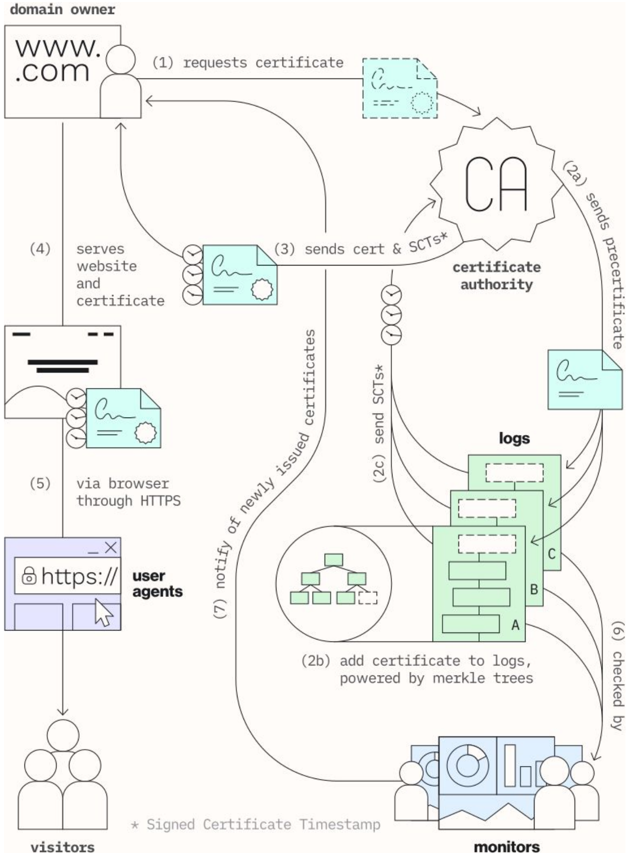
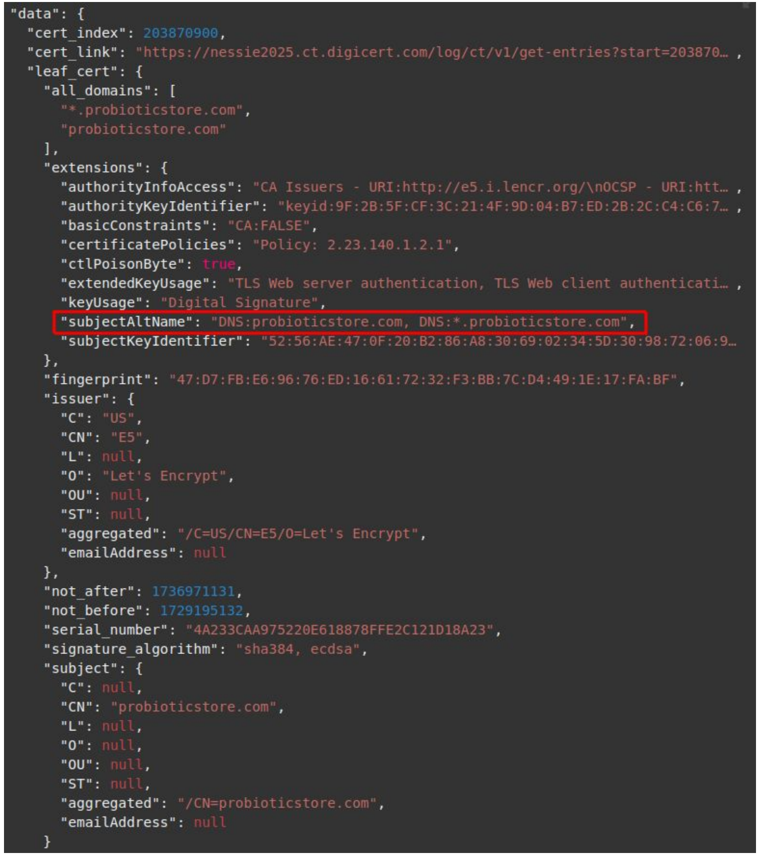
Catching Phish Using Publicly Accessible Information

