Deceitful Drug Rehab Operation: Exposing the criminals and their fraud scheme

How to get from a single domain to a complete fraud set
INTRODUCTION

• DANIEL SCHWALBE, DIRECTOR OF ENGINEERING & DEPUTY CISO AT FARSHOT SECURİTY

• CHAD LOS SCHUMACHER, LEAD INVESTIGATOR, iTHREAT CYBER GROUP

• MICHAEL LEWIS, CTO iTHREAT CYBER GROUP
Nearly every online transaction – **good or bad** -- begins with a DNS lookup.

IPs or domain names provide a starting point and initial clue to an investigation.
DNS AS A MAP

- Most everything we do on the Internet...
  - B2C Web, B2B Web, E-mail, I-M, <your idea here>
  - ...relies on TCP/IP, and begins with a DNS lookup

- Mobile Internet is dominated by search...
  - ...but search itself relies extensively upon DNS

- DNS has a rigorous internal structure
  - Things that are in fact related, are related in DNS
  - You can have whois privacy, email privacy but not DNS privacy
We observe and record DNS resolutions worldwide as they happen and store all associated record types, i.e. MX, NS...
OUR SENSOR ARRAY

DIVERSE SOURCES
- Consumer
- Government
- Education
- Enterprise
- ISPs & Mobile
- Social media

REAL-TIME & HISTORIC
- 200k+ Resolutions / sec
- 2+ TB / Day
- 35+ Billion DNS Resolutions

GLOBAL COVERAGE
FARSIGHT SECURITY SOLUTIONS

01 SECURITY INFORMATION EXCHANGE (SIE)
Sensor data collection and distribution platform

02 DNSDB

03 NEWLY OBSERVED DOMAINS (NOD) & NEWLY OBSERVED HOSTNAMES (NOH)
Real-time visibility to domains and hostnames when first seen on the internet

04 BRAND SENTRY
Real-time alerting to possible phishing and infringing domain names

05 DOMAIN SENTRY
Real-time alerting to changes to an organization’s domain and ip infrastructure
TWO WAYS TO EMPOWER SECURITY OPERATIONS

I. SECURITY INFORMATION EXCHANGE

- Proactively detect and block
- Empower your Firewall & Mail Servers
- 200,000+ observations/second
- RPZ / RBL

II. DNS INTELLIGENCE DATABASE – DNSDB

- World’s largest historic database of DNS resolution and all records
- Empower your SIEM and Threat Platform
- Started in 2010, updated in Real-Time, 35+ Billion resolutions recorded
HOW TO USE IT

- Indicator of Compromise correlation
- Historical resolution lookups
- Time-based analysis
- Fully qualified domain name lookups
- SIEM event enrichment
- Domain or IP enrichment to proactively hunt for threats
WE FIT INTO YOUR CYBER SECURITY ECOSYSTEM

- Threat Platforms
- SOC Teams
- Firewalls
- Mail Servers
- SIEMs
- Orchestration & Automation
- Machine Learning
- Bulk Queries

FARSIGHT SECURITY
Do you need connectivity more than you need food?

66% of those surveyed said they would choose to take their mobile device to work over their lunch.

StatisticBrain.com
COMPUTING COST DESCREASING

Cost of Computing Power Equal to an iPad 2

Note: The iPad 2 has computing power equal to 1600 million instructions per second (MIPS). Each data point represents the cost of 1600 MIPS of computing power based on the power and price of a specific computing device released that year.
Source: Moravec n.d.
The Internet & Television Association
In 2016 there were about 7.4 billion people in the world. 3.4 billion of them had internet access.

internetlivestats.com
Only 8% of internet users live in the United States.

internetlivestats.com
<table>
<thead>
<tr>
<th>EVERY SECOND</th>
<th>EVERY 10 MINUTES</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Instagram" /> 770 photos</td>
<td>462,000</td>
</tr>
<tr>
<td><img src="image2.png" alt="Twitter" /> 7,537 tweets</td>
<td>4.5 million</td>
</tr>
<tr>
<td><img src="image3.png" alt="Google" /> 59,185 searches</td>
<td>35.5 million</td>
</tr>
<tr>
<td><img src="image4.png" alt="Internet Traffic" /> 42.7 TB</td>
<td>25,610 TB</td>
</tr>
</tbody>
</table>

Internetlivestats.com
The number of active sites has stabilized over the last 5 years, but the number of hostnames continues to grow.

*Netcraft Web Server Survey*
How do we keep up?

Cheap computing power
Millions of connected people and devices
Constant streams of data
Understanding the Internet
The Internet Corporation for Assigned Names and Numbers

NONPROFIT Organization based in California

Coordinates the maintenance and procedures of several databases related to the namespaces of the internet, ensuring the network's stable and secure operation

Oversees the registration processes of Top-level domains usage

Generic TLDS
.com .org .gov .edu

Country code TLDS
.uk .ca .cz
<table>
<thead>
<tr>
<th>Registrant</th>
<th>A person or organization that owns a domain name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NW3C</td>
<td>is a registrant. It owns nw3c.org (a domain).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Registrar</th>
<th>An organization certified by the registry operators to sell domains.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If you own a domain, you probably bought it from a registrar.*</td>
</tr>
<tr>
<td></td>
<td>*or a reseller affiliated with a registrar.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Registry</th>
<th>A master database for all domain names registered under each top-level domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top-level domains</td>
<td>.org .com .edu .gov .uk .beer</td>
</tr>
</tbody>
</table>
## REGIONAL INTERNET REGISTRIES

