remains the most common delivery mechanism, with Verizon’s 2025 DBIR reporting that phishing was present in 19% of all breaches, while pretexting and baiting techniques are increasing in sophistication. In particular, the SlashNext 2024 Phishing Intelligence Report found that credential phishing campaigns surged by 703% in late 2024, with brand impersonation tripling and nearly every mailbox facing weekly phishing attempts.[5]

> “Fileless attacks: invisible, in-memory, and immune to signature-based defenses.”
> **Lumifi Cyber**

Payload Stage Two: Fileless Malware and Living-off-the-Land Attacks

Modern phishing campaigns are often only the first stage. The second payload frequently consists of fileless malware, which uses PowerShell, .NET reflection, or WMI to execute code directly in memory. These attacks avoid dropping files to disk, thereby evading signature-based antivirus tools. Lumifi Cyber has noted a steep rise in fileless and “living-off-the-land” techniques across 2025 campaigns.[6]

> “CVE disclosures could hit 50,000 in 2025—risk management is now a race against volume.”
> **Computer Weekly**

Vulnerability Disclosure Hits Record Highs

The 2025 CVE disclosure rate is on track to reach 45,000–50,000, according to Computer Weekly[7] and vulnerability analysts, marking an 11% increase over 2024. This dramatic growth is driven by open-source dependencies, rapid development cycles, and expanding regulatory scrutiny, including Europe’s legislative pressure via NIS2 and the CRA.

In Summary

The attack surface is expanding as fast as attackers are innovating. From supply chain compromises and OT system infiltration to phishing and polymorphic malware, defenders face a layered and increasingly evasive threat landscape. The rise in ransomware and credential theft, backed by data from Verizon’s 2025 DBIR and supporting threat intelligence partners, confirms that foundational controls such as vulnerability management, file inspection, and phishing defense must evolve—and fast.

[1] https://www.verizon.com/business/resources/reports/dbir/

[2] https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/

[3] https://www.precedenceresearch.com/cyber-security-market

[4] https://www.hornetsecurity.com/en/blog/monthly-threat-report-january-2025/

[5] https://slashnext.com/wp-content/uploads/2024/12/SlashNext-2024-Phishing-Intelligence-Report.pdf?_hsmi=339039502

[6] https://www.lumificyber.com/blog/5-most-common-types-of-malware-in-2025/

[7] https://www.computerweekly.com/news/366619678/CVE-volumes-head-towards-50000-in-2025-analysts-claim

[8] https://www.pivotpointsecurity.com/why-file-based-malware-dominates-cyberattacks/

03

Uncovering Behavioral Insights

Key Threat Campaigns Unfolding Over Time

This section highlights major threat activity observed through OPSWAT analysis in the last 12 months. Each entry reflects real-world campaigns, techniques, and payloads captured, revealing how attackers evolve over time and adapt to evade detection.

Apr. - June 2024

- Evasion through .LNK abuse seen in espionage campaigns (UNC1151, MustangPanda)
- Phishing campaign impersonating DocuSign and other brands

July - Sept. 2024

- Fileless injection on the rise
- Multilayered obfuscated script-based attacks
- C2 channels hiding in trusted Google infrastructure (Calendar and Sheets)

Oct. - Dec. 2024

- Abuse of AI-related themes to deliver installers using unusual, compiled PE (JavaScript and Python)
- Credential flusher used to trap users on fake login pages
- Intentionally corrupted Office documents, zero-day exploitation

Jan. - Mar. 2025

- UTF-16 BOM markers in batch scripts to confuse detection parsers
- CVE-2025-21298: a critical Windows OLE zero-click flaw enabling RCE via email
- WebDAV abused in StrelaStealer campaigns for stealthy remote payload delivery
- QR code evasion via intentional pixel cropping

Apr. - June 2025

- Sharp rise in RAT & Stealers, supported by current Cybercrime as a service (XWorm, Lumma)
- Campaigns abusing steganography to hide PE in images
- Stealthy .NET loaders, with malicious Bitmap resource
- Emergence of ClickFix and FileFix , simple but highly effective social engineering techniques

THREAT CLUSTER OVERVIEW

Practical Examples of Attack Vectors

Threat activity over the past year reveals consistent clusters of techniques, each representing repeatable playbooks observed across campaigns. Rather than isolated IOCs, these clusters reflect the chaining of tactics like script obfuscation, geo-fencing, and adaptive social engineering. Each example in this section is grounded in real-world timelines and validated through sandbox telemetry. Together, they showcase how adversaries combine simplicity and stealth to evade detection—and how adaptive sandboxing unmasks their strategies.

Filescan.io
Community

To view the links to the Filescan.io reports and access advanced queries, sign up for free here.

By joining the filescan.io community, you'll be able to uncover hidden threats with insightful malware analysis powered by emulation. The local threat graph has 74M+ IOCs and MD Cloud Reputation is adding 40B+ Hashes, IPs, and Domains for maximum protection.

Multi-layered & Obfuscated Script Attacks

Threat actors increasingly rely on chaining lightweight, obfuscated scripts to bypass detection. Initial access vectors observed this year range from uncommon file types like .lnk shortcuts to more traditional phishing documents.

What follows is a combination of scripts—Batch, PowerShell, VBS, JavaScript—each obfuscating the next stage, chained together in varying orders and depth. These script chains are designed for simplicity and modularity, which paradoxically makes them harder to catch. The execution is fast, and traces are minimal. A standout example was seen in targeted espionage campaigns across Eastern Europe, where LNK files served as silent launchers for heavily obfuscated script chains.

View the Threat Cluster Hunting Query

How an Adaptive Sandbox Helps
An adaptive sandbox unravels the entire execution chain—revealing each script stage, decoding obfuscated layers, and exposing the final payload. It provides analysts with clear visibility into the attack flow, helps bypass runtime obfuscation, and uncovers recurring patterns used across campaigns. These insights feed directly into Attack Pattern Analysis, supporting threat hunting, detection engineering, and long-term defensive strategy.

Evasion-Specialized Attacks & Geofencing

This past year marked a clear shift toward precision-based strategies, favoring stealth and precision over volume. Attack actors put effort on exploiting previously unknown or rarely seen techniques—what can be described as zero-day evasion techniques—not just for exploitation, but to systematically defeat detection pipelines.

These ranged from malformed file delivery (e.g., intentionally corrupted Office documents) to obfuscation tricks that target specific detection blind spots, such as UTF-16 BOM markers embedded in batch scripts to break parsing logic. In other cases, we see payloads wrapped in unexpected file formats—compiled JavaScript or Python—rarely associated with malware.

Adding another layer of stealth, many of these operations embedded geo-aware logic. Payloads were only delivered or unpacked in specific regions, making them invisible to traditional sandboxing. This approach deliberately isolates the campaign's visibility, ensuring it stays below the radar.

View the Threat Cluster Hunting Query

How an Adaptive Sandbox Helps
By continuously scanning the threat landscape, the sandbox stays ahead of emerging evasion techniques—ensuring detection capabilities are in place before they become widespread. Its emulation-based approach allows it to bypass many of the environmental checks and regional filters used by attackers. This makes it effective against campaigns designed to evade traditional sandboxes and enables early identification of stealth techniques before they gain traction.

Cybercrime as a Service

The commoditization of cybercrime continues. RATs and stealers like Lumma, XWorm, and Snake Stealer dominate the threat space. Many come wrapped in stealthy .NET loaders with custom stagers leveraging bitmap resources, malicious logic with chunks of authentic, non-functional app code, and control flow obfuscation to hinder intentions. Cybercrime does not innovate on malware core logic but heavily on distribution and evasion. The protective wrappers are often more advanced than the payload itself.

View the Threat Cluster Hunting Query

How an Adaptive Sandbox Helps
The sandbox disrupts the endless stream of cybercrime attempts. It reveals the underlying payloads and maps them to well-known families, even when heavily protected. A comprehensive classification system tracks evolving variants, linking campaigns—building long-term intelligence on the cybercrime ecosystem.

Trusted Infrastructure as C2*

Threat actors increasingly abuse platforms with built-in reputation: Google Sheets and Calendar are in the crosshairs now. By hiding command-and-control traffic inside legitimate SaaS, attackers make detection harder and burn less infrastructure. These channels are also resilient, as they don't rely on easily blockable hosts, but rather on widely used services.

Also, WebDAV has reemerged in 2025, campaigning as a stealthy way to load remote payloads while appearing benign at the network level. These are not fallback channels; they are deliberate design choices from the start.

View the Threat Cluster Hunting Query

How an Adaptive Sandbox Helps
C2 infrastructure is limited only by the attacker's imagination. When threat actors hide behind trusted platforms, the sandbox exposes how they turn legitimate services into covert C2 channels. It gives deep visibility into these abuses and provides actionable insights to shape network detection strategies. These findings also support effective threat hunting across enterprise environments.

*: Command and Control Infrastructure

Phishing & Social Engineering

Social engineering continues to be the lowest-effort, highest-impact vector. We have seen countless cases of traditional phishing: brand impersonation, QR phishing, fake login pages—all still effective at scale. But the shift goes beyond email.

Recent campaigns do not focus on payload sophistication. Instead, they exploit the user's judgment as ClickFix does. This threat tricks users into running malicious commands that are silently copied to their clipboard. Fake reCAPTCHA pages and "bot protection" screens are used as bait, often placed between redirects or fake download gates. Its simplicity makes it hard to detect—and effective enough that even nation-state APT groups have adopted it.

View the Threat Cluster Hunting Query

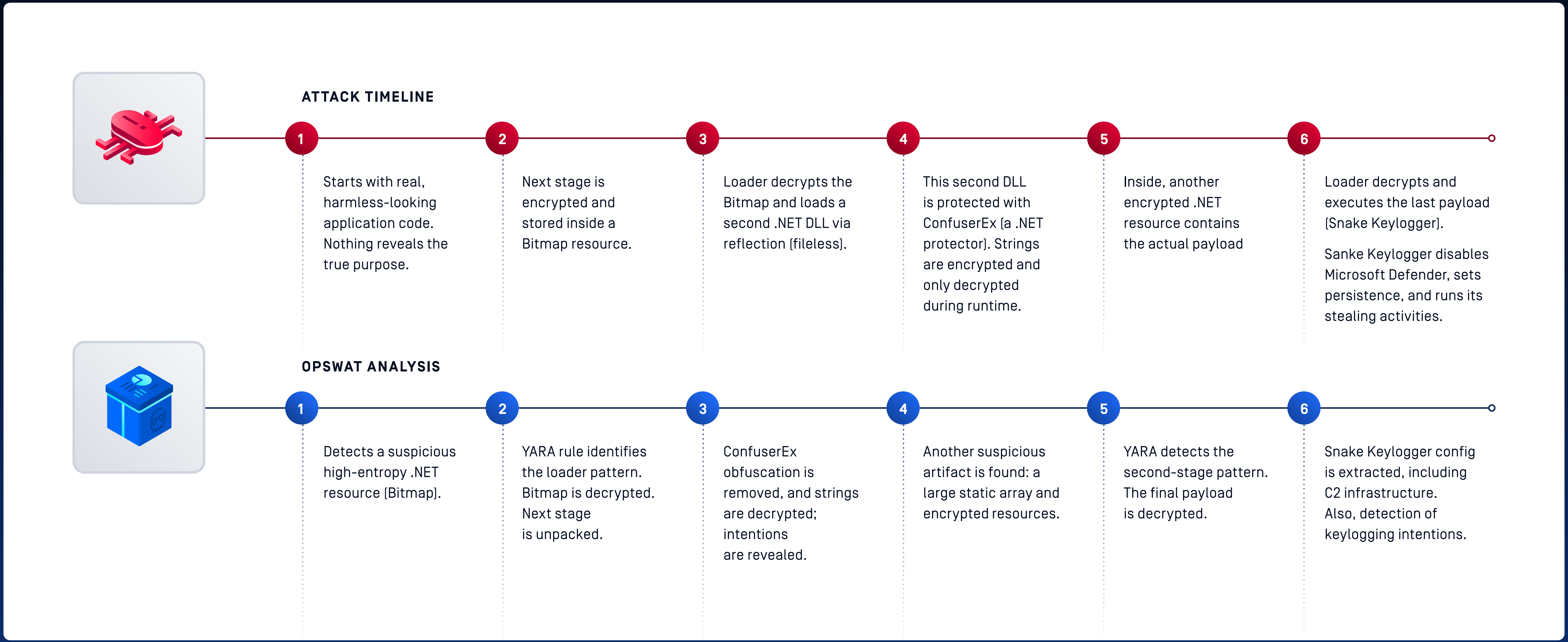
How an Adaptive Sandbox Helps
Users remain the weakest link—and the sandbox acts as a safeguard. It uncovers how social engineering tactics are executed in real time, capturing the full flow from lure to execution. This provides unique threat context around new campaigns and helps detect emerging attack vectors before they reach end users.

SHOWCASES

Candidate #1: Stealthy .NET Loader with Bitmap Payload – Snake Keylogger

Use Case: Unpack the .NET loader to reach the payload and extract the malware configuration.

View Analysis



ATTACK TIMELINE

1. Starts with real, harmless-looking application code. Nothing reveals the true purpose.
2. Next stage is encrypted and stored inside a Bitmap resource.
3. Loader decrypts the Bitmap and loads a second .NET DLL via reflection (fileless).
4. This second DLL is protected with ConfuserEx (a .NET protector). Strings are encrypted and only decrypted during runtime.
5. Inside, another encrypted .NET resource contains the actual payload
6. Loader decrypts and executes the last payload (Snake Keylogger).

   Sanke Keylogger disables Microsoft Defender, sets persistence, and runs its stealing activities.

OPSWAT ANALYSIS

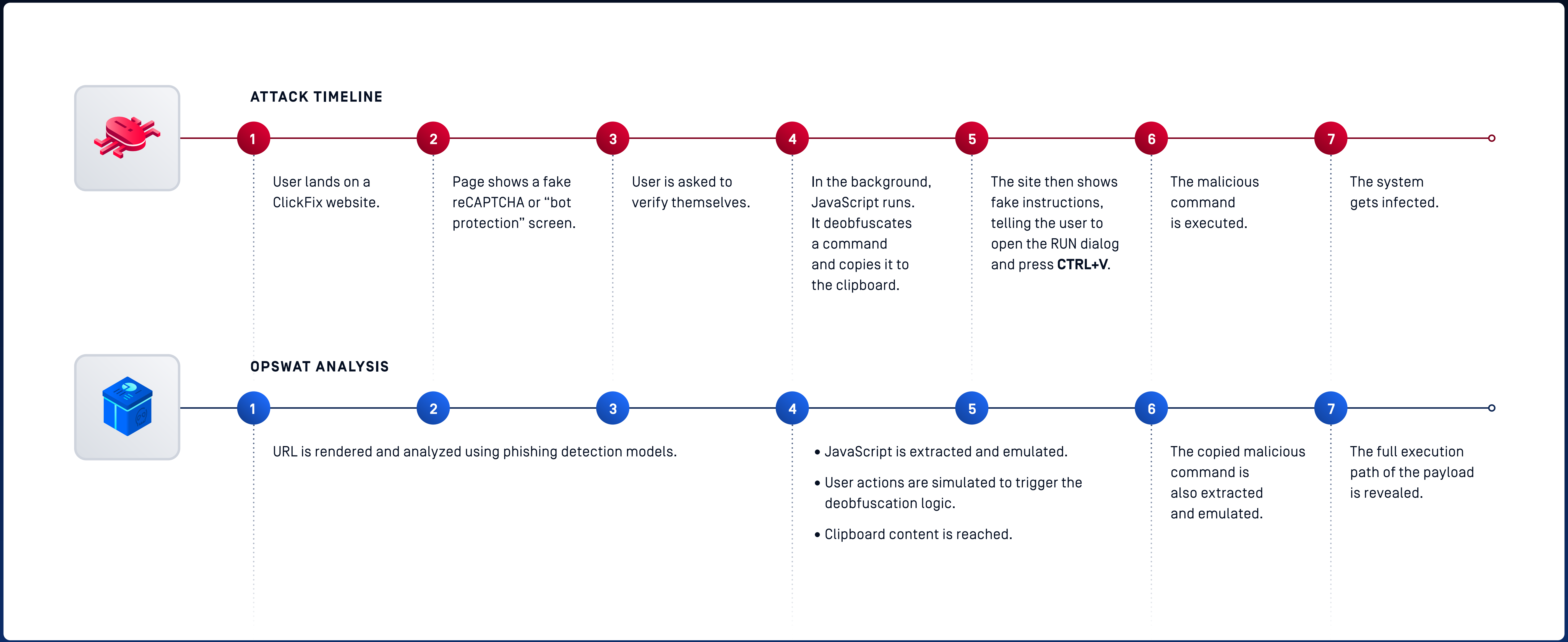
1. Detects a suspicious high-entropy .NET resource (Bitmap).
2. YARA rule identifies the loader pattern. Bitmap is decrypted. Next stage is unpacked.
3. ConfuserEx obfuscation is removed, and strings are decrypted; intentions are revealed.
4. Another suspicious artifact is found: a large static array and encrypted resources.
5. YARA detects the second-stage pattern. The final payload is decrypted.
6. Snake Keylogger config is extracted, including C2 infrastructure. Also, detection of keylogging intentions.

