

It pays to be a forever student

 blog.talosintelligence.com/it-pays-to-be-a-forever-student

Joe Marshall

April 23, 2026



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

If I haven't said it in a newsletter before, I'll say it now: If you want to be good at cybersecurity, be a forever student. Cultivating and feeding your desire to know how things work is one of the key ingredients to being a hacker. It's not always about understanding the micro details, but the macro of how systems work. And not just computers or software or networking systems — those are ecosystems we're usually quite familiar with — but what about economics? agriculture? material sciences? human behavior? music and art? Do any of those carry any value into this profession?

They damn sure do. Many, many times I have had to branch my technical research into domains that arbitrarily seem to provide no immediate value for technical problems. Learning how maritime insurance fraud works was interesting to me — and a short time later, led to cyber insurance and understanding how risk guides security investment in massive companies. Understanding international agriculture helped me research threat actor targeting and ransomware cartel victimology.

One of the topics I've been researching heavily lately is economics, specifically industrial organization. It's a branch of economics that studies how companies structure production, how markets form around them, and how costs operate at scale. For me, the natural target of my curiosity was Ford Motor Company. Henry Ford didn't invent the car or the assembly line, but he was darn sure able to build and scale car production in a way that set the standard for all others in that space to emulate. I've learned about fixed vs. variable costs, how artisans had their knowledge crystalized within the assembly line process, and how and how amortized costs drove down prices, allowing the Ford Model T to exceed 900,000 units annually by the early 1920s. By that time, more than half of the registered automobiles in the world were Fords. Not half of American cars, *half of all cars on Earth*.

So what? Well, what took Ford Motor Company 17 years to achieve in cost and ceiling reductions, the AI industry has done in 2.5 years. The rapid and massive influx of investments, fierce competition, and available compute has shown what industrial organization means in a world where AI now almost permeates everything we see and touch. What does this mean for AI replacing jobs? Are we the artisans who move to the frontier of security? What does this mean for enabling threat actors who can move up a step to threatening others with tools developed using an AI corpus already trained on security? There are lots of questions, and to be honest, the future isn't clear here. One thing is for certain: We can look to the past to understand the future. Henry Ford said it best: "Progress happens when all the factors that make for it are ready, and then it is inevitable."

As much as we tend to be myopic as security professionals and focus on our tradecraft, we are all part of a series of interconnected systems that lets humanity function. Learning those systems — their quirks, their limitations, and their vulnerabilities — makes you a better hacker. Stay curious, friends.

The one big thing

Cisco Talos Incident Response (Talos IR) is sharing [Q1 2026 incident response trends](#). Phishing has officially reclaimed its crown as the top initial access vector. In a notable first, responders observed adversaries leveraging Softr, an AI-powered web development tool, to rapidly generate credential-harvesting pages. Meanwhile, actual ransomware deployments hit absolute zero this quarter thanks to swift mitigation by Talos IR, though pre-ransomware activity accounted for 18% of engagements this quarter.

Why do I care?

The barrier to entry for cybercriminals is plummeting, and they are increasingly using our own tools against us. The use of AI platforms to spin up phishing infrastructure means even unsophisticated actors can launch high-speed, code-free attacks. Furthermore, threat actors are

abusing legitimate developer tools like TruffleHog and native cloud APIs to quietly hunt for exposed secrets, making detection incredibly difficult for defenders already struggling with logging gaps.

So now what?

It's time to get back to basics and lock down your perimeter. Organizations must implement properly configured multi-factor authentication (MFA), specifically restricting self-service enrollment to stop attackers from registering new devices. Defenders also need to prioritize robust patch management and ensure centralized logging via a SIEM is in place so forensic evidence remains intact. Read the [full blog](#) for a deeper dive into this quarter's trends and adversary tactics.

