Unknown Title

Thorsten Rosendahl ⋮ ⋮ 9/11/2025

Beaches and breaches

By Thorsten Rosendahl

Thursday, September 11, 2025 14:00
Threat Source newsletter

Welcome to this week's edition of the Threat Source newsletter.

I took a two-week vacation (thanks to Bill for covering my author shift last week) and made the deliberate choice to leave my laptop behind. No emails, IMs, no IT at all. Thank you, European work culture! It was a complete break.

Well, almost.

The weather didn't always cooperate, so instead of freezing on a beach, I found myself catching up on TV — mostly news and a few series. But wherever I clicked, I just couldn't escape the daily dose of AI. What can we do about invasive mosquitos? Ask AI. Government doesn't move the needle? Ask AI. Want the weather forecast? AI, obviously. There are countless ads with people asking AI whether or not to wear a jacket "because it might rain." Even with your favorite TV shows, gone are the days when the hoodied hacker sits in front of a black terminal with green text running a dangerous (haha) ping or nmap. Now, they're writing lines like, "Did you try breaking the firewall with our latest AI algorithm, bro?"

Coming back to work and catching up on our industry news, I almost expected AI to be dominating the headlines. But it wasn't, and neither was ransomware. Instead, they were all about breaches. Many — but not all — reports referenced compromised OAuth tokens linked to Salesloft's Drift integration, with a notable number of high-profile

victims. Sure, this isn't a scientific or qualitative analysis (ransomware isn't disappearing anytime soon), but the reporting and the headlines have definitely shifted from one to the other.

Looking past the buzzwords and catchphrases, the headlines really boiled down to two main themes: supply chain and identity attacks. In a SaaS world, I think it's time to rethink their definitions and priority levels.

Why? First, supply chain attacks aren't limited to hardware or software anymore. We need to consider the datapath (or where data possibly is processed) as a key part of the supply chain.

Second, identity attacks don't just target users; interconnected applications are increasingly at risk, too. I'm not saying we can ignore the users, especially with current reporting that it started with access through a GitHub account or software vulnerabilities in our "classic" applications, but we absolutely need to broaden our focus. Last week's headlines made that clear.

The one big thing

Cisco Talos' latest blog post details the Cyber Threat Intelligence Capability Maturity Model (CTI-CMM), a framework that helps organizations assess and enhance their cyber threat intelligence programs across 11 key domains. By outlining clear maturity levels and improvement cycles, CTI-CMM can help your team benchmark your current capabilities and develop a strategy for continuous (and practical) growth.

Why do I care?

Understanding and improving your CTI program's maturity can help your organization better anticipate, detect, and respond to cyber threats, no matter your budget or staffing level. It also makes the security investments you do have more effective, and ensure your team's efforts are aligned with business priorities.

So now what?

Check out the CTI-CMM framework to assess where your organization stands, identify gaps and opportunities, and create a roadmap to practical improvements for your organization.

Top security headlines of the week

Huge NPM supply chain attack goes out with whimper
A supply chain attack involving multiple NPM packages had the potential to be one of the most impactful security incidents in recent memory, but such fears seemingly have proved unrealized. (Dark Reading)

Swiss Re warns of rate deterioration in cyber insurance
Increased competition among insurers has led to a third consecutive year of reduced rates, according to the report, as the available supply of cyber coverage has exceeded current demand. (Cybersecurity Dive)

Critical SAP vulnerability actively exploited by hackers
A critical security flaw has been found in several SAP products, and could allow a malicious actor to gain administrator-level control. (HackRead)

No gains, just pains: 1.6M fitness phone call recordings exposed
Sensitive info from hundreds of thousands of gym customers and staff was left sitting in an unencrypted, non-password protected database. Audio recordings spanned from 2020 to 2025. (The Register)

US offers $10M reward for Ukrainian ransomware operator
Volodymyr Tymoshchuk allegedly hit hundreds of organizations with the LockerGoga, MegaCortex, and Nefilim

ransomware families. According to an indictment, the intrusions caused hundreds of millions of dollars in losses. (Security Week)

China accuses Dior's Shanghai branch of illegal data transfer
China's public security authority alleges that Dior's Shanghai branch has transferred customers' personal data to its headquarters in France illegally, leading to a data leak in May. (Reuters)

Can’t get enough Talos?

- **Beers with Talos: How to ruin an APT's day**
  The B-Team is joined by Sara McBroom from Talos’ nation-state threat intelligence and interdiction team. Sara shares her journey from a liberal arts major to tracking some of the world’s most advanced adversaries.
- **Who would sign up to secure a network full of hackers?**
  Our latest video takes you behind-the-scenes at the Black Hat Network Operations Center (NOC) to see how Cisco and SnortML contain the chaos.
- **Patch Tuesday for Sept 2025**
  In this month’s release, Microsoft observed none of the included vulnerabilities being exploited in the wild. However, there are eight vulnerabilities where exploitation may be likely.
- **Cisco: 10 years protecting Black Hat**
  Cisco works with other official providers to bring the hardware, software and engineers to build and secure the Black Hat USA network: Arista, Corelight, Lumen, and Palo Alto Networks.

Upcoming events where you can find Talos

- LABScon (Sept. 17 – 20) Scottsdale, AZ
- VB2025 (Sept. 24 – 26) Berlin, Germany
- Wild West Hackin' Fest (Oct. 8 – 10) Deadwood, SD

Most prevalent malware files from Talos telemetry over the past week

SHA 256: 41f14d86bcaf8e949160ee2731802523e0c76fea87adf00ee7fe9567c3cec610
MD5: 85bbddc502f7b10871621fd460243fbc
VirusTotal: https://www.virustotal.com/gui/file/41f14d86bcaf8e949160ee2731802523e0c76fea87adf00ee7fe9567c3cec610/d
Typical Filename: N/A
Claimed Product: Self-extracting archive
Detection Name: Win.Worm.Bitmin-9847045-0

SHA 256: 9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507
MD5: 2915b3f8b703eb744fc54c81f4a9c67f
VirusTotal: https://www.virustotal.com/gui/file/9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507
Typical Filename: VID001.exe
Claimed Product: N/A
Detection Name: Win.Worm.Coinminer::1201

SHA 256: c67b03c0a91eaefffd2f2c79b5c26a2648b8d3c19a22cadf35453455ff08ead0
MD5: 8c69830a50fb85d8a794fa46643493b2
VirusTotal: https://www.virustotal.com/gui/file/c67b03c0a91eaefffd2f2c79b5c26a2648b8d3c19a22cadf35453455ff08ead0
Typical Filename: AAct.exe
Claimed Product: N/A
Detection Name: PUA.Win.Dropper.Generic::1201