

Signal & Noise

🕒 INCIDENT SPOTLIGHT

Internal Tool Gets Body Double

7 00 milliseconds was all it took for a program to unpack a cryptominer, tell Windows to run it automatically from then on, and delete itself. 92 milliseconds later, a clean copy of the real software was sitting in its place. The applications had identical names.

An internal licensing tool the company built for itself. The user got the license they opened it for. The only difference was that one of the two programs installed a miner on the way.

Malware tends to come from a few predictable places - phishing attachments, malicious sites, bundled software, and infected USB drives. None of which were associated with what our vSOC encountered on this case. The user didn't even download the source, since the tampered file was introduced by an unmonitored NAS (network access storage) that automatically syncs to laptops.

The most sophisticated part of the attack was how it covered its tracks. The payload itself ... was nothing special. A [cryptominer](#) is about as ordinary as malware gets. Cryptocurrency is produced by computers grinding through enormous volumes of calculation, and a miner does that grinding on someone else's machine. Whoever planted it keeps the currency. The owner gets the power bill and a laptop that runs hot.

The delivery mechanism could've carried something far worse than that. Since a cryptominer just needs a laptop to be on. Automatically syncing files means the same NAS could've introduced ransomware or a keylogger. Malware that could halt all business operations. All hidden in plain sight with the same name, in the same location.

IN THIS ISSUE

Incident Spotlight	01
Meet the Analyst	02
Case Spotlight	02
Eye on the Threatscape	02

🕒 THIS WEEK IN CYBER HISTORY

SEP 27 · 2020 · NATIONWIDE

Six years ago this week, [ransomware hit Universal Health Services](#), one of the largest US hospital chains. Systems at over 400 locations started failing at once. UHS pulled its whole network offline and staff went back to pen and paper for everything from medication labels to filing.

🔍 CASE AT A GLANCE

Payload

Cryptominer, set to run automatically

How it arrived

Unmonitored NAS that syncs to laptops

Disguise

Tampered copy of an internal licensing tool

Cover

Clean original swapped back in 92ms later

User action

None, no download involved

⚠️ WHY THIS MATTERS

Typical delivery vectors such as phishing and USB drives are the most common by volume, but attackers can get pretty creative. A compromised NAS syncs automatically to every connected endpoint, and **a trusted source removes the first layer of scrutiny** for users and defenders alike.

The main takeaway here is that bad actors spend as much time **brainstorming ways to evade defenses** as they do developing malware.

MEET THE ANALYST

**Dylan Haase**

SOC ANALYST

Dylan spent his early career in military intelligence before earning a computer science degree from the Colorado School of Mines. He brings blue team expertise to RADICL as a SOC Analyst defending Defense Industrial Base contractors.

Drawn to the full picture of how attackers operate and how defenders catch them, he pursues red team skills on his own time, ranking in the top 1% on TryHackMe.

“

To defend the Defense Industrial Base, you have to think like the people trying to break in. So I practice both.

DYLAN HAASE, SOC ANALYST • RADICL

CASE SPOTLIGHT

BENIGN POSITIVE • LEGACY ARTIFACT

A ransom note was found in LevelDB on a SVN server. vSOC investigated the entire fleet and found no signs of ransomware or related artifacts. The note was leftover from an old attack. Spawning a cold Edge browser from a help click touched the database, which triggered a detection.

TRUE POSITIVE • NO COMPROMISE

Two users clicked on phishing links, one being the CEO. We reviewed both accounts and found no suspicious sign-ins, mailbox permission changes, forwarding rules, or MFA changes. No compromises were found.

BENIGN POSITIVE • AI DEVELOPMENT

A local LLM inference server started up bound to every network interface. The client had a recent insider-threat case, so we checked whether the two were linked. It was on a completely different endpoint and account. Not the best practice but completely benign.

EYE ON THE THREATSCAPE

FBI Warns ShinyHunters Cybercrime Group Following Member's Arrest

“To the remaining members of ShinyHunters: You’ve heard about the arrest of your colleague,” the FBI commented in a [recently released video](#). “Other groups believed anonymity or their friends would protect them and they were wrong. Arrests have a way of changing who is willing to talk, and seized infrastructure has a way of showing us who’s left.”

ShinyHunters is a data-theft and extortion crew that breaks in through social engineering and SaaS platforms, and one of the most active extortion groups right now.



Your dedicated vSOC & compliance partner. Military-grade managed cybersecurity for the Defense Industrial Base.

radicl.com