The Internet Immunity Project

January 5, 2025

Overview

This document describes the Global Cyber Alliance's (GCA) Internet Immunity Project. Its intended audience is prospective partners, consumers, independent auditors, and other interested parties.

The GCA is a not-for-profit organization dedicated to leveraging the collective strengths of stakeholders, global leaders, and cyber experts in order to improve the safety and security of our connected cyber world by identifying and eliminating global systemic cyber risks, creating solutions or leveraging existing solutions, and measuring the results.

Our partner in the Internet Immunity Project, **Packet Clearing House (PCH),** is the international organization responsible for providing operational support and security to critical internet infrastructure, including internet exchange points and the core of the domain name system (DNS).

Background and description

Spammers, spoofers, producers of malware, and other malicious actors are registering malicious domains faster than legitimate users and security personnel can take them down. As a case in point, the Conficker worm of 2008 registered 500 malicious domains daily under several generic top-level domains (TLDs) such as the familiar ".com," ".org," and ".net." When security experts created a method to pre-emptively identify and block the malicious domains, the Conficker authors responded by reinfecting their bots with an updated worm that created *50,000* new malicious domains per day; moreover, these were registered under 110 different country-code TLDs (such as ".uk," ".tw," and ".de") in addition to the generic TLDs. To meet the expanded threat, the anti-Conficker team had to quickly arrange agreements with a mix of private and public institutions, some with national government oversight and many without, to share technical plans and data as well as strategic plans and calendars.

As cyber crime continues to rise across the globe, organizations need new ways to protect their networks from criminals. One of the most prevalent vectors for compromising an organization's network is the human beings clicking away in browsers and inboxes, allowing attackers to penetrate the network through phishing attacks and links to malware-laced domains.

DNS-based filtering is a method that can easily protect an organization's network and its endpoints by leveraging the role of DNS in the network. The GCA's Internet Immunity Project addresses the risk tied to phishing attacks and malware by using the security industry's highest-quality threat intelligence (TI) feeds to block the resolution of known malicious domains. In this way, the Internet Immunity Project can provide an additional, easy-to-use layer of protection from the latest threats identified by the security industry, requiring only a simple change to an organization's DNS servers.

The Internet Immunity Project's primary goal is to provide a high level of blocking protection in a robust and reliable global DNS infrastructure. With GCA building the platform and PCH building the infrastructure, we have created a secure and robust service that can be used by anyone, anywhere. We are able to do this while providing privacy and security to the users of this system by not capturing personally identifying information (PII), by blocking access to known malicious domains, and by enforcing DNSSEC for domains that have it configured. We believe that by building this platform and

enabling the security industry to operationalize its TI, we can provide a basic level of protection to the internet population and help mitigate global cyber risk.

Scope

The goal of this solution is a scalable, secure, performant, and open platform that the larger security community can leverage to operationalize the TI that it collects, analyzes, and produces in the course of its normal activities. This platform will use that TI to block/filter queries that end users are making on the open DNS recursive infrastructure.

This effort is focused on providing the end users of this platform the best protection possible from malware, exploit sites, and other known malicious infrastructure that our security vendor partners (antivirus companies, MSSPs, TI providers, etc.) provide us. At the same time, we do not require them to compromise their privacy provisions and we do not commercialize the data collected through the platform.

High-level requirements

- A community TI platform to generate lists of bad domains
- An open, recursive DNS infrastructure to be built and maintained by GCA that implements “response policy zones” (RPZs) to allow blocking of online threats through DNS
- Metrics for the impact of the GCA-built DNS infrastructure on systemic cyber risk
- In later phases, an open-source TI platform to be built by GCA that collects, analyzes, and generates RPZ policies for organizations, enterprises, and ISPs to consume

Deliverables

- A TI platform based on community input
- A global, open, and free recursive DNS infrastructure
- Anonymized data showing the prevalence of and requests to malicious domains to enable generation of data on risks mitigated and systemic risk generally

Customers and customer costs

- **Organizations and individuals** can reduce risk associated with cyber crime by adding a more robust defense to their networks.
- **Appliance manufacturers** can ensure their IoT products aren’t putting customers at risk through unforeseen vulnerabilities.
- **TI providers** can collaborate with a global community of peers to act on cyber crime and malware, and receive feedback data on DNS requests that have been blocked due to the RPZs.

- **Security teams and operation centers** can reduce the number of security alerts generated by their security devices, allowing them to focus on the most important and critical threats.

The GCA Internet Immunity service is **free of charge** to its users. It will remain freely available to anyone wishing to use it.

In terms of level of effort, setting up DNS filtering requires a simple configuration change. Most organizations or individual users can update their systems in minutes by changing DNS settings in the central dynamic host configuration protocol (DHCP) server, which will update all clients in a few minutes with no action needed on the end devices.

Partners

GCA partners include companies that have TI to share, that wish to use the platform that GCA is building, and that contribute as infrastructure partners in building the service. As such, our partners may provide data/information, technology, expertise, funding, and anything else that is necessary to accomplish a mission/project. Partners can also volunteer to be a test site.

GCA partners are kept informed about the progress of our projects and offered opportunities as they arise.

Those who are interested in becoming GCA partners should contact GCA via our public email: info@globalcyberalliance.org.

