CYBERSECURITY INESTIGATION AND ANALYSIS

The New Crime of the Digital Age

The Internet is not just the hotspot of all things digital and technical. Largely due to its ubiquity and countless (and frequently anonymous) points of entry, the web has given rise to a new breed of outlaw – cybercriminals who prey on the wealth of valuable information available online.

Lloyd's Insurance estimates businesses' global losses from cybercrimes in 2015 were $400B, while some vendors believe losses totaled $500B. Only estimates are available, because many thefts go unreported as security breaches can damage an organization's reputation.

Unfortunately, there is no end in sight. Losses roughly quadrupled from 2013 to 2015 and Juniper Research recently forecasted that in 2019 global losses will reach a staggering 2.1 trillion dollars.

In addition to the enormous financial losses, these online crimes have also ruined reputations of companies and rendered victims vulnerable, as the perpetrators now have access to critical data that may be used against them.

With advances in digital technology, online criminals have grown even more aggressive and creative in their ways, despite efforts to strengthen and tighten online security. The crackdown on these online crimes remains a constant challenge for many law enforcement agencies and private IT security professionals.

Types of Cybercrimes

The first step in combating cybercrimes is understanding the potential threats. With the never-ending breakthroughs in the digital world and the ever-increasing capabilities afforded to users, cybercriminals have also become more intelligent, more creative and more aggressive resulting in more types of cybercrimes than the FBI's, Interpol's and other agency's cybercrime units, or security protocols can effectively prevent.

- **DDoS (also known as distributed denial of service) attacks** occur when compromised computers and other hardware are used to spread malicious codes on networks and websites, causing the network to crash.

- **Hardware hijacking** targets the computer and other digital hardware providing criminals access to the data contained in compromised systems, including one's email, files and folders. Hijacking generally occurs when users open or click certain links, or download malicious files designed to infiltrate the computer.

- **Phishing** is common in email. Many fall victim to these attacks when they click on spam messages in their junk folder that are actually worms or viruses designed to infiltrate the data system. Once in, user information is easily accessed by the cybercriminal.

- **Counterfeit ecommerce** takes advantage of the popularity of online shopping. A fraudulent ecommerce website is set up, luring shoppers to the site and accessing their personal information. Another common form is the selling of fake products, especially luxury brands, in online stores.

- **Identity theft** is a common form of cybercrime where hackers gain access to one's personal accounts or a database and steal critical information, such as credit card details or social security numbers for their own gains.

There are other categories of cybercrimes, including online bullying, stalking, electronic vandalism, and extortion. However, those mentioned above are the most common forms of cybercrime used in targeting companies and individual accounts, and thus can have far-reaching impacts, both on the business and personal fronts.

The Security Strategy

The key to cracking cybercrimes lies in two important elements: the DNS (or domain name system) and the Whois data.

The DNS translates domain and Internet names into IP addresses, which are then used to track computers and networks across the globe. It's the first place to start when looking up sources of transactions on the World Wide Web, including sites that contain malicious codes and links.

The other critical link is the Whois database, which contains domain names, IP addresses, and contact information of registrants (those to whom the domain name is registered). The FBI and Interpol cybercrime units typically start their investigation of cybercrimes here. A search is made on the Whois database to determine who owns the site, how long it's been up, its legitimacy, and the most important information of all - the location of the website owner.

In some cases, the data in the Whois registry may be inaccurate or incomplete. This is why in most investigations, information in the Whois database is correlated and supported by information from the IP address assignment records (through the DNS). According to the FBI, the IP address records often yield information that can generate leads such as the web hosting company.

For example, in the case of a fraudulent online shopping site that has tricked the public into sharing their credit card details under the guise of a product purchase, the first step is to identify the operator and owner of the site. By matching the IP address, a query of the domain name is first made. A search on the Whois database is also carried out to look for information as to the owner of the fraudulent site, the details on how the site was paid for (i.e., credit card), other malicious sites that were also paid for using the same account, and hopefully other leads, such as the location of the domain owner. With these leads, the authorities can then take the necessary next steps to apprehend the criminal.

Cracking cybercrimes

While it is true that these cybercriminals have become more aggressive and creative in the way they operate (in most cases, they work together and are not individual perpetrators), there are a number of simple security measures that businesses and individuals can employ as an added layer of protection. These can include any of the following:

- Not opening suspicious emails in Spam or Junk folders
- Disabling cookies on web browsers to avoid storing any critical information
- Installing a firewall to filter information exchanged with other computers
- Browsing only on secure sites where data is encrypted as a form of security

These are simple measures to safeguard against hacking and information theft, which may be easily employed by an individual. However, for companies and businesses with more to lose, more sophisticated defenses and tools are required, hence the development of software and programs designed to both thwart and trap cybercriminals.

These security solutions primarily rely on Whois data. The Whois record contains information on the domain name, which serves as the starting point of cybersecurity analysis. From the domain name, other critical information may be obtained such as:

- Registrant name
- Registrant email, phone number and address
- Name server

- IP address
- Registrar
- Registration date
- Expiration date
- Updated date

For example, in tracking down malware spreading from unknown sites, investigators first examine information contained in the Whois registry. A website may be suspected of hosting malware if any of the following information is found:

- Recent registration date
- Close expiration date
- Registrant owner is in a high-risk country
- Registrant and website location are different

Besides utilizing Whois data, security solutions also feature the following functionalities and capabilities:

Surface Leads are instrumental in collecting and gathering data, including the following:

- Finding contact information from a single domain name or IP address
- Getting behind Whois privacy records by scouring historical Whois records
- Identifying associated nameservers, IP addresses, MX servers and more for triangulating perpetrator identities
- Correlating the data with external data to strengthen connections and patterns

Scoping the breadth of nefarious activity to identify all fraudulent acts by:

- Identifying all connected domains, websites and IP addresses associated with fraudulent activity
- Searching parsed Whois data to perform a broad search focused on limited data
- Cross-referencing a domain name in the Whois data with other useful DNS data points

Preventing future threat activity by:

- Identifying other sites and networks associated with known-bad sites or actors and shutting them down immediately
- Monitoring domains, IP addresses, nameservers, and registrant information of suspect characters
- Leveraging Brand Monitor to prevent fraudulent domain name registration across all top level domains (TLDs) worldwide

The Whois API Solution

Whois API specializes in providing Whois database access that can be used in tracking cybercriminals and hackers. Whois API's three major products are for businesses and companies with the infrastructure and expertise to carry out Whois database searches to track malicious activity on their sites.