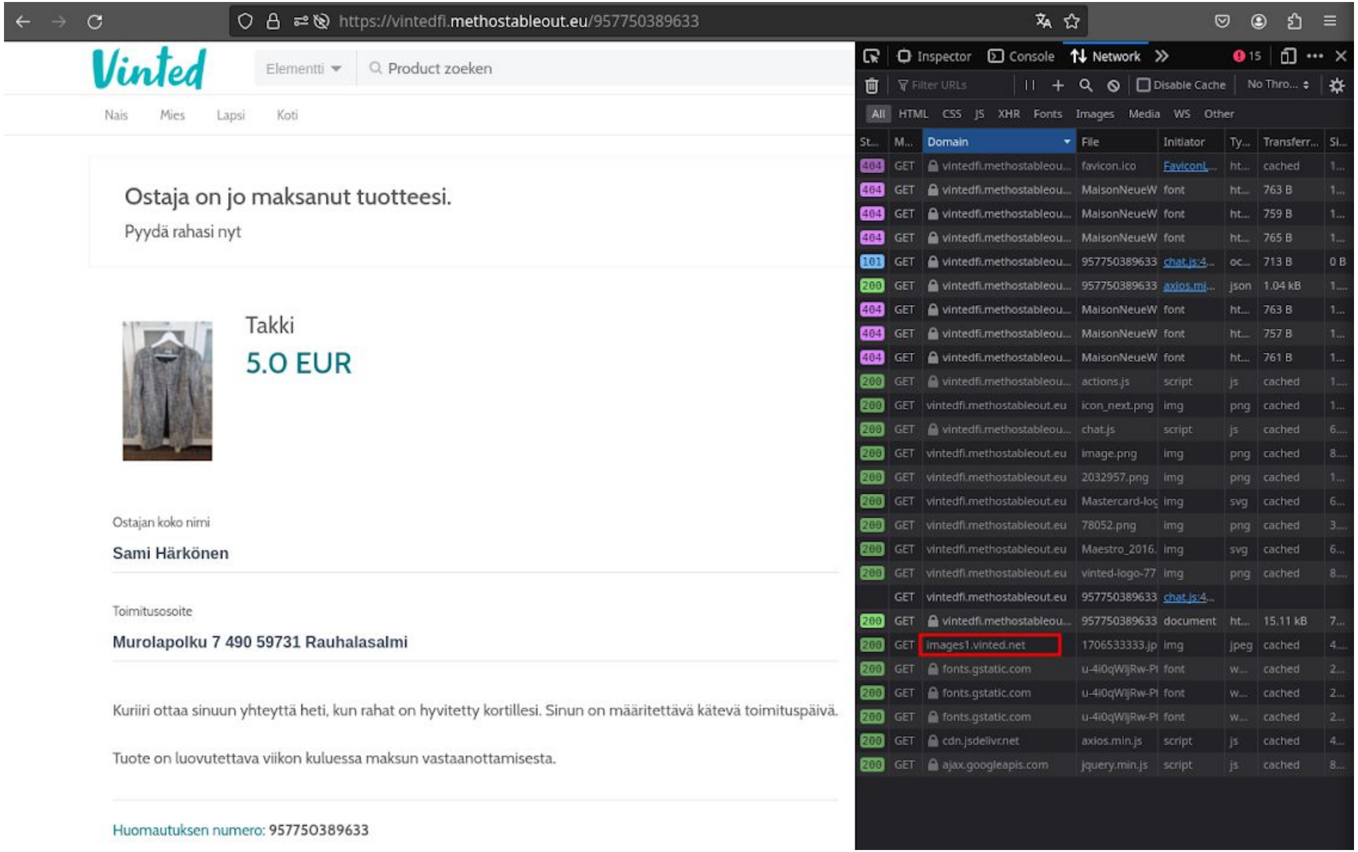
Certificate Transparency (CT)


