LOOKINGGLASS

Reducing Third Party Risk Using Passive DNS Data

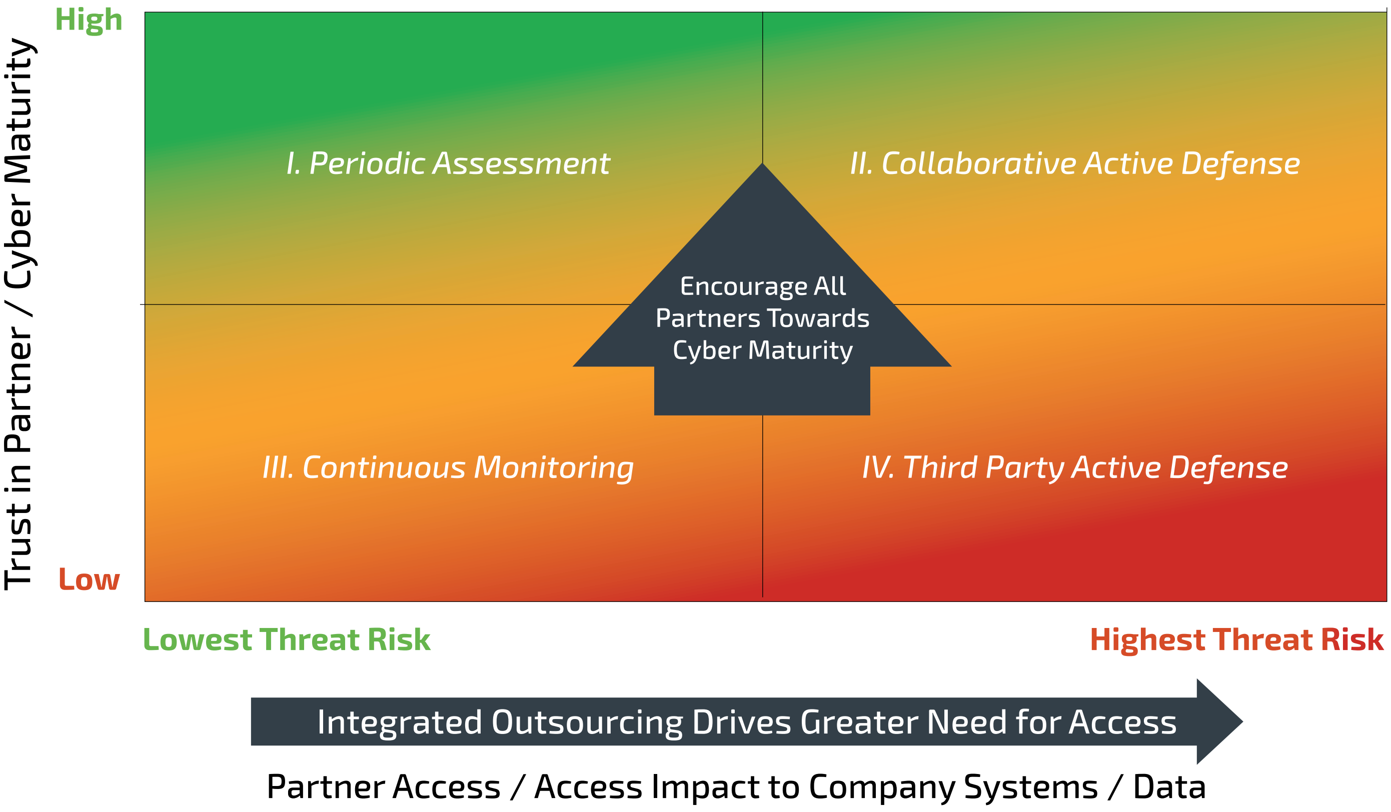
Executive Summary

Today, it's hard to think of an organization that isn't outsourcing at least one part of its business to a third party. As a result, business risk is directly influenced by the security posture of each of their partners, customers, supply chain, and other related third party businesses. It is this reliance on third parties that attackers take advantage of – exploiting vulnerabilities in common software or systems used in almost every modern organization.

Unfortunately, most organizations have a difficult enough time keeping their own systems and networks safe. Adding on the responsibility of third party cybersecurity – especially when they lack visibility into these external security postures – is a new complexity that many organizations aren't equipped to handle. While organizations have many options to evaluate non-cyber aspects of third party business practices (e.g. financial health, organizational leadership, and ability to work with customers), there is no easy way to assess the cybersecurity posture of these third party organizations. This often leaves organizations blind to cyber-vulnerabilities of product and service offerings, internal operations, and public-facing infrastructure.

The Third Party Risk Dilemma: Prioritizing Risk

Determining how to assess third parties for risk is a common barrier to organizations when starting this process. The framework below can help organizations prioritize their limited assessment resources. The first step is to assign each third party organization to one of the four quadrants shown below:


High
Trust in Partner / Cyber Maturity
Low
I. Periodic Assessment
II. Collaborative Active Defense
Encourage All Partners Towards Cyber Maturity
III. Continuous Monitoring
IV. Third Party Active Defense
Lowest Threat Risk
Highest Threat Risk
Integrated Outsourcing Drives Greater Need for Access
Partner Access / Access Impact to Company Systems / Data

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

Quadrants

Quadrant I: Periodic Assessment

Third parties with low access to your systems and highly mature approaches to cybersecurity pose the lowest threat risk. These organizations should be periodically assessed – more often than at vendor contract renewal – to ensure they continue to use sound cybersecurity processes and technologies.

Quadrant II: Collaborative Active Defense

Third parties with high access to your network and high maturity are likely to be your closest allies for enhancing third party cybersecurity. Consider regular sharing of suspicious activity, indicators of compromise, and threat intelligence to build each other's knowledge base and deepen the relationship. The focus here should be promoting a shift from perimeter-based defenses towards extended third party cybersecurity.