SHOWCASES

Candidate #2: Social Engineering Technique – ClickFix

Use Case: Emerging web-based threat that tricks users into running malicious commands silently copied to their clipboard.

View Analysis



ATTACK TIMELINE

1. User lands on a ClickFix website.
2. Page shows a fake reCAPTCHA or "bot protection" screen.
3. User is asked to verify themselves.
4. In the background, JavaScript runs. It deobfuscates a command and copies it to the clipboard.
5. The site then shows fake instructions, telling the user to open the RUN dialog and press **CTRL+V**.
6. The malicious command is executed.
7. The system gets infected.

OPSWAT ANALYSIS

1–3. URL is rendered and analyzed using phishing detection models.

4–5.
- JavaScript is extracted and emulated.
- User actions are simulated to trigger the deobfuscation logic.
- Clipboard content is reached.

6. The copied malicious command is also extracted and emulated.
7. The full execution path of the payload is revealed.

OPSWAT's Methodology and Data Scope

This report draws exclusively on real-world malware submissions from Filescan.io, an emulation-based sandbox and IOC extraction platform operated by OPSWAT. The data reflects both public and private samples, community contributions, and live behavioral outputs—not speculative analysis.

Beyond traditional, static IOC lists, modern threat detection pipelines cluster malware campaigns into behavioral groups. This approach uncovers the evolution of their Tactics, Techniques, and Procedures (TTPs), alongside mapping infrastructure reuse, obfuscation techniques, and cloud-based command and control.

Aggregated metrics (from 2024-07-01 to 2025-06-30) show:

- Unique Samples: 472,648
- YARA Rule Hits: 2,774,291
- Distinct Malware Families: 35
- Average Threat Report Size:

	File Size (MB)	IOC Count
Average	4.2	74
Median	0.1	12

Scan Volume Statistics

Metric	Jul. - Dec. 2024	Jan. - Jun. 2025	▲ / ▼
Files analyzed by Filescan.io	448k	**504k**	▲ 13%
Malicious files analyzed by Filescan.io	194k	**174k**	▼ 10%
Unique SHA-256 hashes	241k	**237k**	▼ 2%
Total AV scans performed by Production Infrastructure	146M	**181M**	▲ 23.9%
Total sandbox scans performed by Production Infrastructure	160k	**730k**	▲ 356%

Threat Complexity Statistics

Metric	Jul. - Dec. 2024	Jan. - Jun. 2025	▲ / ▼
YARA rule hits	1.3M	**1.4M**	▲ 8%
Distinct malware families	29	**31**	▲ 7%
Average file size	3.9 MB	**4.4 MB**	▲ 12%
Average IOC count per threat report	65	**84**	▲ 29%
Unique IOCs (filescan.io)	3,193,089	**3,339,783**	▲ 4.6%
Average emulation nodes on multi-stage malware	8.06	**18.34**	▲ 127%

The above statistics provide high-level insight into both the volume and type of data that has been submitted to the Filescan.io platform.

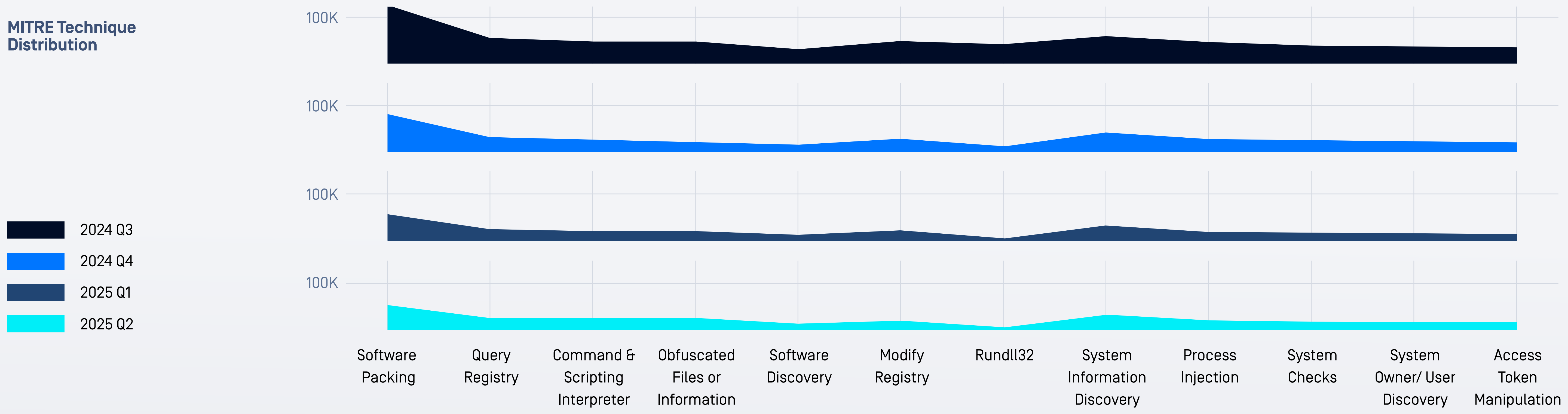
Dissecting this information, a 13% increase in files submitted to the sandbox can be noted, highlighting the growth of Indicators within the Threat Intelligence Database. This data can not only be leveraged for threat hunting investigations but also provides a broader coverage of threat detection through identifying similarities in other submissions within the database.

Whilst an increase has been noted for the overall size of the database, the number of malicious files and unique hashes decreased. This is likely due to a shift in the Initial Access vector, with Threat Actors leveraging Identify based attacks to gain access to a Network through Cloud or VPN Solutions.

A slight increase has been noted in the distinct malware families that are being utilized by Threat Actors, highlighting the continual growth of the threat landscape. Furthermore, Government Agencies may also be contributing to this following their attacks against infrastructure being utilized for Malware as a Service, causing Threat Actors to create new Malware Families.

The average emulation node count for malicious samples increased from 8.06 (24H2) to 18.34 (25H1), indicating a significant rise in **multi-staged malware complexity**. Our internal analysis model suggests an increase in behavior complexity, often seen in evasive loaders and modular payloads.

MITRE Technique Distribution



Key Telemetry and Observed Patterns

Telemetry from OPSWAT's FileScan engine reveals that despite evolving threats, core attacker behaviors persist across the kill chain. Packing, reconnaissance, scripting abuse, and .NET obfuscation continue to dominate malware delivery tactics. Meanwhile, attribution gaps and MITRE mismatches signal the rise of unconventional techniques that evade rule-based models. This section highlights those trends and how enhanced emulation will deepen visibility into emerging obfuscation layers.

Packing Remains a Dominant Evasion Technique

The continued prevalence of Software Packing across all quarters shows that attackers still rely heavily on binary obfuscation to evade static detection and delay analysis. Despite the emergence of more advanced evasion tactics, packing remains a core component in both commodity and targeted malware delivery.

Scripting Abuse Signals Fileless Trends

The persistent use of Command and Scripting Interpreter reflects attacker preference for chaining native scripting engines and LOLBINs to stage payloads. This aligns with the rise in fileless, script-heavy campaigns observed throughout 2024–2025.

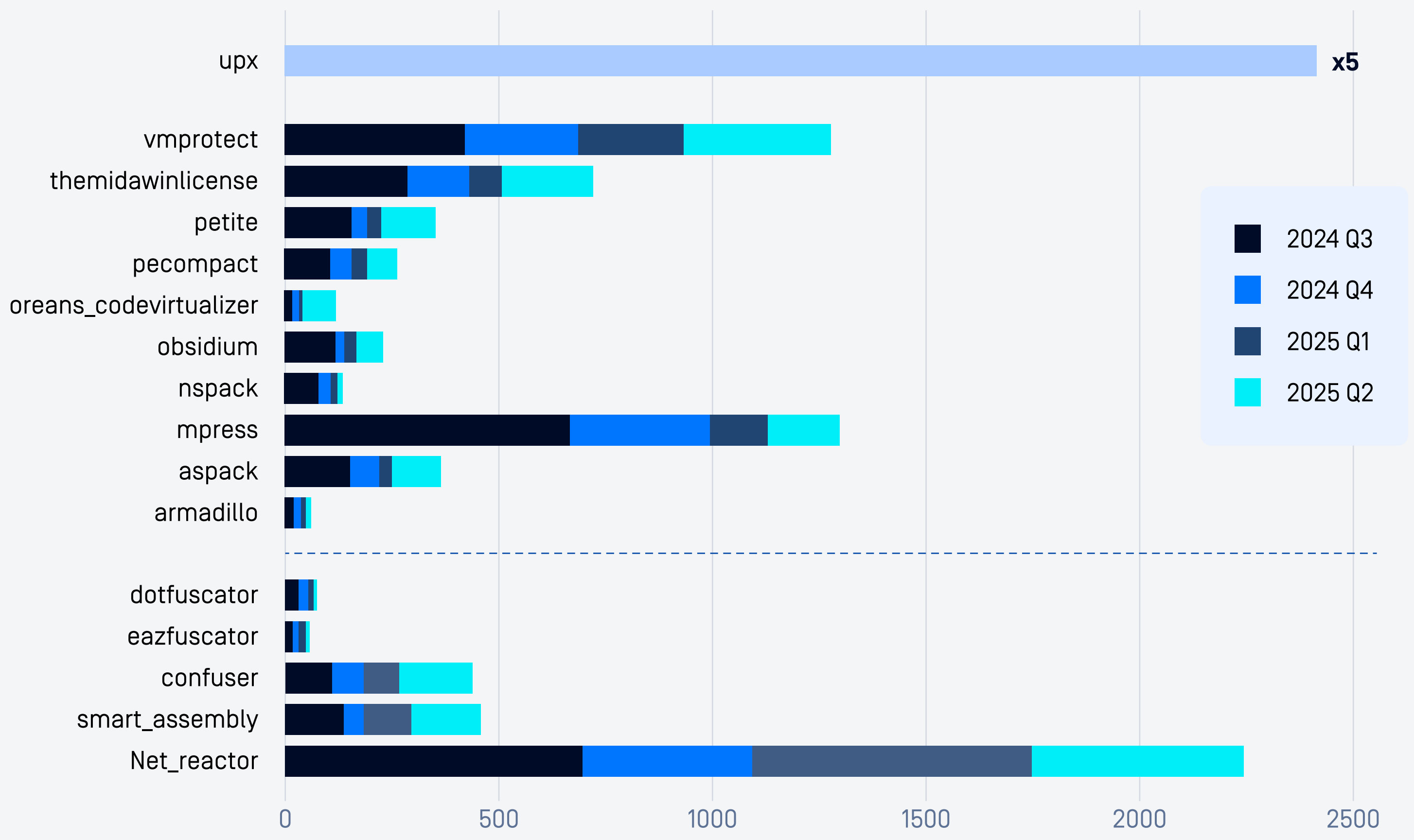
Reconnaissance as a Core Phase

The high frequency of System Information Discovery, Software Discovery, and Query Registry techniques highlights a consistent focus on host profiling. These checks not only support privilege escalation and lateral movement but also serve to detect sandboxed or virtualized environments—allowing threats to evade automated analysis and delay detection.

Evolving Rules Affect MITRE Technique Attribution

Despite an increase in detected malware, the volume of mapped techniques has declined over recent quarters. This suggests that newly observed behaviors may not be consistently attributed to known MITRE techniques, possibly due to the emergence of unconventional tactics.

Native and .NET Packers



.NET Obfuscation at Scale

NetReactor continues to be the most used packer by far, highlighting its role in protecting .NET-based malware in both commodity and custom toolchains. Its widespread use suggests it is a default choice in malware-as-a-service ecosystems.

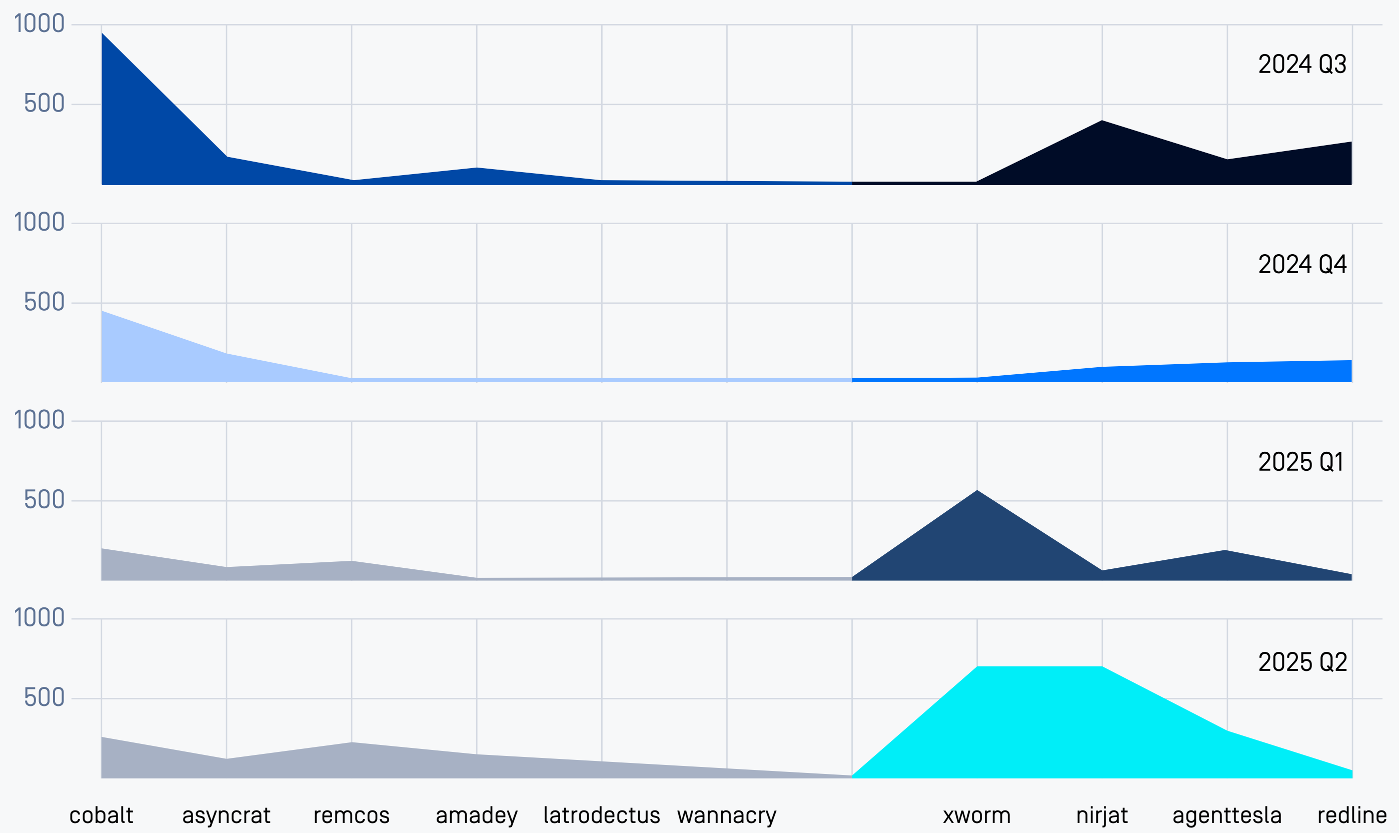
Commercial Packers Blur the Line

MPRESS, VMProtect, and Themida are used in both legitimate and malicious software, often through cracked versions repurposed by attackers. Their dual-use nature complicates detection as their presence alone isn't inherently malicious, unpacking is required to reveal true intent.

Legacy Packers Fading

Minimal use of older packers like PECompact, Petite, and Aspack suggests a decline in legacy tooling, likely due to better unpacking or detection by automatic systems.

