

A stylized radar or sonar graphic with concentric red and blue circles and intersecting lines, set against a dark blue background with glowing red and blue points.

MSSP Report:

Security Industry Threat Landscape

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.

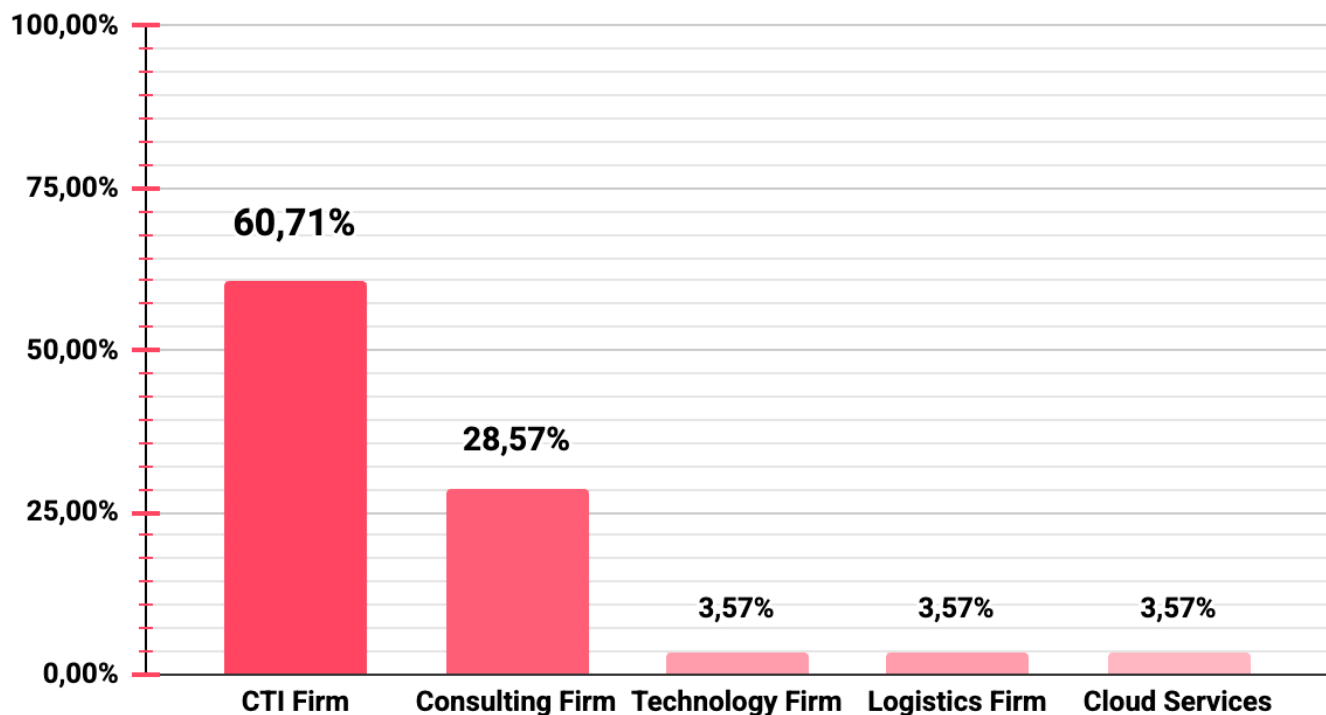
Security tools create their own attack surface:

- 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.

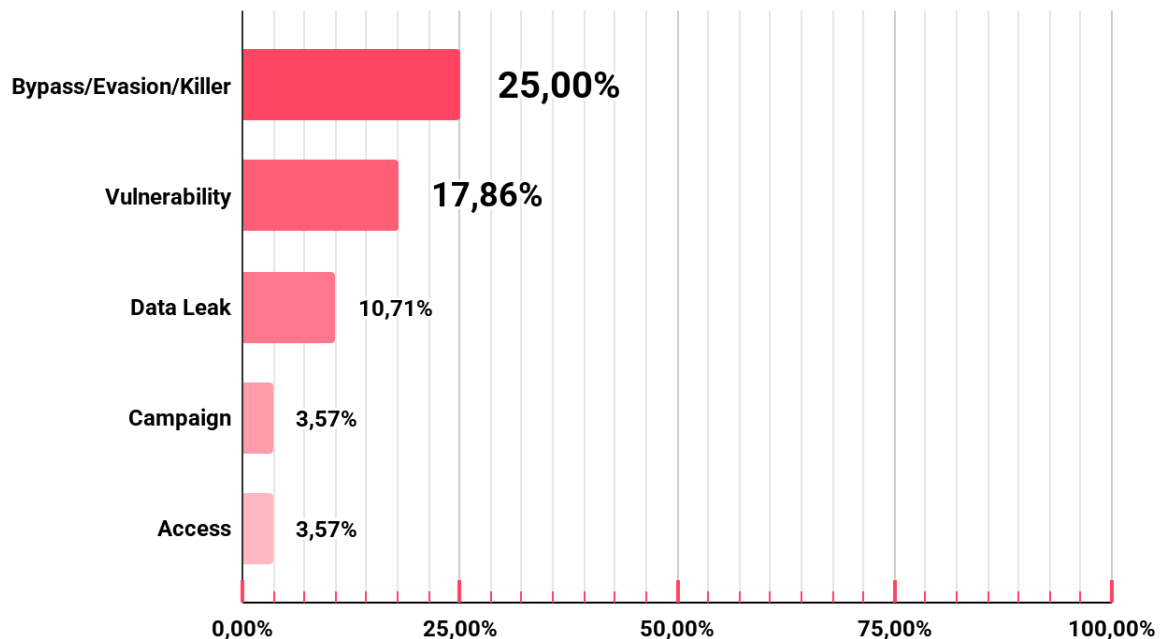
Distribution of Dark Web Threats Across Organizations



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.