domain owner
www.
.com
(1) requests certificate
CA
certificate authority
(2a) sends precertificate
(3) sends cert & SCTs*
(4) serves website and certificate
(2c) send SCTs*
(7) notify of newly issued certificates
logs
C
B
A
(2b) add certificate to logs, powered by merkle trees
(6) checked by
(5) via browser through HTTPS
https://
user agents
visitors
monitors
* Signed Certificate Timestamp



```
"data": {
  "cert_index": 203870900,
  "cert_link": "https://nessie2025.ct.digicert.com/log/ct/v1/get-entries?start=203870… ,
  "leaf_cert": {
    "all_domains": [
      "*.probioticstore.com",
      "probioticstore.com"
    ],
    "extensions": {
      "authorityInfoAccess": "CA Issuers - URI:http://e5.i.lencr.org/\nOCSP - URI:htt… ,
      "authorityKeyIdentifier": "keyid:9F:2B:5F:CF:3C:21:4F:9D:04:B7:ED:2B:2C:C4:C6:7… ,
      "basicConstraints": "CA:FALSE",
      "certificatePolicies": "Policy: 2.23.140.1.2.1",
      "ctlPoisonByte": true,
      "extendedKeyUsage": "TLS Web server authentication, TLS Web client authenticati… ,
      "keyUsage": "Digital Signature",
      "subjectAltName": "DNS:probioticstore.com, DNS:*.probioticstore.com",
      "subjectKeyIdentifier": "52:56:AE:47:0F:20:B2:86:A8:30:69:02:34:5D:30:98:72:06:9…
    },
    "fingerprint": "47:D7:FB:E6:96:76:ED:16:61:72:32:F3:BB:7C:D4:49:1E:17:FA:BF",
    "issuer": {
      "C": "US",
      "CN": "E5",
      "L": null,
      "O": "Let's Encrypt",
      "OU": null,
      "ST": null,
      "aggregated": "/C=US/CN=E5/O=Let's Encrypt",
      "emailAddress": null
    },
    "not_after": 1736971131,
    "not_before": 1729195132,
    "serial_number": "4A233CAA975220E618878FFE2C121D18A23",
    "signature_algorithm": "sha384, ecdsa",
    "subject": {
      "C": null,
      "CN": "probioticstore.com",
      "L": null,
      "O": null,
      "OU": null,
      "ST": null,
      "aggregated": "/CN=probioticstore.com",
      "emailAddress": null
    }
```

HTTP Referer (1)



https://vintedfi.methostableout.eu/957750389633

Ostaja on jo maksanut tuotteesi.

Pyydä rahasi nyt

Takki

5.0 EUR

Ostajan koko nimi

Sami Härkönen

Toimitusosoite

Murolapolku 7 490 59731 Rauhalasalmi

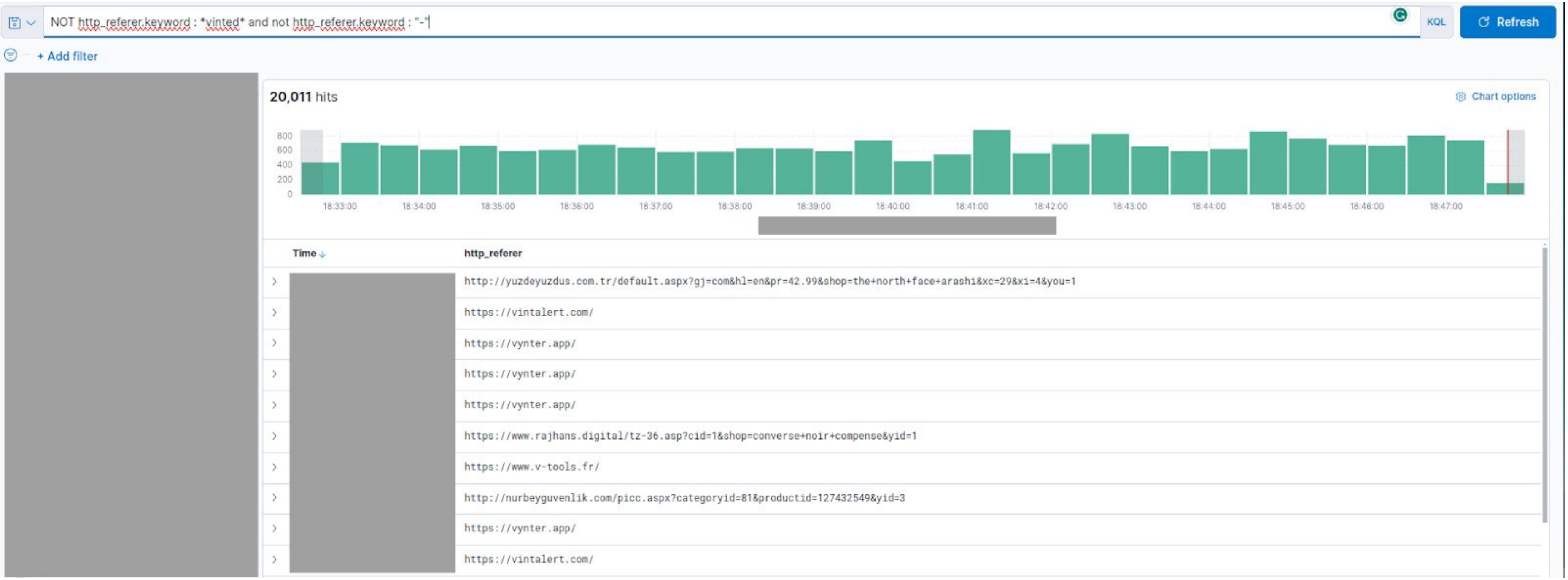
Kuriiri ottaa sinuun yhteyttä heti, kun rahat on hyvitetty kortillesi. Sinun on määritettävä kätevä toimituspäivä.

