It's Probably Nothing
by Sierra Echo Charlie

EDITION 05 / 20 OCTOBER 2026

Ransom negotiators, NetScaler keys and a DeepSeek ban

Who's really across the table, why patching NetScaler isn't eviction, and a hypervisor-level heist.

4 stories / Listen online - 5:32

THE TAKEAWAY

Mostly investigative reporting and research today rather than fresh fires, but the lead story is a genuinely uncomfortable one for anyone whose IR playbook ends with "call the negotiator".

01 / THE BRIEF

Feds reportedly suspect a ransom negotiator helped run ShinyHunters' leak site

KrebsOnSecurity, citing sources close to the investigation, reports that US federal investigators have identified executives at two ransomware negotiation firms with unusually close relations to ShinyHunters. Two sources told Krebs the FBI believes at least one executive at a US consulting firm with more than 1,000 associates played an active role in operating shinywire[.]com, the group's victim-pressure site. Krebs doesn't name the firm or person because nobody there has been charged, so treat this as reported suspicion, not established fact.

Per Krebs, Shinywire ran from about 3 May until 16 October, listing nearly 100 organisations with stolen-file samples; victims who didn't engage within seven days had data dumped on a Tor blog. One source says Signal messages seized at Pepijn van der Stap's 15 September arrest showed frequent chats with Edward Dubrovsky and at least one US consulting executive, and that these executives often knew about new victims before the victims did. The same source claims the chats show Dubrovsky knew the group had stolen sensitive FBI data and didn't tell the bureau. Dubrovsky, a Canadian cybersecurity executive, is charged with extortion-related offences per court records Krebs cites; he's presumed innocent, and Politico reports the records are sealed.

The FBI, via Krebs, puts ShinyHunters' haul this year at more than US$70 million. Cypfer said on 14 October it doesn't make or facilitate ransom payments and, to its knowledge, isn't a target of any investigation.

Even if the specifics never reach a courtroom, it's hard to unhear CyberAcuView chief executive Mark Camillo's point to Krebs: negotiators paid a percentage of the final payment have an inherent conflict of interest. And Krebs's reminder that PowerSchool paid US$2.85 million with CyberSteward's help, only for school districts to later get separate demands using the same data, is a neat illustration of what a paid-for deletion promise is worth. Nobody has alleged ShinyHunters was behind that second wave.

WORTH ASKING

If your insurer or retainer routes negotiations through a third party, it might be worth knowing who that is and how they're paid before you need them.

QUALIFICATIONS

Rests on one outlet's anonymous sources; the US executive is unnamed and uncharged.

SOURCES

Feds Suspect Ransom Negotiator Ran ShinyHunters Extortion Site - Krebs on Security - Primary source

U.S. Investigators Suspect Ransom Negotiator Helped Run ShinyHunters Extortion Site - Reporting / context

02 / THE BRIEF

Rapid7 confirms the NetScaler reboot trick, and the attackers took the keys with them

Rapid7 has published forensics from an early-October compromise of a NetScaler ADC on an affected 14.1 build. Logs show CVE-2026-88771 (pre-auth log poisoning) chained with CVE-2026-88779 (a SAML-parsing crash): the crash knocked over nsaaad, Pitboss rebooted the box, and the call-home crash handler then ran the attacker's payload as root. Rapid7 says this skipped a 24-hour wait for the payload, and repeated reboots over several days let the operator refresh persistence. Using a crash handler as a root scheduler is grimly elegant.

Then they moved in. Cookie-authenticated PHP web shells hid behind CSS-looking LogonPoint aliases and returned output in 404 bodies; /bin/sh was repeatedly set to mode 6555. The implant tried to sync itself to the HA peer and force failover onto the infected node. A FreeBSD Go tool mapped internal DNS (including zone-transfer attempts), LDAP/AD, management services and vCenter. And the attacker exfiltrated ns.conf.0-4 and system backups, which can hold LDAP/RADIUS bind data, SSL private keys and key-encryption material; Rapid7 confirmed one download by an HTTP 200 matching the archive size. Rapid7 says it overlaps with the WHIPSHOT/SLAPSHOT campaign reporting.

These aren't new bugs: CVE-2026-88771 hit KEV on 27 September, and CISA had already flagged CVE-2026-88779 as exploited. What's new is the real-world confirmation that patching neither evicts an implant sitting on both HA nodes nor un-steals your private keys.

WORTH ASKING

If you ran a vulnerable internet-facing NetScaler during the campaign, Rapid7's advice is to treat it as potentially compromised: grab volatile evidence before rebooting, check both nodes of every HA pair, and rotate credentials and keys exposed via /nsconfig.

QUALIFICATIONS

Single incident analysis; no evidence of a new exploitation wave.

SOURCES

NetScaler intrusions chaining CVE-2026-88771 and CVE-2026-88779 - Primary source

Exploited Citrix NetScaler Command Injection Enables Unauthenticated Root Access - Reporting / context

03 / THE BRIEF

FirstVDS customers robbed from underneath, with the fix still incomplete

Russian hosting provider FirstVDS says attackers exploited a flaw in ISPsystem's VMmanager 6 (Xakep dates it to 17 October) to run malware on some virtualisation hosts. That malware mounted customer disks read-only and copied passwords, SSH and API keys, cloud tokens, configs, command history, wallet data and user files. Nothing ran inside guests, so there's nothing for customers to find. FirstVDS hasn't said how many were hit.

As of 19 October, FirstVDS says ISPsystem has shipped several patches, including one overnight Monday, but the hole isn't fully closed and management access stays off. Customers have been told to assume everything was copied and to revoke, not just reissue, keys and tokens.

Direct exposure here is probably small, though The Record notes FirstVDS also hosts in the Netherlands and Kazakhstan. It's a tidy example of the management plane being the whole game.

QUALIFICATIONS

Facts come via The Record and Xakep relaying FirstVDS; exploitation method, versions and attacker are undisclosed.

SOURCES

Hackers steal customer data from major Russian hosting provider FirstVDS - Reporting / context

□□□□□□□□ FirstVDS □□□□□□□□ □ □□□□□□ - □□□□□ - Reporting / context

FirstVDS Customer Data Stolen Through VMmanager 6 Vulnerability - Reporting / context

04 / THE BRIEF

DHS quietly banned DeepSeek from civilian agencies back in June

CyberScoop reports a Federal Register notice, due Tuesday, under which DHS bars civilian agencies from buying any IT products or services from Hangzhou DeepSeek Artificial Intelligence, using the Federal Acquisition Supply Chain Security Act after a Federal Acquisition Security Council review. The kicker: Secretary Markwayne Mullin's order is dated 26 June, so it's been in force for months. His letter cites data stored in China, PII collection and prompts potentially reaching the Chinese government. Agencies must remove existing deployments, exceptions need 60 days' notice and a "compelling justification", and agencies are encouraged to add logging and exfiltration controls until it's gone. DeepSeek is the only Chinese AI model named.

Supply-chain exclusion powers pointed at an AI model maker is a notable precedent, even if the ban itself is old news to the agencies involved.

QUALIFICATIONS

Single-sourced to CyberScoop; the notice itself wasn't yet published or read.

SOURCES

DHS to ban DeepSeek from federal civilian agencies - Reporting / context

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.