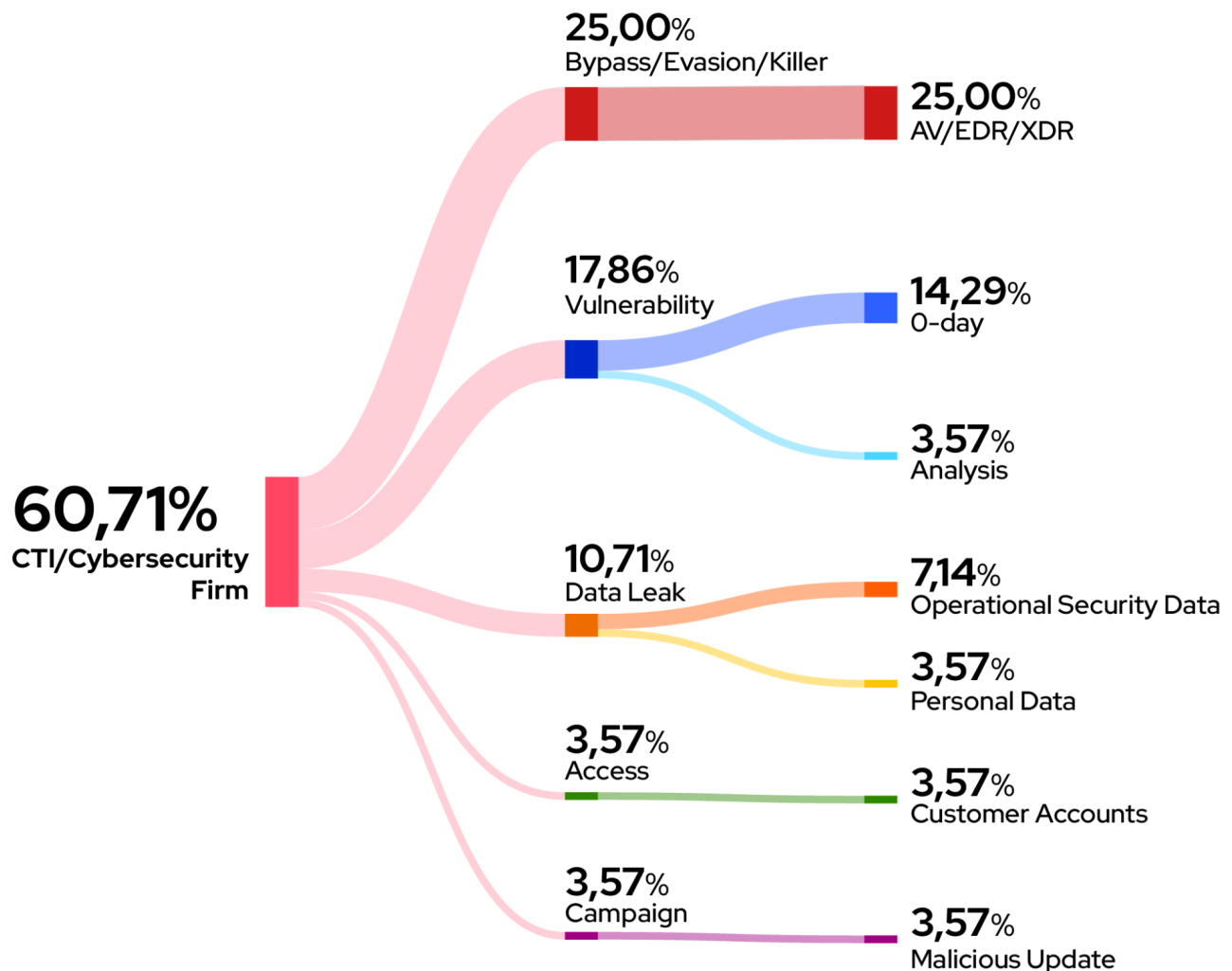


Data leaks and vulnerabilities are just a result; the real problem is how your defense tools are evaded.

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


[FREE TEST] || USG CRIPT || BYPASS AV: DEFENDER • KASPERSKY • ESET || BYPASS EDR: CROWDSTRIKE • SENTINEL ONE
 By Sculptor, October 19 in [Software] - malware, exploits, bundles, crypts

Start a new topic
 Reply to this topic

1 2 3 NEXT > Page 1 of 3


Sculptor
 megabyte
 55 posts
 Joined 10/12/24 (ID: 179108)
 Activity
 coding / coder
 Deposit 0.005094B
 Autogrant 100%

Posted October 19
 Hi all,
 Let me clarify right away: this is not a product presentation or the launch of a service. We're simply providing limited information so you understand where and to whom you're submitting your files for testing. No marketing or fluff—just what you need to know.
 We're preparing the release of our cryptographer. **We've decided to offer it for free testing – we need feedback from real people with real problems.**
 We work with any files except lockers and related files. We look forward to receiving detailed feedback after use.
 We work with anything:
 1. .NET of any version (2.0-4.8) - obfuscated or not. Managed, mixed, any architecture.
 2. Native files (x32/x64) - pure PE with static linking, with any imports.
 3. Hybrids of all kinds - mixed mode C++/cli, .net with native libraries, multi-stage droppers, files with overlays.
 Quote
 An important point about packed files:
 If you have files for upx, themida, vmprotect, and similar programs, they're technically more difficult to work with due to the specifics of the protectors themselves and their internal logic. We can test them

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.


AV Killer + UAC Bypass as a Gift
 By Scarlett, November 7 in [Software] - malware, exploits, bundles, crypts

Start a new topic
 Reply to this topic

1


Scarlett
 byte
 9 posts
 Joined 09/24/24 (ID: 214047)
 Activity
 hacking
 Deposit 0.203051B
 Car warranty 100%

Posted November 7
 Good evening, I am selling a homemade EDR killer from Surtsami. It works by killing EDR from kernel mode. It requires admin rights, so I will give away a .MSC exploit for bypassing UAC for free.
 List of AVs that the software kills:
 1. Microsoft Defender / Windows Security
 2. Kaspersky
 3. ESET NOD32 / Internet Security
 4. Avast / AVG
 5. Norton / Symantec
 6. McAfee
 7. Bitdefender
 8. Trend Micro
 9. Sophos
 10. CrowdStrike Falcon
 11. SentinelOne
 12. Cylance
 13. Palo Alto Cortex XDR
 14. FireEye
 15. Carbon Black (VMware)

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.

What's really flying under VT/AMP/NSA lenses right now?

By zestix, November 24 in Malware

zestix

megabyte

57 posts

Joined

09/16/25 (ID: 213387)

Activity

Security / Malware

Car warranty

OC

Posted November 24

The days of scaring people with old implants like Cobalt Strike or Meterpreter are long gone. They all have static signatures, YARA rules, and EDRs that kill them instantly.

