[BONUS EDITION]

Alphathreat Soup

Burning Actors with Data

$whoami: Brandon Dixon

- **VP of Product for RiskIQ**
- Co-Founder and Developer of PassiveTotal
- Espionage researcher since 2010-Present
- Creator of numerous tools and projects
  - Blockade.IO - block threats in the browser
  - PDF X-RAY - analyze PDF files
  - HyperTotal - submitter profiling in Virustotal
  - NinjaJobs - cybersecurity job board
- Coffee Roaster
  - Find me later if you want to geek out

The ABCs of Data.

Attackers Can’t Avoid the Internet

1. Actions on the Internet emit signals
2. Signals are ephemeral and go unnoticed unless someone’s listening
3. Captured signals can expose stages/elements/infrastructure of an attack
4. Exposed elements can destroy operations or render them less effective
5. Destroyed operations is money wasted

Attackers Can’t Avoid the Internet

Attackers Can’t Avoid the Internet

- IP addresses
- Network blocks
- Autonomous systems
- Internet service (ASN) providers (ISP)

Attackers Can’t Avoid the Internet

- User IP addresses
- User network blocks
- User autonomous systems (ASN)
- User internet service providers (ISP)
- Email provider
- Email subject
- Email body
- Email attachment
- Email headers
- Email language
- Email date/timestamp

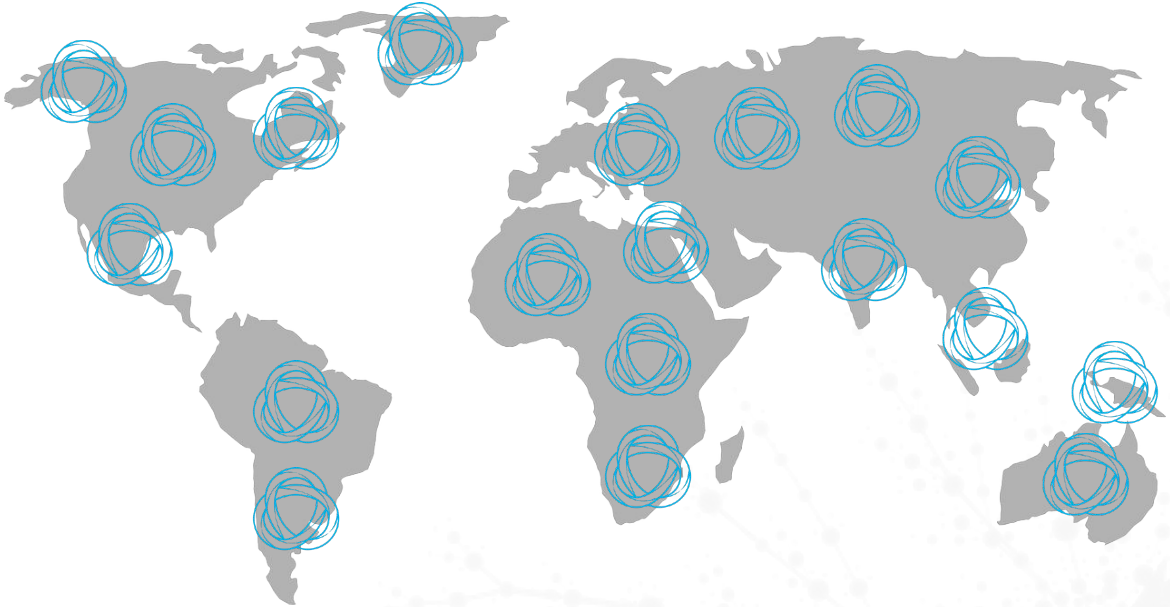
Attackers Can’t Avoid the Internet

- User IP addresses
- User network blocks
- User autonomous systems (ASN)
- User internet service providers (ISP)
- Email provider
- Email subject
- Email body
- Email attachment
- Email headers
- Email language
- Email date/timestamp
- Transit IP addresses
- Transit network blocks
- Transit times
- Transit autonomous systems (ASN)

Attackers Can’t Avoid the Internet

- User IP addresses
- User network blocks
- User autonomous systems (ASN)
- User internet service providers (ISP)
- Email provider
- Email subject
- Email body
- Email attachment
- Email headers
- Email language
- Email date/timestamp
- Transit IP addresses
- Transit network blocks
- Transit times
- Transit autonomous systems (ASN)
- Read date/timestamp
- Read notification
- Reader host operating system
- Reader location

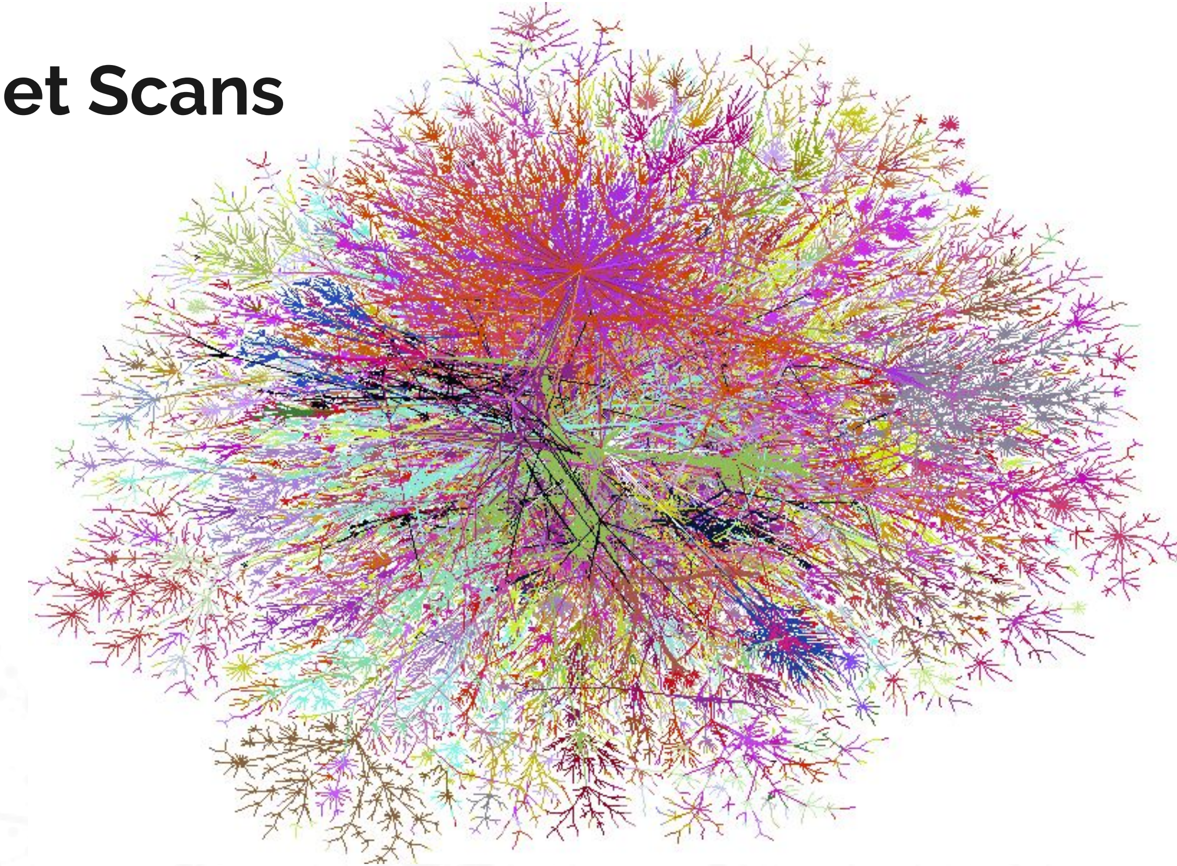
Collection: Global Proxy Network



- Hundreds of rotating proxies across the world
- Combination of residential, commercial and mobile egress points
- Highly configurable settings to emulate specific behaviors

Collection: Internet Scans

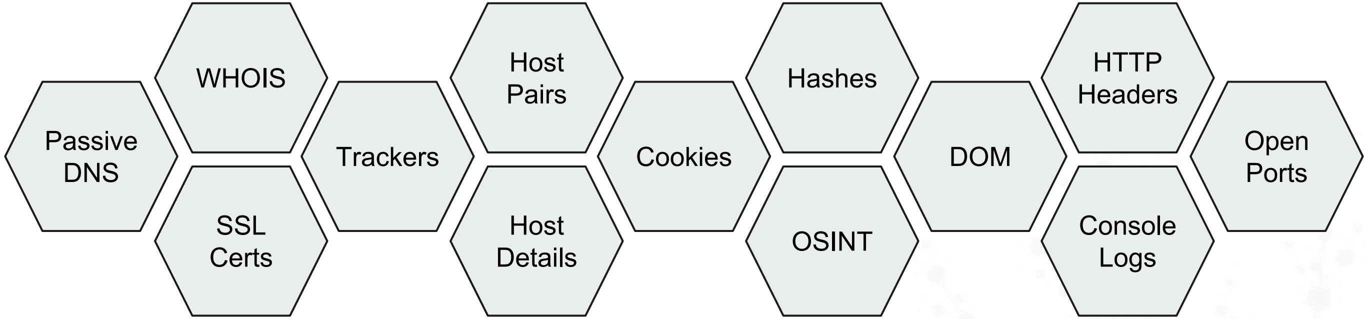
- Conducted on a routine basis across all IPv4
- Preservation of host, first seen, last seen and metadata
- Collection of 110+ ports and service banners associated with host