Trials

The service is currently being tested with several pilot partners in the United States and Western Europe, with multiple anycast systems active across each region. One of these partners, the State of West Virginia, provided this feedback:

> *"Our endpoint malware/virus tickets were cut by just over half, and our Wildfire environment saw about a 30% reduction is malicious files. Those are staggering numbers."*
>
> *—John M. Moore, Cyber Security Operations Manager for the State of West Virginia*

For a description of a trial of RPZs that was conducted independently of the GCA, please see Trial Project: Technical University of Denmark in this document.

Technical Overview

This section gives a basic explanation of the DNS and how the GCA Internet Immunity system works.

The domain name system (DNS)

The DNS is the comprehensive database of domain names and their corresponding internet protocol (IP) addresses. It was created so computers could communicate with each other in their language of numbers while their human users could navigate computer networks in theirs. For instance, while computers resolve "198.41.0.4" and "202.12.27.33," humans can use descriptive, memorable names like "google.com" and "globalcyberalliance.org."

Abuse of the DNS

While legitimate users create websites and load them with news, opinions, marketing content, and cat videos, cyber criminals create websites they load with viruses and worms. The most common abuses are spam emails containing links that execute malware, or websites with similar malicious links. Users have only to click on those links, and the DNS will handily translate them into IP addresses where computers can go to meet their doom.

Traditional protection against DNS abuse

From its inception, the DNS has been neutral, resolving malicious domains along with the good and leaving it to registrars and the security mechanisms on personal computers and various network elements to prevent users from reaching dangerous sites.

There are problems with this type of protection. It can be expensive. It can be slow; a malicious domain can be created in far less time than is required to take it down. It can be thwarted by identity theft or by registrars' privacy provisions. It can rely on IP lookups that alert cyber criminals to investigatory activity while revealing information about the investigator. It can be time-consuming, requiring network administrators to configure proxies, ports, and firewalls. It may require restarting a name server every time there's an update to a blacklist or TI source. It presents a financial incentive to registrars to churn malicious domains, since cyber criminals respond to takedowns of their domains by buying new ones. It can allow slow, insidious, or distributed attacks to go undetected until the moment of detonation.

A new type of protection: Response policy zones

The GCA Internet Immunity service is different because it places protection against DNS abuse right on the DNS itself.

It starts with TI feeds provided by trusted sources such as Ransomware and AlienVault. GCA subscribes to these feeds and passes them to BIND, the most widely used (and open-source) DNS software. End users then configure their own (non-caching) DNS servers, which, thus configured, will respond to queries against malicious domain names with an answer other than a straightforward resolution. These answers are specified in "response policy zones" (RPZs) that are also part of the BIND configuration.

For instance, when a user opens an email and clicks a benign-appearing link that leads to a blacklisted domain, an RPZ can respond by

- Resolving the IP address to the internet root, leading to a “name not found” error on the user’s end
- Resolving the IP address to the TLD (also called an “NXDOMAIN” response), which the user experiences as no answer; **this is the response in the GCA Internet Immunity service**
- Handling the query according to a local override, such as a whitelist or a redirect within an organization’s network to an informative, branded page known as a “walled garden” that can also log the query
- Exempting the query from any of the above policies and passing the true answer through (normal resolution)

Malicious domains can be added to the TI feeds literally as they are discovered. The feeds in turn are added to GCA’s blacklist and propagated throughout the DNS via 24/7 incremental transfers of the RPZs. (The transfers are expedited and protected by DNS’s notification and transaction-signature mechanisms.) A malicious domain can be blocked on multiple continents shortly after being identified.

To return to the Conficker incident, the 50,000 malicious domains that were being registered daily all originated from name servers that hosted no nonmalicious domains. Through the use of RPZs, the security team was able to block the IP addresses of the malicious name servers, instead of attempting 50,000 blocks a day on a domain-by-domain basis.

Risk Mitigation

As with any system involving human judgment and human operation, the GCA Internet Immunity service contains risks, such as stresses on the infrastructure, inadvertent blacklisting of legitimate domains, and risks associated with the presence of sensitive user information. GCA has taken measures to mitigate and in some cases eliminate these risks.

As the project is refined and more capacity added to the infrastructure, additional operation centers will be added globally to provide one of the broadest geographic and network-topology overlays, providing maximum performance and fault resiliency. PCH as the operator of the system is well-suited for this purpose, with approximately 140 locations worldwide where it operates DNS authoritative services for over 300 TLDs and provides network and systems infrastructure for multiple DNS root providers.

The GCA Internet Immunity service also has a whitelisting process to remove domains from the blacklist that may have been inadvertently added; once a domain has been determined to be legitimate, the fix can be propagated within hours.

The infrastructure and the whitelisting process are part of a transparent and auditable design that protects the privacy and independence of the service's users. We invite audits by respected, reputable organizations and will work with them to develop an audit path that satisfies their requirements.