Here's what actually works (tested on air-gapped classified environments + a few European banks that are still in the dark):

Loader = Pure Reflective + Syscall-only (dopk Ekko/Kekeo 2.0 2025)

No more VirtualAllocEx... we write directly via NtMapViewOfSection + the fresh MZ does not fall to disk.

We pull all syscalls directly from rdtbl.dll in the memory of the legitimate process (msbuild.exe, rundll32.exe, cmd.exe, etc.)... 0 Windows API hooks.

New technique: Heaven's Gate 64... Wow64... x86 syscall... return. Most EDRs haven't yet implemented full logging of Wow64 syscalls.

Obfuscation = LLVM-Olivm 18 + custom Control Flow Flattening 2025 + Polymorphic Dispatch

We're forgetting the old Olivm. We're now mixing it with the new "Polymorphic Dispatch" plugin: every implant launch... a completely new dispatcher.

Strings are no longer simply XORed. Now they're AES-256-GCM, with a key extracted from the Intel SGX enclave (yes, the SGX backdoor is still alive, there's no full patch).

Control Flow is not implemented via VMProtect/Hyperion. We wrote our own x86_64 interpreter and runtime JIT recompilation of each basic block (dynamic recompilation on the fly).

Persistence = AppCertDlls + Token Stealing via Isas (Kerberos Silver/Golden Ticket 2.0)

Scheduled Tasks and Run keys are dead. Currently: AppCertDlls (still unpatched as of Windows 11 24H2) + DLL Side-loading in the TrustedInstaller context.

We don't steal the token from Isas. We directly generate a Golden Kerberos Ticket with an AES-256 key from the DC registry (HKLMSecurityPolicy\Secrets). We only need SetTakeOwnershipPrivilege... we can get it via BYOVD (any old signed driver).

C2 = Dead-Drop Resolver via Web3 + QUIC/gRPC

DNS tunneling and DGA are so last century. Now, the Ethereum Name Service (ENS) is a dead-drop resolver: victim-1125.eth... new TXT record every day... new C2 IP.

Real traffic on 443, but the protocol is QUIC (Cloudflare Workers) or gRPC with a custom protobuf.

EDR can't profile: TLS fingerprint 1-to-1 like Chrome 129 (JA3 spoofing via krypton + custom ALPN).

Anti-Forensic & Anti-Sandbox 2025

Time-based evasion: if uptime < 28 days... sleep for 45 days (then self-destruct).

CPURAM check: < 8 logical cores or < 16 GB RAM... suicide.

Hypervisor checks: reginaldshuipit + MAC DUI (00:0C:29:08:00:27 etc)... kill.

New: Intel ME version check. If > 11.8.93 (JTAG disabled)... continue, otherwise suicide.

Fileless LPE 2025 (0-day, not yet public) CVE-2025-0824

Print Spooler... AppContainer bypass... Selimpersonate or PrintNotify service.

Next BYOVD: old signed HP driver (still valid in Win11 24H2)... arbitrary kernel read/write.

Clearing all event logs via direct IOCTL to 'Device\EventLog' + NtClearEvent.

Exfiltration = Steganography v AV1 + Discord/CDN

We hide the data in AV1 video (libaom-av1 build with custom patches).

The video is streamed live via Discord or Cloudflare Stream.

PRISM has not yet learned to detect AV1-steego by November 2025.

The Real KillSwitch

When processes like procmon64.exe, wirehark.exe, autoruns.exe, pestudio.exe, etc. appear, they overwrite themselves with zeros, delete them from the USN journal, and sleep infinitely.

This build lasted at least 90 days in 11 different environments (including a fully air-gapped network with USB-only access) without a single detection. VT 0/72, Carbon Black, CrowdStrike Falcon, SentinelOne, Cortex XDR—all blind.

Never store payloads on GitHub, even in private repos. Only IPFS/Arweave + multilayer encryption.

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.

Crypt exe/dll/bin x64/x86 XDR/EDR bypass tested on live env CrowdStrike EDR - sophos EDR - SentinelOne EDR - FortClient Endpoi

By black.codes, April 24 in [Software] - malware, exploits, bundles, crypto

black.codes

megabyte

3K

Contacts

54ACD38AD294F8A754B48136623F3F42EE18B370F065A22CBED0A55E08114A68582BA3EF8B25

Crypt your payload and bypass all major XDR / EDR, the input / output can be: .exe / .dll / .bin / .ps1

any file native / .net x64 / x86, my encryption is for red teamers can talk about prices and technical / commands in private

Pro: CrowdStrike Falcon Sensor EDR: https://streamable.com/gem4

TOX: 54ACD38AD294F8A754B48136623F3F42EE18B370F065A22CBED0A55E08114A68582BA3EF8B25

I always accept Forum Guarantor.

xxx - https://hxxp://threads/133509/post-947278

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.

Selling AV/EDR Killer
By [Taint](#) • March 30 (posted) • malware, exploits, bundles, crypto

Start a new topic

Taint
byte
19 posts
Joined 03/02/05 (ID: 190721)
Activity
malware / malware
Deposit 0.0011083
Autogrant 0

Posted March 3 (edited)

Selling an AV/EDR killer.

The killer exploits a vulnerable driver, **completely** disabling protection systems, including AV/EDR/XDR. Once the killer is triggered, antivirus programs will no longer launch, even after a reboot. Currently, the killer has been tested against most home, basic antivirus programs, as well as the following **EDR/XDR** solutions:

- SentinelOne
- Sophos Intercept X (XDR)
- Sangfor EDR
- ESET Endpoint Security
- Panda Adaptive Defense 360
- Trend Micro EDR
- Trellix Endpoint
- Kaspersky Endpoint (except for the latest versions 24-25)
- Webroot Endpoint
- GuardCore
- Symantec
- BitDefender EDR
- ZoneAlarm
- Immunet
- CrowdStrike Falcon
- Secrin, QuickHeal
- QAX Endpoint
- Huorong
- eScan
- AhnLab Internet Security
- 360 AV
- WithSecure EDR
- F-Secure
- Avast
- Norton
- Avira
- Other basic, home...

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.

