Uncovering Criminal Bulk Registration Activities with Bulk Domain Name Checkers

Posted on February 4, 2020

To propagate cyberattacks, threat actors use domain generating algorithm (DGA) as an evasion tactic. This algorithm, executed through various subroutines, involves switching or dropping thousands of domains in seconds.

The relative ease with which cybercriminals can purchase domains in bulk makes it possible for them to accomplish DGA-enabled attacks. Dirt-cheap prices and lack of identity verification enable hackers to own domains while also staying anonymous.

In fact, registrars typically offer privacy protection services at a small cost or for free, which nefarious actors may take advantage of to conceal their location and details. Additionally, the introduction of the Temporary Specification for Generic Top-Level Domain (gTLD) data has led to masking or redacting WHOIS data, which, of course, benefits not just those who wish to protect their privacy, but also those with malicious intent.

How Cybercriminals Use Bulk Domains

According to Malwarebytes, DGA is designed in a manner that makes it easy for hackers to change a variable or two without having to rewrite huge chunks of code, all while avoiding detection. DGA has three components:

- **Seed:** The seed is any number, such as a specific time, date, or foreign exchange rate.
- **Time-based element:** The time-based element refers to a condition that changes over time, such as events or trending topics.
- **TLDs:** The TLDs involved are pseudo-random-looking domains that the algorithm dynamically generates by the thousands. Attackers register only a few of these domains for use. An example of a DGA-created domain looks something like this: t3622c4773260c097e2e9b26705212ab85[.]ws. A Dyre banking trojan used this particular domain.

Malware and botnets commonly use DGA domains to query and pivot to communicate with command-and-control (C&C) servers. Once a malware strain compromises a computer, for instance, it begins to query multiple DGA domains to obfuscate C&C traffic.

Summary of Bulk Domain Abuse Findings

The following trends have emerged from our review of existing papers on bulk domain misuse:

- 1. The most abused domain name extensions are .xyz, .cloud, .top, .tokyo, and .us, according to a study by the Interisle Consulting Group. Two of these domains (i.e., .xyz and .top) have been consistently found in the top 20 blocklists maintained by Symantec and Spamhaus in the past two years. To date, new TLDs like .buzz, .country, .link, and .download have also made it to popular watchlists.

- 2. Attackers share the same resources. It only takes one mail server or domain to find out the nest of domains and subdomains they use. Often, these domains have a strong connection with affiliate ad networks or potentially unwanted programs. Hackers are also likely to use IP address spaces and Autonomous System numbers (ASNs) that are home to known threats.

- 3. Incomplete WHOIS details are better than nothing. Incomplete WHOIS records can still guide investigators as they study attacks. Partial results reveal a lot about an attacker's infrastructure, and analysts can use this data to identify other email and IP addresses or domains connected to an event.

- 4. Long-term monitoring is needed to uncover abusive repeated registrations and how domains with high entropy figure in attacks. Indeed, a Danish study last year found that re-registrations for abused .dk domains and the use of high entropy domains in ongoing attacks were irregular. One reason is that DGA has become increasingly sophisticated and harder to detect. Future studies also have to widen the scope of their datasets to entire zones to improve the quality of samples.

- 5. Similar to the last point, it is critical to monitor parked domains even if they're not actively abused. According to the Interisle study, some domains don't make it to a blocklist right away following registration. This finding implies that hackers buy and hold on to domains for later use.

- 6. One of the hallmark characteristics of domains registered in bulk is the presence of random-looking strings. These strings are often the result of automation, suggesting that a registrar-owned name generator may have been used to create them.

How Bulk Domain Name Checkers Can Help Thwart Attacks

Registrars, cybersecurity professionals, and antimalware vendors can evaluate known and undiscovered risky domains with the help of a **bulk domain checking** solution. One example of this is Bulk WHOIS Search, which provides bulk WHOIS records for multiple domains. With the tool, users can:

- **Block malicious domains effectively:** Users can quickly validate whether the traffic they're receiving comes from legitimate sources or blacklisted sites. WhoisXML API has indexed over 6.7 billion historical WHOIS records from authoritative sources to provide the most accurate results.

- **Monitor domains for brand research and protection:** Brand managers can rely on Bulk WHOIS Search to curb fraud and trademark abuse. They can use the application to routinely search for domain names that resemble or infringe their assets. The API can also be used to obtain WHOIS records for electronic discovery and domain disputes.

- **Resolve security incidents on time:** Bulk WHOIS Search simplifies the process of querying WHOIS records for multiple domains found in firewall logs. The tool can also be used to reveal patterns when changes to WHOIS records are made, such as those concerning creation dates, contact names (before privacy), and registrars.

Complete WHOIS data is invaluable to security professionals to respond timely to cyberattacks. When used with other threat intelligence solutions, **bulk domain checking** tools like Bulk WHOIS Search

facilitates the swift detection of criminal actors’ servers and domains.