Quadrant III: Continuous Monitoring

Third parties that your organization does not trust to effectively manage cybersecurity on their own and that have low access to your systems or data. However, monitoring the third party's network from afar is a challenge.

Since these third parties are not trusted to follow proven cybersecurity practices, it is important to ensure they are appropriately using their access without introducing vulnerabilities to your data or systems. Whenever unsafe practices are identified, they should be protected against and brought to the third party's attention to encourage greater awareness of the need for cybersecurity.

Quadrant IV: Self-Active Defense

Posing the highest threat risk are third parties that require access to sensitive systems/data but have weak cybersecurity capabilities of their own.

This whitepaper focuses on those third parties that fall into Quadrant III: Continuous Monitoring. We will specifically highlight how that discipline can be assisted with passive DNS, which provides invaluable visibility into potential attack surfaces and enables organizations to determine not only where third parties are vulnerable and thus open to an attack, but also potential attack methods.

Before we dig into the use of passive DNS and its role in third party risk monitoring, we suggest you consider reading our whitepaper dicussing the background on broader aspects of 3PRM.

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

Passive DNS: *A Brief Overview*

DNS: A Faithful Diary of Online Activity:

Virtually everything that happens on the Internet begins with a Domain Name System (DNS) lookup. Passive DNS collects DNS queries and responses. Passive DNS operators index the DNS data they've collected so cybersecurity analysts can gain insight into online threats such as:

- Distributed Denial of Service (DDoS) Attacks
- Bot-related Activity
- Phishing
- Brand and Trademark Infringement
- Covert Data Exfiltration

*I Want It **ALL**...*

One challenge cybersecurity analysts face is the ease with which bad actors can create resilient infrastructure for their criminal activity. Bad guys don't rely on just one domain or one IP address; instead, they'll often use hundreds or even thousands of names and IPs. That way, if cyber defenders do stumble across one or two of those domains or IP addresses and manage to successfully get them taken down, the bad guys may not even notice since there will still be hundreds or thousands of other domains or IPs that are not known by the good guys.

With passive DNS, a cybersecurity analyst can leverage a starting "clue" (such as a suspicious domain name seen in a phishing email or a suspicious IP address found in a firewall log) and find virtually ALL of the related domains and IP addresses associated with the original indicator; thereby increasing the likelihood that takedowns and other remediations will be complete and impactful.

Historical DNS

Regular "real-time" DNS tells you how a domain name resolves today. Passive DNS, such as Farsight DNSDB®, can act as a "time machine" and let you "go back in time" to see what DNS looked like at an earlier time, in some cases up to 10 years in the past.

Using passive DNS, you can either see the full history of a domain name or focus on a particular period of time, such as during an incident or immediately before/after a change was made to a site's DNS configuration. Time-limiting the returned results is referred to as "time fencing."

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

We're All Explorers

Passive DNS can also be used to find all the hosts living beneath a delegation point, or all the hosts known to have used a particular IP address range, or all the hosts that share a common name server or mail server. These are very powerful "pivots," allowing an analyst to connect the dots from a domain name to associated IPs to new domain names to new associated IPs, etc.

Avoiding Collateral Damage

We've all seen reports in industry media of takedowns gone wrong – you know, a bad guy gets successfully knocked offline, but in the process of taking that bad guy down, numerous innocent parties were harmed – "*Oops!*"

Passive DNS can help prevent security teams from "shooting themselves in the foot" by providing the ability to understand potential collateral damage to third party sites on an IP or domain, thereby ensuring that strategically important takedown efforts don't turn into public relation debacles.

Continuous Monitoring:
A Passive Way to Reduce Risk

As threats to an organization evolve in terms of scope and sophistication, strategic and tactical responses to threats require historical context and timely actionable intelligence. A weekly or monthly risk report can prove useful in some scenarios, but this is only a snapshot of third party risk. As we see it, there are three issues that arise from relying on a risk report: 1) If it is issued hours before the disclosure of a critical, remotely exploitable hole in a common open source platform, that report will be unavoidably out-of-date by the time it is read, and if it is only issued as (*or after!*) an attack occurs, it will be too little, too late. 2) Security teams are constantly bombarded with notifications. If the notification isn't timely and actionable, it will be ignored and then exploited later. 3) The lead time on notifications needs to be more than just hours; teams need days or even weeks. Like Goldilocks and the Three Bears, we need timely actionable intelligence, neither too early nor too late.

That's why organizations require continuous monitoring of their own cyber infrastructure, and the cyber infrastructure of third parties they work with, including any relevant domains and IP addresses. That infrastructure needs to be carefully monitored for any indicators of compromise, infection, or illicit use that may increase organizational risk.

