KORTNIT GROUP – OSINT Driven Threat Intelligence Assessment

Executive Summary

This assessment provides an OSINT-based analysis of potential cyber threats facing **Kortnit**, the world's largest home improvement retailer. Using publicly available intelligence, reconnaissance tools, and threat actor profiling, the study identifies exposures in the organization's external footprint and evaluates ransomware groups most likely to target the retail sector.

Findings reveal that The Kortnit's digital presence—over **2,000 domain hosts**, **10 exposed IP addresses**, and publicly available **emails and employee information**—creates a broad attack surface vulnerable to exploitation. If leveraged by sophisticated actors, such exposures could enable **phishing, impersonation attacks, credential theft, and ransomware campaigns**.

Two active and relevant threat groups—**Scattered Spider (UNC3944)** and **ALPHV/BlackCat**—were analyzed. Both possess capabilities to target large retailers, but Scattered Spider is assessed as the **highest-risk actor** due to its active focus on U.S. retail companies, reliance on help-desk impersonation, MFA fatigue, and abuse of remote access tools.

Overall, the assessment concludes that while no direct compromise of Kortnit's core systems is currently confirmed, **prior employee data leakage via third-party vendors** increases phishing susceptibility, and the current retail threat landscape elevates ransomware risk. Proactive mitigation, human-centric defenses, and enhanced monitoring are essential.

Scope and Methodology

Scope

- **Organization:** The Kortnit (Primary Domain: **kortinit.com**)
- **Sector:** Retail, global operations (brick-and-mortar and e-commerce)
- **Focus Areas:**

- External digital footprint exposures
- Threat actor profiling (active ransomware groups)
- Mapping of findings to MITRE ATT&CK
- Risk assessment and remediation recommendations

Methodology

1. **OSINT Reconnaissance**
    - Tools: Recon-NG, theHarvester, Shodan, Maltego, Sublist3r, Amass
    - Outputs: Enumeration of domains, sub-domains, IPs, employee emails, and related infrastructure.
2. **Threat Actor Analysis**
    - Reviewed recent campaigns and TTPs of relevant groups (Scattered Spider, ALPHV/BlackCat).
    - Mapped observed activities to **MITRE ATT&CK framework** for tactical relevance.
3. **Risk Evaluation**
    - Analyzed potential impact of exposed assets if exploited.
    - Assessed likelihood based on active campaigns against retail peers.
4. **Evidence Collection**
    - **Evidence sources: News outlets, vendor blogs (CrowdStrike, ReliaQuest), government advisories (IC3/CISA), and security news (Bitdefender, HIPAA Journal). (Key references are cited throughout.)**

Introduction

This project was conducted to gather **publicly available intelligence** on **The kortnit**, with the goal of identifying organizational exposure, assessing current threat actor relevance, and providing actionable recommendations.

Organization Overview:

The Kortnit is the **world's largest home improvement retailer**, serving DIY customers, professional contractors, and the home maintenance sector. The company offers a wide range of products including tools, lumber, paint, and appliances. Known for its **large store formats**, **customer service expertise**, and **exclusive brands**, Kortnit has also established a strong **e-commerce presence**. Beyond business, the company is recognized for **philanthropic efforts**, particularly supporting veterans through the Kortnit Foundatio**n.**

Detailed OSINT Findings (from your reconnaissance & corroborated OSINT)

1) External footprint — inventory and exposure

- **Domains / subdomains: > 2,000 discovered domain hosts and subdomains associated with `kortnit.com` and related brands/services (staging, dev, marketing, legacy). (Discovered via subdomain enumeration tools listed above.)**
- **Public IPs: 10 publicly visible IPs hosting services tied to Kortnit external infrastructure (catalog, marketing endpoints, vendor portals).**
- **Personnel data: Employee names and work emails (~10K employee records previously leaked publicly by a threat actor) were observed in open sources and breach-forum postings. AJCBitdefender**
- **Third-party exposure: Evidence of leaked employee data resulting from a third-party vendor incident (IntelBroker leak, Apr 2024). This increases successful-phishing risk because attackers can craft credible spear-phish and voice/social telephony attacks. SC MediaAJC**

2) What is exposed / immediate attack vectors

- **Phishing & spear-phishing (enabled by employee emails and subdomain footprint).**

- **Help-desk impersonation / vishing (attackers can use employee details and vendor info to convincingly spoof requests).**

- **Subdomain takeover potential where stale DNS/CNAME entries point to decommissioned services.**

- **Exposed admin portals / remote access (public IPs that may host services such as RDP, VPN concentrators, remote-admin panels).**

- **Third-party SaaS & vendor risk (vendor compromise used as pivot or source of leaked PII).**

3) Evidence of prior compromise or leak

- **Employee data leak (Apr 2024): IntelBroker publicly posted names and corporate email addresses for ~10,000 Home Depot employees on BreachForums; reported by major outlets. No confirmed ransomware of Kortnit corporate systems in public reporting, but phishing and impersonation risks are materially increased. BitdefenderAJC**

