FARSIGHT SECURITY

DNS Dictionary

This dictionary contains key terminology, abbreviations, and acronyms related to the Domain Name System and covers topics spanning security, infrastructure, malware, and essential organizations.

DNS Dictionary

FARSIGHT SECURITY

A

A Record - An "A" record maps a fully qualified domain name to an IPv4 address.

AAAA ("quad-A") Record - A AAAA record maps a fully qualified domain name to an IPv6 address. AAAA records are normally verbalized as "quad-A records".

ACL (Access Control List) - Range of IP addresses filtered or allowed by a firewall, border router, or other network device. ACLs are often used to block sources of network attack traffic or to allow case-by-case access to a resource that's normally publicly inaccessible.

AFRINIC (African Network Information Center) - The African Network Information Centre is the Regional Internet Registry (RIR) for Africa, responsible for the distribution and management of IP addresses and Autonomous System Numbers (ASNs). It services Africa and the Indian Ocean region. For more information, see afrinic.net.

APNIC (Asia Pacific Network Information Center) - The Asia Pacific Network Information Center is the Regional Internet Registry (RIR) for the Asia-Pacific region, responsible for the distribution and management of IP addresses and Autonomous System Numbers (ASNs). It is headquartered in Australia and covers the entire Asia Pacific region, which is comprised of 56 countries in Asia and Oceania. For more information, see apnic.net.

ARIN (American Registry for Internet Numbers) - As the Regional Internet Registry (RIR) for Canada, the United States, and many Caribbean and North Atlantic islands, ARIN manages the distribution of IP addresses (IPv4 and IPv6) and Autonomous System Numbers (ASN). For more information, see arin.net.

ASCII (American Standard Code for Information Interchange) - A character encoding standard used to represent English characters as numbers in electronic communication.

Authoritative Name server - Authoritative name servers are used by domain name owners to connect domain names to IP addresses. They provide the link between a domain name, such as www.farsightsecurity.com, and the IP address where that domain name is hosted. Authoritative name servers answer DNS queries from anywhere on the network, but only for the specific domain names that they're authoritative for.

DNS Dictionary

FARSIGHT SECURITY

AXFR (Zone Transfer) - Protocols used to replicate DNS zone files, typically from a master DNS server to one or more distributed secondary DNS servers. AXFR is used to transfer full zones, while IXFR (Incremental Zone Transfer) handlesdoes incremental zone updatess. In an effort to avoid disclosing all domains that may exist in a given zone, Zone transfer access is normally restricted exclusively to a small list of specifically authorized parties.

B

Bailiwick - In the DNS world, "in-bailiwick" has two formal definitions in RFC 7719, "DNS Terminology".

(a) An adjective to describe a name server whose name is either subordinate to or (rarely) the same as the zone origin. In-bailiwick name servers require glue records in their parent zone [...]

(b) Data for which the server is either authoritative, or else authoritative for an ancestor of the owner name. [...]

For example, under definition (a), ns1.example.com might be an "in-bailiwick" name server for example.com, while ns2.whatever.net would be "out-of-bailiwick" for example.com. This definition is the way the term "in-bailiwick" is most commonly used by people who are part of the technical DNS community.

The bailiwick concept is important because some malicious name servers may try to provide "out-of-bailiwick" and potentially wrong or misleading results along with the information they were asked to provide. Paying attention to a name server's "bailiwick," as defined in definition (b), is an important part of data quality assurance.

BGP (Border Gateway Protocol) - BGP is the wide area routing protocol used to get network traffic from source to destination over the Internet. It is used on Cisco, Juniper, and similar routers. BGP is core to Internet operations.

BIND (Berkeley Internet Name Daemon) - The Internet's most widely used name server software (see http://www.isc.org/downloads/bind/).

Blocklist (or Blacklist) - A list of unwelcome content sources, typically IP addresses or domain names, detected as associated with spam. The first DNS blocklist, the Realtime Blackhole List (RBL), was initially created in 1997 as a BGP (see definition above) feed by Vixie and Dave Rand, and then turned into a DNSBL by Eric Ziegast as part of the Mail Abuse Prevention System (MAPS).

Broadcast Traffic - Network traffic that is sent to all hosts on a network segment.

C

CA (Certificate Authority) - Also called "Certification Authority," the CA is an entity that issues digital certificates to certify ownership of a public key, allowing others to trust signatures or assertions made by the corresponding private key. Best known for issuing publicly-trusted certificates for use by TLS-secured web servers.

CAA (Certificate Authority Authorization) - A security measure for domain owners to specify (in their DNS) which CAs are authorized to issue certificates for their domain.

Cache - Repository used to temporarily remember recently seen information; in the DNS case, this contains DNS resource records, remembered until those records time out and are purged (see TTL).

Cache Poisoning (aka DNS Spoofing) - Cache poisoning is the intentional replacement of legitimately cached web content with false information.

ccTLD (Country Code Top Level Domain) - A 2-character TLD allocated to a country based on 2-letter ISO country codes (e.g., .us, .ca, .mx, etc.).

CERT (Computer Emergency Response Team) - Teams of operational cyber security people who work to improve computer security for a defined constituency by handling incidents. A list of generally-trusted CERT teams can be seen here: http://www.first.org/members/teams (note that some CERTS may have national scope, while others may represent a university, company, or other organization).

Checksums/Checksum Errors - When packets are sent over the network, random noise or other interference may occasionally result in some packets getting accidentally damaged. Checksums are lightweight mathematical value used to check data for errors should they occur. If you know the checksum of the original file, you can verify the integrity of your copy. Checksums can happen during transmission or storage, typically without the user being aware that it's even happening.

CIDR (Classless Internet Domain Routing Notation) - Succinct way of expressing the size of a block of network addresses. In the case of IPv4 addresses, some common CIDR values include:

```
/8      2^24=16,777,216 addresses <-- formerly known as a "class A" block
/16    2^16=65,536 addresses <-- formerly known as a "class B" block
/17    2^15=32,768 addresses
/18    2^14=16,384 addresses
/19    2^13=8,192 addresses
/20    2^12=4,096 addresses
/21    2^11=2,048 addresses
/22    2^10=1,024 addresses
/23    2^9=512 addresses
/24    2^8=256 addresses <-- formerly known as a "class C" block
/25    2^7=128 addresses
/26    2^6=64 addresses
/27    2^5=32 addresses
/28    2^4=16 addresses
/29    2^3=8 addresses
/30    2^2=4 addresses
```

CIRA (Canadian Internet Registration Authority) - CIRA is the organization that manages the ".CA" country code top-level domain and policies that support Canada's Internet community international Internet governance.

