DomainTools

Case Study

How a Fortune 15 Technology Enterprise Proactively Detects Advanced Threats With DomainTools

Fortune 15 Enterprise

Customer Profile

- Fortune 15 technology provider of cloud, information security and data storage solutions.

Business Objective

- Identify malicious and copycat domains that might be used as a future attack vector against their infrastructure
- Block and blacklist suspicious domains before an attack campaign is initiated

DomainTools Solution

- Whois History
- Brand Monitoring
- Registrant Monitoring
- Nameserver Monitoring
- Domain Monitoring
- API Integration

Business Outcomes

- Accelerated identification and response to potential domain-based threats
- Proactive alerting of domains registered that might infringe on one of the company's 30,000 protected domains

"DomainTools provides us with insights that allow us to identify potential threats before they occur."

Global Manager
Critical Incident Response Center

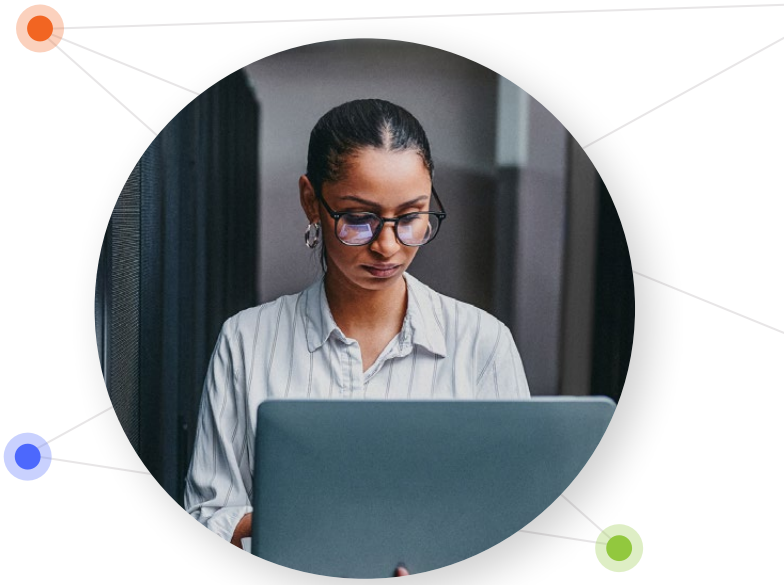
Business Challenge

In the sci-fi Philip K. Dick short story “Minority Report” the author imagines a not-so-distant future in which the police employ a trio of mutant humans known as “Precogs” to predict crimes before they happen. While we are likely a long way from this vision becoming a reality, forward-thinking security analysts are beginning to leverage new tools and technologies to better help them predict and proactively identify threats before a major data or application breach occurs.

One DomainTools customer, a Fortune 15 multinational technology company, is at the forefront of this approach. The Global Manager of their Critical Incident Response Center (CIRC) is a security leader who embraces the maxim ‘knowledge is power’. His team of security analysts collaborates with the company’s Incident Response team to defend a global enterprise infrastructure that spans several continents and tens of thousands of employees.

“The primary focus of our team is to research, identify, and quickly respond to a range of high-level threats that might compromise the integrity of our network,” noted the senior security analyst on his team. “These threats run the gamut from cyber-espionage, and intellectual property infringement to malware that’s propagated via doppelganger and typo domains. Given the high velocity and variety of threat types, we are always looking for ways to get ahead of the curve, prioritize threats and automate as much of the data collection process as possible so our Level 3 security team can spend a greater portion of their time doing what they do best – analyzing and remediating threats.”

As a widely known global enterprise that provides a broad range of security, cloud, and storage solutions to other enterprise businesses, this customer’s brand is synonymous with trust. With so much on the line, it is only natural that they would push the envelope when it comes to ensuring that their approach to security is at once holistic and proactive. “We’ve long recognized that understanding all dimensions of a domain is critical in both the investigative phase as well as the response phase. This is why we decided to upgrade our membership to their enterprise offering.”



Approach

"We've been using DomainTools Whois History as a standalone tool for more than three years now so we recognized its value as a forensic tool that helps us connect the dots in our cyber investigations," he said. "Before upgrading our DomainTools subscription, we cobbled together a few free utilities to investigate domain information but it was a very manual, ad hoc process. We recognized that we needed to automate this function as much as possible if we were going to achieve the situational awareness needed to effectively respond to a constantly evolving threat landscape."

With more than 15 years of complete Whois domain record data now at their disposal, his team of security analysts leverages the DomainTools API to ingest and store this wealth of historical domain information and integrate it with a variety of third- party security tools including SIEM, messaging, and DNS-based filtering products. With this critical piece in place, his security team can begin running high volume record analysis, enabling them to identify questionable domains and proactively block them if they meet a pre-defined scoring threshold.

