Dark Peep #17: Dark Web Manifesto, Hacker Forums, and Ransomware Misadventures

Published: 2024-12-17 · Archived: 2026-04-05 17:34:29 UTC

If the events from dark web this series were a script, it would be the kind of thriller where everyone fumbles their part. From ransomware gangs accidentally losing their own ransom records to threat actors leaking millions of records, it's a chaotic mix of ambition and irony.

Take DonutLeaks, for example—the ransomware group that somehow destroyed its own chat database and is now awkwardly asking victims to reconnect through a contact form. Imagine a cyber heist movie where the mastermind forgets their own getaway plan. That's DonutLeaks: high-tech extortion with a touch of slapstick.

Threat actors clashing in a cage with bats, under SOCRadar's control and oversight. (Image created by DALL-E)

Meanwhile, Nam3L3ss is busy posting sensitive data on dark web forums, leaking millions of records while claiming to expose systemic flaws in cloud security. Their dramatic manifesto might belong in a dystopian anime… Once data starts circulating on the dark web, it never really disappears—it just becomes fuel for phishing attacks and fraud.

And then there's Qilin Ransomware, who mixed up their victims so badly that payroll data for dentists somehow ended up attributed to a highway department. It's like watching a villain in a crime drama press the wrong button and accidentally blow up their own hideout.

From espionage experts like Turla, who infiltrate rival hacker infrastructure, to honeypots like Jinn Ransomware Builder, which tricked over 100 would-be hackers into exposing themselves, this week's cyber stories are proof that the dark web isn't just dangerous—it's unpredictable, ironic, and occasionally, downright absurd.

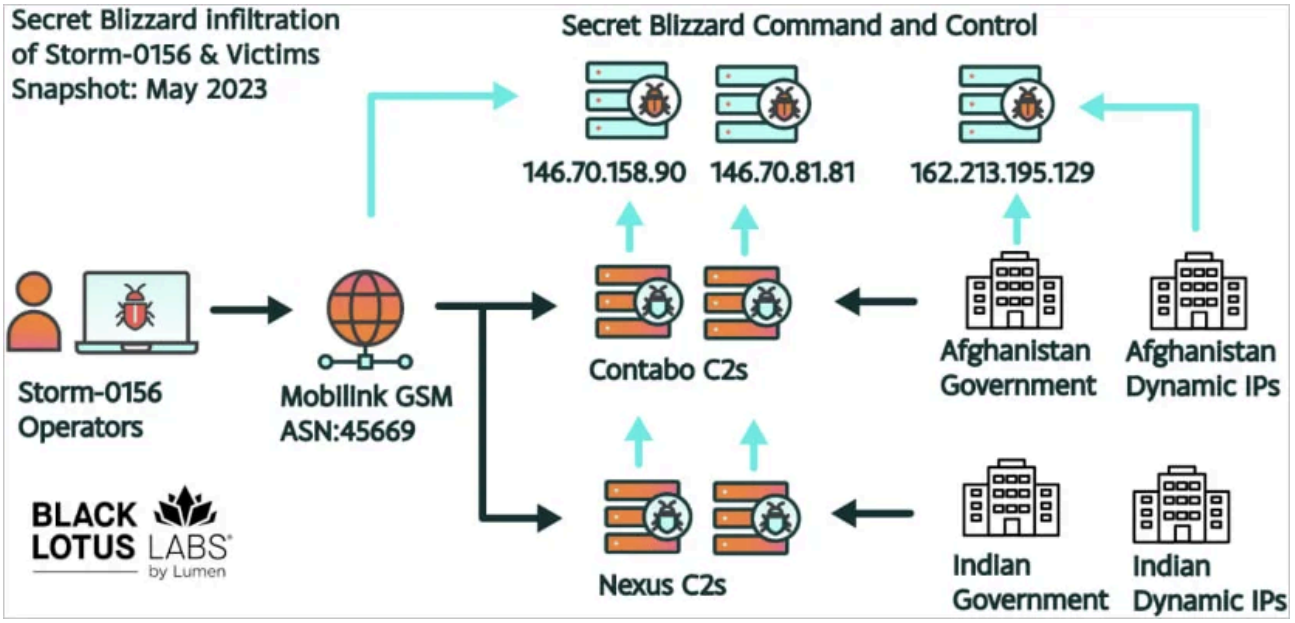
Bridges, Potholes, and… Root Canals?

