DOMAINTOOLS

# DNS FORENSICS: WHERE INTUITION MEETS EXPERIENCE

BY BYRON ACOHIDO, THIRDCERTAINTY

Copyright DomainTools, 2017. All Rights Reserved.

## EXECUTIVE SUMMARY

It has become a business imperative to proactively defend against cyber threats. Any organization that transacts digitally with employees, clients and suppliers, while storing sensitive data, on premises or in the cloud, must inevitably come to grips with this truism of the digital age. Today most large enterprises make prodigious investments in complex, layered defenses; and most small and mid-sized businesses, when pressed, will acknowledge that attaining their growth objectives hinges on becoming more security-mature.

This is reflected in an immense global market[1] for cybersecurity products and services, one that is on track to top $202 billion in 2021, up from $122 billion in 2016, a compound annual growth rate of 10.6 percent. Demand from the financial services sector and U.S. federal government have been the major drivers behind this burgeoning market. But no industry sector is immune. Companies of all sizes, in all vertical markets, are compelled to do more each year to address rising cyber exposures.

An abundance of sophisticated hardware and software certainly is readily available to help secure business networks. Cybersecurity solutions run the gamut from the latest iterations of endpoint, firewall and SIEM systems to cutting-edge breach detection, data loss prevention and unified threat management technologies. A recent DomainTools survey of 552 security professionals affirmed that companies rely on myriad security systems to quell the daily onslaught of malicious attacks. Yet the respondents also reinforced numerous other threat report findings, such as those from Verizon[2] and Cisco[3], that malicious activity and successful network breaches, nonetheless, continue to occur at alarmingly high rates.

1 http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

2 http://www.prnewswire.com/news-releases/verizons-2016-data-breach-investigations-report-finds-cybercriminals-are-exploiting-human-nature-300258134.html

3 http://www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html



Copyright DomainTools, 2017. All Rights Reserved.

On the front line of this never-ending battle are the hands-on security analysts. These include the threat hunters that large enterprises in the security best practices vanguard house in well-equipped Security Operations Centers (SOCs) and give carte blanche to detect and deter network intruders. They also include security researchers, analysts and other IT staffers, hustling to make the most of modest security budgets at small- and mid-sized businesses (SMBs.) Whether the security analyst sits in a state-of-the-art SOC or toils as his or her IT department's designated security specialist, the core mission is the same: isolate and attempt, as much as possible, to fully understand suspicious artifacts hidden in the ocean of daily network events.

This paper outlines attack patterns security analysts are seeing and examines a fresh forensic approach some of them have begun using, one that is producing some notable success stories. It is an approach that is helping threat hunters in large enterprise SOCs, as well as security specialists in SMBs, to quickly and thoroughly bring a network intruder's footprints into high relief.

This new approach essentially brings both human and machine intelligence to bear on the common denominator to virtually every type of cyber attack found pervasively in the Internet wild today: manipulation of infrastructure identified in the Domain Name System (DNS.) Three case studies will be presented, including one singularly stunning example of a threat hunter unraveling a deeply invasive, meticulously hidden network breach.

## DNS YIN VS. YANG

When DNS was first standardized in 1984 as a means to generate a human readable label for an underlying IP address, the Internet was comprised of a collection of universities and research organizations that were either part of the federal government or working under a federal contract. The employees of these entities were generally polite and uniformly trustworthy. DNS was designed with those high-character people in mind.

Thus DNS was made trivially accessible. No one could have predicted that this characteristic would cause DNS to arise as a linchpin for allowing the Internet to rapidly become the foundation for digital commerce as it stands today. To this day it remains very easy for anyone to inexpensively buy a domain name, obtain an IP address and set up a host server. DNS, in short, enabled the rise of Internet commerce and the use of business networks as we know them today. This is most clearly demonstrated by the human behaviors we now take for granted, that were unimaginable at the start of this century — the ability to globally express ourselves, socialize, learn, collaborate, recreate, bank and shop online.



Copyright DomainTools, 2017. All Rights Reserved.

Clearly, in those instances in which DNS has been used as intended, in a trustworthy manner, productive things resulted. However, it has always been just as easy for the criminally-minded to use domains and IP addresses with malicious intent. That's something the designers of DNS did not account for. Nor did they include any function by which to cut off people who choose to leverage Internet infrastructure for malicious purposes.

Thus, DNS also arose as a key component of the most pervasive and persistent types of cyber threats companies must defend against. For instance, manipulation of a targeted company's name for malicious purposes is something cyber criminals now do routinely. By registering domains that slightly alter an organization's legitimate domain name, or by redirecting someone trying to navigate to that company's website to a rogue server, criminals can execute an array of scams, such as phishing, click fraud, brandjacking or typosquatting.

