Confidential

Monthly Report: August 2025

Intelligence Summary:

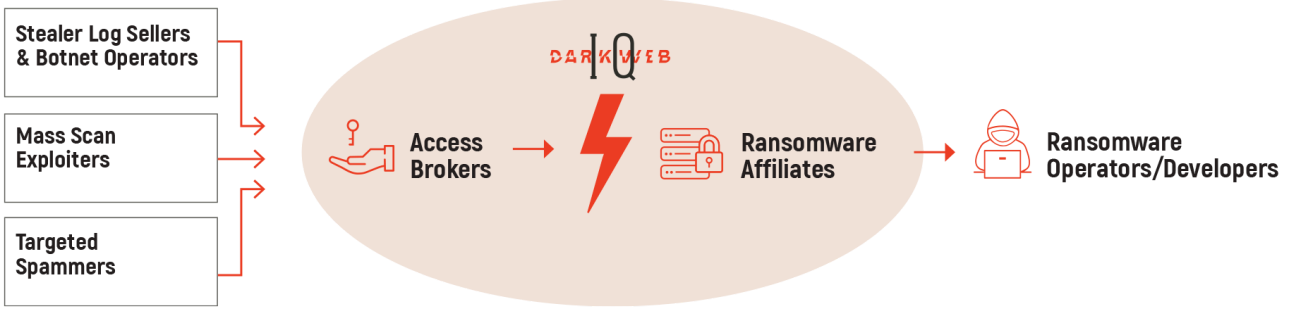
Darkweb IQ (“DWIQ”) conducted **59 Attack Interceptions** in August and conducted **an additional 66 FBI notifications** with actionable intelligence on other active compromises by credible threat actors.

Dashboard Statistics:

DWIQ Comprehensive Interception Statistics (All Clients):

Access Broker Interceptions This Month:	59
All-Time Access Broker Interceptions:	2005
FBI Notifications This Month:	66
All-Time FBI Notifications:	2580
All-Time Threat Actors Engaged:	548