Collection: Virtual Users (web crawlers)

- Highly configurable to scroll, click, emulate specific technologies, conduct searches, etc.
- Saves all browser details: DOM, links, console messages, cookies, headers, dependent requests and files
- Billions of requests a day

Signals at Our Disposal



Passive DNS

WHOIS

SSL Certs

Trackers

Host Pairs

Host Details

Cookies

Hashes

OSINT

DOM

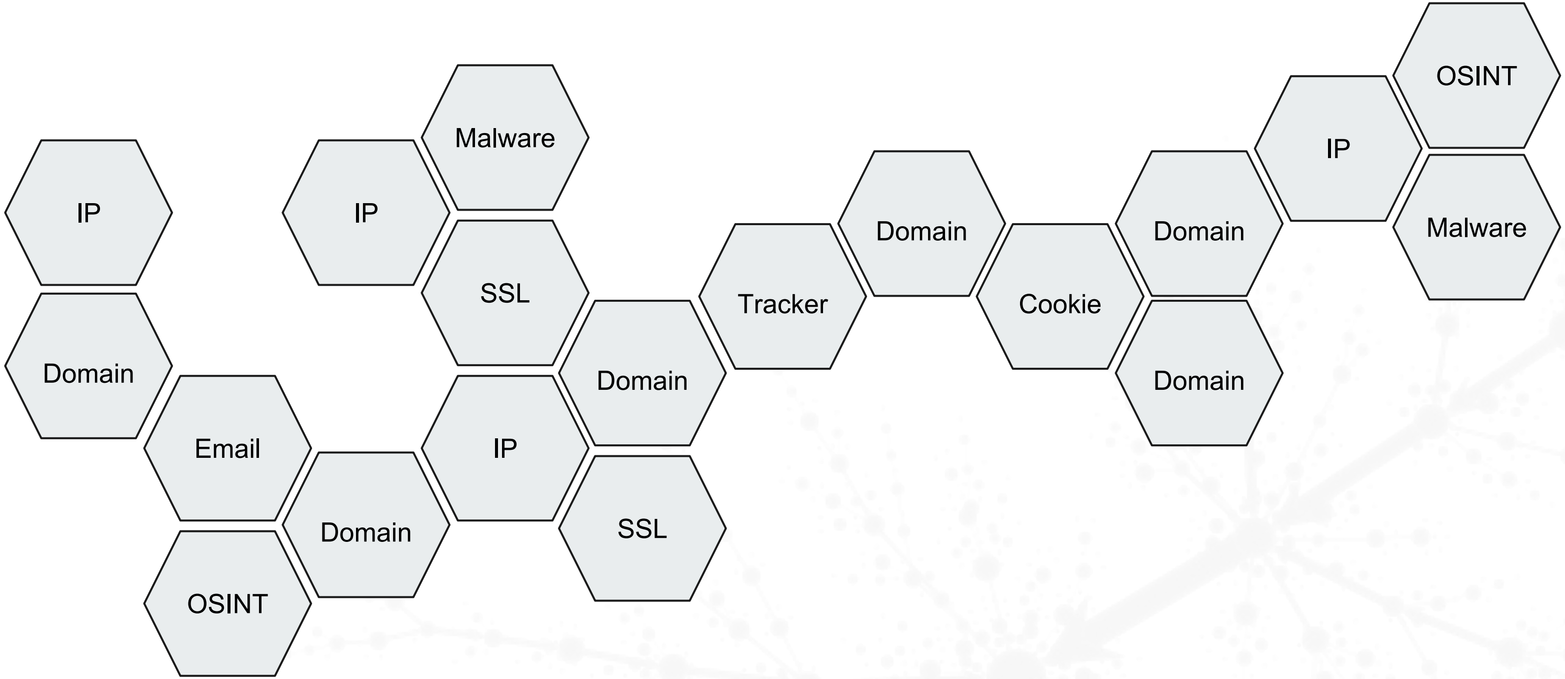
HTTP Headers

Console Logs

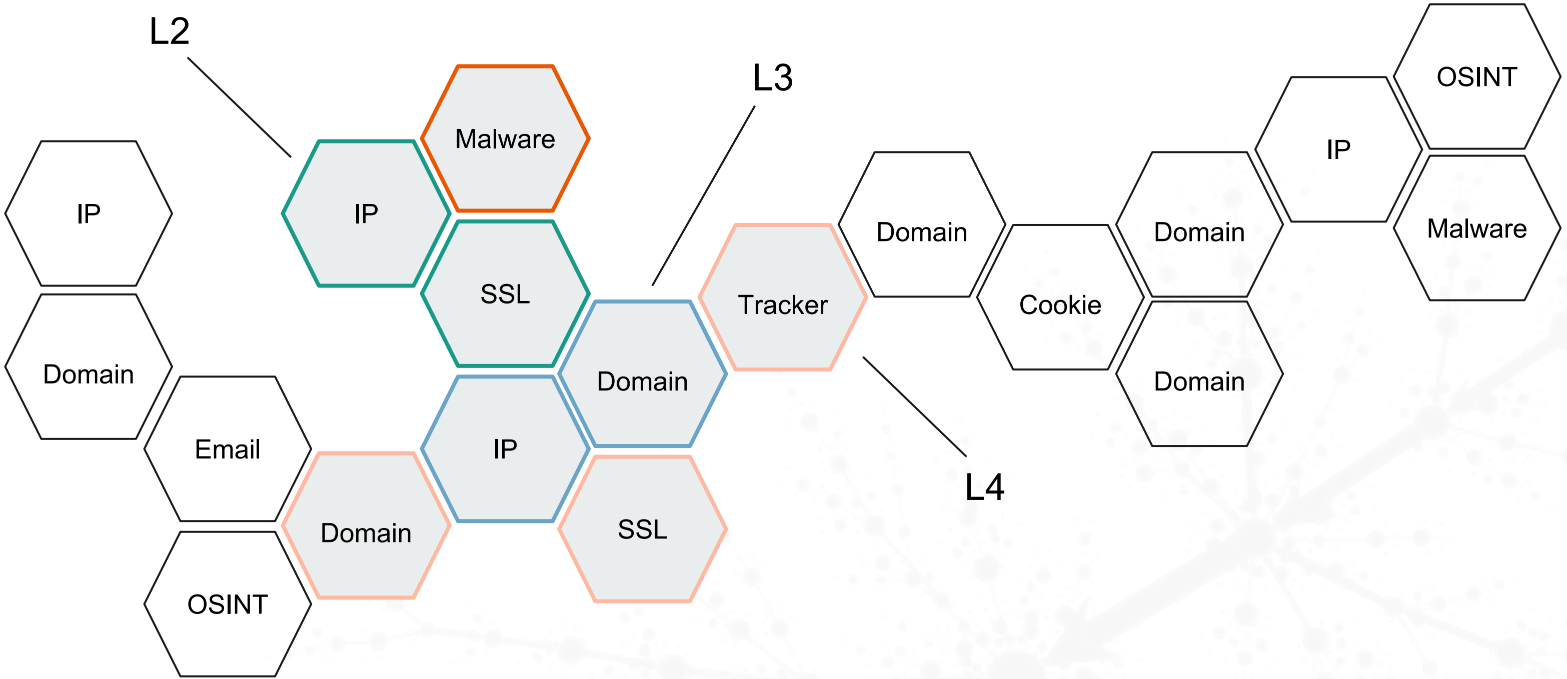
Open Ports

- Globally-placed sensors and proxies
- Headless web crawlers performing billions of requests a day
- Regular IPv4 internet scans for ports and data
- Mined open source intelligence and results

Infrastructure Chaining™ Illustrated

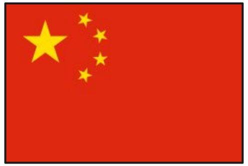


Infrastructure Chaining™ Illustrated



Build upon layers to form new connections and insights

Lets Burn.