Top security headlines of the week

Third U.S. security expert admits helping ransomware gang

According to the Justice Department, Martino abused his role as a ransomware negotiator for five companies by providing the BlackCat/Alphv cybercrime group with information useful in negotiating a ransom payment. ([SecurityWeek](#))

22 BRIDGE:BREAK flaws expose thousands of Lantronix and Silex serial-to-IP converters

Successful exploitation of the flaws could allow attackers to disrupt serial communications with field assets, conduct lateral movement, and tamper with sensor values or modify actuator behavior. ([The Hacker News](#))

How hackers “trojan-horsed” QEMU virtual machines to bypass security and drop ransomware

In recent incidents, attackers used QEMU, an open-source machine emulator and virtualizer, to run hidden environments where malicious activity remained largely invisible to endpoint defenses and left minimal evidence on the host system. ([TechRadar](#))

Mastodon says its flagship server was hit by a DDoS attack

The cyber attack targeting Mastodon comes days after Bluesky, another decentralized social network, resolved much of its days-long outages following a lengthy DDoS attack. ([TechCrunch](#))

Exploits turn Windows Defender into attacker tool

Threat actors are using three publicly available proof-of-concept exploits (two are unpatched) to attack Microsoft Defender and turn the security platform's primary cleanup and protection functions against organizations it is designed to protect. ([Dark Reading](#))

Can't get enough Talos?

[Bad Apples: Weaponizing native macOS primitives for movement and execution](#)

Talos documented several macOS living-off-the-land (LOTL) techniques, demonstrating that native pathways for movement and execution remain accessible to those who understand the underlying architecture.

[AI phishing, fake CAPTCHA, and real-world cyber threat trends](#)

The Talos team breaks down findings from Q1 2026 — including phishing returning as the top initial access vector, and how attackers are using AI tools to build credential harvesting campaigns in almost no time at all.

[UAT-4356's targeting of Cisco Firepower devices](#)

UAT-4356 exploited n-day vulnerabilities (CVE-2025-20333 and CVE-2025-20362) to gain unauthorized access to vulnerable devices, where the threat actor deployed their custom-built backdoor dubbed “FIRESTARTER.”

Upcoming events where you can find Talos

- [PIVOTcon](#) (May 6 – 8) Málaga, Spain
- [OffensiveCon](#) (May 15 – 16) Berlin, Germany
- [Cisco Live U.S.](#) (May 31 – June 4) Las Vegas, Nevada

Most prevalent malware files from Talos telemetry over the past week

SHA256: 9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507

MD5: 2915b3f8b703eb744fc54c81f4a9c67f

Talos Rep: https://talosintelligence.com/talos_file_reputation?s=9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507

Example Filename: VID001.exe

Detection Name: Win.Worm.Coinminer::1201

SHA256: 96fa6a7714670823c83099ea01d24d6d3ae8fef027f01a4ddac14f123b1c9974

MD5: aac3165ece2959f39ff98334618d10d9

Talos Rep: https://talosintelligence.com/talos_file_reputation?s=96fa6a7714670823c83099ea01d24d6d3ae8fef027f01a4ddac14f123b1c9974

Example Filename: d4aa3e7010220ad1b458fac17039c274_63_Exe.exe

Detection Name: W32.Injector:Gen.21ie.1201

SHA256: 90b1456cdbe6bc2779ea0b4736ed9a998a71ae37390331b6ba87e389a49d3d59

MD5: c2efb2dcacba6d3ccc175b6ce1b7ed0a

Talos Rep: https://talosintelligence.com/talos_file_reputation

[s=90b1456cdbe6bc2779ea0b4736ed9a998a71ae37390331b6ba87e389a49d3d59](#)

Example Filename: APQ9305.dll

Detection Name: Auto.90B145.282358.in02

SHA256: 5e6060df7e8114cb7b412260870efd1dc05979454bd907d8750c669ae6fcbcf

MD5: a2cf85d22a54e26794cbc7be16840bb1

Talos Rep: https://talosintelligence.com/talos_file_reputation?

[s=5e6060df7e8114cb7b412260870efd1dc05979454bd907d8750c669ae6fcbcf](#)

Example Filename: a2cf85d22a54e26794cbc7be16840bb1.exe

Detection Name: W32.5E6060DF7E-100.SBX.TG

SHA256: 3c1dbc3f56e91cc79f0014850e773a7f12bbfef06680f08f883b2bf12873eccc

MD5: d749e0f8f2cd4e14178a787571534121

Talos Rep: https://talosintelligence.com/talos_file_reputation?

[s=3c1dbc3f56e91cc79f0014850e773a7f12bbfef06680f08f883b2bf12873eccc](#)

Example Filename: KitchenCanvas_753447.exe

Detection Name: W32.3C1DBC3F56-90.SBX.TG