4) Risk level summary (based on likelihood × impact)

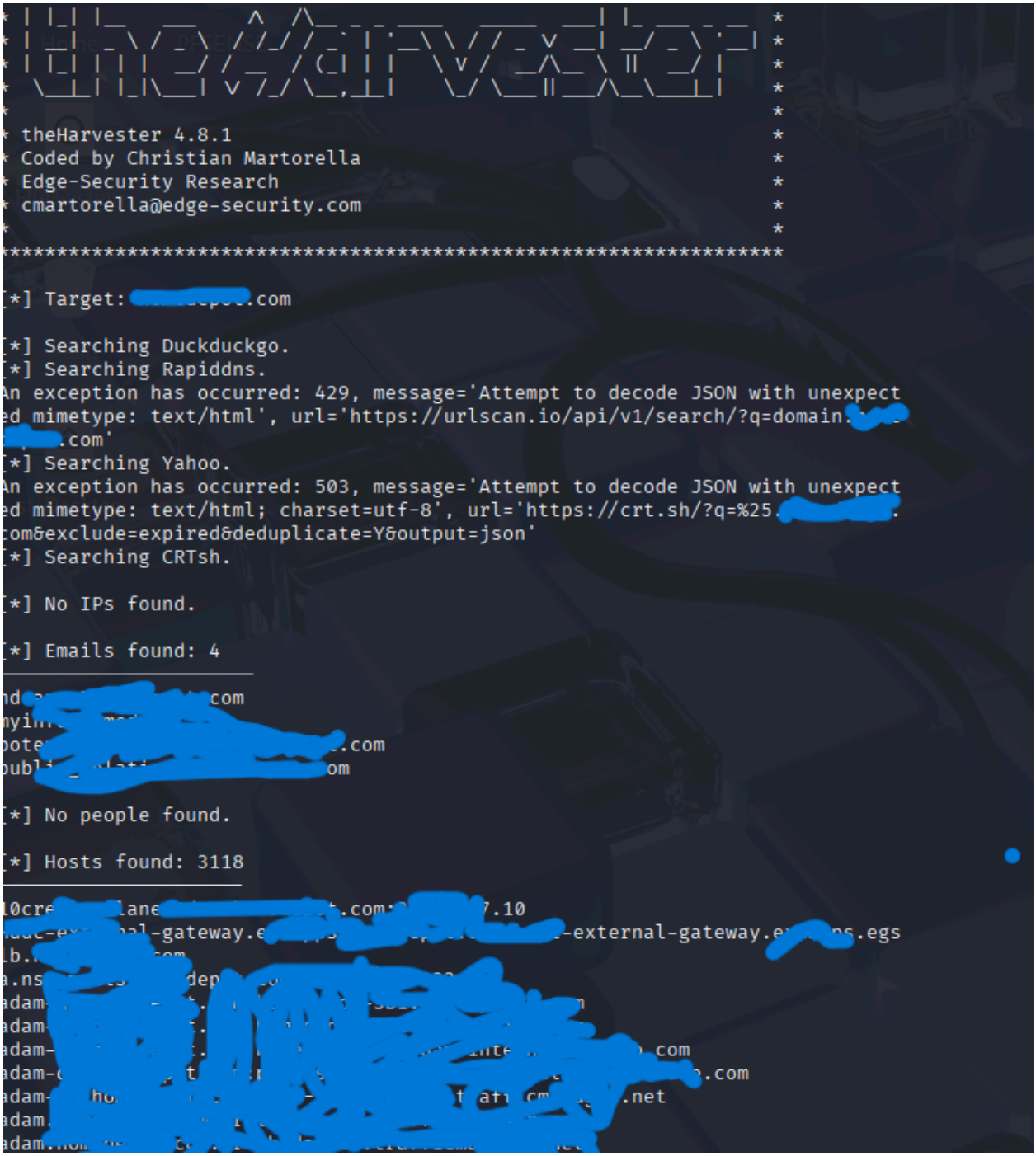
- **Phishing / credential compromise: High (employee emails public + active retail-targeting campaigns).**

- **Help-desk impersonation → privileged access: High (adversaries are actively using this vector in retail).**