Client - In client/server computing architectures, the client is a software program typically run by an end user connecting to a server run by an online service provider. For example, thinking about http, the client will normally be a web browser (such as Firefox or Google Chrome or Edge), and the server might be Apache or nginx or Microsoft IIS.

CNAME Record (Canonical Name Record) - An alias for another domain in the DNS system. Various restrictions apply. For example, a CNAME must point to another domain name, and NOT to an IP address, CNAMEs should not point to other CNAMEs, etc.

Conficker Working Group (CWG) - Focused industry effort to tackle the Conficker malware epidemic. See http://www.confickerworkinggroup.org/wiki/.

Cybersquatting - To purchase and hold domain names with the intention of reselling them at a profit, often infringing on a trademark or registered name.

CZDS (Centralized Zone Data Service) - An online portal where any interested party can request access to the Zone Files provided by participating generic Top-Level Domains (gTLDs). See: https://czds.icann.org/home

D

DANE (DNS-Based Authentication of Named Entities) - A security protocol that enables the administrators of domain names to specify the keys used in that domain's TLS servers. (Requires DNSSEC)

Darknet - Sometimes referred to as a "dark space telescope." It is created by announcing a carefully monitored range of unused network addresses, and then watching to see what systems on the Internet probe, scan, or otherwise try to interact with those addresses. In a perfect world, nothing would attempt to interact with dark address space, but in reality, many miscreants (and legitimate researchers) are continually scanning the entire Internet). See for example The UCSD Network Telescope: http://www.caida.org/projects/network_telescope/.

Data Dictionary - A description of the data in a database, including field names, expected contents of those fields, any coded table values (for example, "OR"=="Oregon"), etc.

DDNS (Dynamic DNS) - 1.) ISPs provide residential customers with IP addresses that frequently change. DDNS is a service that automatically updates DNS records when an IP address changes. 2.) The standardized method of dynamically updating domain name server records is prescribed by RFC 2136, commonly known as dynamic DNS update. See: https://en.wikipedia.org/wiki/Dynamic_DNS#Standards-based_dynamic_DNS_update

Debian - A distribution of the Linux operating system.

Debian Sid - Codename for the version of the Debian Operating System that will be released.

Codename	*Version*
Stretch	*9*
Jessie	*8*
Wheezy	*7*

For full production releases, see: https://wiki.debian.org/DebianReleases

Dedupe - Eliminating duplicate observations.

Delegation - DNS is a series of delegations, for example from the root . zone, to the .com zone, to the .example.com zone. Delegation is the process that links the zones together, pointing the authority to the next in the chain.

dig - A Unix command line tool used to manually resolve domain names for testing or analysis.

DKIM (Domain Keys Identified Mail) - An email authentication protocol that allows the receiver to verify that an email was authorized by the domain owner. This is done by giving the email a digital signature as a header that gets encrypted and added to the message.

When the receiving system can determine that an email is signed with a valid DKIM signature, it can be certain that enumerated parts of the email have not been modified. For more, see http://dkim.org/.

DMARC (Domain-Based Message Authentication, Reporting, and Conformance) - An email authentication, policy, and reporting protocol that does two things: it explains what to do if email fails to successfully authenticate, and it provides reports about email auth to domain holders. See https://dmarc.org/

DNAME RRtype (Delegation Name Record) - Just as a CNAME creates an alias for a single DNS record, a DNAME creates an alias for an entire DNS subtree. See http://tools.ietf.org/html/rfc6672.

DNS Dictionary

FARSIGHT SECURITY

DNS (Domain Name System) - The distributed online system by which symbolic names (such as www.farsightsecurity.com) get translated to IP addresses (such as 66.160.140.81) and vice versa. Designed by Dr. Paul Mockapetris in 1983 at UCLA. Mockapetris is now a member of the Farsight Security Board of Directors. For more on DNS, see http://en.wikipedia.org/wiki/Domain_Name_System

DNSCrypt - A protocol that authenticates communications between a DNS client and a DNS resolver. It prevents DNS spoofing. It uses cryptographic signatures to verify that responses originate from the chosen DNS resolver and haven't been tampered with. See https://dnscrypt.info/faq/

DNSDB (DNS Database) - A database that stores and indexes both the passive DNS data available via Farsight Security's Security Information Exchange as well as the authoritative DNS data that various zone operators make available. DNSDB makes it easy to search for individual DNS RRsets and provides additional metadata for search results such as first seen and last seen timestamps as well as the DNS bailiwick associated with an RRset. DNSDB also has the ability to perform inverse or rdata searches. See https://www.dnsdb.info/.

DNSKEY - Public key DNSSEC record. See http://tools.ietf.org/html/rfc4034#section2.

DNS over HTTPS - A protocol for performing remote Domain Name System (DNS) resolution via the HTTPS protocol. A goal of the method is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data by man-in-the-middle attacks. See: https://en.wikipedia.org/wiki/DNS_over_HTTPS

DNS over TLS - A security protocol for encrypting and wrapping Domain Name System (DNS) queries and answers via the Transport Layer Security (TLS) protocol. See: https://en.wikipedia.org/wiki/DNS_over_TLS

DNS Propagation - The period of time it takes recursive resolvers across the world take to update their caches with a new DNS information for a domain; if TTLs are short, propagation is fast, but if TTLs are long, propagation can take hours or even days to take place.

DNSqr (DNS Query Response) - A nmsg type for capturing DNS query/response state. See https://archive.farsightsecurity.com/NmsgType_ISC_dnsqr/.

DNS Dictionary

FARSIGHT SECURITY

DNSSEC (Domain Name System Security Extensions) - Cryptographic protection for DNS, eliminating the risk of cache poisoning attacks if authoritative DNS servers digitally sign their data and recursive resolvers routinely validate those digital signatures.

Read more on why it's important: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

DNStable - Encoding format, library, and utilities for passive DNS data used in DNSDB. See: http://www.caida.org/workshops/isc-caida/1210/slides/isc1210_redmonds.html

Domain Hijacking - An attack in which the registration of a domain name is changed without the permission of its original registrant. Domain hijacking is typically committed with the intention to associate malicious content with a trusted and legitimate domain.

