DNS Abuse in the Age of CoViD-19

IGF 2020 Pre-Event #47
2 November 2020

ICANN

Today’s Agenda

1
Introduction to DNS

2
DNS Abuse: What is It and Why?

3
DNS Abuse and CoViD-19: ICANN’s View

4
DNS Abuse and CoViD-19: CTI-League’s View

Today's Presenters

Elena Plexida
Vice President,
Government & IGO Engagement

Adiel Akplogan
Vice President,
Technical Engagement

Dr. Samaneh Tajalizadehkhoob
Lead Security, Stability, &
Resiliency Specialist

Marc Rogers
Vice President,
Cybersecurity at OKTA
Co-Founder of the CTI-League

Introduction to DNS

The DNS is a Fundamental Internet Technology

E-mail

The DNS was created to solve an e-mail problem.

Elena.Plexida@icann.org

Everything to the right of the @ sign uses the DNS to resolve.

The World Wide Web

Humans do not easily remember IP addresses

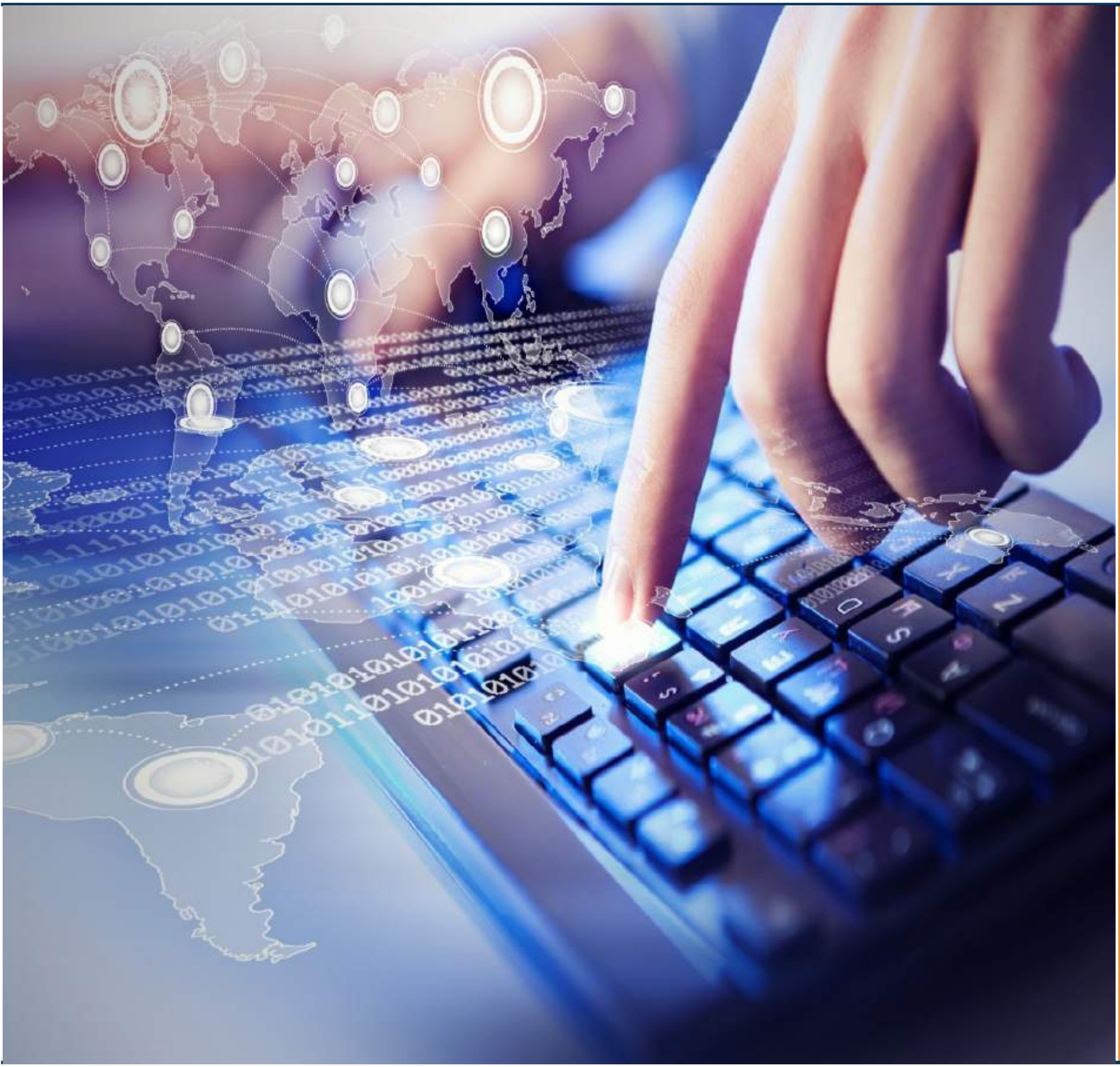
Instead of navigating to 192.0.7.10, it is much easier to navigate to www.icann.org.

And it is a lot easier to remember!

Brands

The domain name is a brand identity, regardless of whether an organization is commercial, governmental, educational, or otherwise.

Internet Users Expect the DNS Will Always Work



Most Internet users are not aware of the DNS.

They do not realize they use it 100+ times each day.

In turn, the expect it will **always** work. If it does not work, they call their ISP and report “The Internet is down!”