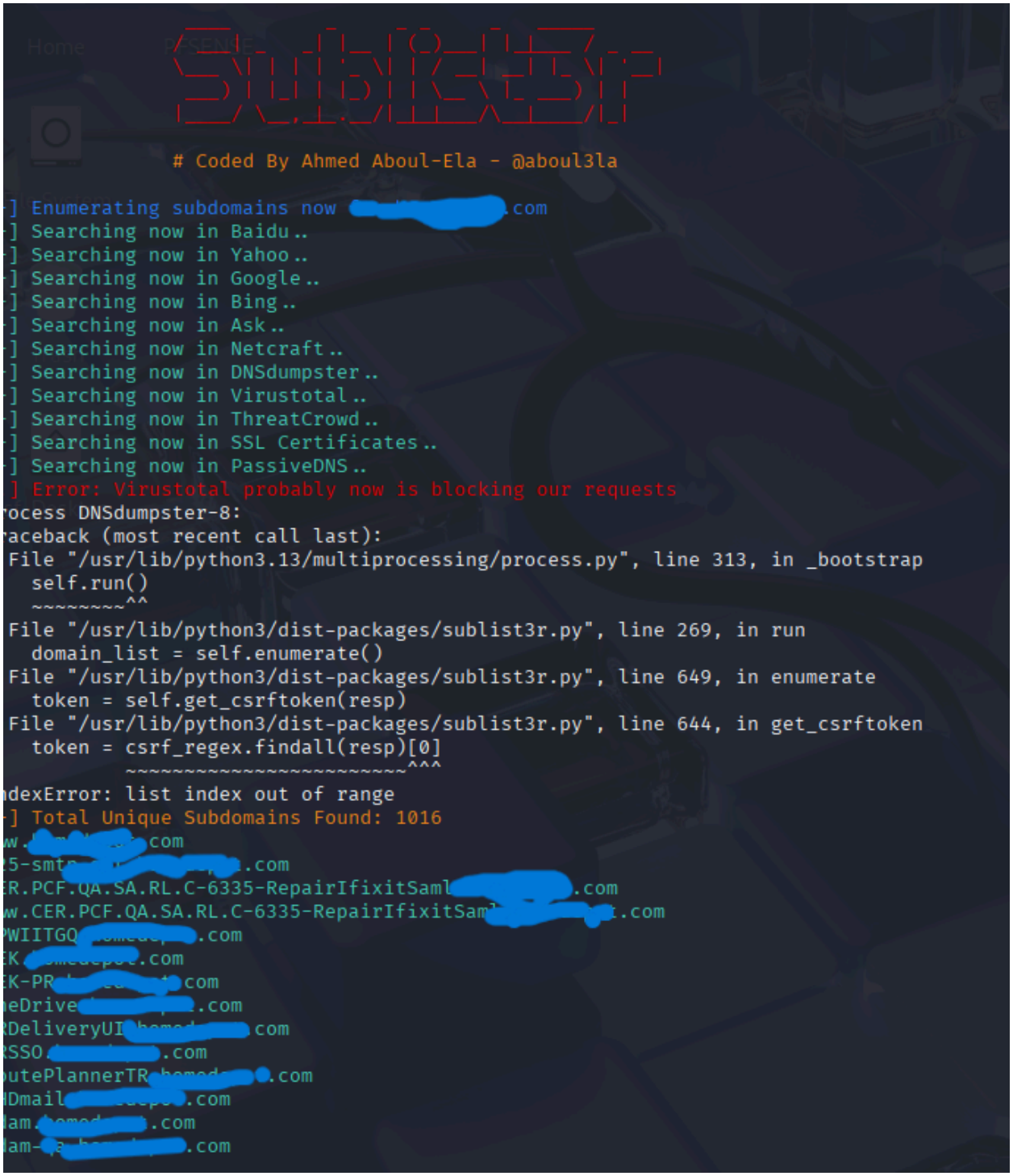
- **Ransomware / extortion event: High (probable) if initial access is achieved; retail operations and POS/logistics systems are attractive, high-impact targets.**

- **Data leak / compliance fines / reputational damage: High (customer data exposures, downtime, and regulatory scrutiny).**