Domain Name - A unique name used to find and identify computers on the Internet and links to one or more IP addresses.

Domain Slamming - A type of scam in which a domain owner is tricked into re-registering their domain name, resulting in the domain name being fraudulently transferred to another registrar.

Domain Tasting - The purchase of a domain names formerly came with a five-day grace period to accommodate unexpected circumstances (e.g. typos). Domain tasting is the practice of abusing this grace period to test the profitability of multiple domains and ultimately returning the ones that prove less profitable. Measures have been implemented to discourage this, see https://en.wikipedia.org/wiki/Domain_tasting#Anti-domain_tasting_measures.

DOS/DDOS (Denial-of-Service/Distributed Denial of Service Attacks) - A cyber-attack in which the perpetrator makes a website or computer unavailable by overloading it with requests or unsolicited answers. In a DDoS attack, the incoming traffic originates from many different sources which are often infected with malware.

DS Resource Record - Refers to a DNSKEY RR and is used in the DNS DNSKEY authentication process. A DS RR refers to a DNSKEY RR by storing the key tag, algorithm number, and a digest of the DNSKEY RR. See http://tools.ietf.org/html/rfc4034#section5.

E

EDNS0 (Extension Mechanisms for DNS) - The extension mechanisms for DNS, defined in [RFC6891]. Sometimes called "EDNS0" or "EDNS(0)" to indicate the version number. EDNS allows DNS clients and servers to specify message sizes larger than the original 512 octet limit, to expand the response code space and to carry additional options that affect the handling of a DNS query. See: https://tools.ietf.org/html/rfc8499

F

False Positive - in the context of spam: determining that a message appears to be spam, when it is truly ham.

Contrast false positives with false negatives: in the false negative case, the categorizer misses spam, deciding that a message appears to be ham when it is truly spam.

Fast Flux - Rather than having a domain name map to one (or a small number) of stable IP addresses, fast flux domain names map to a constantly changing (and often large) set of botted computers, typically distributed all over the Internet. Because those domain names are constantly changing, it is extremely difficult to take down fast flux domain names by targeting the systems on which they're hosted.

If a domain's name servers also are fluxing, this is typically referred to as "double fast flux" domain names.

A 154 page ICANN report discussing Fast Flux hosting can be found: http://gnso.icann.org/en/issues/fastfluxhosting/fastfluxfinalreport06aug09en.pdf

FastRPZ - An RPZ (see "RPZ") implementation for Bind and Unbound created by Farsight Security as a reward for sensor operators. Unlike other RPZ implementations, FastRPZ is able to handle large policy zones totaling more than a million entries without performance degradation.

Firewall - Often installed at or near the border between an organization and the Internet, a firewall is meant to filter unwanted Internet traffic from reaching the organization.

Forwarding - Various usages, including:

-- Forwarding is the process whereby a web site directs a visitor to a different website.
-- Forwarding is the process whereby a packet makes its way across the Internet
-- Forwarding can also be done for email messages, as from an old email account to a current one, etc.

FQDN (Fully Qualified Domain Name) - The complete domain name for a specific computer or host on the internet. An FQDN is written with the hostname and the delegation point. For instance, www.example.com would be a FQDN.

Freemail or "Free Email" - Mail services that offer free (effectively non-attributable) accounts to anyone who cares to sign up for one. Examples include Google mail (Gmail), Hotmail, Yahoo, etc.

Front Running - In relation to domain names, it's the practice whereby a registrar uses insider information to register a domain name wanted by someone else in order to resell it at a higher price or to encourage the registrant to sign the name with that particular registrar. https://en.wikipedia.org/wiki/Domain_name_front_running

G

Glue Records - The IP-address of a name server stored on the registry. Glue records are required when a domain has name servers that are in the domain itself. They statically define the IP addresses of a domain's name servers and are therefore only needed when a domain's name servers are "in" the same domain.

Grey Listing - Antispam technique that initially temporarily rejects email; legitimate email senders will retry after a delay, at which point, the email will be accepted. Most spam delivery systems do not retry.

gTLD (Generic top-level domains) - a type of top-level domain (TLD) in the DNS maintained by the IANA. There are currently 21 classic gTLDs, categorized as:

generic (e.g.: .com, .net, .org, .info) - used for general purposes

sponsored (e.g.: .aero, .coop, .edu, .gov, .int, .mil, .asia, .cat, .jobs, .mobi, .tel, .xxx and .travel) - industry-specific use

generic restricted (e.g. .biz, .name, and .pro:) - only for their specified purposes

Infrastructure (.arpa) - used exclusively to support operationally-critical infrastructural identifier

See: https://archive.icann.org/en/tlds/

H

Ham - In a spam context, good (NONspam) messages.

Hostname - Hostnames allow users to access Internet resources (not just websites) by name rather than IP. Also "hostname" can be used two ways:
1.) just the leftmost label in a name
2.) the entire FQDN

In the second usage, info.farsightsecurity.com would be the hostname.

Hosts File - An alternative name resolution mechanism to DNS. At one point, every computer had a hosts file that listed the name and IP address of every computer on the network. This isn't scalable today.

In many operating systems, mappings contained in the Hosts file are set to trump any information that would be retrieved from a DNS server. Therefore, they're largely used for testing, or to intentionally block access to an unwanted domain.

DNS Dictionary

FARSIGHT SECURITY

I

IANA (Internet Assigned Numbers Authority) - The organization that allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet. http://www.iana.org/

ICANN (Internet Corporation for Assigned Names and Numbers) - A nonprofit organization that maintains the central repository for IP addresses, helps coordinate the supply of IP addresses, and manages the domain name system and root servers. http://www.icann.org/

ICMP (Internet Control Message Protocol) - IP does not have a built-in mechanism for sending error and control messages and therefore network devices like routers must depend on ICMP to report errors and manage queries.

IDN (Internationalized Domain Names) - IDNs enable a multilingual Internet. Using IDN standards and protocols, Internet-users are able to register and use domain names in scripts other than Basic Latin. https://info.farsightsecurity.com/farsight-idn-research-report

IDS (Intrusion Detection System) - IDS's monitor network traffic, looking for attack attempts. Examples include Snort (https://www.snort.org/), Zeek (https://www.zeek.org/), and Bro (https://www.bro.org/).