Users Expect the DNS Will be Secure

A Secure DNS

Internet users can navigate to the correct sites

E-mail is delivered properly to the intended recipient

Apps can be trusted to do what they are expected to do

VS

An Insecure DNS

Navigation unexpectedly takes us to the wrong site

Our computing devices become infected with malware

Our identities or our money are stolen from us

Introduction to DNS Abuse

Cyber Criminals Target the DNS

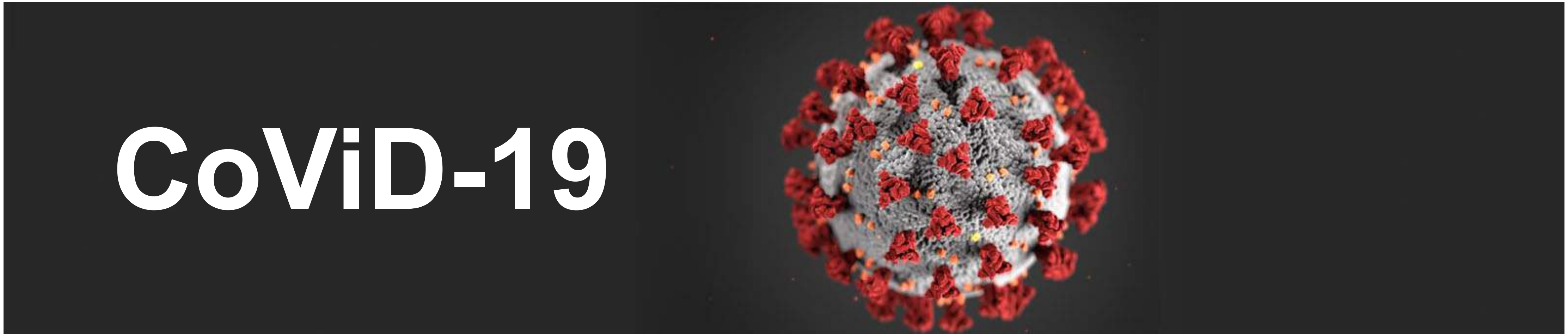
The DNS is an invaluable tool for bad actors. It can be targeted to aid criminals in their attacks against sites and on individuals.

DNS Abuse

- Disrupt the DNS and you disrupt merchant transactions, government services, social networks
- Exploit the DNS and you can trick, defraud or deceive users
- Vectors for exploitation:
  - Maliciously register domain names
  - Hijack the process the DNS uses to “resolve” the IP address behind a domain name
    - Cache Poisoning
  - Hijack the registration process or data that underpins the DNS
  - Corrupt the DNS data on devices
    - Malware that changes a device’s resolver ← **this is *really bad* and hard to detect**

Users are Generally Unaware of DNS Abuse

Enter the Pandemic



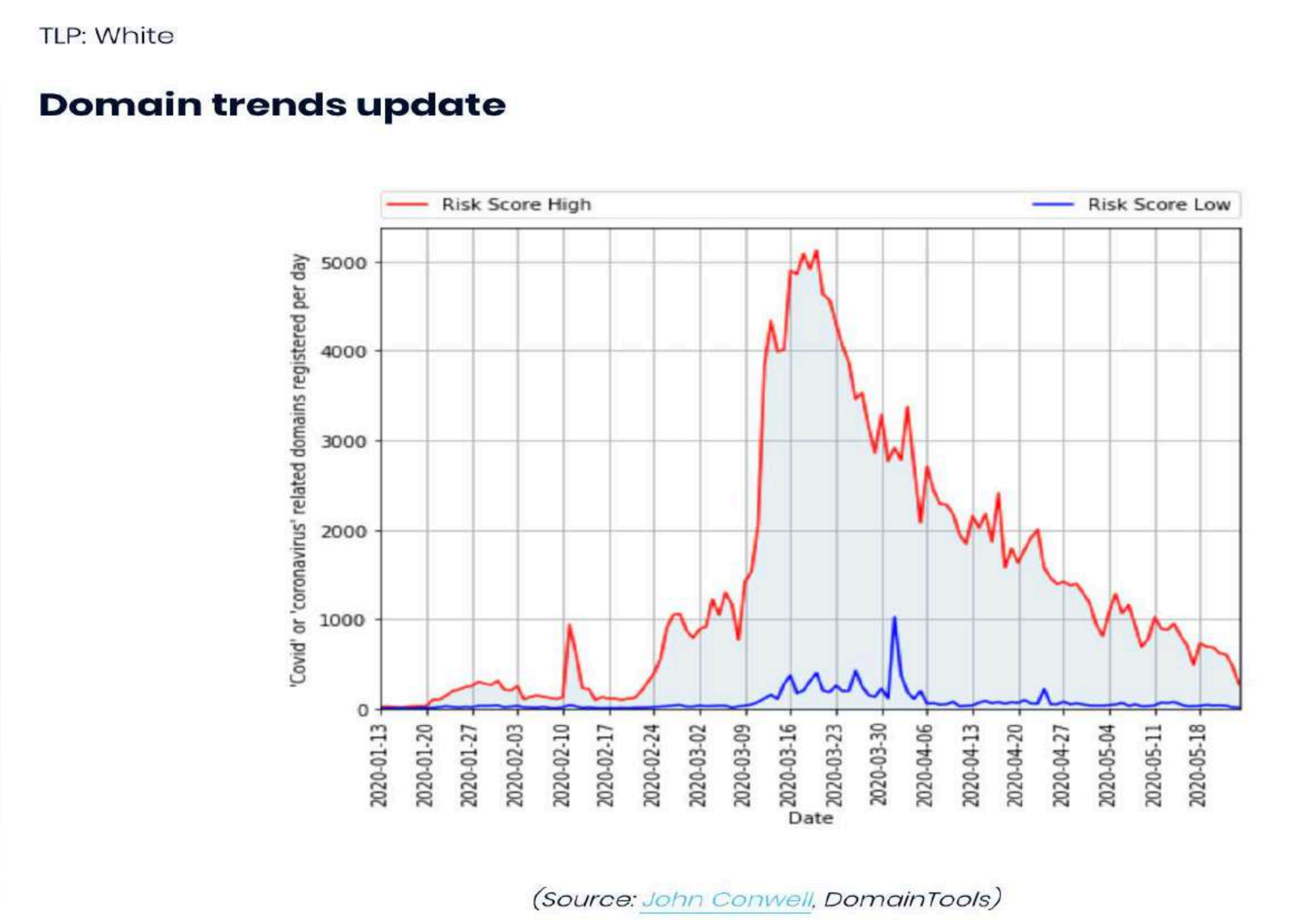
What happens when you combine the motivation of bad actors to attack the DNS with a global pandemic?

