Exploring IoCs and Their DNS Narratives

Posted on July 10, 2024

No matter how stealthy attackers try to be, they almost always leave a trail behind—digital breadcrumbs known as “indicators of compromise (IoCs)” after a cyber attack or an attempted intrusion.

Let's take the Black Basta ransomware attacks as an example. Cybersecurity authorities like the Cybersecurity and Infrastructure Security Agency (CISA) identified hundreds of IoCs associated with this ransomware-as-a-service (RaaS) variant. These IoCs include cyber resources like file hashes, domain names, and IP addresses, and serve as digital footprints pertaining to the attackers’ activities. They provide invaluable clues for cybersecurity professionals, helping them understand what happened and prevent similar attacks in the future.

But while IoCs tell us something suspicious happened, they don’t reveal the whole story. Security professionals often need to tap into several resources to turn IoCs into actionable intelligence. That’s where the real detective work begins, and in this blog post, we’ll explore how shedding DNS light on IoCs can help strengthen cybersecurity defenses.

Turning to the DNS for Clues

We’ve established that IoCs are essentially digital breadcrumbs attackers leave behind. But how do we make them useful? The answer, or at least part of it, lies in the DNS as a critical source of cyber intelligence.

The DNS can reveal hidden threats, notably through various red flags. This information can thus make security solutions more powerful when used alongside with other threat intelligence sources, such as IoC lists. Below are some of the most common clues the DNS provides.

Multiple Failed DNS Queries to Unusual Domain Names

Once installed on target systems, malware must communicate with control servers, often identifiable via domain names. To evade detection, attackers may use domain generation algorithms (DGAs) that churn out a vast number of domain names containing random characters. Here's an example of a group of possible DGA-created domains obtained from the Early DGA Data Feed for reference.

- money4click-jpq[.]buzz
- money4click-yub[.]buzz
- money4click-ste[.]buzz
- money4click-pqj[.]buzz
- money4click-npl[.]buzz
- money4click-vbr[.]buzz
- money4click-raj[.]buzz
- money4click-ucj[.]buzz
- money4click-qus[.]buzz
- money4click-dol[.]buzz
- money4click-kjj[.]buzz
- money4click-oye[.]buzz

- money4click-fds[.]buzz
- money4click-eov[.]buzz
- money4click-mdt[.]buzz
- money4click-pbw[.]buzz
- money4click-sin[.]buzz
- money4click-jxi[.]buzz
- money4click-amn[.]buzz
- money4click-cdr[.]buzz

Malware will keep contacting the DGA-created domains from client IP addresses until they establish a connection with the command-and-control (C&C) server. The communication continues while malware would attempt to exfiltrate and transmit stolen data. The process often results in multiple failed DNS queries since only a few DGA-created domains are activated. As such, failed DNS requests to suspicious domain names can signal an ongoing attack.

Unexpected DNS Query Volume at Unusual Times

Employees accessing internal resources or browsing the Web generate a specific level of DNS activity from client IP addresses. However, this activity dips significantly after office hours. So, a sudden spike in DNS requests from the same client IP addresses outside regular business hours can be a cause for concern. This anomaly may indicate unauthorized access or malicious activity in progress. Security professionals can leverage this information to investigate further and potentially prevent a security breach before it unfolds.

Similarly, a single IP address or domain name generating an unusually high volume of DNS requests can be a sign of something suspicious. This spike may indicate malware attempting to

connect with a C&C server.

Blocked Outbound Traffic

As firewalls constantly monitor and filter incoming and outgoing traffic, they are bound to deny or block unauthorized or suspicious communication attempts. These attempts include traffic generated by malware contacting C&C servers for further instructions or to transmit stolen data.

While a single denied outbound traffic from a client IP address may not raise an alarm, continuous attempts to connect (despite being constantly blocked by firewalls) should trigger a red flag.