IETF (Internet Engineering Task Force) - An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. https://www.ietf.org/about

IESG (Internet Engineering Steering Group) - Members elected for technical management of IETF activities and the Internet standards process. https://www.ietf.org/about/groups/iesg/

IOCs (Indicators of Compromise) - Typically identified in conjunction with a particular attack. Examples include hash values for known-malicious executables or known command and control IP addresses (or domain names) seen directing activities involving a compromised system.

DNS Dictionary

FARSIGHT SECURITY

IP Address - Numeric address of an Internet resource. Can be either IPv4 (the classic/traditional type of IP address still used by virtually all sites), or IPv6 (the new longer IP address format typically deployed alongside IPv4, or in lieu of IPv4).

See below for IPv4 & IPv6.

IP Management Interface (IPMI) - A set of computer interface specifications for an autonomous computer subsystem that provides management and monitoring capabilities independently of the host system's CPU, firmware (BIOS or UEFI) and operating system. See: https://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface

IP Protocol - Type of Internet Protocol traffic. The two most common types are TCP and UDP, (see below) but there are many other types, too. A list of defined protocols can be found here: http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.

IP Range - Range of IP addresses specified by a starting and stopping address. For example: 69.172.200.0 - 69.172.201.255

IPv4 - "Normal" Internet addresses, comprised of four integers (having values from 0 to 255), separated with dots. For that reason, they're often called a "dotted quad." Example: 69.172.201.208

Because the Internet has largely consumed the available supply of IPv4 addresses, sites have begun to employ IPv6 addresses in addition to, or instead of, just continuing to use IPv4 addresses. When a host natively uses both IPv4 and IPv6 addresses, this is normally known as being "dual stack."

IPv6 - The "next generation" of Internet addresses and substantially longer than legacy IPv4 addresses (128 bits vs. 32 bits for IPv4). A typical IPv6 address looks like 2001:470:b0::81. Each chunk of an IPv6 address can be up to four hexadecimal digits, and leading zeros within a chunk can be omitted. Chunks are separated by colons, rather than the dots used in IPv4 addresses. Two successive colons are routinely used as shorthand for a run of one or more chunks of all zeros in the middle of an IPv6 address.

ISAC (Information Sharing and Analysis Center) - A nonprofit organization providing a central resource for information on cyber threats to critical infrastructure and two-way sharing of information between the private and public sector. For a list of ISACs: https://en.wikipedia.org/wiki/Information_Sharing_and_Analysis_Center

ISP (Internet Service Provider) - Vendor of Internet access services for home or business customers.

Iterative Query - In iterative queries, the DNS server responds with the best answer it has. In cases where the DNS server doesn't know the answer, it will respond with referrals to other DNS servers until an answer is received or the query fails.

IXFR (Incremental Zone Transfer) - *See "AXFR"*

J

JSON Lines - A convenient format for storing structured data that may be processed one record at a time. See: http://jsonlines.org/

K

Keyloggers - Software or hardware devices that record everything a user types in order to gain access to passwords and other sensitive information.

Knot DNS - Open-source authoritative-only server for the DNS. It is actively developed by CZ.NIC, the .CZ domain registry. https://www.knot-dns.cz/

L

LACNIC (Latin America and Caribbean Network Information Centre) - An international non-government organization established in Uruguay in 2002. LACNIC is responsible for assigning and managing Internet number resources (IPv4, IPv6), Autonomous System Numbers, and Reverse Resolution for the region–more than 8500 network operators providing services in 33 Latin American and Caribbean territories. https://www.lacnic.net

Law Enforcement Agency (LEA) - Sworn criminal LEA with the power to investigate crimes and make arrests. In the US, they are often be trained and certified by FLETEC (https://www.fletc.gov/). Examples include: Federal Bureau of Investigation; Oregon State Police; Lane County Sheriff; Eugene, Oregon Police Department.

Distinguishes criminal law enforcement agencies from civil enforcement agencies such as the FTC, state Attorney General's Offices, etc., who may have different or more limited enforcement powers (such as the ability to impose administrative sanctions or compel changes in business practices).

LEO (Law Enforcement Officer) - Sworn criminal "Law Enforcement Officer" with the power to investigate crimes and make arrests. Distinguish LEOs from non-sworn employees who may work for an LEA and who, while they may do critical work for the agency, do not have sworn status. A representative example of a non-sworn law enforcement employee might be a forensic laboratory specialist.

Localhost - Localhost is the local system's loopback interface. It always has the IPv4 address 127.0.0.1. Only users or programs running on the local system can access that address. This is normally named lo or lo0.

M

MAC Address - A unique address assigned to an Ethernet card at the time of manufacture. No two Ethernet cards in the world should ever have the same MAC address. Used for Ethernet switching purposes and embedded in some types of automatically-configured ("SLAAC") IPv6 addresses.

Malware - Overarching term for unwanted or malicious software (e.g. computer virus, computer worm, Trojan horse program, root kit, adware, spyware, bot, etc.).

Maltego - Proprietary software used for open-source intelligence and forensics, developed by Paterva for timely mining and gathering of information as well as the representation of this information in an easy to understand format.

Metadata - Literally "data about data." For example, a picture taken with a cellphone camera might include metadata such as the type of camera phone that was used to take the picture, the date and time the picture was taken, the geolocation (latitude and longitude) where the picture was taken, etc.

MLAT (Mutual Legal Assistance Treaty) - Pronounced "emLAT," it is a legal framework under which law enforcement agencies agree to formally cooperate on international investigations.

Mtbl - A type of sorted string table. See http://www.caida.org/workshops/isc-caida/1210/slides/isc1210_redmonds.html

MX Record (Mail Exchanger Record) - DNS record that defines where email for a domain should be sent. For example:
farsightsecurity.com. 3600 IN MX 10 mail.fsi.io.

M3AAWG (Messaging, Mobile and Malware Anti Abuse Working Group) - A technology-neutral, non-political working body that systematically focuses on operational issues of Internet abuse including technology, industry collaboration and public policy. See https://www.m3aawg.org/.

N

NANOG (North American Network Operators Group) - A professional association for Internet engineering, architecture and operations. See https://www.nanog.org/.