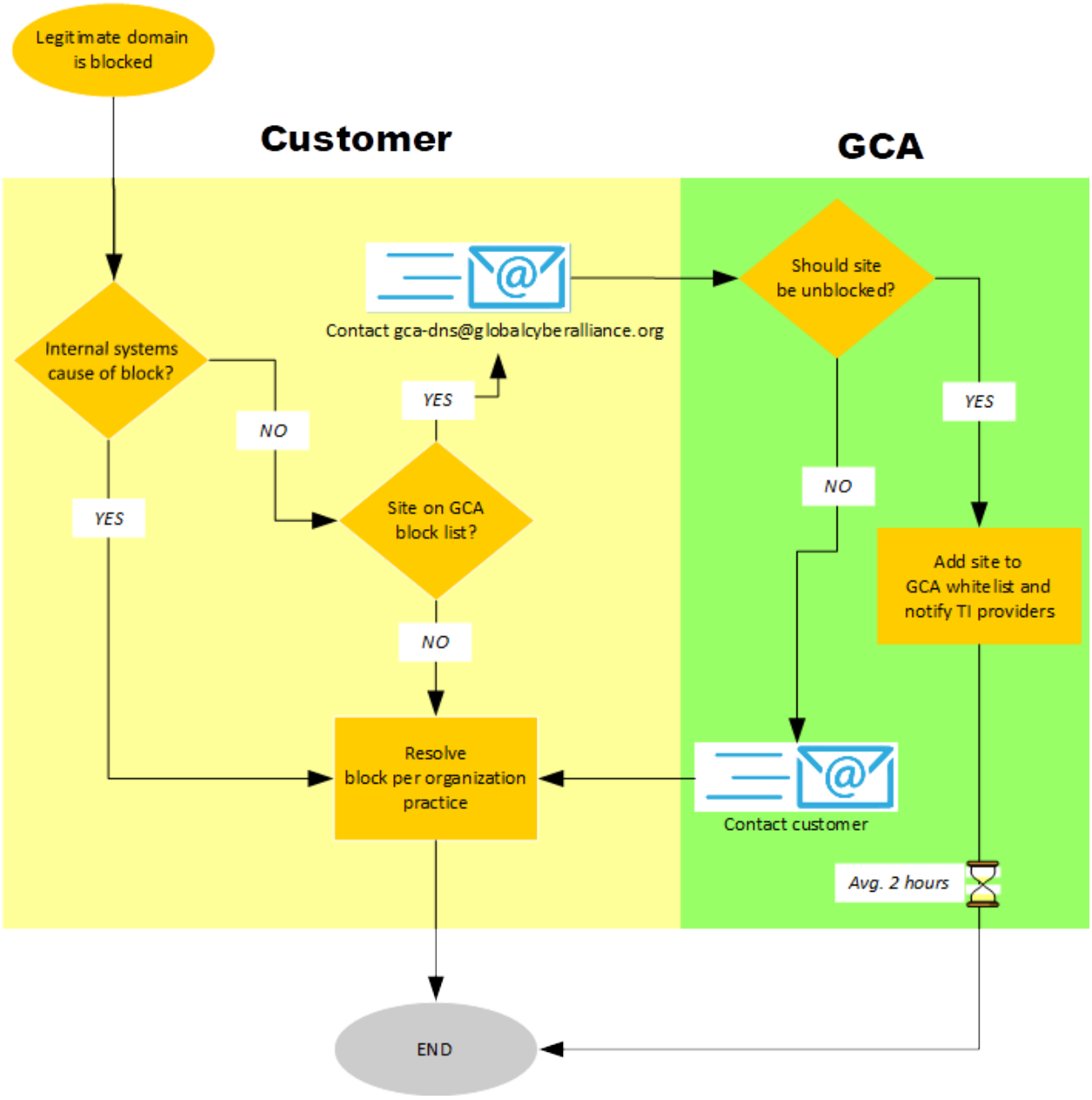
In addition, users can always customize their (non-caching) DNS servers to override policy defaults from GCA by using their own RPZs, whitelists, and blacklists.

The GCA Internet Immunity service will not

- Collect PII, source IPs, or demographic data
- Compile a list of domain owners, content producers, or other netizens that would potentially be subject to exposure
- Create a content inspection system or impose any content-based controls
- Create a single, centralized authority that picks reputational winners and losers
- Create a system with invisible, default opt-ins or troublesome opt-outs
- Redirect users to advertising-based websites

Whitelisting

GCA provides a process for removal requests in case an organization or individual believes it has been blacklisted in error. This process is represented at a high level in the graphic below.



GCA business hours are 8:00 am–6:00 pm EST Monday through Friday. Off-hours requests are best effort and are handled the next morning at the latest.

Service incident of April 5, 2017

Summary

On April 5, 2017, GCA Internet Immunity service users started reporting a high number of legitimate domains being blocked through the service, most of them hosted at Amazon AWS and Microsoft Azure infrastructures. Although those domains were whitelisted in our system, analysis discovered a bug in the portion of the code that splits/normalizes a domain when generating the RPZ files. Our developers quickly implemented a fix and pushed it out to the production system. Due to the way DNS works and the size of our infrastructure, it took some time for the new zone files to be propagated to all edge resolvers around the globe. We estimate that a code fix currently would take about one hour to propagate.

Analysis

Before the influx of legitimate AWS and Microsoft Azure domains into the TI feeds, we had been transitioning the code that splits/normalizes domain names from an in-house implementation to one provided by a credible third party (Google). We had unit tests in place for both approaches, and were—at the time—confident that we could migrate the code to the third-party module without any difference in results.

However, the unit test cases weren't comprehensive enough; the in-house module was being used when domain names were ingested into the system, and the third-party module was being used for whitelist management. Mismatches between the modules began to show in more intricate domain names.

For instance, given domain name

```
example.compute.amazonaws.com.cn
```

the in-house module would split the domain name into the following tuple:

```
('', 'example', 'compute.amazonaws.com.cn')
```

and insert it into the database as a domain to block. However, the third-party module would return a different tuple for the whitelist:

```
('example.compute.amazonaws', 'com', 'cn')
```

When the blacklist was constructed, `example.compute.amazonaws.com.cn` would not reach the whitelist because the domain-name–splitting caused a mismatch in the second and third items of the tuple.