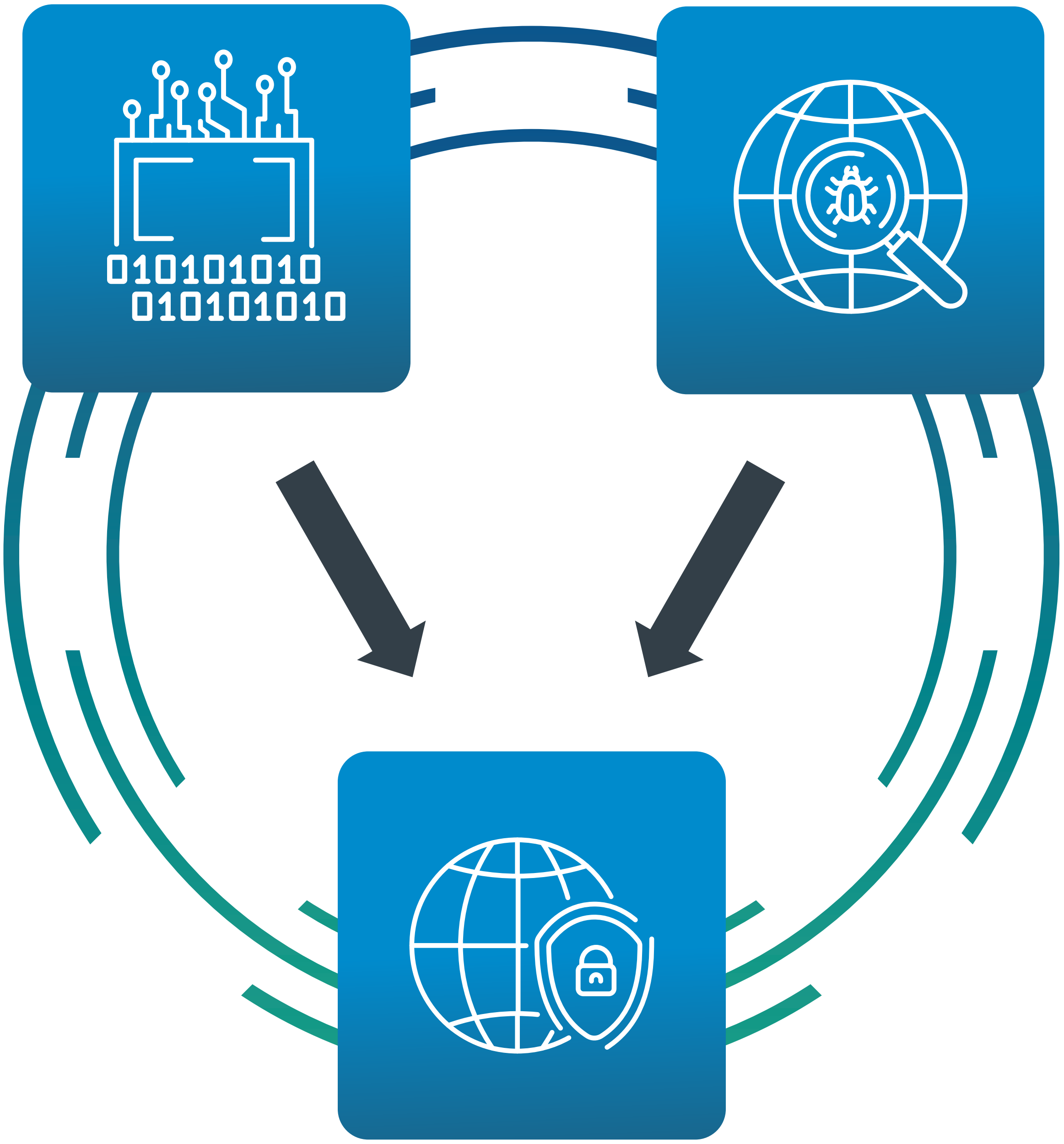
© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

Continuous Monitoring (cont.):

To begin continuous monitoring, there are related aspects to understanding the attack surface that organizations need to monitor:

Connected Graph of ***Internet Intelligence***
(BGP, ASN, CIDR, Ownership)

Connected Graph of ***Threat Intelligence***
(Cyber, OSINT, Darknet, Actors, etc.)



Connect Internet + Threat Intelligence with
Machine / Human ***Insight***

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

Understanding the Intelligence Driven Attack Surface

Step 1: Establishing a baseline of the Company's Attack Surface

This step allows an organization to establish a baseline understanding of its own attack surface and the attack surface of any related third parties.

First, identify the organization's Internet points of presence, and those of all related organizations. This critical intelligence must include how those networks are connected and how traffic gets routed to them. This is one of the key aspects of using passive DNS as part of the foot printing process. It allows defenders to gather virtually all relevant networks (fully-qualified domain name [FQDNs] and public IPs) associated with the organization and any related businesses.

As an additional step, organizations should consider monitoring Border Gateway Protocol (BGP) for route changes as well as domain and IP address ownership information to detect either malicious reconfiguration or hijacking attempts.

Step 2: Enrich the Attack Surface Understanding with Threat Intelligence

This step builds upon the baseline established in Step 1 by considering relevant threat intelligence across the footprint established.

There are many sources of threat intelligence that could be relevant to an organization's attack surface. Intelligence selection and refinement is a key part of maximizing the benefits to security operations. Organizations should consider choosing intelligence that can provide insight to the behaviors associated with malicious activities and any indicators (network, social, host) that can give insight into active attacks.

Structured Threat Intelligence –

- Malware hosting/distribution infrastructure, particularly for malware that has been crafted to attack an organization's specific systems (or infrastructure associated with actors known to attack organizations in your market segment)
- Command-and-Control activity that may be detected in any phase of the kill-chain
- Malicious scanning behavior
- Spamming or phishing observed or as provided by third party reports that would target users or systems within your organization
- Asset use within organizational networks or connected networks that may be attributed to misuse or activities deemed outside of acceptable business practices
- Emergent vulnerabilities specifically relevant to particular organizational systems
- Malware network parameters and malicious certificate information that can be used to detect such behavior

Unstructured Threat Intelligence –

- Compromised account credentials of any organization admins and known third parties that are responsible for organization maintenance
- Reported breaches of third parties, especially those third parties that are responsible for some aspect or use of systems within your own organization
- Vulnerabilities found/announced in a third party's product that could be used to attack the organization environment
- Suspicious domain registrations & spear phishing exposure that would result in attacks being launched against organization infrastructure identified during the Internet intelligence phase

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

Step 3: Connecting the Dots with Human Insight

Understanding the attack surface collected during Steps 1 and 2 alone may not yield results as powerful as what an effective machine + human intelligence combination can provide.