Tuote on luovutettava viikon kuluessa maksun vastaanottamisesta.

Huomautuksen numero: 957750389633

St...	M...	Domain	File	Initiator	Ty...	Transferr...	Si...
404	GET	vintedfi.methostableou...	favicon.ico	FaviconL...	ht...	cached	1...
404	GET	vintedfi.methostableou...	MaisonNeueW	font	ht...	763 B	1...
404	GET	vintedfi.methostableou...	MaisonNeueW	font	ht...	759 B	1...
404	GET	vintedfi.methostableou...	MaisonNeueW	font	ht...	765 B	1...
101	GET	vintedfi.methostableou...	957750389633	chat.js:4...	oc...	713 B	0 B
200	GET	vintedfi.methostableou...	957750389633	axios.mi...	json	1.04 kB	1....
404	GET	vintedfi.methostableou...	MaisonNeueW	font	ht...	763 B	1...
404	GET	vintedfi.methostableou...	MaisonNeueW	font	ht...	757 B	1...
404	GET	vintedfi.methostableou...	MaisonNeueW	font	ht...	761 B	1...
200	GET	vintedfi.methostableou...	actions.js	script	js	cached	1....
200	GET	vintedfi.methostableout.eu	icon_next.png	img	png	cached	1...
200	GET	vintedfi.methostableou...	chat.js	script	js	cached	6....
200	GET	vintedfi.methostableout.eu	image.png	img	png	cached	8....
200	GET	vintedfi.methostableout.eu	2032957.png	img	png	cached	1...
200	GET	vintedfi.methostableout.eu	Mastercard-loc	img	svg	cached	6...
200	GET	vintedfi.methostableout.eu	78052.png	img	png	cached	3....
200	GET	vintedfi.methostableout.eu	Maestro_2016.	img	svg	cached	6...
200	GET	vintedfi.methostableout.eu	vinted-logo-77	img	png	cached	8....
	GET	vintedfi.methostableout.eu	957750389633	chat.js:4...			
200	GET	vintedfi.methostableou...	957750389633	document	ht...	15.11 kB	7...
200	GET	images1.vinted.net	1706533333.jp	img	jpeg	cached	4....
200	GET	fonts.gstatic.com	u-4i0qWIjRw-Pl	font	w...	cached	2...
200	GET	fonts.gstatic.com	u-4i0qWIjRw-Pl	font	w...	cached	2...
200	GET	fonts.gstatic.com	u-4i0qWIjRw-Pl	font	w...	cached	2...
200	GET	cdn.jsdelivr.net	axios.min.js	script	js	cached	4...
200	GET	ajax.googleapis.com	jquery.min.js	script	js	cached	8...

