MSSP Report:

Security Industry Threat Landscape

SOCRadar®
Your Eyes Beyond

socradar.io

The Strategic Case for MSSP Partnership

In a threat landscape where 60% of underground discussions directly reference security vendors and their products, the question is no longer whether your defenses are good enough; it's whether they're being actively monitored, adapted, and evolved. This report examines how threat actors systematically study, test, and bypass widely deployed security products, and why partnering with a Managed Security Service Provider (MSSP) is essential for true operational resilience.

The Pain Point: Organizations invest significantly in security tools, yet face a critical gap. The primary risk is not the absence of security technology; it is the false assumption that products can defend themselves. Threat actors openly analyze security products, share evasion methods, and design malware to pass through common defenses. With 25% of Dark Web posts focused specifically on bypassing security products, even organizations with mature security stacks remain exposed through methods that do not trigger traditional alerts.

The Threat Reality: Dark Web forums, leak sites, and private channels contain frequent references to major security vendors, configurations, and bypass techniques. These discussions often precede real-world incidents by days or weeks. This demonstrates that security tools are not only defensive controls but also active targets of attacker research, making proactive intelligence and human-led operations essential.

The MSSP Advantage: Security effectiveness depends not on what tools you own, but on how they are monitored, interpreted, and adapted over time. An MSSP provides the external threat intelligence, continuous analysis, and operational expertise required to maintain detection capability against evolving evasion techniques. This transforms static product deployment into dynamic, human-led defense.

Why Your Security Stack Alone Is Not Enough

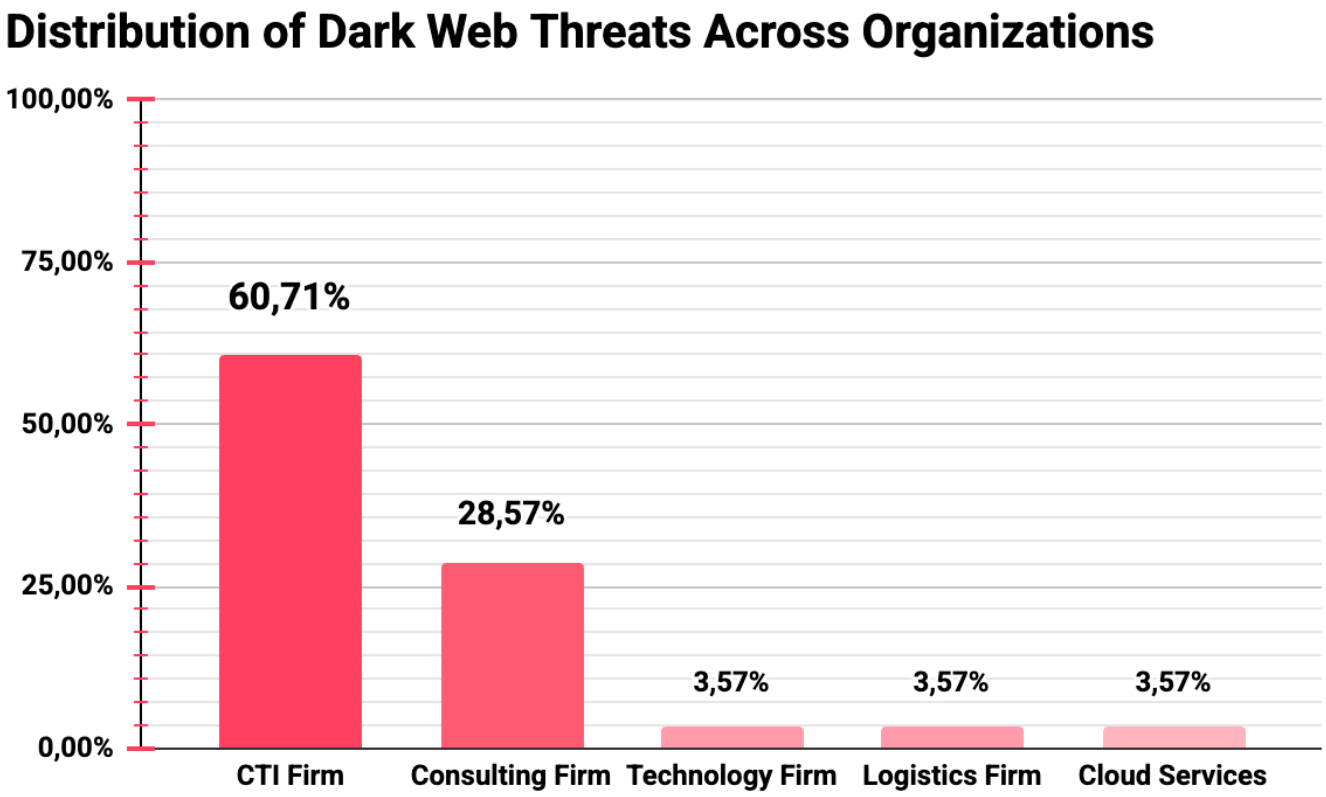
Your security tools, **regardless of vendor or price point,** are commercial software. They are widely deployed, well documented, and tested in predictable ways. This makes them visible not only to your security team but also to threat actors who systematically study how these products work in real environments. No tool, no matter how advanced, operates in isolation from attacker's knowledge.

Security tools create their own attack surface:

- Bypass techniques and exploits for security products are actively traded.
- Evasion methods and misconfigurations are tested before real attacks.
- Control effectiveness depends on continuous monitoring against attacker behavior.
- Most organizations lack the resources to sustain this in-house.

The data speaks clearly: approximately 60% of all collected posts and discussions in underground forums directly reference CTI and cybersecurity companies. The organizations responsible for defending others are themselves frequent subjects of attacker research.

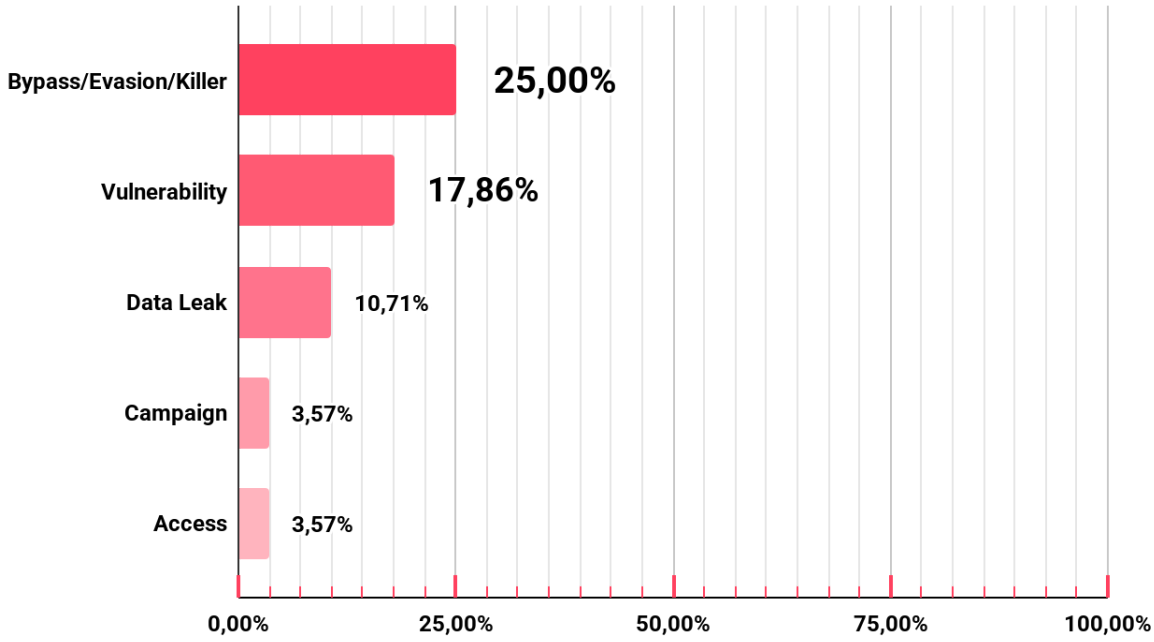
This is the gap that an MSSP strategic partnership addresses.



Threat actors treat your AV, EDR, SIEM, and CTI platforms as attack surfaces, not obstacles. They analyze how these tools detect activity, how alerts are generated, and where blind spots exist. Underground community discussions consistently focus on how to evade, disable, or operate around the very controls you rely on. Without continuous monitoring and adaptation, your security investment may provide a false sense of protection.