LEAD/WINNTI

- Operating since ~2013
- Targets include
  - Gaming companies
  - ICT companies
  - Hosting providers
  - Basically everyone now
- Techniques used
  - Spearphishing
  - Registered domains & Dynamic DNS
  - Implants: RbDoor, zxShell, others

- See Kaspersky's "More Than A Game" and Trend Micro's "Of Pigs & Malware" reports

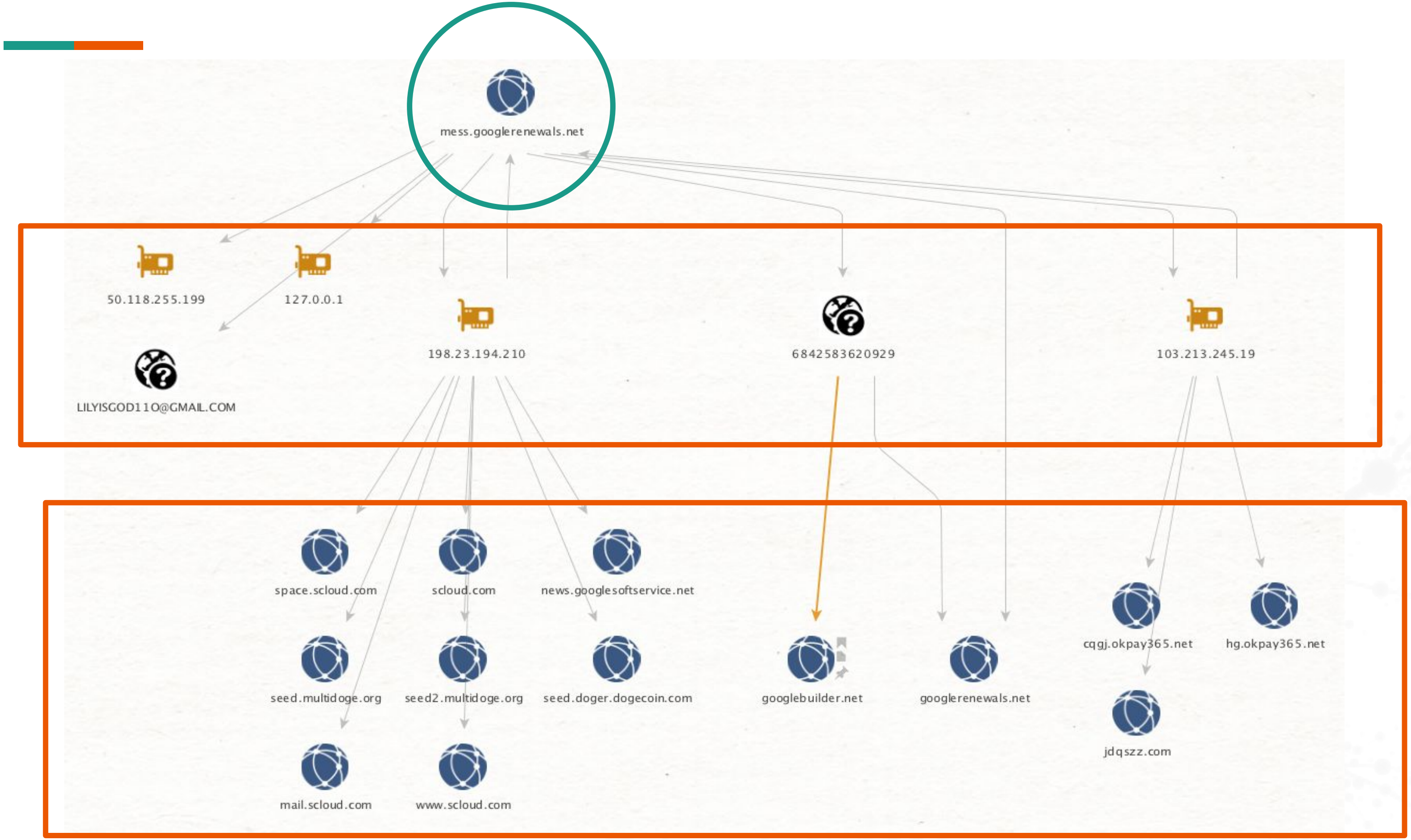
LEAD/WINNTI: Building Chains

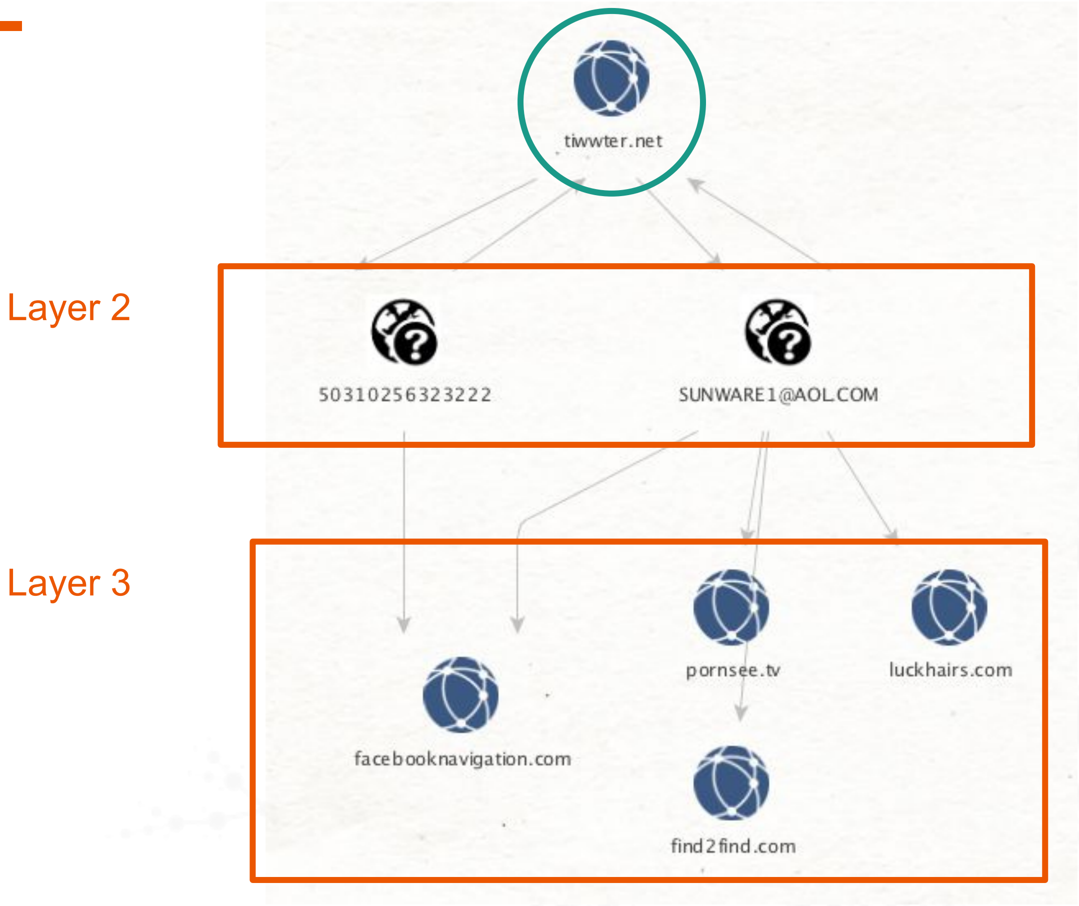
mess.googlerenewals[.]net, www.tiwwter[.]net