The fix

After weighing the advantages and disadvantages of both modules, we opted to stick with the in-house implementation, as it maintains an up-to-date list of domain name suffixes. This enables us to be more accurate in whitelisting and will prevent the problem from recurring.

Notes

- Both our in-house code and the third-party code used the Public Suffix List as the ruleset for denoting domain name suffixes.

- The Public Suffix List is updated several times per week, and our in-house module updates its locally cached copy as soon as the public feed is updated.

- Our in-house module allows us to add custom domain suffixes to the ruleset. Normally, we avoid adding custom information to a canonical, authoritative list, but in a very few cases, it has been helpful. For example, when we started the project, the Public Suffix List was missing a ccTLD rule for .ke (Kenya) domain names. The suffix has since been added to the Public Suffix List, and we have removed it from our “custom TLDs” list.

- The third-party module had a code-generation step that downloaded the Public Suffix List and preprocessed it, generating a space-efficient table of domain name suffixes. Unfortunately, it was being updated only when the package authors would get around to regenerating the suffix table. If we had run the code generation steps to generate the domain name suffix table ourselves, this would have resulted in a divergent fork of the third-party module.

Metrics

GCA will consider the success of the project to lie in its effectiveness and the breadth of its use. We can measure these through the following DNS server statistics:

- Number of queries per day
- Number of queries against malicious domains that were blocked
- Geolocation data (city and country) on the origin of queries for malicious domains
- Number of queries for a specific domain
- First-time-seen and last-time-seen timestamps for malicious domains

Key performance indicators

These are the statistics on our key performance indicators as of October 13, 2017.

1. Number of data feeds/providers: 18
2. List of TI providers (those we cannot publicly discuss not listed):
    - AlienVault
    - 360.cn
    - APWG/eCrimeX
    - Bambenek Consulting [about 800K DGA domains]
    - CleanMX
    - EmergingThreats
    - Eset
    - F-Secure
    - Internet Storm Center
    - Malc0de
    - MalwareDomains
    - OpenPhish
    - PhishLabs
    - PhishTank
    - Ransomware Tracker
    - RISKIQ
    - ThreatGrid
    - ThreatStop
3. Number of endpoints protected: approximately 600k
4. Cities where we have points of presence (resolver clusters) as of October 13, 2017:
    - IAD Reston US
    - ABJ Abdijan CI
    - AKL Auckland NZ
    - AMS Amsterdam NL
    - ATL Atlanta US
    - BER Berlin DE
    - BOS Boston US

- BUR Burbank US
- CAI Cairo EG
- DFW Dallas US
- DUB Dublin IE
- DUR Durban ZA
- DXB Dubai AE
- EVN Yerevan AM
- FRA Frankfurt DE
- GND St. Georges GD
- IST Istanbul TR
- JAX Jacksonville US
- JKT Jakarta ID
- JNB Johannesburg ZA
- KTM Kathmandu NP
- LGA New York US
- LHR London UK
- LOS Lagos NI
- MIA Miami US
- MKE Milwaukee US
- MPM Maputo MZ
- NBO Nairobi KE
- NRT Tokyo JP
- ORD Chicago US
- OTP Bucharest RO
- PAO Palo Alto US
- PDX Portland US
- PER Perth AU
- PNH Phnom Penh KH
- PRG Prague CA
- QPG Singapore SG
- RIC Richmond US
- RNO Reno US
- SCL Santiago CL
- SEA Seattle US
- SFO San Francisco US
- SGU St. George US
- SNA Los Angeles US
- SOF Sofia BG
- STL St. Louis US
- SYD Sydney AU
- VIE Vienna AT
- WAW Warsaw PL
- WLG Wellington NZ
- YOW Ottawa CA
- YUL Montreal CA
- YWG Winnipeg CA
- YXE Saskatoon CA
- YYC Calgary CA
- YYZ Toronto CA

- ZRH Zurich CH

5. Blocks per day: 200–250

Feedback Data for Threat Intelligence Providers

The DNS **Threat Intelligence API** will provide a means for TI providers to receive telemetry data generated from DNS requests that have been blocked by the RPZs on the DNS servers maintained by PCH.

GCA receives, parses, and curates the TI feeds provided by its partners. GCA also maintains "the whitelist," a list of well-known, nonmalicious domain names. The whitelist is looked up during RPZ generation, and any domain names found in both lists are omitted in the generated RPZ.

Services that will run alongside the DNS servers will generate telemetry data from information emitted by the facilities; these can be running BIND, Unbound, Knot, PowerDNS, or dnsdist. Data will be generated only from DNS queries that have resulted in an NXDOMAIN response due to an RPZ.

For each of these records, the telemetry data will include

- A timestamp indicating when the DNS query was resolved
- The name (QNAME; "example.com")
- The type (QTYPE; "A", "AAAA", "TXT", "CNAME," etc.)
- High-level geolocation data on the query

Only the first three octets of the user's IPv4 address will be used to retrieve geolocation data. Once the geolocation has been determined, the IP address will be discarded. At no point will the user's IP address in part or in whole be emitted from the telemetry service.