DELIVERY EXPLOITS - Any EDR bypass - WD bypass - Smart Screen Bypass - Win+R (ClickFix) And Html + Lnk - 100% FUD
By [ImpactSolutions](#) • October 28 (in [banned]) • malware, exploits, bundles, crypto

ImpactSolutions
Impact Solutions
17 posts
Joined 11/09/02 (ID: 111430)
Activity
malware / malware
Deposit 0.000344
Autogrant 0

Posted October 28 (edited)

Introducing Impact Solutions EDR edition — the most reliable and stealthy delivery methods builder on the market. Designed for professionals who demand zero compromises, this service ensures your exploits will bypass any security solution. Each EDR Edition Builder undergoes rigorous manual testing against all major AVs and EDRs. Weeks of fine-tuning have been invested to optimize every aspect of the exploits, ensuring maximum stealth — including no PowerShell windows or detectable indicators. If you have no margin of error, this tool is for you.

This builder offers 2 main methods:
Html + Lnk >
<https://vimeo.com/1137280258>
Win+R (ClickFix) >
<https://vimeo.com/1141683429>

Hide contents

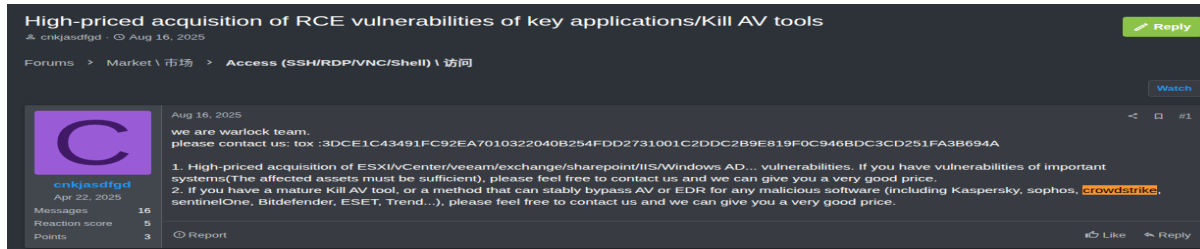
Note: this variation of ClickFix supports comments to hide the commands:

And has almost no pop up windows.
A free subscription to the PRO tier of <https://forum.exploit.in/over/250550/> is also included.

Watch real EDRs bypasses:
Html + Lnk
Hide contents

- Windows Defender - <https://vimeo.com/1131150209>
- Kaspersky EDR - <https://vimeo.com/1131150065>
- Eset EDR - <https://vimeo.com/1131149564>
- Trellix - <https://vimeo.com/1131150187>
- SentinelOne - <https://vimeo.com/1131150123>
- Harmony - <https://vimeo.com/1131150028>
- Fortinet - <https://vimeo.com/1131149614>
- BitDefender - <https://vimeo.com/1131149616>
- Cortex XDR - <https://vimeo.com/1136114135>
- Sophos - <https://vimeo.com/1136114248>
- CrowdStrike Falcon Pro - This EDR is very strict with Lnk files, and we managed to find a bypass, but we are not comfortable sharing it in a public video. Please contact us privately for more info about it.

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.

Zero-day vulnerabilities in Palo Alto Networks firewall caused by basic developer errors

Man Nov 24, 2024



Man
Professional
Messages: 3,224
Reaction score: 1,130
Points: 113

Nov 24, 2024

Attackers are exploiting a combination of two vulnerabilities to bypass authentication and escalate privileges through the PAN-OS web-based management interface to gain root access on Palo Alto Networks firewalls.

Palo Alto Networks has released patches for two actively exploited vulnerabilities affecting its firewalls and virtual security appliances. Together, these flaws allow attackers to execute malicious code with the highest possible privileges on the underlying PAN-OS operating system, gaining complete control over the devices.

Earlier this month, Palo Alto issued an advisory alerting customers that it was investigating reports of a potential remote code execution (RCE) vulnerability in the PAN-OS web-based management interface and advised them to follow recommended steps to secure access to this interface.

During the investigation, the company discovered that the RCE attack was the result of not one, but two vulnerabilities, both of which had already been exploited in limited attacks on devices whose management interfaces were exposed to the internet.

Authentication bypass and privilege escalation

The first vulnerability (CVE-2024-0012) is rated critical with a score of 9.3 out of 10. By exploiting this issue, attackers can bypass authentication and gain administrative privileges in the management interface, allowing them to perform administrative actions and change configurations.

While this is bad enough, it won't directly lead to a full system compromise unless this functionality can be used to execute malicious code in the underlying operating system. It turns out that attackers found such a way through a second vulnerability (CVE-2024-9474), which allows anyone with administrative rights in the web interface to execute code in Linux-based operating systems as the root user—the highest possible privilege.

Both vulnerabilities affect PAN-OS 10.2, PAN-OS 11.0, PAN-OS 11.1, and PAN-OS 11.2, all of which have already received patches.

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.

[SELLING] Palo Alto Firewall / Exploit Full-Chain 0day / (RCE - POC Golang)

Nov 19, 2024

ESCROW AVAILABLE IN THIS THREAD!

[New deal](#)

Please note, if you want to make a deal with this user, that it is blocked.

Price: \$5000
Contacts: AD7BA7E0863EAFCE7E9DD9532F0ADD0C6601D6694C3185B829501B184F7DBE85A2190B0845DC1

This offer provides a **full-chain 0-day exploit** targeting Palo Alto Firewalls, enabling **Remote Code Execution (RCE)** with proof-of-concept (POC) developed in **Golang**.

Key Features:

- Full-Chain Exploit > Exploits an undisclosed chain of vulnerabilities in Palo Alto Firewalls.
- RCE Capability > Achieves remote execution of arbitrary code on targeted devices.
- Proof of Concept (POC) > Written in Golang, ensuring efficiency, portability, and easy integration.
- Zero-Day Status > Exploit targets a currently unpatched vulnerability, offering exclusivity and value. **OVER 14k UNPATCHED SERVERS**

Proof:

- We can send POC Exploitation Video

BIN = 12k, Step = 1k\$, Blitz = 15k

ESCROW IS A MUST! NO ESCROW NO PURCHASE!
Taxes are from buyer's

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.