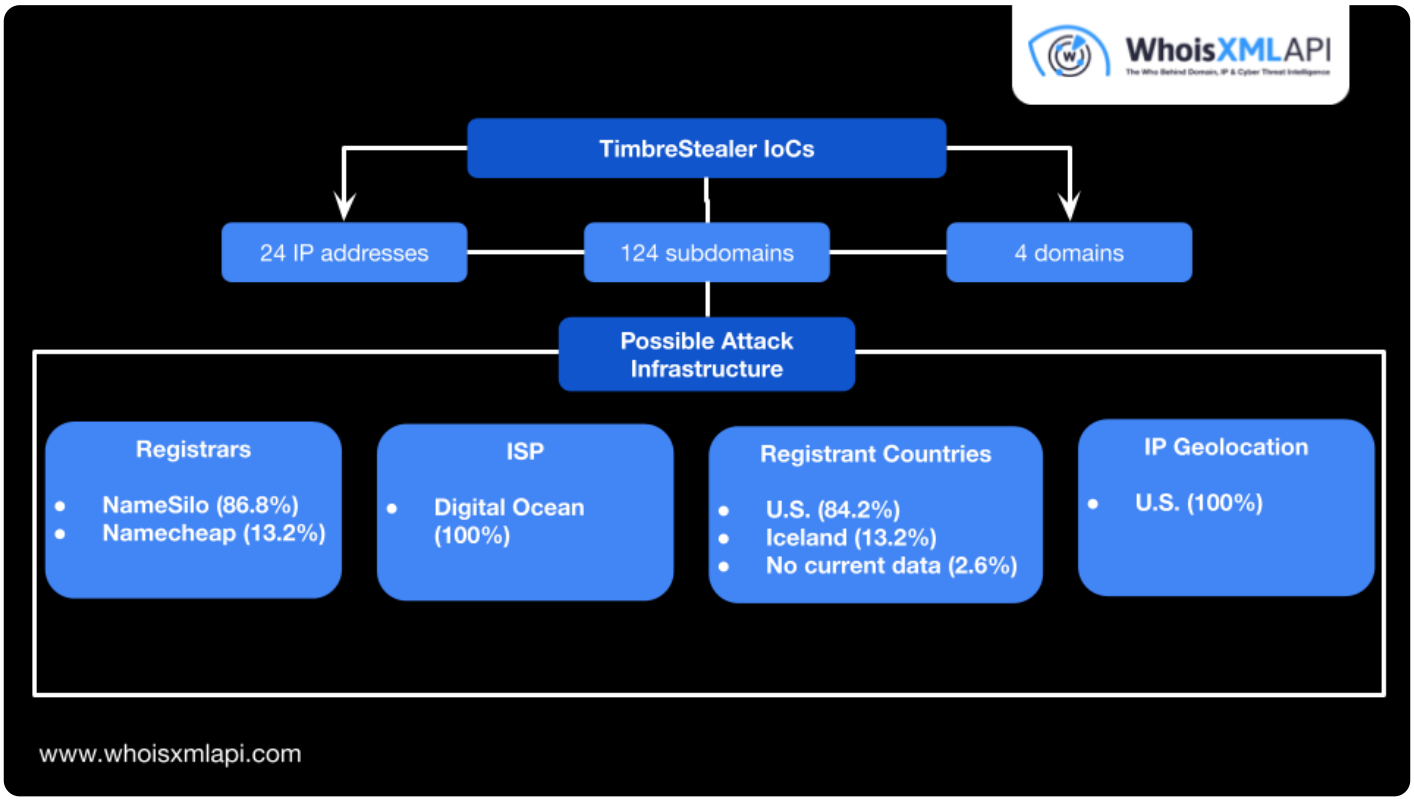
What IoCs with DNS Intel Can Reveal

When given a list of IoCs, security teams and solutions can immediately block access to and from them to ensure they won't cause harm. However, when used alongside DNS traffic analysis, security teams can do much more.

Reveal Attacker Infrastructure

IoCs often include malicious domain names or subdomains used in attacks. In fact, tens of thousands of malicious domains are detected every week. These IoCs can be C&C domains malware use for communication with attacker-controlled servers. Analyzing them aided by DNS intelligence can help identify attackers' C&C infrastructure. In some cases, the analysis can even help law enforcement agencies disrupt botnets.

By analyzing these domains alongside DNS information, security professionals can discover registrar and registrant information, hosting providers, subdomains, IP addresses, ISPs, and geolocations. Take a look at an example of the details we discovered after analyzing TimbreStealer malware IoCs in one of our threat reports. TimbreStealer is a relatively new information-stealing malware detected by Cisco Talos early this year.



Analyze Threat Actor Behaviors

IoCs may expose attack patterns. For example, the characteristics of domain IoCs can hint at the use of Punycode or DGAs to create and register domains. For instance, DGA-created domains were prominent among the TimbreStealer IoCs. Take note that it's not only for this particular malware. The use of DGAs is not surprising since MITRE has named them as one of the most common attacker techniques (T1568.002).

Beyond that, IoC lists often contain IP addresses, URLs, domain names, and other identifiers associated with past malware campaigns or malicious actors. Checking these IoCs for DNS traces can help security professionals and tools identify if:

- A client IP address is attempting to communicate with known malicious domains or IP

addresses

- There is a sudden surge in DNS requests for a specific domain or system, primarily a domain known to be malicious or suspicious, which can be a strong indicator of active exploitation attempts