The telemetry data will be transmitted back to GCA's servers for storage and analysis. Analyses applied to the telemetry data will be limited to very simple aggregations, such as the sum of RPZ hits per country and country region (i.e., state or province). Concurrently, another process will consume the generated telemetry data and attempt to correlate the DNS QNAME to a TI provider. When a correlation is made, a copy of the telemetry data will be placed in a queue specific to the TI provider. If a single telemetry message is correlated to multiple TI providers, it will be placed in each provider's queue. These queues will collect the data until the TI provider connects to the API and consumes the data.

Auditors will be able to inspect the logic that provides the data to the TI providers.

Technical documentation

Authorization

The API exposes an HTTP/WebSocket interface. Upon connecting to the API at https://telemetry.dns.globalcyberalliance.org, the user provides an authorization token in the `Authorization` HTTP request header:

```
Authorization: Token {token}
```

Upon authorization, the stateless HTTP connection is upgraded to a WebSocket connection. (Failure to provide a valid token results in an "HTTP 401 Unauthorized" response.)

Consuming the feed

The API sends the client JSON-encoded telemetry messages with the following structure:

```
{
  "id":                                    "1234567890",
  "qname":                                "example.com",
  "qtype":                                          "a",
  "timestamp":                           1494283069,
  "city":                      "New                 York",
  "region":                                        "NY",
  "country":                                       "US"
}
```

Each telemetry message has an `id` field holding an identifier for the message. For each received message, the client must send an acknowledgment. Acknowledgments are JSON objects with a single field, `id`, holding the identifier of the message it is acknowledging

```
{

  "id": "1234576890"

}
```

Acknowledgment rules

The following rules apply to all client-server communications over the WebSocket connections:

- All messages received by the client must result in an acknowledgment sent back to the server
- Acknowledgments must be sent in order
- Acknowledgments must be sent as soon as possible

Failure to comply with these rules will almost certainly result in the WebSocket connection being closed by the API server. Additionally, messages that are not acknowledged are re-sent the next time the client connects.

Generating an API key

API keys for clients can be generated using the `new-token` subcommand of the `threat-intel-api(1)` program. An example of its usage is as follows:

```
$ threat-intel-api -c path/to/config.yml new-token {topic}
```

where `{topic}` is the name of an existing Kafka topic holding telemetry messages for the TI provider. If the specified Kafka topic does not exist before this command is executed, no token will be created.

Upon a successful invocation, the command prints the new authorization token to STDOUT.

API key management

All API key management is performed through subcommands to the `threat-intel-api(1)` program. Tokens can be created and altered, but not deleted.

Support

This section describes GCA's customer support for the Internet Immunity Project and all customer needs.

Mission

Our mission is to help our customers make the best use of internet immunity by providing a single point of contact and responsibility for rapid closure of their technology and process concerns.

Services

The Global Cyber Alliance does not offer any dedicated personalized support services.

General support

Systems administrators should be considered the initial, self-help tier; all issues should pass through these representatives first. When an issue is escalated to GCA Support, GCA will try to reproduce and validate the issues by working with the system administrators, and then work on mitigating the problem if validated. Information GCA may request from the organization includes errors, warnings, logs, screenshots, and sequences of steps for re-creating an issue.

Email contact: gca-dns@globalcyberalliance.org

Email responses during business hours (8:00 am-6:00 pm EST, Monday through Friday)

> It is our goal to provide responses to all tickets within an hour and have tickets resolved on an average basis of 2 hours per ticket.

Email responses during nonbusiness hours

> Off-hours requests are best effort and will be handled the next business day.

Glossary of Terms

Anycast
A network addressing and routing method in which multiple machines may share an IP address, allowing a DNS query to be routed for resolution to the closest, lowest-cost, or healthiest server on the least congested route. This reduces response time. GCA's partner, Packet Clearing House, pioneered the use of DNS anycast to distribute DNS load among more servers in more places.

BIND
An acronym for "Berkeley Internet Name Domain," the mostly widely used (and open-source) software for configuring DNS servers. GCA configures TI and passes it to BIND; users may then configure their own DNS (non-caching) servers to use the GCA Internet Immunity service.

Blacklist
In general, a list of malicious elements. In the GCA Internet Immunity service, a list of malicious domain names that we block based on high-quality TI feeds.

ccTLD
An acronym for "country code top-level domain," a TLD generally reserved for a country identified with a country code. Examples are ".de," ".uk," and ".tw" for Germany, the United Kingdom, and Taiwan in domain names such as "google.de" and "bbc.co.uk." The GCA Internet Immunity service will protect users by resolving queries on malicious domains to the TLD of the domain name, resulting in an NXDOMAIN response.

DHCP server
A server that uses *dynamic host configuration protocol* to generate IP addresses for host computers on a network. It is the most common method of obtaining IP addresses.

DNS
An acronym for "domain name system," the global database of IP addresses and their corresponding domain names.

DNS notification
The protocol in which a DNS primary server notifies a secondary server of any changes to a zone. DNS notification supports secure and authentic *zone transfers*, the mechanism for propagating new TI data throughout the GCA Internet Immunity infrastructure on a round-the-clock basis.

DNS transaction signature
The protocol in which a DNS zone transfer is authenticated between the originating and receiving servers. DNS transaction signatures support secure and authentic *zone transfers*, the mechanism for propagating new TI data throughout the GCA Internet Immunity infrastructure on a round-the-clock basis.

DNSSEC
An acronym for "DNS Security Extensions," a technology that authenticates domain names and IP addresses against each other. This technology does not conflict with the GCA Internet Immunity service or infrastructure.

