DomainTools

Case Study

Major Metropolitan Government Agency Embraces Domain Intelligence to Pre-emptively Block Threats

GOVERNMENT AGENCY

Customer Profile

- Top 15 metropolitan government agency serving a population of 3.5 million people and 12,000 city employees across 36 departments

Business Objective

- Anticipate and block threats before they breach their network perimeter
- Improve their collective intelligence about historical domain data so they could optimize limited IT resources

DomainTools Solution

- Iris Investigation Platform

Business Outcomes

- Monitor inbound traffic and proactively block suspicious IP addresses and domains
- Accelerated forensic analysis of threats enables faster remediation of breaches and the early identification of potential bad actors

Business Challenge

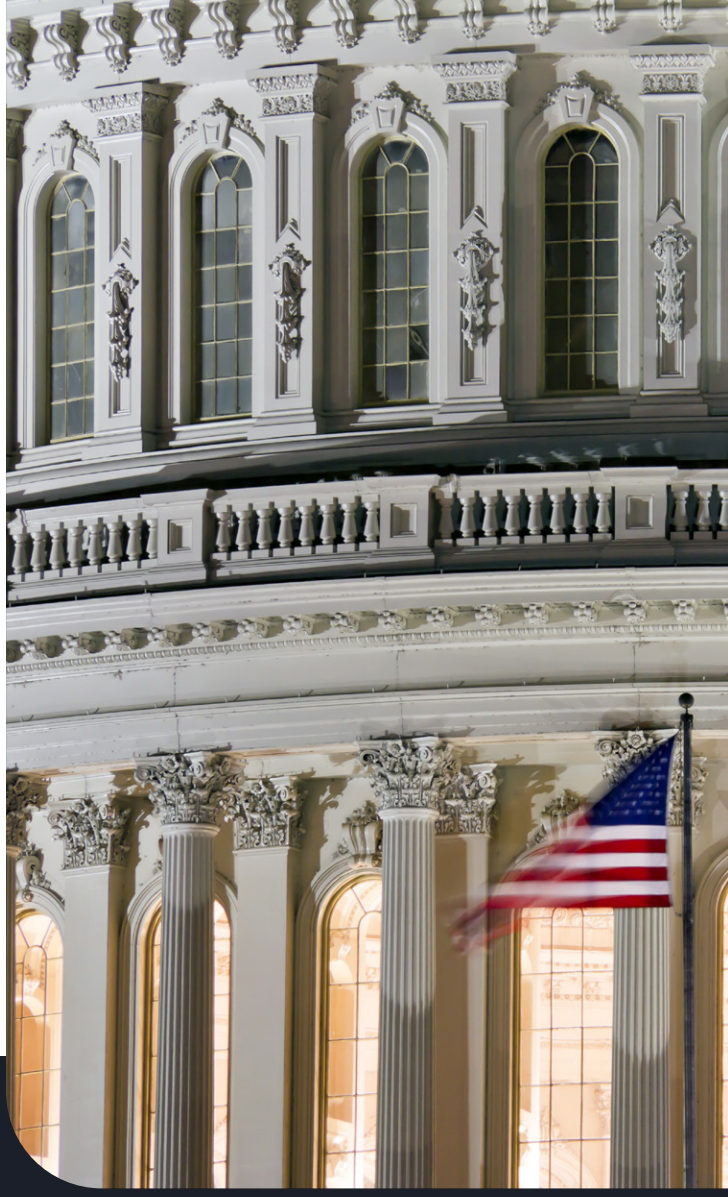
Detecting the next generation of advanced threats requires an almost Jedi-like clairvoyance. As Yoda might say, 'how do you see that which is not there?' Just ask the CISO at a top 15 major metropolitan city government agency. A 20-year information security veteran, this CISO is responsible for ensuring that a federation of 36 individual city agencies remains secure and productive. From utilities and wastewater to housing and criminal justice, his team of five security specialists must contend with an increasingly diverse threat landscape.