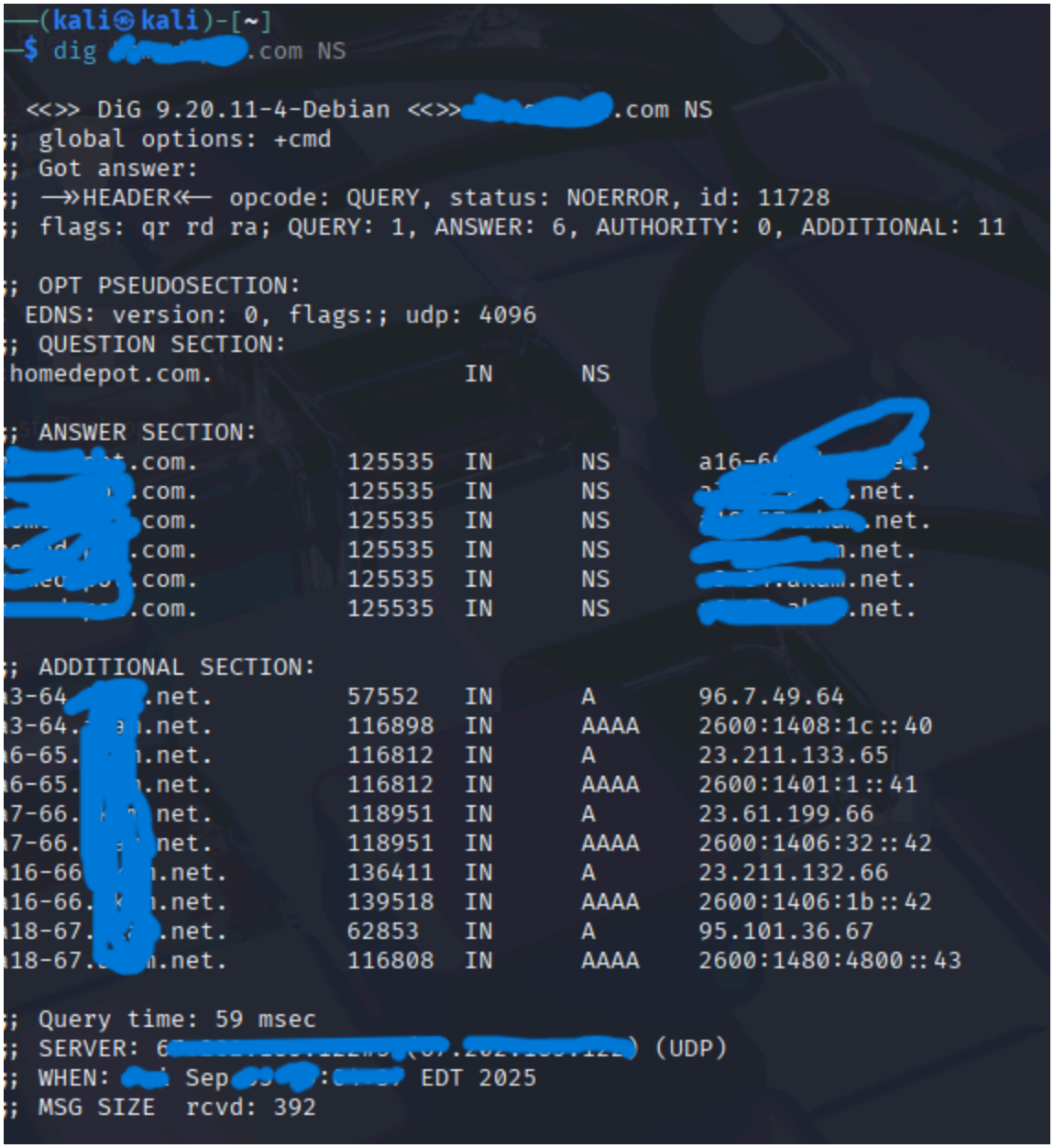
Some ScreenShort of the OSINT Reconnaissance tools used and its Results.
theHarvester.



