DOMAINTOOLS

DomainTools

Cybercrime Investigation

Connecting the Dots of Online DNA

DOMAINTOOLS SOLUTION BRIEF

WWW.DOMAINTOOLS.COM

INTRODUCTION

UNDERSTANDING THE DNA OF DNS DATA

As anyone who has watched modern crime television knows, DNA of some form is often left behind at the scene of a crime. Similarly, when a cybercrime is perpetrated it is not unusual that traces of evidence are left behind in the form of Domain Name System (DNS) and Whois data.

Cybercrime costs businesses billions of every year. A 2012 Ponemon study found that cyber crime cost businesses on average $8.9 million each year (based on a study of 56 organizations), with a range of $1.4 million to $46 million. And attacks are becoming more frequent—The same study found that attacks were up 42% from the previous year. Whether it's cybersquatting, the theft of valuable intellectual property, financial account hacking or the sale of counterfeit goods on a fraudulent domain, cybercriminals continue to grow more brazen and sophisticated in their tactics. To effectively combat this costly criminal behavior, cyber investigators must employ a range of new tools and techniques to quickly and proactively identify attackers.

RESPONSE AND INVESTIGATION

Whether you are attacked via a DDOS, phishing, malware or Advanced Persistent Threat tactics, one thing is consistent: in every case, there is a communication protocol applied. That is, all types of cyber attack involve sending information from one node on the Internet to another. DomainTools can help map these nodes and their connections, thereby providing investigators and response teams with the necessary information to stop further attacks and identify perpetrators.

More specifically:

1. **DDOS Attacks**
   A DDOS attack originates from one or more IP addresses somewhere on the globe. IP addresses have Whois records. Whois records contain identifying information such as name, email address, phone number, address and registrar:

2. **Phishing**
   A phishing email is sent from an email address that has a domain name at its root. And the links embedded in the email will go to websites that reside on domain names that are pointed to name servers and IP addresses. Domain names and name servers also have Whois records.

3. **Malware**
   Malware is delivered on domain names that are pointed to name servers and IP addresses, and often attempt to communicate back to command and control servers located on the Internet.

4 **Counterfeit eCommerce**

Counterfeit E-commerce happens on typo domain names. Fraudulent ads are bought on search engines and users are sent to fake sites selling knock-off goods. These cybersquatted domains have Whois records, registrars, IP addresses and name servers. Money has to be collected through a legitimate ecommerce site, which represents a solid connection to the criminals. While criminals are good at switching these up, over time they tend to use repeat services.

When it comes time to start an investigation, it is useful to think of the domain name as the unique identifier, because all domain names are unique by definition. By combining Whois data and DNS data, we can associate the following fields with a given domain name:

- Registrant name (Individual or Organization)
- Registrant email (sometimes more than one)
- Registrant phone number
- Registrant address
- Name server
- IP address
- Registrar

This is where DomainTools comes in. DomainTools provides the best suite of research tools for domain-based and DNS cybercrime forensics. These research tools help you connect the dots in your online investigation and illuminate the map of criminal activity.

THE UNDISPUTED LEADER IN DOMAIN AND DNS INTELLIGENCE

DomainTools is the undisputed industry leader in Whois and DNS research tools for cybercrime investigation.

DOMAIN AND WHOIS RESEARCH TOOLS

Whois Lookup – The most comprehensive Whois record database across more than 250 million domains
Reverse Whois – Provides all domains associated with any Whois record parameter such as registrant's name, company name, email address or street address
Domain Search – Provides all the domains that contain your keyword or brand name across 13 years of domain name registrations

DNS RESEARCH TOOLS

Reverse IP Lookup – Find all domains associated with an IP address
Reverse Name Server Lookup – Find all domains associated with a name server
Reverse IP Whois – Maps all IPv4 addresses. Provides all IP address ranges for a domain or company name
Reverse MX – Provides MX (mail server) records and SPF records for a domain or company

HISTORICAL SEARCH TOOLS

Whois History – Over 10 years of Whois records and change reports for over 470 million domains
Hosting History – A comprehensive report of all IP address, name server and registrar changes over 10 years of a domain's history
Screenshot History – Snapshots of website home pages at regular intervals back through time.

BEST DOMAIN AND DNS DATA IN THE INDUSTRY

With over 15 Billion data points, covering over 470 million domains, all gTLDs and over 300 ccTLDs, and over 10 years of historical records, no one in the industry has more comprehensive and accurate data of who is doing what on the Internet.