Among posts referencing CTI and cybersecurity firms, the dominant theme is bypass and evasion. Approximately 25% of these posts promote or explain services designed to disable, evade, or neutralize security products, including the tools your organization may currently deploy. This is why MSSP partnership is not optional; it is essential for maintaining effective protection.

This is followed by vulnerability related content and Data leaks form the third major category.

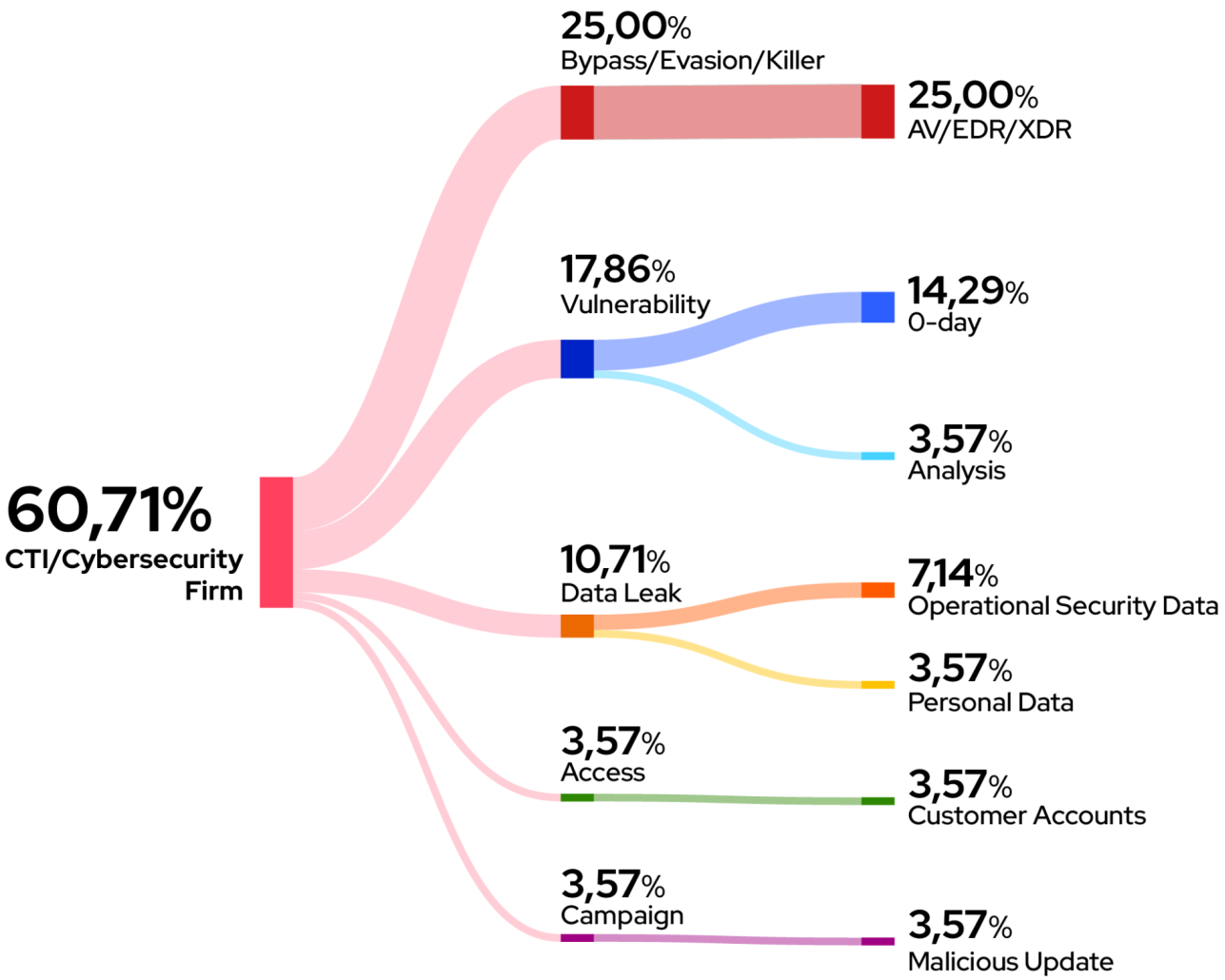


Data leaks and vulnerabilities are just a result; the real problem is how your defense tools are evaded.

How Attackers Target Security Providers: An Overview for MSSPs

When we look into the details of these posts we realize that 0-day vulnerabilities account for 14.29% of the posts, while detailed technical analysis of other vulnerabilities represents 3.57%.

Leaked information from these firms includes operational and security related data at a rate of 7.14%, along with personal data at 3.57%.



Distribution of Dark Web Threats

Dark Web Ecosystem Overview for MSSPs

The research covered several types of underground spaces, each serving a different role in the attacker ecosystem.

- Elite technical forums were monitored for exploit sales, vulnerability discussions, and initial access trading among vetted members.
- Data leak platforms were observed for the distribution of stolen databases and corporate credentials.
- Additional markets also provided visibility into niche exploits and compromised assets.
- Ransomware leak sites and extortion blogs were also tracked to identify victimized service providers before public disclosure.
- Illicit Telegram channels were monitored due to their use for rapid data leakage, real time collaboration, and malware distribution disguised as legitimate updates.

These platforms together form the operational backbone of the cybercriminal economy.

Participants in these communities operate as specialized actors within a supply chain.

- Initial access brokers sell VPN, RDP, and cloud access to corporate environments.
- Malware developers test loaders and stealers against common security stacks.
- Ransomware affiliates seek verified access for deployment.
- Data brokers monetize stolen credentials and internal documents.
- Many actors focus only on selling components that others use during intrusions.

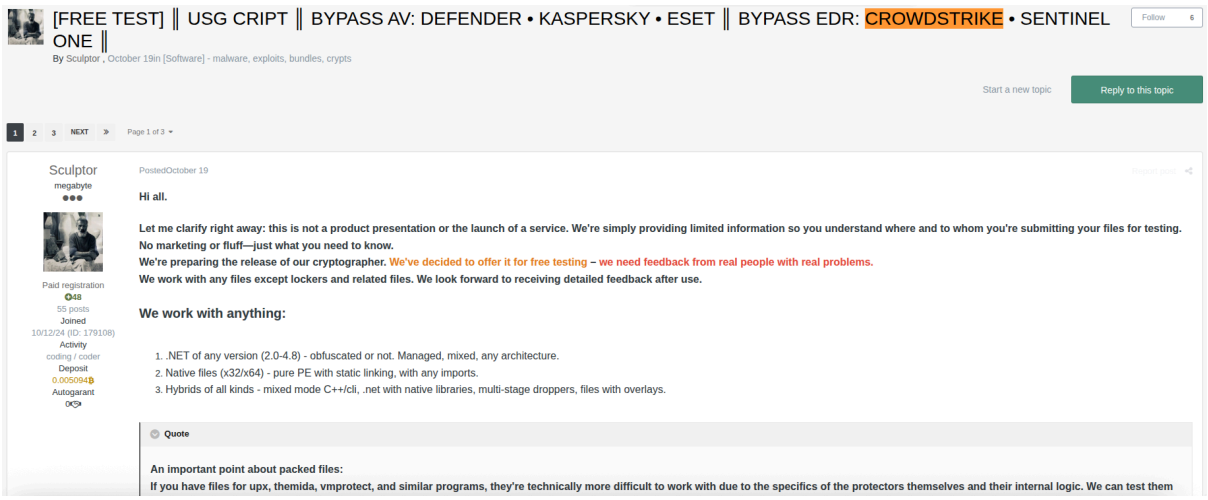
These forums rely on structured trust and reputation systems similar to legitimate marketplaces.

- Vendor ratings, escrow services, and transaction histories are common.
- Sellers often must provide proof of access before a sale is approved.
- Private sections are accessible only to trusted members, and moderators remove fraudulent actors to maintain credibility.
- This structure increases the reliability of claims related to access, data, and bypass methods.