[SELLING] Palo Alto Firewall / Exploit Full-Chain 0day / (RCE - POC Golang)

exploitsdev 6 minutes ago · 1 · 0

Price: 15000
Contact: AD7BA7E0863EAF7E9D093526FDADC6601DE694C218588295018184F7DBEE5A219080845DC1

This offer provides a **full-chain 0-day exploit** targeting Palo Alto Firewalls, enabling **Remote Code Execution (RCE)** with proof-of-concept (POC) developed in **Golang**.

Key Features:

- **Full-Chain Exploit** > Exploits an undisclosed chain of vulnerabilities in Palo Alto Firewalls.
- **RCE Capability** > Achieves remote execution of arbitrary code on targeted devices.
- **Proof of Concept (POC)** > Written in Golang, ensuring efficiency, portability, and easy integration.
- **Zero-Day Status** > Targets a currently unpatched vulnerability, offering exclusivity and value: **OVER 14K UNPATCHED SERVERS**

Proof:

- We can send POC Exploitation Video

Tox: AD7BA7E0863EAF7E9D093526FDADC6601DE694C218588295018184F7DBEE5A219080845DC1

100% = 100, 50% = 50, 0% = 0

!ESCROW IS A MUST NO ESCROW NO PURCHASE!
"Fees are from buyer's"

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.

[Sell] Palalto PAN-OS 0day RCE
By hello_enenen, 11 minutes ago in [Software] - malware, exploits, bundles, crypts

hello_enenen
byte

Posted 11 minutes ago

Selling 0day in Paloalto.
more information contact me on jabber: hello_enenen@exploit.im
(Provide proof of btc first)

+ Quote

Paid registration
0
6 posts
Joined
09/09/23 (ID: 153061)

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

Mandiant Advantage intel

by snicker941 - Thursday April 21, 2022 at 12:15 AM

snicker941



New User

MEMBER

Posts: 3

Threads: 1

Joined: Apr 2022

Reputation: 0

6 hours ago (This post was last modified: 5 hours ago by snicker941.)

Downloaded all reports, screenshotted threat actor alerts, etc.

Some of you are on this aka @[mont4na](#) @[NetSec](#) (you guys were on the Mandiant Advantage threat activity alerts for today)

English-Speaking Actor 'NetSec' Shares Data Leak of U.S. Chemicals Management Solutions Provider on [breached.co](#)

English-Speaking Actor 'mont4na' Advertises Logins Extracted from Multiple Companies on [breached.co](#)

Just proves you need to vet your potential buyers

Also selling a few accounts on there. You need 2FA enabled (required), I will give you the TOTP secret key.

DM me

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.

US-RDP-DA-rights-\$130kk

newsudo · Today at 12:22 PM

newsudo

Premium

Joined: Aug 21, 2024

Messages: 10

Reaction score: 1

Escrow deals: 2

Deposit: 0.0517 B

Today at 12:22 PM

Price: 3500

Contacts: tox

US RDP = Domain admin access rights

AV I can't find + windows defender

PS C:\> ([adsisearcher]"(ObjectClass=computer)").FindAll().count = 665

Revenue: ~\$128 Million

Industry: Transportation

list of DCs: 5

domain trusts: 1

zoominfo will never send

1 hand sell (The first person to buy will be announced here and the topic will be closed)

+Escrow

Report

Guest

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


ANY.RUN
@anyrun_app

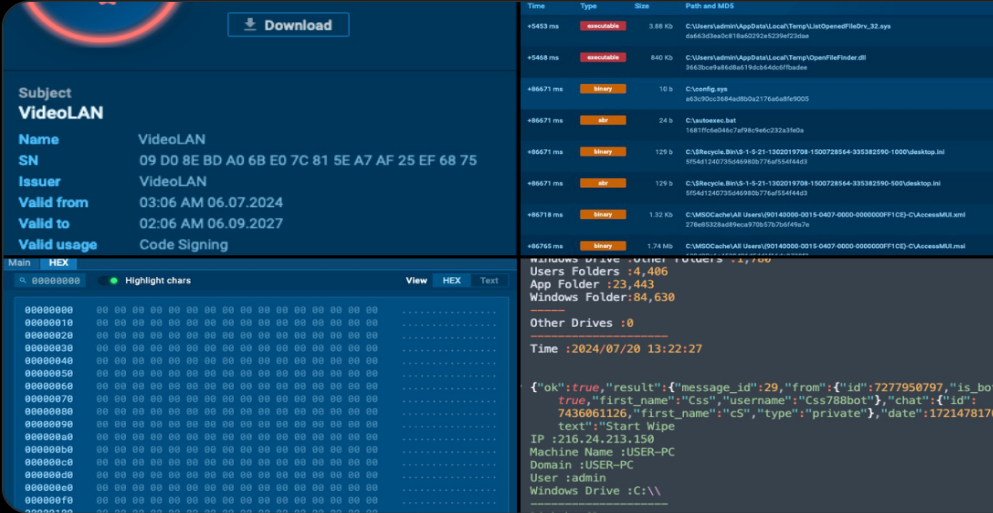

When seeking a fix users affected by the **#outage** can destroy their entire system.

Attackers are now distributing a data **#wiper** disguised as **#CrowdStrike** update. It decimates the system by overwriting files with zero bytes and then reports it over **#Telegram**.

See the destruction process  app.anyrun/tasks/14fc6a8a...

To appear more trustworthy, it displays a window asking the user if they want to "install the update".