Malware Family Distribution



Cybercrime Leans Toward .NET

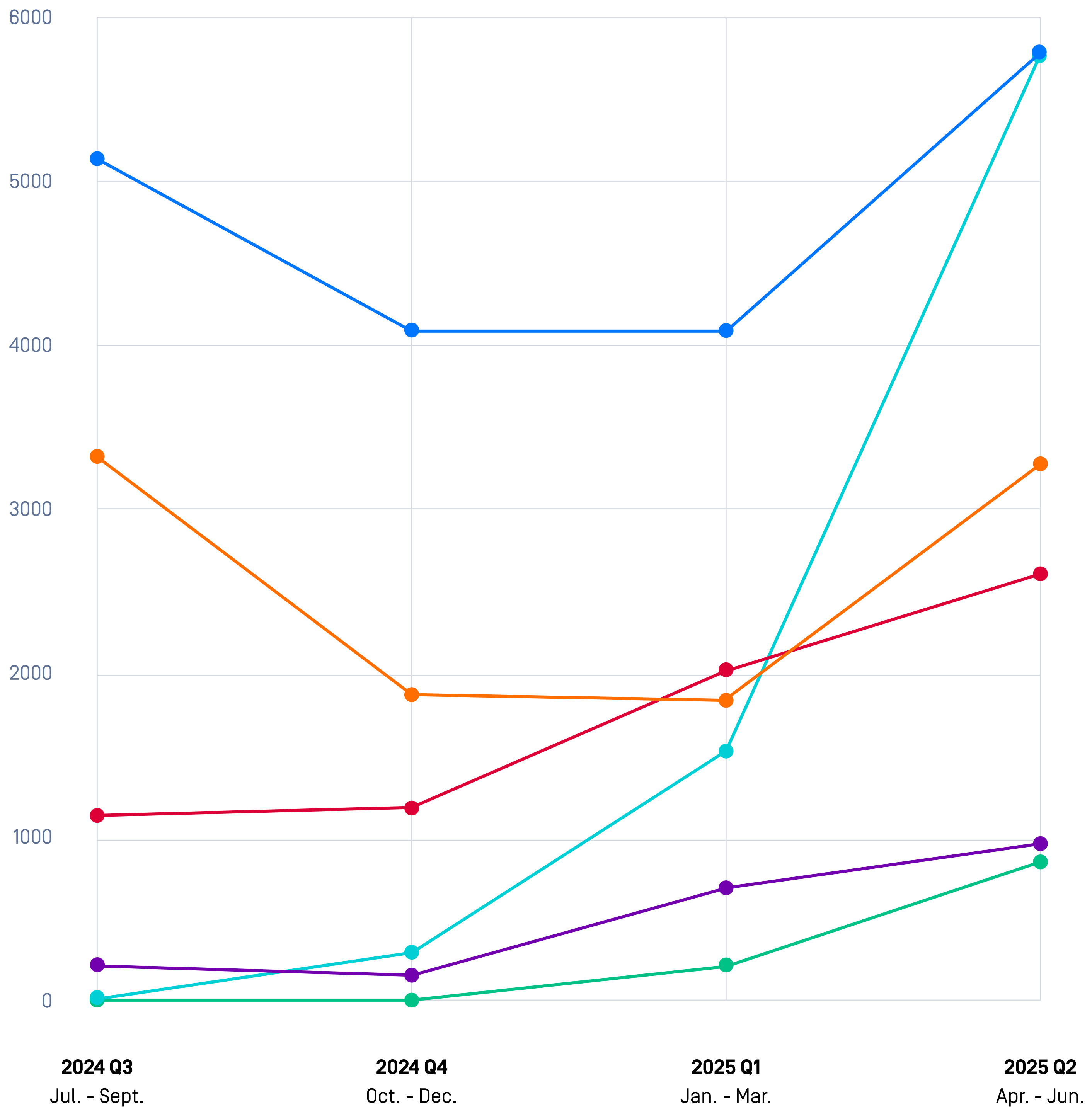
The rise of .NET-based malware reflects its ease of use, fast development, and strong obfuscation support. Its deep Windows integration enables powerful functionality without complex native code, making it ideal for stealers and RATs.

XWorm & NjRAT's steep rise reflects ease of access, cracked builds, and active development in threat communities.

Obfuscation Layers Obscure Payload Visibility, But New PE Emulator Will Close the Gap

The observed decline in some malware families is due to the increasing use of custom packers and loaders that prevent clear attribution at initial stages. However, with the addition of a PE emulator to the analysis pipeline, we expect a significant boost in unpacking and runtime decryption, enabling deeper visibility and more accurate malware family detection in upcoming quarters.

Trending Threat Indicators



Sandbox Evasion Checks

Sandbox Evasion Checks remain dominant, with a strong rebound in Q2 after a dip. This highlights that anti-sandbox logic continues to be a foundational evasion strategy in modern malware.

Invalid Code Signature

Invalid Code Signature detections are rising again after a low in Q4 and Q1, suggesting renewed use of malware with broken, forged, or repurposed certificates — often seen in fake signed or compromised executables.

Hidden .NET Artifacts

Hidden .NET Artifacts are surging, becoming one of the most triggered indicators by 2025 Q2. This reflects a growing reliance on .NET-based malware that hides payload logic from static inspection.

Obfuscated Script

Obfuscated Script activity is climbing steadily, confirming that attackers continue to chain and heavily obfuscate scripts as part of multi-stage infection chains.

Encrypted Payload Delivery

C2 Communication

Both **Encrypted Payload Delivery and C2 Communication** triggers showed consistent growth — two techniques that often go hand in hand. Modern malware tends to reach out to its C2 infrastructure only after staging or decrypting its core functionality, indicating a clear shift toward stealthy, in-memory execution. This reflects how newer threats are not only modular but also increasingly protected through encryption or custom loaders, making early-stage analysis more difficult.

Understanding Phishing Site Longevity and Template Strategies for Effective Detection

Phishing websites are designed for rapid deployment and short lifespans, with the majority being taken down within the first 24 hours. As shown, only a small fraction of phishing sites remain active beyond this critical window, underscoring the need for swift detection and response.

Furthermore, while most phishing sites employ unique templates to evade reputation-based defenses, a significant minority (20%) reuse identical HTML templates across multiple domains. This tactic allows attackers to bypass traditional detection methods that rely on domain reputation or blacklists.

These insights highlight the importance of real-time, content-based detection strategies. By understanding the lifecycle and template reuse patterns of phishing sites, security teams can prioritize rapid, adaptive defenses that are resilient to both fast turnover and template-based evasion techniques.

Unknown-OSINT Files Get Reclassified

Why it matters: Automated detonation trims the blind spot between public-intel silence and first outbreak by ~24 h on average.

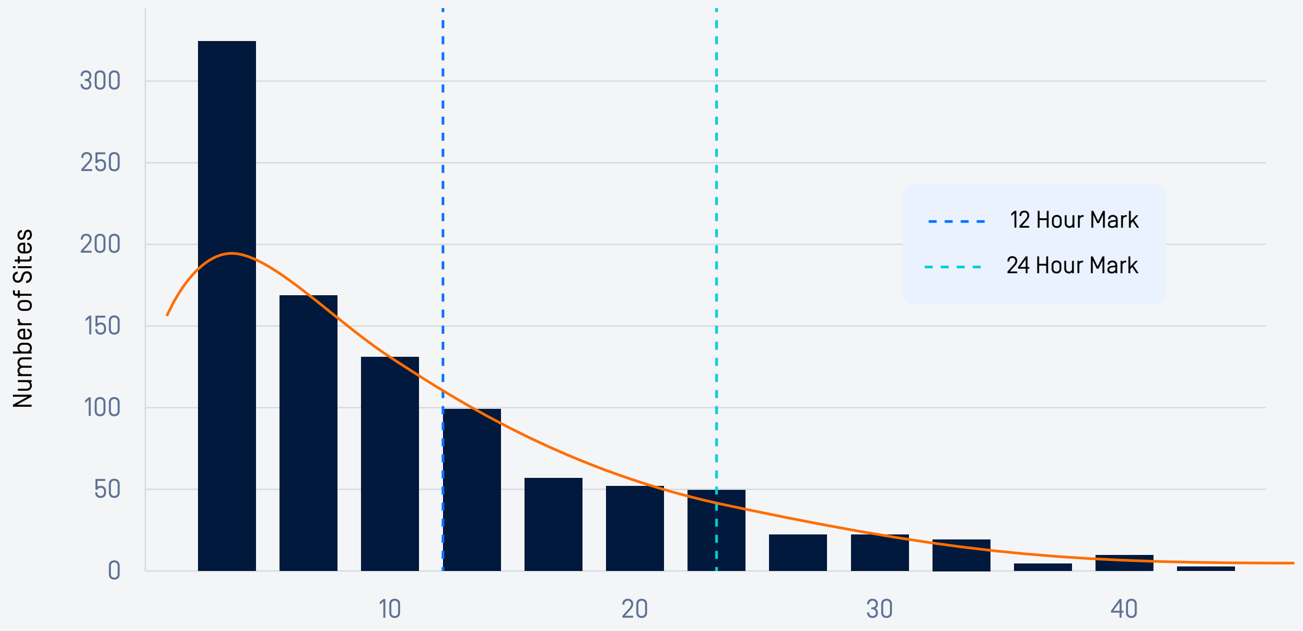
One in 14 files ignored by public feeds turned out to be malicious.

OSINT Verdict	Sandbox Re-Grade	Count	Share of Unknowns
Unknown → **Benign**	8,221	**45.4%**	
Unknown → **Suspicious**	4,205	**23.2%**	
Unknown → **Likely Malicious**	912	**5.0%**	
Unknown → **High-Confidence Malicious**	414	**2.3%**	
Potential Zero-Day Window (Likely + Malicious)	—	**1,326**	**7.3%**

This OSINT blind spot also applies to phishing kits. Heuristic-based detection catches early-stage threats that automated crawlers often miss. Refer to Section 6 or recommendations on how to solve this challenge.

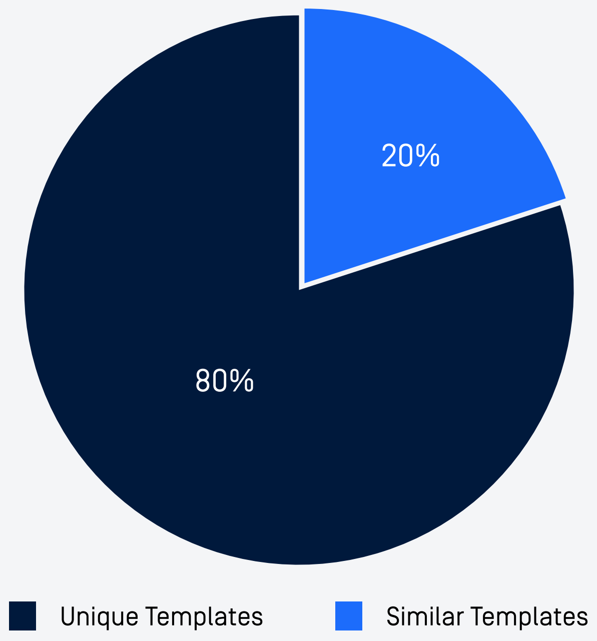
Phishing Website Lifecycle Distribution Trending

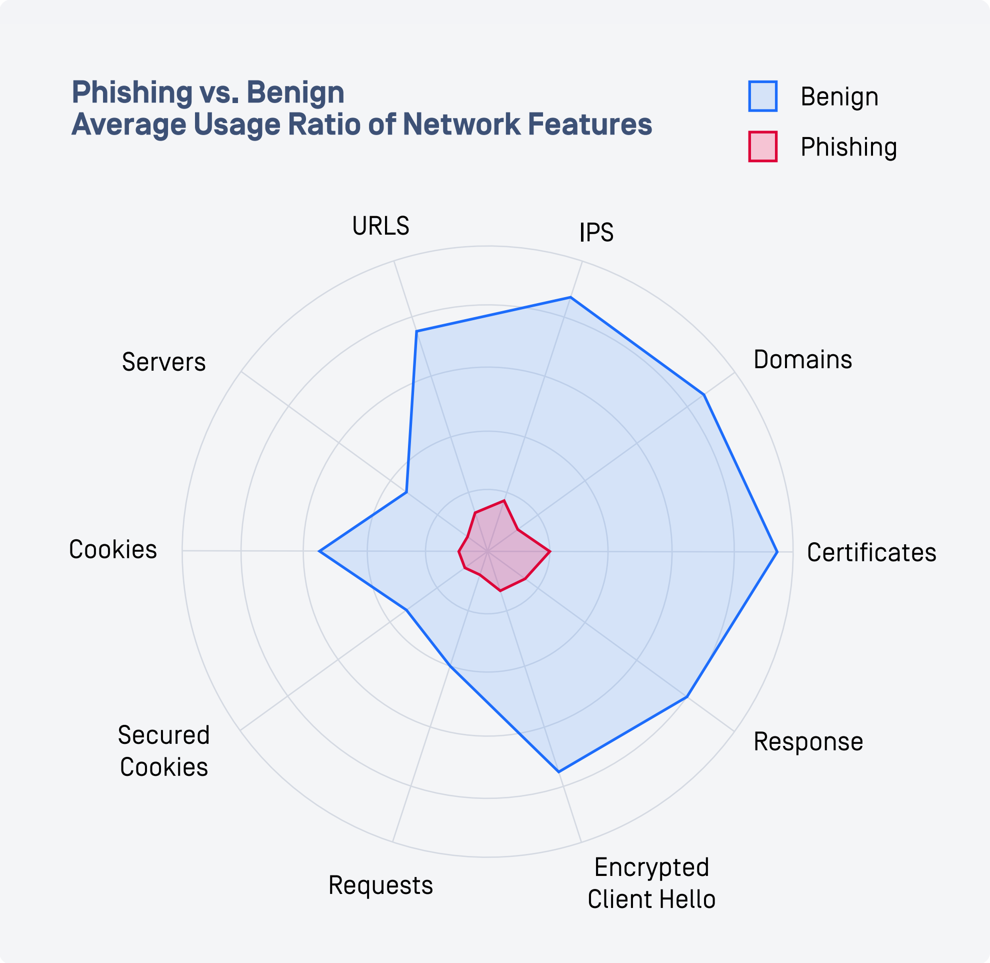
Of daily 500 phishing sites, only 80 survive beyond the 24-hour mark

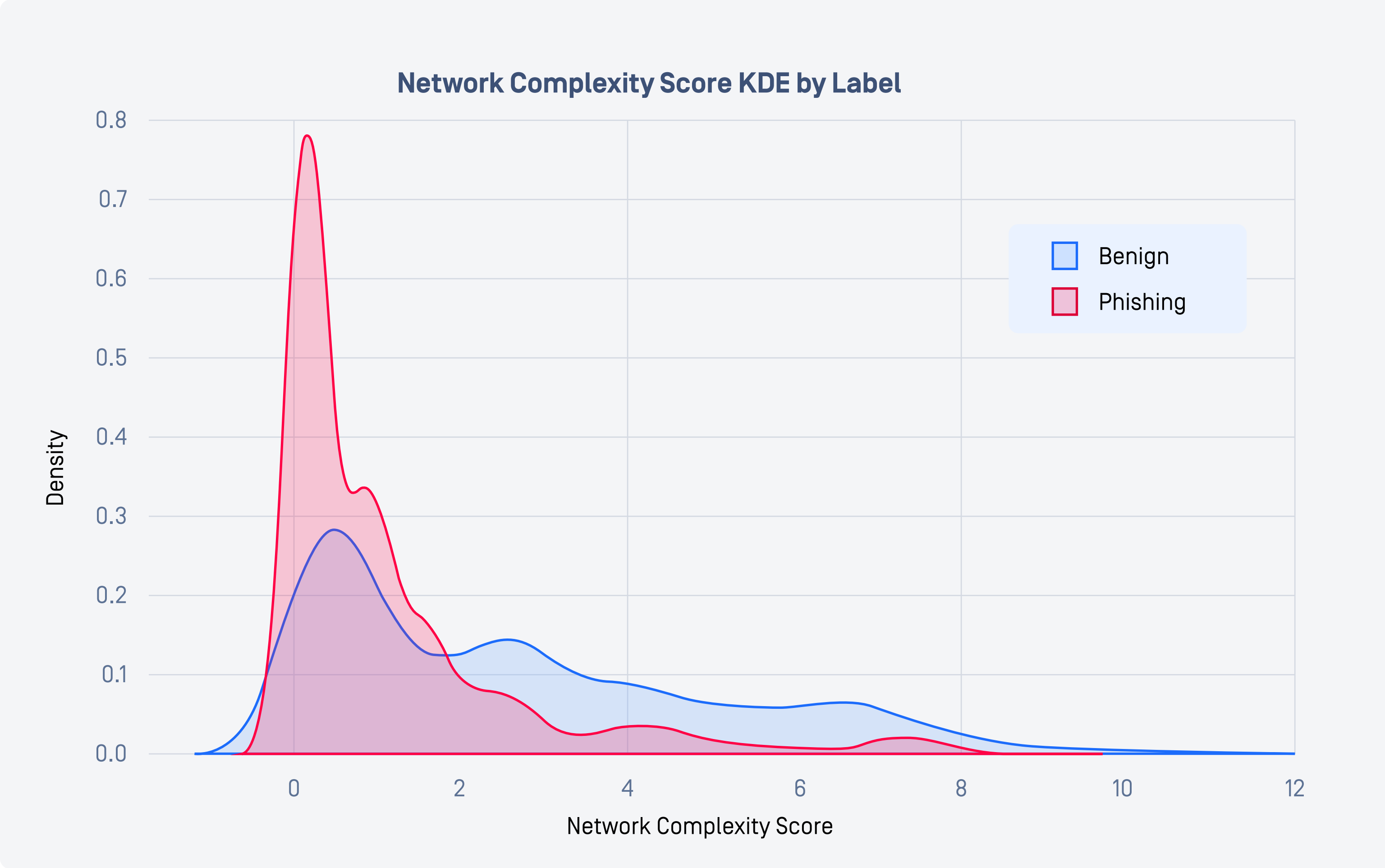


Analysis of 50,000 Phishing Sites Template Usage

20% of phishing sites use identical HTML templates with different domains, making traditional reputation-based detection ineffective.