<table>
<thead>
<tr>
<th>RIR</th>
<th>Abbreviation</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>African Network Information Center</td>
<td>AfriNIC</td>
<td>Africa</td>
</tr>
<tr>
<td>Réseaux IP Européens Network Coordination Centre</td>
<td>RIPE</td>
<td>Europe, Middle East, Russia</td>
</tr>
<tr>
<td>American Registry for Internet Numbers</td>
<td>ARIN</td>
<td>North America, Antarctica, parts of Caribbean</td>
</tr>
<tr>
<td>Asia-Pacific Network Information Centre</td>
<td>APNIC</td>
<td>Asia, Australia, New Zealand</td>
</tr>
<tr>
<td>Latin America and Caribbean Network Information Centre</td>
<td>LACNIC</td>
<td>Central and South America, part of Caribbean</td>
</tr>
</tbody>
</table>

Manages IP address resources based upon geographic region. Forms the Internet Assigned Numbers Authority (IANA).
IPs are allocated by Regional Internet Registries (RIRs) to consumers (companies, governments, ISPs).

RIRs delegate IPv4 and IPv6 addresses.
IPV4 & IPV6

**IPV4**

Deployed 1981

*Address Size:* 32-bit number
*Address Format:*
  - Dotted Decimal Notation: 192.149.252.76
  - Prefix Notation: 192.149.0.0/24
*Number of Addresses:*
\[2^{32} = \sim 4,294,967,296\]

**IPV6**

Deployed 1999

*Address Size:* 128-bit number
*Address Format:*
  - Hexadecimal Notation: 3FFE:F200:0234:AB00:0123:4567:8901:ABCD
  - Prefix Notation: 3FFE:F200:0234::/48
*Number of Addresses:*
\[2^{128} = \sim 340,282,366,920,938,463,463,374,607,431,768,211,456\]
"The DNS (Domain Name System) is a massive network of servers that comprises the largest digital database on the planet."

PCNames.com

Nameservers (also called DNS servers) are like phone books for the internet.
They resolve domain names to IP addresses.

nw3c.org → 50.207.180.30
Questions so far?
Where do we begin?
How do you look up this information? Are you sure you have a complete picture?
LIMITATIONS OF FREE TOOLS AND LOOKUPS

- Domain Whois Info (CentralOps.net, Whoxy.com)
  - Unknown 3rd parties possibly collecting information.
  - Per-day query limitation.
  - Strictly returns ownership, some historical info.

- IP Address Info (IPLocation.net, CentralOps.net)
  - Returns limited amounts of information that can vary wildly.
  - Does not necessarily show additional contextual information.

- Contact Info (Pipl.com, Spokeo.com)
  - What are these platforms logging?
  - Connections sometimes made abstractly, unreliably.

Are you getting the full picture for each query? Do you trust the providers?
WHAT CAN CYBERTOOLBELT DO?

**Domain Info**
- Who owns it and how often is it changing?
- How can I view it without my IP address showing up in the site analytics?
- Provides historic WHOIS data, related IPs, related domains.
- Badness information.

**IP address**
- Who owns the IP and abuse contacts?
- What websites are on it?
- Where does it geolocate to?
- Provides historic WHOIS data, related IPs, related domains.

**Email address**
- What domains are registered to this email?
- Does anyone use this handle for social media or other email accounts?
- Any spam-related issues prevalent?

**Name/address/phone number**
- What domains are associated with this information?
- What connections can I make through Whitepages?

Simplifies and enhances investigations
BEYOND WHOIS: CONNECTING THE DIGITAL DOTS
CASE STUDY

Misleading Rehab Facility
An individual was looking into a drug rehab network.

He only had a single domain where a victim’s story originated.

Open source registration records unmasked larger operation.
DECEITFUL ADVERTISING

Right Path Drug Rehab Green Bay
310 W Walnut St, Green Bay, WI, United States
4.8 ★★★★★ 8 reviews

Joiie Kim
a year ago
★★★★★ I would have never thought that my brother would become pressured to do well in school and keep up with his social life. His drug... but Right Path Drug Rehab in Green Bay ... More

Vernice Oakley
10 months ago
★★★★★ I had the best case manager ever. She really understood me... say when I was feeling down about myself. I didn't think I was going to it... drug rehab center.

Lanny Rahim
a year ago
★★★★★ I felt like addiction snuck up on me. I didn't know the drugs were so addicting. I used them around friends and when I'd go out, but I knew I had developed a problem. After searching ... More
UPFRONT RECOVERY LLC

[Diagram of interconnected entities related to Upfront Recovery LLC]
A NEW SIDE OF THE BUSINESS
THE NOT-UPFRONT BUSINESS
CONCLUSION

• The group only had one “luxury” rehab facility in California that billed several thousand dollars a day to insurance.

• If the group couldn’t accept the patient, they would refer and get a kickback of the amount billed
  ✓ (This is illegal in the US – it is a violation of the Stark Law).
ICG - CYBER TOOLBELT SOLUTION SUITE
Thank you for your attention.

QUESTIONS?
Deceitful Drug Rehab Operation: Exposing the criminals and their fraud scheme

How to get from a single domain to a complete fraud set