HTTP Referer (2)



```
NOT http_referer.keyword : *vinted* and not http_referer.keyword : "-"
```

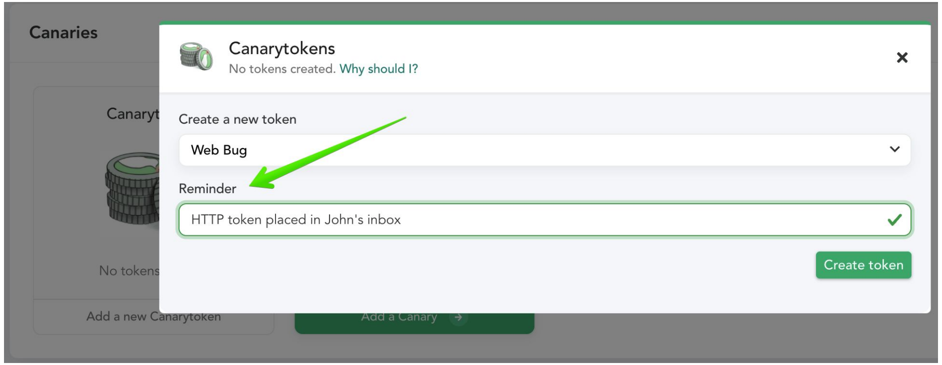
[redacted]

20,011 hits

[redacted]

Time ↓	http_referer
[redacted]	http://yuzdeyuzdus.com.tr/default.aspx?gj=com&hl=en&pr=42.99&shop=the+north+face+arashi&xc=29&xi=4&you=1
[redacted]	https://vintalert.com/
[redacted]	https://vynter.app/
[redacted]	https://vynter.app/
[redacted]	https://vynter.app/
[redacted]	https://www.rajhans.digital/tz-36.asp?cid=1&shop=converse+noir+compense&yid=1
[redacted]	https://www.v-tools.fr/
[redacted]	http://nurbeyguvenlik.com/picc.aspx?categoryid=81&productid=127432549&yid=3
[redacted]	https://vynter.app/
[redacted]	https://vintalert.com/

Canary Tokens



Canarytokens

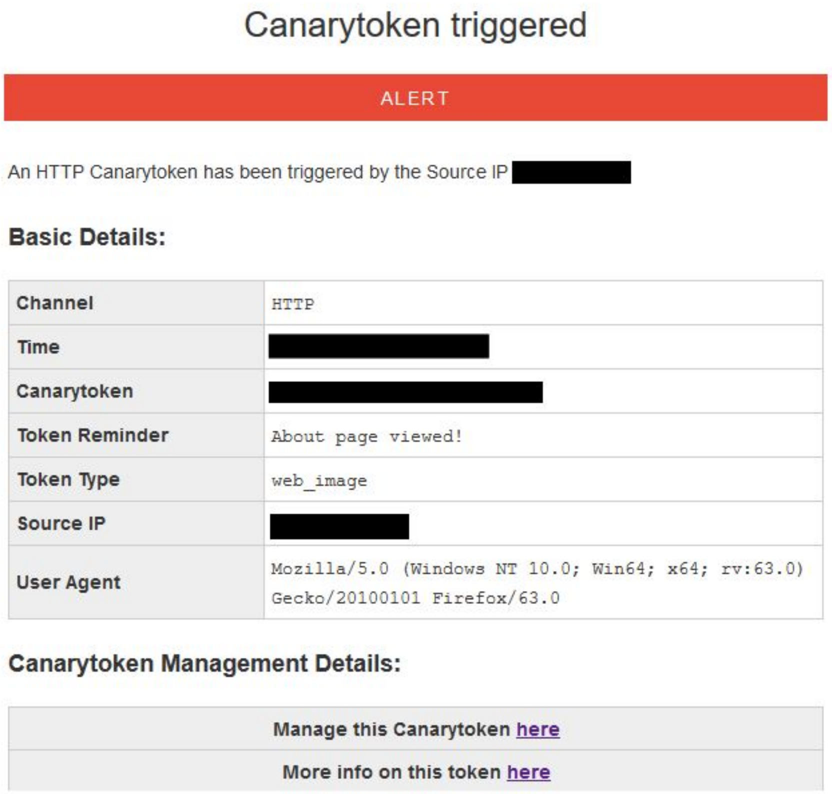
No tokens created. Why should I?

