CASE STUDY

DOMAINTOOLS

Cyber Forensics Firm Uses DomainTools to Crack Global Hacking Syndicate

HORIZON FORENSICS

Customer Profile

- Headquartered in Cape Town, South Africa, Horizon Forensics is a digital forensics consulting firm that specializes in helping corporations protect their valuable brand assets from online threats

Business Objective

- Identify the criminal syndicate responsible for a series of hacks targeting a major online casino provider causing estimated damages in excess of $500MM

DomainTools Solution

- Iris Investigation Platform helps gather evidence in their investigations and generate relevant leads for their investigators to pursue

Business Outcomes

- In the course of an ongoing investigation, Horizon has helped their online gaming client identify the individuals responsible for the hack and directly negotiate settlement terms

"DomainTools saves our investigators an enormous amount of time which means our clients save a significant amount of money."

Dean Oberholzer, Consultant, Horizon

BUSINESS CHALLENGE

'It has long been an axiom of mine that the little things are infinitely the most important.' These words were spoken by super-sleuth Sherlock Holmes and is a sentiment that Peter Allwright, co-founder of Horizon Forensics, adheres to as he and his team regularly sift through reams of data in order to identify and isolate the small yet critical pieces of digital evidence that enable them to unmask the perpetrators of international hacking crimes.

In early 2016, a major online casino operator contracted Horizon to assist them in the investigation of a data breach that threatened to undermine their business. The global online gaming market is massive with an estimated market size of more than $50 billion in 2016 alone. It goes without saying that when it comes to wagering real money in a virtual arena, trust along with hardened security, are table stakes.

"This client is a major player in the online gaming world and they came to us because they discovered that their network had been compromised and their customer database had been stolen," recalls Allwright. "While no customer payment information was lost, that was never the intention of the hackers."

In the world of online gaming, the cost of acquiring new customers is significantly higher than other businesses. Says Allwright, "We've seen some instances where an online casino would pay an affiliate a bounty of up to $50,000 Euros to get a high roller to switch from one online platform to another." Consequently, hackers realized they could make tens of millions of dollars by setting up a series of affiliate accounts and then using the stolen contact database of one online casino to identify and target the most profitable customers. The hacking syndicate would then use false contact information to populate their affiliate accounts but link them to active yet anonymous offshore bank accounts.

"While on the surface it might seem like a relatively harmless scam, our client estimates that on the conservative side, the potential loss could easily exceed $500 million dollars," said Dean Oberholzer, a forensic consultant who worked alongside Allwright on this case. With so much on the line, it was not enough to simply mitigate the attack vector – he also wanted to understand how the breach was conducted and unmask the individuals behind it.

DOMAINTOOLS

APPROACH

Horizon began by creating a series of fictitious 'seed' accounts on their client's gaming platform. Over the course of several months, these accounts would help Horizon determine a few important data points, including the frequency in which their client's customer database was being compromised as well as how the hackers were 'marketing' to these stolen accounts.

Says Allwright, "From the seeding exercise we were able to prove that the hackers were returning once every three months and just stealing the latest batch of new customers to supplement their affiliate scam."

Once the attack vector was isolated and remediated via two-factor authentication, the Horizon team focused their energies on uncovering the identity of the hackers.

"DomainTools has been especially crucial in helping us to unmask the cloak of anonymity of the hacking syndicate responsible for the attack," says Allwright. "They used hundreds of random domains as staging sites which allowed them to collect their affiliate fees. Of course, they also employed Whois Privacy to mask their identity which meant that we were limited to investigating IP addresses since all of the website MX records typically linked back to the Google subnet."

Armed with thousands of IP addresses, the investigators had a starting point. But finding a signal in a sea of noise would prove to be a daunting task. Fortunately, DomainTools Iris provided the team with an invaluable system of record that streamlined the domain research process and helped organize the results into a visual framework that ultimately accelerated their ability to both identify and locate the hackers.

RESULTS

Ultimately, the big break for the Horizon team came when they were conducting the historical research on the target list of IP addresses and discovered that the Moniker Whois privacy protection on one of the questionable domains had briefly lapsed. "With so many domain names to keep track of, it's easy to see how even a disciplined team of hackers might accidentally let the privacy controls slip on one or two domains over the course of several years," says Allwright. "What they probably didn't realize is that this one small mistake on their part would serve as a kind of cipher that we could use to decrypt and correlate other clues."

Within a couple of months of initiating their investigation, the Horizon investigators had not only identified the ringleader of the syndicate behind the attack but had also set up a meeting with him in Thailand where they disclosed evidence linking him to the attack and were able to negotiate settlement terms. Allwright concludes, "Iris was an absolutely critical resource in this particular investigation and we are confident that it will be at the center of many future projects. Domain Tools didn't just help us generate more frequent leads for our team, it enabled us to quickly pivot on the different data points so we could elevate the most relevant pieces of evidence and provide a much clearer overall picture."

CUSTOMER BENEFITS

- **Accelerate Time-Sensitive Investigations:** DomainTools Iris enabled Horizon investigators to accelerate the way leads were generated, tracked, and pursued.
- **Automated Domain Research Process:** Prior to using Iris, investigators had to manually research and track every domain relevant to an investigation. With Iris, the team could automate this function and spend more time analyzing the results.
- **Visual Map of Domain Registration:** The ability to take a screenshots of target domains over time and visually organize them provided a major breakthrough in the investigation
- **Historical Domain Information:** Horizon investigators could track domain ownership over the course of years to yield new insights

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.