## PIECEMEAL NETWORK DEFENSE

It's clear that business networks continue to be inundated on a daily basis with such malicious activity enabled at a fundamental level by DNS manipulations. To get a sense of what this looks like in the real world, DomainTools conducted its Global Survey of Security Analysts[4], a poll of security professionals from organizations in the technology, government, finance, healthcare and retail sectors carried out in December 2016. The 552 survey respondents included:

- C-level executive, 43
- VP or SVP, 28
- IT manager,100
- Security researcher or analyst, 207
- Threat hunter, 21
- Other, 28

The respondents came from organizations of all sizes:

- 1- 99 employees, 29%
- 100-999 employees, 18%
- 1,000 - 9,999 employees, 23%
- 10,000 or more employees, 30%

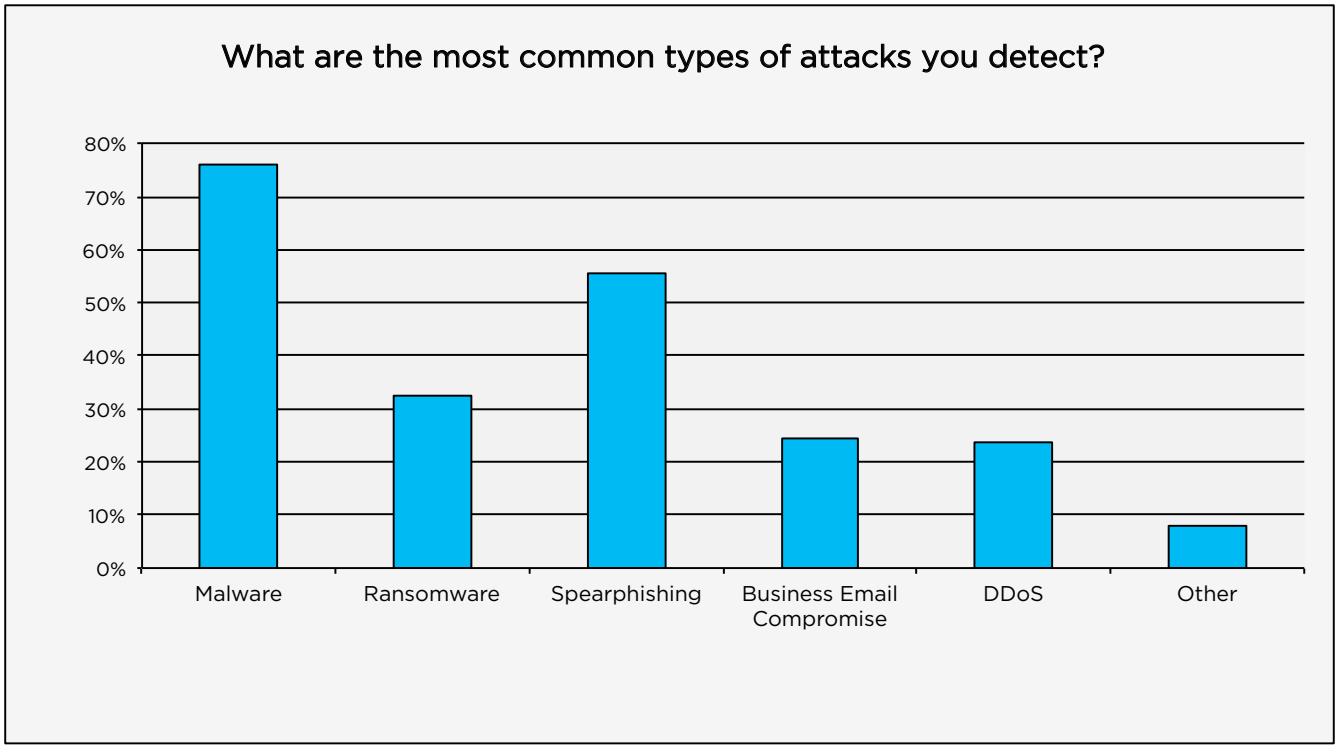
Their responses showed that there is no one-size-fits-all approach to achieving security maturity. The majority of respondents reported that their companies have adopted piecemeal systems to secure their networks. Use of a threat intelligence platform was reported by 42% of respondents; use of a next generation firewall (NGFW), intrusion prevention system (IPS,) or antivirus (AV,) by 63%; use of security information and event management (SIEM,) 52%; and use of use anti-phishing or other messaging security software, 57%.

4 http://www.domaintools.com/resources/white-papers/survey-report-2017-cybersecurity-report-card



Copyright DomainTools, 2017. All Rights Reserved.

Some 33% of respondents reported that they detect malicious activity several times a day, with 26% reporting that their companies sustained a network breach within the past 12 months; 23% said they did not know if a breach occurred. The most common types of malicious activity seen was malware, 76%; spearphishing, 56%; ransomware, 33%; Business Email Compromise (BEC,) 25%; and Distributed Denial of Service attacks (DDoS,) 24%. Of the breaches mitigated 11% were the result of a targeted attack; 22% spun off malware; 16% involved spear phishing; and 13% was ransomware.