Gönderiyi çevir

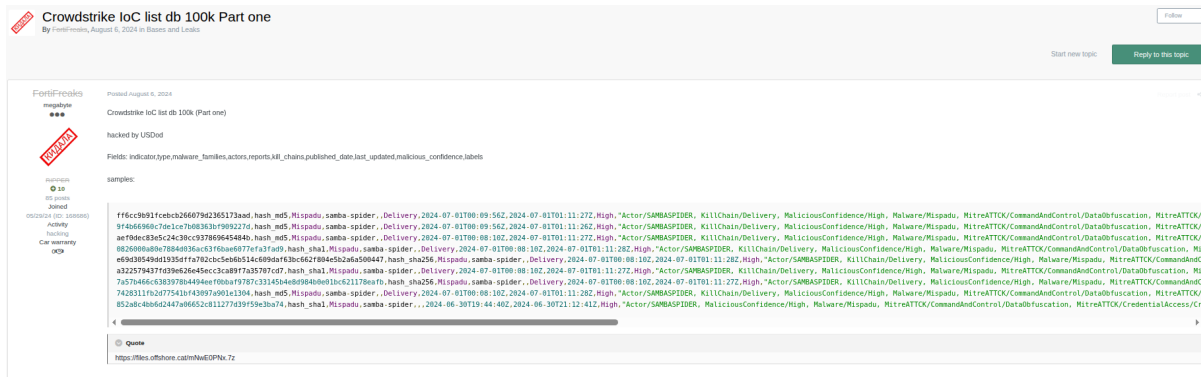


The screenshot displays the ANY.RUN interface. On the left, a 'Download' button is visible. Below it, a 'Subject' section shows 'VideoLAN' with details like 'Name', 'SN', 'Issuer', 'Valid from', 'Valid to', and 'Valid usage'. The main area is split into two panes. The top pane shows a list of files being distributed, including 'C:\Users\admin\AppData\Local\Temp\Temp\FailFolder.dll' and 'C:\Users\admin\AppData\Local\Temp\Temp\FailFolder.dll'. The bottom pane shows a 'Main' section with a 'HEX' tab and a 'Highlight chars' section. The 'HEX' tab displays a hex dump of the file content, and the 'Highlight chars' section shows a list of characters. The bottom right pane shows a 'Users Folders' section with details like 'App Folder: 23,443' and 'Windows Folder: 84,630'. Below this, a 'Time' section shows '2024/07/20 13:22:27'. The bottom right pane also shows a 'Other Drives' section with details like 'IP: 216.24.213.150' and 'Machine Name: USER-PC'.

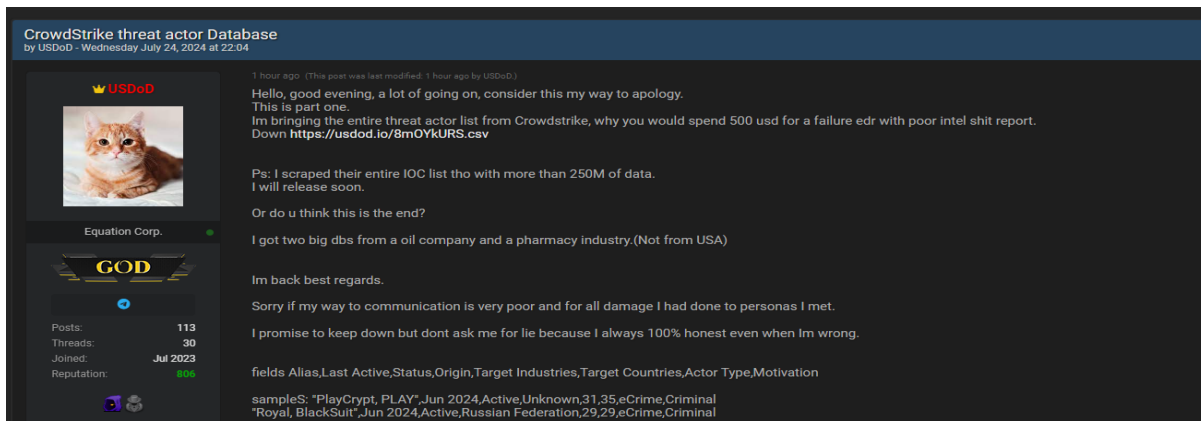
ÖS 4:46 · 20 Tem 2024 · **28,3 B** Görüntüleme

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.

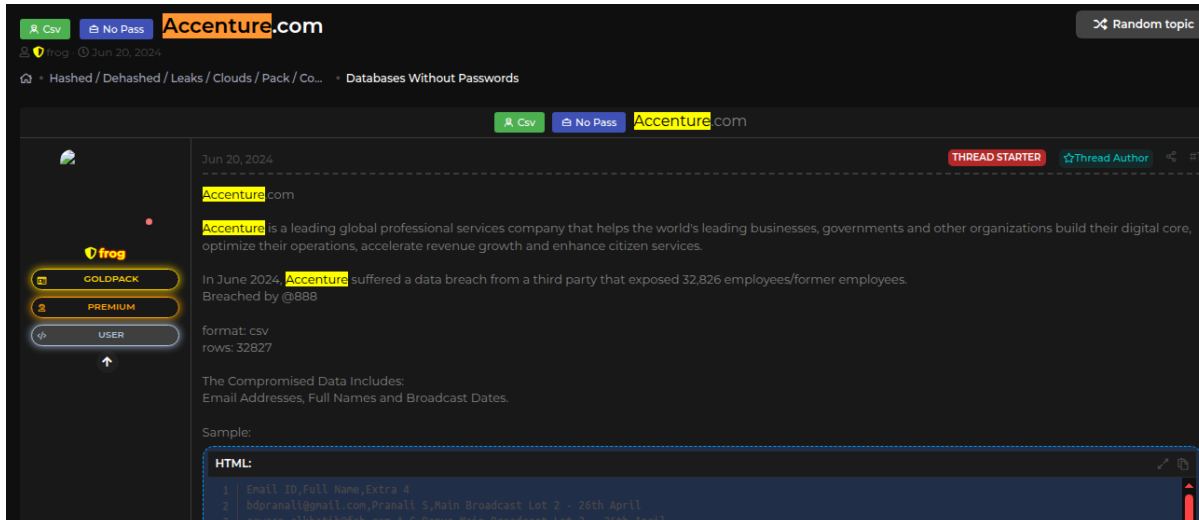
Data Leak Posts



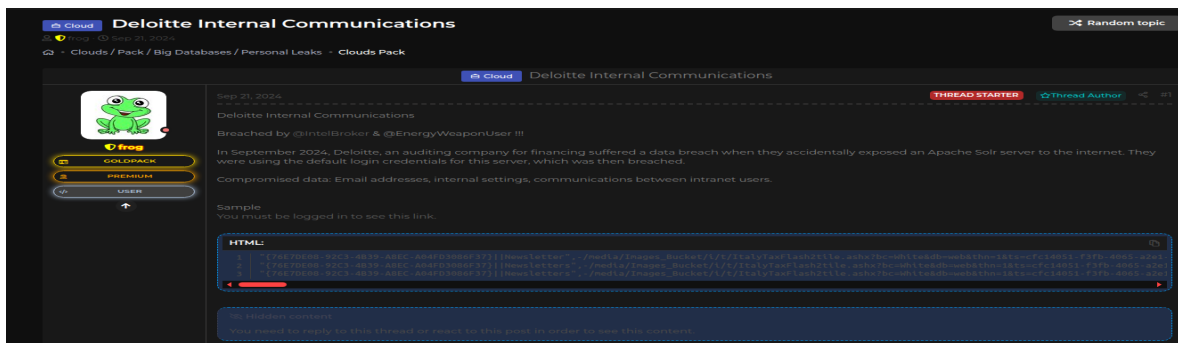
A post on a Dark Web forum advertised a leaked database titled "CrowdStrike IoC list db 100k Part one," allegedly shared by the actor USDod. The dataset is described as containing around 100,000 CrowdStrike Indicators of Compromise, including malware family mappings, kill chain stages, and confidence 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.