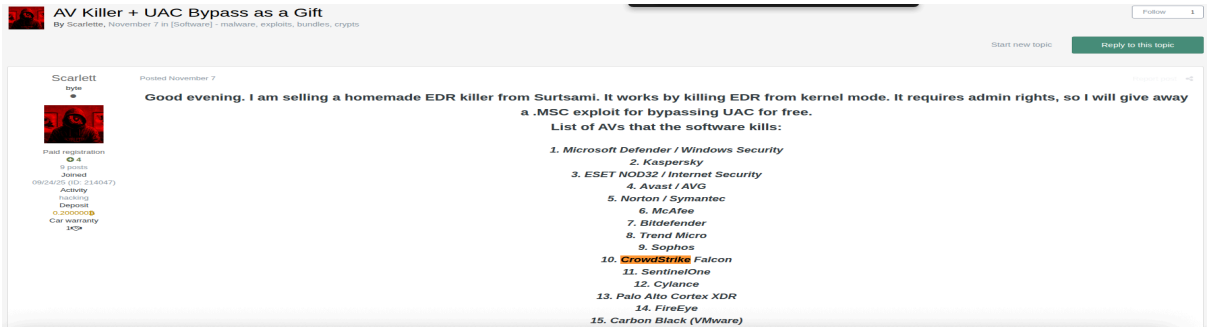
Findings from these underground sources were continuously correlated with threat intelligence enrichment and digital footprint analysis through the SOCRadar Platform. Open source intelligence from social media and technical sandbox reports was used to validate technical claims.

MSSP Takeaways from Threats to Cybersecurity Firms

Bypass/Evasion/Killer Posts

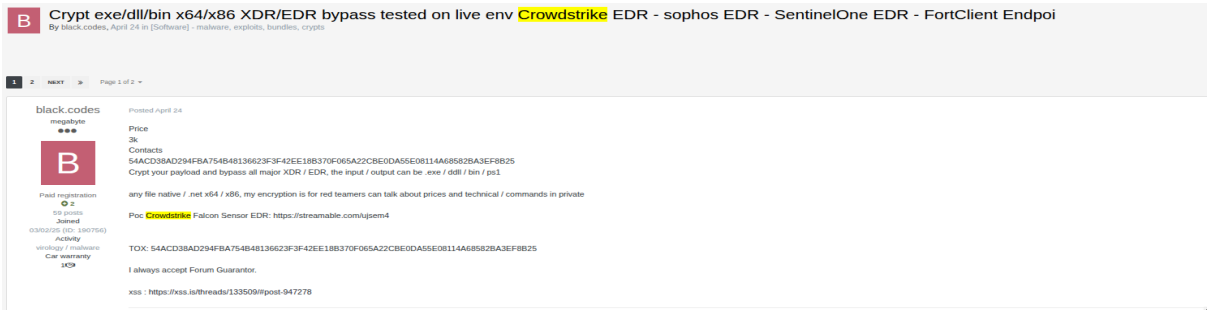


A Dark Web forum post by the actor “Sculptor” promotes a free testing offer for a new obfuscation tool claimed to evade major AV and EDR products, including CrowdStrike and SentinelOne. The actor invites users facing real evasion challenges to test the tool and provide feedback. Such posts often serve as informal field testing for malware packing and obfuscation techniques designed to bypass behavioral and signature based detection.

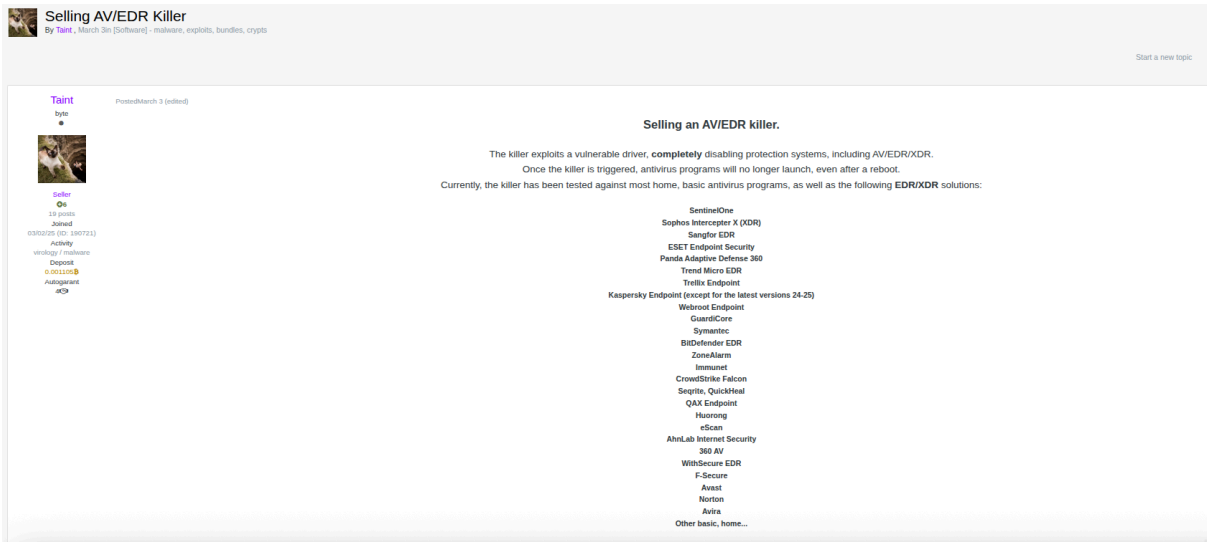


A Dark Web forum post advertises a “homemade EDR killer” combined with a UAC bypass, claimed to run in kernel mode. The seller lists specific targets the tool can disable, including CrowdStrike Falcon, SentinelOne, Palo Alto Cortex XDR, and FireEye. Listings of this type indicate active efforts to develop and commercialize tooling aimed at neutralizing endpoint protection before payload execution.

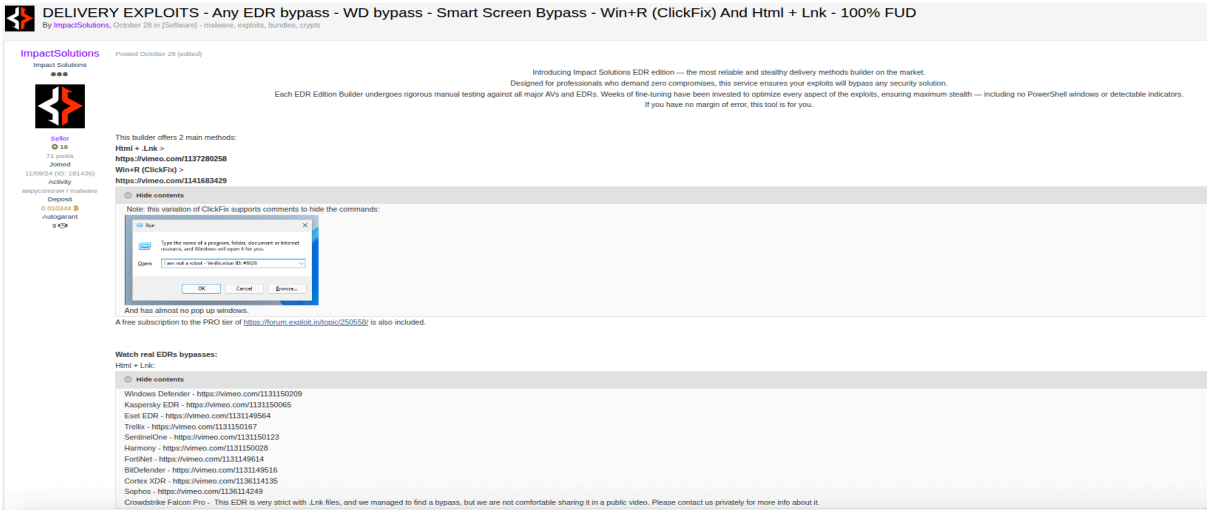
A thread on a Dark Web forum features a technical discussion on evasion methods such as direct syscalls, encrypted strings, and polymorphic execution. The author claims their build avoided detection for 90 days across multiple environments, including those running CrowdStrike Falcon, SentinelOne, and Cortex XDR. Discussions of this nature show how actors exchange practical knowledge to refine techniques that reduce endpoint visibility and delay detection.



