abusix

Abusix Guardian Intel

Detailed Overview & Breakdown of Abusix Data

OVERVIEW

Today's attack surfaces are broad. Email, in particular, continues to be one of the most utilized surfaces by malicious actors. To help combat threats, Abusix has developed Guardian Intel.

Abusix Guardian Intel offers a unique approach to traditional Threat Intelligence (TI). Abusix's data is derived from our positioning within the Email protection space for major Internet Service Providers and Telecommunications companies. Within the TI data provided, customers will see unique IOC data regarding several known nefarious attack vectors that Abusix has developed due to our proprietary methodologies.

With most TI data being provided from the lens of the endpoint, Guardian Intel is unique to the mail space and provides preemptive discovery of the attack surface. IOC Data Points included in Guardian Intel are:

- IP data of known Malicious Infrastructure
- Hashes of Attachments received in Spam, Malware, and Phishing emails
- Bitcoin Wallets
- Malicious and Spam Domains
- Authentication (SSH/SMTP AUTH) Abuse
- URL Shortener and Drive URL hashes

With Guardian Intel, Abusix recommends utilizing the IOC data in infrastructure protection (Edge Firewalls and Endpoint), threat hunting, and SIEM/XDR alert augmentation.

Guardian Intel feeds include...

1. Black List (Blocking Recommended)

IP Feed	Domain Feed	URL & Host-name Feed	Attachment Feed	Email Address Feed	Bitcoin Wallet Feed
Spam Sources	Trapped URLs	Trapped Short-ened URLs	Malicious Attach-ments (SHA-1) Hashes	Spam Sources	Wallet Addresses (In Malicious Messages)
Nearby Spam Sources	Redirector Domains	Honeypot Hits			
Compromised Hosts	Trapped Affiliates				
Addresses using our Fake Proxies					
Honeypot Hits					
Spoofing trap IPs					

2. Grey List (Analysis Recommended)

IP Feed	Domain Feed	URL & Host-name Feed	Attachment Feed	Email Address Feed	Bitcoin Wallet Feed
Invalid Return Path	High Volume Senders	Messaging Service URLs		Dropboxes	Wallet Addresses
Web Signatures	Newly Observed Domains	Google Docs URLs			
High Volume Senders	Parked Domains	Drive URLs			
Newly Observed	SPF +all				
PHP Access	Proxy Traffic				
Proxy Traffic					

Black List Source and Data Descriptions:

Attachments Feed

Sources: spam traps and blackhole.mx service

Streams: `streams.attachments.*` `streams.abusix.attachments.potentially-malicious`

Description: Malicious attachments are seen in our spam traps and blackhole service.
Potential-Malicious stream calculates the SHA-1 hash of the binary data.
The `streams.attachment.*` streams ONLY provide the binary data's raw base64 with no other metadata.

IP Addresses: Spam Sources

Sources: spam traps and blackhole.mx service

Streams: `internal.email.pre_data.`

Description: This is a list of IP addresses abusing our infrastructure:

- Attempting to use our SMTP servers as an open relay.
- Using SMTP AUTH credentials to send email through our SMTP server.
- Using our “fake” HTTP/SOCKS proxies to attempt to send mail via SMTP.

OR

- IP is trying to send messages to our spam traps.
  - Only messages hitting our “pristine” spam traps are routinely listed.
  - Messages sent to other non-pristine spam traps are only added if they are “spoofing” our trap domains in some way or are using some “well-known” spam tools to send the message.

We exclude Challenge/Response spam filter messages, Mailing List administrative messages, Bounce Messages, and Auto-Responses/Auto-Replies like Out-of-Office or Opt-In confirmations.

IP Addresses: Spam Sources nearby

Sources: spam traps and blackhole.mx service

Streams: `internal.email.pre_data`

Description: This looks explicitly for IPs hitting non-pristine spam traps, where we have pristine IP listings in the same /24 network. If this happens, we allow the non-pristine spam traps to cause a listing, as it’s either a lousy network or spam-related to someone spreading their email traffic amongst many IP addresses.

Bitcoin Wallet Addresses

Sources: spam traps and blackhole.mx service

Streams: `streams.attachments.*` `streams.abusix.attachments.potentially-malicious`

Description: We look for Bitcoin wallets in incoming messages; anything found in pristine trap messages is listed immediately. We track the Bitcoin Wallet addresses, and if we see an address being sent to non-pristine spam traps but from 2 or more different /24s, then this is also listed.

Domain Names

Sources: spam traps and blackhole.mx service

Streams: `internal.email.urls`

Description: This looks at domain names being seen sent to spam traps and includes unshortened URLs (where this is possible). Any domains found in messages to pristine spam traps are included. We only list domains found in messages sent to non-pristine sources if we see other spam or phishing indicators or deliberate obfuscation of URLs using Google AMP, open web redirectors, etc.

All domains are masked against the Tranco Top 1m domains, except when we have exceptions sub-domains. e.g. services like [`onmicrosoft.com`](http://onmicrosoft.com) which provide a sub-domain per tenant.