Qilin Ransomware strikes again—this time proving that even cybercriminals can mess up their paperwork. They proudly posted their latest haul, only to mix up their victims. Unless the Whitestone, New York Highway Department has suddenly diversified into dental care, those payroll records for a dental director, two dentists, and five hygienists are just a bit out of place.

Moral of the story? When even ransomware gangs can't keep their stolen data straight, trusting them is like trusting your dentist to fix a pothole.

Turla Hijacks Hackers to Hide Its Tracks

The Russian cyber-espionage group Turla pulled off another stealthy move, hijacking **Storm-0156**'s infrastructure to hit Afghan and Indian government targets. Instead of breaching fresh systems, Turla piggybacked on networks Storm-0156 had already compromised, deploying their signature malware tools like TinyTurla and TwoDash.

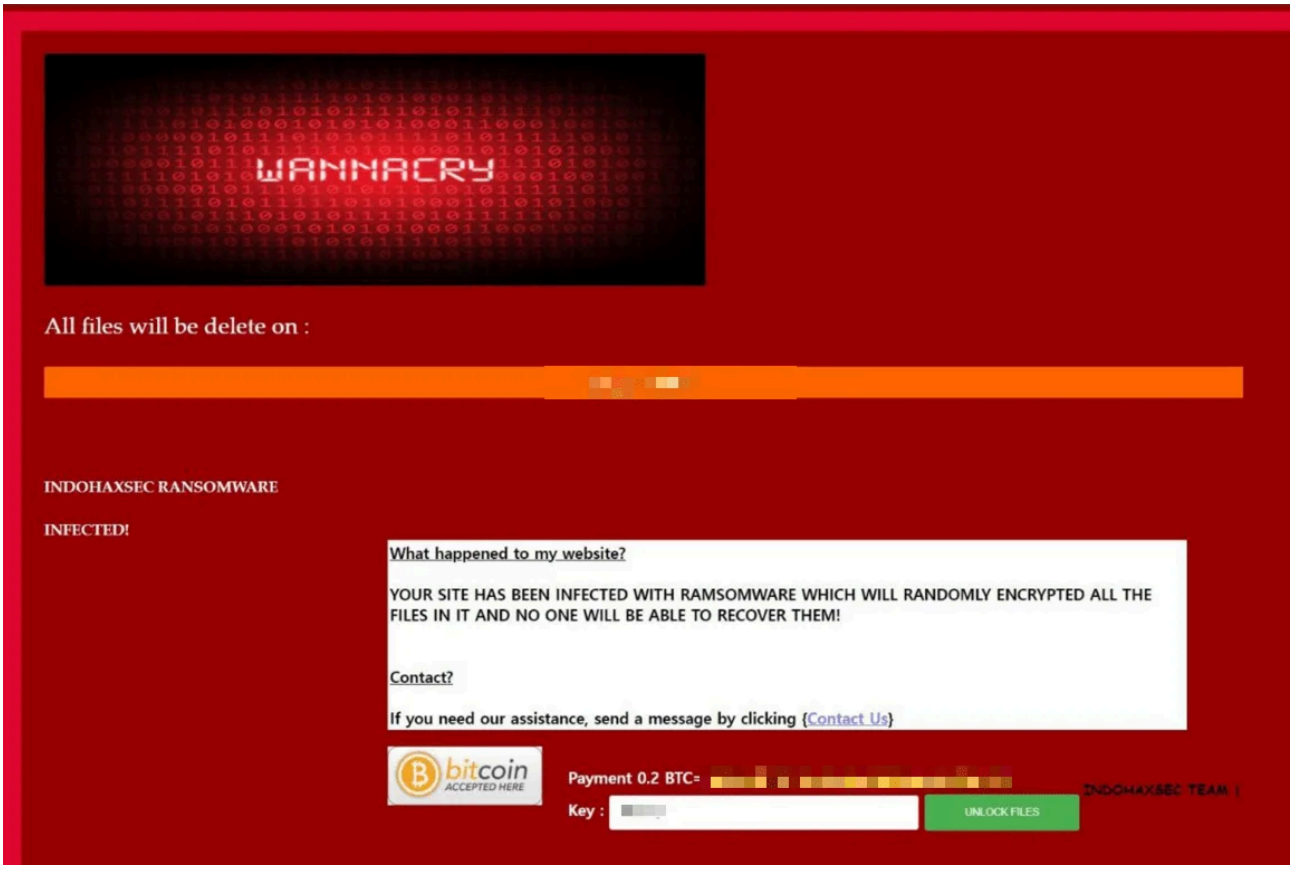


Turla's activities observed within Storm-0156's infrastructure (Source: Lumen)