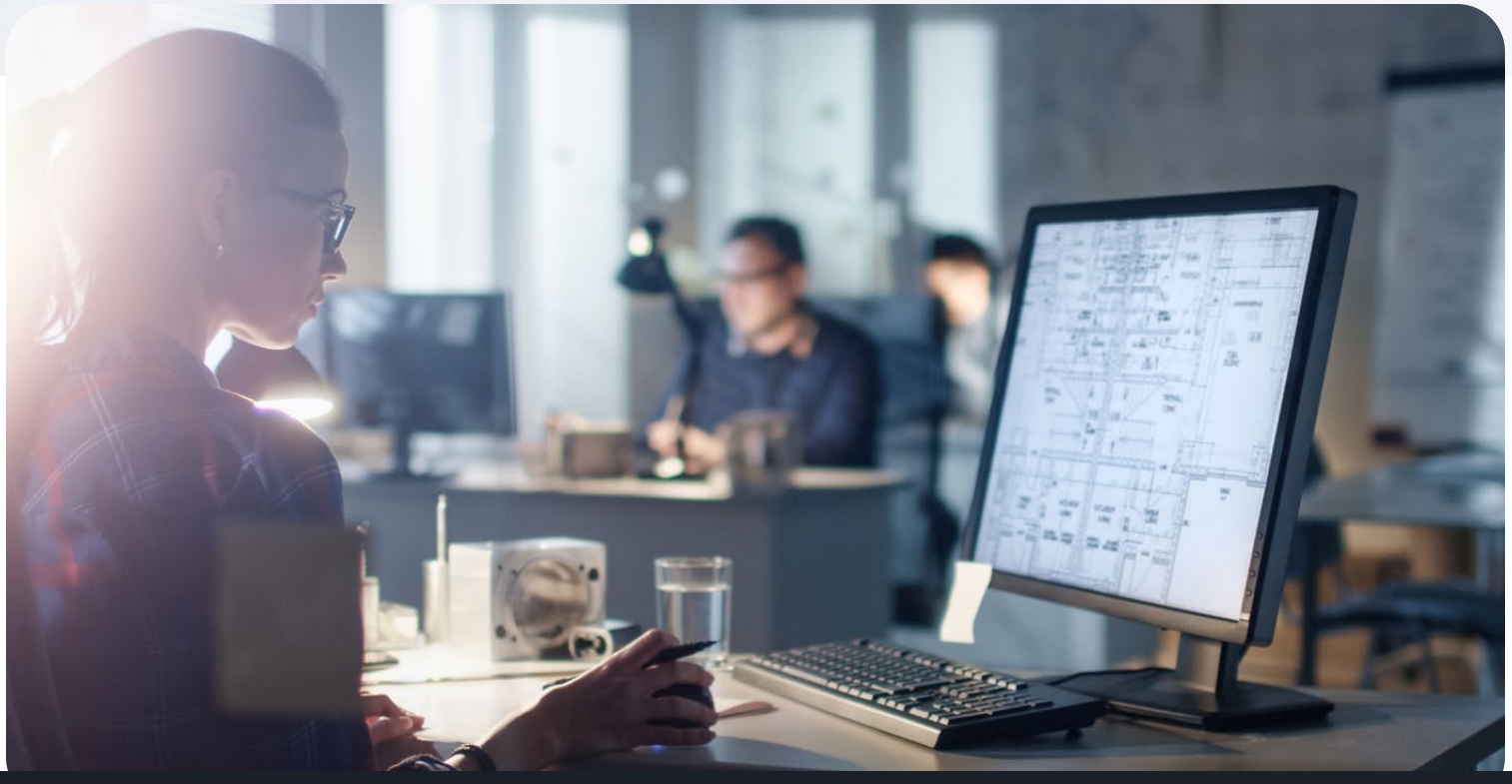
> With more than **30,000** registered domains stored locally on a MongoDB instance, his team's goal is to automatically perform Whois queries on the more than **50,000** domains that are pinged on a daily basis.

Results

Although this customer has only been subscribing to the complete DomainTools suite of solutions for a short time now, they've already seen tangible results. "While we're still only in the research and collection phase, DomainTools data is already crucial in helping our team streamline and systematize our threat investigation and remediation process."

One particular aspect of the DomainTools suite which has added immediate value for their security analysts is the Brand Monitoring solution, which automatically sends real-time alerts notifying administrators if a fake or typo domain is registered by a third party. Using this service, he says that they now proactively flag between 3-5 suspicious domains every day, enabling them to quickly blacklist potentially malicious domains before they can launch an attack.

And this is just the start of what promises to be a long and fruitful journey. As the team embraces the complete capabilities of the DomainTools Iris platform, he's confident that rich, historical domain data joined with advanced Big Data analytics will allow his team to better predict and respond to the next wave of emerging threats.



Features And Benefits

Domain Intelligence

With more than 15 years worth of comprehensive historical domain data on tap, security analysts can more effectively correlate domain information with other data to accelerate domain identification

Domain Monitoring

Automated monitoring provides daily alerts every time a related domain is registered

Robust APIs

DomainTools'APIs provide fast, high-volume access with a wide array of tools and can be integrated directly into a customer's security workflow

"Historic domain information is crucial to threat forensics and only DomainTools provides the rich and detailed domain information our team requires."

About Domaintools

DomainTools helps security analysts turn threat data into threat intelligence. We take indicators from your network, including domains and IPs, and connect them with nearly every active domain on the Internet. Those connections inform risk assessments, help profile attackers, guide online fraud investigations, and map cyber activity to attacker infrastructure. Fortune 1000 companies, global government agencies, and leading security solution vendors use the DomainTools platform as a critical ingredient in their threat investigation and mitigation work. Learn more about how to connect the dots on malicious activity at domaintools.com or follow us on Twitter: @domaintools.