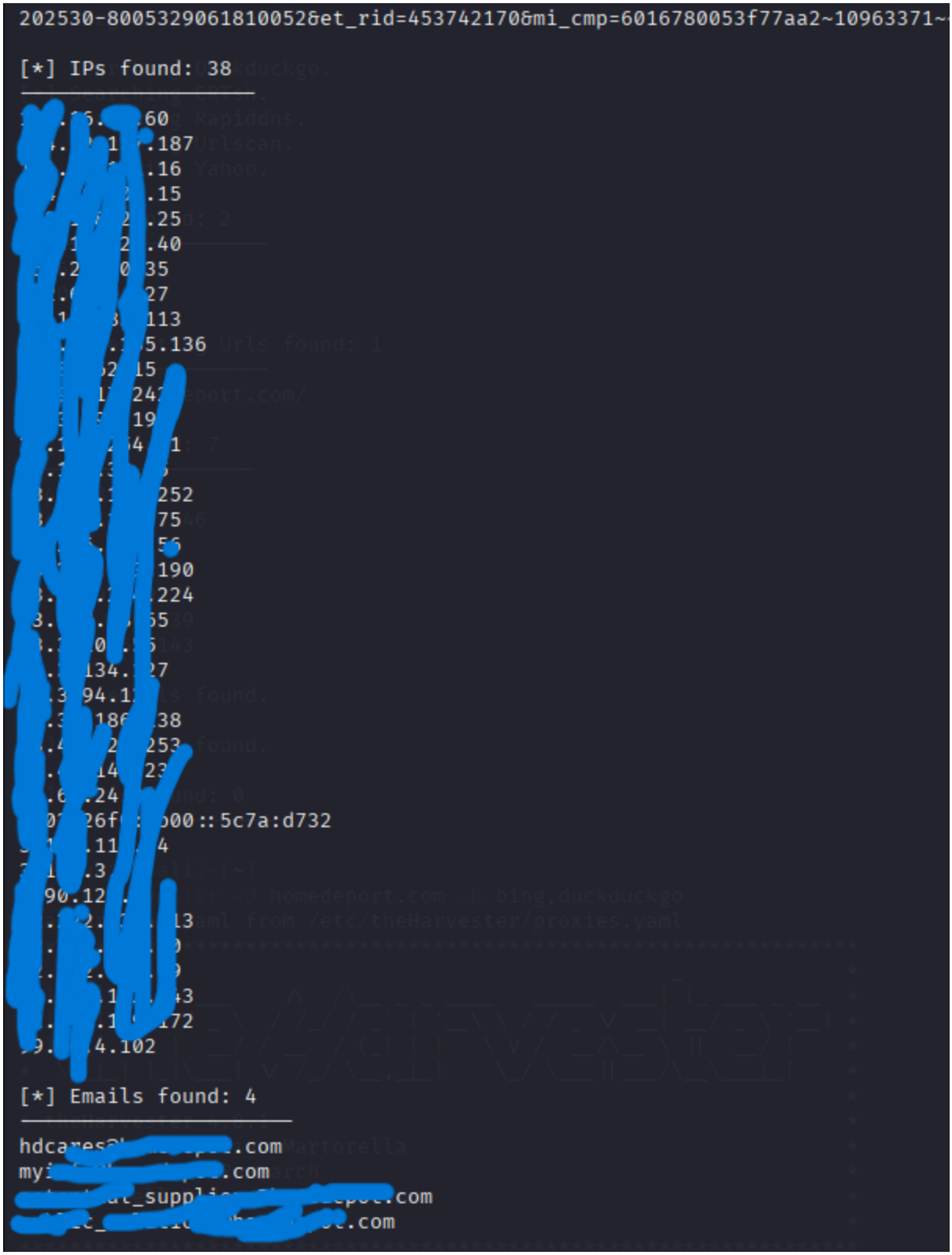
the Sublist3r


Coded By Ahmed Aboul-Ela - @aboul3la
] Enumerating subdomains now [redacted].com
] Searching now in Baidu..
] Searching now in Yahoo..
] Searching now in Google..
] Searching now in Bing..
] Searching now in Ask..
] Searching now in Netcraft..
] Searching now in DNSdumpster..
] Searching now in Virustotal..
] Searching now in ThreatCrowd..
] Searching now in SSL Certificates..
] Searching now in PassiveDNS..
] Error: Virustotal probably now is blocking our requests
rocess DNSdumpster-8:
raceback (most recent call last):
File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
self.run()
~~~~~~~~^^
File "/usr/lib/python3/dist-packages/sublist3r.py", line 269, in run
domain_list = self.enumerate()
File "/usr/lib/python3/dist-packages/sublist3r.py", line 649, in enumerate
token = self.get_csrftoken(resp)
File "/usr/lib/python3/dist-packages/sublist3r.py", line 644, in get_csrftoken
token = csrf_regex.findall(resp)[0]
~~~~~~~~~~~~~~~~~~~~~~~~^^^
ndexError: list index out of range
] Total Unique Subdomains Found: 1016
[redacted].com
[redacted].com
[redacted].com
[redacted].com
[redacted].com
[redacted].com
[redacted].com
[redacted].com
[redacted].com
[redacted].com
[redacted].com
[redacted].com
[redacted].com