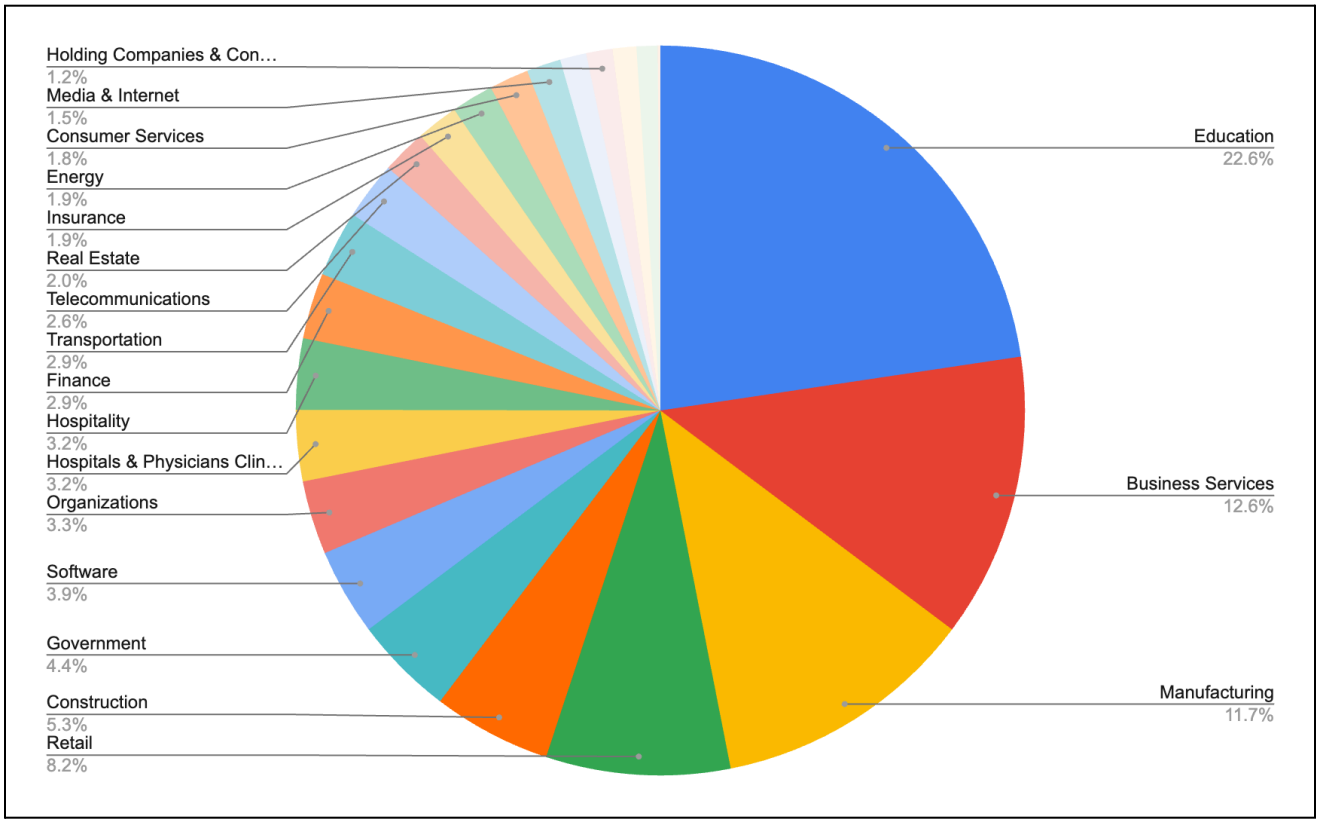
Ransomware Supply Chain



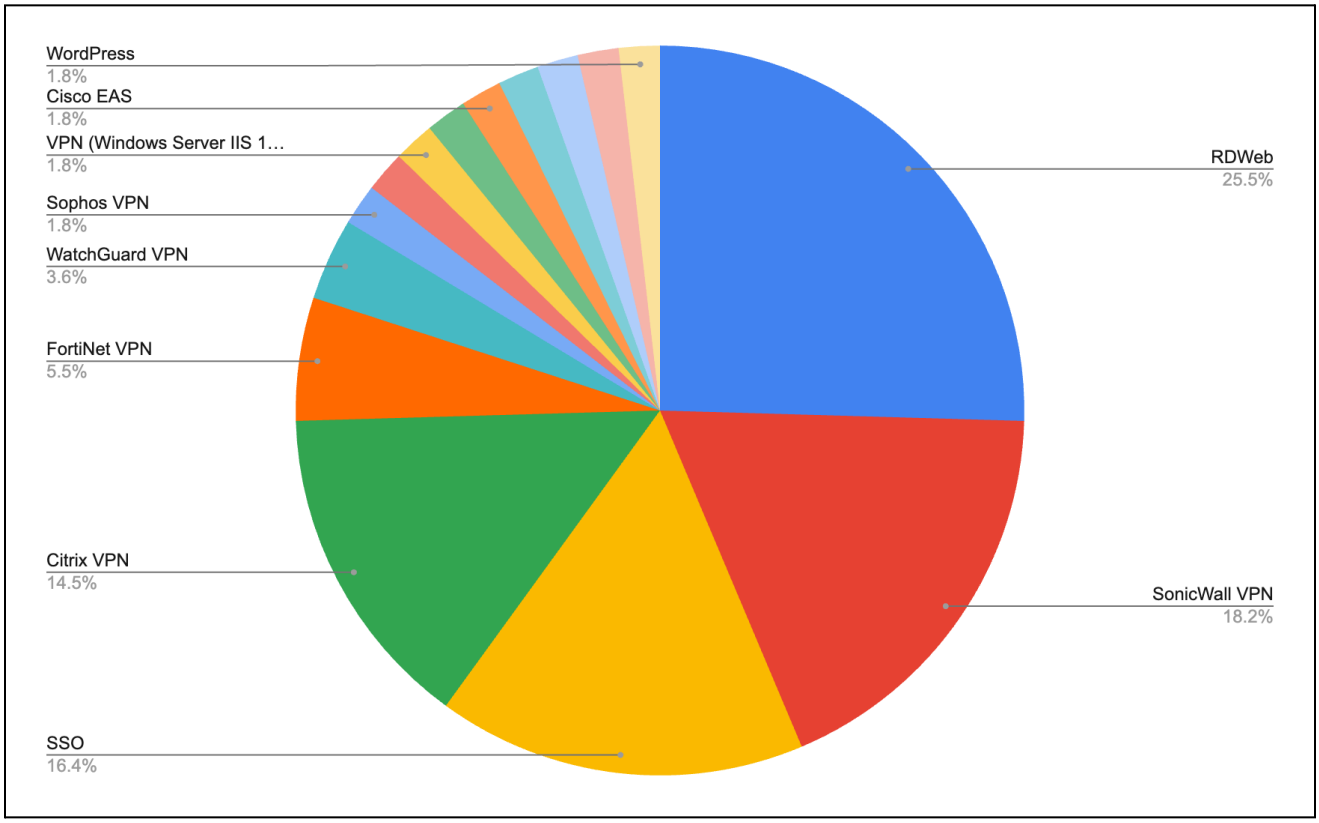
Intelligence Commentary:

In August, **DWIQ was privately offered network access to 860 U.S., Canadian, and European-based corporate environments.** This represents a 41% increase over August 2024.

Initial Access Broker Victims by Industry:



Initial Access Broker Victims by Access Type:



Critical Supply Chain Databases, Old but Critical CVEs, and a Different Attack Vector

BLOT:

In August, Darkweb IQ operatives disrupted a threat actor leveraging **Burp Suite** to probe critical infrastructure, including exploitation of the legacy **CVE-2020-6287 (SAP RECON)** vulnerability. The actor gained reconnaissance-level access to an industrial supplier and created administrative accounts within a healthcare supply chain subdomain before intervention halted activity.