Turla didn't stop at stealing access—they looted Storm-0156's workstations, swiping malware tools like **CrimsonRAT** and stolen credentials. Turns out, even hackers need better cybersecurity.

WannaCry Returns?

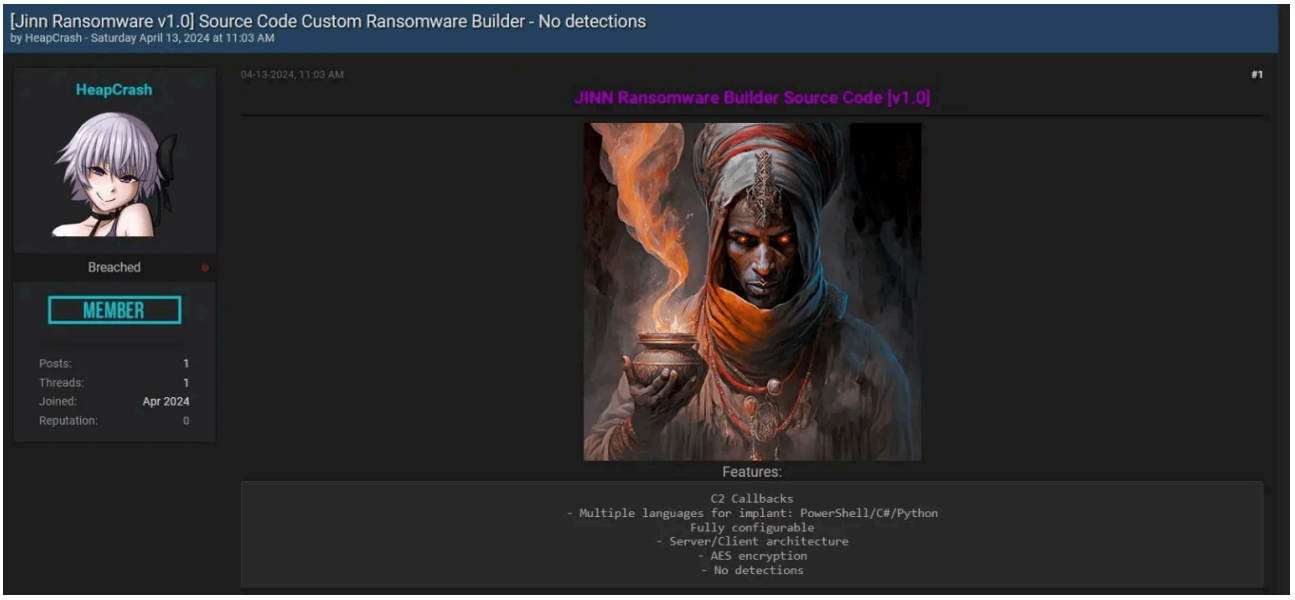
The Indonesian group **INDOHAXSEC TEAM** claims to have developed a web-based version of WannaCry, but whether they truly have the technical chops to pull it off remains uncertain. Creating ransomware of this scale requires significant expertise, and groups often exaggerate their capabilities for attention. While their claims of encrypting websites and demanding Bitcoin are bold, it's worth waiting for verified evidence before raising alarms.



A ransomware message on a red screen labeled "WannaCry," demanding 0.2 BTC to unlock encrypted files

Hackers Tried to Hack Ended Up Hacked

Jinn Ransomware Builder appeared on BreachedForums as a customizable ransomware creation tool, promising C2 callbacks, AES encryption, and multi-language support. In reality, it was a honeypot crafted by security researcher Cristian Cornea to trap curious hackers and script kiddies. Over 100 victims fell for the bait.