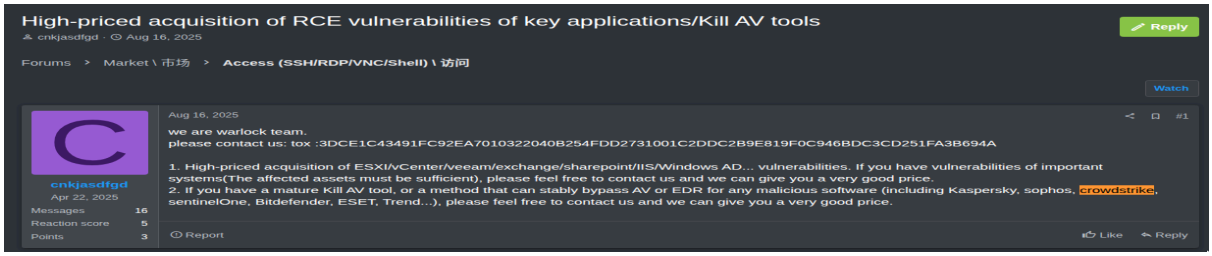
A Dark Web forum post advertises a paid crypting service for executables and libraries, priced at $3,000. The seller claims successful EDR and XDR evasion against products including CrowdStrike, Sophos, SentinelOne, and Fortinet, and shares a proof-of-concept video showing a purported bypass of the CrowdStrike Falcon sensor. The offer is marketed toward those seeking to evade endpoint controls, reflecting the commercial demand for obfuscation services designed to bypass modern detection.



A Dark Web forum post advertises an AV and EDR disabling tool that allegedly abuses a vulnerable driver to neutralize endpoint protections. The seller lists targets including SentinelOne, Sophos Intercept X, CrowdStrike Falcon, and Trellix Endpoint, and claims the tool prevents these agents from starting even after a system reboot. Such offerings highlight continued interest in driver level techniques to impair endpoint defenses before other malicious activity begins.



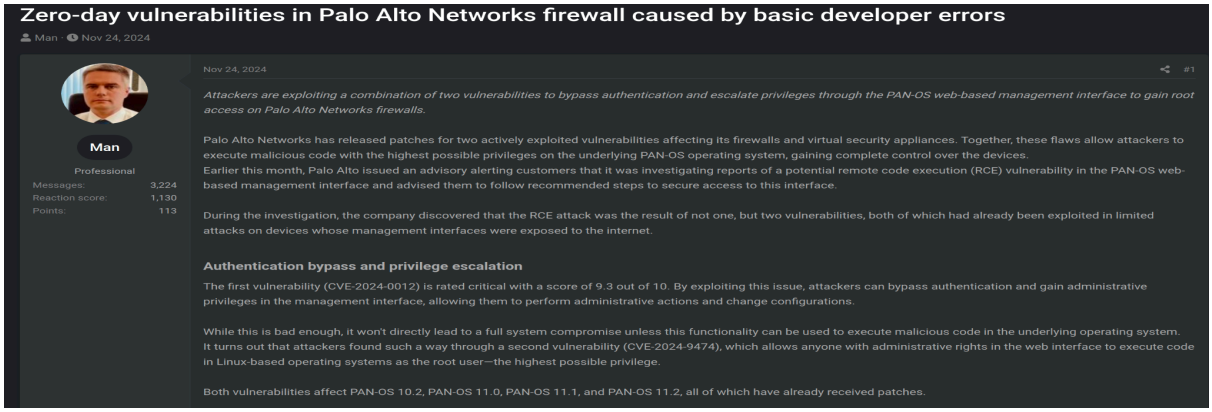
A Dark Web forum post promotes an “EDR Edition Builder” service. The seller shares video demonstrations of bypassing products such as Kaspersky, SentinelOne, and Cortex XDR, and notes having a private bypass for CrowdStrike Falcon Pro that is not disclosed publicly. Posts like this reflect the market for tailored payload builders that prioritize evasion during the initial delivery stage.



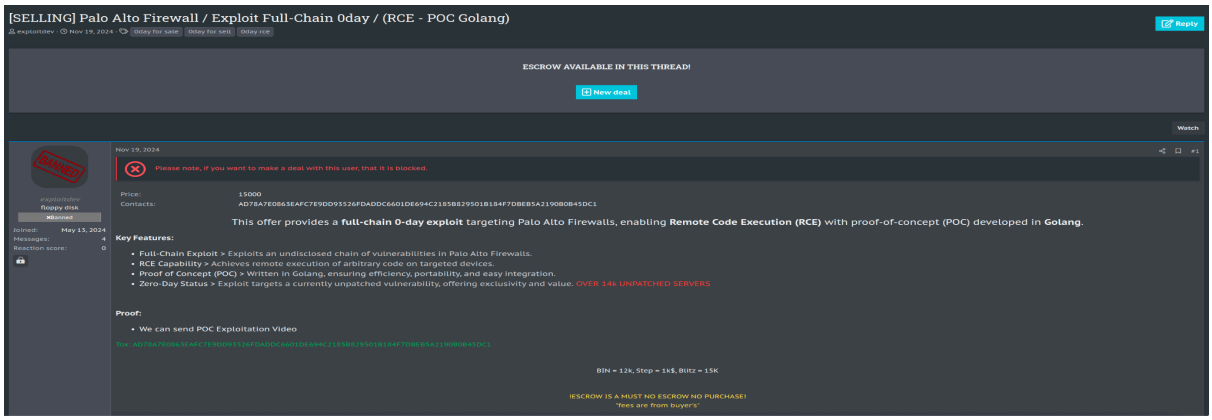
A Dark Web forum post attributed to the “warlock team,” solicits the purchase of mature RCE exploits and reliable “Kill AV” tooling or bypass methods for major endpoint platforms. The request explicitly names CrowdStrike, SentinelOne, Sophos, and Trend Micro. Such solicitations indicate active demand for proven techniques that can disable or evade endpoint defenses as part of intrusion workflows.

Vulnerability Posts

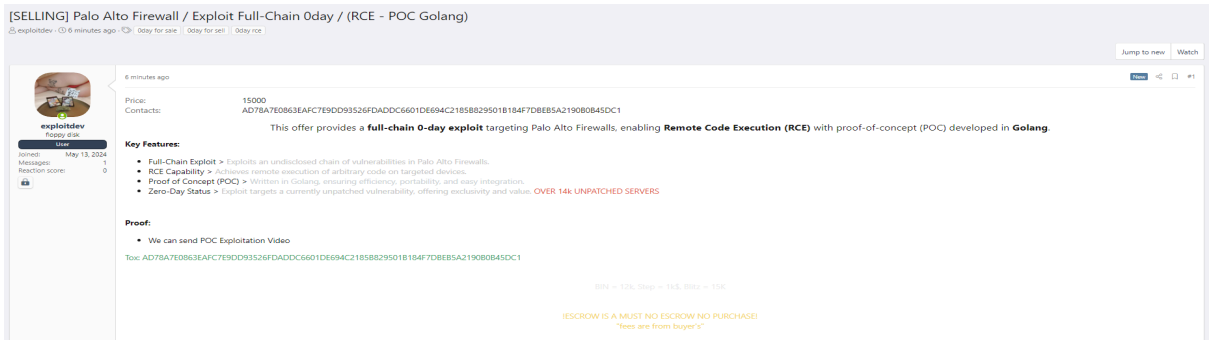
A technical post on a Dark Web forum discusses exploitation of CVE-2023-36874 for local privilege escalation on Windows. The author references CrowdStrike’s public analysis of the zero-day and uses it to explain how the vulnerability can be operationalized. This illustrates how threat actors study vendor research and incident reports to refine exploitation methods and accelerate weaponization.



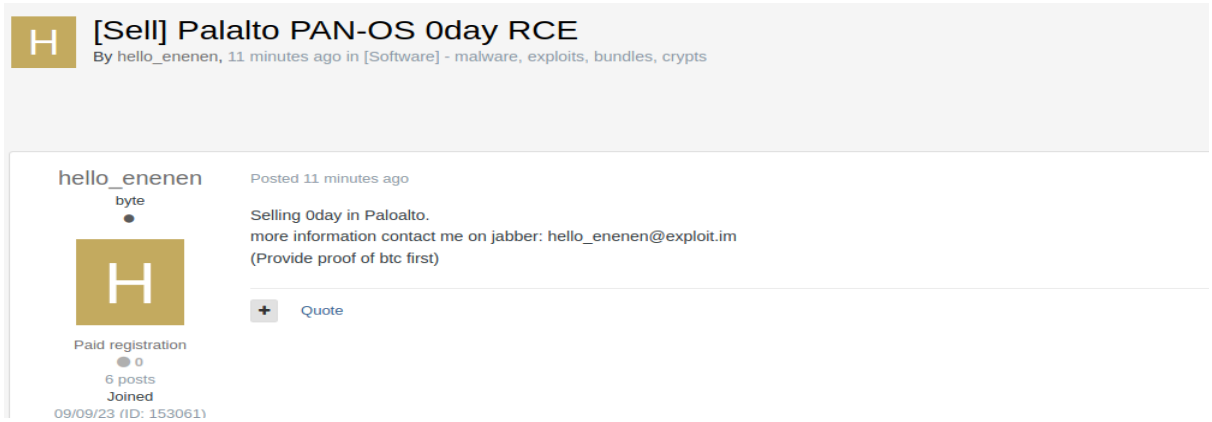
A discussion on a Dark Web forum focuses on the active exploitation of Palo Alto Networks firewall vulnerabilities, specifically CVE-2024-0012 and CVE-2024-9474. They describe how these flaws enable authentication bypass and root level access. The thread reflects how quickly vulnerability details circulate in underground forums once exploitation becomes practical.