DNS Abuse in the Age of CoViD-19: ICANN’s View

Context

- Big events have associated bursts of domain name registration
- COVID-19 no different
  - – The extra related stress, worry and working from home makes it the perfect storm

Context



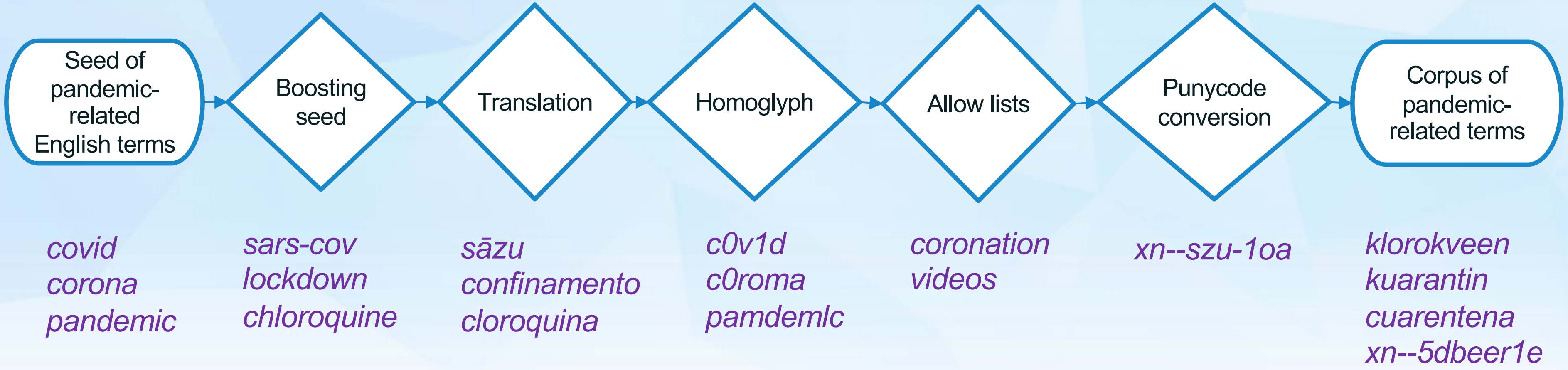
TLP: White

Domain trends update

(Source: John Conwell, DomainTools)

How Does our Identification Approach Work?

- Our approach for identification:
  - – Pandemic-related keyword search within zone files (gTLDs + a few ccTLDs)