IoT

An acronym for the "internet of things," encompassing all devices that can connect to the internet, such as smart phones, identity chips in animals, remotely programmable kitchen appliances, and heart monitors. The GCA Internet Immunity service can protect such devices by protecting the computers and devices they connect to.

IP

An acronym for "internet protocol," a set of rules governing the generation and format of the unique numerical identifier assigned to each host computer on the internet. In the DNS, a computer's IP address corresponds to a unique domain name.

IPv4

An acronym for "internet protocol version 4," the fourth revision of the IP, which formats IP addresses in four octets of binary numbers separated by periods. Translated to decimal, an IP address might look like "198.41.0.4" or "202.12.27.33" (the IP addresses for the "a" and "m" root servers). GCA uses the last three octets of a querying computer to provide geolocation usage data to TI providers; removing the first octet protects the privacy of the user.

MSSP

An acronym for "managed security service provider," an internet service provider that provides a customer with some amount of network security management, which may include virus blocking, spam blocking, intrusion detection, firewalls, and virtual private network (VPN) management. MSSPs are potential GCA Internet Immunity Project partners.

Name server

The designated web server that manages the domain names and IP addresses of an ISP's accounts. Cyber criminals may create or utilize name servers specifically to resolve the malicious domains they create. The GCA Internet Immunity service can block name servers that list nothing but malicious domains.

Netblock

A range of IP addresses.

Non-caching DNS server

A DNS server that does not cache IP address/domain name correspondences. GCA Internet Immunity service users must configure their non-caching DNS servers to implement the service.

NXDOMAIN

The resolution of a query to the domain's TLD. For instance, if a user clicks on a blacklisted and malicious domain called *www.bad-domain.com*, the name server returns the IP address for the ".com" server, which the user experiences as no answer. The GCA Internet Immunity service responds to queries on malicious and blacklisted domains with an NXDOMAIN, thus preventing an end user from reaching a malicious domain.

PCH

An acronym for "Packet Clearing House," the international organization responsible for providing operational support and security to critical internet infrastructure, including internet

exchange points and the core of the domain name system. As GCA's partner in the Internet Immunity Project, PCH provides the infrastructure for the service.

Phishing attack

An attempt to obtain sensitive information such as user names and passwords or to trigger malware by disguising a malicious domain as a trustworthy entity in an electronic communication such as an email or text message. The GCA Internet Immunity service can thwart phishing attacks by blocking known malicious domains when users click on benign-appearing links in spam emails.

PII

An acronym for "personally identifiable information," which can be used to identify an individual. Examples are social security numbers, names, and addresses. Email addresses and IP addresses can reveal PII or be used to trace PII. The GCA Internet Immunity service protects PII from phishing attacks, without ever collecting PII or data that can be used to uncover PII.

QNAME

The domain name being queried.

QTYPE

The "resource record" requested in a query, common examples being for domain names, name servers, and email servers.

Query

The request sent from a client computer to the DNS to find the IP address that corresponds to a domain name that a user (generally) has clicked on in a link or typed into a browser.

Recursion

The handling of a query by routing a domain from the client to any number of DNS servers until the query is resolved with either 1) an IP address or 2) no response.

Resolve

The process the DNS performs of matching a domain name to an IP address.

Root

The topmost domain of the internet; the implied end of every domain name. There are 13 root authorities in the world listed as the letters "a" through "m," which handle queries by returning name servers for TLDs. Packet Clearing House, GCA's infrastructure partner in the Internet Immunity Project, hosts multiple root letters.

RPZ

An acronym for "response policy zone," a mechanism on top of the global DNS that allows a name server to look up custom information in order to handle queries via specific types of responses. The GCA Internet Immunity service uses RPZs to resolve malicious domains with the NXDOMAIN response.

Telemetry data

Data generated via an automated communication process from remote or inaccessible points and transmitted to receiving equipment for monitoring. The GCA Internet Immunity service will obtain data for metrics by running services alongside the DNS servers to generate telemetry data from information on queries that have resulted in an NXDOMAIN response due to an RPZ.

TI

An acronym for "threat intelligence," information on malicious domains, IP addresses, netblocks, and name servers. The GCA Internet Immunity service uses TI feeds from reputable providers to create blacklists to protect users from phishing attacks and malware.

TLD

An acronym for "top-level domain," a domain immediately below the internet root. Examples are ".com," ".net," and ".org." The GCA Internet Immunity service protects users by resolving queries on malicious domains to the TLD of the domain name, resulting in an NXDOMAIN response to dangerous queries.

Transfer (incremental zone transfers)

The process of transferring zones between DNS servers throughout the world. The GCA Internet Immunity service propagates newly added TI data in its blacklist via round-the-clock incremental transfers of the RPZs.

Walled garden

An environment or web page that controls a user's access to the internet or network services. For internet security, a query on a malicious domain may be redirected to a walled garden, which blocks the user's access to the malicious domain and may also be configured to log the query. GCA Internet Immunity service users may customize their systems to redirect queries on malicious domains to walled gardens instead of blocking via NXDOMAIN responses.

Zone

A hierarchical arrangement of domains and their corresponding IP addresses. The GCA Internet Immunity service transfers zones and RPZs on a round-the-clock basis to propagate newly added TI data in the blacklist.

FAQs

1. **What is the DNS?**

   The domain name system (DNS) is the worldwide internet database of unique numerical computer addresses and their corresponding user-friendly domain names. It enables people to to more easily navigate the internet by using memorable, meaningful names instead of the complex numerical ("IP") addresses.