A post on a Dark Web forum advertises the sale of a purported full chain 0-day exploit for Palo Alto firewalls, with claimed remote code execution capability and a price of $15,000. The listing underscores the high underground value placed on reliable exploits against perimeter security appliances, which can provide broad network access when compromised.

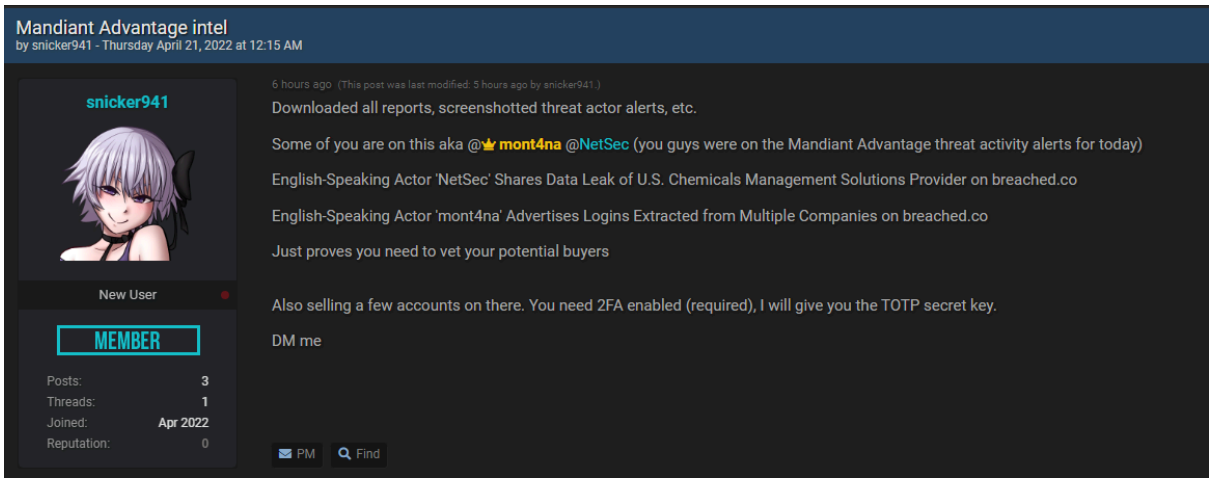


A listing on a Dark Web forum advertises a purported full chain 0-day exploit for Palo Alto firewalls, developed in Golang and priced at $15,000. The seller claims the exploit provides remote code execution and affects more than 14,000 unpatched servers worldwide. The post highlights the underground market value assigned to exploits that target widely deployed security appliances.

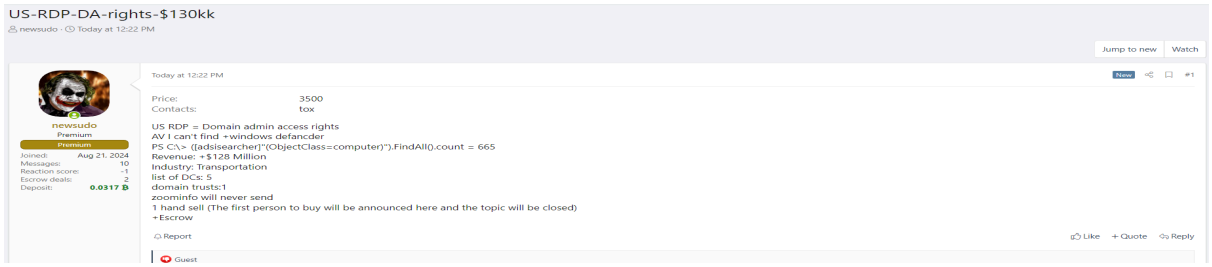


A post on a Dark Web forum advertises a 0-day remote code execution exploit for Palo Alto PAN-OS. The listing contains minimal detail and directs interested buyers to make contact over Jabber, with a requirement to show proof of Bitcoin funds before further information is shared. The post reflects typical underground sales practices for high value exploits targeting widely deployed network security platforms.

Access Sale Posts

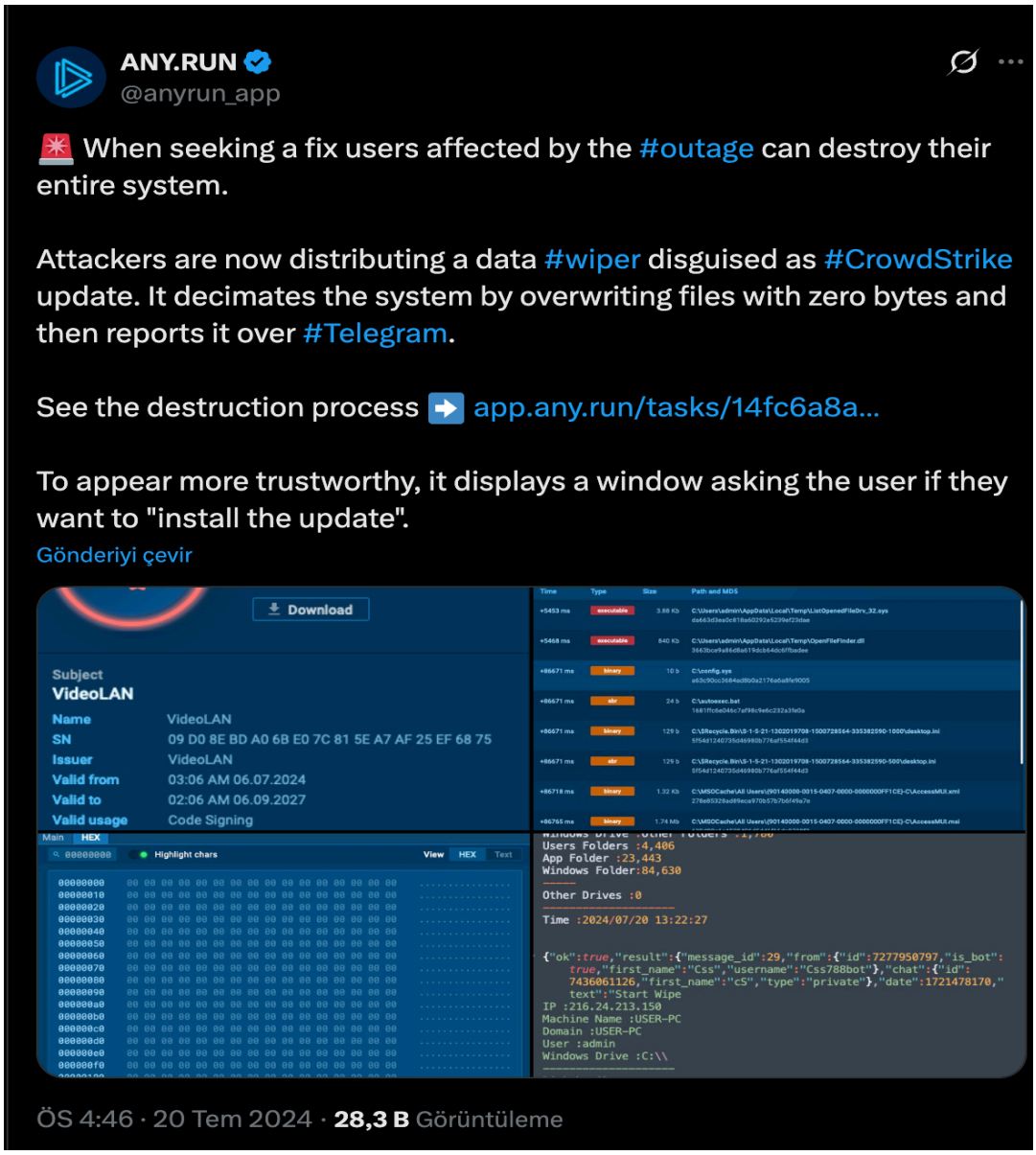


A post on a Dark Web forum advertises the sale of access to Mandiant Advantage accounts. The seller demonstrates visibility into threat activity alerts, implying possible compromise of customer credentials or portal access. Such listings indicate the risk posed when access to commercial intelligence platforms is exposed, as it can reveal sensitive threat reporting and customer specific insights.