Seed of pandemic-related English terms

covid
corona
pandemic

Boosting seed

sars-cov
lockdown
chloroquine

Translation

sāzu
confinamento
cloroquina

Homoglyph

c0v1d
c0roma
pamdemlc

Allow lists

coronation
videos

Punycode conversion

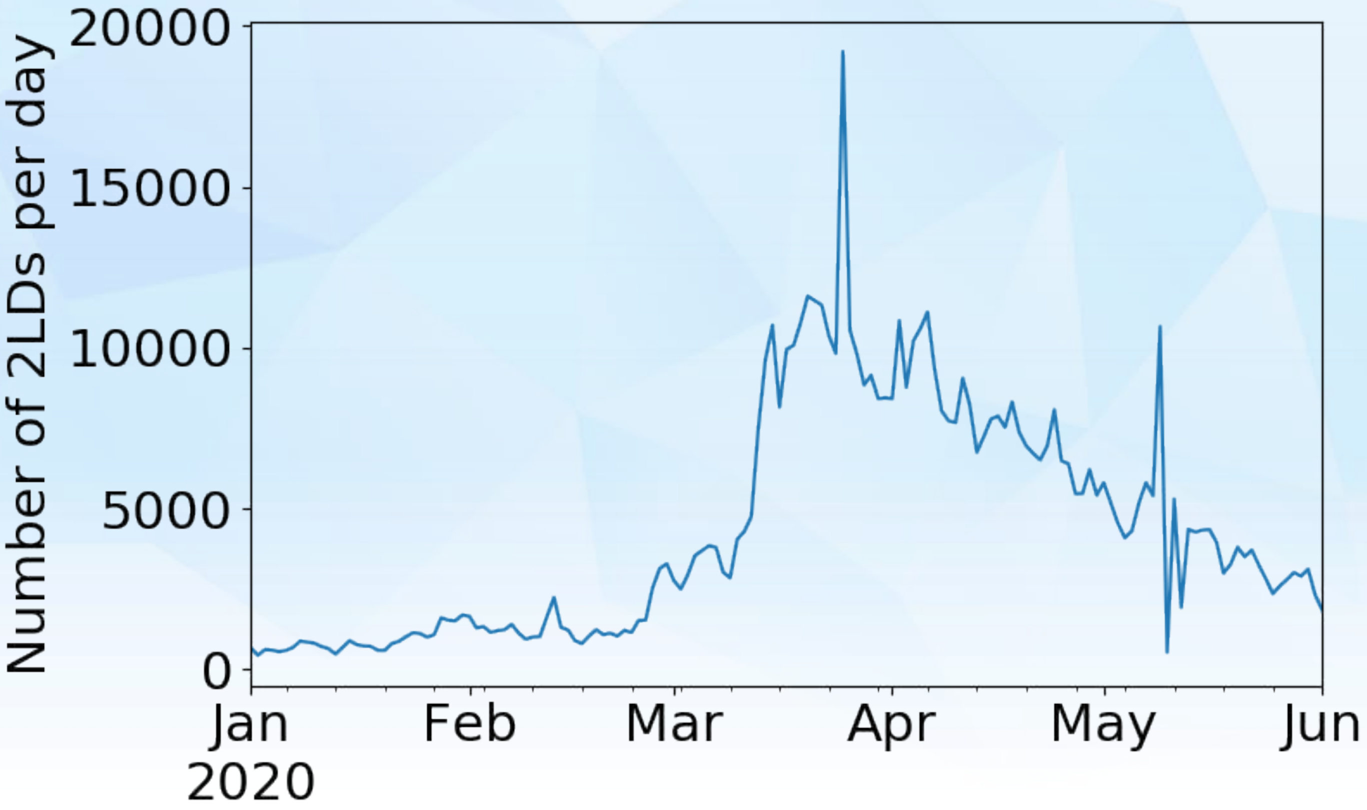
xn--szu-1oa

Corpus of pandemic-related terms

klorokveen
kuarantin
cuarentena
xn--5dbeer1e

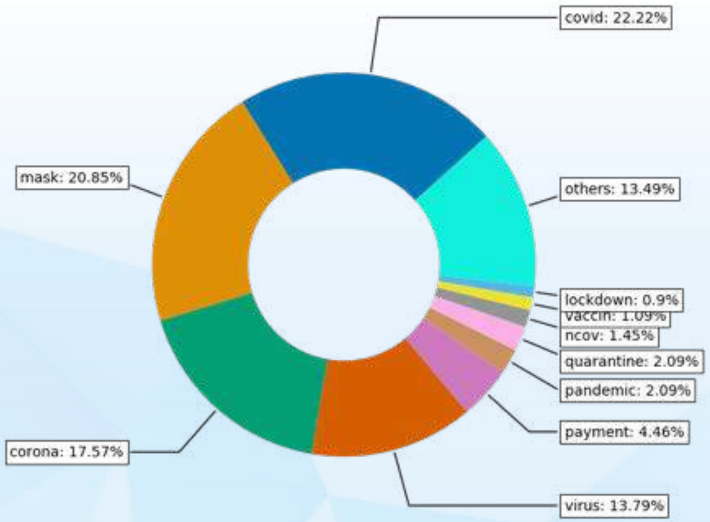
How Many Domains Have We Identified?

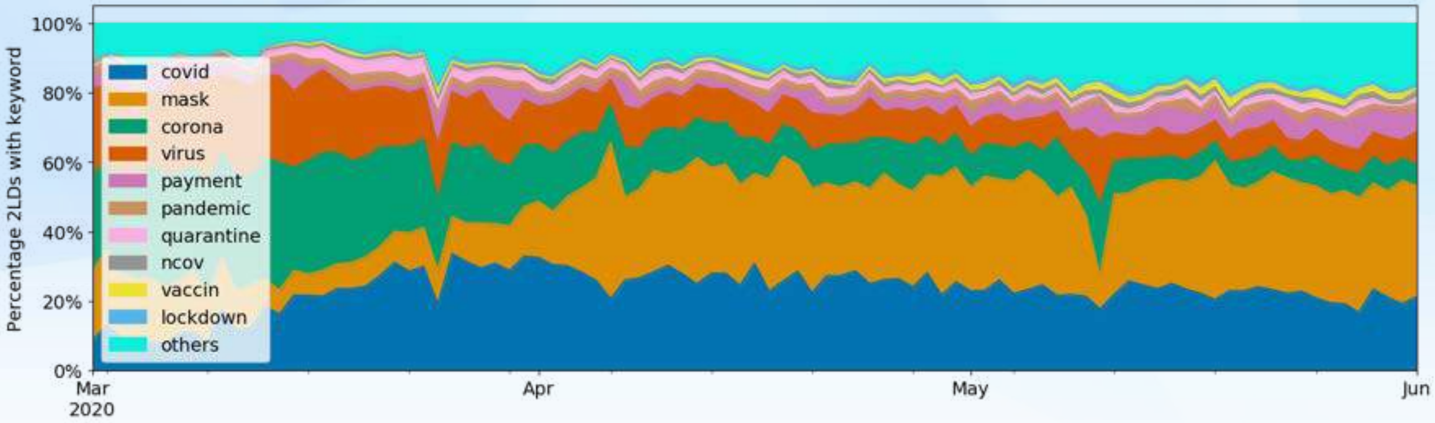
- 662,111 domains were identified since January 2020

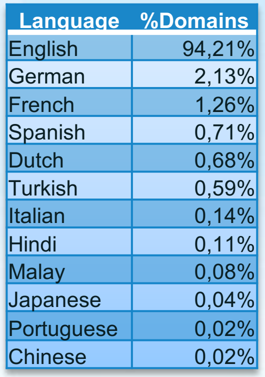


What Keywords do These Domains Contain?

- Most of the domains related to 3 keywords
  - 4 keywords account for 73% of the domains
  - Different keywords categories:
    - Disease name (covid, ncov, sars, …)
    - Pandemic countermeasures (mask, lockdown, quarantine,…)
    - Collateral (zoom, webex, conference, …)
  - Significant number of domains matches non-English terms







Language	%Domains
English	94,21%
German	2,13%
French	1,26%
Spanish	0,71%
Dutch	0,68%
Turkish	0,59%
Italian	0,14%
Hindi	0,11%
Malay	0,08%
Japanese	0,04%
Portuguese	0,02%
Chinese	0,02%