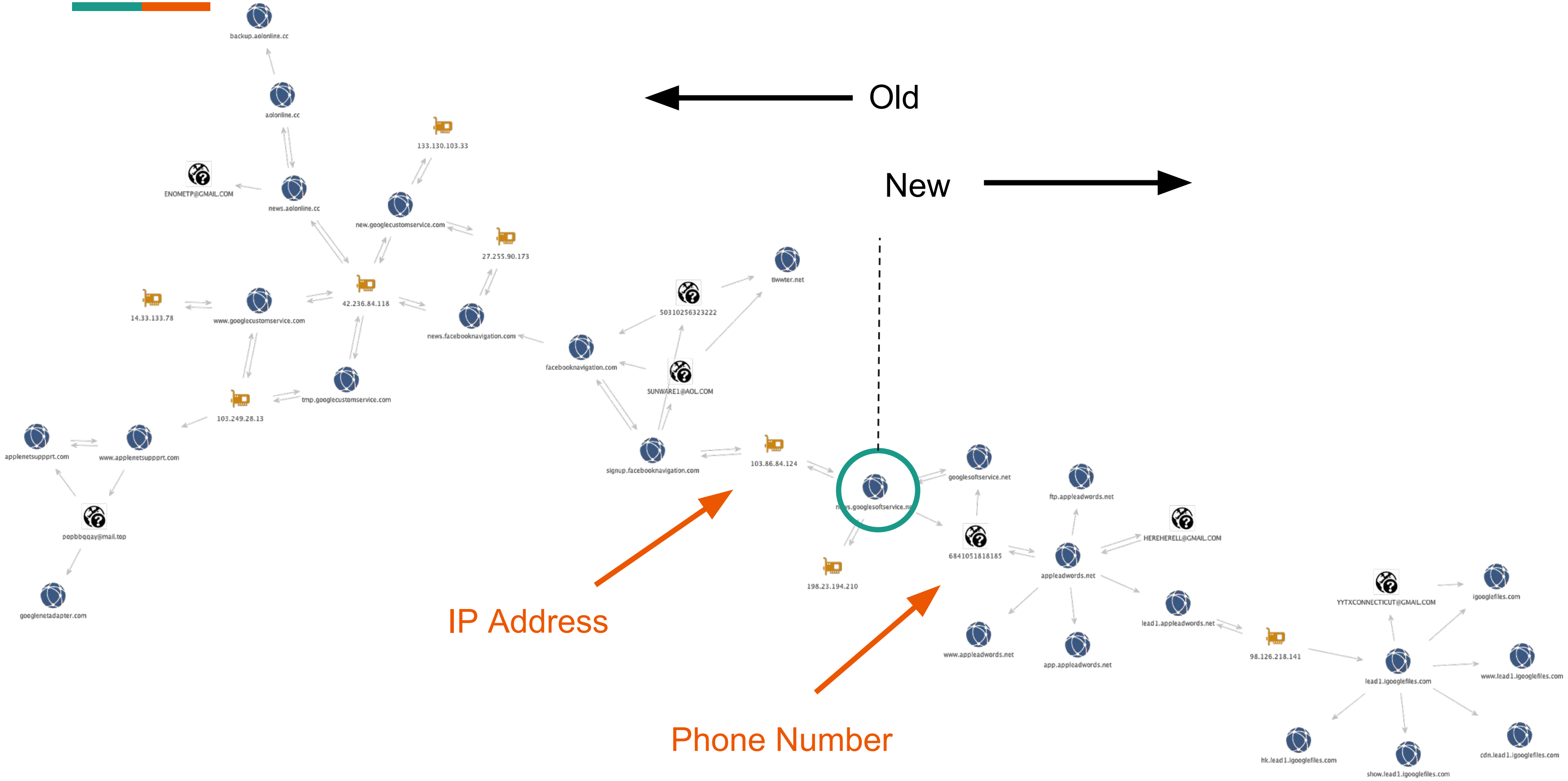
- Registered domains without privacy protection
- Theme around social media providers/typosquat-domains
- Lively infrastructure: many observed changes
- Unique subdomains following core media theme

Layer 2

Layer 3




tiwwter.net
Layer 2
50310256323222
SUNWARE1@AOL.COM
Layer 3
pornsee.tv
luckhairs.com
facebooknavigation.com
find2find.com



Old

New

IP Address

Phone Number

LEAD/WINNTI: Burn Report

Connections

- **L2**: 18 IP addresses, 2 WHOIS email, 2 WHOIS Phone, 14 subdomains, 15 hashes, 2 OSINT (LEAD/Casper/WINNTI)
- **L3:** 39+ domains, 1 WHOIS email, 40+ IP addresses, 50+ hashes, 1 domain (WHOIS phone), 4 domain (WHOIS email)

Breakdown

- 13 hours of pivoting to build chains
- OPSEC fail: WHOIS and hosting reuse
- Monitor WHOIS email & phone, social media in domains, IP addresses for reuse

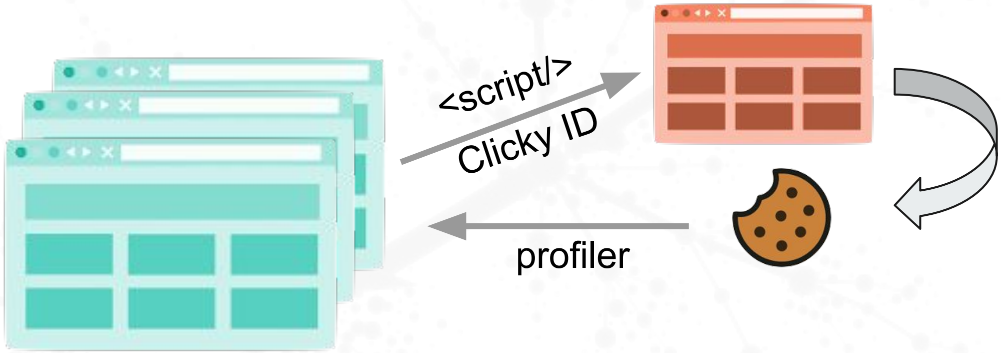
Turla

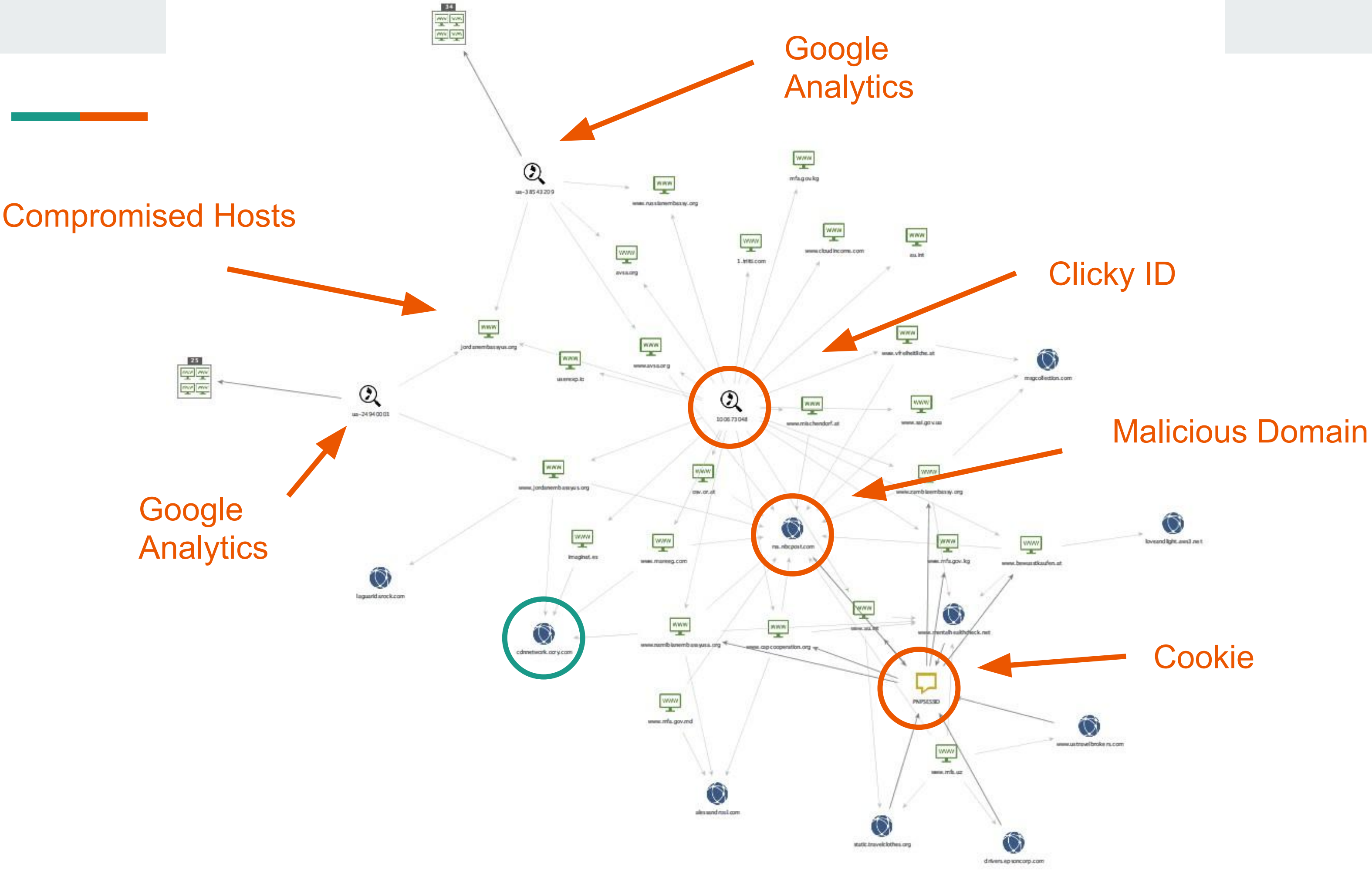
- Active since at least 2005
- Targets include
  - Embassies
  - MFA’s
  - Enterprises
- Techniques used
  - Implants: snake, uroburous, wipbot, skipper, carbon, more..
  - SATCOM

Turla: Building Chains

cdnnetwork.ocry[.]com

- Dynamic DNS domain
- Observed within a compromised web page disguised as Clicky Analytics
- Referenced via script tag
- Deployed profile script against visitors





Google Analytics

Compromised Hosts

Clicky ID

Malicious Domain

Google Analytics

Cookie

Turla: Burn Report

Connections

- **L2:** 2 IP addresses, 10 hashes, 9 host references, 4 host details
- **L3:** 35 compromised web pages, 8 domains, 3 analytics accounts, 1 cookie name