Machine algorithms can be effective at processing large volumes of data and well-known patterns that can be easily computed without ambiguity. In some cases, machine algorithms can learn to improve their function provided sufficient data (training data) and appropriate learning algorithms are applied with suitable guidance from skilled experts.

However, human insight is often the key to providing context that the machine cannot (data gaps). For example, the human element can identify multi-factor context and relationships across unrelated network behaviors that without substantial effort, relationships that machine-learning systems could not identify with enough accuracy. For organizational protection, having human expertise complement machine driven analysis is a vital check-and-balance for both detection and response, especially when making automated decisions to mitigate threats driven by intelligence.

Step 4: Enable Continuous Monitoring

Continuous monitoring and assessments of third parties and supply chain organizations should be built into your security program after completing steps 1-3. This will help bring awareness and active response to weak spots in your defensive perimeter.

Here are some important questions to consider when monitoring organizations continuously:

1. Do you have the capability to detect new or active application vulnerabilities in your own organization as well as in third parties?

2. If a third party could be used to indirectly attack your organization, how will you detect that risk? What are the detection and response strategies for such an attack and how do they differ from an internal or external adversary?

3. If a third party is compromised and involved in a data breach, are you able to detect that? Do you know what data has been leaked from the third party?

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

Putting it Together:

Passive DNS + Continuous Monitoring for Third Party Breaches

On its own, continuous monitoring provides a wealth of knowledge into the security of third party attack surfaces. Organizations can be alerted to any number of risk indicators that could ultimately lead to a breach, including malware hosting or malware distribution from a monitored organization's network and infection by computer viruses or botnet activity. This can only be accomplished with a tool that continuously monitors for:

- Network Attack Surface
- System Compromises & Infections
- Account Compromises
- External Facing Vulnerabilities
- Domain & Spear Phishing Risk
- Intelligence Indications & Warnings

Passive DNS is able to monitor for these and more because it provides visibility of the changing Internet. Using this non-judgement, observational data, organizations can gain greater visibility of its online infrastructure to expose common infrastructure problems such as misconfigurations.

In addition to asset monitoring, Passive DNS is invaluable to advancing attack investigations. When an organization identifies a suspicious domain name or IP address, Passive DNS can be used to uncover other DNS-related assets such as a shared name server or second- or third-level domains. Since bad actors can move between DNS assets such as domain names, the ability of Passive DNS to provide a timestamp for these changes is critical to identify ongoing malicious campaigns and expose specific attack patterns that can help uncover additional attacks against an organization.

Farsight Security® intentionally collects passive DNS data in a way that does not expose user personally identifiable information (PII), all while providing insight into an organization's publicly exposed systems and network infrastructure. For example, it provides information on web servers, mail servers, and name servers and often a whole lot more – and that's potentially important because the first thing a potential attacker wants – and the first thing a defender also needs – is a list of potentially vulnerable targets.

Sometimes the number of publicly-known systems can be surprising to a site's system and network administrators. For example, some enterprise, government or military sites may underestimate the extent to which the world knows about their systems and thus the extent of their potential exposure to targeted or indiscriminate automated attack tools.

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

Case Study:

pDNS & Continuous Monitoring in Action

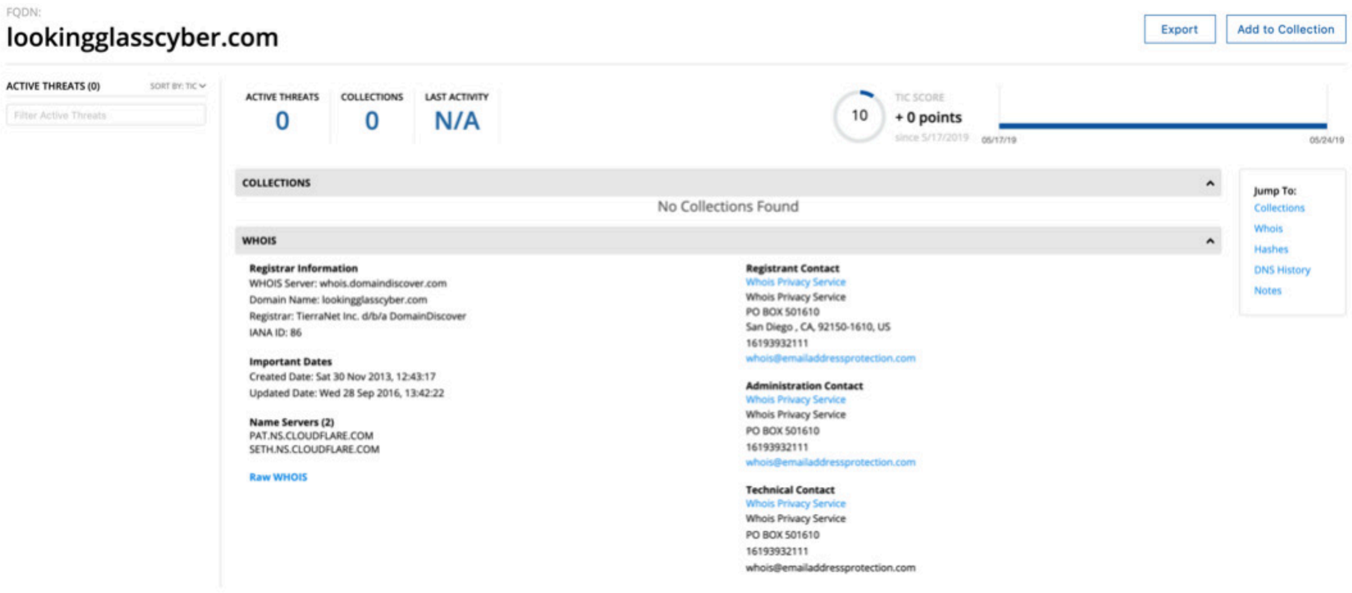
Using Farsight passive DNS in concert with scoutPRIME® provides enhanced attack surface monitoring features including initial identification and verification and monitoring for DNS changes that may impact the organization's security posture. Below we've laid out an example of...

