FUJITSU

# Going the extra mile: Real-world OSINT discoveries

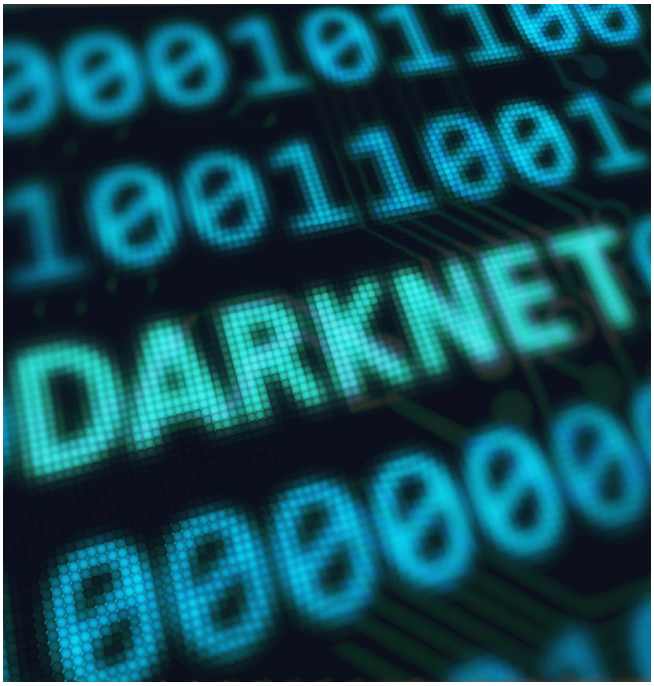
Darknet Monitoring Q&A

**In this anonymised Q&A, we speak with a senior penetration tester about how proactive OSINT investigations led to the discovery of multiple serious cyber security threats. These real-world cases highlight the importance of continuous monitoring, darknet surveillance, and having a trusted partner who goes beyond expectations.**

## What sets our security team apart from traditional providers?

We don't see ourselves as just a provider — we see ourselves as your security partner. That means we think like attackers, act like defenders, and always have your back. Our clients trust us because we proactively monitor, investigate, and even dig into the darkest corners of the web to identify threats before they reach your doorstep.

When new credential dumps, breaches, or darknet activity show up, we don't wait for a ticket to come in — we go looking. That mindset is what led us to a particularly troubling case just a few days ago.



Forgotten subdomain, live for 5+ years — and vulnerable to RCE. Entirely discoverable via OSINT.

Continuous external monitoring is vital — old assets don't vanish, they become easy targets.

"This wasn't about misconduct — this was someone being targeted"

# Can you walk us through what happened?

A few days ago, one of our senior penetration testers picked up on a fresh credential leak. As we were verifying the data, we noticed credentials tied to one of our monitored domains — a client we actively protect. While investigating that, another domain we track came up unexpectedly.

It turned out to be a forgotten subdomain, dormant for over five years — but still live. Worse, it was vulnerable to remote code execution (RCE). Anyone with the right payload could've taken control. That kind of exposure could be catastrophic — and it was entirely discoverable using OSINT techniques.

This is why continuous external monitoring is so vital — your forgotten assets don't disappear just because they're old. They become low-hanging fruit for attackers.

# The other discovery you mentioned — the one that hit closer to home?

That was deeply disturbing. While we were combing through a darknet source — an onion site known for hosting some of the most repugnant content — we found an email address tied to another client. But this wasn't just a credential dump. It included personal data linked to an older female staff member who had no prior leaks or digital footprint exposure.

We believe she may have been redirected unknowingly through a malicious ad or spoofed giveaway site — possibly something like a fake "You've won an iPhone" campaign — which silently harvested her details. Her data was then posted on an onion site adjacent to highly illegal material.

We had a tough but necessary conversation with the client and explained that this wasn't about misconduct — this was someone being targeted. The implications were horrifying, but catching it early allowed us to help contain the risk and support her.

"It's not just about risk scores - it's about real people, real assets, and real consequences"

# How do you respond when you find these types of threats?

Swiftly and quietly. The moment we validate a risk, we contact the client — discretely. Our objective is to inform, not to frighten. We provide technical proof, impact assessments, and help them take control before anyone else notices.

In both cases, our monitoring and OSINT capabilities meant we could prevent a potential breach and reputational nightmare. This is why we go the extra mile. It's not just about risk scores — it's about real people, real assets, and real consequences.

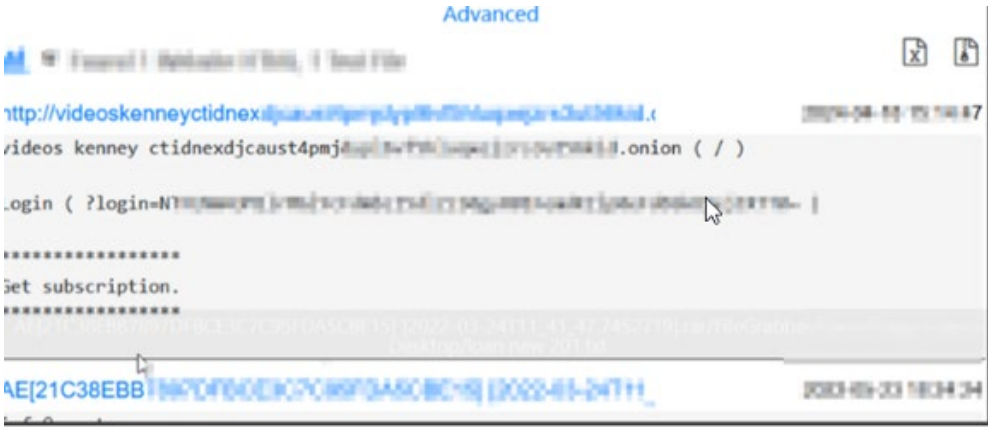
# What's your message to businesses reading this?

Don't wait to become a case study. The threats are out there, and they're evolving. **You need a partner who watches the internet like a hawk** — not just a compliance checkbox.

Monitor your public footprint. Audit your shadow IT. Track your domains — even the ones you forgot. Because your adversaries are already doing it.

## Example: Redacted Darknet leak screenshot

The image below shows a redacted example of a credential leak found on a darknet site. Domain names and email addresses have been anonymised to protect client identity.




# Contact us

**Please reach out to learn more about our Darknet Monitoring service**