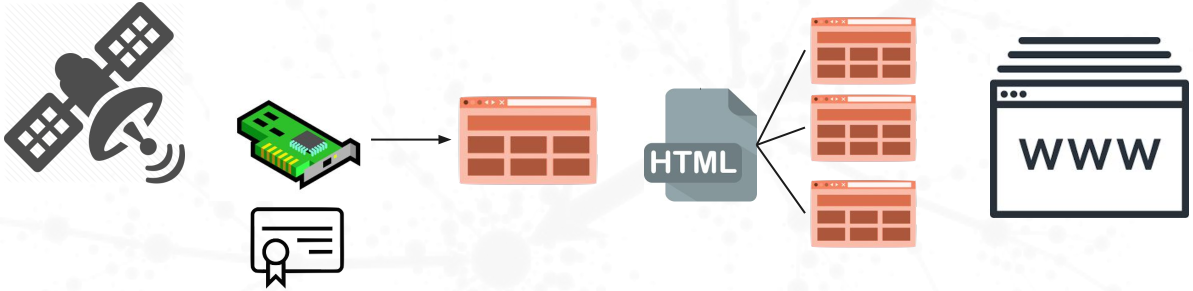
Breakdown

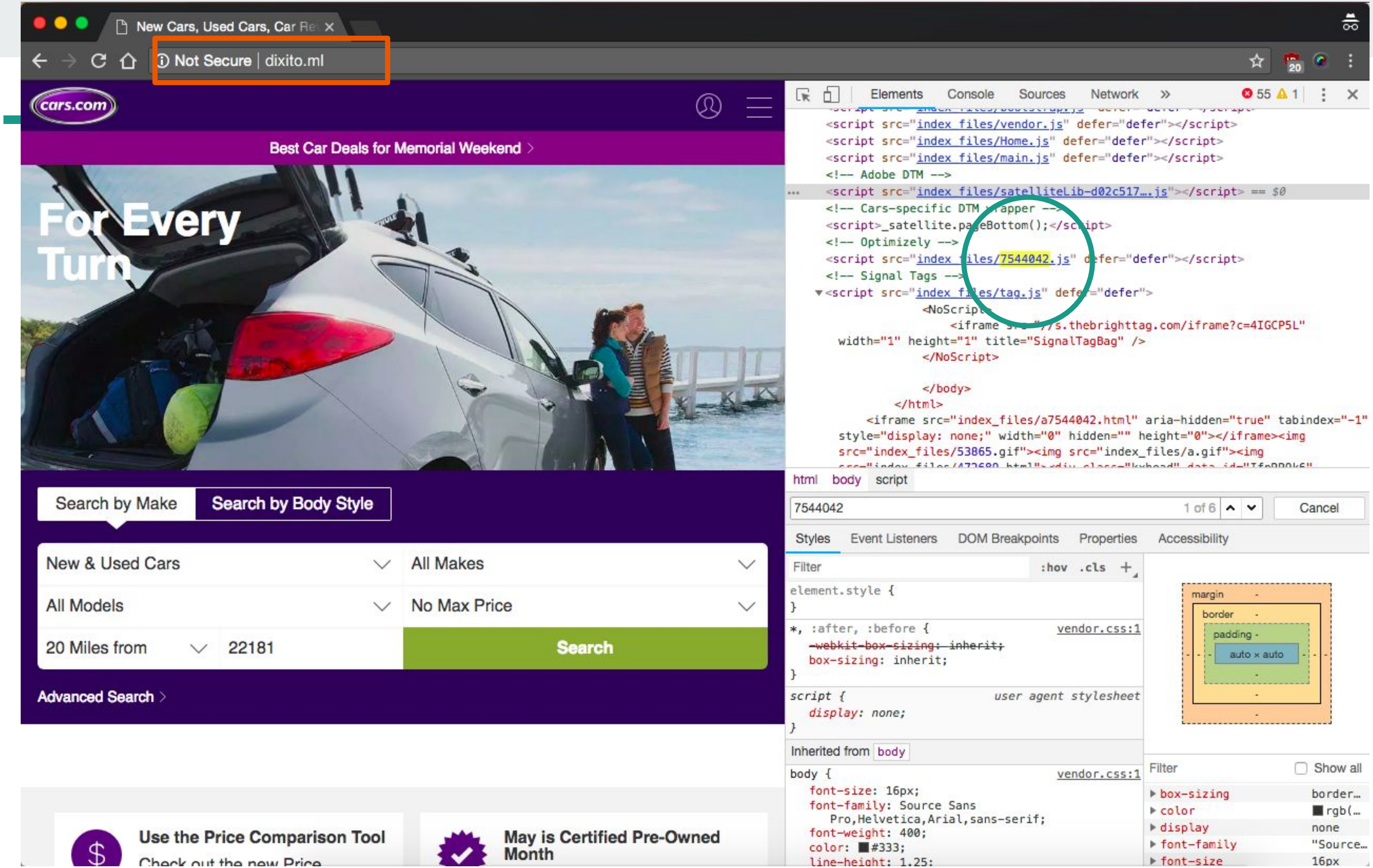
- 1+ year of following the actor
- OPSEC fail: deviation from dynamic DNS, reuse of cookie name, tracker IDs
- Monitor cookie names, host redirections and analytic IDs for new compromises

Turla: Bonus Material

81.199.160.11 (previously known satellite usage)

- Lost tracking via SSL Certificates and compromised hosts
- References to cars.com showed up on IP address (cookies, redirects)
- Cars.com found as a decoy page on numerous dynamic DNS domains
- Actors forgot to remove the unique tracking codes }:)





New Cars, Used Cars, Car Re

Not Secure | dixito.ml

cars.com

Best Car Deals for Memorial Weekend

For Every Turn

Search by Make | Search by Body Style

New & Used Cars | All Makes

All Models | No Max Price

20 Miles from | 22181 | Search

Advanced Search

Use the Price Comparison Tool
Check out the new Price

May is Certified Pre-Owned Month

Elements | Console | Sources | Network | 55 | 1

```
<script src="index files/vendor.js" defer="defer"></script>
<script src="index files/Home.js" defer="defer"></script>
<script src="index files/main.js" defer="defer"></script>
<!-- Adobe DTM -->
<script src="index files/satelliteLib-d02c517….js"></script> == $0
<!-- Cars-specific DTM wrapper -->
<script>_satellite.pageBottom();</script>
<!-- Optimizely -->
<script src="index files/7544042.js" defer="defer"></script>
<!-- Signal Tags -->
▼<script src="index files/tag.js" defer="defer">
        <NoScript>
            <iframe src="//s.thebrighttag.com/iframe?c=4IGCP5L"
  width="1" height="1" title="SignalTagBag" />
        </NoScript>

        </body>
    </html>
  <iframe src="index_files/a7544042.html" aria-hidden="true" tabindex="-1"
  style="display: none;" width="0" hidden="" height="0"></iframe><img
  src="index_files/53865.gif"><img src="index_files/a.gif"><img
```

html body script

7544042 | 1 of 6 | Cancel

Styles | Event Listeners | DOM Breakpoints | Properties | Accessibility

Filter :hov .cls +

```
element.style {
}
*, :after, :before {                vendor.css:1
  ~~-webkit-box-sizing: inherit;~~
  box-sizing: inherit;
}
script {               user agent stylesheet
  display: none;
}
Inherited from body
body {                              vendor.css:1
  font-size: 16px;
  font-family: Source Sans
    Pro,Helvetica,Arial,sans-serif;
  font-weight: 400;
  color: #333;
  line-height: 1.25;
```

Filter □ Show all

box-sizing	border…
color	rgb(…
display	none
font-family	"Source…
font-size	16px

Turla: Bonus Burn Report

Connections

- **L2:** 67 domains (most dynamic DNS), 6 trackers, 1 SSL certificate, 63 cookies
- **L3:** 236 domains, 1 OSINT, 7 IP addresses

Breakdown

- 2 hours to unearth hundreds of dynamic DNS infrastructure
- OPSEC fail: reused one IP address, shared the same website content
- One previous connection to old infrastructure connected tons of new infrastructure
- Tons of monitoring potential and layer 3 connections

APT32/Oceanlotus

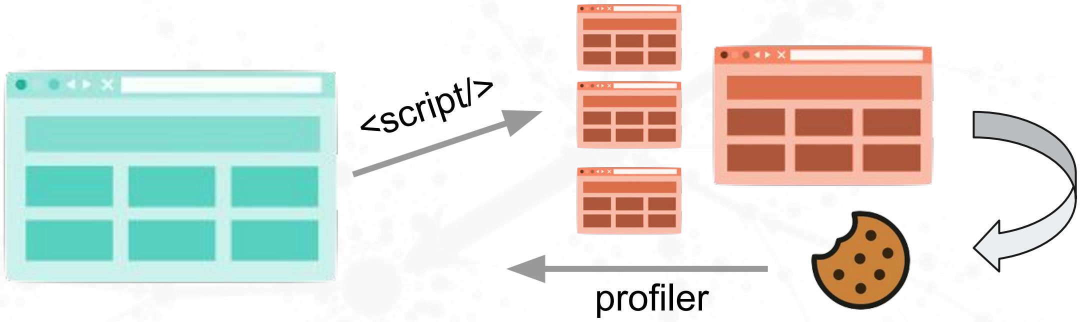
- Targets usually include ASEAN nations
- Compromises web pages and redirects traffic to first-level collectors
- Uses complex payload delivery
    - Leverages cookies to track users

