DOMAINTOOLS®

Best Practices Guide:

Getting Started with DomainTools for Threat Intelligence and Incident Forensics

Introduction

Cybercrime represents a major threat to both government and businesses, costing the economy hundreds of billions of dollars in losses every year. Often, the most challenging part for an investigator is discovering the *who* behind an attack. Is it a coordinated attack orchestrated by a criminal syndicate or an amateur hacker looking for a backdoor into your network? If the actual individual cannot be identified—as is too often the case—then investigators can build a Threat Intelligence Profile on the suspect that uniquely "finger prints" the organization and how they act. Threat investigators need to use all the tools at their disposal in order to identify the individuals and organizations involved in an online attack. DNS and Whois data is an essential tool that should be leveraged by every incident response team.

This guide will show you how DomainTools products can be applied during the course of an investigation to identify the perpetrator, build a profile of a cyber-attack, and proactively protect your data, infrastructure and intellectual property.

Five Ways to Use DomainTools in Cybercrime Forensics

What follows are five steps that can be used to identify the source of an online attack, how to gather evidence and how to improve your domain security posture. Each of these methods is explained in greater detail below; however, the individual steps can be summarized as follows:

1. Develop a Suspect Profile
2. Map Associated Activity
3. Identify the Source (Attribution)
4. Build a Case of Evidence
5. Proactively Monitor Your Domain Assets

Using DomainTools products, and the wealth of data behind them, investigators can solve puzzles of attribution, discovery and identity in their efforts to connect all of the dots throughout the course of their online investigation.

Common Attack Vectors

The following four methods represent the most common forms of cyber-attack:

DDoS – Distributed Denial of Service: A form of cyber attack meant to 'take down' a website. By flooding a webserver(s) with traffic from hundreds or thousands of IP addresses simultaneously, a DDoS attack can render a webserver unable to respond to normal user requests, effectively making a website inaccessible.

Phishing: A form of cyber-attack, normally administered via email, which attempts to trick a user into thinking the email is from a trusted source, and whose embedded links send a user to a fake site which hosts some kind of malware or nefarious attempt to capture the user's login credentials.

Malware/Virus: Used generically to describe a piece of executable code that gets installed on a target's computer by any number of methods, including download, application exploit, or even 'drive-by' on a website.

Targeted Hacking/Advanced Persistent Threat: Perhaps the greatest threat to the enterprise, targeted hacking and Advanced Persistent Threats are designed to remain undetected for a long period of time with the intent of stealing private data rather than trying to bring a network down.

In each of these methods, a communication protocol is present. That is, all types of cyber-attacks involve sending information from one node on the Internet to another. Data points gleaned from sources such as Whois records, IP addresses, and name servers surfaced by DomainTools can help map these individual nodes to one another, thereby creating a trail of useful information that can be used to help identify the individuals or organizations behind a given attack.

Step 1. Develop a Suspect Profile

Similar to a crime that occurs in the physical world, a cybercrime investigator should first create a profile of a suspect based on the data points left behind. In the case of a cyber attack, domain data represents a starting point for gathering the necessary intelligence that will help aid the identification process. A Suspect Profile can be defined using some of the following domain data components, all of which can be gleaned from various DomainTools products. These discrete data points might include:

- Domain name registration data (Whois record)
- IP address information
- Name server
- Hosting information
- Autonomous System Number (ASN)
- Mail server

Following an incident, almost every investigation will start by trying to identify who is behind an attack. If a specific domain can be associated with an attack, a **Whois Lookup** search can be executed to research a specific domain name to determine if there is any useful contact information associated with a specific domain address. However, nowadays most criminals mask their identity by either enabling Whois privacy or forging Registrant Whois information, forcing an investigator to reverse engineer identifying data points in the effort to build a composite suspect profile. But even the fake registrant information in the Whois record can be used to track an attacker and find other domains they own, as they often use the same, or similar, credentials to register multiple sites.

Thus by tracking the false registrant, a profile of associated domain names can oftentimes be developed. If only the IP address is known, it is best to start with an **IP Whois Lookup** to get a profile on the IP address and a **Reverse IP Lookup** to get a list of domains associated with that address. From there, and if the list is not excessively long, it is good to pull the Whois records on each domain to build a list of suspects.

To reverse engineer other identifying data points, an investigator will often map the associated activity (Step 2) in order to build a behavioral profile on the suspect and collect more data points from which to search for identifying information.

Building a Suspect Profile with DomainTools Products

- **Whois Lookup:** DomainTools Whois Lookup features the industry's the most comprehensive Whois database, covering more domains and TLDs than any other domain intelligence tool in the market.
- **Whois History**: DomainTools maintains the largest and most accurate database of Whois records, including an archive that spans almost 12 years of domain registration data.
- **Reverse Name Server Lookup:** DomainTools' Reverse Name Server Lookup provides a list of all domains hosted on a queried name server.
- **Reverse IP Lookup:** DomainTools' ReverseIP search will identify all domains hosted on the same IP Address.