Virtually all of this steady flow of malicious activity, aimed squarely at companies, leverages the central role DNS plays in facilitating Internet traffic. Cyber criminals have taken full advantage, finding ingenious, lucrative ways to exploit the intrinsic security soft spots. Take, for example, botnets. The infected computing nodes, or bots, that stand at the ready to respond to instructions from a controller have to get their commands from somewhere. So bots periodically beacon out to domains created expressly for the purpose of delivering next level attack commands. Or take the example of a spear phishing email sent to a specific employee as part of an attempt to infiltrate a targeted company. Such a campaign may rely on a series of spoofed domains as part of the social engineering component of the attack.

In either case – botnet deployment or phishing campaign – the attacker typically will stand up dozens, hundreds or even thousands of malicious domains to stay one step ahead of detection systems and blacklists. Ultimately, each one of these malicious domains will tie back a smaller subset of related IP addresses that the attacker has likewise gone through some pains to keep resilient and hidden.



Copyright DomainTools, 2017. All Rights Reserved.

## PURSUING 'DOMAIN INTELLIGENCE'

What if it were possible to correlate instances of certain parties registering new domains and IP addresses to the subsequent deployment of those assets in malicious activities? Depending on how far one could take such a correlation, clarity might start to emerge about how and where the threat originated; the scale and scope of the attack; whether the attacker might be aligned with other intruders; and, especially, how to recognize and better defend future attacks from the same threat actor or others closely connected to them.

This, in fact, is the essence of the fresh approach some security analysts are finding great success with. It can be summed up as pursuing domain intelligence. And it starts at a place where attackers invariably leave the most revealing clues: in Whois records containing information about the registered users or assignees of each domain name and IP address block.

The trend of security analysts taking a domain intel approach to investigations began with security analysts using Whois to look up and comb through records manually, one record at a tie. Use of the method accelerated with the release of DomainTools Iris in 2015. Iris is a browser-based platform that empowered users to delve deep into DomainTools' vast store of historical registration and hosting data to make pivots, correlations and deductions in intuitive ways that's impossible to do manually.

## IN PRACTICE

For example, a Fortune 15 technology provider has used Iris to identify malicious and copycat domains it suspects may be used in future attacks against its infrastructure. And a Top 15 metropolitan government agency, with 12,000 employees, is using Iris to anticipate and block threats before a network breach can occur. Both of these enterprises additionally have begun to ingest Whois historical records into their third-party security tools. The tech company has begun running high volume record analysis to pinpoint questionable domains with more speed and accuracy; and the metro agency is seeking ways to optimize its IT budget.



Copyright DomainTools, 2017. All Rights Reserved.

## HORIZON FORENSICS CASE STUDY: BREAKTHROUGH CORRELATIONS

Another recent marker of the potential for domain intelligence to dramatically improve security forensics, for companies of all sizes, comes from a small private investigations consultancy, Horizon Forensics, based in Cape Town, South Africa. In May 2016, a United Kingdom-based online casino retained Horizon Forensics to get to the bottom of a data breach and an ensuing cash-out scheme that had, to that point, caused the casino to lose tens of millions of dollars of betting revenue.

Investigators Peter Allwright and Dean Olberholzer began with these facts: someone had obtained the head of security's logon and used it to gain access to the casino's customer database to steal email addresses and betting records. Subsequent to that data theft, a casino marketing affiliate began sending emails to the UK casino's high rollers, enticing those bettors to switch their patronage to rival casinos.

Using the stolen email addresses, this affiliate offered the UK casino's customers cash incentives to make the switch, and then would earn up at a 30% cut of whatever the gambler subsequently bet on the rival site. Meanwhile, the UK casino lost all of that revenue.

Olberholzer began by examining registration information for the IP and email addresses the affiliate used to make the marketing pitches. Using Iris, Olberholzer was able to quickly correlate unique IP and email identifiers to recently registered domain names. He learned that the names, addresses and telephone numbers used for the IP and email addresses were all fictitious. Even so, this affiliate had no trouble setting up a sprawling matrix of hundreds of shell-company domains all tied to the same subset of IP and email addresses. Anticipating that someone like Oberholzer might come nosing around, the affiliate also took the added precaution of using the Moniker privacy service to anonymize registration details for each of the hundreds of domains under his control.

To overcome that roadblock, Olberholzer came up with the idea to use Iris to begin correlating the affiliate's email addresses to all domains ever registered, in reverse chronological order. "We discovered that in 2012, his Moniker subscription lagged and with that we were able to find the actual registrant of the domain name," says Olberholzer. "Although it had faked details, we were able to find a fresh email address that we could work with to identify new leads."

