CASE STUDY

DOMAINTOOLS

G2 Web Services Uses DomainTools to Help Thwart Payment Fraud and Prevent Illegal Transactions

G2 Web Services

Customer Profile

- Provider of merchant risk intelligence solutions for acquirers, commercial banks and their value chain partners.

Business Objective

- Identify connections between questionable websites and "front" merchants to catch and stop transaction laundering and payment fraud.

DomainTools Solution

- G2 Web Services relies on a variety of DomainTools products including Iris, Brand Monitor, Registrant Monitor, Whois, Reverse Whois, Reverse IP, IP History, and API Integration.

Business Outcomes

- Valuable component of G2's transaction laundering detection service, which provides tens of thousands of dollars of savings for G2 clients and accurately and quickly verify connections between transactional laundering 'pairs' helping the team to further investigate suspected fraud.

BUSINESS CHALLENGE

In the movie *Catch Me if You Can*, Frank Abagnale Jr's character masters the art of deceit by harnessing the trust society has in accredited financial institutions in order to commit fraud. Although checks are no longer a universally accepted method of payment, a common practice in the ecommerce world is for merchants to pose as a legitimate business while at the same time selling unlawful goods and services.

One DomainTools customer, G2 Web Services, is on the front lines of fighting payment fraud and transaction laundering for banks and merchants. A provider of merchant risk intelligence solutions for acquirers, commercial banks and their value chain partners, G2 supports close to 60 percent of global merchant outlets. At this scale, their team of analysts pore over threat intelligence data to uncover merchants selling illicit goods while posing as legal businesses. These criminals selling "mal content" can be difficult to detect, as they often utilize a variety of legitimate merchants to funnel transactions for the illegal ones. G2 must identify networks or make connections between transaction laundering 'pairs,' before they can dig deeper and verify whether fraud has occurred.

APPROACH

Using a variety of products from DomainTools, including the Iris Investigation Platform and the domain information it provides, G2 analysts work to build out the network of entities related to a suspect website and confirm connections where fraud may be taking place. When the company launched its transaction laundering detection program in 2015, it became evident early on that domain registrant information would be critical to making these connections. DomainTools stood out as the most accurate and comprehensive among the domain databases G2 evaluated, and early on was built into the workflows behind this service offering.

"In this type of work, the reliability of our data sources is paramount. If we can't trust the entire database, the process of drawing important connections between questionable merchants and fraudulent payment activity becomes very tenuous. DomainTools has a range of features that help us investigate the network of a website, and provides us with the information we need to take the next steps of confirming relationships between sites and verifying whether fraud has taken place." – Sarah Nortz, Senior Program Manager, Transaction Laundering Detection, G2 Web Services

© 2018 DomainTools, All Rights Reserved. | sales@domaintools.com | (206) 838-9020 | www.domaintools.com

DOMAINTOOLS

G2 analysts use data in Iris to map relationships between certain suspicious websites every day. One recent matter was particularly challenging because the websites had privacy protected registrant information, making it difficult to confirm transaction laundering, even after initial connections were found. Searching in Iris, the team found that two of the sites shared security infrastructure and one of these sites matched the merchant data that appeared for transactions from the suspected website. From this information, the team was able to make the associations they needed to prove a laundering relationship existed.

"G2 is also leveraging DomainTools' API integration in another of our service offerings. Our team can leverage information from DomainTools to run an instant check for connections between new merchants being on-boarded by our clients and any known bad actors." – Brandon Megrath, Product Manager, G2 Web Services

RESULTS

By identifying and stopping even one instance of this type of fraud, G2 is saving its clients upwards of $25,000. DomainTools supports this effort with domain information that helps validate the team's identification of connections and conviction that they have discovered a transactional laundering relationship.

"Our business has grown from one client in 2015 to more than 200 today. DomainTools has become a trusted partner, supporting us in that growth and improving our ability to make accurate connections to verify fraudulent activity and save our clients money. DomainTools has also provided valuable hands-on training and education on its products, to help our analysts constantly improve efficiency, which in turn further strengthens client service and helps us scale." – Nortz

Beyond providing the critical domain-based information G2 needs to thwart transaction laundering, DomainTools Iris has also helped make the work more enjoyable for the analysts. Working on these types of investigations day in and day out can become monotonous, and Iris provides an engaging way for the team to work with cutting edge technology, allowing them to work smarter and get more satisfaction out of their jobs.

"DomainTools has become our ally on multiple fronts. The team provides us guidance for new ways to use the technology, and is eager for our feedback on how the tools are working for us. Beyond that, they have been a great partner in helping us follow, respond to and manage the evolving state of Whois regulations, which can significantly impact the way we serve our clients. Not a lot of vendors will go the extra mile like DomainTools has." – Karina Sinclair, Chief Operating Officer, G2 Web Services

FEATURES AND BENEFITS

- **Iris Investigation Platform:** Proprietary threat intelligence and investigation platform that combines enterprise-grade domain intelligence and risk scoring with industry-leading passive DNS data
- **Domain Intelligence:** With more than 15 years-worth of comprehensive historical domain profile data on tap, security analysts can more effectively correlate domain information with other data to accelerate domain identification
- **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

"Not a lot of vendors will go the extra mile like DomainTools has."

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 www.domaintools.com or follow us on Twitter: @domaintools.

© 2018 DomainTools, All Rights Reserved.