WEEKLY THREAT BRIEF

Signal & Noise

RADICL
radicl.com
vSOC PUBLICATION
ISSUE 18 · WEEK OF NOV 2, 2026

INCIDENT SPOTLIGHT

A Card Skimmer Hiding in Plain Sight

You've probably heard of card skimmers: the little devices crooks stick on gas pumps and ATMs to copy your card as you swipe. This one lived inside a real small business's online store, and it was built to do the same thing to anyone typing their payment details into the checkout page.

Our vSOC caught it when a client's computer reached out to a three-month-old domain on our threat-intel list. Our research team has since reported it to AWS.

It works like the well-known **Magecart** attacks: hack the store's website, not the shopper, and slip in code that copies whatever customers type, card numbers included.

We can't say who was behind this one, but the page looks and works the same, so nobody notices.

What made it hard to spot is where it hid: tacked onto the end of standard code the site needs to run, served fresh by the attacker's server on each visit. A clean check today proves nothing about tomorrow.

The user visited the store three times, and the attacker's server answered on the third. They never reached checkout, and we found no sign anything was taken. But a skimmer runs inside the browser, where most endpoint tools never look.

IN THIS ISSUE

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

THIS WEEK IN CYBER HISTORY

NOV 2 · 1988 · UNITED STATES

38 years ago this week, a Cornell grad student released the Morris Worm, one of the first worms to spread across the internet. A coding mistake made it reinfect the same machines over and over, and within a day it had crashed about 10% of the roughly 60,000 computers then online. He became the first person convicted under the Computer Fraud and Abuse Act.

CASE AT A GLANCE

What fired
Threat-intel match on a new domain

How it arrived
Hidden skimmer on a legitimate store

What it was
Web skimmer, Magecart-style technique

Likely goal
Card and checkout data theft

Response
Domain blocked, reported to AWS

WHY THIS MATTERS

There was nothing to avoid here. The user visited a real business's website, and the skimmer ran as part of that site: no download, no attachment, no warning. **A trusted website is only as safe as its server.**

It was caught on the network side, because someone was watching where traffic went. And if you take payments online yourself, **your customers are trusting your checkout page too.**

MEET THE ANALYST



Maya Douglas

SOC ANALYST II

Maya's security career began during her CS undergrad at CU Boulder and has spanned contracting at Microsoft and running cybersecurity for MSPs. Four years writing for Her Campus means she came into security already knowing how to tell a story.

A Girl Security alum, WiCyS member, and CTF designer, she believes the best defenders come from everywhere. RADICL's focus on the Defense Industrial Base fits her passion for the segment that gets overlooked and underprotected.

> **The companies that get hit hardest are the ones everyone assumes are too small to be a target.**
>
> MAYA DOUGLAS, SOC ANALYST II · RADICL

CASE SPOTLIGHT

BENIGN TRUE POSITIVE · AI AGENT

An AI agent searched a machine's saved credentials, decrypted one, and used it to pull job-cost data from the client's accounting system. It turned out to be an established workflow, seen on four hosts going back to September. Still, an agent hunting for stored passwords on its own is exactly what an attacker would do, and that agent now runs on 30 machines.

FALSE POSITIVE · LOST IN TRANSLATION

A lookup of a strange-looking foreign domain turned out to be a local IP address. Someone most likely typed 192.168.137.1, the Windows hotspot gateway, on an Arabic keyboard, so the digits came out in Arabic-Indic numerals. Windows read it as a website name instead of an address.

FALSE POSITIVE · LEGACY SOFTWARE

Thirteen minutes after we first saw a brand-new laptop, someone ran a 2000-era installer off the IT department's own software share. It tripped a detection rule because "pdf" was in the filename. Old, but legitimate, and now on our list of known misfires for that rule.

EYE ON THE THREATSCAPE

North Korea Pulled $6.3 Billion Out of Binance Through One Laptop

On October 29, attackers drained about $6.36 billion from Binance hot wallets across 10 blockchains, most of it in roughly 20 minutes. That's about four times the size of the Bybit hack, the previous record. Binance says the way in was an engineer's laptop, which gave the attacker a service container that could submit withdrawals. They didn't need to crack a single key.

The FBI has attributed it to TraderTraitor, the same North Korean unit behind Bybit. About $3 billion has been frozen, Binance says it will cover every loss, and withdrawals are back up. The lesson isn't really about crypto. A single employee endpoint with access to automated systems can be worth billions to the right attacker.

RADICL™

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

radicl.com