2. **Does my computer use DNS?**

   To access websites on the internet, your computer must leverage a DNS service. It is usually configured by your internet service provider or your network administrator.

3. **How does the GCA Internet Immunity service protect me from malicious domains?**

   GCA brings together cyber threat intelligence about malicious domains from a variety of trusted sources and blocks access to those malicious domains when your system attempts to contact them.

4. **How will the GCA Internet Immunity service help protect my data?**

   When you use the service, attackers and malware cannot leverage the known malicious domains to control your systems, and their ability to steal your data or cause harm will be hindered. The GCA Internet Immunity service is an effective and easy way to add an additional layer of security to your infrastructure for free.

5. **Will the GCA Internet Immunity service filter content?**

   No. The service will not provide a censoring component and will limit its actions solely to the blocking of malicious domains around phishing, malware, and exploit kit domains.

6. **How will the GCA Internet Immunity service prevent the accidental blocking of legitimate domains?**

   GCA implements whitelisting algorithms to make sure legitimate domains are not blocked by accident. However, in the rare case of blocking a legitimate domain, the GCA Internet Immunity team has a process to work with the user to quickly whitelist that domain. Please see information in this document on our general Support and our process for handling whitelisting requests.

7. **How does GCA ensure that it has the latest threat intelligence?**

   GCA gathers threat intelligence from all its providers and public sources on a daily basis and updates the GCA Internet Immunity infrastructure with this information.

8. **Why do threat intelligence providers share their data with GCA, and what do they get out of it?**

   GCA gives anonymized telemetry back to the threat intelligence providers only for the malicious domains they share with GCA. This telemetry does not include source IP information of the users.

9. **Does the GCA Internet Immunity service collect and store personal data?**

   The GCA Internet Immunity service does not store any personal data about its users. You can read our complete Data Policy at https://www.globalcyberalliance.org/data-policy.html.

10. **How does the GCA Internet Immunity service ensure my privacy?**

    When an entity or an individual is using the service, their IP address is not logged in our system. We do, however, log the geolocation (city, state, country) of the system, and use this information for malicious campaign and actor analysis, as well as a component of the data we provide to our threat intelligence partners.

11. **What does GCA log/store about the DNS queries?**

    We store details of the domain queried, timestamps, and the city, state, and country from where the query came. We do not store source IP information of the users.

12. **Does GCA share the DNS data that is generated with marketers?**

    GCA does not and never will share any of its data with marketers, nor will it use this data for demographic analysis. Our sole purpose is fighting cyber crime on the internet and to enable individuals and entities to be more secure. We do this by increasing visibility into the threat landscape by providing generic telemetry to our security industry partners who contribute data for blocking.

13. **How resilient is the GCA Internet Immunity service?**

    No infrastructure is 100% safe from attacks and failures. However, GCA has partnered with Packet Clearing House (PCH) to build and maintain a very robust and resilient DNS infrastructure. PCH has been working since 1995 to make the domain name system faster, more scalable, and more resilient against attack. PCH pioneered the use of DNS anycast to distribute DNS load among more servers in more places, anycasting top-level domain name servers since 1997, and root name servers since 2001. PCH is the largest authoritative DNS service network in the world, hosting multiple root letters and more than 300 top-level domains on thousands of servers in 150 locations around the world. PCH is also the operator of the only FIPS 140-2 Level 4 DNSSEC signing platform other than the root itself.

14. **How do I install/use the GCA Internet Immunity service?**

    Your systems are already using a DNS service either through your ISP or some other third-party provider. Switching to the GCA Internet Immunity system takes less than 10 minutes and is a very straightforward process. Specific configuration will depend on your network configuration, and we are happy to assist you during the onboarding process. Get in contact with us via gca-dns@globalcyberalliance.org.

15. **How much does the GCA Internet Immunity service cost an organization to install?**

    The service does not have an additional cost to an organization and does not require any additional software or hardware to be installed.

16. **How long has the GCA Internet Immunity service been in production?**

    The service was brought online in August of 2016 with the first beta users. Since that time, more threat intelligence has been added, more resolvers brought online, and more users added to the system.

17. **What has your DNS up-time been?**

    GCA Internet Immunity is a global anycast service. Multiple points of presence around the world means redundancy is built into the system. If a resolver goes down, the traffic is automatically routed to the next-closest resolver. To date, our up-time has been 99.999%.

18. **How long does it take to push a new malicious domain name out to secondary servers?**

    It can take five seconds to push a new malicious domain name to hundreds of secondary servers on multiple continents.

19. **Can a customer create their own blacklist or whitelist for local use?**

    Although GCA does not provide customization of feeds, users may configure their local resolvers to add their own blacklists locally. Users may consult the BIND documentation (available at https://www.isc.org/downloads/bind/doc).

20. **How do RPZs work with DNSSEC?**

    If a domain name is blacklisted, the RPZ "turns off" DNSSEC, preventing it from being signed. If a domain is whitelisted or not listed at all, it will be subject to DNSSEC as usual.

21. **How do RPZs affect page load time?**

    Where no recursion takes place, caching servers may be up to 2% slower.

22. **If maintenance needs to happen on the GCA Internet Immunity infrastructure, how is that coordinated and how much lead time is given to the end users?**

    Maintenance is performed continuously, and users should not experience any disruption in service.