Step 2. Map Associated Activity

Most of the discrete data points collected over the course of an investigation will not yield a great deal of intelligence on their own. To help make sense of all of these individual data points, investigators will often create a map of associated online activity in order to define a more complete picture of a potential criminal network. Once these single data points (i.e., IP address, name server, host, etc.) are mapped and connected together, a more complete picture can be brought into focus.

However, investigators often only have a single piece of identifying information to start with and will have to employ a variety of research tools to create this type of map. **Reverse Whois** is a useful place to start and can map any piece of registration data (i.e., e-mail address, phone number) to discover all of the domains that a registrant either currently owns or has owned in the past.

A **Reverse Name Server Lookup** and Reverse IP lookup can also be effective methods by which to map domains together according to a common name server or IP address. This can be used both as a way to validate connections between offending domains as well as to eliminate potential 'false-positives.'

Similarly, mail servers can be used as another triangulation point. If a mail server is associated with a suspect domain or IP address, it may host other suspect domains. And any one of these points may provide the investigator clues to the identity of the organization or how they operate.

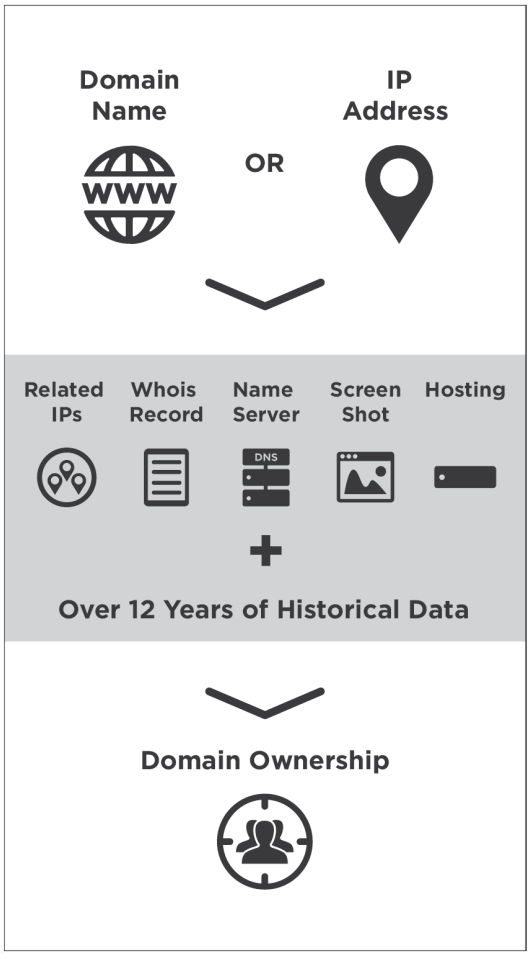
Following a domain's hosting history (history of changes on IP address, name server and registrar) provides yet another investigative path to follow. This can be particularly useful to find a change in ownership when the first instance of a domain might be on a more revealing IP address or host.

Mapping Associated Activity with DomainTools Products

- **Reverse Whois Lookup:** The DomainTools Reverse Whois Lookup tool allows you to enter one or more unique identifiers (such as an individual's or a company's name, phone number, email address or physical address) and learn all the domain names they own or have ever owned.
- **Reverse IP Lookup:** DomainTools' patented Reverse IP Lookup tool will display domains currently hosted there. Results include gTLD domains and ccTLD domains.
- **Reverse Name Server Lookup:** DomainTools' Reverse Name Server lookup provides a list of domains hosted on a queried name server.
- **Hosting History:** DomainTools' Hosting History tracks changes to a domain's IP address, name server and registrar over time.
- **ReverseMX Lookup:** ReverseMX provides a list of domains and IP addresses associated with a mail server, or conversely the mail servers associated with a domain.

Step 3. Identifying the Owner (Attribution)

One of the greatest challenges for anyone investigating the origins of an attack is circumnavigating Whois Privacy, which is often used by criminals as a cloak to conceal their true identity. There are two primary ways by which investigators can source domain attribution in the event an attacker has shielded their identity using Whois Privacy. The first method uses contact information from current or historical Whois records to pinpoint ownership or to establish connections between domains. If contact information is not present, a second method involves using IP address or name server information, ultimately to the same end: to uncover connections between domains and, in some cases, ownership of domains (in an indirect way).



If the current Whois record for the domain is fully privacy-protected, **Whois History** can be an effective way to source attribution. Because many domain owners originally registered their domains without privacy in place, Whois History can sometimes uncover the real owner of a domain that is currently veiled by privacy. If a non-protected record is found in Whois History, an investigator can compare what the domain looked like before and after it transitioned to Whois Privacy. If the before-and-after screenshots in **Screenshot History** are consistent, there's a high probability that you have identified the actual owner of the domain, which has since been cloaked by privacy.