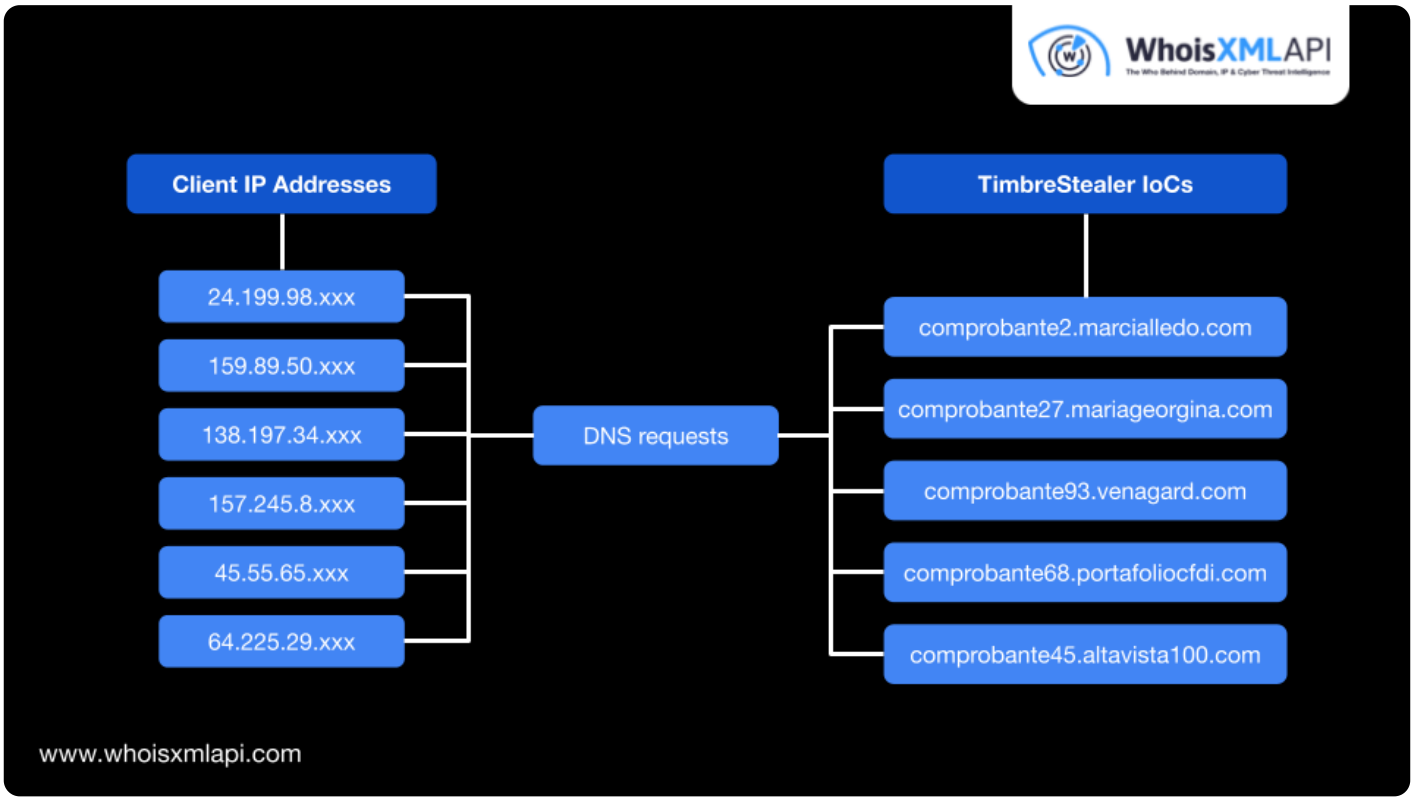
- A client IP address is constantly querying for alternative resolutions of a known malicious domain, which may indicate attackers are trying to evade detection by using different subdomains or typosquatting techniques

- The geographic sources of DNS requests for IoCs align with associated threat groups' target locations or if they are targeting a new region

Identify Newly Targeted Victims

Research by Sophos revealed that the cyber attack dwell time (i.e., the period of time from the start of an attack to its detection) is eight days and five days for ransomware attacks. However, the same research also says it takes less than a day for ransomware attackers to reach the Active Directory, one of an organization's most critical assets. This scenario highlights the speed at which any malware can move laterally within a victim's network and the crucial need for early threat detection.

Using DNS intelligence is an effective way to support early threat detection. If multiple client IP addresses attempt to resolve one or more malicious domains listed as IoCs, it may indicate device and network infection.



Conclusion

The cybersecurity community recognizes that a solution enabled by passive DNS (pDNS) data can help stop 92% of malware. During the early attack stage, such as in malware distribution through phishing, DNS-based security tools can help users avoid unknowingly visiting known phishing sites and downloading malware.

The same strategy can help detect and foil attack execution while malware communicate with C&C servers. In addition, DNS intelligence can shed more light on IoCs, helping security teams identify attack infrastructure, attacker behaviors, and even active malicious campaigns.

Learn how you can glean more actionable intelligence from IoCs using DNS intel. Contact us now for more information about our data solutions.