Network-Based Attack Insights

Network Feature “Richness” is a Legitimacy Marker

Benign footprint
Benign sessions light up almost every spoke on the radar chart, showing high values for certificates, domains, cookies, URLs, and modern TLS features.

Phishing footprint
Phishing sessions hug the hub, with low or zero values for most features.

Deduction
Minimalist network profiles are a robust, low-cost heuristic for phishing detection. The radar chart provides a visual summary of this “richness gap.”

Operational Rule
Minimalist network profiles (few certificates, domains, cookies) are a strong red flag for phishing.

Network Complexity: Simplicity is Suspicious

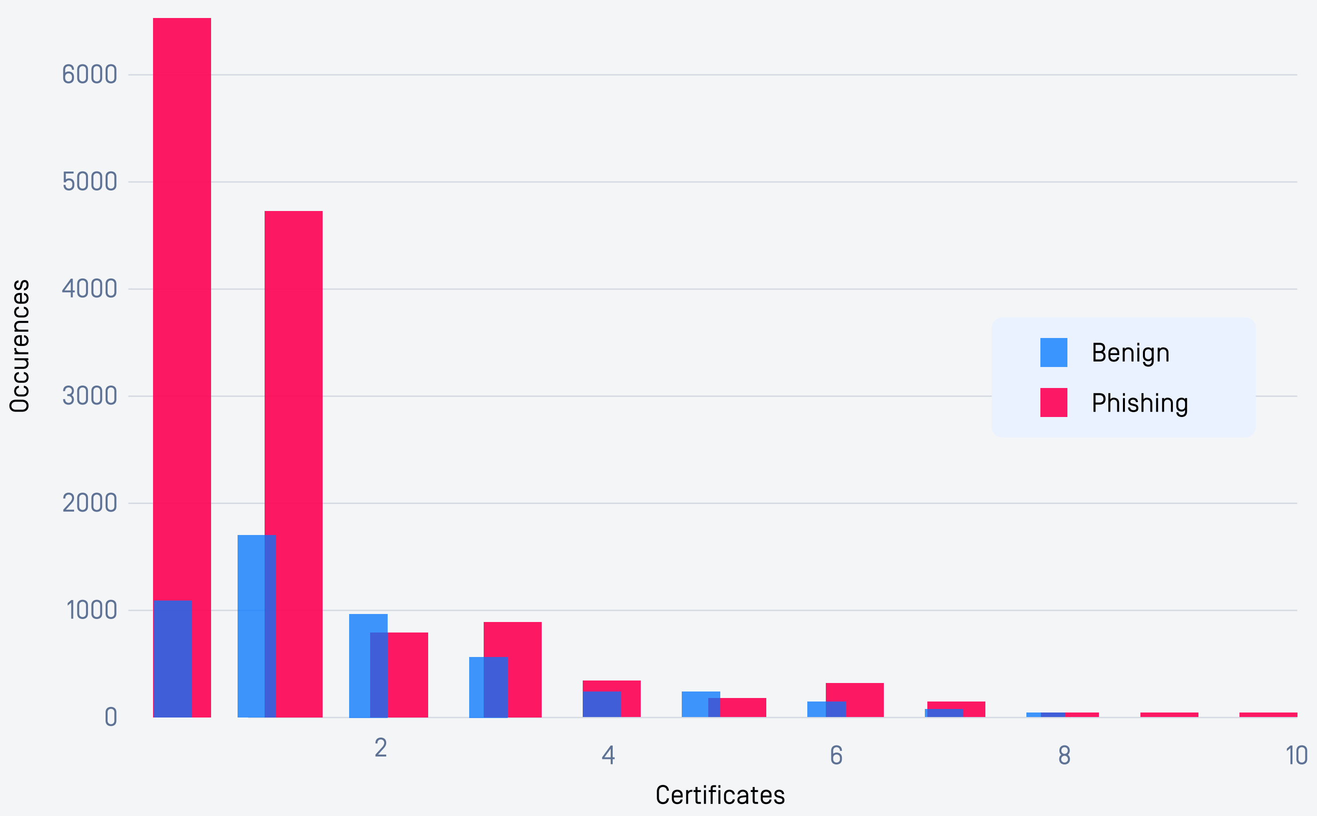
Benign footprint
Benign sessions show higher network complexity scores, reflecting diverse and distributed asset loading.

Phishing footprint
Phishing sessions cluster at low complexity, indicating simple, single-page architectures.

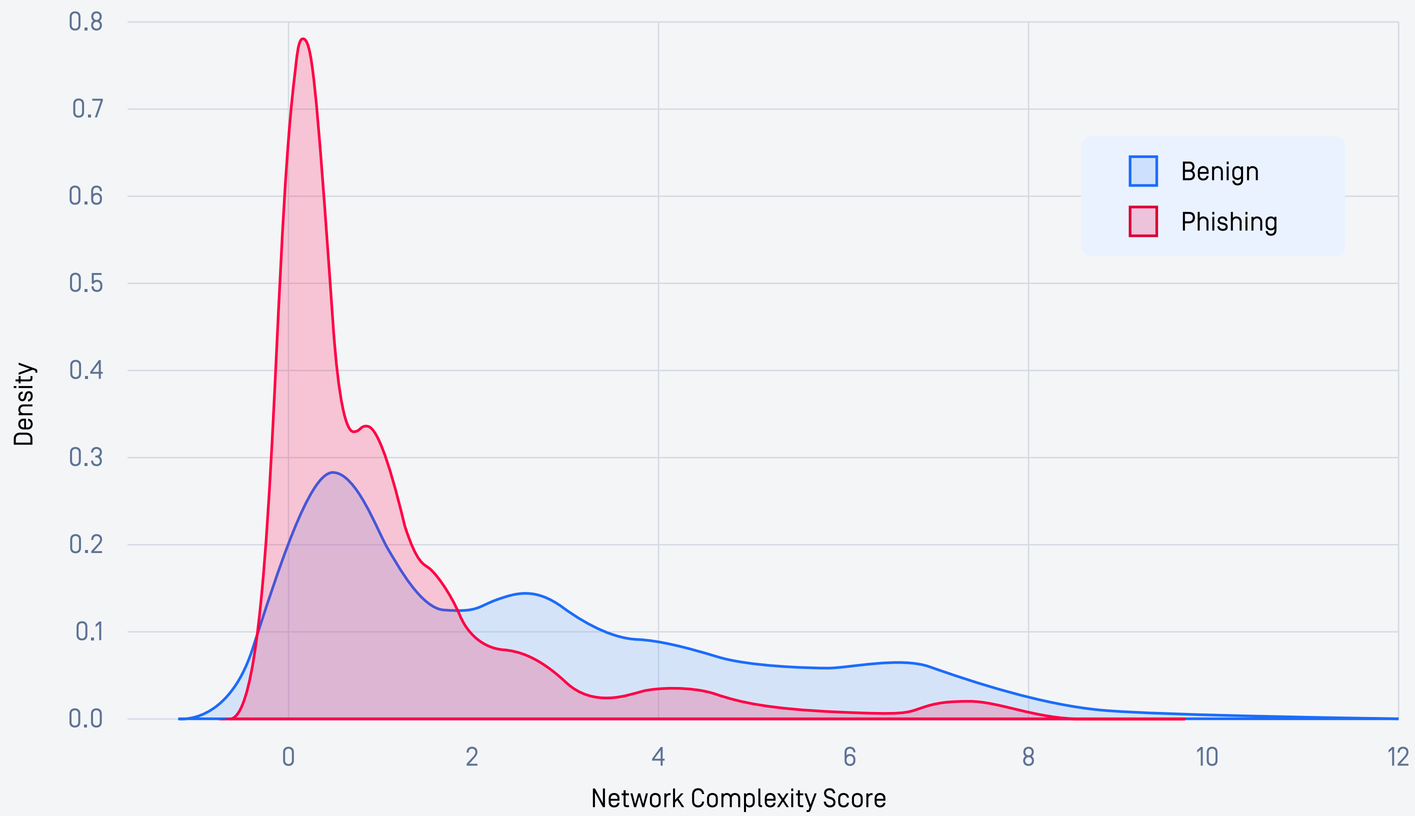
Deduction
Low network complexity is a reliable indicator of phishing, as confirmed by the clear separation in the KDE plot.

Operational Rule
Low network complexity is a strong phishing indicator.

Occurrences of Certificates for Benign and Phishing URLs



KDE (Kernel Density Estimate) of Certificates



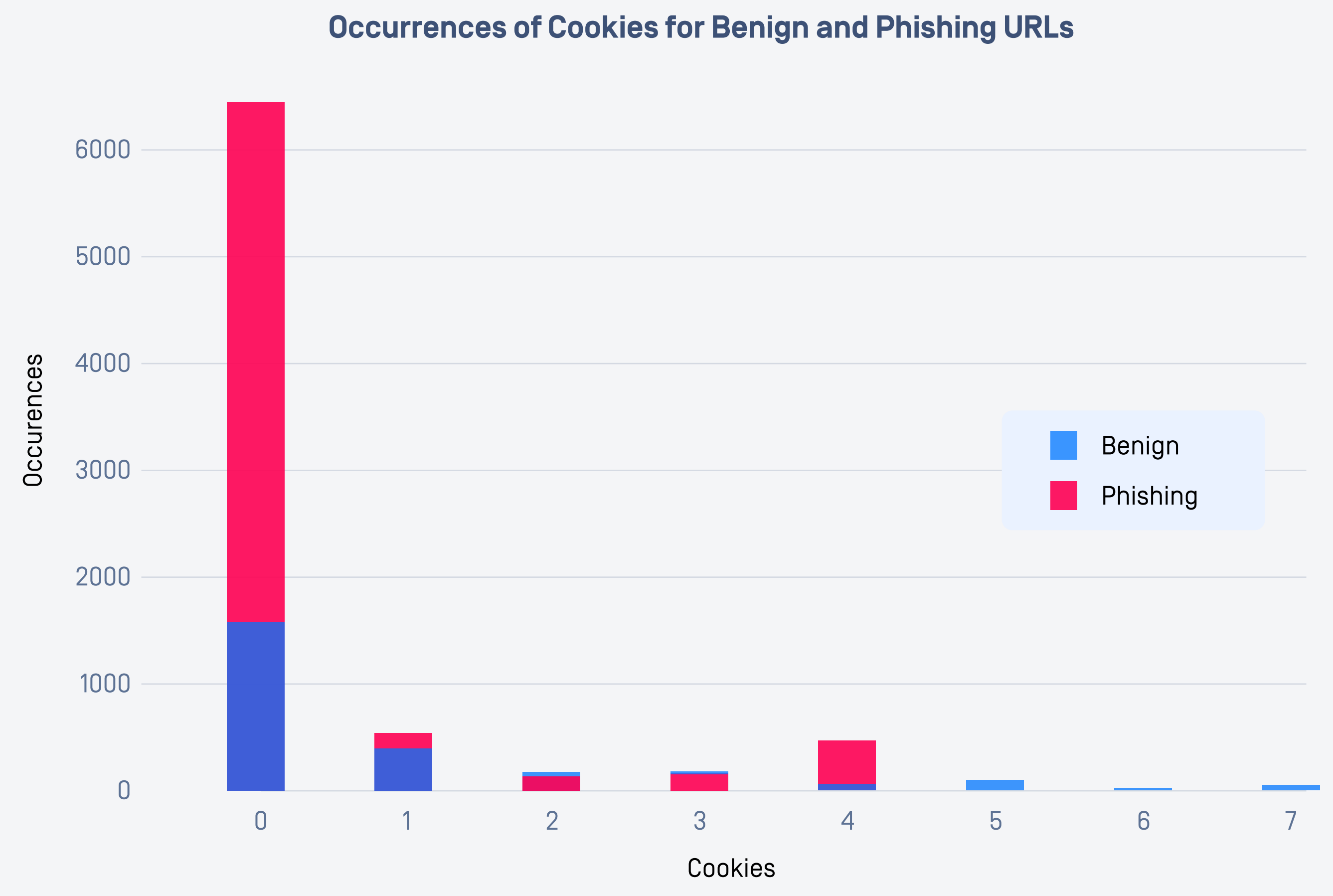
Certificates: A Strong Discriminator

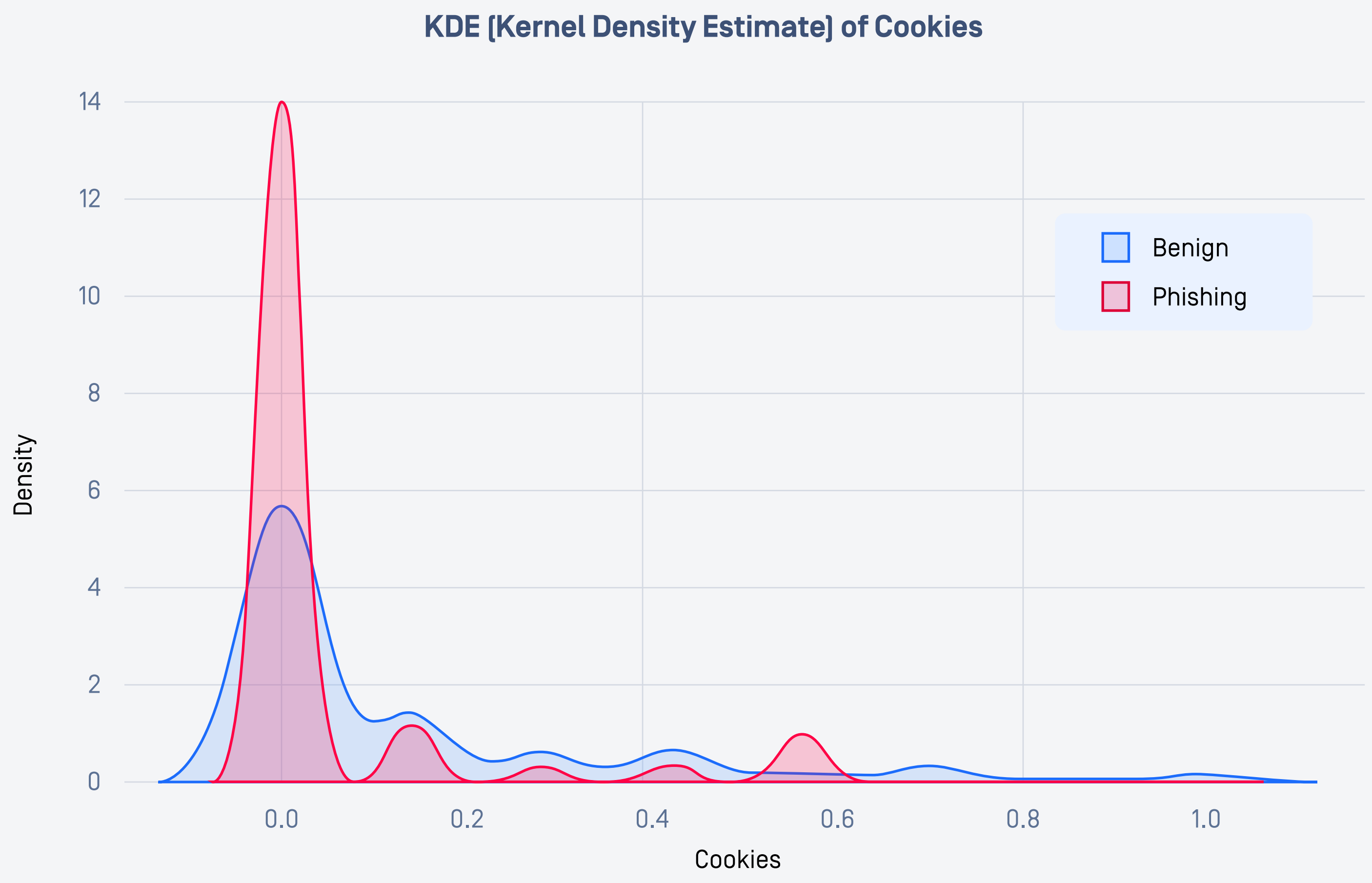
Benign footprint
Benign sessions almost always present at least one certificate, often more, reflecting standard security practices and asset diversity.