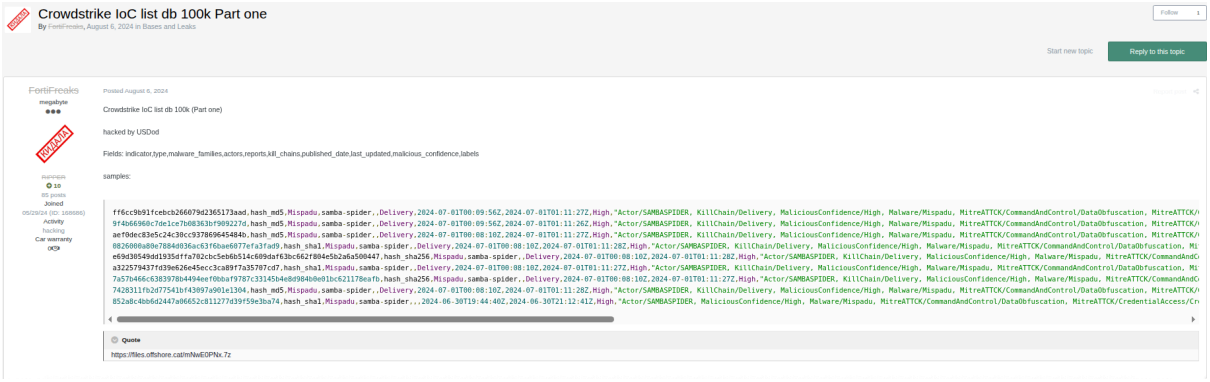
A post on a Dark Web forum offers Domain Admin access to a US transportation sector company for $3,500. The seller notes the organization’s reported revenue and states that Windows Defender is the only active antivirus observed, implying limited endpoint protection maturity. Listings of this type show how verified administrative access to mid sized enterprises is commoditized and sold at relatively low prices in underground markets.

Campaign Posts



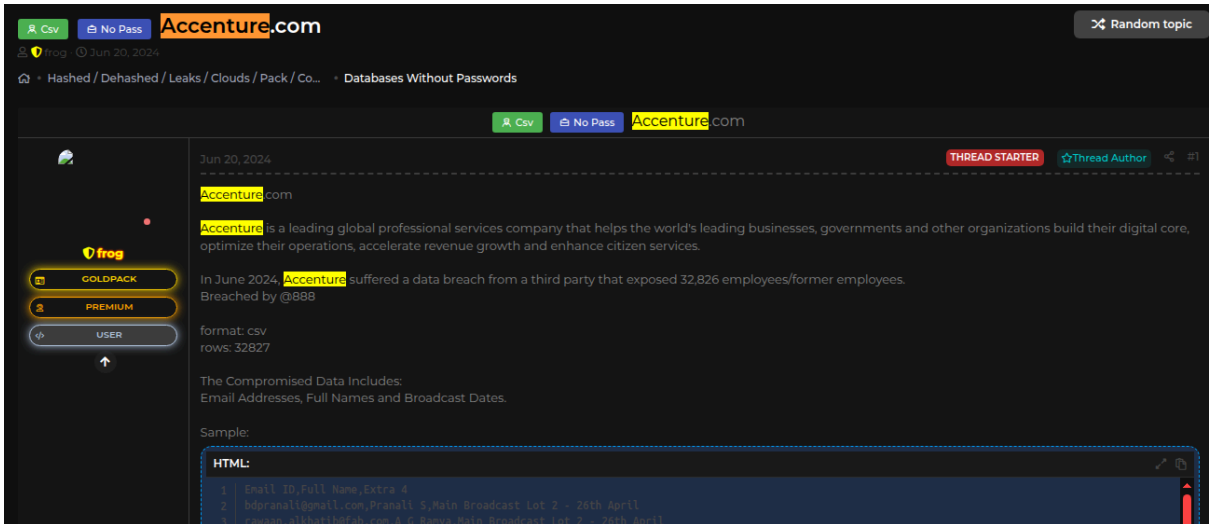
An alert shared via X warned of a malware campaign distributing a data wiper disguised as a CrowdStrike software update following the global outage. Attackers leveraged the vendor's brand and the timing of the incident to increase the credibility of the lure. The case shows how major security events are quickly weaponized.

Data Leak Posts

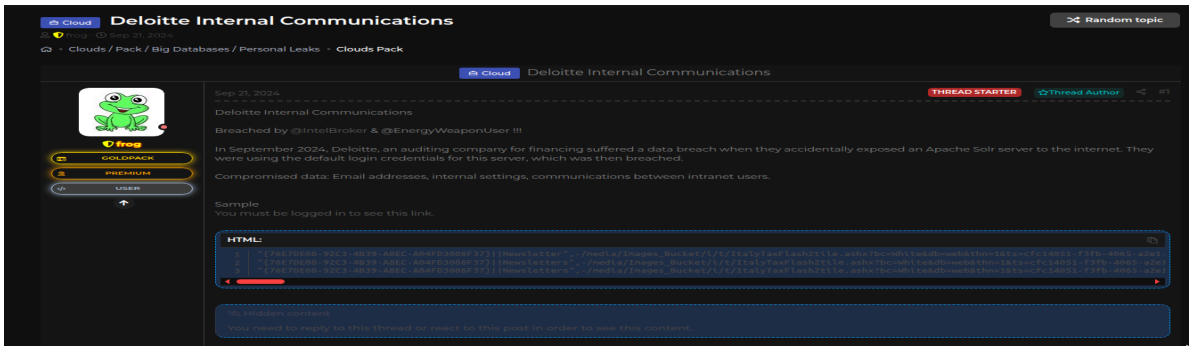


A post on a Dark Web forum advertised a leaked database titled “CrowdStrike IoC list db 100k Part one,” allegedly shared by the actor USDoD. The dataset is described as containing around 100,000 CrowdStrike Indicators of Compromise, including malware family mappings, kill chain stages, and confidence assessments. The exposure of structured IoC intelligence on a public forum may allow threat actors to study detection logic and adapt their tooling to evade defensive controls.

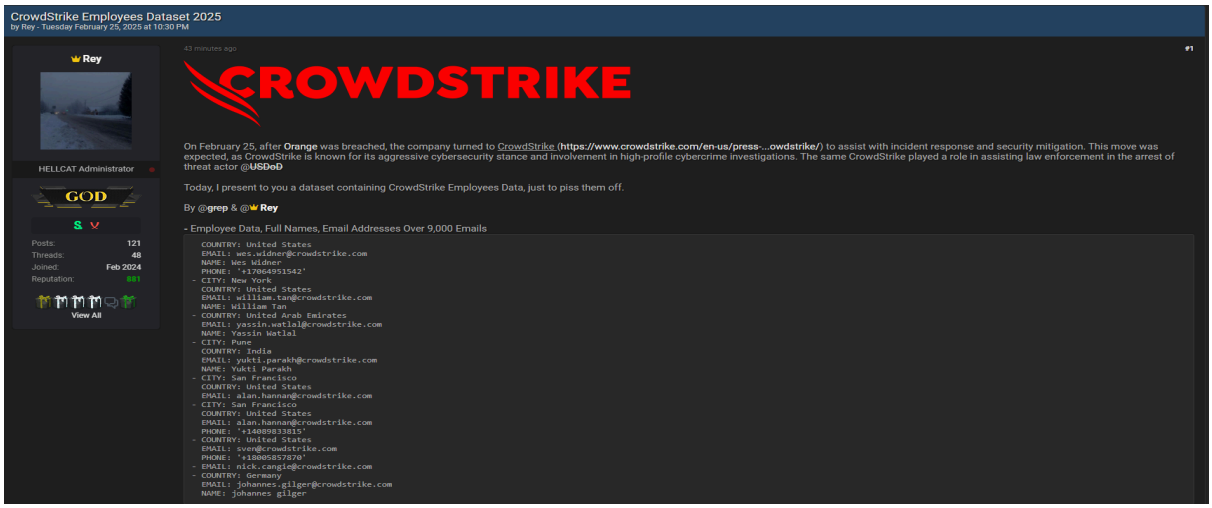
A Dark Web forum post claims that the actor USDoD released CrowdStrike’s full threat actor database, allegedly scraped from the vendor’s intelligence platform. The leak is presented as a way to expose the contents of paid intelligence reporting. Such data can help adversaries understand how threat actors are tracked, labeled, and profiled, and adjust their operations to avoid attribution and detection.