Jinn Ransomware builder honeypot

The builder disguised its true purpose by backdooring the system. A hardcoded “CmD.eXE” executable connected to a remote server while pretending to run encryption tasks. The multi-language feature? Just a prompt. AES encryption? Purely cosmetic, designed to hide the malicious code in plain sight.

The zero detections on VirusTotal gave it credibility, but that’s the catch—low detection doesn’t mean safe. Hackers running the payload unwittingly opened their systems to a reverse compromise.

Moral of the story? Hackers got hacked. Script kiddies got schooled. All thanks to a well-played honeypot—creativity meets irony in the best way.

When Hacktivists Turn on Each Other

In November, hacktivist group Rippersec pointed fingers at Azzasec for shutting down several Telegram accounts belonging to rival hacktivists. The twist? Azzasec’s *former owner* reportedly offers a Telegram takedown service for $300.

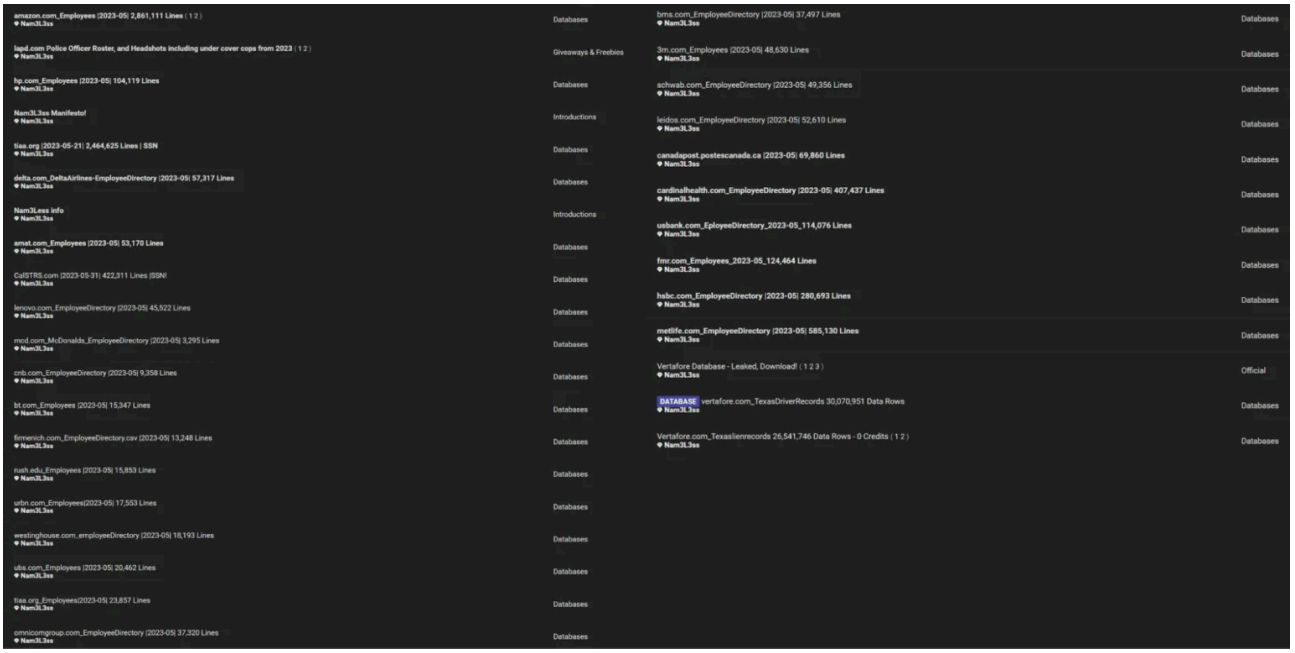
Claiming roots in Italy, Azzasec once worked alongside pro-Russian groups and even claimed to have a ransomware variant. Targeting Telegram accounts isn’t groundbreaking—mass reporting has been a favorite tactic—but turning it into a paid service adds a new layer of chaos to the hacktivist world. Turns out, if you can’t beat them, you can always buy their page’s demise.

RansomHub Says Data Will Be Used for Criminal Purposes

Well, of course it will. It's not like they're planning a charity fundraiser or a bake sale with your stolen data.

