DomainTools

Case Study

DomainTools Iris Helps L3harris Technologies Investigate Advanced Persistent Threats and Cyber Espionage Attempts

L3Harris Technologies

Customer Profile

- Global aerospace and defense technology innovator with $18 billion in revenues.

Business Objective

- Brand monitoring, phishing detection and defending against APTs and Nation-State threats.

DomainTools Solution

- Iris Investigate Platform, Domain Risk Score API

Business Outcomes

- Ability to quickly pivot on domain information and increase the speed and quality of threat investigations.
- Support in defending against threats and attempts at stealing valuable information.

Business Challenge

"I know how to search your mind and find your secrets." These words from Dominic Cobb, a professional thief who enters his adversaries' dreams in the film Inception, could keep anyone up at night. But for security professionals tasked with protecting their organization, Cobb may bear resemblance to today's advanced threat actors: motivated and sophisticated in the art of extracting valuable information. While it's not (yet) possible to control the architecture of our dreams, the CSIRT team at L3Harris Technologies has found a way to efficiently and effectively triage threats and prevent future cyber attacks.

As one of the largest global defense companies, L3Harris provides mission-critical solutions to connect and protect the world, serving customers in more than 130 countries. Given the nature of the company's industry, L3Harris faces numerous facets of cybersecurity threats from advanced adversaries and nation states. The company's 24x7 computer security incident response team (CSIRT) analysts operate in a highly advanced security atmosphere that is continually growing more complex.

> **"Cyber espionage is one of the biggest threats our organization faces. Nation-State activity is on the rise for many industries, but is particularly aggressive in the defense industry. The more we understand about these highly sophisticated adversaries, the more effective our team is at reinforcing our protections against them. It also helps us draw possible connections between domains that we know are nefarious and new ones that show up in alerts."**
>
> **—Devin McLean**

Devin McLean, SOC Manager and IRT Engineer at L3Harris, says the cybersecurity threat landscape has become notably more challenging in recent years. He attributes this to a variety of converging factors, including an increase in the volume of security alerts his team receives each day and an increasing attack surface. The global cybersecurity resource shortage is another challenge, squeezing bandwidth and making it difficult for organizations to staff their teams with additional support.

The process of enriching indicators has also become more complicated. McLean points to a growing and varied matrix of data (e.g. DNS information, SSL data, surface evidence, etc.) that analysts must review to better understand their indicators. The ability to quickly investigate and pivot upon indicators is critical to effective incident response.

Approach

Using products from domaintools, including the Iris Investigate platform, the CSIRT team at L3Harris leverages domain intelligence to establish an extra layer of security around the company's infrastructure.

Focused on staying ahead of advanced persistent threats (APTs), the team utilizes insights provided by DomainTools to better understand the networks and infrastructure of state-sponsored actors and other parties looking to gain entry and/or spy on the organization. L3Harris initially implemented DomainTools to enable brand monitoring alerts, so the team would know when a threat actor was staging a phishing campaign or attempting to register a domain associated with the company name. With the complementary capabilities in Iris Investigate, the team has deepened its use of domain information to inform threat investigations. McLean and the team of analysts at L3Harris use Iris to pivot on these data points and expand their list of domains associated with suspicious IP addresses and domain registrant information. That information is cross-referenced against other domains across the environment. This approach has uncovered connections between the registrations of numerous domains, providing the team with robust intelligence to further investigate networks of adversaries and block those that were previously known. In Iris Investigate, Domain Risk Scores that predict the likelihood that a domain is malicious, even before it is weaponized, and SSL Profile data panels that allow the analysts to examine certificates in detail, are key features for the L3Harris team. Using these tools, they can close the window of vulnerability between when a malicious domain is registered and when it is observed causing harm. They also help the team better understand the profile and screenshots of a website without navigating to it, and in some cases, uncover additional pivot points not otherwise available.

> **"Our team averages a 96 percent month-over-month increase in security alerts, and every day we process indicators from intelligence reports and more than 1,000 emails reported as suspicious by our users. Many of these include some level of domain information. The ability to automatically process those indicators and suspicious IP addresses quickly instead of manually significantly decreases the amount of time it takes to conduct the investigation, which is a major boost to our work."**
>
> **— McLean**

The Results

The CIRT work at L3Harris is critical in ensuring a strong, 360-degree defense against state-sponsored actors and APT groups. The domain insights and pivoting capabilities provided in Iris Investigate support McLean and his colleagues in successfully combating an increasingly challenging range of threats, maximizing the effectiveness of the available resources of security organizations.

DomainTools is also helping L3Harris improve the quality of its investigations by giving the team a way to automatically enrich indicators quickly and spend less time manually gathering information. This, combined with a highly intuitive user interface, allows analysts to accelerate incident response and focus on threat hunting. With rich data at their fingertips, they can act more quickly, make accurate decisions about alerts and rapidly escalate them when needed.

About DomainTools

DomainTools is the global leader for internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape. Learn more about how to connect the dots on malicious activity at domaintools.com or follow us on Twitter: @domaintools.