NCAP - A network capture utility like libpcap (on which it is based) and tcpdump. ncap is used within Farsight Security's SIE to transfer packet traces from sensors to collectors. See https://www.dns-oarc.net/tools/ncap.

Netblock - A range of IP addresses (e.g. 196.25.0.0-196.25.255.255)

NMSG - The NMSG format is an efficient encoding of typed, structured data into payloads which are packed into containers which can be transmitted over the network or stored to disk. Each payload is associated with a specific message schema. Modules implementing a certain message schema along with functionality to convert between binary and presentation formats can be loaded at runtime by libnmsg. See https://archive.farsightsecurity.com/nmsgtool/.

NMSGtool - The command line interface to libnmsg, the reference implementation of the NMSG binary structured message interchange format. Reading or writing data in a non-NMSG format requires the use of an external module (called a "nmsgpb module") to convert to or from NMSG format. nmsgtool selects a nmsgpb module based on a vendor ID and message type. See https://archive.farsightsecurity.com/nmsgtool/.

DNS Dictionary

FARSIGHT SECURITY

NOD (Newly Observed Domains) - Farsight observes millions of domains each day and detects that more than 100,000 of those are newly used from the perspective of the historical DNSDB database. Leveraging more than 2 TB of daily real-time Passive DNS data, NOD discovers newly configured domains when they are first used. This is far lower latency than using other discovery methods such as TLD Zone File Access (which averages 17 hours delay between time-of-registration and visibility in zone file downloads) and can be "gamed" by registering domains and then letting them sit for days or weeks before beginning to actually use them). For a complete description, see https://www.farsightsecurity.com/Services/NOD/

NOERROR - One of several possible status codes returned by a DNS server in response to a query. Commonly seen when a domain successfully resolves, but also when a AAAA record is requested for a domain but that domain isn't doing IPv6.

NSEC (Next-Secure Record) - The NSEC resource record lists two separate things: the next owner name (in the canonical-ordering of the zone) that contains authoritative data or a delegation point NS RRset, and the set of RR types present at the NSEC RR's owner name [RFC3845]. The complete set of NSEC RRs in a zone indicates which authoritative RRsets exist in a zone and form a chain of authoritative owner names in the zone. This information is used to provide authenticated denial of existence for DNS data, as described in [RFC4035]. See here: http://tools.ietf.org/html/rfc4034#section4.

NSEC3 - Similar to NSEC, except it provides authenticated denial of existence for DNS data, while simultaneously also being resistant to zone walking/zone enumeration. A nice discussion of this can be seen here: http://info.menandmice.com/blog/bid/73645/Take-your-DNSSEC-with-a-grain-of-salt.

NSEC3PARAM - A DNSSEC-related record type that specifies the hash algorithm used, how many times the hash algorithm is applied, the salt value for the hash, and whether or not delegations are signed.

NS Record (Name Server Record) - DNS record type defining the authoritative name servers used by a domain. For example:
farsightsecurity.com. 3600 IN NS ns7.dnsmadeeasy.com.
farsightsecurity.com. 3600 IN NS ns5.dnsmadeeasy.com.
farsightsecurity.com. 3600 IN NS ns6.dnsmadeeasy.com.

nTLD (New Top Level Domain) - TLDs are the letters found at the end of an Internet address, such as .com, .net, or .org. Any TLD that does not represent a country, or a territory is known as a generic TLD, or gTLD. The New gTLD Program has enabled hundreds of new top-level domains in ASCII characters and in different scripts (Internationalized Domain Names) to enter into the Internet's root zone since the first delegations occurred in October 2013. https://newgtlds.icann.org/en/about/program

DNS Dictionary

FARSIGHT SECURITY

NXDOMAIN (Non-Existant Domain) - DNS status code returned when a name doesn't exist.

NXDOMAIN Attack - Akin to DDoS attacks in which a large number of clients send queries to resolve non-existent or invalid domains. While the recursive server tries to resolve the non-existing domain, its cache is flooded with NXDOMAIN results.

In the second case, a 3rd party attacker spoofs the source address of the 3rd party victim and floods the recursive resolver with queries that seem to be coming from the targeted 3rd party.

O

OOB (Out Of Band) - A communications channel that doesn't follow an existing path. For example, a dialup modem as a backup to a dedicated Internet line.

P

Packet - Unit of data moved between a source and destination on packet switched networks such as the Internet.

Parked Domain - A domain that's registered but not used for a website or other purpose, repurposed to show paid advertising when a user inadvertently visits the site

Passive DNS - Passive DNS uses observed DNS traffic to build a database detailing relationship between domain names and IP addresses. It provides visibility into how domains and IPs have been used in the past and includes all DNS record types.

The historical data can then be queried to answer questions like:

Which domains have been seen associated with a particular IP or IP range
Which IPs have been seen associated with a particular domain name
What domain names are known to be using a particular name server, etc.
The date and time range associated with the above, etc.
How long has this domain or hostname been unused.

See https://www.farsightsecurity.com/Services/DNSDB/

DNS Dictionary

FARSIGHT SECURITY

PCAP - Packet CAPture library used by tcpdump. http://www.tcpdump.org/

Phishing - Process of attempting to use social engineering to trick users into divulging secrets such as their credit information, the password to their accounts, etc.

PII (Personally Identifiable Information) - While the legal definition of PII varies from jurisdiction to jurisdiction, a representative list can be seen on page 12 of California's "Making Your Privacy Practices Public" (https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf). See also: https://gdpr-info.eu/issues/personal-data/.

Port - Network ports allow a single system to host (deliver) multiple services. For example, port 443 is the port normally used for HTTPS (secure web) servers, port 25 is the port normally used for SMTP (email) servers, and (secure shell) normally runs on port 22. A full list of standard port assignments can be seen here: https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

Can also refer to a program that has been taken from one operating system and modified for use on a new one. ("That code originally ran under Linux, but we ported it to the Mac and Windows, too.")

Promiscuous Mode - Normally, even though a network interface might see traffic for multiple systems, network interfaces are "polite" and only pay attention to their own traffic. Network interface cards can be specially configured, however, to listen to any or all traffic that comes their way, much like a snoopy neighbor on an old "party line" ; telephone. Promiscuous mode is routinely and legitimately used by network engineers for troubleshooting or measurement purposes.