Of course, just because there is information listed in a particular registration, it doesn't mean that it's true. However, even false registration data can point to a likelihood that a group of fraudulent domains are owned by the same entity. **Reverse Whois** can be used to show all of the domains that share a common—and even spurious—data point such as an email address, person name, organization name, phone number, or physical address.

Identifying the Owner with DomainTools Products

- **Whois History:** DomainTools maintains the largest and most accurate database of Whois records, including an archive that spans almost 12 years of domain registration data.
- **Screenshot History**: DomainTools Screenshot History tool is used to showcase screenshot images, collected over time, of a specific domain's website.
- **Reverse Whois:** The DomainTools Reverse Whois Lookup tool allows you to enter one or more unique identifiers (such as an individual's or a company's name, phone number, email address or physical address) and learn all the domain names they own or have ever owned.

Step 4. Build a Case of Evidence

Once you have succeeded in pinpointing the identity of the attacker, it's time to move to the next stage of the investigation: building a case of evidence. Just as in a court of law, an investigator will need to assemble, document, and organize an archive of evidence that can be used in the event that prosecution is pursued. DomainTools products can be used to collect present or historical Whois records, evidentiary screenshots, inventories of connected domain names, and other relevant information that can be used to build a case for IP/domain takedown, sinkholing, or legal action.

When a "bad domain" is identified, forensic investigators should use screenshot tools to snap a screenshot of the offending site, which can then be submitted as evidence in court. This can also be a useful tool for documenting any "typo domains" which are engaged in liability causing activities (i.e., distributing malware via drive-by download). Creating a record of screenshots, noting the creation date of the domain from the Whois record, allows a litigant to effectively prove how long a fraudulent act has been taking place.

Building a Case of Evidence with DomainTools Products

- **Screenshots**: A simple and effective way to snap and timestamp screenshots for evidentiary purposes
- **Screenshot History:** DomainTools Screenshot History tool is used to showcase screenshot images, collected over time, of a specific domain's website.
- **Domain Report:** A unified and fully formatted PDF report that collects, collates and formats all of a requested domain's information
- **Whois History:** DomainTools' Whois History enables users to track ownership and registrant information over the past 12 years and record domain ownership and ownership changes to show length of domain ownership.

Step 5. Proactively Monitor Your Domain Assets

For companies that want to take a more proactive stance against cybercrime, monitoring services identify changes to an IP address, name server, domain or registrant as they happen. For instance, a **Registrant Monitor** service can be used to send alerts when a registrant (in this case one who has been observed to be nefarious) registers new domains; these domains can then be proactively blocked or subjected to additional security scrutiny.

In a similar fashion, a proactive **IP or Name Server Monitor** can alert an organization to new domain activity tied to a specific IP address or name server, providing another layer of security. Both of these approaches are similar to credit monitoring services used by consumers to protect them from identity fraud and be an effective way to monitor phishing, typo-squatting sites, or other as of yet undiscovered vectors by which an attacker can compromise valued domain assets.

Proactively Monitor Domain Assets with DomainTools Products

- **Registrant Monitor:** Registrant Monitor will proactively monitor when the given registrant registers a new domain.
- **IP Monitor:** The IP Monitor tool monitors any additions and changes to registered domain names associated with an IP address. This can be used to keep a close eye on suspect IP addresses and known "bad IPs" or to track your own IP range to ensure sure unauthorized websites are not pointed to your IP addresses.
- **Name Server Monitor:** DomainTools' Name Server Monitor will check daily for new domains added, deleted or transferred to or out of a monitored name server.
- **Brand Monitor**: Brand Monitor will notify you of new domain name registrations that include a pre-defined text string (e.g., a brand).
- **Domain Monitor:** Domain Monitor monitors for ownership changes or expirations of a specified domain.

Conclusion

Most types of cyber attacks leave a trail of network information evidence, including domain names and IP Addresses. DomainTools' data services 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. DomainTools maintains the most extensive and accurate database of DNS data available on the Internet.

To learn more about how DomainTools can help you in your investigations, please visit us at: **domaintools.com/solutions/cybercrime-investigation**

Try DomainTools Free

To see the power of DomainTools, **start a 7-day free trial**. Get access to the same tools that top cybercrime investigators have leveraged for years to slam the door on criminals and fraudsters. Visit **www.domaintools.com** for more information, or contact us at **sales@domaintools.com**.

About DomainTools

DomainTools is the leader in Domain Name and DNS research products. We help security pros and cybercrime investigators with threat intelligence, scoping and attribution. We have the world's largest database of current and 12-years' historical data on domain ownership, Whois records, IP, name server, mail server, SSL cert, screenshots and more.