Create a new token

Web Bug

Reminder

HTTP token placed in John's inbox



Canarytoken triggered

ALERT

An HTTP Canarytoken has been triggered by the Source IP [redacted]

Basic Details:

Channel	HTTP
Time	[redacted]
Canarytoken	[redacted]
Token Reminder	About page viewed!
Token Type	web_image
Source IP	[redacted]
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0

Canarytoken Management Details:

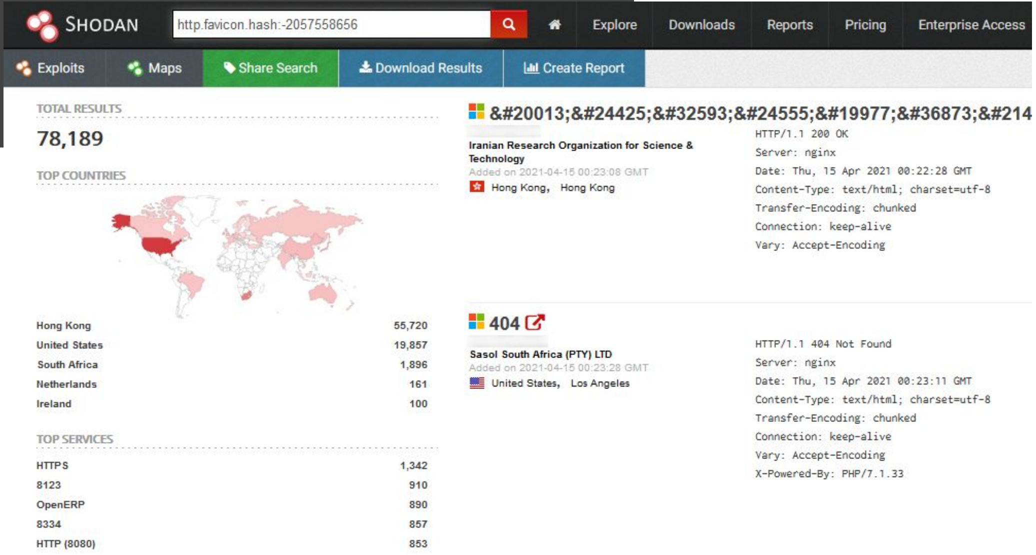
Manage this Canarytoken here
More info on this token here

MurmurHash3

```
import requests, mmh3, base64

response = requests.get('https://c.s-microsoft.com/favicon.ico')
favicon = base64.encodebytes(response.content)
hash = mmh3.hash(favicon)

print(hash)
```



http.favicon.hash:-2057558656

TOTAL RESULTS

78,189

TOP COUNTRIES

Hong Kong	55,720
United States	19,857
South Africa	1,896
Netherlands	161
Ireland	100

TOP SERVICES

HTTPS	1,342
8123	910
OpenERP	890
8334	857
HTTP (8080)	853

&#20013;&#24425;&#32593;&#24555;&#19977;&#36873;&#214

[redacted]

Iranian Research Organization for Science & Technology
Added on 2021-04-15 00:23:08 GMT
Hong Kong, Hong Kong