Redirector Domains

Sources: spam traps and blackhole.mx service

Streams: `internal.email.urls`

Description: This looks for domains with some open redirection, as spam and phishing heavily abuse these to obfuscate and hide the domains hosting relevant content.

Domains seen using Affiliate Links

Sources: spam traps and blackhole.mx domains

Streams: `internal.email.urls`

Description: Affiliate marketing programs are familiar sources of spam, and it's easy for someone to outsource the spamming to someone else and then claim it's not their fault because an affiliate did the spamming.

This looks for URLs containing affiliate identifiers `aff_id` or `aff_i` and lists the associated domain names.

Short URLs

Sources: spam traps and blackhole.mx domains

Streams: `internal.email.urls`

Description: This looks for Short URLs, which are commonly used to hide the actual URLs of spam/phishing/malware, as it makes it much harder for security gateways to follow these links to their ultimate destination and causes additional complexity to resolve the destination and to check it against domain blocklists..

Email Addresses: Spam Sources

Sources: spam traps and blackhole.mx domains

Streams: `internal.email.pre_data`

Description: This list includes email addresses that we have seen originating spam where we know the address has not been forged or are the destination addresses for replies to received spam.

IP Addresses: Compromised or Infected Hosts

Sources: all inputs

Streams: `incoming-streams.ami.post_metadata`

Description: This looks for behavior of SMTP clients that indicates they are compromised or infected in some way. Specifically, we're looking for behavior that a genuine SMTP server/client would never do. Including:

- Connecting and sending SMTP AUTH to our SMTP servers, but not injecting any mail.
- Sending HELO/EHLO that we know to be bogus (or using our domains/IPs).
- Use a return path that is our domain.
- Change their HELO/EHLO domain identity frequently.
- Send unqualified HELOs (e.g., not a domain or hostname).
- Identity as an MUA, but no Received headers are present.
- Use an IP-Literal as a HELO and a return path that fails SPF.
- Authenticates to our trap network using SMTP AUTH.

IP Addresses: Using our Fake Proxies

Sources: HTTP/SOCKS proxy honeypots

Streams: `incoming-streams.fake_proxy_traffic`

Description: This lists all IPs connecting to our fake proxy honeypots, irrespective of the destination ports.

IP Addresses: Accessing our T-Pot Honeypots

Sources: T-Pot Honeypot infrastructure

Streams: `data_channels_eu-central-1_nifi_honeypot_all`

Description: We have our version of T-Pot: https://github.com/telekom-security/tpotce, which reports data into our infrastructure; the IP addresses of hosts accessing these honeypots are then stored.

IP Addresses: Spoofing our trap domains

Sources: T-Pot Honeypot infrastructure

Streams: `data_channels_eu-central-1_nifi_honeypot_all`

Description: Through a special `includes:` SPF record containing SPF macros and a custom DNS server, we can see a real-time view of all IP addresses sending mail from one of our spam trap domains.

IP Addresses: Accessing our Cowrie SSH/Telnet honeypots

Sources: cowrie honeypots

Streams: `incoming-streams.abusix.ssh`

Description: We record hosts that access our Telnet/SSH honeypots, run commands, and perform actions. This is also recorded if a command is run to access external hosts by IP, e.g., curl/wget to download malware.

Hostnames: Being used to download something onto Cowrie SSH/Telnet honeypots

Sources: cowrie honeypots

Streams: `incoming-streams.abusix.ssh`

Description: The hostname is recorded here if someone uses the Cowrie honeypots to download something (e.g., malware) onto the honeypot.

Grey List Source and Data Descriptions:

Email Addresses: Dropboxes

Sources: SMTP infrastructure (using all trap domains)

Streams: `internal.email.smtp-auth-abuse`

Description: These are the recipient addresses used by malicious actors who abuse our SMTP infrastructure to relay email through our platform. Typically, the actor will send SMTP AUTH credentials and attempt to send a message to an email address under their control, which contains the details and credentials used to send the message (e.g., host, port, authentication type, along with the credentials).

IP Addresses: Sending mail with invalid return-path domains

Sources: spam traps and SMTP transaction feeds.

Streams: `internal.email.pre_data` `incoming-streams.realtime_smtp_transactions`

Description: We are looking specifically for hosts sending mail that contains invalid return paths. For example, a message has an SMTP MAIL FROM with a hostname/domain label that returns a DNS NXDOMAIN or is invalid, e.g., the IP address is an RFC1918 address, or the MX record points to a domain that doesn't exist.

We limit this to return-path domains that match the organizational domain of the IP address's rDNS; otherwise, this can cause excessive listings for poorly configured hosting platforms that do not have sufficient checks for this case outbound.

Invalid return paths are bad because they "hide" issues from the sender (because this is the address to which bounces are sent). Message bouncing on delivery will cause problems for the recipient postmaster. And they are generally dangerous; if someone starts making exceptions for invalid return paths, those domains are extremely easy to Phish.

IP Addresses: Web Signatures

Sources: spam traps, SMTP transaction feeds, real-time lookups (on Portal), real-time delists, and real-time expiry events.