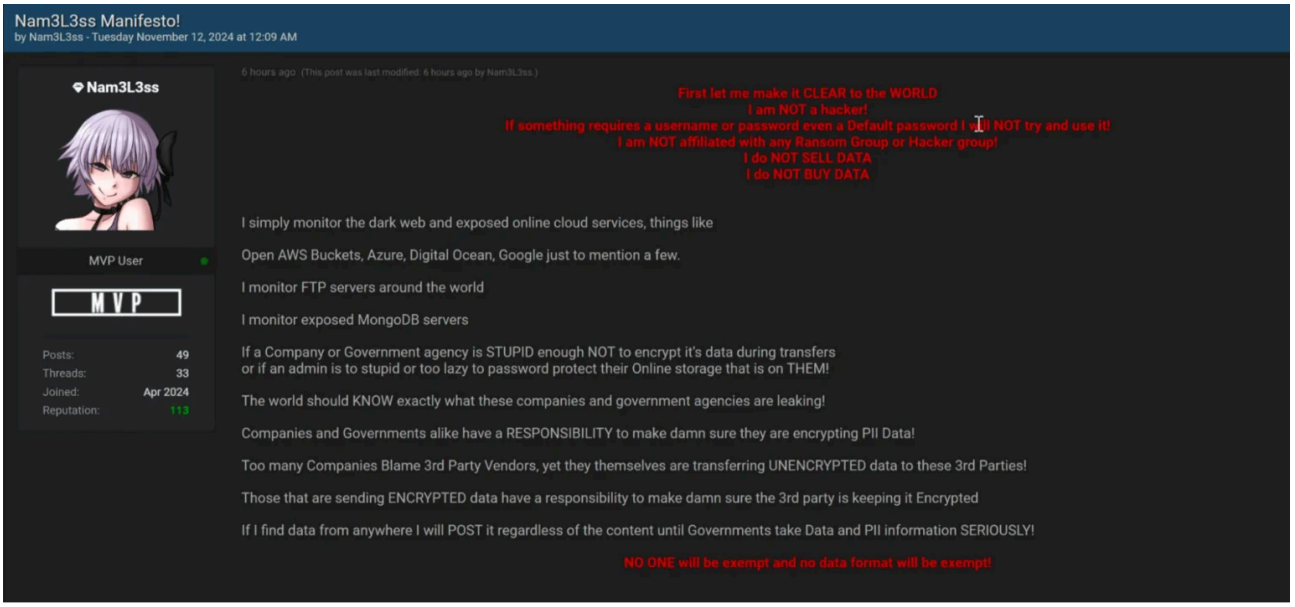
Once a Leak Begins, It Never Truly Ends

The infamous MOVEit vulnerability (CVE-2023-34362) has resurfaced, this time linked to a new threat actor named Nam3L3ss, who claims no affiliation with ransomware groups like Cl0p but continues to release sensitive data on BreachForums. High-profile victims, including Amazon, HSBC, McDonald's, and U.S. Bank, have had internal employee directories leaked, exposing names, contact details, and organizational hierarchies.



The threat actor's posts, allegedly featuring the latest MOVEit-related databases

Nam3L3ss, calling themselves a "watcher" rather than a hacker, insists their actions highlight systemic security negligence—specifically misconfigured cloud services and unprotected databases. Yet, their leaks, now millions of records deep, are a roadmap for phishing attacks, impersonation schemes, and fraud.