PTR Records (Pointer Records) - Also called "Inverse Address or 'in-addr' Records," PTR Records resolve an IP address to an FQDN (as opposed to A Records which resolves an FQDN to an IP address). For example:

108.14.244.104.in-addr.arpa. 86400 IN PTR web1.iad1.fsi.io.

Private Registration - When registering a domain name, ICANN requires that some of your contact information gets automatically published to the public WHOIS database. Private registration is the option to make your domain name registration information private. Note that with GDPR, it is quite uncommon to see unredacted point of contact data in Whois, even when private/proxy registrations haven't been done.

Proxy Server - A dedicated computer or software system that acts as an intermediary between end users and the websites they browse. When a proxy server is used, your Internet traffic runs through the proxy server, which has a different IP address, to the address you requested. A proxy server can act to minimize repetitive retrievals of highly popular web pages, thereby saving bandwidth. A proxy server can also act as a network control point, filtering disallowed content. Proxy servers can also act as anonymizers, making it more difficult to track who may be accessing particular content.

Python - An interactive programming language, sometimes compared to or contrasted with Perl.

R

Ransomware - A type of malicious software designed to block access to a computer system by encrypting data with a key which is unknown to the victim. Until a sum of money is paid, the victim will not be able to use their system.

Real-Time - As-it-happens.

Recursive Query - Recursive queries are the result of requesting information from a DNS server that is set to query other DNS servers until it gets an answer, or the query fails.

Recursive Resolvers - Computers that respond to user requests by translating a domain name into an IP address. Broadband providers will normally provide recursive resolvers for the use of their customers as part of their service. Recursive resolvers will resolve any domain name, but normally only for their closely limited or well-defined customer base.

Recursive resolvers that will answer queries for any user are normally considered to be misconfigured, and are usually referred to as “open recursive resolvers.” That said, there are a small number of intentionally open and (very carefully operated) recursive resolvers too (e.g. Google’s well known 8.8.4.4 and 8.8.8.8, Cloudflare’s 1.1.1.1, and Global Cyber Alliance’s 9.9.9.9)

RedHat - A popular distribution of the Linux operating system.

Red Team - An independent group that assumes the role of attackers by imitating real-world attacks that can hit an organization and therefore exposing vulnerabilities that pose a threat to the organization’s cybersecurity.

DNS Dictionary

FARSIGHT SECURITY

REFUSED - A response code potentially seen from authoritative name servers. Typically seen when a name server is unwilling to respond to your queries.

Registrant - The entity that owns or holds a domain name.

Registrar - An organization accredited by a gTLD or ccTLD registry that manages the reservation of domain names.

Registry - An organization that manages the administrative data for TLD domains under its authority, including zone file data throughout the Internet. See https://whois.icann.org/en/domain-name-registration-process

Registry Lock - Security measure available at the registry level. Requesting a registry lock will prevent operations such as DNS server modification, domain transfer or deletion, and more. Unlocking requires owner authentication.

Note that both registrar and registry locks are potentially available. In addition to locks created on request as a security measure, a registrar or registry may also lock domains that may be fraudulently registered or otherwise abusive.

Reseller - A third-party company that offers domain name registration services through a registrar but not all are ICANN-accredited registrars. https://www.icann.org/resources/pages/reseller-2013-05-03-en

Response Policy Zones (RPZ DNS) - Sometimes referred to as a "DNS firewall." In a nutshell, when you can identify a domain name associated with Internet badness, RPZ allows you to block local access to those zones. It's another DNS-related innovation from Dr. Paul Vixie, see "Taking Back the DNS" (http://www.circleid.com/posts/20100728_taking_back_the_dns/) and the additional resources here: https://dnsrpz.info/. Farsight Security delivers some content for use with RPZ, such as our "Newly Observed Domains" data feed.

REST (Representational state transfer) - A software architectural style that defines a set of constraints to be used for creating Web services. Web services that conform to the REST architectural style, called RESTful Web services (RWS), provide interoperability between computer systems on the Internet.
See: https://en.wikipedia.org/wiki/Representational_state_transferA

Reverse DNS - See "PTR Records."

RIPE NCC (Réseaux IP Européens Network Coordination Centre) - The Regional Internet Registry for Europe, the Middle East and parts of Central Asia. The RIPE NCC allocates and registers blocks of Internet number resources to Internet service providers (ISPs) and other organizations.

root - 1. apex of the DNS hierarchy, literally "." Often referred to in conjunction with DNSSEC, where for many years DNSSEC deployment was handicapped by the fact that the "root wasn't signed" (thankfully now handled). A list of all approved top level domains (immediately subordinate to the DNS root) can be retrieved from IANA (see: http://data.iana.org/TLD/tlds-alpha-by-domain.txt).

2. The root account on a Unix or Linux host; super user; the sysadmin account; a privileged administrator account endowed with the ability to run any command or access any users' files, etc.

Rootkit - A collection of computer software that can modify the OS to make a backdoor.
See: https://en.wikipedia.org/wiki/Rootkit

Root Servers - Name servers for the root zone of the DNS (aka "dot"). https://www.iana.org/domains/root/servers

RRset - A set of DNS resource records of the same name, class, and type. For example, a server that is doing load balancing via DNS might have two, three, or even more A records for a given fully qualified domain name. (see https://www.ietf.org/rfc/rfc2136.txt just above section 1.1) For example:
www.google.com. 300 IN A 74.125.227.145
www.google.com. 300 IN A 74.125.227.148
www.google.com. 300 IN A 74.125.227.146
www.google.com. 300 IN A 74.125.227.144
www.google.com. 300 IN A 74.125.227.147

RRsig - DNSSEC uses public key cryptography to sign and authenticate DNS resource record sets (RRsets). Digital signatures are stored in RRSIG resource records and are used in the DNSSEC authentication process described in [RFC4035]. A validator can use these RRSIG RRs to authenticate RRsets from the zone." See http://tools.ietf.org/html/rfc4034#section3.

RRtype - DNS Resource Record types are described here: http://tools.ietf.org/html/rfc6895#section3.1.

S

Scanning - The use of automated tools to check wide swaths of IP address space, often looking for a particular misconfiguration or vulnerability, or as reconnaissance prior to a cyber attack. Popular examples of scanning tools: nmap (http://nmap.org/) and zmap (https://zmap.io/).

DNS Dictionary

FARSIGHT SECURITY

Scout - The DNSDB plugin for Chrome and Firefox.