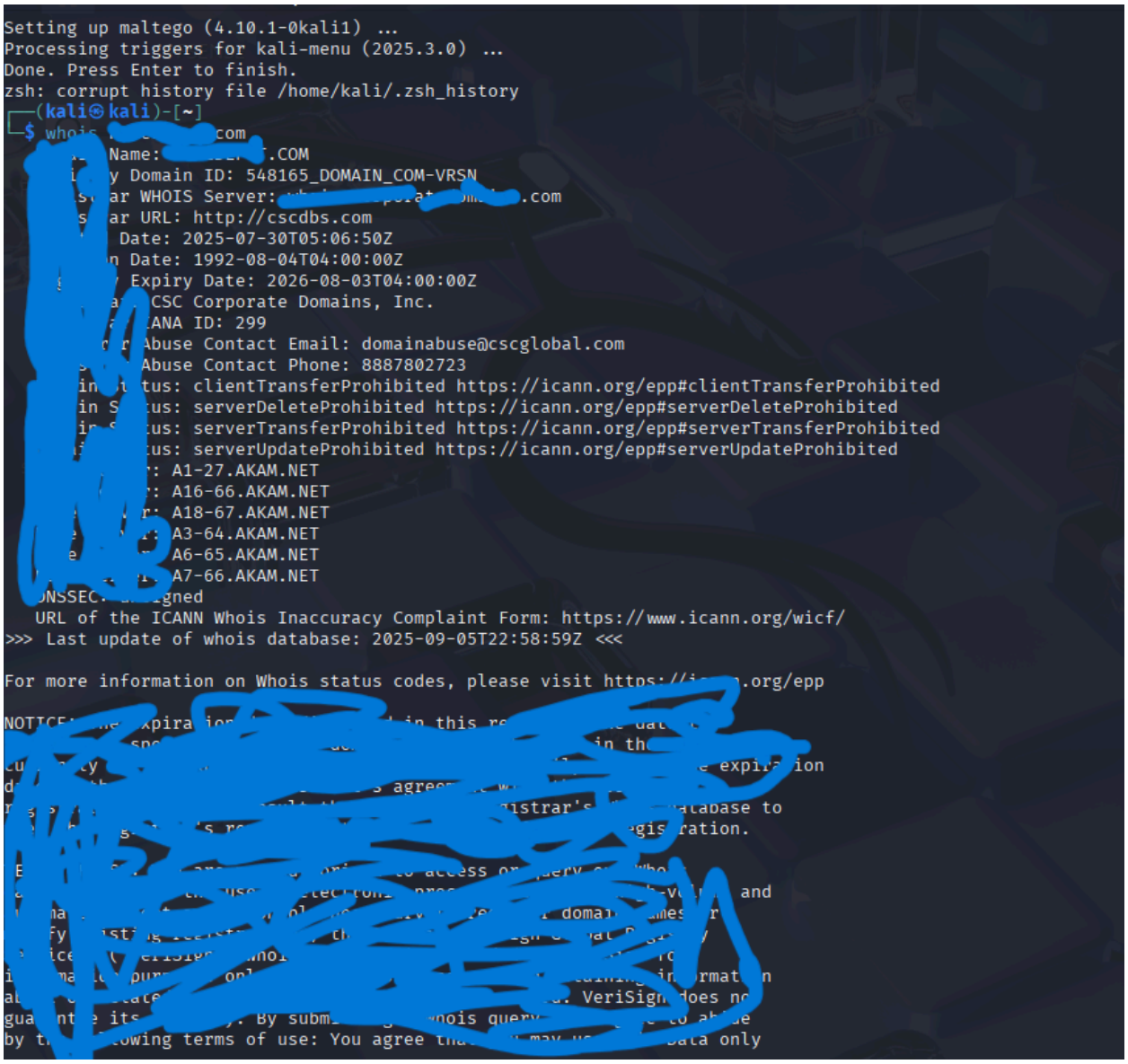
the Shodan


(kali㉿kali)-[~]
$ dig [redacted].com NS
<<>> DiG 9.20.11-4-Debian <<>> [redacted].com NS
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11728
; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 11
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; QUESTION SECTION:
homedepot.com. IN NS
; ANSWER SECTION:
[redacted].com. 125535 IN NS a16-6[redacted].
[redacted].com. 125535 IN NS [redacted].net.
[redacted].com. 125535 IN NS [redacted].net.
[redacted].com. 125535 IN NS [redacted].net.
[redacted].com. 125535 IN NS [redacted].net.
[redacted].com. 125535 IN NS [redacted].net.
; ADDITIONAL SECTION:
[redacted].net. 57552 IN A 96.7.49.64
[redacted].net. 116898 IN AAAA 2600:1408:1c::40
[redacted].net. 116812 IN A 23.211.133.65
[redacted].net. 116812 IN AAAA 2600:1401:1::41
[redacted].net. 118951 IN A 23.61.199.66
[redacted].net. 118951 IN AAAA 2600:1406:32::42
[redacted].net. 136411 IN A 23.211.132.66
[redacted].net. 139518 IN AAAA 2600:1406:1b::42
[redacted].net. 62853 IN A 95.101.36.67
[redacted].net. 116808 IN AAAA 2600:1480:4800::43
; Query time: 59 msec
; SERVER: [redacted] (UDP)
; WHEN: [redacted] Sep [redacted] EDT 2025
; MSG SIZE rcvd: 392

the Amass


202530-8005329061810052&et_rid=453742170&mi_cmp=6016780053f77aa2~10963371~
[*] IPs found: 38
[*] Emails found: 4

Maltego



Threat Actor Profiles (two prioritized actors)

A — Scattered Spider (UNC3944 / “Scattered Spider”) — *Highest Immediate Risk*

Why relevant to Kortnit, (summary):

- **Recent, high-profile campaigns targeted major retailers (e.g., Marks & Spencer, Co-op, Harrods) causing prolonged outages and large financial impact; reporting indicates English-speaking social-engineering specialists focusing on retail help desks and support workflows. This actor type is highly relevant given Kortnit’s large, geographically distributed retail workforce and reliance on help-desk**

operations. The GuardianCybersecurity Dive

Recent activity / attribution (selected):

- **April–May 2025 retail campaigns in the UK impacted M&S and others; U.K. NCA and major publications tied the activity to Scattered Spider. Public advisories and vendor blogs describe escalation of such activity into mid-2025. The GuardianCrowdStrike**

Primary motivations: Financial extortion (ransom, double-extortion), opportunistic disruption.