#1: Attack Surface Identification and Verification

When initially starting to monitor organizational risk, it is critical to ensure that all public Internet-facing points of presence owned by the organization are identified including 1st, 2nd and 3rd level domains that are exposed via DNS on the Internet.

Within scoutPRIME, a user can search based on common names or words within an organization's primary entity name to find all domains matching on those names or words.

Example 1: Search results for LookingGlassCyber.com covering WhoIs, any active threat intelligence



FQDN:
lookingglasscyber.com

ACTIVE THREATS 0 | COLLECTIONS 0 | LAST ACTIVITY N/A

10 + 0 points since 5/17/2019

No Collections Found

Registrar Information
WHOIS Server: whois.domaindiscover.com
Domain Name: lookingglasscyber.com
Registrar: TierraNet Inc. d/b/a DomainDiscover
IANA ID: 86

Important Dates
Created Date: Sat 30 Nov 2013, 12:43:17
Updated Date: Wed 28 Sep 2016, 13:42:22

Name Servers (2)
PAT.NS.CLOUDFLARE.COM
SETH.NS.CLOUDFLARE.COM

Raw WHOIS

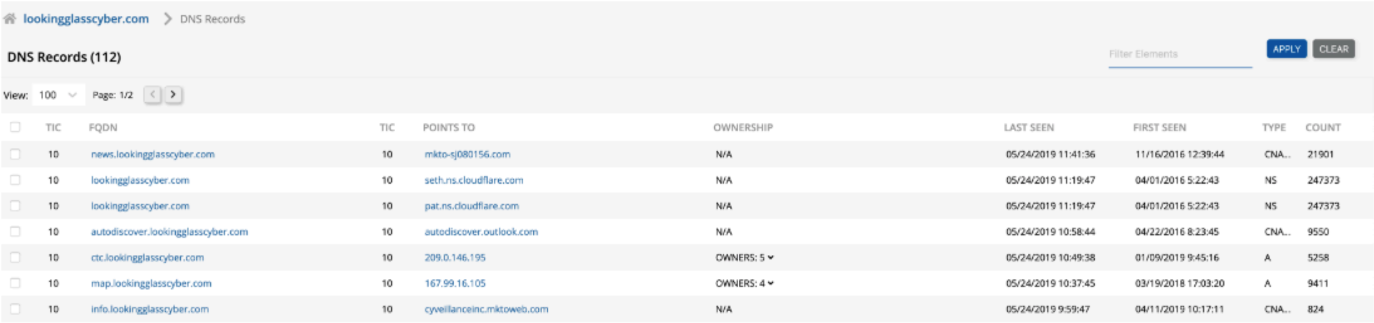
Registrant Contact
Whois Privacy Service
Whois Privacy Service
PO BOX 501610
San Diego , CA, 92150-1610, US
16193932111
whois@emailaddressprotection.com

Administration Contact
Whois Privacy Service
Whois Privacy Service
PO BOX 501610
16193932111
whois@emailaddressprotection.com

Technical Contact
Whois Privacy Service
Whois Privacy Service
PO BOX 501610
16193932111
whois@emailaddressprotection.com

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

Example 2: Select Passive PDNS Results for LookingGlassCyber.com



lookingglasscyber.com > DNS Records

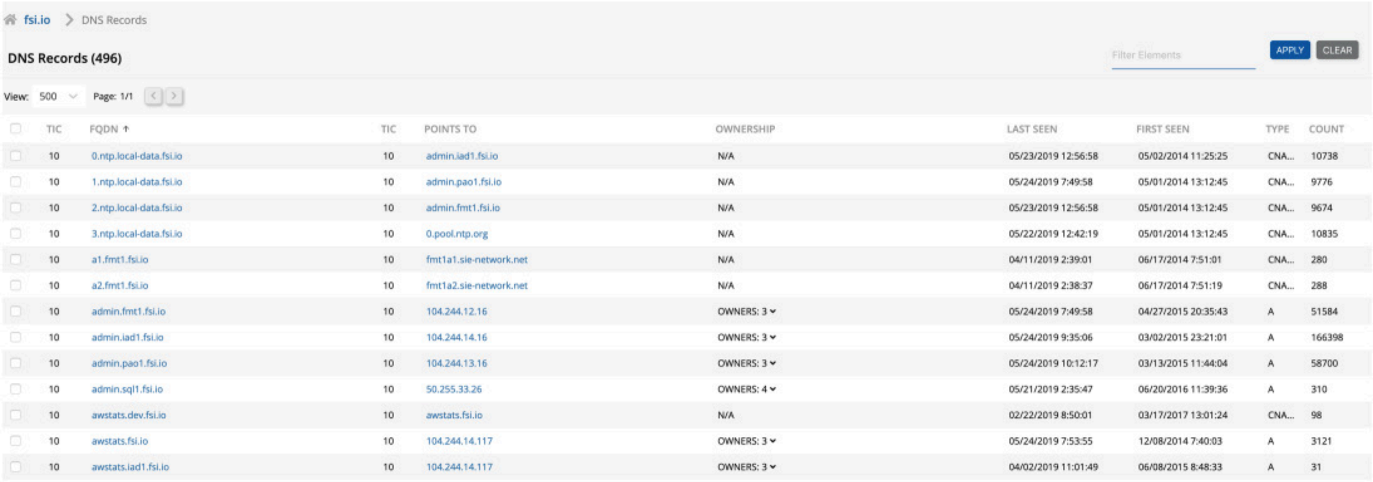
DNS Records (112)