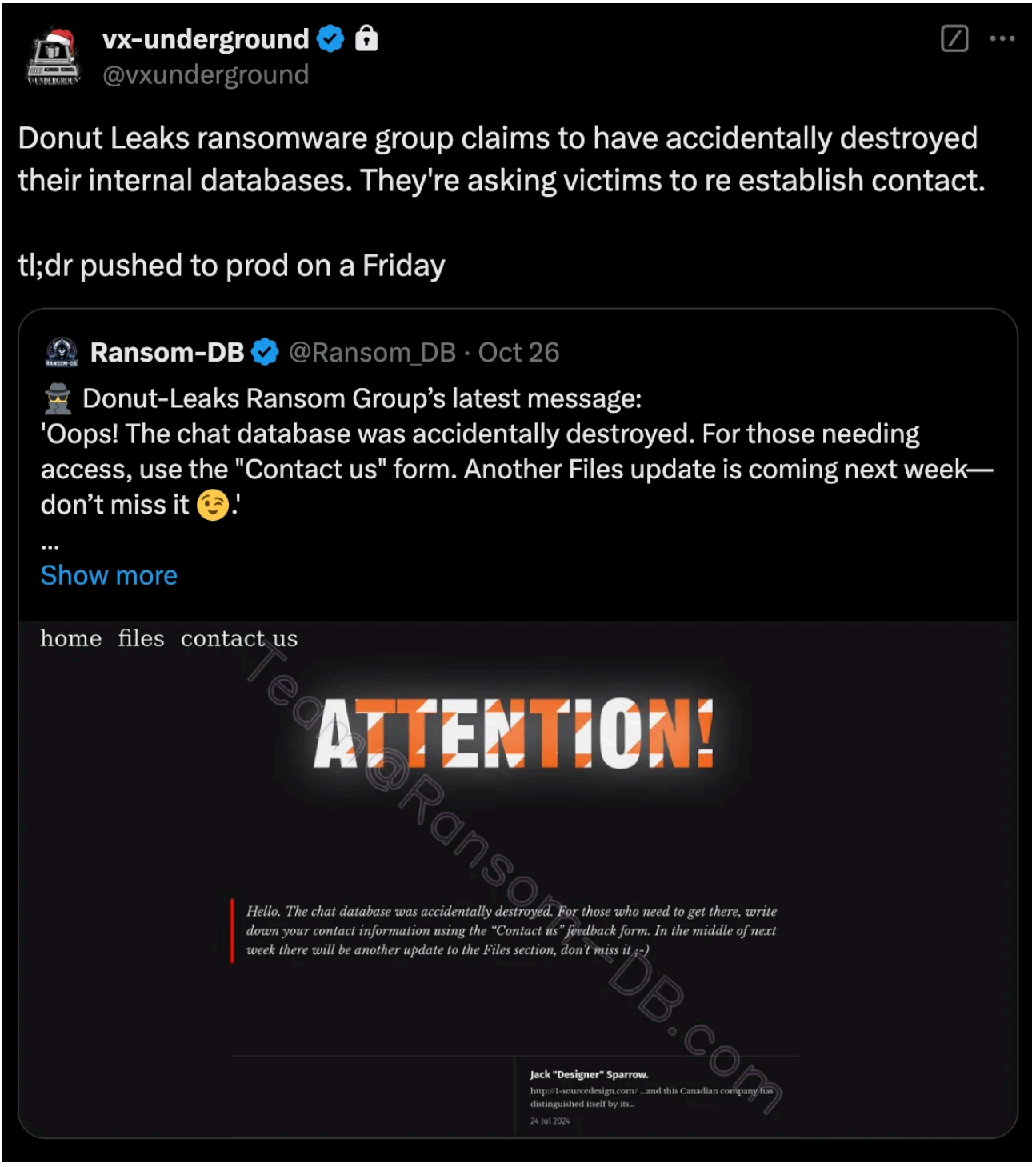
A manifesto posted by the threat actor alongside the MOVEit data leak posts

Their message may come wrapped in self-righteousness, but once the floodgates of stolen data open, there's no closing them. A breach, once begun, doesn't simply end. Data lives on, passed around like digital contraband, resurfacing years later in new forms of exploitation. Nam3L3ss allegedly reviving Avaddon's 2020 data linked to American Bank Systems is proof—breaches don't die; they just evolve, becoming new risks for old mistakes.

So, while Nam3L3ss claims to be the messenger, their chilling edge remains: *"If you can't protect it, I'll show the world just how broken it is."* The leaks may start with exposure, but the consequences ripple endlessly.

DonutLeaks: When Hackers Lose Their Own Data

The DonutLeaks ransomware group has found themselves in an ironic twist—they claim to have accidentally destroyed their internal chat database. Now, they're requesting victims to reconnect through a contact form, promising updates on leaked files soon.



DonutLeaks' statement (Source: X)

It's a rare moment when the hackers become victims of their own disorganization, proving that even cybercriminals can fumble their operations in unexpected ways.