23. **Is there a URL we can check to see if a given domain is blocked, and what a user might get if they go to a blocked site?**

    If a site is blocked, users receive an "NXDOMAIN" response, so the end-use system acts as if the domain does not exist. GCA is working on a website where you will be able to conduct searches for domains to see whether we are blocking them. We will let users know when the site goes live.

24. **How do we become a Device Manufacturer partner?**

    Send an email to dns-device-partner@globalcyberalliance.org with your organization details and contact information.

Appendix A: Trial Project: Technical University of Denmark

This section describes a test of RPZs that was conducted independently of the GCA.

In late 2012, the Department of Environmental Engineering (ENV) at the Technical University of Denmark undertook a four-week trial of RPZs, for which Spamhaus provided their TI feed gratis. The ENV followed the Internet Security Consortium's (ISC) specification dated October 2011 to configure BIND. Two reports of the trial have been published: one by the trial's author, Hugo Connery, Head of IT at the ENV (available at DNS Response Policy Zones); and the other by Spamhaus. This section synthesizes and condenses both reports.

ENV is an international research organization with significant communities from six continents. As such, it generates internet traffic of a wide variety in language, culture, subject, and geographic location. Any automated internet filtering must be agnostic to these variables and focus only on the actual malicious domains.

The goals of the trial were to

- Increase client system security by preventing access to dangerous domains
- Increase client system security by informing the community of the risk of visiting dangerous domains
- Increase general security by raising the awareness among the department's IT staff of dangerous domains

The default policy for an RPZ is to answer a query on a malicious domain by returning no IP address, thus giving the end user no means to differentiate between a malicious site and a merely nonexistent one. Since raising awareness was a goal of the trial, its authors chose to use another policy option, namely to redirect users to a "walled garden"—an informative site within a user's network. The ENV designed a site with its departmental logo and a means of submitting feedback.

Over the four-week trial, approximately 5,000 attempted contacts to malicious sites were intercepted and 75 client systems were defended via the RPZs. The RPZs had no impact on productivity, but increased security by

- Preventing contact with dangerous sites
- Identifying locally infected systems (despite their being installed with commercial antivirus software and current definitions)
- Increasing the awareness of the IT organization to threats

One report of inappropriate filtering was received, which turned out to be legitimate; it was an email harvesting website. Thus, no inappropriate filtering was reported.

Appendix B: Partner Agreement

GLOBAL CYBER ALLIANCE

globalcyberalliance.org
New York | London

Global Cyber Alliance
Partnership Confirmation

Thank you for your interest in supporting the mission of the Global Cyber Alliance (GCA). GCA is an international, non-profit organization founded to collectively confront systemic cyber risks. GCA seeks the participation of all organizations with interest or expertise in addressing key systemic cyber risks. Joining GCA is easy and free.

GCA addresses cyber risks with a cross-sector, global approach. GCA acts as an action-oriented organization identifying cyber risks on which little progress is being made. Solutions are identified and implemented with the input and collaboration of partners.

GCA will:

- Collaborate with global, public, and private organizations to identify top systemic cyber risks;
- Develop an understanding of the risks and how to measure them;
- Identify or develop solutions to confront the risks;
- Build teams to execute the solutions; and
- Measure success in mitigating the risks.

To achieve these goals, GCA relies on the commitment of partners willing to work together. Collective efforts create a force multiplier effect and maximize the impact we have in combating cyber risks.

Partners are encouraged to take one or more roles in the mission to reduce systemic cyber risk, including:

- Supporting GCA's mission;
- Contributing subject matter or technical expertise;
- Making a substantive contribution to cyber risk eradication;
- Promoting GCA to a specific constituency, through leadership and communication;
- Participating in GCA projects;
- Adopting GCA solutions; and/or
- Contributing to GCA's long-term sustainability.

For your organization to become a Global Cyber Alliance partner please fill out the information below.

_____
Name

_____
Title

_____
Name of Organization (as it should appear on our partner list)

_____
Address of Organization

Phone

Email

Signature

As a partner, GCA would like to post your organization's name and logo on the GCA Website and promote our partnership through our social media accounts and outreach materials. GCA has permission to post my corporation's logo and/or name on the GCA Website and promote the partnership through GCA social media channels and outreach materials.

- ☐ Yes
- ☐ No

If so, please provide your logo in a high-resolution format to mrdaughlin@globalcyberalliance.org

We want to connect with you! Please provide your social media information:

Twitter:_____

Facebook:_____

LinkedIn:_____

Other:_____

As a GCA partner, we would like to keep you informed of our activities, project progress, new initiatives and travels. If you would like to be included in these communications, please click here to be included on our mailing list: https://www.globalcyberalliance.org/#signup.

Bibliography

1. Hugo Connery, DNS Response Policy Info, *Response Policy Zone History, Usage and Research*, https://dnsrpz.info/RPZ-History-Usage-Research.pdf, May 16, 2013.

2. Hugo Connery, Spamhaus, *A Case Study at DTU Environment, DNS: Response Policy Zone,* https://dnsrpz.info/spamhaus-rpz-case-study.pdf, October 2012.

3. Internet Systems Consortium, *BIND 9 Documentation*, Last modified: November 2, 2016 at 11:03 pm, https://www.isc.org/downloads/bind/doc, last accessed 10/6/2017.

4. Paul Vixie and Vernon Schryver, The Internet Engineering Task Force, *DNS Response Policy Zones (RPZ),* https://tools.ietf.org/pdf/draft-vixie-dns-rpz-03.pdf, December 16, 2016.