- **Largest Data Set**: Over 7 billion Whois records covering over 470 million domains
- **Global Coverage**: Whois records on over 100 million ccTLD domains
- **Historical Archive**: Whois, hosting and screenshot records, dating back over 10 years
- **DNS Change Logs**: 15 billion DNS data points on IP address, name server and registrar
- **Accurate IP Mapping**: Over 8 million manually mapped IPv4 IP address range subdelegations
- **Fresh Data**: The most frequently updated data, making research more accurate and relevant
- **New gTLD Coverage**: Ready for the millions of domains that will come from new gTLDs in 2014
- **Innovative**: Multiple new products inflight on powerful DNS and website data sets

GLOBAL COVERAGE

Breadth of domain and TLD (Top Level Domain) coverage is critical for an online cybercrime investigation as many fraudulent and suspect characters attempt to shield their true identity in foreign, less strict or little known TLDs. While .COM is by far the most popular and most frequented TLD, there are now more than 350 other TLDs, including over 300 ccTLDs (country code TLD), on which nefarious Internet activity is often initiated.

Additionally, the new gTLDs being issued by ICANN next year will likely open the floodgates to a new wave of online fraud and cybersquatting. Over 1800 applications for new gTLDs are currently active with ICANN and there is the possibility that ICANN will allow an infinite number of gTLDs in the coming years. DomainTools has architected its scalability and product suite to be ready for new gTLDs when they launch.

REVEAL THEIR TRUE IDENTITY

CIRCUMNAVIGATING WHOIS PRIVACY

A significant obstacle that many investigators encounter when working to discover the identity of a cybercriminal is the prevalence of Whois privacy. While there are a number of legitimate reasons for opting to keep domain information private, cybercriminals almost always employ Whois privacy in order to cover their tracks. According to a study of Whois privacy data completed by DomainTools in November 2012, nearly 15 percent of all domain Whois records are under privacy protection.

Assuming that a domain has not been under privacy protection from its initial registration, Whois history data represents an especially effective method for defeating Whois privacy. Which is why it is critical that an investigator has access to a comprehensive archive of historical Whois data that can be

used in the discovery process. DomainTools houses the industry's most comprehensive repository of historical Whois data, including more than 10 years of archived Whois records, which can be essential for investigators who are working to identify and track down the current owner.

PROACTIVE RESEARCH & ONGOING MONITORING

GETTING AHEAD OF THE CYBERCRIME BATTLE

DomainTools also provides a number of proactive monitoring tools. DomainTools **Domain Search** surfaces all the domain names that contain a given brand string. Clients plagued by cybersquatting activity can simply search for all the domains that contain their brand(s), and filter the results on helpful criteria to quickly hone in on serious threats.

Similarly, the DomainTools **Brand Monitor** will proactively tell you every time a domain gets registered with your brand in it. Moving quickly to combat nefarious domain registrations is often a very effective technique. Bad guys will generally focus on companies that aren't paying attention, so proving that you are is often enough of a deterrent.

DomainTools **Registrant Monitor** allows you to keep an eye on registrant individuals or organizations that you have identified as suspect. Every time they register a domain name we will notify you. DomainTools **Name Server Monitor** and **IP Monitor** work the same way. If a domain gets pointed to a target name server or hosted on a target IP address, you will receive an email notification.

These automatic monitoring tools provide a nice complement to the active investigation techniques that are necessary for in-process cyberattacks. Organizations most effective at leveraging domain and DNS data to fight online crime are using these monitoring services to stay ahead of online criminal activity.

CONCLUSION:

Most types of cyber attacks leave a trail of network information evidence, including domain names and IP addresses, and DomainTools' data can help uncover the people or organizations behind them. Phishing and spam come from an email address that has a domain name and MX records attached to it; Malware in its various forms can be delivered through clicks or even drive-by on domain names; DDOS attacks come from one or multiple IP addresses. Any online threat investigation can therefore either begin with, or be informed by, detailed DNS data. By DNS data we mean domain name and IP address Whois data and data that associates domain names, IP addresses and name servers to each other and to individual people and organizations. DomainTools has the largest and most accurate database of DNS data available anywhere. With over 10 years of proven experience, we help you connect the dots in cybercrime investigations. DomainTools is the singular source for all your DNS and domain data needs, and all queries are 100% private and confidential. Give us a call and let us walk you through a demo of our tools in action.

ABOUT DOMAINTOOLS:

DomainTools offers the most comprehensive searchable database of domain name registration and hosting data geared to monitor, protect and investigate online fraud, cyber crimes and brand fraud. Users of DomainTools.com can review over 470 million historical domain name and Whois records, over 3 billion DNS data points (IP addresses, name servers, mail servers, hosting history), and 6 years of Screenshot history. The Company's comprehensive snapshots of past and present domain name registration, ownership and usage data, in addition to powerful research and monitoring resources, help customers by unlocking everything there is to know about a domain name.

Visit the website at **http://www.domaintools.com**