Know Your Foe

Threat Infrastructure Analysis Pitfalls

Who Are We?

- Founders of PassiveTotal
- Analysts/researchers with 10+ years of collective experience

- Interested in
  - Better UX/UI for security systems
  - Improving/re-thinking analyst workflows
  - Imparting our knowledge

1.
Analysis Background

What's the threat research process?

Threat Analysis Lifecycle

- Signatures and monitors
- In-house data collection and analysis
- Proactive research to identify threats
- Paid feeds of data and threat intelligence

Threat Analysis Lifecycle

- Collect data from all OSINT sources
- Pay for analysis or data feeds from providers
- Preserve any relevant activity for the case
- Contact private research groups or networks

Threat Analysis Lifecycle

- Aggregate enough data to derive the full picture
- Consult multiple sources and weight opinions
- Use subject matter expertise to determine good or bad

Tell Me About “youtubee.xyz”

- Resolves to 185.86.167.27
- Geolocation of Turkey
- Active since June 1st 2015
- Uses Ideal Hosting as a provider
- Known malware associated with domain and IP
- WHOIS information is privacy protected
- Labeled as phishing on blacklist
- Uses AS29262
- Part of /24 subnet on 185.86.167.0/24
- Domain is not dynamic DNS
- IP address is not a sinkhole
- Large amount of associations to IP

2. Common Pitfalls

Avoid weak connections and false conclusions

Connections using Subnets.

Subnets are network allocations given to potential businesses or organizations to host Internet-facing infrastructure.

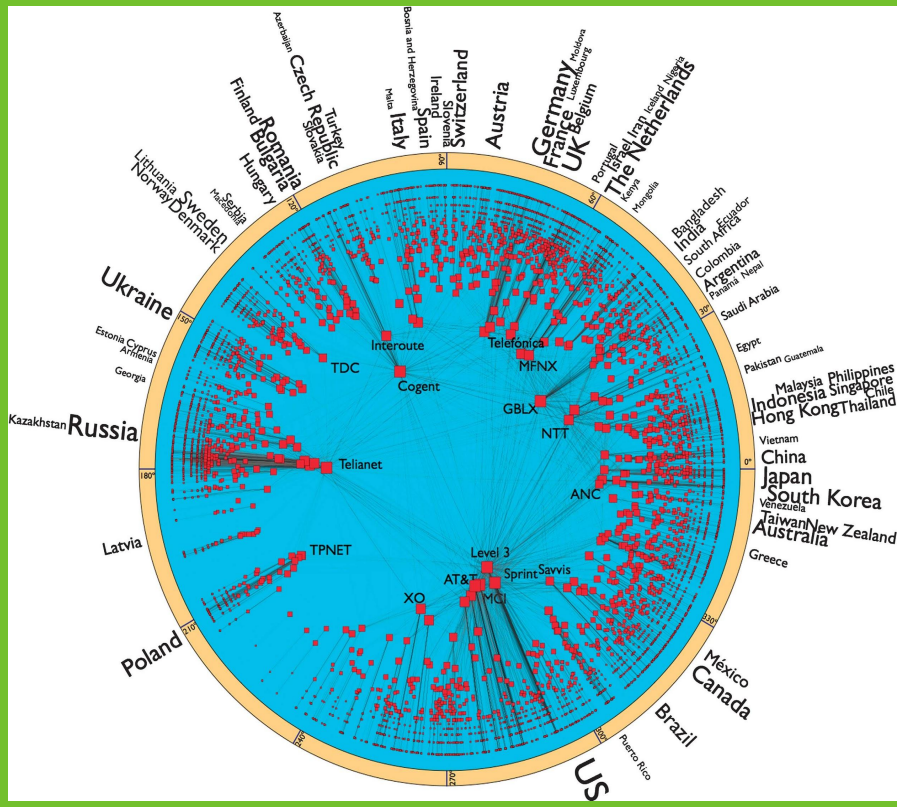
Example: 185.86.167.27 is part of 185.86.167.0/24

Pitfalls with Subnets

- Subnet sizes could include thousands of potential addresses
- Allocations are not clearly delegated
  - Who owns the allocation?
  - Is it being resold?
- Contiguous block of addresses may have no relation to each other
- **Medium-to-low connection value**

Connections using AS.

Autonomous systems advertise subnets on the Internet and link through peering agreements using routing protocols.



Example: 185.86.167.27 is part of AS29262

#knowyourfoe | @PassiveTotal

Pitfalls with Autonomous Systems

- Similar to subnets only larger (100,000s)
- AS name may not reflect the true operator of the network
- Subject to influence and disruption (BGP hijacking, DDoS)
- **Low connection value**

Connections using WHOIS.

WHOIS is a protocol that lets anyone query for information about a domain, IP address or subnet.

Example: youtubee.xyz WHOIS reveals little

Pitfalls with WHOIS

- Data is easily faked and not verified by a central registry
- Privacy protect services obfuscate real data
- Domains change owners over time
- Direct data match does not imply connection
- **Medium connection value**

Connections using Dynamic DNS.

Dynamic DNS provides an alternative to the traditional process of managing DNS records for infrastructure that frequently changes IP addresses.

