

Signal & Noise

🕒 INCIDENT SPOTLIGHT

Free App, Rented Connection

One of our clients' laptops spent a night working for strangers. Over six and a half hours it made nearly 11,000 outbound connections to thousands of different sites, and none of them came from the user.

The cause was a free watch-party app, the kind you install to stream a movie with friends. Alongside its real features, it shipped a "web indexing" component that rented out the computer's internet connection to proxy networks. Those networks sell that access to their own customers, who then browse, scrape, and sign in to sites from your IP address.

Nobody had tampered with the app. The code was signed by its developer and matched the official release. The developer's server decided which networks to switch on, and each one ran in its own hidden process.

Our vSOC was alerted when one of those hidden processes looked up a web service that a desktop app had no reason to use. Once we looked closer, the rest became clear: connections to email servers, "what is my IP" checks, fraud-screening services that run on login and checkout pages, and bulk crawling of retail and news sites.

The app did ask permission. Its consent screen named two companies "and partners." The code carried 13 networks. Declining appeared to block use of the free app.

We isolated the laptop, removed the app, confirmed the traffic had stopped, and put it back on the network within a few hours. We found no remote access to the laptop, no sign of data theft, and nothing else installed. But for that night, anything those customers did online traced back to our client's IP address.

IN THIS ISSUE

Incident Spotlight	01
Meet the Analyst	02
Ask an Analyst	02
Eye on the Threatscape	02

🕒 THIS WEEK IN CYBER HISTORY

OCT 21 · 2016 · UNITED STATES

Ten years ago this week, a botnet built from hijacked webcams and DVRs took down big parts of the internet. Mirai flooded Dyn, a major DNS provider, in three waves, knocking Twitter, Netflix, Reddit, and GitHub offline for hours. Most of the devices still had factory-default passwords.

🔍 CASE AT A GLANCE

What fired

Desktop app contacting a web service it had no reason to use

How it arrived

Free watch-party app installed by the user

What it was

Signed app bundling 13 proxy networks

The money

Renting out the laptop's internet connection

Response

Isolation, removal, verified clean

⚠️ WHY THIS MATTERS

Proxyware turns your IP address into **someone else's cover**. When a proxy customer hits a login page or a mail server, the traffic comes from your company's address, and that address is what ends up in the other site's logs and on blocklists.

The consent screen is the weak point. Free apps pay for themselves somehow, and "allow partners to use your connection" is easy to click past. **On company devices, installing consumer apps shouldn't be left to each user.**

MEET THE ANALYST

**Brendan DeWyse**

SOC ANALYST I

Brendan got his start at FirstBank, interning on the IT and security teams and later running badge access and camera systems. Alongside that, he spent nearly two years triaging client alerts on a SOC team at Centurion SECURED. He joined RADICL's vSOC in March to work alert triage and incident response.

He finished his Computer Science degree at MSU Denver while working, and he served as vice president of the school's club baseball team. Between patrolling buildings as a security guard and watching networks as an analyst, he's worked both sides of the door.

“

Physical or digital, most break-ins start with a door somebody assumed was locked.

BRENDAN DEWYSE, SOC ANALYST I • RADICL

ASK AN ANALYST

CYBERSECURITY AWARENESS MONTH

How would I know if my computer was being used by someone else?

"On Windows, open Task Manager (Ctrl+Shift+Esc); on a Mac, open Activity Monitor. Look for anything using your CPU or network while you're idle, or starting up with your computer that you don't remember installing, and report it instead of just closing it."

BRENDAN DEWYSE • SOC ANALYST I

EYE ON THE THREATSCAPE

Eight Broken Certificates Put the Internet's Trust System on High Alert

On October 20, researchers revealed that eight certificates belonging to eMudhra, an India-based certificate authority, had private keys so weak they could be guessed almost instantly. Anyone holding those keys could create a trusted certificate for any website, letting an attacker on the same network pose as a login page, a bank, or a VPN without triggering a warning. Most major browsers blocked all eight within hours, though Edge on Windows 10 was still trusting them at the time of reporting, and there's no sign yet that the keys have been misused.

Browsers were the easy fix. The long tail is everything else that keeps its own list of trusted certificates, like VPNs, Linux servers, IoT devices, and older software, so apply this week's OS and firmware updates and give extra scrutiny to any Windows 10 machines still in service.



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

radicl.com