Phishing footprint
Phishing sessions overwhelmingly have zero or only one certificate, indicating a lack of proper TLS setup and minimal infrastructure.

Deduction
Sessions with fewer than two certificates are highly likely to be phishing. This is visually confirmed by the sharp drop-off in the phishing distribution on both the bar and KDE plots.

Operational Rule
If the number of certificates is less than 2, the session is highly likely to be phishing (82.1% of such cases are phishing).





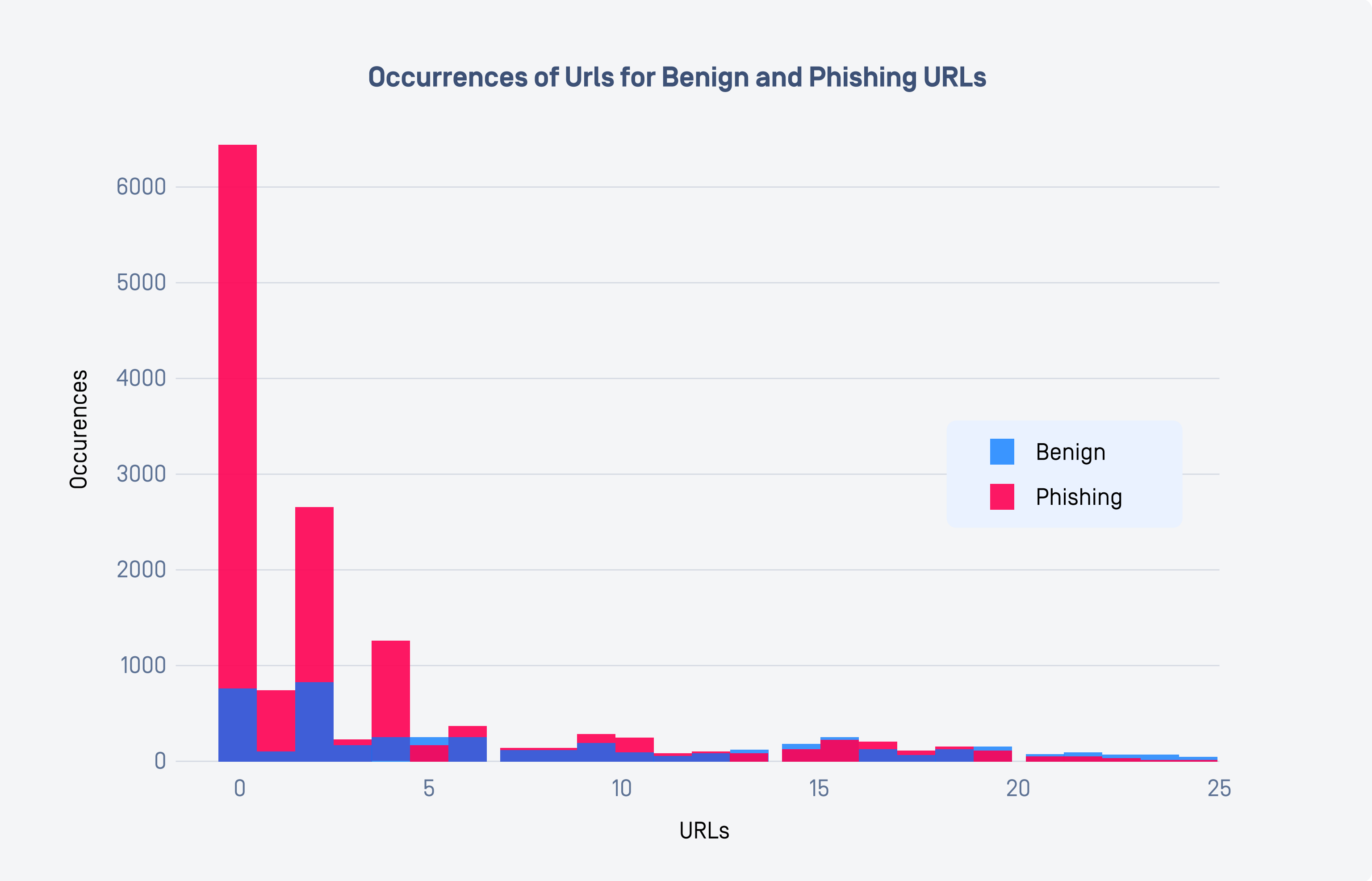
Cookies and Secure Cookies: Absence Signals Phishing

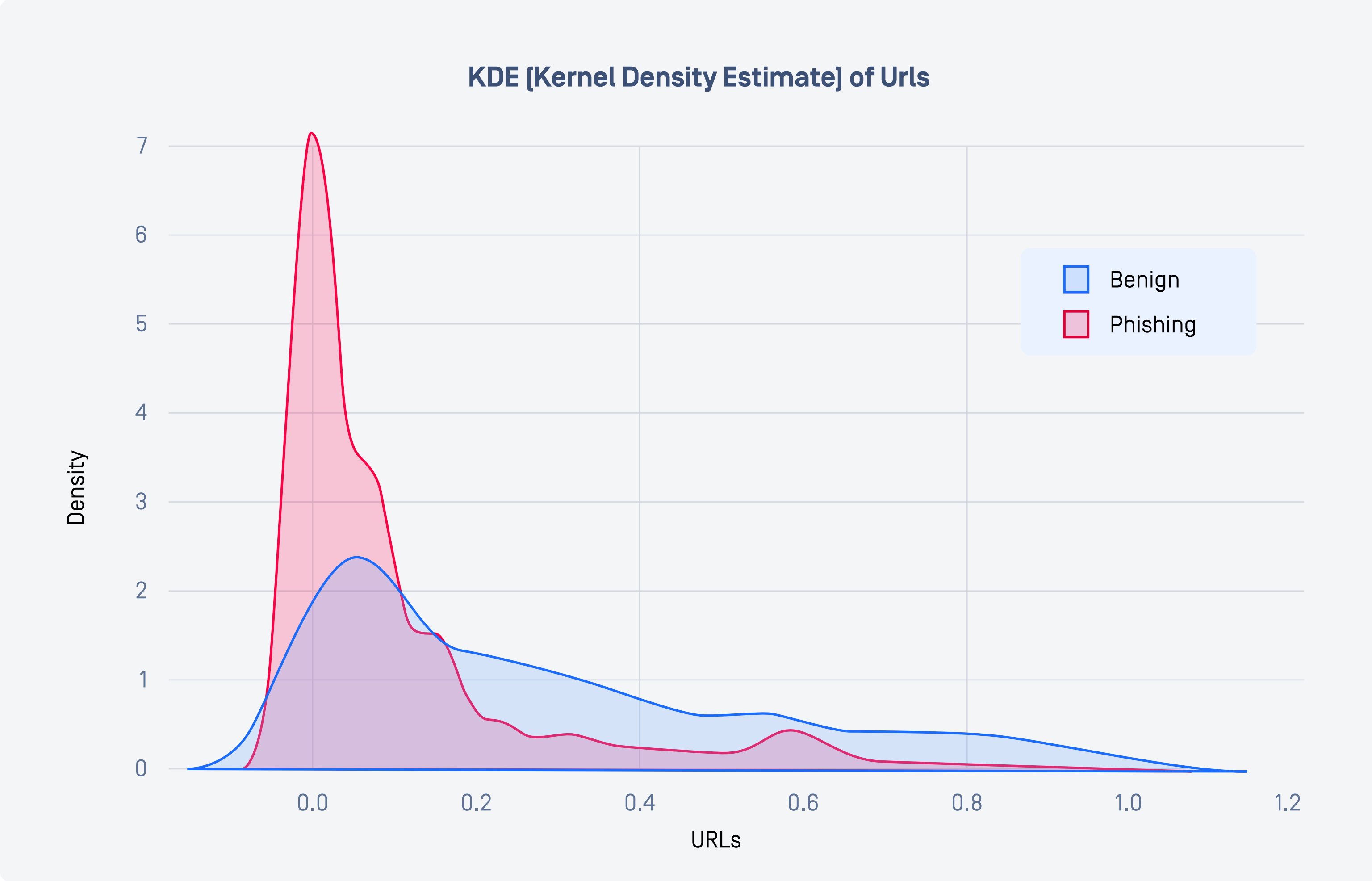
Benign footprint
Legitimate sites routinely set multiple cookies, including secure cookies for authentication, user preferences, and analytics.

Phishing footprint
Phishing sessions rarely set any cookies, and secure cookies are almost entirely absent.

Deduction
The absence of cookies, especially secure cookies, is a strong negative signal for legitimacy. The plots show a clear clustering of phishing sessions at zero cookies, while benign sessions are distributed across higher values.

Operational Rule
If cookies or secure cookies are present but certificates are lacking, the likelihood of phishing is over 82%.





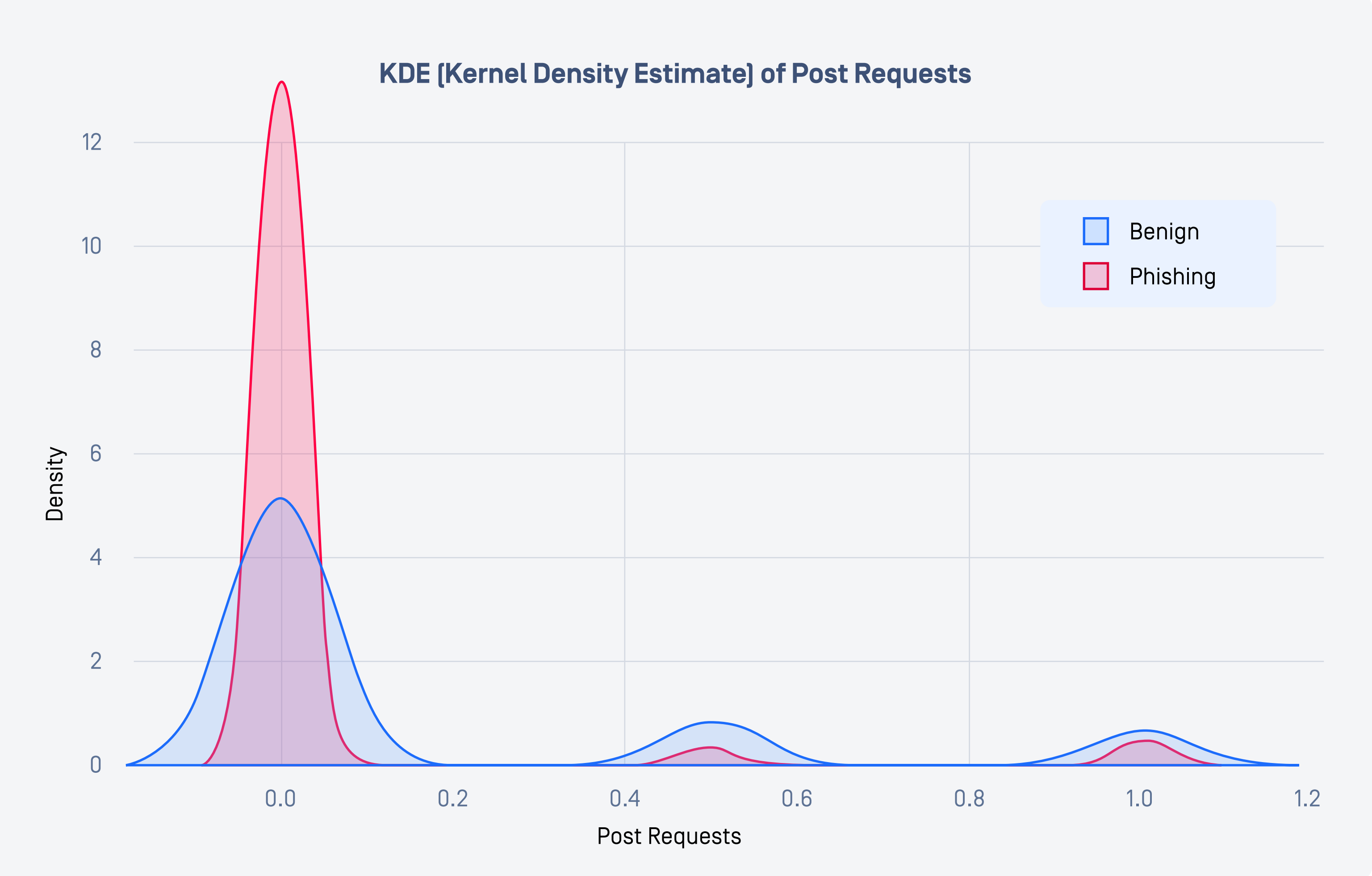
URL Diversity: Legitimate Sites vs. Kits

Benign footprint
Benign sessions load assets from multiple URLs, reflecting the distributed and modular nature of modern web applications.

Phishing footprint
Phishing sessions are typically confined to a single URL or a very limited set, as shown by the sharp peak at zero or one in the phishing distribution.

Deduction
Low URL diversity is a hallmark of phishing kits. Sessions with fewer than six URLs are much more likely to be phishing, as confirmed by the bar and KDE plots.

Operational Rule
If the number of URLs is less than 6 and cookies (or secure cookies) are present, over 83% of such sessions are phishing.



POST Requests: Another Negative Signal

Benign footprint
Benign sessions frequently generate POST requests for logins, forms, and analytics.

Phishing footprint
Phishing sessions rarely make POST requests, or only do so after user interaction, which is often delayed or obfuscated.

Deduction
The lack of POST requests is typical for phishing kits. If POST requests are present but certificates are lacking, the session is likely phishing.

Operational Rule
If certificates are lacking but POST requests are present, the session is likely phishing (82.1%).

Actionable Heuristics

Rule	% Phishing Probability
If cookies ≥ 0 and certificates < 2	82.1%
If certificates < 2 and secure cookies ≥ 0	82.1%
If certificates < 2 and POST requests ≥ 0	82.1%
If URLs < 6 and cookies ≥ 0	83.4%
If URLs < 6 and secure cookies ≥ 0	83.4%

Summary

These heuristics, derived from empirical data and visual analysis, provide high-confidence, low-cost rules for real-time phishing detection. Each rule leverages the clear behavioral gaps between benign and phishing sessions, as seen in the plots. Implementing these checks at the network edge or in SIEM workflows enables rapid identification and containment of phishing threats, with minimal false positives. Combining these rules with existing detection logic can significantly improve coverage and operational efficiency for SOC teams.

Structural Based Attack Insights

Inline Script Usage: A Subtle Legitimacy Indicator

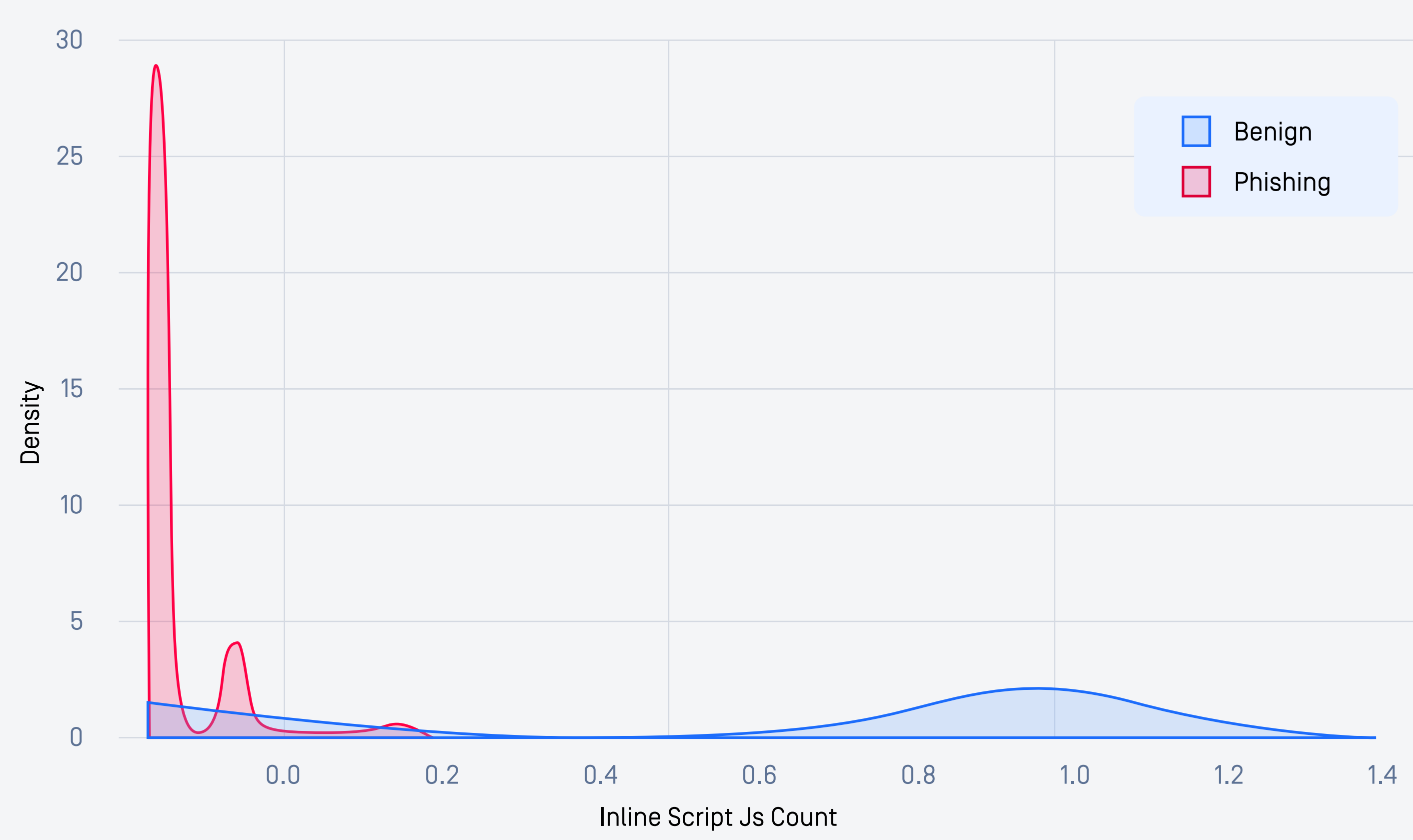
Benign footprint
Benign pages typically have a low inline script JS count, reflecting a preference for loading JavaScript from external resources (CDNs or their own servers) rather than embedding scripts directly in the HTML. This is a hallmark of modern, well-structured web development.