The Moniker breakthrough opened up fresh trails and Olberholzer teased out new branches of correlations. Not all bore fruit. But more key breakthroughs soon began to accumulate. Says Olberholzer: "Instead of spending hours manually around each domain name, we could just do it really, really quickly with Iris and our own software, based on unique identifier. We were able to quickly see which unique identifiers were truly unique. We kept generating new leads, and we never really had to stress about losing the bread crumb trail because, whenever we needed to, we could always go back to something we found earlier."



Copyright DomainTools, 2017. All Rights Reserved.

## COMPREHENSIVE RELATIONSHIP PROFILING

Olberholzer began to correlate information from other sources, such as Google AdSense, AdWords and Analytics, as well as Facebook and Skype. By taking a domain-centric approach to the investigation, he was ultimately able to insert the affiliate into a detailed relationship-flow chart. This stunning visual display highlighted many of the Horizon Forensics' breakthrough findings. These included:

1 Uncovering the affiliate's true identity and his location in Israel.

2 Outlining the affiliate's wider activities and business associates.

3 Showing how cash flowed from casinos to affiliates to bank accounts in Cyprus, Seychelles and Panama.

4 Identifying a kingpin and his second-in-command, based in Thailand.

5 Showing how several other casinos based outside of the UK had also been breached and victimized by switch schemes.

6 Projecting an aggregate revenue loss of $500 million sustained by the targeted casinos.

Peter Allwright, Director of Horizon Forensics, has 20 years of experience as a forensic investigator specializing in white-collar crime investigations. Allwright served as liaison to the casino operators during this investigation. Allwright received logistical support from the casino operators to set up in-person meetings, first with the affiliate in Israel, followed by a meeting with the kingpin in Thailand. He brought a copy of the comprehensive relationship-flow chart with him. Both the affiliate and the kingpin, he says, confirmed the accuracy of the chart.

The meetings produced one more important finding. The kingpin asserted that the switch scheme ring purchased the stolen customer emails in the cyber underground, and had nothing to do with the network breaches, nor the actual data theft from the casinos. Authorities have been alerted and other safeguards have been taken by the casinos. Meanwhile, the investigation into the network breach and data theft continues.



Copyright DomainTools, 2017. All Rights Reserved.

## CONCLUSION

Taking a DNS-centric approach to unraveling sophisticated attacks can bring stunning results quickly, as the Horizon Forensics investigation shows. This nascent methodology proactively blends the analyst's experience and intuition with the outputs of whatever security systems the organization happens to have up and running, as well as other public sources of information.

Iris is a tool that puts intuitive data mining techniques into the hands of security analysts, with a full archive of domain names, IP addresses, email, and web server data, and many other datapoints that may provide key correlating evidence. Early successes, like these three case studies, show the potential that threat actor profiling holds for companies to more thoroughly understand who is generating suspicious domains. This can lead to more clarity about which criminal groups have targeted their organizations in the past, and may target them in the future.

## ABOUT THE AUTHOR

Byron Acohido is one of the nation's most respected cybersecurity and privacy experts. Acohido first began paying close attention to cybersecurity and privacy in 2004. He conceived and delivered a nationally-recognized body of work for USA Today, chronicling the frenetic evolution of cybercrime in its formative stages. Acohido's deeply-reported cybersecurity stories and videos are the gold-standard for smart coverage of complex security and privacy topics distilled for an intelligent audience. He is currently the editor-in-chief at ThirdCertainty and can be found on Twitter: @ByronAcohido.



Copyright DomainTools, 2017. All Rights Reserved.

## ABOUT DOMAINTOOLS

DomainTools is the leader in domain name, DNS and Internet OSINT (Open Source Intelligence)-based cyber threat intelligence and cybercrime forensics products and data. With over 15 years of domain name, DNS and related 'cyber fingerprint' data across the Internet, DomainTools helps companies assess security threat risks, profile attackers, investigate online fraud and crimes, and map cyber activity in order to stop attacks.

Our goal is to stop security threats to your organization before they happen, using domain/DNS data, predictive analysis, and monitoring of trends on the Internet. We collect OSINT data from many sources, along with historical records, in a central database. We index and analyze the data based on various connection algorithms to deliver actionable intelligence, including domain scoring and forensic mapping.

DomainTools has over 10 billion related DNS data points to build a map of 'who's doing what' on the Internet. Government agencies, Fortune 500 companies and leading security firms use our data as a critical ingredient in their threat investigation and cybercrime forensics work.

For over 15 years, DomainTools has been the most popular Whois research service on the internet because we have the most comprehensive coverage of generic and country code Top Level Domains. We have also collected and stored Whois and related hosting/DNS data to provide the most complete historical records in the industry.


Copyright DomainTools, 2015. All Rights Reserved.