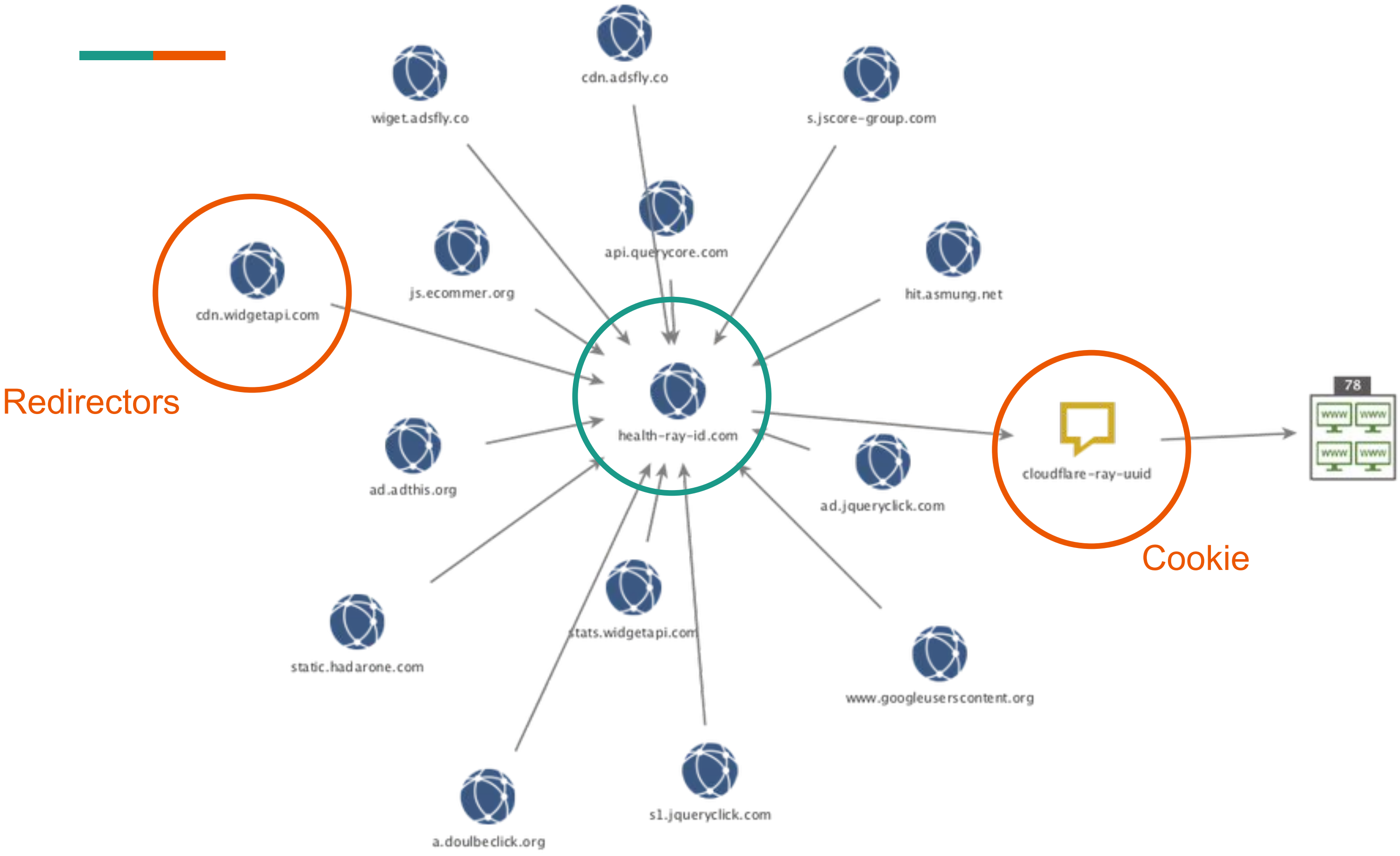
- See FireEye's "APT32 and the Threat to Global Corporations" report

APT32/Oceanlotus: Building Chains

health-ray-id[.]com

- Registered domain, privacy protected WHOIS
- No shared overlap via passive DNS
- Several connections to CDN and Ad service typo-squats
- Extensive connections with legitimate web pages with years of history

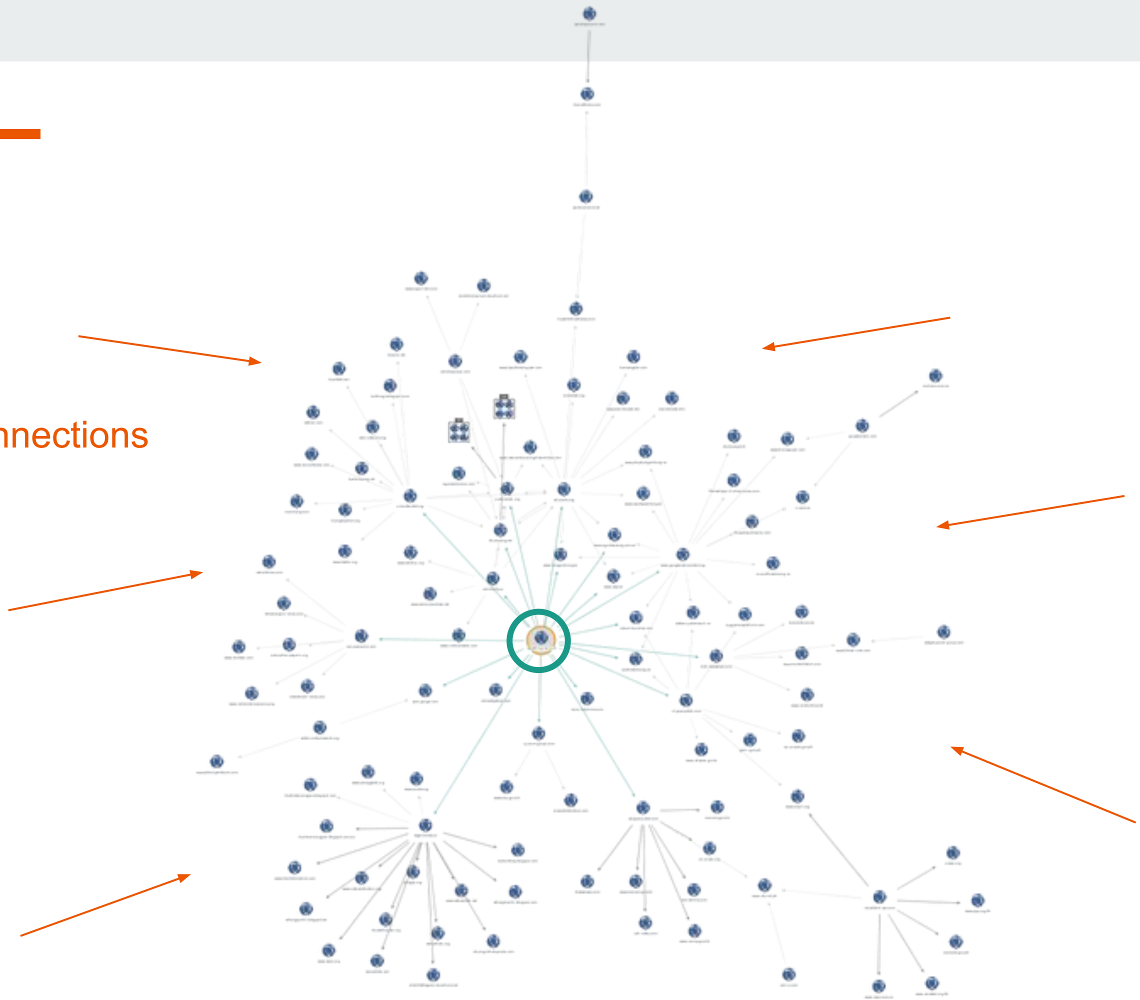




Redirectors

Cookie

All Connections



APT32/Oceanlotus: Burn Report

Connections

- **L2**: 2 IP addresses, 22 website references, 1 cookie name, 8 host details, 2 OSINT
- **L3**: 33 IP addresses, 150+ compromised web pages, 3 cookie names, 2 SSL certificates, 7+ hashes

Breakdown

- 5 hours of pivoting to build chains from OSINT
- OPSEC fail: reuse of infrastructure, single centroid node, common cookie name
- Monitor cookie names and host redirections for new compromises

APT32/Oceanlotus: Bonus Material

cloudflare-ray-uuid (cookie name)

- Burned operations throughout 2017, infrastructure shut down
- Continued delivery of the same tracking cookie with new domains