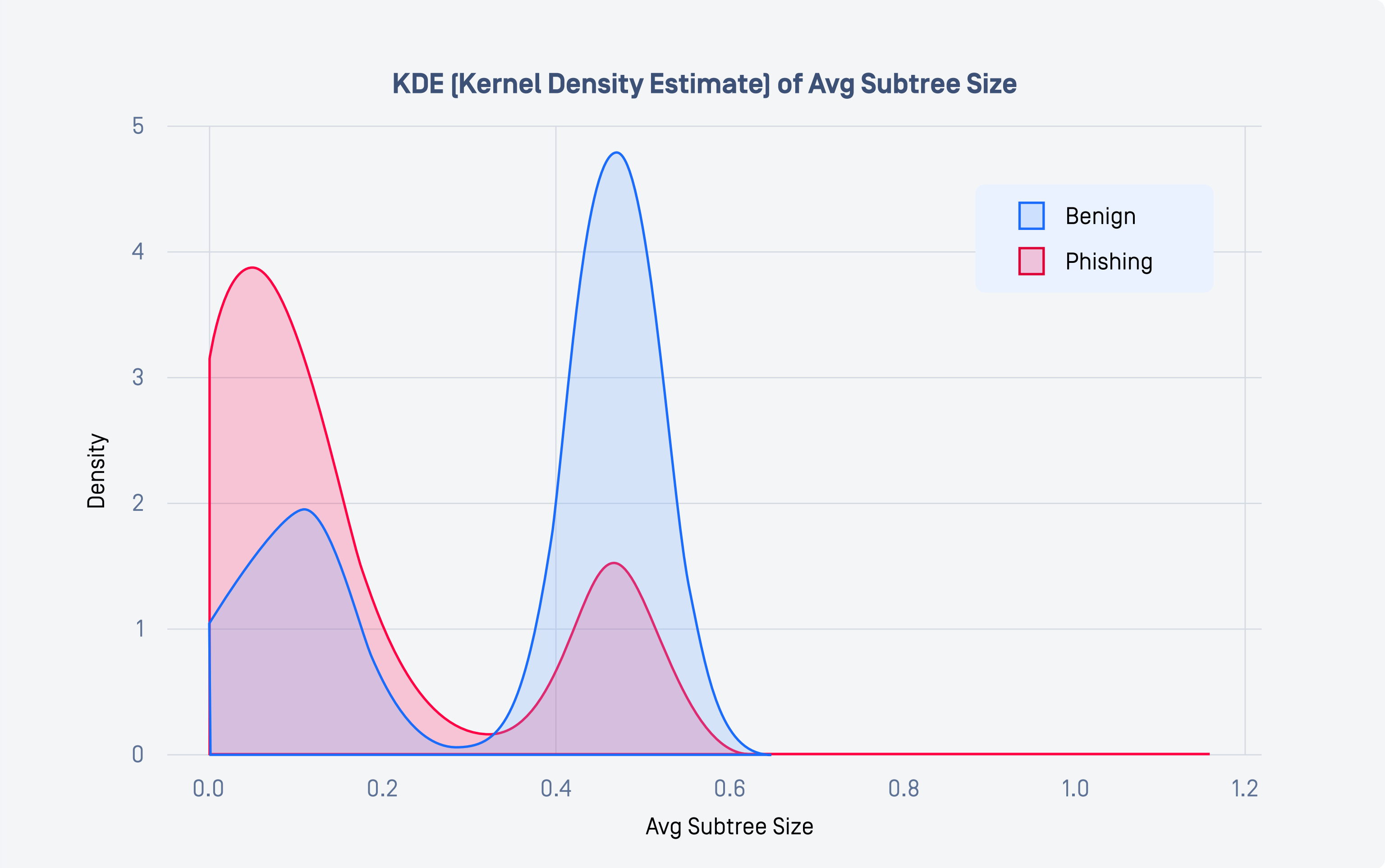
Phishing footprint
Phishing pages show a sharp spike at higher inline script JS counts, indicating a tendency to embed JavaScript directly within the HTML. This approach allows attackers to deliver malicious payloads quickly and avoid detection or blocking of external resources.

Deduction
A high inline script JS count is a strong indicator of phishing, while a low count suggests a legitimate site that relies on external JavaScript files.

Operational Rule
Heavy use of inline JavaScript is a red flag for phishing. Legitimate sites usually keep inline scripts to a minimum and load most JavaScript externally.

KDE (Kernel Density Estimate) of Inline Script Js Count





DOM Complexity: A Hallmark of Legitimacy

Benign footprint
Benign pages peak at higher average subtree sizes, indicating more complex and deeply nested DOM structures. This is typical of modern, content-rich websites that use sophisticated layouts and components.

Phishing footprint
Phishing pages cluster at lower average subtree sizes, reflecting simpler, flatter DOMs. This simplicity is often due to the use of basic templates or minimal content, making the page easier to generate and less resource-intensive for attackers.

Deduction
Low average subtree size is a strong signal for phishing, while higher values are associated with legitimate sites.

Operational Rule
Minimal DOM complexity (low avg subtree size) is a strong red flag for phishing. Complex, deeply nested DOMs are a hallmark of benign pages.

Structural Actionable Heuristics

Rule	% Phishing Probability
If the count of scripts >= 1.00 and the average subtree size < 2.69	82.3%
If the number of DOM nodes < 13.00 and the count of scripts >= 1.00	83.5%
If the count of scripts < 1.00 and the average subtree size >= 2.69	95.8%

Summary

These rules, informed by clear separations in the KDE plots, offer fast and reliable phishing detection by targeting the structural patterns unique to phishing pages. Their simplicity enables efficient, real-time deployment in security systems, reducing false positives and strengthening automated defenses against phishing threats.

04

Modern Threat Detection Pipeline: Why Behavioral Context Matters

As malware continues to evolve beyond static indicators and known signatures, defenders must adopt a new mindset—one that prioritizes execution context over static classification. Today's threats are dynamic, adaptive, and increasingly embedded in seemingly benign activity. From obfuscated loaders and memory-resident payloads to social engineering tactics like ClickFix, attackers exploit blind spots that evade traditional detection systems.

To address this, OPSWAT's file-based Threat Detection Pipeline embraces behavioral analysis at its core. By combining adaptive sandboxing, machine learning, and real-time correlation, the platform reveals how malware behaves—not just what it looks like. This shift from reactive to proactive detection uncovers deeper layers of intent, enabling defenders to expose hidden threats earlier in the kill chain, reduce false positives, and act with greater confidence.

Understanding the intent behind a file or process requires more than just identifying known indicators—it demands visibility into how threats behave across time and context. OPSWAT's detection pipeline is purpose-built to surface these deeper insights. The following three sections break down how behavioral intelligence enables defenders to stay ahead of attackers by mapping their evolution, exposing their obfuscation, and detecting malicious actions cloaked in benign environments. This layered approach forms the foundation for a resilient defense against modern threats.

Iteration is Intelligence: Unmasking Evolutions Through Consistent TTPs

Threat actors regularly pivot their file formats, scripting languages, and delivery methods. However, their TTPs and infrastructure reuse remain trackable. Threat clustering, as demonstrated by Filescan.io, effectively captures these evolutionary footprints.

Beyond Static IOCs: The Imperative of Behavioral Emulation

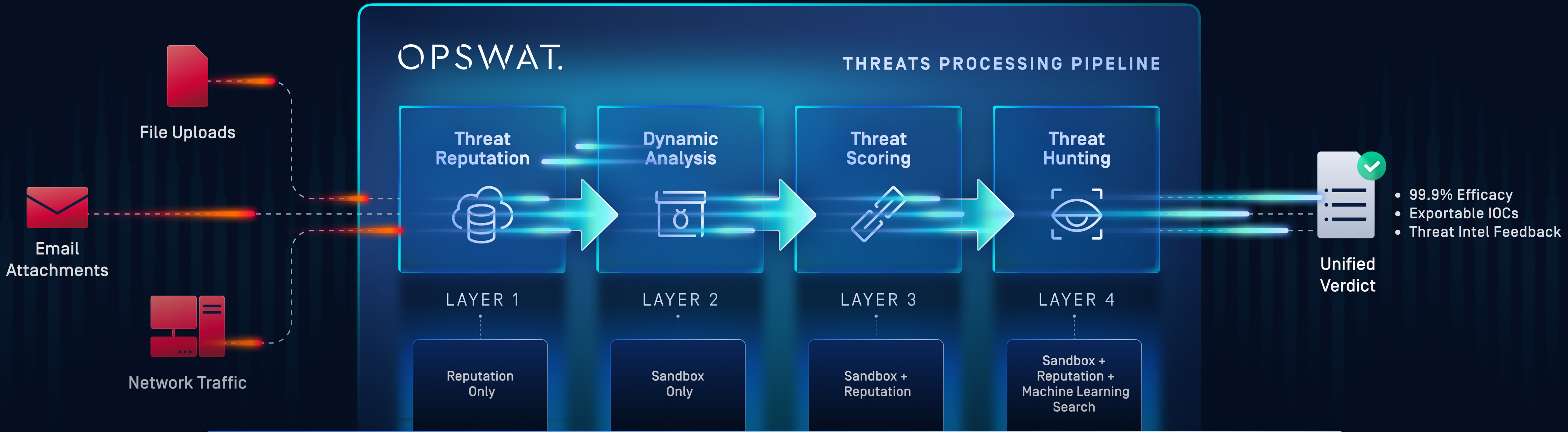
Filescan.io's telemetry reveals that many evasive malware samples were undetected by 90%+ of AV engines at the time of submission. This underscores that traditional file-based indicators are insufficient. Emulation, execution context, and correlation across samples are essential for comprehensive detection.

As we look deeper into correlation, identifying similarities in submissions is a powerful mechanism that empowers analysts to conduct Threat Hunting investigations. Utilizing the Hunting section of the Sandbox, also referred to as Similarity Searching, analysts can pivot across their Threat Intelligence Database to understand more about the evolution of Malware Families such as their behavior and techniques. Analysts can also conduct Threat Hunts from Mitre Att&ck Tactics and Techniques, as well as our in-house library of over 800 Threat Indicators.

Sandbox efficacy: “date_end”: “2025-7-1”, “date_start”: “2025-4-1”

The Camouflage Effect: Detecting Threats in Benign Contexts

Attackers increasingly blend into normal traffic, leveraging benign contexts like QR codes, Google Sheets, and GitHub-hosted payloads. This necessitates a shift in defensive strategies: defense must move from merely blocking indicators to truly understanding behaviors.



File Uploads

Email Attachments

Network Traffic

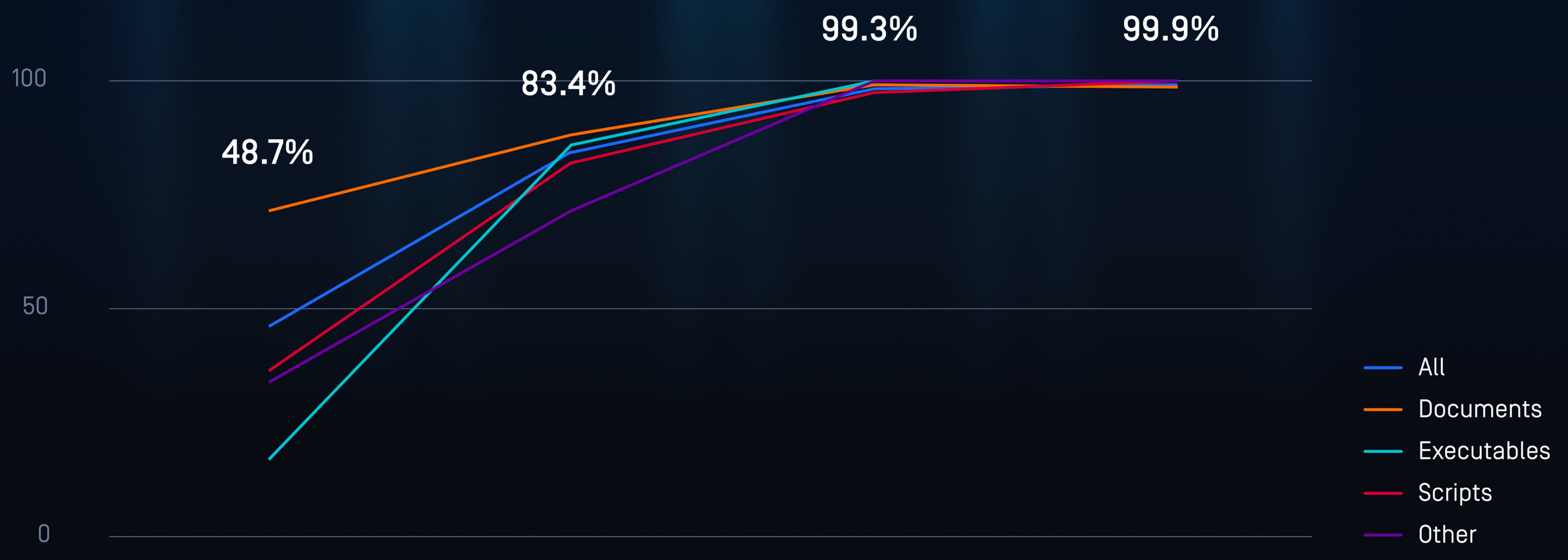
OPSWAT.