Typical TTPs (observed & mapped to MITRE ATT&CK):

- **Initial Access**
    - **Spearphishing (T1566) — targeted emails using leaked employee info. Bitdefender**
    - **Phone-based social engineering / vishing (T1598 / T1476). ReliaQuest**
    - **SIM swap / account takeover to defeat MFA (T1535?). Google Cloud**
- **Execution / Persistence**
    - **Use of legitimate remote-access tools (AnyDesk, TeamViewer) and remote support sessions (T1219, T1021). ReliaQuest**
    - **Creating/compromising valid accounts (T1078) via help-desk resets.**
- **Defense Evasion**
    - **MFA fatigue or bypass (T1529 / T1110 variant behaviors), masquerading as support employees (T1036).**
- **Exfiltration / Impact**
    - **Data theft and extortion (data-leak sites, public shaming, operational disruption). Retail Council of Canada**

Observed or expected IOCs (public reporting / operational indicators):

- **Behavioral IOCs (most reliable):**
    - **Unusual brute-force or MFA-bypass attempts from known public networks.**
    - **Spikes in support-desk password resets originating from unexpected channels.**
    - **AnyDesk/TeamViewer sessions initiated from external IPs tied to new accounts.**
    - **Typosquatted domains mimicking vendor or vendor-support sites used in phishing campaigns.**
- **Documented references & advisories: IC3/CISA advisory on UNC3944 / Scattered Spider contains specific observables and recommended responses (see reference). Internet Crime Complaint Center**

Past impacted sectors / examples: Retail (M&S, Co-op, Harrods), Hospitality (MGM/Caesars historically linked to similar social-engineering chains), Cloud customers (reporting indicates cloud service account compromises tied to social engineering). Retail Council of CanadaCybersecurity Dive

Why this is highest risk for Home Depot: Scattered Spider prioritizes live social-engineering against help desks, and Home Depot's large, distributed support/IT help ecosystems (store associates, third-party vendor support) present many human-centric attack opportunities.

B — ALPHV / BlackCat — *Strategic / Capable RaaS Threat*

Why relevant to Kortnit:

- **ALPHV (aka BlackCat) is a sophisticated RaaS that has performed large, high-impact attacks with double-extortion and robust encryption; retail organizations are within their sector set due to valuable POS / customer data and ability to cause major operational disruption. kortnit's size and revenue profile make it a high-value target. The HIPAA JournalThe Record from Recorded Future**

Recent activity / attribution (selected):

- **ALPHV affiliates conducted major operations in healthcare and enterprise targets (Change Healthcare, Feb 2024), and ALPHV/BlackCat behavior and successors**

have been tracked in 2024–2025 reporting. Some successor groups or rebrands (e.g., Embargo) show continued activity. [The HIPAA Journal](#)[The Record from Recorded Future](#)

Typical TTPs (mapped to MITRE ATT&CK):

- **Initial Access: Phishing, compromised credentials (T1566, T1078), exploitation of public-facing apps (T1190).**
- **Lateral Movement / Privilege Escalation: RDP/VPN compromise (T1021), exploitation of vulnerabilities for privileged access (T1068/T1210).**
- **Impact: Encryption (T1486), exfiltration (T1041) followed by double-extortion on leak sites.**
- **Post-compromise: Use of custom loaders, potential use of Rust-based payloads (observed in reporting). [The HIPAA Journal](#)**

IOCs & Observables (public reporting):

- **ALPHV has been associated with public leak sites and certain wallet addresses and infrastructure tracked by incident responders; specific IOCs are available in vendor incident reports (referenced sources). [The HIPAA Journal](#)[The Record from Recorded Future](#)**

Why this is a significant but slightly lower immediate risk than Scattered Spider: ALPHV is highly capable but often requires more technical initial access (exploits, lateral movement) or an affiliate with social-engineering capability. Scattered Spider's focused, human-centric approach increases likelihood of initial compromise against Kortnit's exposed human and domain footprint.

Comparative Threat Decision

- **Greatest immediate threat: Scattered Spider (UNC3944) — active, retail-focused social engineering and help-desk attacks documented in 2025 make successful initial access against Kortnit plausible. [The Guardian](#)[Internet Crime Complaint Center](#)**
- **Secondary, high-impact threat: ALPHV / BlackCat — capable of devastating ransomware operations if initial access is obtained or if an affiliate targets Home**

Depot's environment. [The HIPAA Journal]

Indicators of Compromise (IOCs) — practical list & where to look

Note: Many precise IOCs (files, C2 IPs, wallet addresses) change rapidly. Use the vendor/government advisories and your TI platform for up-to-date indicators. Below are reliable behavioral and observable classes to hunt for.

1. **Help-desk / admin anomalies**
    - **Sudden surge in password resets, account unlocks, or admin privilege elevation requests from non-typical IPs (especially from foreign IP ranges).**
    - **Password reset requests initiated via support channels outside normal business hours.**
2. **Remote access tool usage**
    - **AnyDesk / TeamViewer / other remote-support sessions initiated from new external IPs or to non-standard endpoints.**
    - **Sessions that request unattended access or new install tokens.**
3. **Phishing & domain indicators**
    - **Typosquatted / newly registered domains that mimic internal vendor or portal names (monitor domain registration feeds).**
    - **Phishing emails using employee names, org units, or HR/benefits language consistent with previously leaked PII.**
4. **Network & endpoint**
    - **New or unusual RDP endpoint exposures, suspicious VPN connections, anomalous lateral movement.**
    - **Unusual file encryption activity or mass deletion of backups.**