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 15 Apr 2021 00:22:28 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
```

404

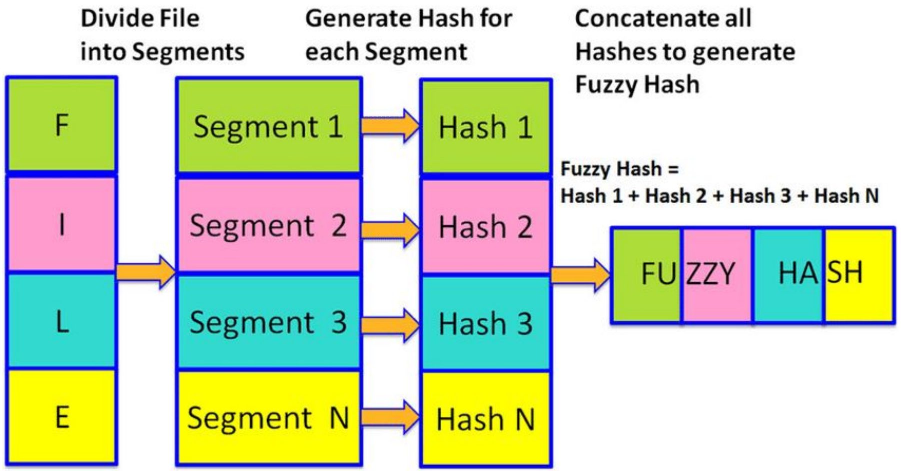
[redacted]

Sasol South Africa (PTY) LTD
Added on 2021-04-15 00:23:28 GMT
United States, Los Angeles

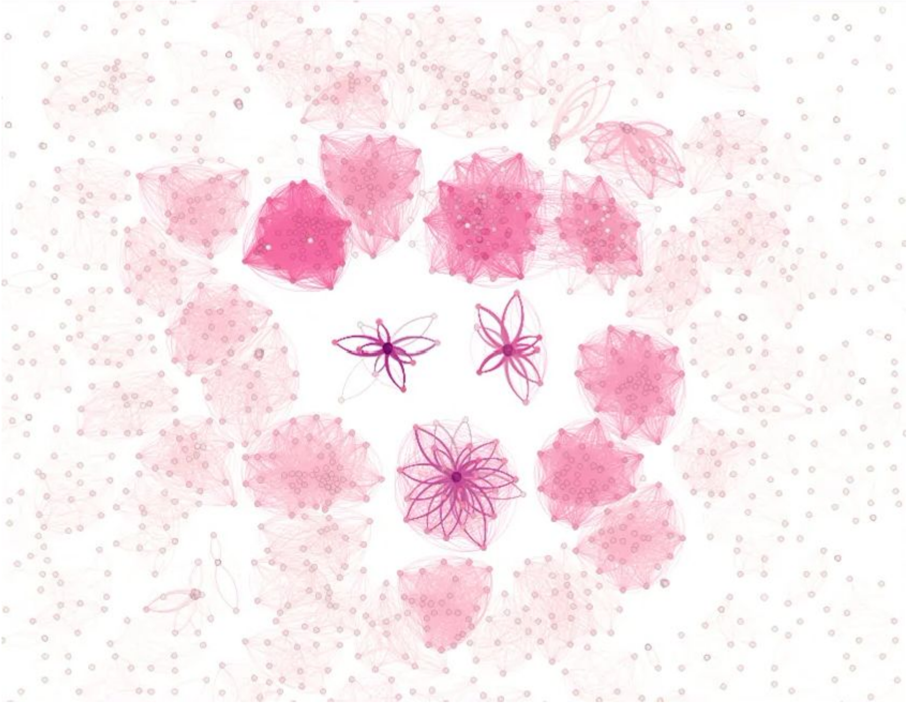
```
HTTP/1.1 404 Not Found
Server: nginx
Date: Thu, 15 Apr 2021 00:23:11 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/7.1.33
```

Fuzzy Hash

1. Compute a fuzzy hash (ssdeep, TLSH) for the HTML and DOM (Document Object Model)
2. Check if there are similarities between legit and phishing site


Divide File into Segments
Generate Hash for each Segment
Concatenate all Hashes to generate Fuzzy Hash
F
I
L
E
Segment 1
Segment 2
Segment 3
Segment N
Hash 1
Hash 2
Hash 3
Hash N
Fuzzy Hash =
Hash 1 + Hash 2 + Hash 3 + Hash N
FU
ZZY
HA
SH

Phishing campaign detection

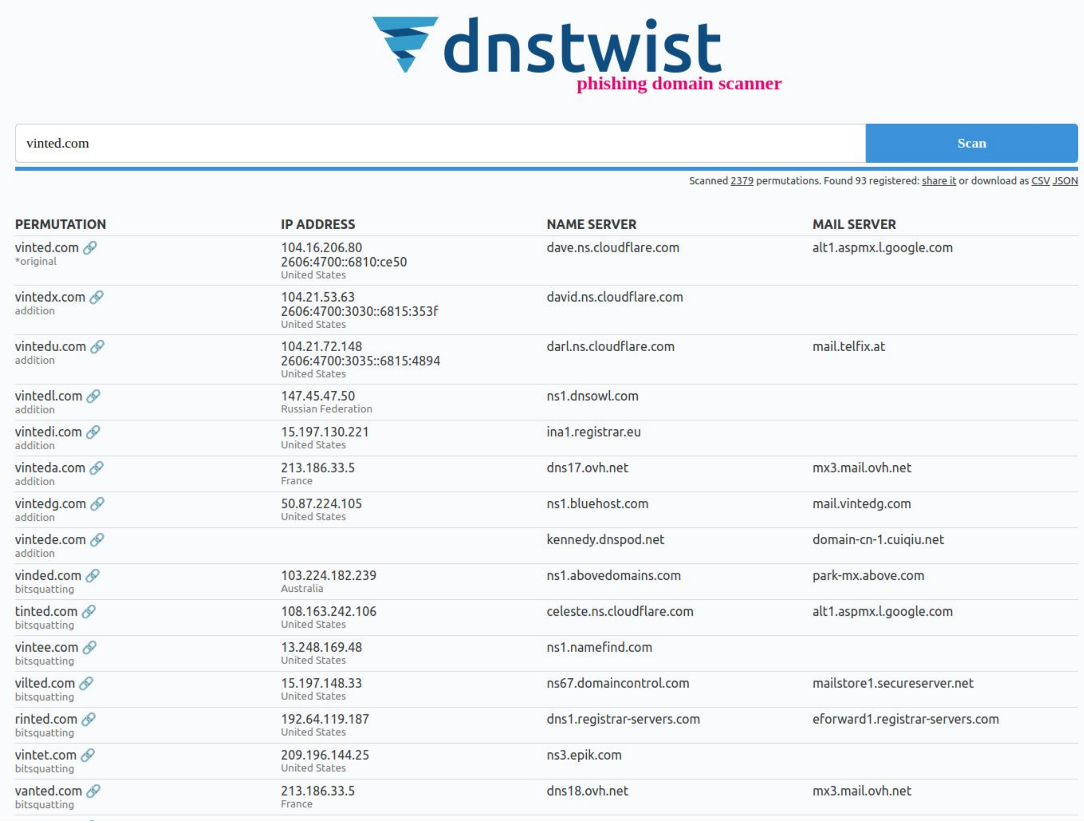


- Graph DB (neo4j) of ssdeep hashes, URLs, and targeted spoofed brands
- Strongly correlated clusters of nodes represent different phishing campaigns derived from a unique source code hosted on a unique domain

Visualizations using https://gephi.github.io/

dnstwist

- Bitsquatting
- Homoglyph
- Hyphenation
- Insertion
- Omission
- Addition
- Repetition
- Replacement
- Transposition
- Subdomain
- Vowel swap
- etc.