THREATS PROCESSING PIPELINE

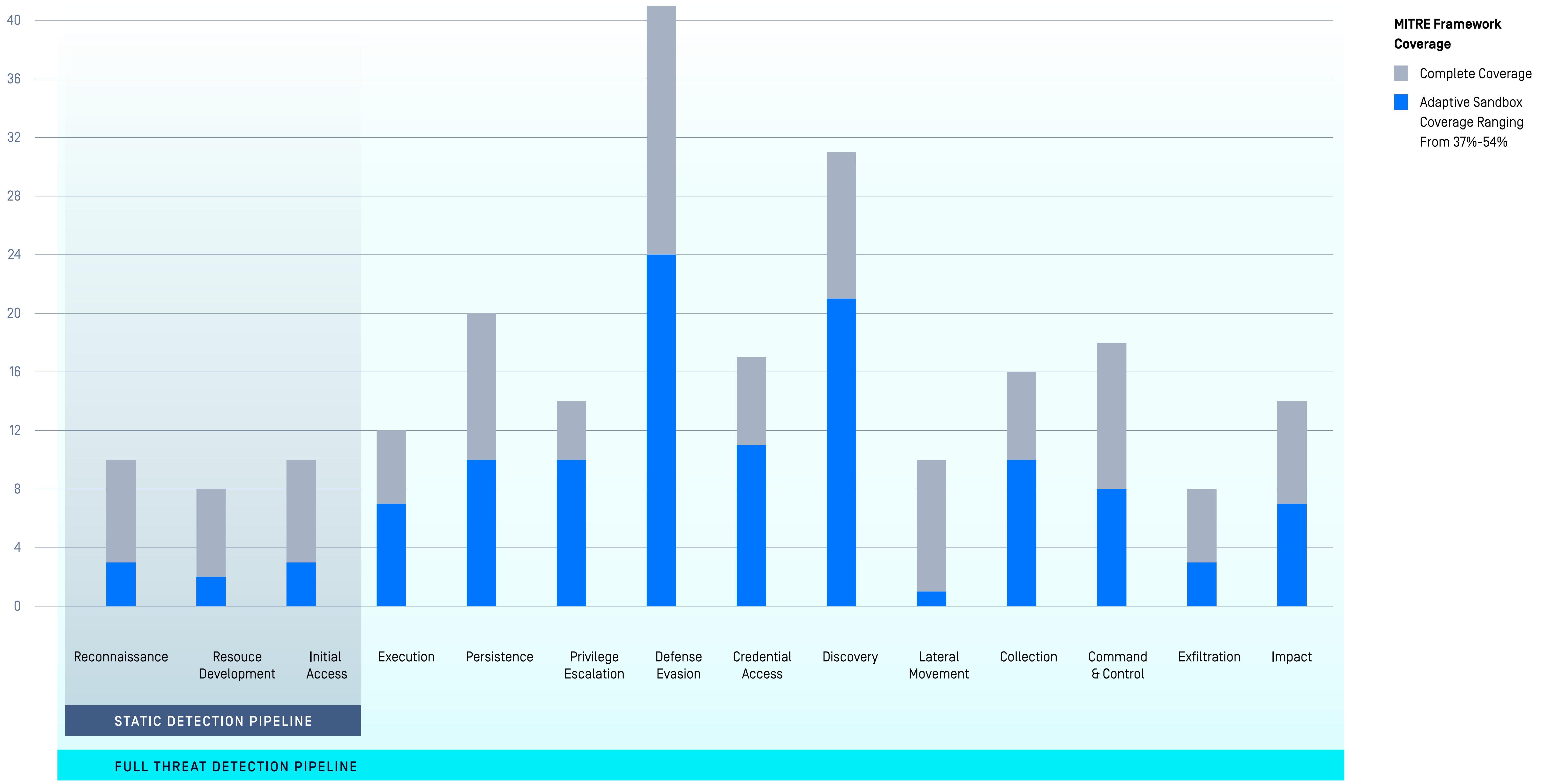
Threat Reputation	Dynamic Analysis	Threat Scoring	Threat Hunting
LAYER 1	LAYER 2	LAYER 3	LAYER 4
Reputation Only	Sandbox Only	Sandbox + Reputation	Sandbox + Reputation + Machine Learning Search

Unified Verdict

- 99.9% Efficacy
- Exportable IOCs
- Threat Intel Feedback



Static Detection vs. Modern Threat Detection Pipeline



05

Introducing Breakthrough Portable Executable (PE) Emulation

OPSWAT is committed to continuously evolving our capabilities to address the dynamic threat landscape. In a significant leap forward, we are integrating a powerful new Portable Executable (PE) emulator into our Filescan.io and MetaDefender Adaptive Sandbox solutions. This enhancement provides unprecedented insight into runtime behaviors that are specifically designed to evade static analysis and traditional sandboxing.

This emulator introduces breakthrough attack vector detection capabilities.
Key advancements include:

Detection of Memory-Only Payloads

By tracing in-memory execution, we can now defeat malware that never touches the disk, such as dynamically decrypted shellcode, process injections, and others, which are invisible to static analysis.

Unmasking Evasive Execution

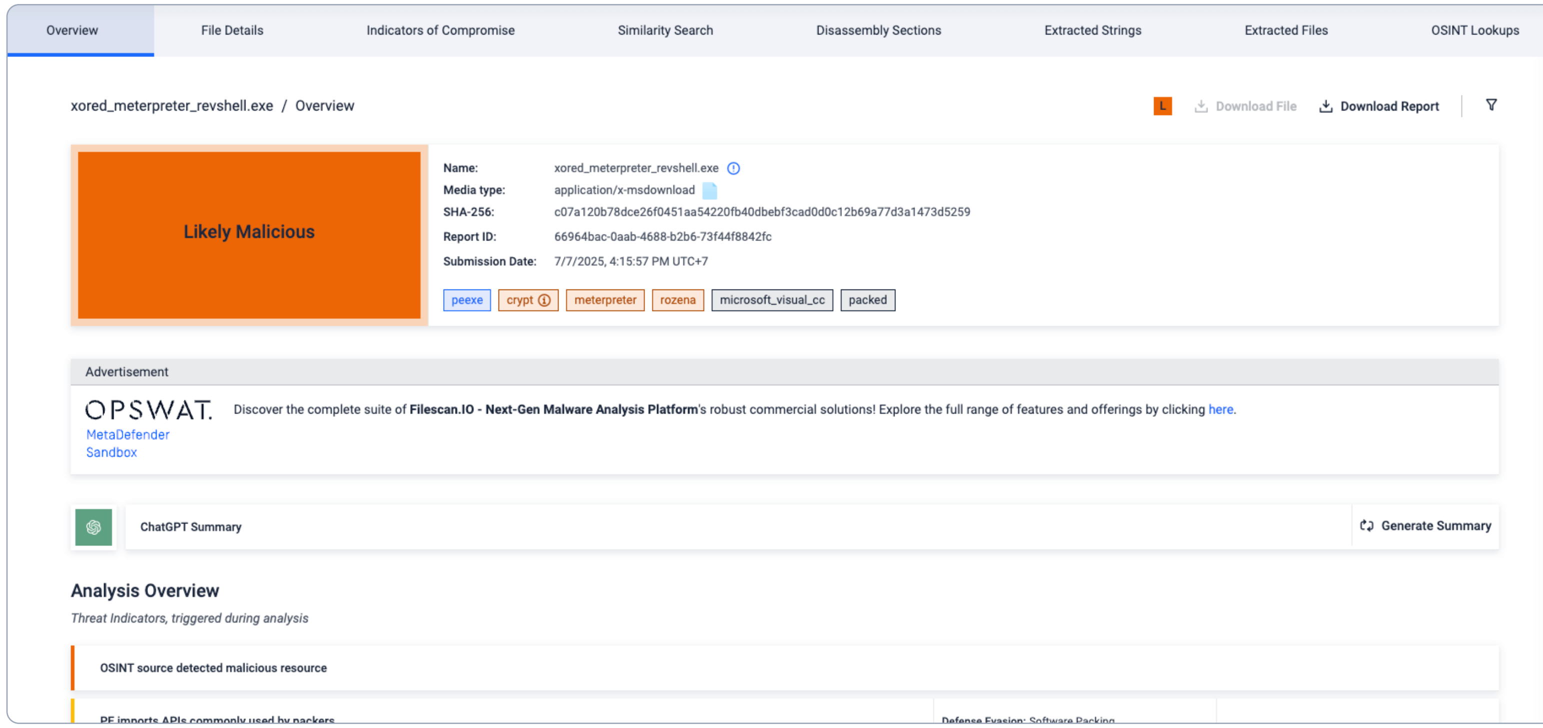
Our emulator traces execution from unconventional starting points, such as TLS callbacks used by APTs to run hidden payloads, and bypasses dynamic API resolution tricks and system checks used to conceal malicious behavior chains.

Live C2 and Payload Analysis

We can now identify and follow malware that uses known and custom packers which involves “section hopping” to execute code from different memory regions, a common tactic for polymorphic loaders and ransomware. Defeating packers enables dynamic payloads and potential malware family attributions.

Filescan.io
Community

To view the links to the Filescan.io reports and access advanced queries, sign up for free here.



xored_meterpreter_revshell.exe / Overview

Name: xored_meterpreter_revshell.exe
Media type: application/x-msdownload
SHA-256: c07a120b78dce26f0451aa54220fb40dbebf3cad0d0c12b69a77d3a1473d5259
Report ID: 66964bac-0aab-4688-b2b6-73f44f8842fc
Submission Date: 7/7/2025, 4:15:57 PM UTC+7

Advertisement

OPSWAT. MetaDefender Sandbox

Discover the complete suite of **Filescan.IO - Next-Gen Malware Analysis Platform**'s robust commercial solutions! Explore the full range of features and offerings by clicking here.

ChatGPT Summary

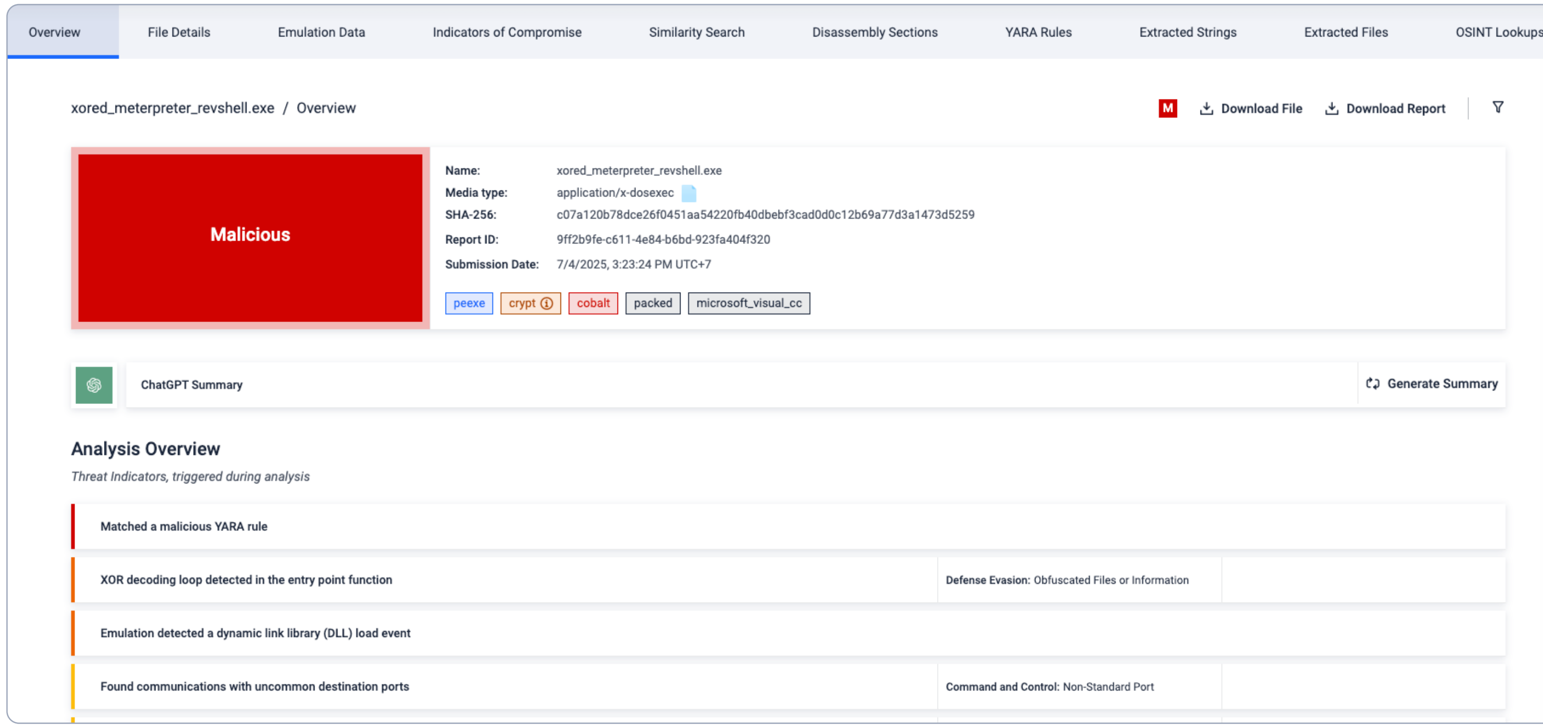
Analysis Overview

Threat Indicators, triggered during analysis

OSINT source detected malicious resource

PE imports APIs commonly used by packers **Defense Evasion:** Software Packing

View the Report



xored_meterpreter_revshell.exe / Overview

Name: xored_meterpreter_revshell.exe
Media type: application/x-dosexec
SHA-256: c07a120b78dce26f0451aa54220fb40dbebf3cad0d0c12b69a77d3a1473d5259
Report ID: 9ff2b9fe-c611-4e84-b6bd-923fa404f320
Submission Date: 7/4/2025, 3:23:24 PM UTC+7

ChatGPT Summary

Analysis Overview

Threat Indicators, triggered during analysis

Matched a malicious YARA rule

XOR decoding loop detected in the entry point function **Defense Evasion:** Obfuscated Files or Information

Emulation detected a dynamic link library (DLL) load event

Found communications with uncommon destination ports **Command and Control:** Non-Standard Port

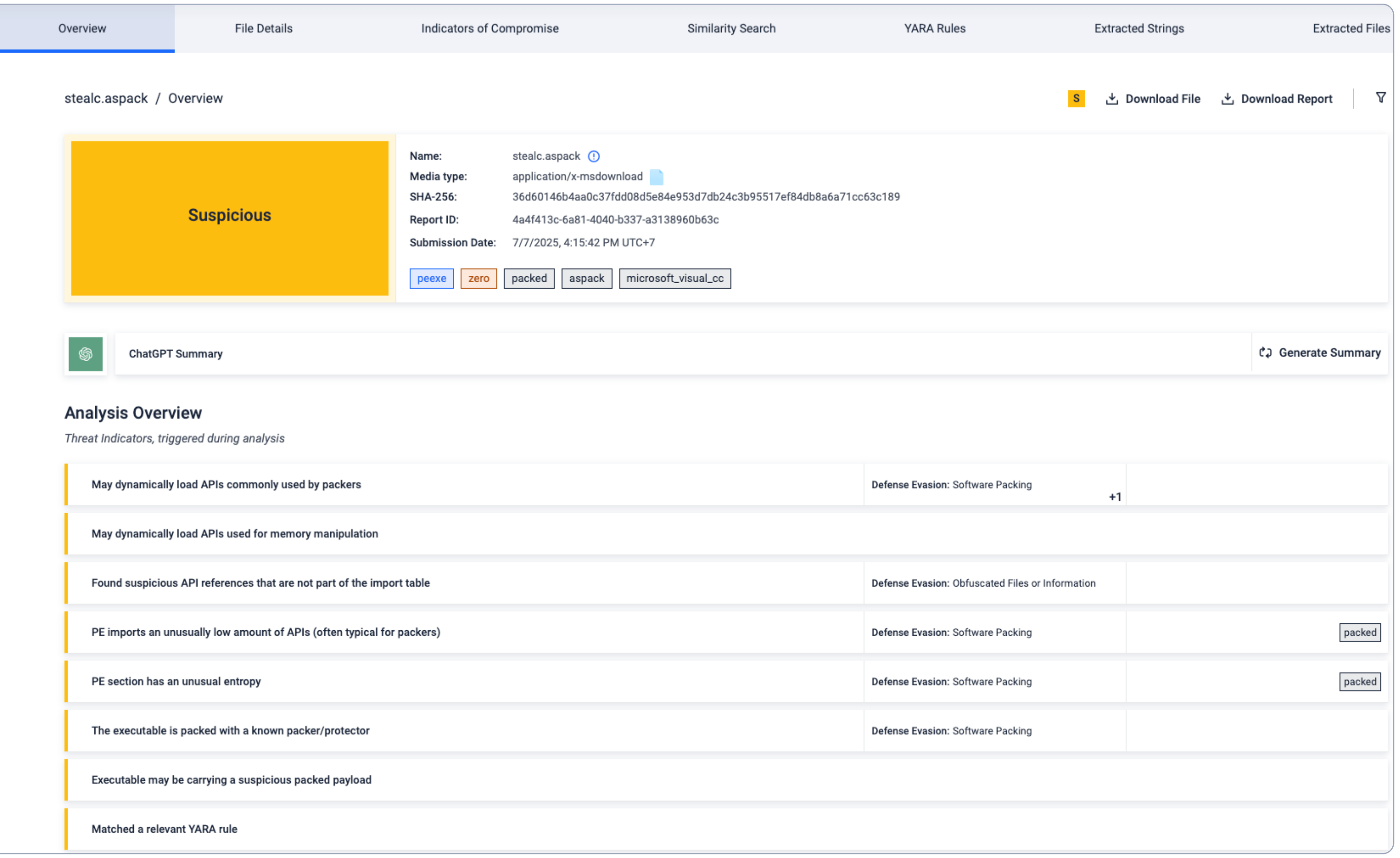
View the Report

Defeating Advanced Packers

We can now identify and follow malware that uses known and custom packers which involves "section hopping" to execute code from different memory regions, a common tactic for polymorphic loaders and ransomware. Defeating packers enables dynamic payloads and potential malware family attributions.