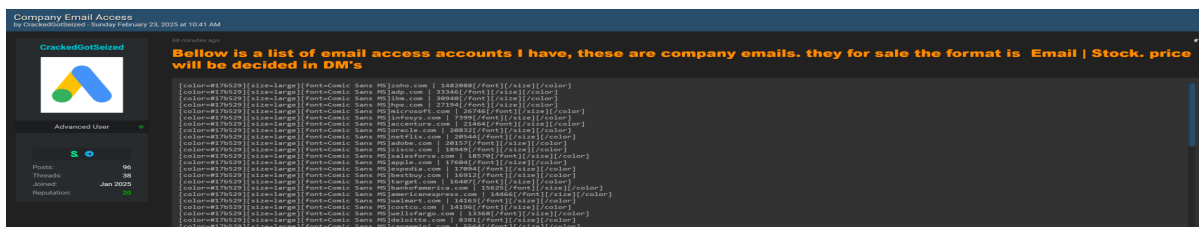
A threat actor on a Dark Web forum claims a breach of Deloitte. The actor says they accessed an exposed Apache Solr server using default credentials. The alleged data includes employee email addresses, internal settings, and intranet communications.

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.

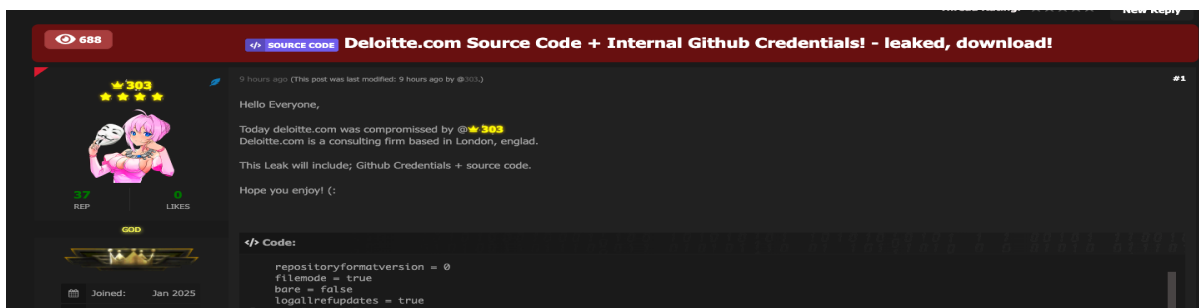
A listing advertises a bulk sale of corporate email data. The seller claims the dataset contains about 8 million email addresses linked to major firms, including Accenture, Infosys, Capgemini, Deloitte, and KPMG. The post suggests broad global exposure of contact information for these service providers.



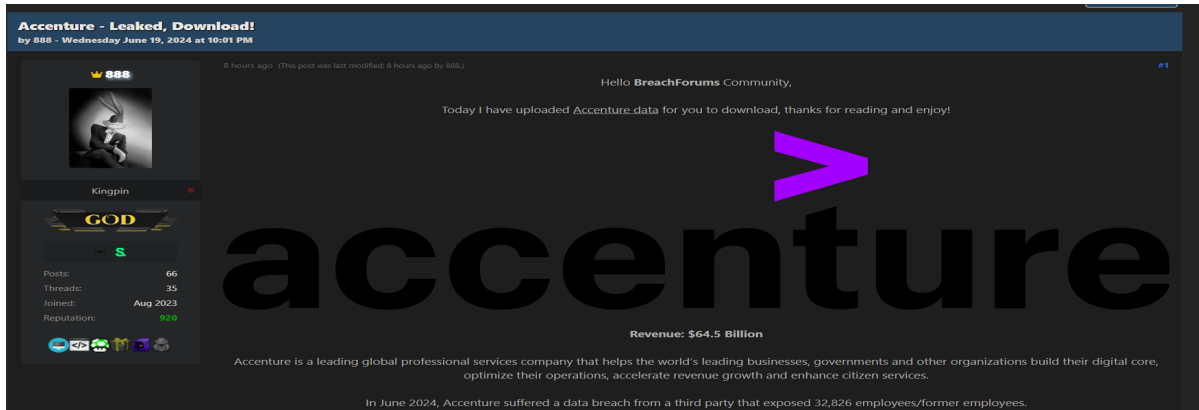
A post on a Dark Web forum claims a major data breach involving Capgemini. The actor alleges the leak includes about 20GB of data. The exposed content reportedly contains source code, private keys, API keys, credentials, and internal threat reports.



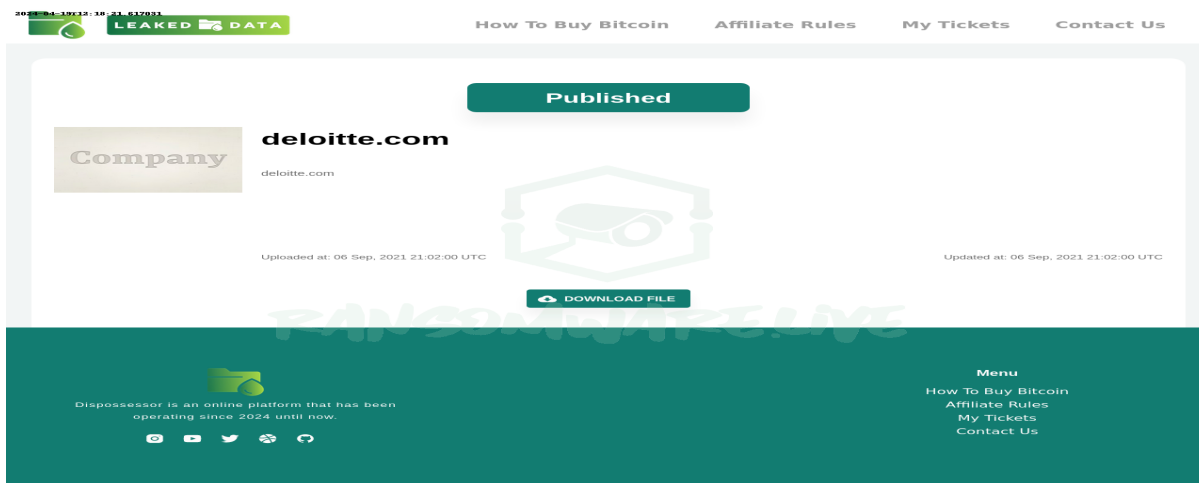
A post on a Dark Web forum advertises the sale of compromised corporate email accounts. The actor claims access to email accounts linked to major consultancies, including Accenture, Deloitte, Capgemini, and KPMG. The listing highlights large volumes, with about 21,000 Accenture accounts, 8,000 Deloitte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