- [!] Discovered by teaching classes on threat hunting and seeing new data

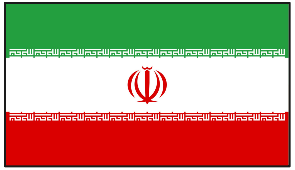
APT32/Oceanlotus: Bonus Burn Report

Connections

- **L2**: 3 deliver domains, 12 reference domains, 10 IP addresses
- **L3**: 80+ domains, 15 IP addresses, 112 SSL certificates, 9 cookie names

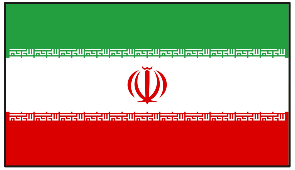
Breakdown

- Weekend of work to burn all 2018 infrastructure based on one mistake
- Identified changes to delivery methods
- Uncovered live phishing examples pretending to be Gmail
- Instantly block or monitor for future intelligence
- Deploy signatures to discover deliver in the future



Charming Kitten

- Iran groups targeting security, media, individuals, etc.
- Often attempts to phish by mimicking news or technology companies
- Reads news about their attacks and does not seem to worry about being caught
- Known to reuse infrastructure



Charming Kitten: Building Chains

Dump of 125 IOCs (domain, IP) previously seen in attacks

- Several OSINT reports and mentions of infrastructure
- Not completely groomed and unclear of exact timeframes
- Good use case for a complete intelligence build-out

https://community.riskiq.com/projects/4ff831f7-5825-05ec-c990-fcbec167acf9

Charming Kitten: Burn Report

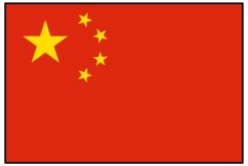
Connections

- **L2**: 125 domains and IP addresses
- **L3**: 923 domains, 67 SSL certificates, 56 WHOIS emails, 38 WHOIS phone, 27 IP addresses, 18 WHOIS name, 5 WHOIS address

Breakdown

- Successful testing and output of IOC grooming
  - Inspect each layer, tag and classify, add new observations, repeat
- Identification of newer infrastructure not yet reported
- Potential to stop attacks before they happen

Demo or More?



APT19/Codoso Team

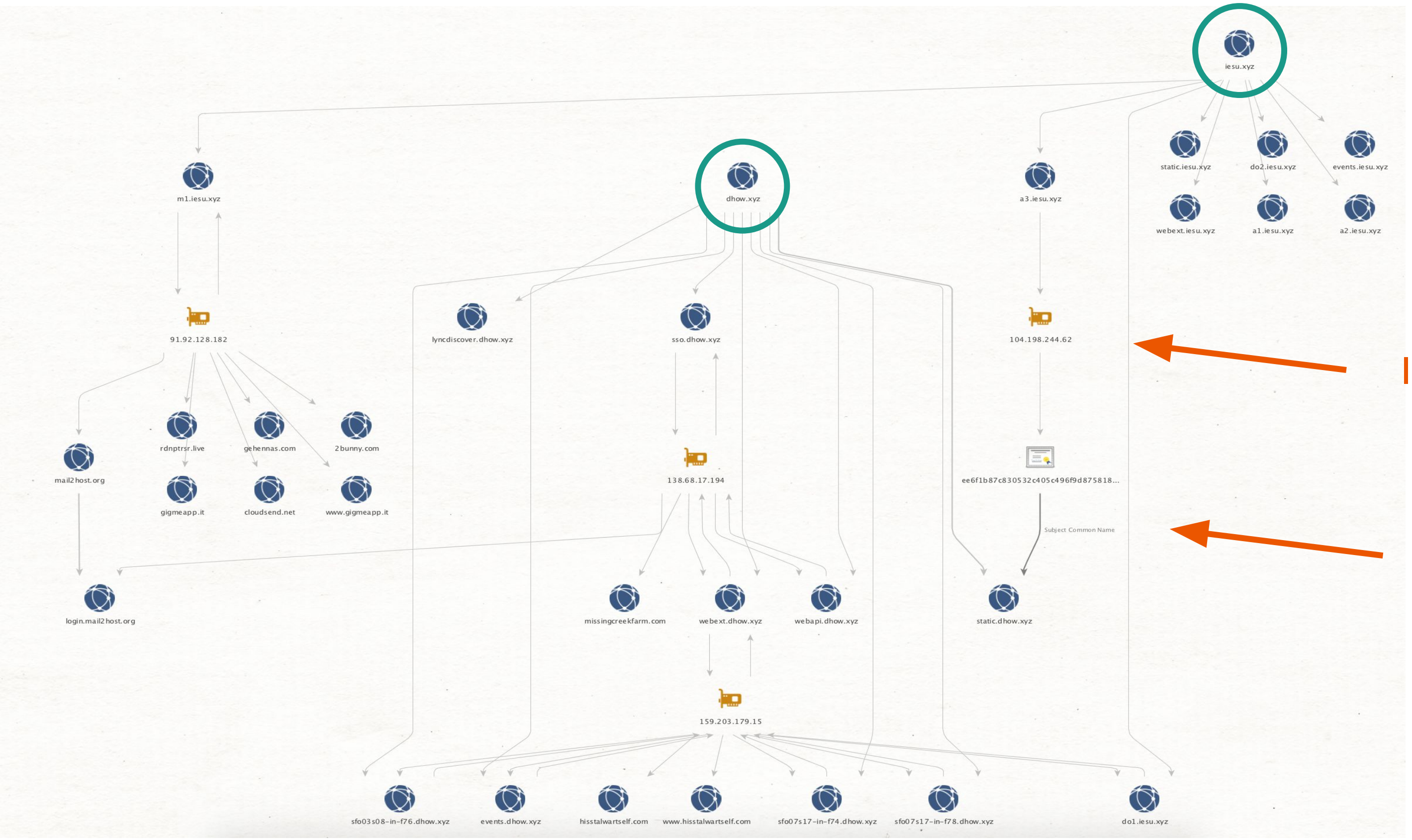
- Targets include
  - Legal
  - Investment
  - Financial
- Techniques used
  - Cobaltstrike
  - Spearphishing
  - Registered domains

- See bubble's presentation from SAS 2017

APT19/Codoso Team: Building Chains

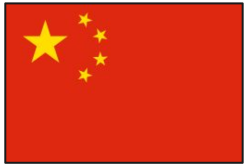
2bunny[.]com, dhow[.]xyz, iesu[.]xyz

- Registered domains, privacy protected
- Leverage Cloudflare to obfuscate direct infrastructure
- Heavy overlap through subdomain usage



IP address

SSL Cert



APT19/Codoso Team: Burn Report

Connections

- **L2**: 7 IP addresses, 40 subdomains, 36 host details, 27 cookies
- **L3:** 10+ domains, 4 SSL certificates, 3 cookies

Breakdown

- 7 hours of pivoting to build chains
- Monitor IP addresses and common names for new SSL certificates, cookie domains
- Instantly block or monitor for future intelligence