High-Fidelity Behavioral IOCs

This technology allows us to observe MITRE TTPs as they happen, such as the creation of registry autoruns or scheduled tasks for persistence. IOCs are no longer theoretical or heuristic; they are extracted and confirmed from live runtime behavior, providing high-confidence, actionable intelligence for threat hunting.



stealc.aspack / Overview

Name: stealc.aspack
Media type: application/x-msdownload
SHA-256: 36d60146b4aa0c37fdd08d5e84e953d7db24c3b95517ef84db8a6a71cc63c189
Report ID: 4a4f413c-6a81-4040-b337-a3138960b63c
Submission Date: 7/7/2025, 4:15:42 PM UTC+7

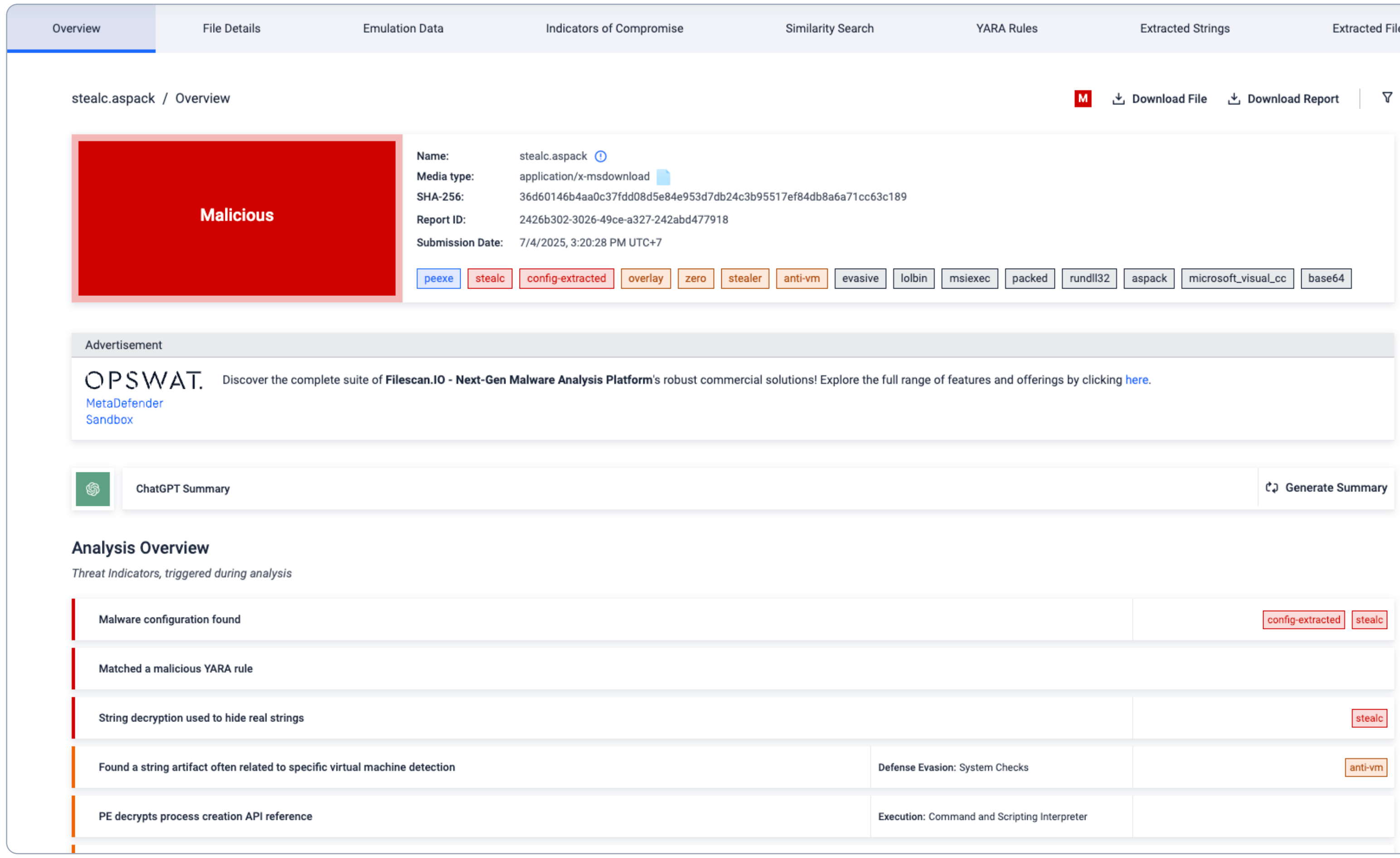
peexe zero packed aspack microsoft_visual_cc

Analysis Overview

Threat Indicators, triggered during analysis

May dynamically load APIs commonly used by packers	**Defense Evasion:** Software Packing +1	
May dynamically load APIs used for memory manipulation		
Found suspicious API references that are not part of the import table	**Defense Evasion:** Obfuscated Files or Information	
PE imports an unusually low amount of APIs (often typical for packers)	**Defense Evasion:** Software Packing	packed
PE section has an unusual entropy	**Defense Evasion:** Software Packing	packed
The executable is packed with a known packer/protector	**Defense Evasion:** Software Packing	
Executable may be carrying a suspicious packed payload		
Matched a relevant YARA rule		

View the Report



stealc.aspack / Overview

Name: stealc.aspack
Media type: application/x-msdownload
SHA-256: 36d60146b4aa0c37fdd08d5e84e953d7db24c3b95517ef84db8a6a71cc63c189
Report ID: 2426b302-3026-49ce-a327-242abd477918
Submission Date: 7/4/2025, 3:20:28 PM UTC+7

peexe stealc config-extracted overlay zero stealer anti-vm evasive lolbin msiexec packed rundll32 aspack microsoft_visual_cc base64

Advertisement

OPSWAT. MetaDefender Sandbox

Discover the complete suite of **Filescan.IO - Next-Gen Malware Analysis Platform**'s robust commercial solutions! Explore the full range of features and offerings by clicking here.

Analysis Overview

Threat Indicators, triggered during analysis

Malware configuration found		config-extracted stealc
Matched a malicious YARA rule		
String decryption used to hide real strings		stealc
Found a string artifact often related to specific virtual machine detection	**Defense Evasion:** System Checks	anti-vm
PE decrypts process creation API reference	**Execution:** Command and Scripting Interpreter	

View the Report

06

Recommendations & Defender Implications

The evolving threat landscape requires a robust and proactive defense strategy, with a well-defined Security Operations Center (SOC) playing a pivotal role. Security Teams must pair strategic priorities with telemetry-driven quick wins and role-tailored playbooks.

> Sandboxing rescues nearly one-quarter of 'intel-silent' files. 1 in 14 are outright malicious.

Strategic Priorities — Remain Ahead of the Curve

Elevate Continuous Detection & Continuous Response
This approach ensures constant monitoring for malicious activities, enabling swift, automated actions to contain and eradicate threats as and when they are identified.

Prioritize Behavioral Analytics and Threat Correlation
By analyzing deviations from normal system and user behavior, alongside correlating disparate security events, organizations can uncover sophisticated, novel threats that evade traditional signature-based detection, whilst also reducing false positives.

Optimize Vulnerability Management
Proactively identify, assess and remediate security weaknesses across systems and applications with risk-based patch prioritization to keep pace with the 45 000-plus CVEs forecast for 2025.

Integrate Regulatory Compliance (NIS 2, EU CRA, SEC cyber-rules)
Undertake as a core pillar of resilience rather than a box-ticking exercise to ensure complete coverage and control implementation.

Telemetry-Driven Actions: What the Data Tells Us to Do Now

Action	Why (H1 2025 telemetry)	Pay-Off
Sandbox every OSINT-silent file.	11788 (45%) objects arrived with an "Unknown" public-intel verdict; sandboxing re-classified **7.3% as Likely/ High-Confidence malicious**.	**Closes the zero-day gap** —1 in 14 formerly invisible threats neutralized within 38s.
Low-link pages (<2) with minimal script payloads (<100B) often indicate hastily deployed phishing traps. Automated crawlers and basic heuristics frequently miss these, making them prime candidates for stealth deployment. Prioritize blocking these thresholds to disrupt bulk phishing ops while minimizing false positives against legit assets.*	This lightweight structural + network heuristic achieved 90.1% hit-rate against live phishing ops.	This heuristic nukes phishing kits before users even touch them, cratering exposure while dumping incident response overhead into the trash.
Feed sandbox IOCs back to OSINT within 24h.	Detonation achieves verdicts ~24h before the first public YARA match.	**Shrinks community detection lag**, boosting collective defense.

Signal details (Selitys)

"Low-link pages" are commonly used in phishing kits to avoid detection, since they aren't deeply integrated into site link graphs.

"<100B script payloads" suggests extreme minimalism—typical of throwaway or rapidly generated phishing kits.

Persona-Specific Playbooks

The development of persona-specific playbooks is crucial for ensuring a coordinated and effective response to cyberattacks. Outlined below are the top priority tasks for each role within Security Operations, with insight into CISO & Risk Owner roles.

Role	Priority Tasks
SOC Operator	▪ Prioritize security alerts based on severity and potential impact, with focus on correlated detections as opposed to alerts in isolation. ▪ Develop Response Playbooks that are inline with the Mitre D3fend Framework empowering analysts to respond effectively using a common language. ▪ Integrate 3rd Party Applications, that can provide reputational and behavioral analysis, with SOAR solutions so that all indicators as part of an alert can receive necessary enrichment with the aim of reducing false positives. ▪ Leverage CMDB repositories as they provide contextual information regarding assets within an organization that can then allow for automated containment through a risk-based approach.
Detection Engineer	▪ Ensure all Detective Controls are mapped to the Tactics, Techniques & Procedures of the Mitre Att&ck framework, with a focus on procedural detections for a more granular threat view. ▪ Conduct Threat Modelling by analyzing Incident and Threat Intelligence Reports to identify missed detection opportunities, providing additional coverage to an organization's detective capability. ▪ Develop Correlation rules that focus on attack chains utilized by Threats Actors. This approach will reduce false positives, increasing the fidelity of alerting. ▪ Pivoting from Threat, ensure detective controls are also focused on Log Ingestion rates & Data Quality to prevent data outages as and when an incident occurs. ▪ Create Threat Monitoring dashboards for high volume-based USE Cases that can be used by Threat Intelligence or SOC Analysts for investigative purposes.
Threat Intelligence Analyst	▪ Contribute to Incident Response by providing critical threat context and insights so that SOC Analysts can respond effectively, with validated intelligence. ▪ Continuously monitor and integrate with external threat intelligence feeds to remain informed with the latest threat indicators. ▪ Automate 1st Level Threat Intelligence processes by integrating multiple reputational services that provide additional contextual awareness regarding an Indicator or Infrastructure identified as part of an attack. ▪ Track & automate the identification of Threat Actor Infrastructure, learning from their behavior and storing accordingly, so that trend analysis can be performed, leading to early alerting for new infrastructure being identified prior to an attack.
Threat Hunting Analyst	▪ Adopt Hypothesis-Driven Investigations that search for anomalous system or user driven activity, uncovering initial access, lateral movement and potential control misuse. ▪ Conduct proactive threat research to uncover the latest adversary TTPs and emerging attack techniques. ▪ Provide Threat Reports that aid the Detective Engineering function in developing new controls to mitigate potential gaps.
CISO & Risk Owner	▪ Define organizational Risk Appetite relative to both the threat landscape and the inhouse capability ▪ Support the development, implementation and testing of Incident Response plans to minimize the potential operational, financial, and reputational impact during an incident. ▪ Strengthen both the existing and onboarding Supply Chain process through vendor risk assessments, strict access controls for 3rd party partners, and continuous monitoring to mitigate risks across the supply chain.

07

KEY TAKEAWAYS & KILL CHAIN COVERAGE

How a Modern Threat Detection Pipeline Closes Security Gaps

The data presented throughout this report highlights a sobering truth: adversaries are rapidly innovating, while many defenders still rely on static signatures and point-in-time tools that fail to keep pace.

From the resurgence of Living-off-the-Land techniques and highly obfuscated .NET loaders, to the weaponization of QR codes and Google infrastructure, it's clear that modern malware is designed not only to evade—but to exploit—the blind spots in traditional security pipelines.

OPSWAT's Threat Intelligence solution directly addresses these challenges through an integrated, adaptive detection pipeline that spans the entire attack chain. By combining reputation checks, behavior-based sandboxing, machine learning (ML) similarity search, and automated threat scoring, the solution bridges critical detection gaps and delivers high-fidelity intelligence for threat hunting, both at speed and at scale.

From Initial Access to Execution: Closing the Entry Points

File-based vectors remain dominant, with archives, PDFs, and HTML files delivering both commodity and custom payloads. In response, OPSWAT applies reputation checks at ingest to immediately filter known bad files while fast-tracking unknowns into the sandbox. Even at this early stage, Filescan.io provides actionable verdicts—reclassifying 7.3% of "intel-silent" files as malicious within seconds, far ahead of OSINT feeds.

Emulation Reveals What Signatures Can't

Throughout 2024–2025, attackers have heavily obfuscated their malware using packers like NetReactor, ConfuserEx, and even steganography. OPSWAT's adaptive emulation sandbox defeats these techniques, tracing behaviors regardless of packaging or evasion logic. This is particularly vital for uncovering script-heavy chains, fileless loaders, and regional payloads that bypass signature-based AV and conventional sandboxes.

Use cases like ClickFix, which hijacks clipboard behavior, or stealthy Bitmap-embedded Snake Keylogger campaigns, show how OPSWAT's sandbox reveals the full execution timeline—even when attackers try to operate in memory only. The result: deeper visibility, clearer attribution, and faster mitigation.

Threat Clustering & Similarity Search: Campaign-Level Context

Unlike static threat feeds that focus on isolated IOCs, OPSWAT's platform applies ML-powered similarity search across all sandboxed files. This enables threat hunting at scale—connecting related samples across campaigns, versions, and evasion techniques. Analysts can pivot on shared TTPs, command-and-control infrastructure, obfuscation patterns, and behavior clusters to track adversary evolution in near real time.

By automatically extracting IOCs and feeding them into both internal and public intelligence systems, this pipeline dramatically reduces the time-to-detection for new malware families, particularly those using malware-as-a-service (MaaS) wrappers or abusing trusted cloud infrastructure like Google Sheets or WebDAV.

Measurable Impact: Over 99% Detection with Full Pipeline

Independent internal efficacy analysis (Q2 2025) confirms that combining OPSWAT's **Reputation + Sandbox + Machine Learning-Powered Similarity Search** yields superior results:

Detection Layer	Total Accuracy (%)
Reputation Only	48.70
Sandbox + Reputation	99.32
Full Pipeline (with Machine Learning Search)	**99.97**

This near-perfect detection is especially critical in categories like scripts and executables, where fileless behavior, LOLBIN chaining, and evasive logic dominate.

Attack Chain Coverage: Mapping Detection to Attacker Tactics

MITRE Phase	OPSWAT Capability
Initial Access	Reputation Check, Phishing Heuristics
Execution	Adaptive Sandbox (Fileless & Script Analysis)
Persistence	PE Emulation, Registry Autorun Detection
Privilege Escalation	Behavioral IOCs, Memory-based Detection
Defense Evasion	Obfuscation Bypass, Packed File Unpacking
Credential Access	Keylogger Detection, Machine Learning Similarity Linking
Command & Control	Detection of Covert Channels (e.g., SaaS C2)
Exfiltration	Network Indicators from Live Payloads
Impact	Threat Scoring, Correlation with Known Campaigns

This integrated attack chain coverage ensures defenders can detect threats at every phase—not just block files at the perimeter. As threat actors evolve, detection must shift from static indicators to dynamic, behavior-based context.

OPSWAT's Threat Intelligence solution transforms raw telemetry into meaningful action—powering real-time analysis, informed threat hunting, and predictive defense across the full attack chain.

Build the best threat detection pipeline at scale with OPSWAT's Threat Detection and Intelligence Solution.

METADEFENDER™

Threat Intelligence

Detect and Contextualize Emerging Threats

Make your organization more resilient to file-based attacks by combining our adaptive sandbox and reputation service to ensure robust detection with an efficacy of 99.9%—enabling fast, informed responses to zero-day threats and evasive malware.

Learn More or Start a Trial

METADEFENDER

Sandbox™

AI-driven analysis that quickly detects even the most evasive malware. With multi-layered, lightning-fast detection and adaptive threat analysis, it provides the deep insights needed to protect critical assets from zero-day attacks.

Learn More

OPSWAT.

Protecting the World's Critical Infrastructure

For the last 20 years OPSWAT, a global leader in IT, OT, and ICS critical infrastructure cybersecurity, has continuously evolved an end-to-end solutions platform that gives public and private sector organizations and enterprises spanning Financial Services, Defense, Manufacturing, Energy, Aerospace, and Transportation Systems the critical advantage needed to protect their complex networks from cyberthreats.

Built on a "Trust no file. Trust no device.™" philosophy, OPSWAT solves customers' challenges like hardware scanning to secure the transfer of data, files, and device access with zero-trust solutions and patented technologies across every level of their infrastructure. OPSWAT is trusted globally by more than 1,700 organizations, governments, and institutions across critical infrastructure to help secure their devices, files, and networks from known and unknown threats, zero-day attacks, and malware, while ensuring compliance with industry and government-driven policies and regulations.

Discover how OPSWAT is protecting the world's critical infrastructure and securing our way of life; visit www.opswat.com.