Hosted Whois Webservice

The Hosted Whois Webservice is an online service that returns well-parsed Whois fields for every URL request made in common formats, such as the XML and JSON. This web service offers the following key features:

- **Accessible platform.** The Whois Webservice works on basic HTTP so it circumvents firewall restrictions, which can limit access to Whois servers on port 43.

- **Comprehensive Whois database.** To ensure that a search has covered all of the Whois registrars to yield complete information, this web service follows the Whois registry referral chains to track down the correct Whois registrars, in order to recover the most complete Whois data.

- **Powerful infrastructure.** This product utilizes smart mechanism and powerful protocols to avoid query limits posed by Whois registrars during searches.

- **Readable format.** Whois query yields exceptionally freeform data, translated into well-structured and readable formats (XML and JSON) that are compatible with most applications. It can reveal very specific information, such as name, organization, street, city, state/province, postal code, fax number, and telephone numbers. The data is also cleanly displayed by eliminating header and footer text.

  The parser is fault tolerant as it is constantly tested and improved, and parsing support for all Whois registers is available.

  It also returns registry dates (creation, most recent update, and expiration) in original and normalized formats.

The Whois Hosted Webservice has a wide range of applications, covering simple to more serious online offenses. It may be used for queries and activities involving the following:

- Tracking domain registrations to discover owner details
- Detecting credit card fraud
- Investigating spam, fraud, intrusions, and other online misbehaviors
- Checking advanced Whois web pages
- Providing geographical location of users

In addition to cybercrime investigation, the web service is also handy for researching internet infrastructure and usage. One example is of this is website setup and creation. Web developers may consult the Whois database to determine the availability of a domain name for a website they're deploying.

Whois Database Download

Whois API also provides an offline alternative to the hosted web service in the form of the Whois Database Download. Organizations may access a downloadable an archived Whois database containing complete history of a domain name. Records may be displayed in either raw text only, or raw text and parsed formats, and are downloaded as database dumps (MYSQL or MYSSQL dump) or CSV files (Office Excel-based). This service offers Whois archived records for most of the major GTLDs (generic top-level domains) such as, .com, .net, .org, .us, .biz, .mobi, .info, .pro, .coop, and .asia.

In addition to cybercrime investigation, the database download may also be used for statistical research analysis and to extract fine-grained information, including archived Whois records.

Reverse Whois

Tracking and investigating online crimes is frequently a game of trial and error, and random searches. In other cases, "inactive" cybercriminals and hackers may be identified using a simple random search on the Whois database. And yet, in a few more cases, searches made on the Whois database are not to purposely track and investigate cybercriminals, but to simply look up and research a domain name intended for legitimate business purposes. This is where the Reverse Whois or Registrant Search comes in.

There are a number of business uses and functions of this service, among these are the following:

- Website owners and managers use this service to identify new business and partnership opportunities, and to locate potential buyers through the contact details provided in the Whois database.
- Brand agents use Reverse Whois to protect their intellectual property and to check for potential trademark infringements through random searches scoping domain name similarities, duplicates, or copycats.
- Domain investors sometimes use information from random searches on the Reverse Whois to evaluate their competition and identify investment opportunities.

Whether you're a company looking for a domain name for your site, or you're out to catch hackers, the Reverse Whois enables searches on the Whois database using a single piece of data to gather a plethora of information via keyword matching.

Users may only have a name or an email address which they can use to retrieve more information about the registrant from the Whois database. The Reverse Whois Database allows advanced searches using multiple search terms on both current and historic Whois databases. This service produces results viewable online, or downloadable in CSV and PDF formats.

These services prove invaluable when undertaking the first steps to identify and thwart cybercriminals. Without these features and databases accessible to the public, it will be doubly difficult for the FBI and Interpol Cybercrime and concerned authorities to identify the masterminds behind online crimes. And at the same time, the Whois and DNS records also serve business and commercial functions.

Taking the Next Steps

When dealing with cybercrimes, it's important to remember that many criminals and suspected characters conceal their true identity in foreign and less regulated and less popular TLDs. This is why looking at the breadth of domain and TLD coverage remains a critical step in cybercrime investigations.

While .com is the most popular and commonly used TLD, there are approximately 350 other TLDs, as well as more than 300 ccTLDs where fraudulent Internet activity also occurs.

Furthermore, with the ICANN issuing new gTLDs next year, most internet security experts anticipate an increase in online fraud and cybersquatting. Currently, there are over 1800 active applications for new gTLDs and quite possibly, even more applications may be made in the coming years, and thereby likely a new wave of cybercriminals to catch.

Security solutions companies cannot be left behind. Whois API has enhanced its scalability and product suite in preparation for the launch of the new gTLDs, and to continue providing critical data and tools to combat cybercrimes.

Visit us at http://www.whoisxmlapi.com for more information on how Whois API may assist your organization.