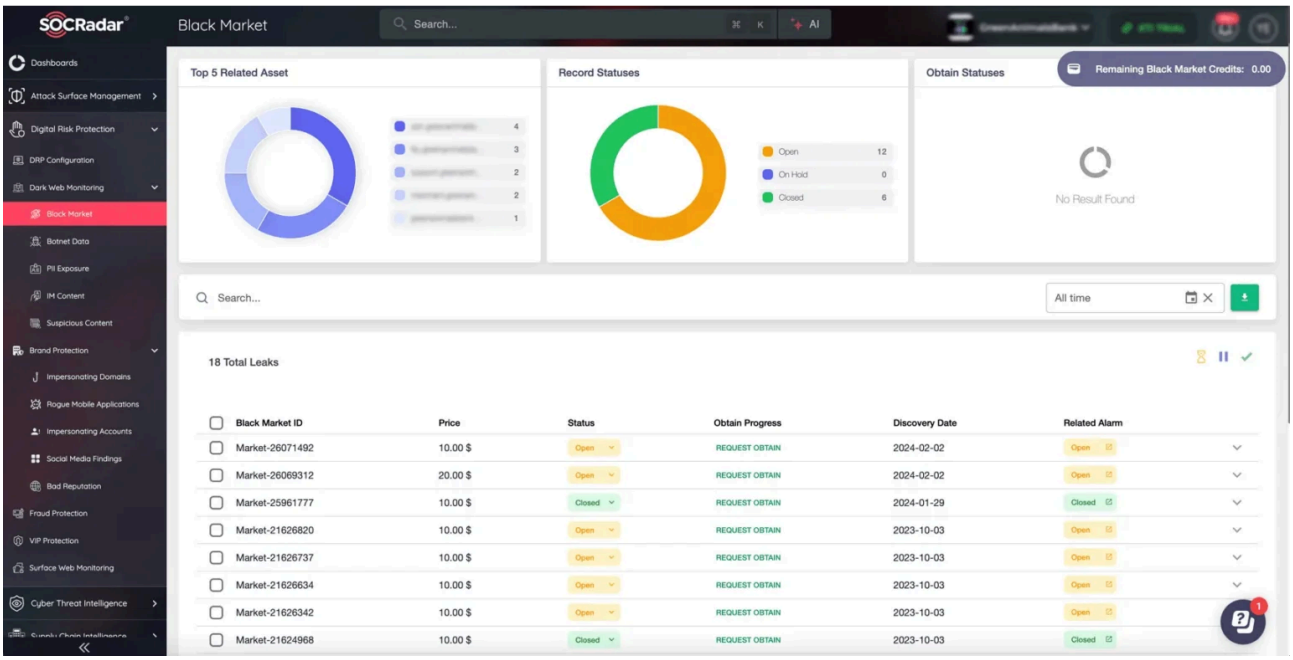
Laughs Aside, the Stakes Are Real

This edition of Dark Peep proves once again that the dark web and hacker forums are a hotbed of not only danger but also irony and missteps. From ransomware gangs losing their own chat databases to self-styled watchers exposing millions of sensitive records, the cyber underworld is as unpredictable as ever.

While some stories may seem comedic, the reality is far from it. Sensitive employee directories, internal databases, and even healthcare records leaking onto the dark web carry serious implications, from targeted phishing campaigns to large-scale fraud. Organizations must recognize the risks these leaks pose to their operations, reputation, and stakeholders.

This is where SOCRadar comes in. With advanced Dark Web Monitoring capabilities, SOCRadar empowers organizations to stay one step ahead of emerging threats by:

- Providing real-time alerts when their assets are mentioned on the dark web.



Keep track of black market leaks, botnet activity, PII breaches, and more using SOCRadar's Dark Web Monitoring

- Identifying and tracking compromised credentials, helping mitigate risks before further breaches occur.
- Offering tools like Integrated Takedown to neutralize fake domains and phishing campaigns targeting their brand.

In today's landscape, where every leak could ripple into long-term consequences, SOCRadar's solutions provide the edge organizations need to protect their assets and reputation. The dark web may be chaotic, but with the right tools, you can navigate it confidently.

Source: https://socradar.io/dark-peep-17-dark-web-hacker-forums-ransomware/