Scanned 2379 permutations. Found 93 registered: share it or download as CSV JSON

PERMUTATION	IP ADDRESS	NAME SERVER	MAIL SERVER
vinted.com *original	104.16.206.80 2606:4700::6810:ce50 United States	dave.ns.cloudflare.com	alt1.aspmx.l.google.com
vintedx.com addition	104.21.53.63 2606:4700:3030::6815:353f United States	david.ns.cloudflare.com	
vintedu.com addition	104.21.72.148 2606:4700:3035::6815:4894 United States	darl.ns.cloudflare.com	mail.telfix.at
vintedl.com addition	147.45.47.50 Russian Federation	ns1.dnsowl.com	
vintedi.com addition	15.197.130.221 United States	ina1.registrar.eu	
vinteda.com addition	213.186.33.5 France	dns17.ovh.net	mx3.mail.ovh.net
vintedg.com addition	50.87.224.105 United States	ns1.bluehost.com	mail.vintedg.com
vintede.com addition		kennedy.dnspod.net	domain-cn-1.cuiqiu.net
vinded.com bitsquatting	103.224.182.239 Australia	ns1.abovedomains.com	park-mx.above.com
tinted.com bitsquatting	108.163.242.106 United States	celeste.ns.cloudflare.com	alt1.aspmx.l.google.com
vintee.com bitsquatting	13.248.169.48 United States	ns1.namefind.com	
vilted.com bitsquatting	15.197.148.33 United States	ns67.domaincontrol.com	mailstore1.secureserver.net
rinted.com bitsquatting	192.64.119.187 United States	dns1.registrar-servers.com	eforward1.registrar-servers.com
vintet.com bitsquatting	209.196.144.25 United States	ns3.epik.com	
vanted.com bitsquatting	213.186.33.5 France	dns18.ovh.net	mx3.mail.ovh.net