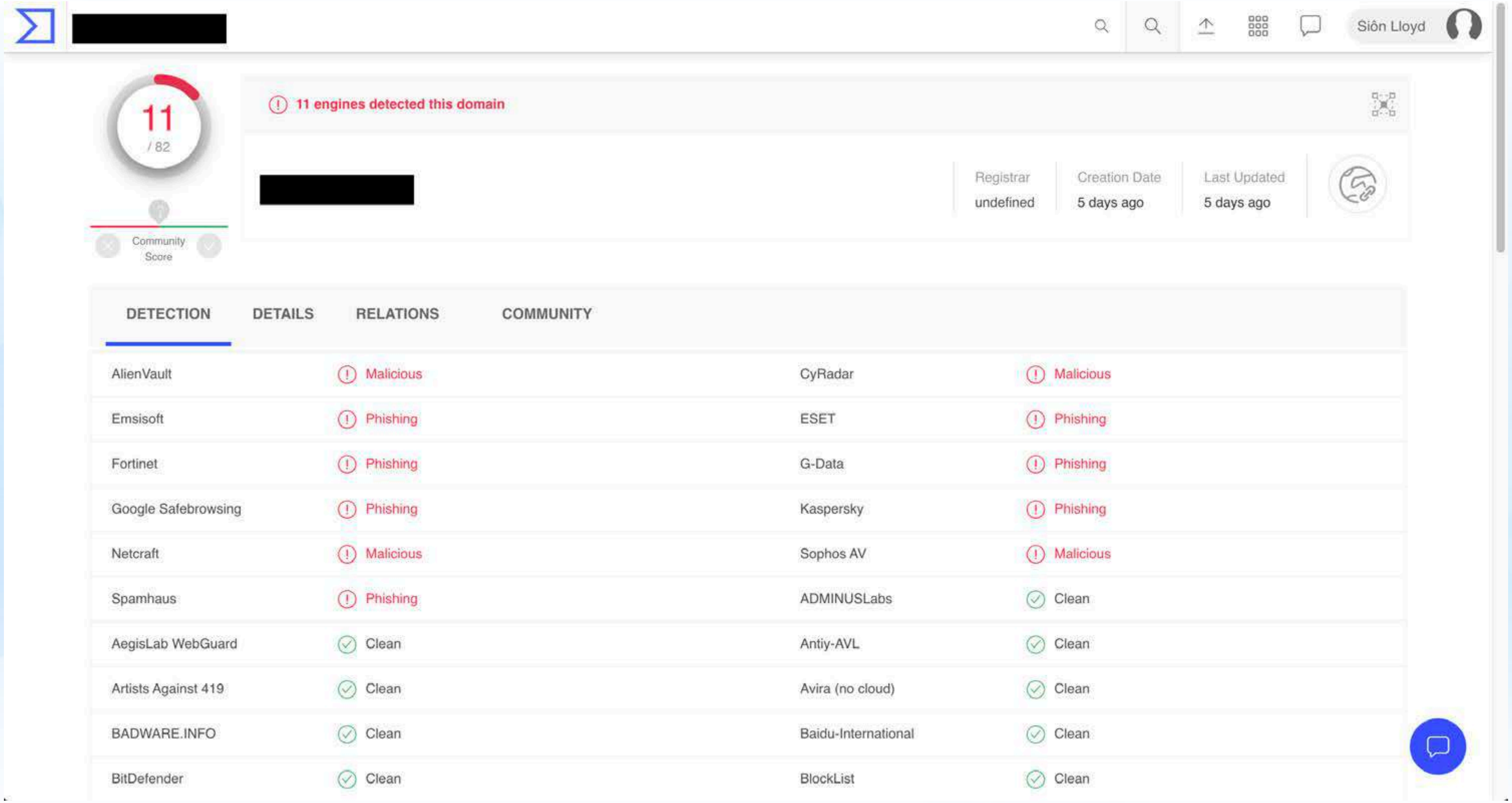
Interpretation?

This is “data”, **not** “intelligence”

There will be benign domains, unrelated domains, defensive registrations, parked domains… along with anything malicious

What **evidence** can we find, do we trust it?

API Calls – VirusTotal



[redacted]