Commentary:

While Burp Suite is a licit penetration testing tool, malicious use enables systematic web application reconnaissance, endpoint discovery, and backend fingerprinting. In this case, the actor exploited **CVE-2020-6287**, a critical unauthenticated RCE vulnerability in **SAP NetWeaver AS Java (7.3–7.5)** with a CVSS score of 10.0. Exploitation permits arbitrary code execution through the LM Configuration Wizard. The actor had advanced to reconnaissance and unauthorized account creation in healthcare supply chain infrastructure before takedown. This incident underscores the persistence of "old but critical" CVEs, which remain viable years after disclosure when production systems are unpatched.

Defensive Considerations:

- Verify patch levels of SAP NetWeaver AS Java and remediate systems running versions 7.3–7.5.
- Monitor web logs for reconnaissance-style activity: **high volumes of 404/500 errors, sequential path enumeration, abnormal query-string fuzzing, and repeated probing of hidden endpoints**.
- Alert on anomalous HTTP verbs or malformed requests that suggest automated scanning tools.

The Manual of a Major Ransomware Gang

BLOT:

In early August, DWIQ obtained a **manual used by RansomHub ransomware affiliates**, providing detailed TTP guidance for initial access, lateral movement, privilege escalation, and network encryption.

Commentary:

The manual describes techniques including RDP and Kerberos brute-forcing, credential harvesting with **Rubeus** and **Netexec**, domain trust discovery via LDAP, and credential dumping with **Secretsdump**. Affiliates are instructed to disable Windows Defender via GPO, use **PSExec** and

WMI for lateral movement, and deliver payloads through .bat scripts and executables. Event logs are cleared with wevtutil and PowerShell post-encryption.

While no radically new TTPs were revealed, the manual confirms several ongoing affiliate practices of intelligence value:

- Increased targeting of **Windows-based SSTP VPN endpoints**, which run over TCP/443 and often blend with normal HTTPS traffic.
- Interest in **MeshCentral** (legitimate RMM software) as a beaconing and persistence tool.
- Continued use of legacy but effective credential and lateral movement tools.

Defensive Considerations:

- Harden RDP and Kerberos authentication against brute-forcing with MFA and rate-limiting.
- Monitor for suspicious use of PSExec, WMI, and .bat script deployment.
- Audit for abnormal GPO changes (e.g., disabling Defender) and unauthorized MeshCentral deployments.

Forum Takedown Causes Confusion, but Does Not Stop Access Sales

BLOT:

The late July arrest of a suspected XSS forum operator and related disruption fragmented the Russian-speaking cybercriminal forum landscape, spawning multiple successor forums but not pausing IAB sales activity.

Commentary:

Successor forums include:

- A restored XSS instance on the old onion and new clearnet domains with new administrators.
- A second forum on a new domain led by former moderators.
- A third smaller forum launched by a prominent member.

Despite initial momentum, none have drawn significant adoption. Many actors remain wary, suspecting honeypot operations. Authorities have not confirmed the arrested individual's exact role within the forum hierarchy, and no evidence of backend compromise has been released. IAB listings have largely paused, with some brokers privately confiding they will avoid forums temporarily. Nonetheless, IAB trade continues off-forum, and activity is expected to rebound following the summer lull.

The disruption primarily affects **trust-building and recruitment of new buyers**, rather than halting established broker operations. DWIQ's persistent engagement with IABs ensures continuity of collection despite forum instability.

Other CVEs

CVE-2025-8069 (AWS Client VPN for Windows)

In August, a known IAB with ties to Akira, RansomHub, Play, and INC Ransom claimed successful exploitation of CVE-2025-8069 against a U.S.-based company. The vulnerability allows **local privilege escalation** during installation by abusing a writable OpenSSL configuration path. The actor described their process: placing a malicious config file, locating the VPN client, and escalating to SYSTEM-level access upon VPN launch. Passive scan data confirmed that the IP address provided resolves to infrastructure owned by the claimed victim. The actor's description aligns with AWS's advisory, though technical validation of the credential's usability is pending.

Defensive Considerations:

- Apply AWS Client VPN patch **v5.2.2** immediately to Windows systems.

- Restrict write access to C:\usr\local\windows-x86_64-openssl-localbuild\ssl\.
- Monitor for unauthorized file creation in the above path prior to vpnclient.exe execution.

CVE-2025-232756 (Fortinet Products)

A medium-credibility actor offered a working exploit for a **stack-based buffer overflow** in Fortinet products. Exploitation requires sending HTTP requests with crafted hash cookies. The actor admitted few vulnerable hosts exist, limiting profitability. The exploit is based on a public PoC and offered at a low price, lowering the barrier to entry for opportunistic actors.

Defensive Considerations:

- Patch Fortinet appliances to vendor-recommended versions.
- Monitor for abnormal HTTP traffic patterns targeting hash cookie parameters.

Your Feedback Matters

We're committed to providing you with valuable insights and actions to protect your interests. Please share your feedback or topics of interest for future commentaries.