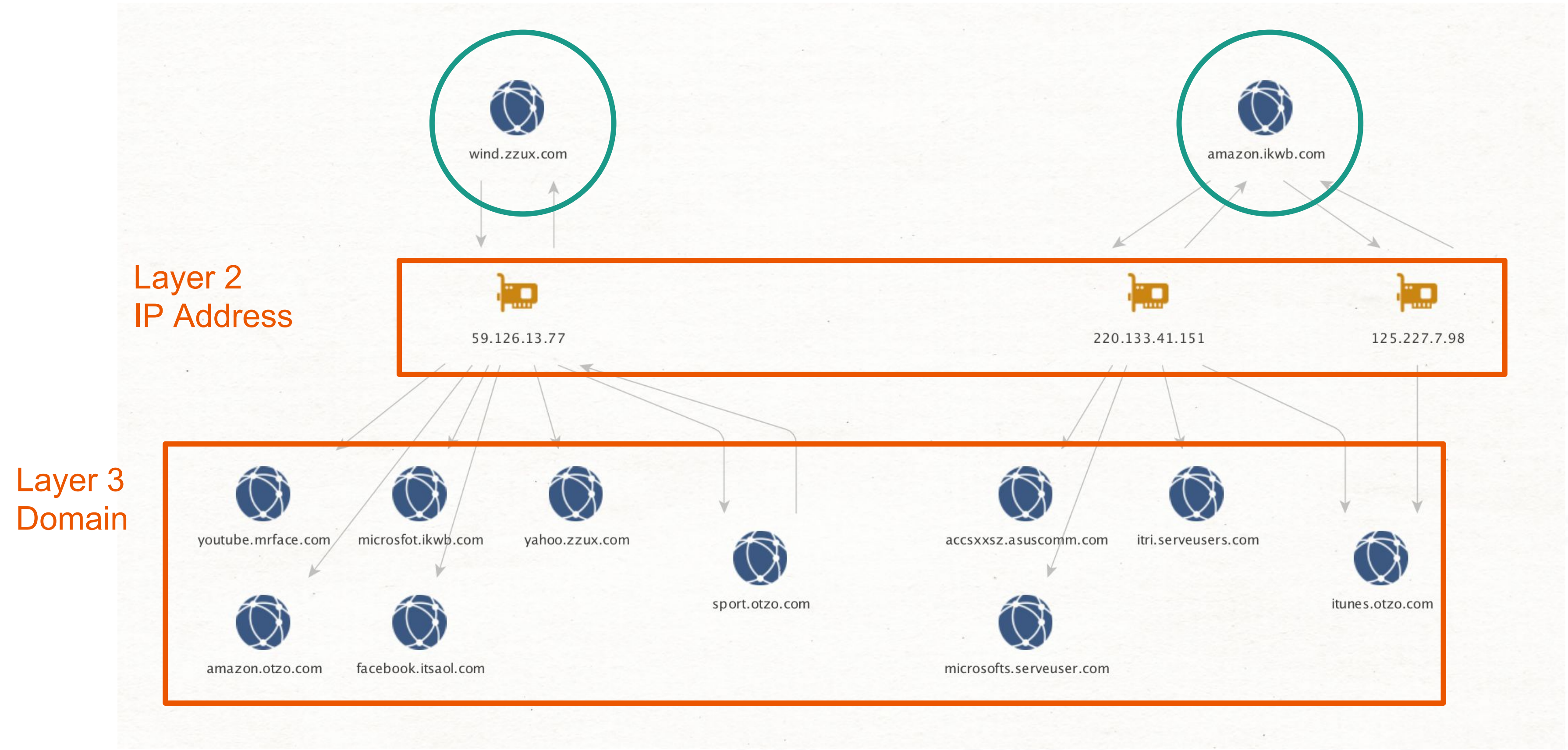
Mobwork

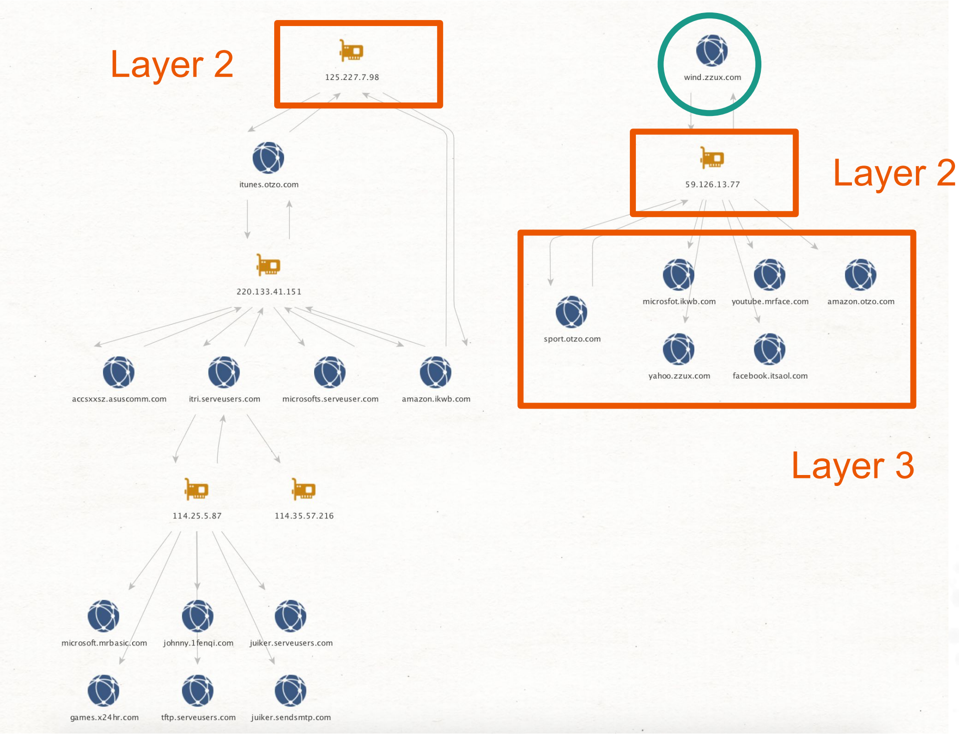
- Operating since 2008
- Historically have focused targeting on TW
- Techniques used
  - Registered domains & Dynamic DNS
  - Compromise of Home & SME Routers
  - Implants: TSCookie/Frontshell, Linopid, 9002

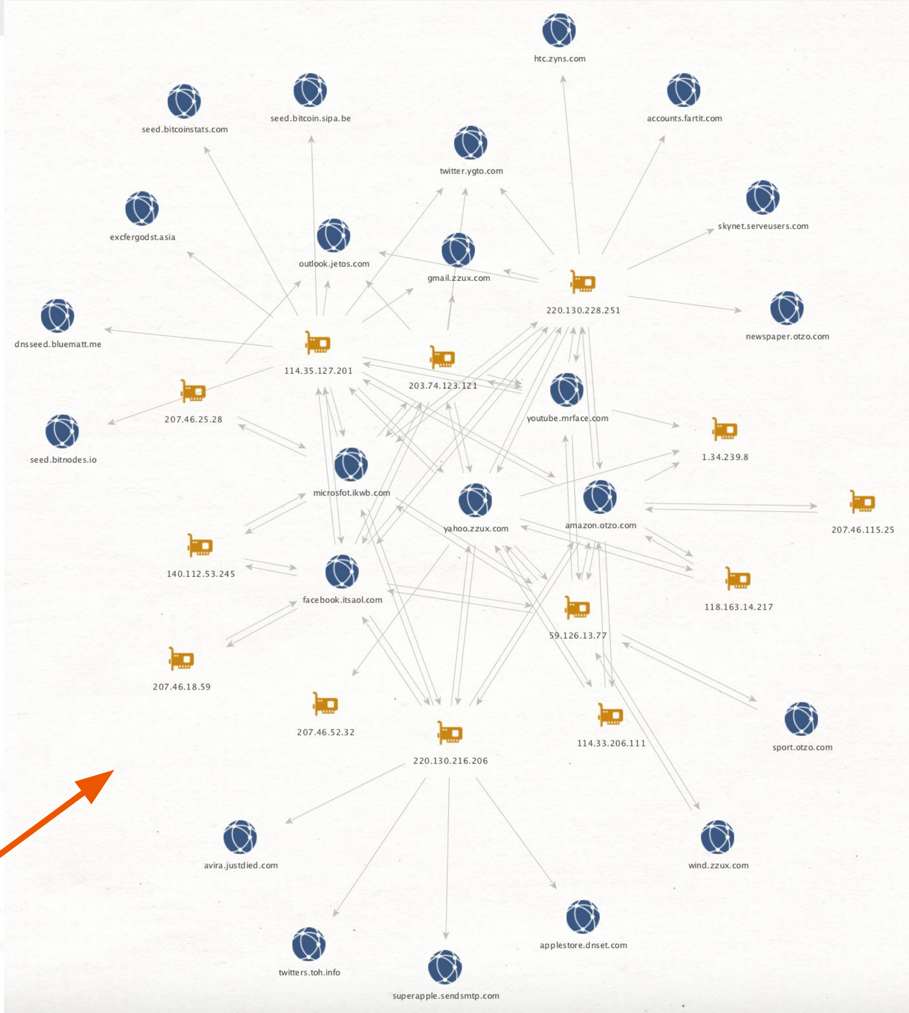
Mobwork: Building Chains

sport.otzo[.]com, wind.zzux[.]com, amazon.ikwb[.]com

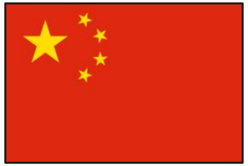
- Dynamic DNS domains: no WHOIS value and subdomain explosion
- Extensive history of passive DNS: years of reuse
- Connect based on overlap, shared themes, timeframes


wind.zzux.com
amazon.ikwb.com
Layer 2
IP Address
59.126.13.77
220.133.41.151
125.227.7.98
Layer 3
Domain
youtube.mrface.com
microsfot.ikwb.com
yahoo.zzux.com
sport.otzo.com
accsxxsz.asuscomm.com
itri.serveusers.com
itunes.otzo.com
amazon.otzo.com
facebook.itsaol.com
microsofts.serveuser.com





Interconnected Relations



Mobwork: Burn Report

Connections

- **L2**: 5 IP addresses, 4 hashes
- **L3**: 15 hashes, 55 domains, OSINT (BlackTech)
- **L4**: 100+ domains, tens of IPs, hashes all over, OSINT overlap

Breakdown

- 3 hours of pivoting to build chains
- Monitor IP addresses for new domain alerts as they come online
- Instantly block or monitor for future intelligence

Conclusions

- Any action, even inaction will generate signals
- More collection means more signals means more connections
- Burning nation-state actors can be done by any analyst
- Don’t ignore OSINT and always revisit your investigations

Questions?

brandon.dixon@riskiq.com

Know non-profit, NGO or journalists who are targeted?
Learn about Blockade.io, https://www.blockade.io

Access our data sources and investigate!
Register for free at https://community.riskiq.com

SWAG