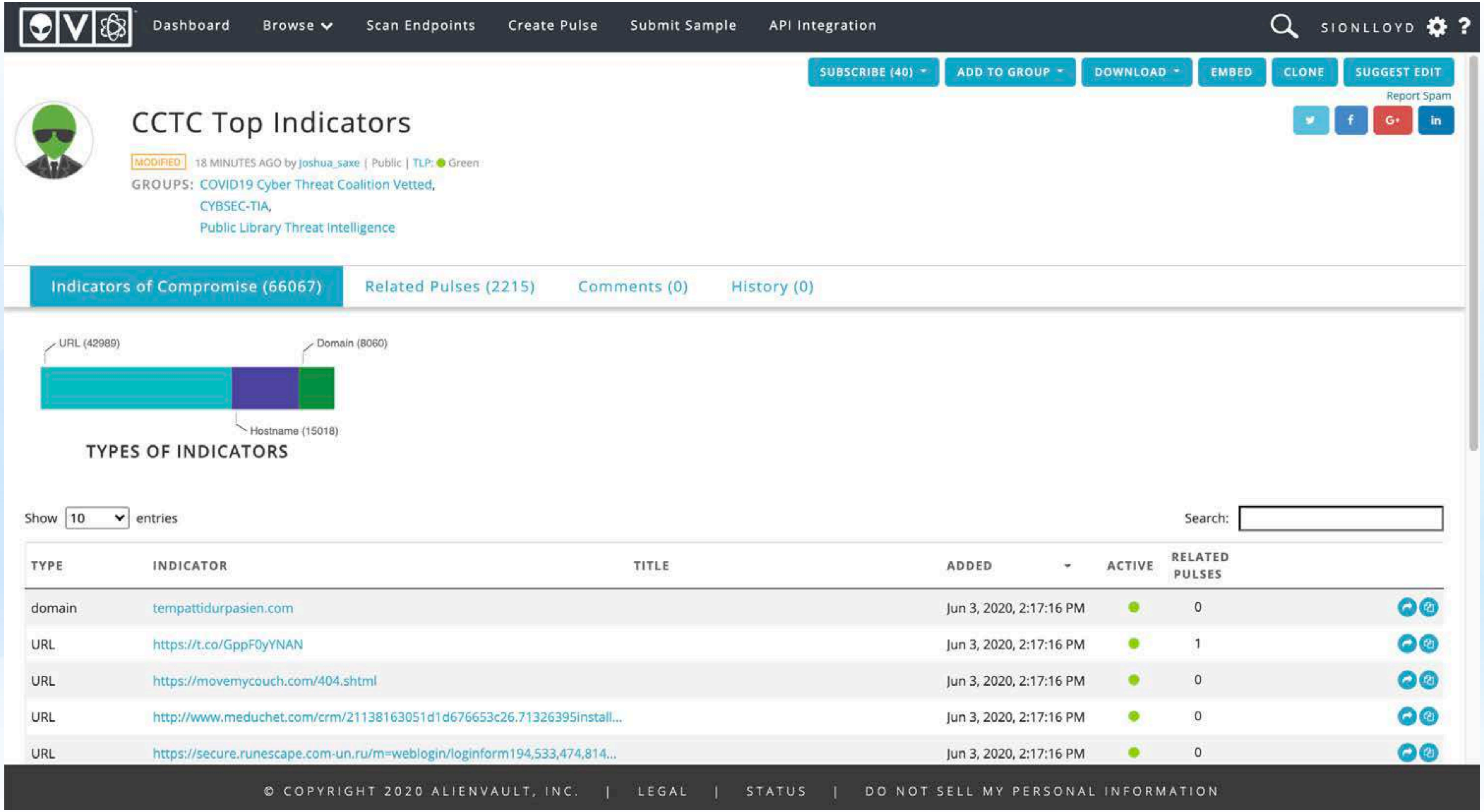
11 engines detected this domain

[redacted]

Registrar	Creation Date	Last Updated
undefined	5 days ago	5 days ago

AlienVault	Malicious	CyRadar	Malicious
Emsisoft	Phishing	ESET	Phishing
Fortinet	Phishing	G-Data	Phishing
Google Safebrowsing	Phishing	Kaspersky	Phishing
Netcraft	Malicious	Sophos AV	Malicious
Spamhaus	Phishing	ADMINUSLabs	Clean
AegisLab WebGuard	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	Avira (no cloud)	Clean
BADWARE.INFO	Clean	Baidu-International	Clean
BitDefender	Clean	BlockList	Clean

API Calls - AlienVaultOTX



CCTC Top Indicators

MODIFIED 18 MINUTES AGO by Joshua_saxe | Public | TLP: ● Green

GROUPS: COVID19 Cyber Threat Coalition Vetted,
CYBSEC-TIA,
Public Library Threat Intelligence

Indicators of Compromise (66067) | Related Pulses (2215) | Comments (0) | History (0)

TYPES OF INDICATORS

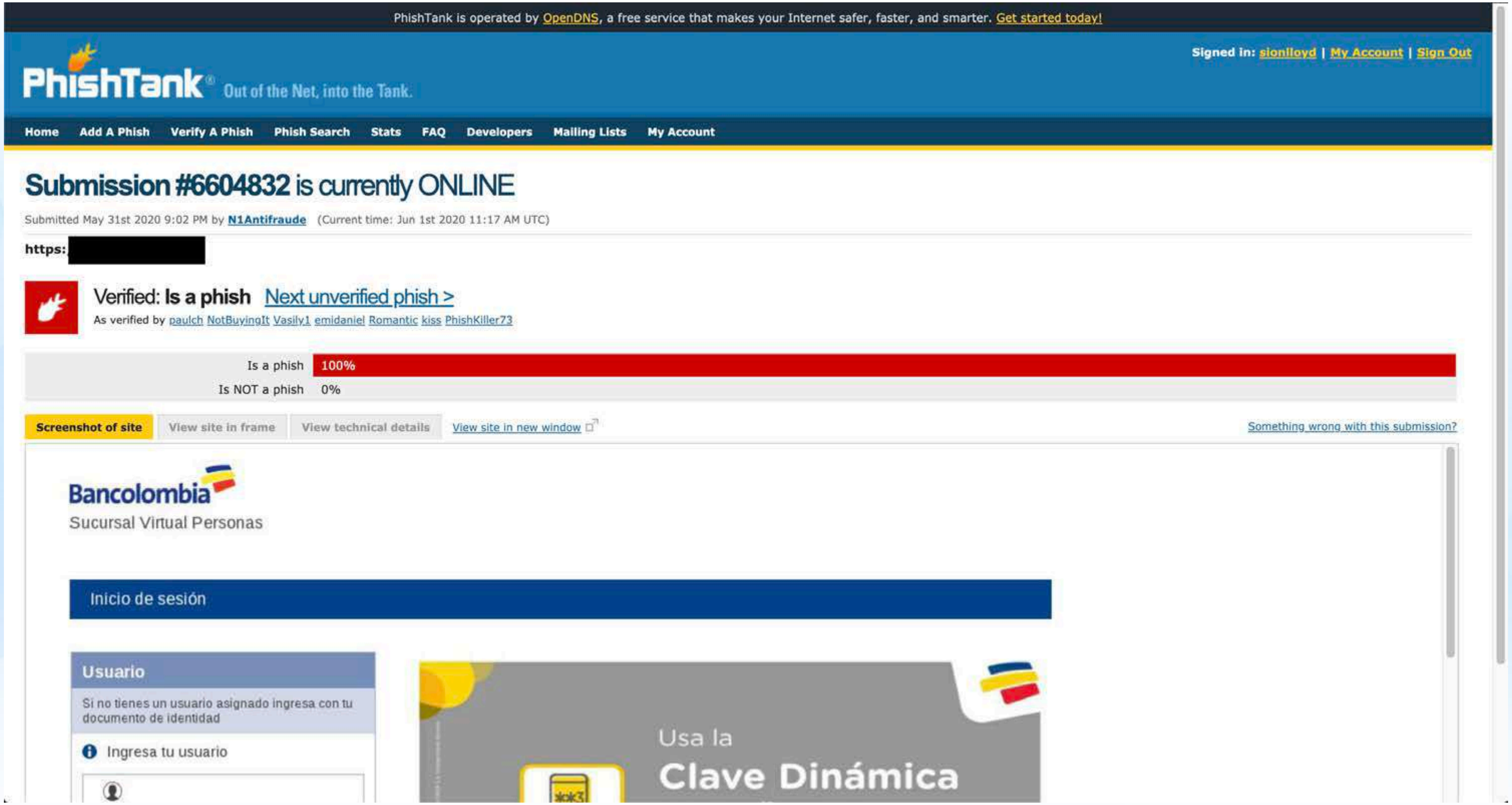
Show 10 entries

Search:

TYPE	INDICATOR	TITLE	ADDED	ACTIVE	RELATED PULSES
domain	tempattidurpasien.com		Jun 3, 2020, 2:17:16 PM	●	0
URL	https://t.co/GppF0yYNAN		Jun 3, 2020, 2:17:16 PM	●	1
URL	https://movemycouch.com/404.shtml		Jun 3, 2020, 2:17:16 PM	●	0
URL	http://www.meduchet.com/crm/21138163051d1d676653c26.71326395install...		Jun 3, 2020, 2:17:16 PM	●	0
URL	https://secure.runescape.com-un.ru/m=weblogin/loginform194,533,474,814...		Jun 3, 2020, 2:17:16 PM	●	0

© COPYRIGHT 2020 ALIENVAULT, INC. | LEGAL | STATUS | DO NOT SELL MY PERSONAL INFORMATION

API Calls - Phishtank



PhishTank is operated by OpenDNS, a free service that makes your Internet safer, faster, and smarter. Get started today!

Signed in: sionlloyd | My Account | Sign Out

Submission #6604832 is currently ONLINE

Submitted May 31st 2020 9:02 PM by N1Antifraude (Current time: Jun 1st 2020 11:17 AM UTC)

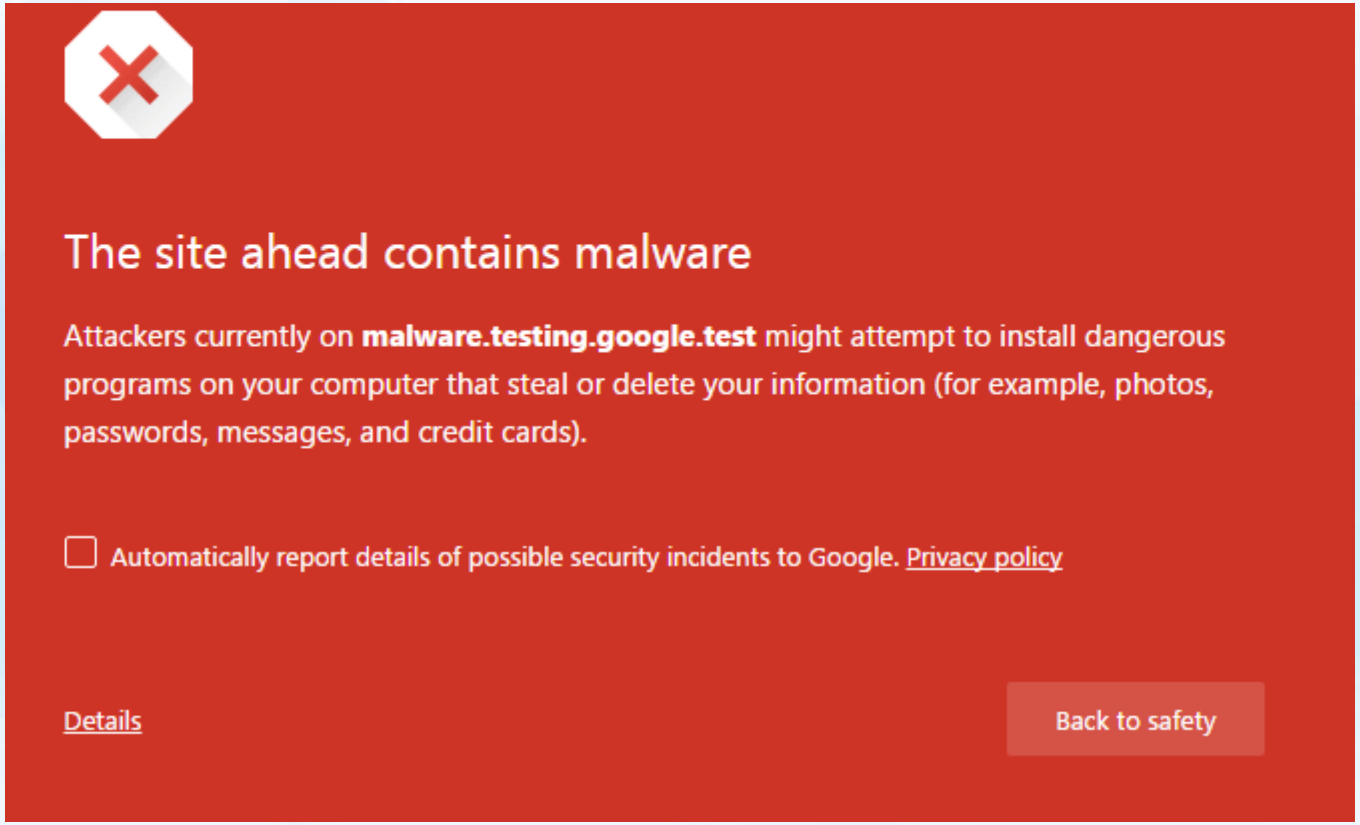
https:[redacted]

Verified: **Is a phish** Next unverified phish >

As verified by paulch NotBuyingIt Vasily1 emidaniel Romantic kiss PhishKiller73

Is a phish	100%
Is NOT a phish	0%

API Calls – Google Safe Browsing



The site ahead contains malware

Attackers currently on **malware.testing.google.test** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards).