View: 100 Page: 1/2

□	TIC	FQDN	TIC	POINTS TO	OWNERSHIP	LAST SEEN	FIRST SEEN	TYPE	COUNT
□	10	news.lookingglasscyber.com	10	mkto-sj080156.com	N/A	05/24/2019 11:41:36	11/16/2016 12:39:44	CNA...	21901
□	10	lookingglasscyber.com	10	seth.ns.cloudflare.com	N/A	05/24/2019 11:19:47	04/01/2016 5:22:43	NS	247373
□	10	lookingglasscyber.com	10	pat.ns.cloudflare.com	N/A	05/24/2019 11:19:47	04/01/2016 5:22:43	NS	247373
□	10	autodiscover.lookingglasscyber.com	10	autodiscover.outlook.com	N/A	05/24/2019 10:58:44	04/22/2016 8:23:45	CNA...	9550
□	10	ctc.lookingglasscyber.com	10	209.0.146.195	OWNERS: 5	05/24/2019 10:49:38	01/09/2019 9:45:16	A	5258
□	10	map.lookingglasscyber.com	10	167.99.16.105	OWNERS: 4	05/24/2019 10:37:45	03/19/2018 17:03:20	A	9411
□	10	info.lookingglasscyber.com	10	cyveillanceinc.mktoweb.com	N/A	05/24/2019 9:59:47	04/11/2019 10:17:11	CNA...	824

For each domain returned from Passive DNS, an additional step can be performed where the DNS records associated with that entity can be inspected to find other 2nd or 3rd level domains. This may highlight additional domains or IP networks that should be added to the collection for monitoring.

Example 3: Select Passive DNS Results for fsi.io and associated sub-domains



fsi.io > DNS Records

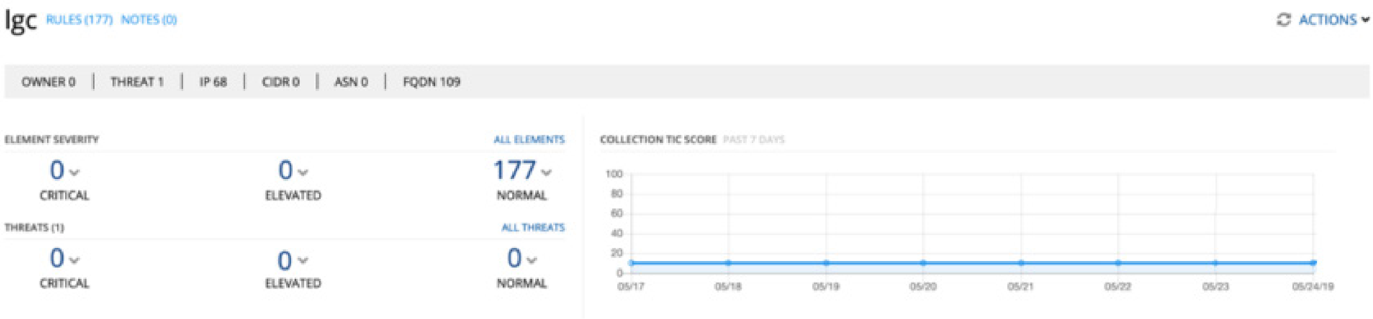
DNS Records (496)

View: 500 Page: 1/1

□	TIC	FQDN ↑	TIC	POINTS TO	OWNERSHIP	LAST SEEN	FIRST SEEN	TYPE	COUNT
□	10	0.ntp.local-data.fsi.io	10	admin.iad1.fsi.io	N/A	05/23/2019 12:56:58	05/02/2014 11:25:25	CNA...	10738
□	10	1.ntp.local-data.fsi.io	10	admin.pao1.fsi.io	N/A	05/24/2019 7:49:58	05/01/2014 13:12:45	CNA...	9776
□	10	2.ntp.local-data.fsi.io	10	admin.fmt1.fsi.io	N/A	05/23/2019 12:56:58	05/01/2014 13:12:45	CNA...	9674
□	10	3.ntp.local-data.fsi.io	10	0.pool.ntp.org	N/A	05/22/2019 12:42:19	05/01/2014 13:12:45	CNA...	10835
□	10	a1.fmt1.fsi.io	10	fmt1a1.sie-network.net	N/A	04/11/2019 2:39:01	06/17/2014 7:51:01	CNA...	280
□	10	a2.fmt1.fsi.io	10	fmt1a2.sie-network.net	N/A	04/11/2019 2:38:37	06/17/2014 7:51:19	CNA...	288
□	10	admin.fmt1.fsi.io	10	104.244.12.16	OWNERS: 3	05/24/2019 7:49:58	04/27/2015 20:35:43	A	51584
□	10	admin.iad1.fsi.io	10	104.244.14.16	OWNERS: 3	05/24/2019 9:35:06	03/02/2015 23:21:01	A	166398
□	10	admin.pao1.fsi.io	10	104.244.13.16	OWNERS: 3	05/24/2019 10:12:17	03/13/2015 11:44:04	A	58700
□	10	admin.sql1.fsi.io	10	50.255.33.26	OWNERS: 4	05/21/2019 2:35:47	06/20/2016 11:39:36	A	310
□	10	awstats.dev.fsi.io	10	awstats.fsi.io	N/A	02/22/2019 8:50:01	03/17/2017 13:01:24	CNA...	98
□	10	awstats.fsi.io	10	104.244.14.117	OWNERS: 3	05/24/2019 7:53:55	12/08/2014 7:40:03	A	3121
□	10	awstats.iad1.fsi.io	10	104.244.14.117	OWNERS: 3	04/02/2019 11:01:49	06/08/2015 8:48:33	A	31

Upon reviewing these domains, a user can select which domains belong to the organization based on WhoIs records or other knowledge of the entity and add those domains to a scoutPRIME collection that will be used to continuously monitor those domains.