Example: youtubee.xyz is not using dynamic DNS

Pitfalls with Dynamic DNS

- Freely available or extremely cheap
- Difficult to derive ownership or usage time
- Mimics semantics of a real domain
- Thousands of possible combinations
- **Medium-to-low connection value**

Connections using Sinkholes.

Sinkholes are tools used by defenders to redirect traffic destined to malicious resources in order to identify victims and avoid future compromises.

Example: 185.86.167.27 is not a sinkhole

Pitfalls with Sinkholes

- No single registry of sinkhole information
- May appear to connect unrelated infrastructure
- Could be mistaken for hosting provider
- Skews time of operations
- **Low connection value**

Connections using Hosting Providers.

Hosting providers like content delivery networks, web hosting and virtual private servers make the Internet run.

Example: 185.86.167.27 is part of iDeal Hosting in Turkey

Pitfalls with Hosting Providers

- Associates a lot of activity into one place
- Potentially obfuscates the true source of a destination
- Could easily be re-used due to resource constraints
- Comes with numerous defaults
- **Low connection value**

Avoiding Pitfalls

- Use analyst systems that allow for feedback and automated collection
- Create a checklist of items to lookout for
  - Known sinkholes, dynamic DNS providers, hosting providers, etc.
- Validate conclusions with multiple data points

3.

PassiveTotal to the Rescue

A platform created for analysts, by analysts

Core Platform Features

Multiple Sources

Deduplicated data from the major passive DNS sources into one common format.

Detailed Enrichment

Enrichment data including WHOIS, malware samples, SSL certificates, Geolocation and more.

Visual Indicators

Rich tags and visualizations that quickly provide key facts about the queried results.

Persisted Research

Simple feedback loops through classifications and analyst tagging.

BULK UPLOAD | MY ACCOUNT | LOGOUT

PASSIVE TOTAL

ENTERPRISE API LEARN BLOG

Search for a domain, IP or tag...

Focus	185.86.167.27
First Seen	2015-05-31 04:29:41
Last Seen	2015-08-26 21:06:06
Resolutions	1674
Network	185.86.167.0/24
ASN	29262 (IDEALHOSTING)
Country	N/A
Ever Compromised?	true false
Sinkhole	true false
Classify	t c m b
Monitor	

Tags

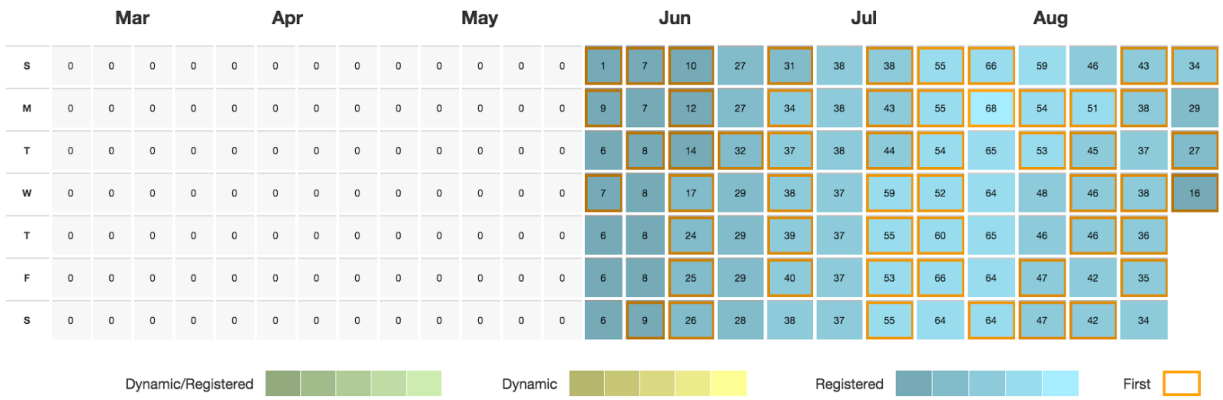
routergate idealhosting malware watching active

Add tag... +

Unique

copy

Heatmap Certificate Potential Malware 4



	Resolve	First	Last	Source	Tags
☐	friends.kim	2015-07-25 22:21:16	2015-08-26 21:06:06	mnemonic	bepush
☐	orgads.com	2015-08-25 01:38:54	2015-08-26 19:08:30	mnemonic	bepush ✖
☐	birakingelsin.xyz	2015-08-25 21:34:47	2015-08-26 18:28:09	mnemonic	bepush ✖
☐	youtubee.xyz	2015-06-01 05:38:15	2015-08-26 18:22:36	mnemonic	bepush
☐	winstonred.com	2015-08-26 17:59:22	2015-08-26 17:59:22	mnemonic	bepush
☐	specialvideosx.attorney	2015-07-03 08:30:08	2015-08-26 17:24:18	mnemonic	bepush
☐	snredtti.business	2015-07-15 16:19:32	2015-08-26 17:00:09	mnemonic	bepush
☐	staticedl.click	2015-06-18 14:44:26	2015-08-26 16:48:25	mnemonic	bepush
☐	hdresimler2.com	2015-08-26 16:41:14	2015-08-26 16:41:14	mnemonic	bepush ✖

Thanks!

Any questions?

Steve Ginty
steve@passivetotal.org
Brandon Dixon
brandon@passivetotal.org