Streams: `internal.email.pre_data` `incoming-streams.realtime_smtp_transactions` `amiEvents.lookup` `amiEvents.expire` `amiEvents.delist`

Description: We look for IPs with open ports 80 and/or 443 and normalize and hash the HTML on any open ports. If the computed hash matches our list OR the content matches some regular expressions, then we list the IP.

Bitcoin Wallet Addresses

Sources: spam traps and blackhole.mx domains

Streams: `internal.email.cryptocurrencies`

Description: We look for Bitcoin wallets in incoming messages; anything found in pristine trap messages is listed immediately. We track the Bitcoin Wallet addresses, and if we see an address being sent to non-pristine spam traps but from 2 or more different /24s, then this is also listed.

Messaging Service URLs

Sources: spam traps and blackhole.mx domains

Streams: `internal.email.urls`

Description: This looks for the following messaging service URLs:

- t.me
- telegra.ph
- telegram.me
- api.whatsapp.com

Google Docs URLs

Sources: spam traps and blackhole.mx domains

Streams: `internal.email.urls`

Description: This looks for Google Docs or Google Forms URLs currently being used to hide the destination URLs of spam, phishing, and malware.

Drive Service URLs

Sources: spam traps and blackhole.mx domains

Streams: `internal.email.urls`

Description: This looks for URLs from drive services commonly used to store Phishing/Malware.:

- Google Drive
- Yandex Disk
- Microsoft OneDrive
- Amazon S3
- IPFS
- Google Firebase
- DigitalOcean Spaces
- Azure Blob Storage

IP Addresses: High Volume

Sources: spam traps, blackhole.mx domains and SMTP transaction feeds

Streams: `incoming-streams.ami.new_high_volume_ip`

Description: IP addresses sending high volumes of SMTP transactions (> 30 transactions/sec).

Domains: High Volume

Sources: spam traps, blackhole.mx domains and SMTP transaction feeds

Streams: `incoming-streams.ami.new_high_volume_ip_domain`

Description: Domain and associated IP sending high volumes of SMTP transactions (> 30 transactions/sec).

IP Addresses: High Volume Composite

Sources: spam traps, blackhole.mx domains and SMTP transaction feeds

Streams: `incoming-streams.ami.new_high_volume_ip_domain`

Description: This combines high-volume sending with other factors to determine if the sending IP is terrible; this includes:

- Newly observed IP (e.g., new IP sending SMTP traffic for the first time).
- IP in a range handled by "Bad" abuse contact (e.g., the registered abuse address is FreeMail).
- The domain associated with the IP is "Parked" by the registrar.
- Domain is newly observed.
- IP and domain are "all-in-one," e.g., A, NS, MX all point to the *same* IP or sending mail for a domain with a +all modifier.

Domains: Newly Observed

Sources: all inputs (spam traps, blackhole.mx domains, SMTP transaction feeds)

Description: These domains only pertain to email context. A third party receives this data and uses its passive DNS replication sensors and data to output a list of domains when first seen being used on the Internet (*not* first registered).

IP Addresses: Newly Observed Composite

Sources: all inputs (spam traps, blackhole.mx domains, SMTP transaction feeds)

Description: This looks for newly observed IPs that also exhibit other behaviors to raise confidence in blocklisting them for email uses only:

- Immediately high volume of traffic (no warm-up).
- Hitting recycled/blackhole spam traps.
- Sending messages to non-existent domains.
- Sending messages to competitor's trap domains.
- Sending messages with SPF failures.
- Sending messages from parked domains.

Domains: Parked

Sources: all inputs (spam traps, blackhole.mx domains, SMTP transaction feeds)

Description: This looks for domains parked at their registrar's primary hosting provider (e.g., Namecheap, GoDaddy, etc.), but we see them used as HELO and rDNS for hosts injecting mail.

Domains: SPF +all

Sources: spam traps, blackhole.mx domains, SMTP transaction feeds

Description: Domains that specify +all in their SPF record allow *anyone* to send mail on their behalf and have no real-world use because it's impossible to tell the difference between other SPF mechanisms setting the Pass value or the +all modifier matching the record. Because of this, these domains are typically targeted for use in spam/phishing/malware.

IP Addresses: High Volume Composite

Sources: spam traps, blackhole.mx domains

Streams: `internal.email.pre_data.`

Description: Most hosted PHP systems will set `X-PHP-Script` and `X-PHP-Source` headers, which state the path of the executed PHP script, the UNIX UID/GID of the user running the script, and the IP address of the HTTP client accessing it.

We store the IP addresses of these HTTP clients as they perform actions that cause email messages to hit our spam traps. These clients usually abuse web forms, run compromised WordPress code, etc.

Proxy Traffic (Capability Arriving in Q4 2024)

Description: This is a general note about the HTTP/SOCKS proxy traffic. Only 25/TCP and 587/TCP traffic is intercepted and redirected to the spam trap SMTP infrastructure. While recording things like the IPs hitting the proxies, we also intercept other ports (or record destination port activity) and redirect port 22 to our T-Pot or Cowrie honeypots.

Contact us to learn more about Abusix Guardian Intel

sales@abusix.com www.abusix.com