Example 4: Collection 'lgc' summary for LGC organization



lgc RULES (177) NOTES (0)

OWNER 0 | THREAT 1 | IP 68 | CIDR 0 | ASN 0 | FQDN 109

ELEMENT SEVERITY

0 CRITICAL | 0 ELEVATED | 177 NORMAL

THREATS (1)

0 CRITICAL | 0 ELEVATED | 0 NORMAL

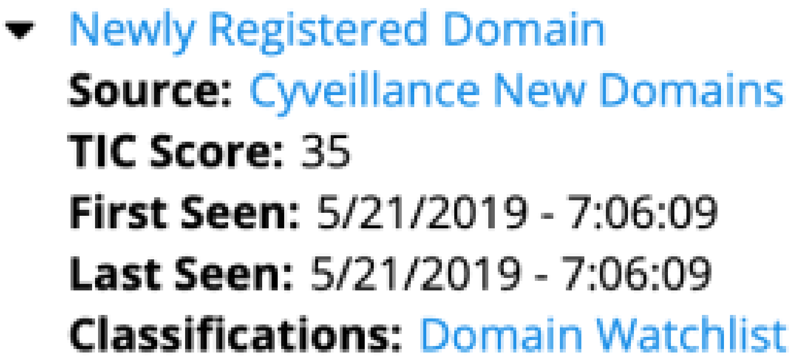
© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

#2: Attack Surface DNS Changes

Once an organization has established the footprint to monitor for their organization and any associated third parties, the next step is to watch for any changes to that footprint that may be indicative of malicious activities.

Changes to DNS for your organization or third parties can be the result of new domains being added or existing domains being pointed at a different destination or deleted. For example, if a new domain is registered but not yet used, then LookingGlass would show that as part of the Newly Registered Domain feed within scoutPRIME as well as the Whois records.

Example 5: Newly Registered Domain Intelligence



▾ Newly Registered Domain

Source: Cyveillance New Domains

TIC Score: 35

First Seen: 5/21/2019 - 7:06:09

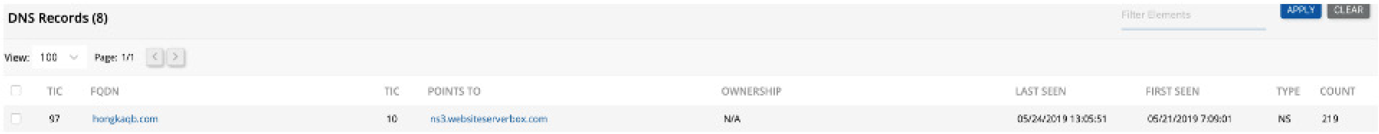
Last Seen: 5/21/2019 - 7:06:09

Classifications: Domain Watchlist

With third party continuous monitoring, organizations should pay attention to newly registered domains for any evidence of malicious activities that may lead to malicious activities including phishing attacks.

If this newly registered domain has been referenced or used within DNS then passive DNS can provide context on when that domain was first seen, last seen and associated DNS meta-data including usage counts.

Example 6: Farsight Passive DNS Entry



DNS Records (8)

□	TIC	FQDN	TIC	POINTS TO	OWNERSHIP	LAST SEEN	FIRST SEEN	TYPE	COUNT
□	97	hongkaqb.com	10	ns3.websiteserverbox.com	N/A	05/24/2019 13:05:51	05/21/2019 7:09:01	NS	219

Understanding the associated record type information and usage counts can help identify DNS entries and their legitimacy.

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

Example 7: Rapid DNS Changes

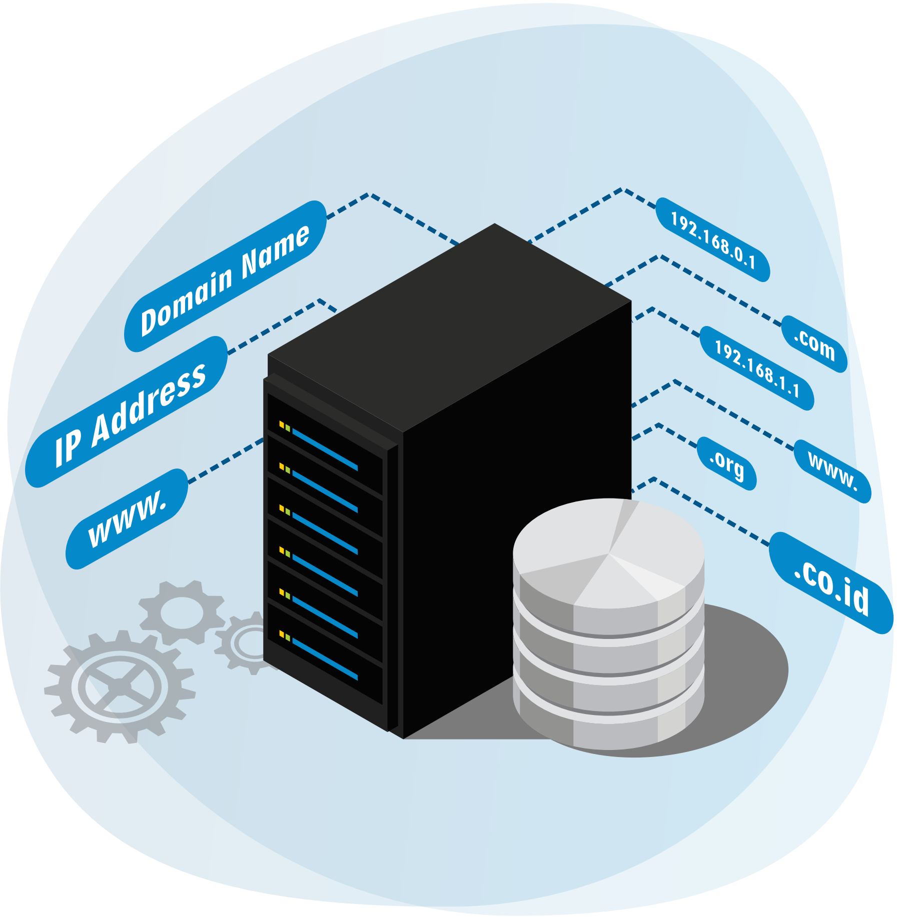
A domain name may repeatedly change IP addresses. Rapidly changing IP addresses may be a sign that a domain name...

