DomainTools

Case Study

DomainTools Helps Global Telecommunications Company Protect Brand and Thwart Phishing Attempts

Customer Profile

- Leading global telecommunications company with reach into all forms of electronic B2B and B2C voice and data services.

Business Objective

- Brand monitoring; proactive defense and response to phishing, credential harvesting, and other intrusions.

DomainTools Solution

- Iris Investigate Platform.
- SOAR and SIEM integrations, including the Splunk App.
- Brand, Name Server, and Registrant Monitors.

Business Outcomes

- Real-time monitoring of domain-based threats and historically enriched indicators of threat infrastructure.

Business Challenge

Given the company's high profile and multi-billion-dollar assets, along with the irreplicable value of their intellectual property, they face multifaceted cybersecurity challenges across multiple business lines from highly sophisticated threat actors and cybercriminals.

The company has consistently focused on protecting its brand online, as its customers and internal employees are the targets of threat actors creating a nearly daily barrage of spoof domains to activate phishing, credential harvesting, or other cybercriminal campaigns. These criminals have targeted public-facing properties as well as sensitive employee-only systems.

Because the company's security operations count on enrichment of indicators seen in DomainTools Monitors as well as those flagged by the company's Threat Intelligence Platform (TIP), the wide variety of data sets within Iris Investigate is of considerable value. This breadth is particularly important as data protection and privacy laws such as the EU General Data Protection Regulation (GDPR) have limited the visibility of some of the data traditionally used for identifying, assessing, and sharing information on potential threats and known attack infrastructure.

Approach

Focused on staying ahead of relentless cybercriminals, the security organization utilizes the DomainTools Iris Investigate Investigation Platform collaboratively across several primary teams, including the Operations Group, incident response, threat intelligence, threat hunting, and threat assessment teams.

A key member of this company's SecOps Engineering and Intelligence team said that DomainTools gives the teams consistently high-quality monitoring alerts to research suspicious domain registration activity and also provides his team with high-quality enrichments when it comes to assessing the risk of new adversary assets. "The day starts with reviewing the domains that DomainTools Monitors have surfaced since the previous day," this analyst said. "I have a process that I've gotten down to around 5 minutes per day for looking at new potentially dangerous domains [surfaced by the monitors]," he continued.

DomainTools

DomainTools solutions are built on an unmatched nearly two decades of data, which include Whois records, passive DNS data, related screenshots, IP addresses, hosting data, name servers, and other DNS data. This historical archive is a major asset for the company's various threat intelligence and SecOps teams, allowing them to block and coordinate takedown activities against adversary domains. The company's security posture is supported by workflows in DomainTools Iris Investigate and in the DomainTools Splunk App, which make connections and facilitate pivots to expose the infrastructure a given actor influences, controls, or is actively using.

The customer has come to depend on DomainTools to protect its brand, employees, and customers by leveraging its unique visibility into over 315 million current domains. This scope of coverage powers keyword monitoring alerts that signal when a threat actor is in the beginning stages of registering domains—for a phishing campaign or other malicious activity—often, even before the domains are provisioned in DNS. A quick Iris Investigate search allows the team to investigate and build blocklists that expand beyond just the domain name. "We use Splunk to see if any internal users have visited a site being investigated, and if they are, we block that traffic at the proxy" via smooth coordination with the teams administering firewall rules, the analyst says. By seeing the larger infrastructure surrounding a domain name, they are also able to anticipate a threat actor's next move andpreemptively monitor or block domains that otherwise would have seemed unconnected.

"I love the Domain Profile that Iris Investigate generates; it lets me quickly assess the potential threat of a domain," said the Threat Intelligence analyst. "I find the Pivot Engine and passive DNS very useful for finding related domains that may also be malicious. All in all, Iris Investigate saves me a lot of time and streamlines my workflow."

The Results

Thanks to the intelligence provided by DomainTools, the firm initiates takedown proceedings against as many as 50 malicious domains per month just within the team on which this analyst works.

"Other teams are doing the same thing as well," he states. The customer relies on insights provided by DomainTools to stay ahead of emerging infrastructure being prepared by cybercriminals and other malicious actors looking to gain unauthorized network access or credentials.

From thwarting phishing campaigns to identifying and blocking domains seeking to gain unauthorized access to sensitive company information, the company has developed smooth and effective methods for protecting customers against fraud and fighting the ongoing battle against cybercrime. The intelligence analyst concludes, "At any given time, we have at least 1,000 potentially malicious domains we're tracking. Thanks to DomainTools, we have a proven methodology for protecting the company and our customers against malicious actors of various kinds."

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.