Secondary DNS - At setup, a server administrator can designate a DNS server as primary or secondary. Primary servers are the trusted authority for important information, such as the IP address of the domain. Secondary servers get their info from a primary server via a zone transfer. Secondary servers retain read-only copies of the zone file and cannot accommodate changes to a zone's DNS records (unlike primary servers).

Security Information Exchange (SIE) - A central data sharing environment where subscribers access security data feeds, organized as "channels." See https://www.farsightsecurity.com/Services/SIE/.

Security Operations Center (SOC) - Similar to a network operations center but focused around handling security incidents rather than managing networks.

Sensor - In Farsight Security's case, a data collection node. See https://archive.farsightsecurity.com/Passive_DNS_Sensor_FAQ/.

Server - In a client/server architecture, the system to which clients connect. Common usage, "web server," "mail server," "database server," etc.

Server hardware is often optimized for demanding workloads (many processors, lots of memory, fast network interface cards, etc.), high reliability (redundant power supplies, redundant cooling fans, mirrored disks, etc.), or efficient installation and management at scale (rack mount configuration, remote "lights out" management capabilities, etc.).

SERVFAIL (Server Failure) - DNS server response code indicating the name server was unable to process this query due to a problem with the name server.

SIEM (Security Information and Event Management) - Software products and services that combine security information management and security event management to provide real-time analysis of security alerts generated by applications and network hardware.

DNS Dictionary

FARSIGHT SECURITY

Sinkhole - When a botnet command and control host is taken over by the authorities or by a security researcher, communications from botted hosts may be redirected to a replacement system controlled by the authorities (or the researcher). That "sinkhole" host is often heavily instrumented, and may be used to identify hosts that need cleaning, or to characterize the size of the botnet taken over, etc.

An example of a sinkhole is the Conficker Working Group (CWG) sinkhole.

SMTP (Simple Mail Transfer Protocol) - Communication protocol for email transport. https://tools.ietf.org/html/rfc5321

SOA Record (Start of Authority Record) - A resource record indicating which DNS server is the best source of information for the specified domain. They define the various TTLs, the responsible managing party, and master DNS server for that domain. See https://www.ietf.org/rfc/rfc1035.txt at 3.3.13

Source Port Randomization - Partial mitigation for one class of DNS cache poisoning attacks. See https://www.dnso-arc.net/oarc/services/porttest.

Spam - While spam is often defined differently by different national regulatory regimes, some organizations (such as M3AAWG) define it as "abusive email;" another simple definition is "email you don't want and didn't ask to receive." Typically, 80 to 90% of all email is spam. Channel 25 on the Farsight Security SIE is devoted to sharing spam received by spam traps.

Spam Trap - Accounts that are not being actively used, and thus should normally not receive any email. For example: someone registers a brand-new domain and creates several thousand new email accounts on that domain, and then just waits to see what (if anything) gets sent to those accounts. Those email accounts should not normally receive email — any email sent to those accounts is virtually certain to be spam. See for example Project Honeypot (https://www.projecthoneypot.org/statistics.php).

Spearphishing - A type of cyberattack narrowly focused on social engineering a particular targeted group or individual. To increase the likelihood that a victim falls for the scam (e.g. opens an email and downloads a malicious payload or submits a wire transaction), attackers often research their targets for important details to create more tailored and plausible messaging.

SPF Record (Sender Policy Framework Record) - Published to the DNS, these records indicate which IP addresses are authorized to originate email on behalf of a domain.

SPOF (Single Point of Failure) - A critical component, the failure of which will cause a system failure. Redundancy is a common approach to eliminating SPOFs and building resilience.

Spyware - Unwanted software that hides on your device, collecting data and sensitive information to send back to the hacker.

SRAtool - One component of Farsight Security's SRA, enabling remote access to the Security Information Exchange (SIE). Sratool is intended to be used for exploratory debugging or familiarization, enabling cost efficient remote access to all but the most high-volume channels at the SIE. See https://www.farsightsecurity.com/Services/SRA/.

SRAtunnel - The other main component of FSI SRA, meant for production deployment. See https://www.farsightsecurity.com/Services/SRA/.

SRV Record - Defines the hostname/port location of specified services.

SSD (Solid State Disk) - Flash-based storage media for servers; these drives tend to be significantly faster than traditional spinning disks (but not as fast as NVMe storage).

SSH (Secure Shell) - Encrypted replacement for telnet, allowing remote command line terminal sessions. SSH also provides the basis for other secure protocols such as sftp and scp, and the secure tunnels as used by Farsight Security for SRA. One popular implementation of SSH is the one from OpenSSH (http://www.openssh.com/).

SSH Pre-shared Keys - While many users are accustomed to authenticating with a username and password, SSH can also use public key cryptography for authentication. In this mechanism, users create a public/private key pair with the command:

$ ssh-keygen -t rsa -b 4096

Users then provide a copy of their freely shareable ssh public key to the site they wish to access.

If the site installs that key when they subsequently connect with that site, their possession of the corresponding private key is used as proof that they should be allowed to log in. Access to the user's private key on their personal laptop or workstation can be (and should be) locally protected with a password.

SSL (Secure Socket Layer) - Now obsolete and replaced by TLS, see below.

su (Superuser) - Unix "super user" command, enables a regular user to become "root." Sniffing network traffic in promiscuous mode typically requires the user to su to root.

Subdomain - Domain names are often hierarchical. For example, a university might have subdomains for various departments, such as the Chemistry Department, the Math Department, and the Physics Department, with names such as www.chem.example.edu, printer.math.example.edu, and projector.phys.example.edu. Subdomains may be centrally managed or delegated. For example, administration of chem.example.edu might be handled by a central IT organization or the Chemistry department itself.

sudo (Superuser Do) - Unix command that enables users to run programs with the security privileges of another user, by default the superuser (see above).

Sunrise Period - A minimum 30-day period before domain names become available to the public for trademark holders to register domain names that correspond to their trademarks.

T

TCP (Transmission Control Protocol) - Core connection-oriented protocol that carries web traffic, email traffic, and traffic for numerous other popular applications over the Internet. Contrast with UDP, below.

tcpdump - Network packet analyzer application. See http://www.tcpdump.org/.