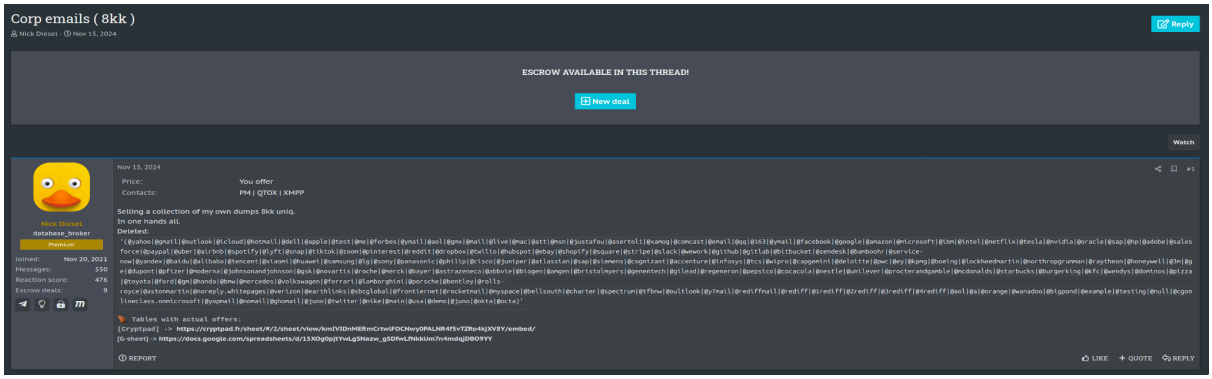
A Dark Web forum post claims a third party breach involving Accenture that exposed personal details of 32,826 employees, including names and email addresses. The listing attributes the incident to a supply chain compromise. Posts of this kind show how employee data from large enterprises is circulated in leak forums following alleged third party breaches.



A threat actor on a Dark Web forum claims a breach of Deloitte. The actor says they accessed an exposed Apache Solr server using default credentials. The alleged data includes employee email addresses, internal settings, and intranet communications.



A post on a Dark Web forum claims a retaliatory data leak involving CrowdStrike. The actor says the leak targets CrowdStrike due to its role in incident response for the company Orange. The dataset allegedly contains details and email addresses for more than 9,000 employees across the USA, UAE, India, and Germany.

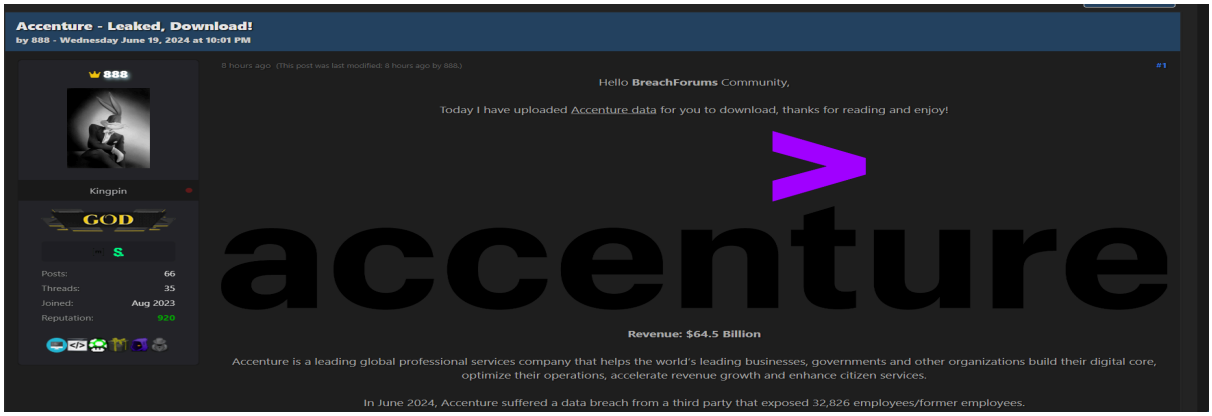


A listing advertises a bulk sale of corporate email data. The seller claims the dataset contains about 8 million email addresses linked to major firms, including Accenture, Infosys, Capgemini, Deloitte, and KPMG. The post suggests broad global exposure of contact information for these service providers.

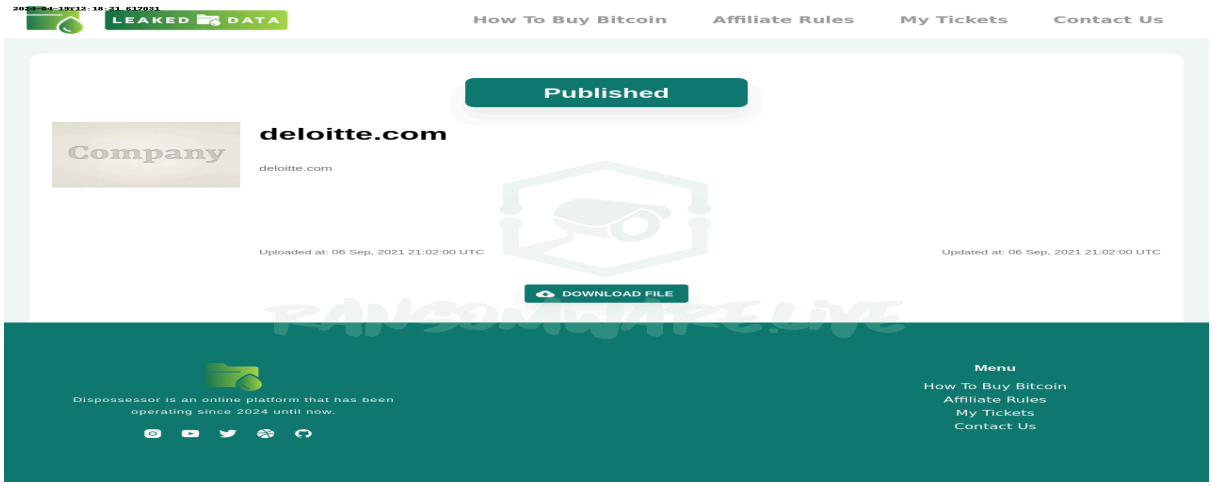
A post on a Dark Web forum claims a major data breach involving Capgemini. The actor alleges the leak includes about 20GB of data. The exposed content reportedly contains source code, private keys, API keys, credentials, and internal threat reports.

A post on a Dark Web forum advertises the sale of compromised corporate email accounts. The actor claims access to email accounts linked to major consultancies, including Accenture, Deloitte, Capgemini, and KPMG. The listing highlights large volumes, with about 21,000 Accenture accounts, 8,000 Deloitte accounts, and 5,000 Capgemini accounts.

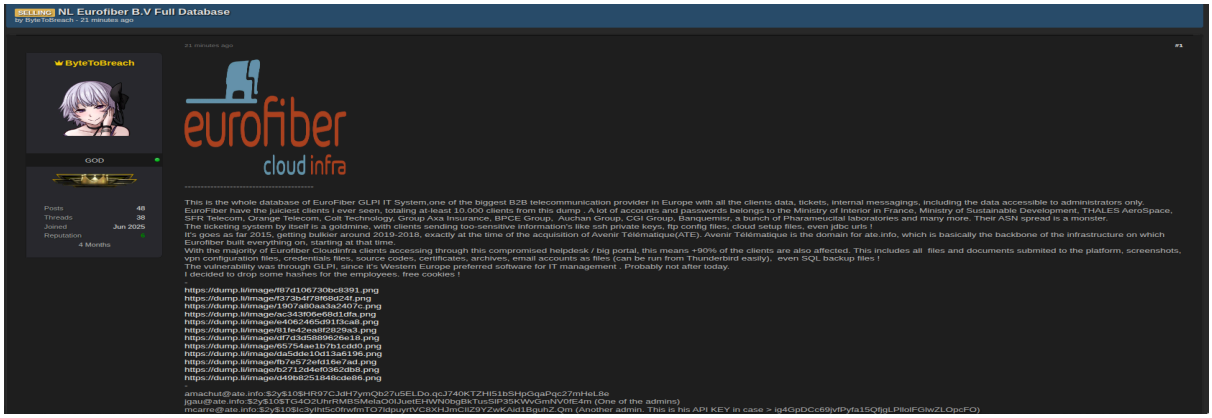
A post on a Dark Web forum claims a compromise of Deloitte.com linked to the UK. The actor alleges the leak includes internal GitHub credentials and source code. The post suggests a high risk to intellectual property and internal security.