"Municipal websites have become a highly attractive target for criminal organizations and hackers as they recognize that many local government agencies are often under-staffed, under-funded, and sit on a mountain of sensitive customer data," said this CISO. "Our city has a reputation for being a technology vanguard and consequently, our residents have high expectations when it comes to how they use technology to interact with city sponsored services. Like so many government agencies, our challenge is to balance the needs and desires of our constituents with the proper security protocols."

> **"Iris Investigate provides us with an important new lens across the threat landscape, allowing our team to literally see things they couldn't see before."**
>
> **—CISO, Major City Agency**

With more than 12,000 city employees—and few restrictions in place in terms of how employees access the Web—the number of attack vectors across agencies is broad, and growing. Whether it's a city employee unwittingly opening an email with a malware payload attached, a spearphishing campaign targeting a high-level city executive, or a new breed of ransomware that encrypts data in exchange for payment, the CISO for this city agency understood the need to embrace new tools that would not only help automate their threat identification and incident response process, but also prioritize which threats might pose the greatest risk.

"It's not just the fact that the type of threats have increased over the past five years, it's the sheer velocity of threats that is overwhelming security teams. Given that we are only a team of five serving an organization of 12,000 individuals, we needed to identify new ways to distinguish the signal versus the noise," says one of the two Cyber Intelligence Analysts on his team. "One of the common threads that runs through all of the threats that we encounter is that they ultimately emanate from a domain. Thus, we recognized that if we are ever going to get ahead of the incident response problem, we needed to vastly improve our domain intelligence."



Customer Benefits

Accelerated Threat Response:

DomainTools Iris Investigate has dramatically accelerated their ability to respond and prioritize the most critical active threats

Improved Threat Intelligence:

By aggregating various aspects of domain profile data into a unified view, they've improved the way they assess and score risk factors

Enhanced Domain Correlation:

Iris Investigate enables them to not only correlate data from disparate sources but also drill down into the data to enable fine-grained analysis

Pre-emptive Blocking:

Using Iris Investigate, this agency can be more proactive in how they respond to a range of threats by pre-emptively blocking suspicious domains

Approach

The security team at this city agency had been using a variety of DomainTools solutions for several years prior to subscribing to the Iris Investigation Platform and thus was already familiar with its capabilities and the millions of detailed domain and registrar historical data points available in its database.

Not only was it critical that they understand who was generating suspicious domains but they also needed a way to improve correlation between threat actors, understand what other threat actors they might be aligned with, and where a threat was originating from.

By building an interactive, visual map of questionable domains with the ability to drill down into historical domain data, his team would be better positioned to anticipate where an attack might emanate and consequently be able to triage and respond to threats before they have a chance to breach the network perimeter.

“We use a variety of third party tools like Trellix for threat research and Websense for IP blocking. The DomainTools Iris Investigate platform is the perfect complement to these and the other tools we use to protect our network as it enables our security analysts to quickly drill down into the details, make connections that they might have otherwise missed, and take aggressive proactive measures like pre-emptively blocking known bad domains.”

Results

Although they have only been using Iris Investigate for a short time, this CISO and his team are already realizing significant value from their investment. “Iris provides us with an important new lens across the threat landscape, allowing our team to literally see things they couldn’t see before.”

As a city agency, they also regularly share information with their peers at the state and federal level and Iris Investigate has already helped them proactively collaborate with these other groups to ensure that known threats do not propagate to other government entities. The advanced visualization capabilities of Iris have served to help the security team achieve those ‘Aha’ moments during an investigation and have also proven valuable as a communications tool with other department heads who don’t want to wade through data heavy spreadsheets.

“The great hockey player Wayne Gretzky used to talk about skating to where the puck is going to be, not to where it is now. The same attitude could be applied to security practices in that to be effective, you need to always anticipate where the next attack might happen. DomainTools not only provides our team with better overall threat intelligence but it has also empowered our team to more accurately assess and score the risk represented by coordinated threat actors. As a result, our small team is even more agile and responsive to the many agencies and constituents that we serve on a daily basis.”

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.