- Is using a content distribution network (such as Akamai's CDN). When this is the case, the domain name will normally have Akamai (or another CDN network's domain names) show up as part of its passive DNS history. When a CDN is involved, changes in DNS mappings are usually a sign that the CDN is using diverse hosts to more efficiently serve requests for content. The changes in that case are perfectly normal and not a cause for concern.

- Is being hosted in dynamic IP address space (such as an ISP's residential customer address space) and is using a dynamic DNS service.[1] In this case, the PTR records for the IPs the domain uses will normally have obviously dynamic names and will usually all come from the same geographical region.

- Has been hijacked (this is often typified by a strictly domestic US domain suddenly popping up as being hosted in locations such as Eastern Europe, Asia, or Latin America).[2]

- Is hosted on so-called "fast-flux hosting."[3]



[1] https://en.wikipedia.org/wiki/Dynamic_DNS
[2] https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-ans-hijacking-attacks/
[3] https://icannwiki.org/Fast_Flux

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

Third Party Risk Continuous Monitoring Summary

Your bottom line relies on the cybersecurity of your third parties just as much as that of your own organization. It is no longer possible to discount the risk brought on from contractors and other third party providers, and many times organizations have limited practical ability to audit or insist on different security practices. With growing third party breach legislation, organizations can no longer sit idle and hope that their third parties are employing proper security practices. Third party risk monitoring – including the use of passive DNS Data – gives organizations a holistic view of their attack surface and should be a core component of every organization's information security program, regardless of industry.

Organizations will be able to monitor what's going on as it happens, capturing both the outward security posture of that organization and less easily measured indicators, such as the security of hosted and cloud-based IT assets and data. It's not enough to receive a one-time scorecard with minimal analysis or actionable intelligence. Passive DNS enhances the early detection provided through continuous monitoring by contextualizing log file data, helping analysts make sense out of the domains and raw IPs you might otherwise find yourself struggling to understand and leverage.

Malicious/Scanning Behavior
Malware
Virus
IOC
Spam
Emergent Vulnerabilities
Breach
Questionable Assets
Phishing
Suspicious Domain Registrations

If you are interested in learning more about
LookingGlass' Third party Risk Monitoring™ Service powered by scoutPRIME,
contact LookingGlass at **https://www.lookingglasscyber.com/about-us/contact-us/**.

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

About LookingGlass®

LookingGlass is the leader in intelligence-driven risk management, offering the industry's most comprehensive and integrated cybersecurity solutions to the market. Our deep portfolio of flexible tools and technologies, supported by a global team of analysts, makes security seamless for enterprises and governments worldwide. We deliver relevant and tailored threat intelligence and response, making LookingGlass an insightful, proactive partner to organizations of all sizes. When intelligence informs product development, you get innovative solutions. Learn more at **http://www.LookingGlassCyber.com**.

LookingGlass Third Party Risk Monitoring is a cost-effective, risk-focused approach to managing and mitigating third party cyber risk. Our continuous monitoring service includes human-review of all flagged incidents, as well as a point-in-time vendor risk report. Built-in reporting allows proper collection and easy metric delivery to organizational leaders, promoting visibility across the organization's security posture.

WHAT WE MONITOR

Structured Data

- Malware hosting/distribution
- Virus/Botnet infection
- Command-and-Control (C2) activity
- Malicious/Scanning behavior
- Observed Spam
- Questionable Asset Use
- Phishing activity
- Emergent vulnerabilities
- Port and cert information

Unstructured Data

- Reported breach of your vendor
- Suspicious domain registrations & spear phishing exposure

LOOKINGGLASS

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.

About Farsight Security®, Inc.

Farsight Security, Inc. is the world's largest provider of historical and real-time DNS intelligence solutions. We enable security teams to qualify, enrich and correlate all sources of threat data and ultimately save time when it is most critical - during an attack or investigation. Our solutions provide enterprise, government and security industry personnel and platforms with unmatched global visibility, context and response. Farsight Security is headquartered in San Mateo, California, USA. Learn more about how we can empower your threat platform and security team with Farsight Security passive DNS solutions at **https://www.farsightsecurity.com** or follow us on Twitter: **@FarsightSecInc**.

ABOUT DNSDB®

Farsight DNSDB, our flagship historical passive DNS solution, can help organizations assess the current state – and the history – of its infrastructure assets. It can answer questions that other security tools are unable to including:

- Where did this domain name point to in the past?
- What domain names are hosted by a given nameserver?
- What domain names point into a given IP network?
- What subdomains exist below a certain domain name?

Farsight DNSDB Availability

Farsight DNSDB is available as a subscription service. You can access the API key using your preferred TIP, SOAR or SIEM platform, or via Google Chrome or Mozilla Firefox browsers using our DNSDB Scout UI.

DNSDB Free API Key

Get a trial DNSDB API Key and use it in any of your preferred platform(s) for 30-days free,
100 Queries/day. Learn more at **https://www.farsightsecurity.com/trial-api/.**

FARSIGHT SECURITY

© 2019 LookingGlass Cyber Solutions, Inc. All rights reserved.