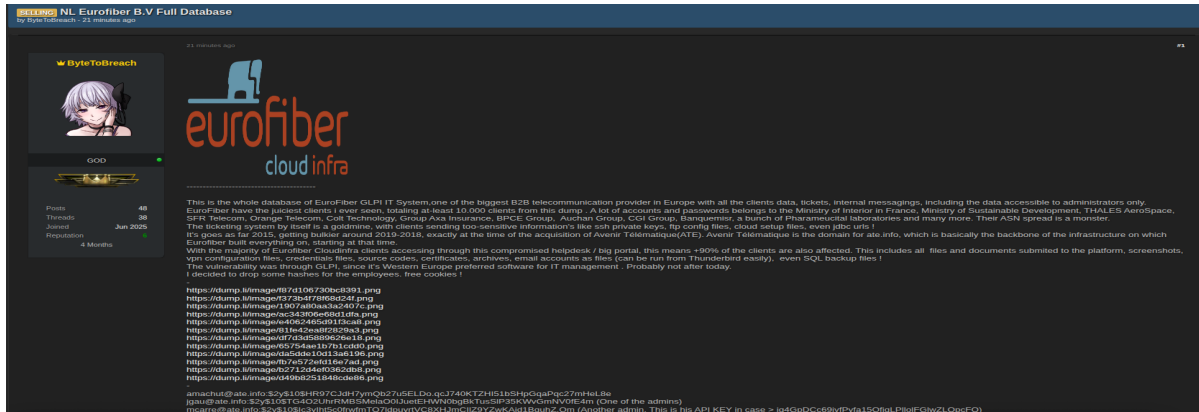
A post on a Dark Web forum claims a compromise of Deloitte.com linked to the UK. The actor alleges the leak includes internal GitHub credentials and source code. The post suggests a high risk to intellectual property and internal security.



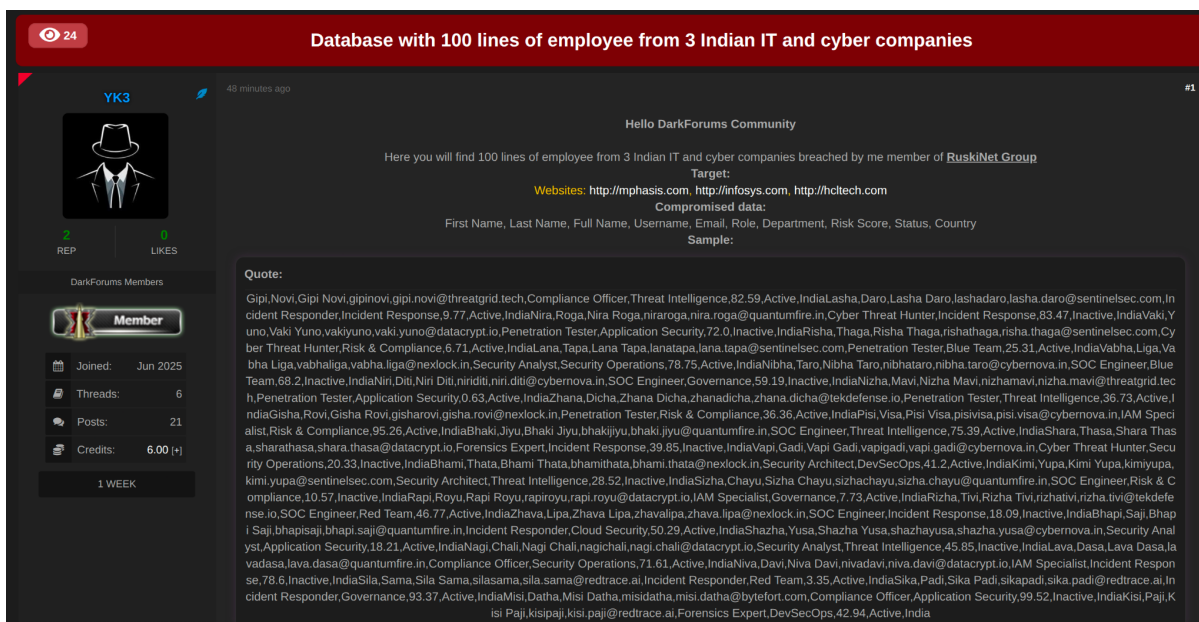
A post on a Dark Web forum shares a re-upload of previously leaked Accenture data. The actor claims the dataset includes information on more than 32,000 current and former employees. The post highlights the continued circulation of Accenture-related data within underground forums.



The Disposessor 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.

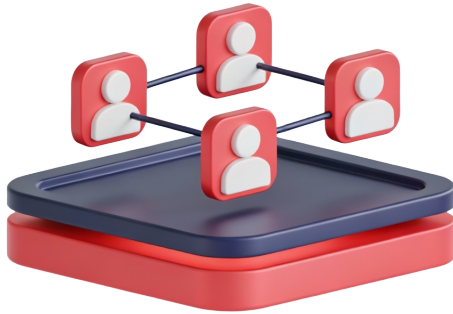
MSSP analysts correlate your internal alerts with external intelligence, underground discussions, and active campaigns. This enables detection of activity that does not yet match known signatures or playbooks, catching threats before they become incidents.



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.