Terminal - Before web graphical user applications became common, computing was often done via commands typed in at the command line prompt on a "terminal." One widely used model of terminal was the Digital Equipment VT100 family. These days, VT100 terminal emulation applications are run in software under Microsoft Windows or on Macs running OS X, while on Linux and BSD systems running X Windows, xterm is the most commonly used terminal app.

Thick Registry - Registries that hold all contact information required for the domain names.

DNS Dictionary

FARSIGHT SECURITY

Thin Registry - A thin registry holds only referral information while the domain contact information is actually held by the registrar.

TLD (Top Level Domain) - The final portion of a domain name that immediately follows the “dot” symbol. Examples of TLDs include .com, .org, and .net.

TLD Servers (Top Level Domain Servers) - DNS servers that maintain information for all domain names with a common domain extension, such as .com. In this example, the .com servers know how to get to the servers for each .com delegation point. However, they won’t know about all .com FQDNs themselves.

TLS (Transport Layer Security) - The protocol that’s used to encrypt web sessions, or to encrypt email traffic in transit between mail servers.

TLSA - DNS record type used in conjunction with DANE. See https://tools.ietf.org/html/rfc6698.

Trojan Horse - Malware disguised as legitimate software, Trojans can be employed by cybercriminals to access a user’s system. Trojans vary from a virus because they attach to non-executable files such as image or audio files. Once activated, they allow cybercriminals to spy on the user, steal sensitive data, and gain backdoor access to their system.

TSIG (Transaction Signature) - A computer networking protocol used by the DNS to authenticate updates to a dynamic DNS database. The TSIG protocol uses shared secret keys and one way hashing to securely authenticate that updates and responses are coming from approved endpoints. https://tools.ietf.org/id/draft-dupont-dnsop-rfc2845bis-01.html

TTL (Time to Live)

1. DNS TTL - time (in seconds) that DNS responses are cached (remembered) in a recursive resolver. By caching records, load on authoritative name servers can be reduced, and brief outages easily handled. On the other hand, if TTLs are set to be too long, flexibility may be lost, and sites may find that they need to patiently wait while long TTLs expire before they can make urgently needed changes to their DNS configurations, and have them noticed by the Internet. http://dnscheck.iis.se/ is an example of a free site that will review a domain’s name server TTL records and offer recommendations if TTL values are missed.

2. IP TTL - when packets are transmitted over the Internet, they start with a TTL value, which may be 64, 128, or even 255. As that packet is routed hop by hop across the Internet, the TTL value gets decremented by one at each hop. If a packet eventually has a TTL of zero, it’s dropped, and an error is returned to the sender.

TXT Record (Text Record) - Unlike A or AAAA records that are used to map domains to IP addresses, TXT records contain text. They may be used to record information about a host, or as a way of creating a generic database in the DNS.

U

UDP (User Datagram Protocol) - Lightweight connectionless protocol used to "send and forget" traffic including DNS and some types of network video. Connectionless (in contrast with TCP), so more efficient and able to scale better, but because it does not require a three-way handshake, it was subject to spoofing. Unlike better-mannered TCP, it is congestion-insensitive.

UDRP (Uniform Domain-Name Dispute Resolution Policy) - A process established by ICANN for resolution of disputes over the registration and use of Internet domain names. https://www.icann.org/resources/pages/policy-2012-02-25-en

Unbound - Popular name server written and maintained by NLnet Labs. See https://unbound.net/.

Unicast Name servers - Non-anycast, "normal" name servers. A given name server will be on a unique IP address, rather than using an IP that's part of a network block that's announced from multiple locations.

URI (Uniform Resource Identifier) - A sequence of characters identifying a resource on a computer network. All URLs (see below) are URIs, but not all URIs are URLs. https://danielmiessler.com/study/url-uri/

URL (Uniform Resource Locator) - A web address, such as https://www.farsightsecurity.com/

V

Virus - A type of malicious code created to spread from system to system with the purpose of modifying or deleting data. A virus works by attaching itself to legitimate executable code. Opening the file can trigger the virus. Once a virus is active, it will infect other programs on the computer.

VLAN (Virtual LAN) - Allows an Ethernet switch to be logically partitioned into multiple virtual switches, among other things.

VoIP (Voice Over IP) - Telephony services using the Internet rather than phone lines.

W

wdns - Low-level DNS library. It contains a fast DNS message parser and various utility functions for manipulating wire-format DNS data. See https://github.com/farsightsec/wdns.

Whitelist - Opposite of a block list. A whitelist lists sites that should NEVER be blocked, typically because collateral damage would be severe. Examples might include Google, Microsoft, Apple, Comcast, CenturyLink, Amazon, eBay/Paypal, etc.

White Hat - Authorized security specialists who test computer systems for security holes via hacking so that they can be fixed.

WHOIS - Online service that tells “who is” using a given domain name or number resource.

WIPO (World Intellectual Property Organization) - A United Nations agency that oversees intellectual property services, policy, information and cooperation. https://www.wipo.int

Worms - Self-replicating malware (and virus) that moves quickly from one computer to another by exploiting network vulnerabilities. When a worm infects a host, it can quickly consume all bandwidth, interrupting and arresting large network and web servers.

Y

Yum - Software for serving Redhat Packages.

DNS Dictionary

FARSIGHT SECURITY

Z

Zone - Chunk of the DNS managed by one individual (or group). For example, farsightsecurity.com might be one DNS zone, as might dnsdb.info

Zone File - A structured text file, stored in a name server, that contains the records for every domain in that particular zone.

#

0mq ("zero mq") - An embeddable networking library and messaging framework for distributed or concurrent applications. See http://zguide.zeromq.org/page:all

301 Redirect - A permanent redirect from one URL to another. It primarily helps search engines locate the correct page. According to search engines, a URL like "http://example.com" looks completely different from "http://www.example.com." A 301 redirect can associate common web conventions like this (i.e. "http://," "www.," etc.) and link them to the correct address.

302 Redirect - A temporary redirect from one URL to another. Unlike, 301 redirects which are permanent, 302 redirects only send users to a new page for a short time or until the original page can once again be used.

404 Error - An HTTP standard response code, a 404 error indicates the client successfully communicated with a given server, but the server was not able to locate the requested page. 404 errors typically occur when the visitor uses an incorrect URL, or the page was removed.

+1-650-489-7919
info@farsightsecurity.com
Farsight Security, Inc.
177 Bovet Rd Ste 180
San Mateo, CA 94402 USA
www.farsightsecurity.com