FOUR18 INTELLIGENCE

Case Study

TradeCraft Cyber Analyst Training Report

Kentucky cyber interns stop China at the door

Background

By the second decade of the 21st century, the Appalachian region of eastern Kentucky, once a jobs juggernaut from underground coal deposits, had fallen to become among the most impoverished and technologically deficient regions in America. Looking to develop new employment options, the Eastern Kentucky Concentrated Employment Program (EKCEP, Inc.), SOAR (Saving Our Appalachian Region) and the region's Community Colleges awarded FOUR18 Intelligence funding from an Appalachian Regional Commission grant in late 2020 to train and upskill dislocated workers with no prior experience in cybersecurity into job-ready Tier 1 Security Operations Center (SOC) Analysts. FOUR18's core differentiator is its DEF3NSE™ real-world threat analysis learning platform where interns develop hands-on job skills by analyzing live threats using a toolkit of standard cyber analysis tools, custom-designed AI and real-time support from practitioner coaches. The realness of the experience closely matches the actual job of a SOC or other cybersecurity analyst.

The Scenario

Using real-time phishing threat detection software installed on the desktops of college staff members, interns monitored this feed in DEF3NSE™ for URL based threats. A second feed of live threats from a global source is curated on the fly and mixed-in with the desktop feed to orchestrate practice in analyzing modern day adversary tradecraft.

"I have already used many skills I learned in your program, especially within the def3nse network regarding analysis of suspicious links."

A Threat Is Found

On April 16th, 2021, less than a week after interns first began investigating live customer data, an unknown URL was seen entering a college administrative staff member's browser by the desktop phishing sensors and was sent to our analyst interns' DEF3NSE™ workspace. This URL, like many in the mix, had an executable payload, which interns are trained to investigate through industry-standard online tools and by detonation in a Virtual Machine-based (VM) analyst toolkit. Although the online tools showed no signs that the executable was malicious, the scoring model of DEF3NSE™ compelled the analyst to investigate further to minimize uncertainty that the executable payload could be trusted.

Following FOUR18's process for investigating real-world adversary tradecraft, the analyst probed the host URL through his VM. Immediately he discovered the link downloaded an internet browser that functioned nominally but seemed to be attempting to mimic a browser family from Microsoft. There were also unsettling signs that it wanted unusual privileges, and the download was observed to have a different file name on five successive visits. A deeper investigation was warranted.

Through a sequence of sandbox detonations and VM-based dynamic malware analyses, our intern discovered the browser siphoning user data and information from the user's web sessions. He also found it installing other files through surreptitious techniques. Further, by cross-referencing these files he identified known malware that he discovered in several other identical sites under different domains – all rated as malicious. This gave him what he needed to trace the malware to a Cypriot shell company impersonating a Florida LLC, and to attribute its true origin to a campaign from China first seen in 2020 that had since vanished.

The Impact

Because the threat was spotted and isolated before it infected the college's desktops, the college was spared exposure. Also, because our interns reported the URL to be malicious in the phishing detection system, a Seattle school was protected from exposure just days later, and other users were protected when the campaign was seen spreading in Google Drive.

Epilogue – Deja Vu

The program landed remote jobs for over 80% of this cohort allowing them to work from home in eastern Kentucky at wages more than 3 times the average household income for the region. Within months of graduation, the lead intern reported back that the campaign was spreading rapidly and persistently throughout his company's customers, but the first-hand knowledge he gained in FOUR18's training allowed them to proactively mitigate the impacts.