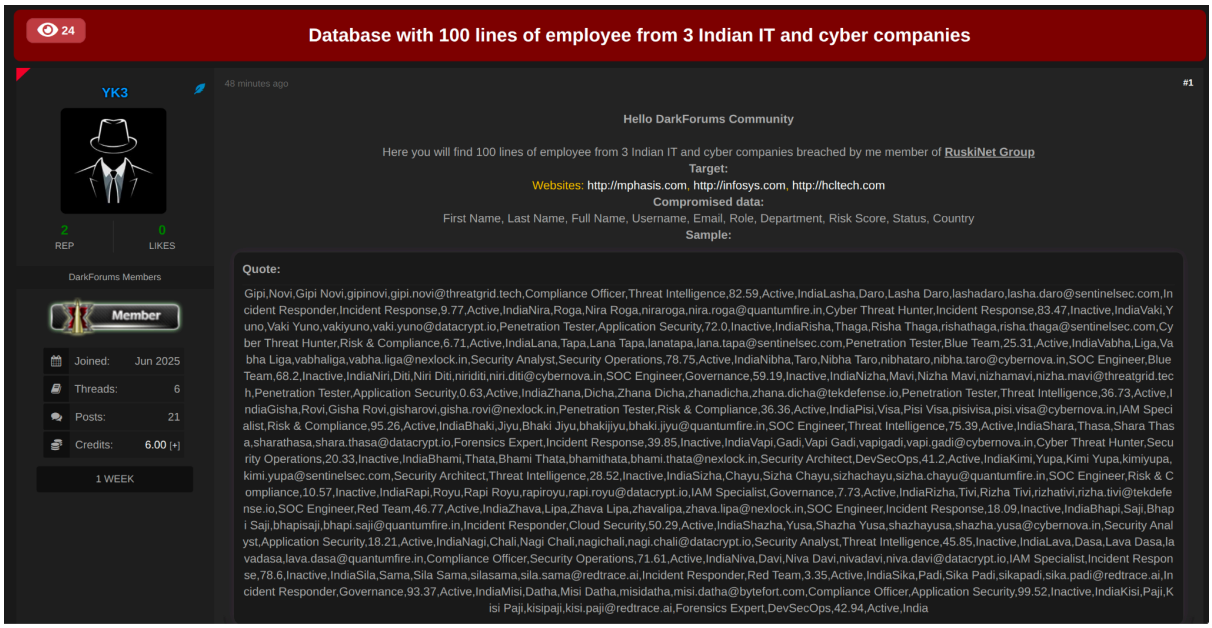
A post on a Dark Web forum shares a re-upload of previously leaked Accenture data. The actor claims the dataset includes information on more than 32,000 current and former employees. The post highlights the continued circulation of Accenture-related data within underground forums.



The Dispossessor ransomware group lists Deloitte on its leak site. The posting suggests that the group published data linked to Deloitte. This listing adds to earlier reports of Deloitte exposure across underground sources.



A Dark Web forum post advertises the sale of the full Eurofiber GLPI IT system database. The actor claims the leak affects more than 10,000 clients. The exposed data reportedly includes SSH private keys and VPN configurations, with named impacts to accounts linked to Accenture, Orange, Thales, and the French Ministry of Interior.



A post on a Dark Web forum claims a leak of employee data from three Indian IT and cyber firms: Infosys, HCLTech, and Mphasis. The actor, linked to the RuskiNet Group, shared a sample of the records. The exposed fields include names, usernames, email addresses, roles, and risk scores, creating a clear risk of targeted phishing against security staff.

The MSSP Strategic Partnership Advantage

Premium security products form the foundation of any defense strategy. Yet our research reveals a critical insight: the same tools designed to protect your organization are being systematically studied, tested, and bypassed by sophisticated threat actors. With 14.29% of underground posts discussing zero-day vulnerabilities and 25% focused on bypass techniques, no product, regardless of reputation, operates outside the attacker's field of vision.

The gap is not in your product's quality; it lies in the operational model. Static deployment creates a false sense of security. Technology alone is no longer a deterrent when attackers actively adapt to circumvent it. True resilience requires a fundamental shift: from "product ownership" to "operational excellence" delivered through strategic partnership.

This is where an MSSP becomes your strategic partner. An MSSP transforms static software deployment into a dynamic, human-led defense that evolves as fast as the threats do, providing the continuous expertise, intelligence, and operational capability that technology alone cannot deliver.

24/7 Expert Analysis

Your security controls generate alerts based on predefined logic. But threat actors evolve faster than these rules can be updated. An MSSP provides continuous human review to interpret weak signals, connect seemingly unrelated events, and recognize early stages of intrusion, capabilities that automated systems alone cannot replicate.

MSSP analysts correlate your internal alerts with external intelligence, underground discussions, and active campaigns. This enables detection of activity that does not yet match known signatures or playbooks, catching threats before they become incidents.

Proactive Threat Adaptation

New evasion techniques surface in forums, private channels, and malware testing discussions before they appear in real-world incidents. Without active monitoring of these sources, organizations rely on vendor updates that arrive after techniques are already in use. An MSSP closes this gap through continuous threat research.

Your MSSP partner tracks how attackers bypass specific products, including the ones you deploy, and rapidly adjusts detection logic, monitoring priorities, and response playbooks to reflect emerging methods before they impact your environment.

Collective Defense Intelligence

Threat actors reuse infrastructure, tools, and access methods across multiple victims. What is observed in one environment often predicts activity in another.

Your MSSP partner operates across many environments and can recognize attack patterns early which is something you can miss as a standalone organization. This enables preventive action before techniques spread to your environment, a capability impossible to achieve operating alone.

Intelligence-Enriched Response

High alert volume does not equal effective security. Many alerts lack the context required to understand whether they are part of a larger intrusion chain. Without intelligence, your team sees noise; with intelligence, they see attacks.

Your MSSP partner enriches alerts with intelligence about actor behavior and current campaigns. This transforms response from reacting to isolated events to proactively disrupting ongoing attacks.

Key Insights: Why MSSP Partnership Is Essential

Your security products are visible to attackers
Threat actors test against the same tools you deploy. With 60% of underground discussions referencing security vendors, your defenses are actively studied. An MSSP provides the continuous adaptation your tools need to stay effective.

Attackers operate as a coordinated supply chain
Malware builders, access brokers, and ransomware operators share knowledge faster than vendors can update. Your MSSP partner monitors these channels and adapts your defenses in real-time, closing the gap between threat emergence and protection.

External intelligence is essential
Your logs and alerts show what's already inside. An MSSP's external intelligence shows who is preparing to attack and how, giving you the foresight to act before compromise, not after.

Initial access bypasses traditional alerts
Credential theft, session hijacking, and MFA abuse don't trigger classic malware alerts. An MSSP detects these subtle access patterns through behavioral analysis and threat intelligence correlation.

Behavior detection outperforms attribution
Attackers reuse proven loaders, stealers, and ransomware kits across groups. Your MSSP partner focuses on behavioral patterns, not group names, detecting threats regardless of who deploys them.

Exposure is visible before exploitation
Your stolen credentials and advertised access appear in underground markets days before incidents. An MSSP's continuous Dark Web monitoring provides the early warning that prevents escalation.

Speed is the attacker's advantage
Time between access sale and ransomware deployment continues to shrink. An MSSP's 24/7 monitoring and rapid response capability is your only reliable countermeasure against this timeline.

Context transforms alerts into intelligence
Without external context, your security team sees isolated alerts. With an MSSP's threat intelligence enrichment, they see campaigns, patterns, and attacker intent, enabling strategic response.

Strategic partnership delivers measurable ROI
Detecting exposure at an early stage prevents escalation into ransomware, extortion, or data theft. An MSSP partnership costs a fraction of a single major incident, making proactive protection the smartest investment in your security posture.

Your Strategic MSSP Partner: SOCRadar

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by **21.000+ companies in 150+ countries**

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep, and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.