5. **Public leak / dark web monitoring**
    - **Mentions of `Kortnit` or related entities on leak sites or criminal forums (automate monitoring for these keywords).**

Sources for curated IOCs: IC3/CISA joint advisories on UNC3944 and vendor-published IoC lists (CrowdStrike, ReliaQuest, Google Cloud threat blog). Internet Crime Complaint CenterCrowdStrikeGoogle Cloud

---

Potential Impact Scenarios (realistic examples)

1. **Help-desk compromise → privileged access**
    - **Attackers socially engineer help-desk, obtain password resets, escalate to domain admin, deploy ransomware — result: store POS and inventory systems offline, multi-day outage, revenue/time lost, customer impact.**
2. **Credential theft via spear-phish**
    - **Compromised employee credentials used to access vendor portals, payment processors, or cloud resources → exfiltration of customer PII and supply chain compromise → regulatory, legal, and reputational damage.**
3. **Double-extortion ransomware**
    - **ALPHV or affiliate encrypts critical systems and exfiltrates data, then posts copies to leak site → ransom negotiation, loss of trust, legal implications, potential fines.**

Actionable Recommendations — prioritized & mapped to findings

Immediate (0–30 days)

1. **Help-desk hardening (Top priority)**

- **Enforce strict multi-factor verification for all password resets and sensitive support actions (callback to pre-known numbers, use of pre-shared secret tokens not stored in email).**

- **Deny password resets requested via email or chat unless verified via multi-channel confirmation.**

- **Run immediate training & situational awareness exercises for help-desk staff to recognize Scattered Spider-style tactics. Google CloudCrowdStrike**

2. **Phishing containment**

    - **Deploy targeted phishing simulations using actual leaked employee details to measure susceptibility and train staff.**

    - **Block known typosquat domains and implement DMARC/DKIM/SPF enforcement for all org domains.**

3. **Inventory & remove stale public assets**

    - **Rapidly identify and decommission stale subdomains, stray DNS entries, and abandoned cloud assets to reduce takeover vectors.**

4. **Monitor & alert on remote-support usage**

    - **Implement detection for anomalous AnyDesk/TeamViewer sessions and alert on connections from suspicious IPs or new accounts.**

Near term (30–90 days)

5. **Third-party risk management**

    - **Reassess vendor access privileges, especially vendors with administrative access to systems; require MFA and just-in-time (JIT) privileged access for vendors.**

6. **Enhance detection & threat hunting**

    - **Hunt for behavioral IOCs: unusual password resets, support ticket anomalies, remote tool usage, MFA bypass attempts. Integrate feeds from CISA/IC3 and vendor TI for Scattered Spider/UNC3944 and ALPHV. Internet Crime Complaint CenterCrowdStrike**

7. **Backup & resilience**
    - **Confirm immutable off-site backups, practice recovery steps, and isolate backups from production networks.**

Strategic (90+ days)

8. **Tabletop exercises & incident playbooks**
    - **Execute tabletop exercises simulating Scattered Spider social-engineering attacks and an ALPHV ransomware event. Validate communication, containment, and restoration plans.**
9. **Technical hardening**
    - **Patch management for internet-facing services, reduce RDP exposure, enforce conditional access policies, and segment high-value systems.**
10. **Threat intelligence subscription & sharing**

- **Subscribe to retail-specific threat feeds and participate in ISACs to exchange indicators (e.g., Retail & Consumer Goods ISAC), and integrate vendor advisories. [Retail Council of Canada]**

Recommended Monitoring Playbook (quick)

- **Hunt query examples: high volume of password resets within short time window; remote-admin sessions to production hosts outside business hours; sudden creation of privileged accounts; new domain registrations mimicking internal vendors.**
- **External monitoring: automated monitors for mentions of `kortnit` on data-leak forums and ransomware leak sites.**
- **Notification: subscribe to IC3/CISA advisories and vendor threat intel (CrowdStrike, Google Cloud, ReliaQuest).**

References (key sources)

1. **U.K. coverage & NCA reporting on Scattered Spider retail attacks (May 2025).** The Guardian

2. **IC3 / CISA joint advisory on UNC3944 / Scattered Spider (Jul 29, 2025).** Internet Crime Complaint Center

3. **CrowdStrike analysis of Scattered Spider escalation (Jul 2, 2025).** CrowdStrike

4. **Google Cloud blog — proactive hardening for UNC3944 (May 6, 2025).** Google Cloud

5. **Home Depot employee data leak reporting (IntelBroker — Apr 2024; outlets: AJC, Bitdefender).** AJCBitdefender

6. **ALPHV / BlackCat campaign reporting (Change Healthcare, 2024; successor activity reporting).** The HIPAA JournalThe Record from Recorded Future

7. **Vendor & sector notices about retail attacks and mitigation guidance (ReliaQuest, Retail Council).** ReliaQuestRetail Council of Canada

---