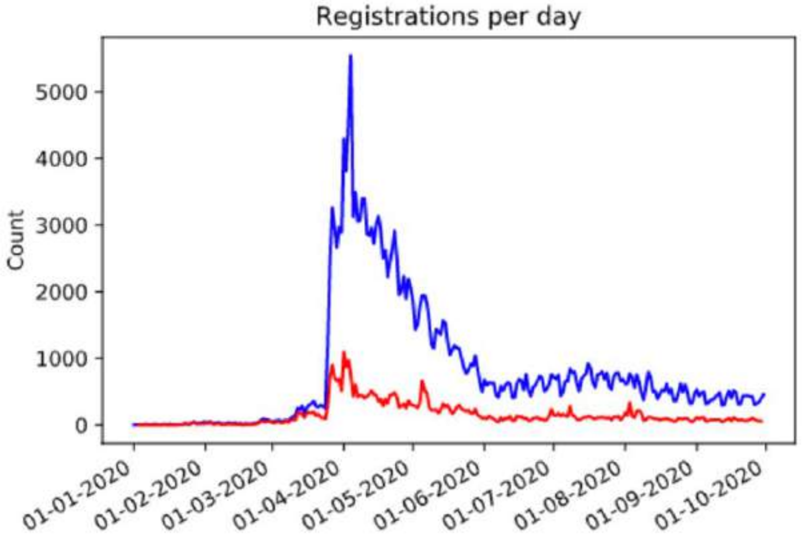
□ Automatically report details of possible security incidents to Google. Privacy policy

Domain Name Security Threat Identification, Collection and Reporting (DNSTICR)

- Jan 2020 to Sep 2020
  - Detected 235,521 pandemic-related domains (both legit and malicious)
  - Only phishing and malware distribution

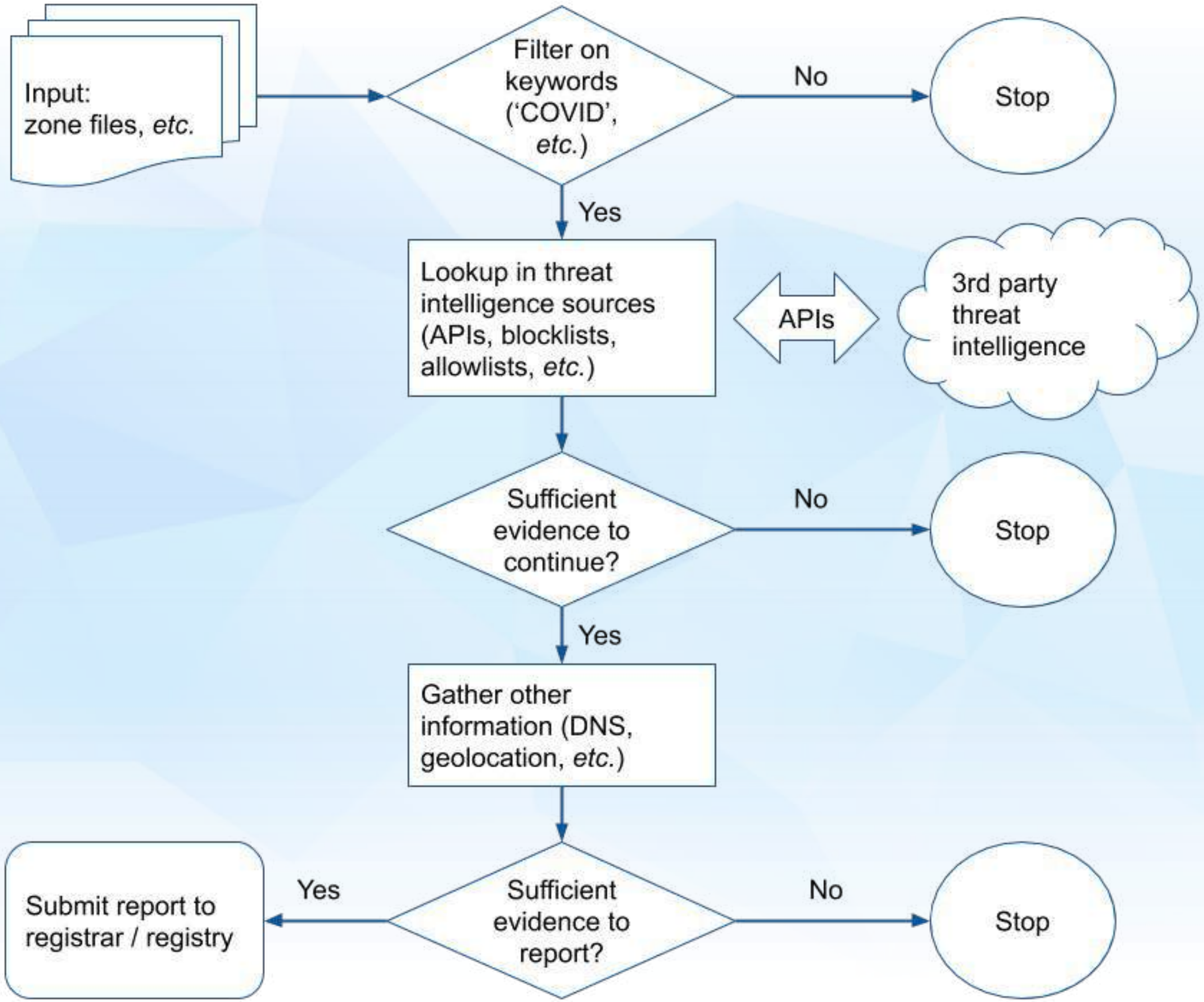
- May 2020 to Sep 2020
  - Consistent collection and analysis period
    - Detected 134,332 pandemic-related domains (both legit and malicious)
    - Of these, 8,577 (6.4%) domains had one or more reports in phishing/malware reputation lists **and** had nameservers or resolved to an IP address
    - High confidence reports: 2,329 (1.7%) domains

- Reporting of high confidence domains to registrars started in June



Registrations per day matching one or more of our filter terms (blue line) plus those which had one or more third-party reports (red line). Dates in DD-MM-YYYY format.

Reporting Data Flow


Input:
zone files, *etc.*
Filter on keywords ('COVID', *etc.*)
No
Stop
Yes
Lookup in threat intelligence sources (APIs, blocklists, allowlists, *etc.*)
APIs
3rd party threat intelligence
Sufficient evidence to continue?
No
Stop
Yes
Gather other information (DNS, geolocation, *etc.*)
Submit report to registrar / registry
Yes
Sufficient evidence to report?
No
Stop

COVID-19: Our Output

Roughly an order of magnitude lost at each gate:

- Thousands of registrations per day
- Some reports on hundreds
- Sufficient evidence on tens

Conclusion

There is definitely bad stuff out there!

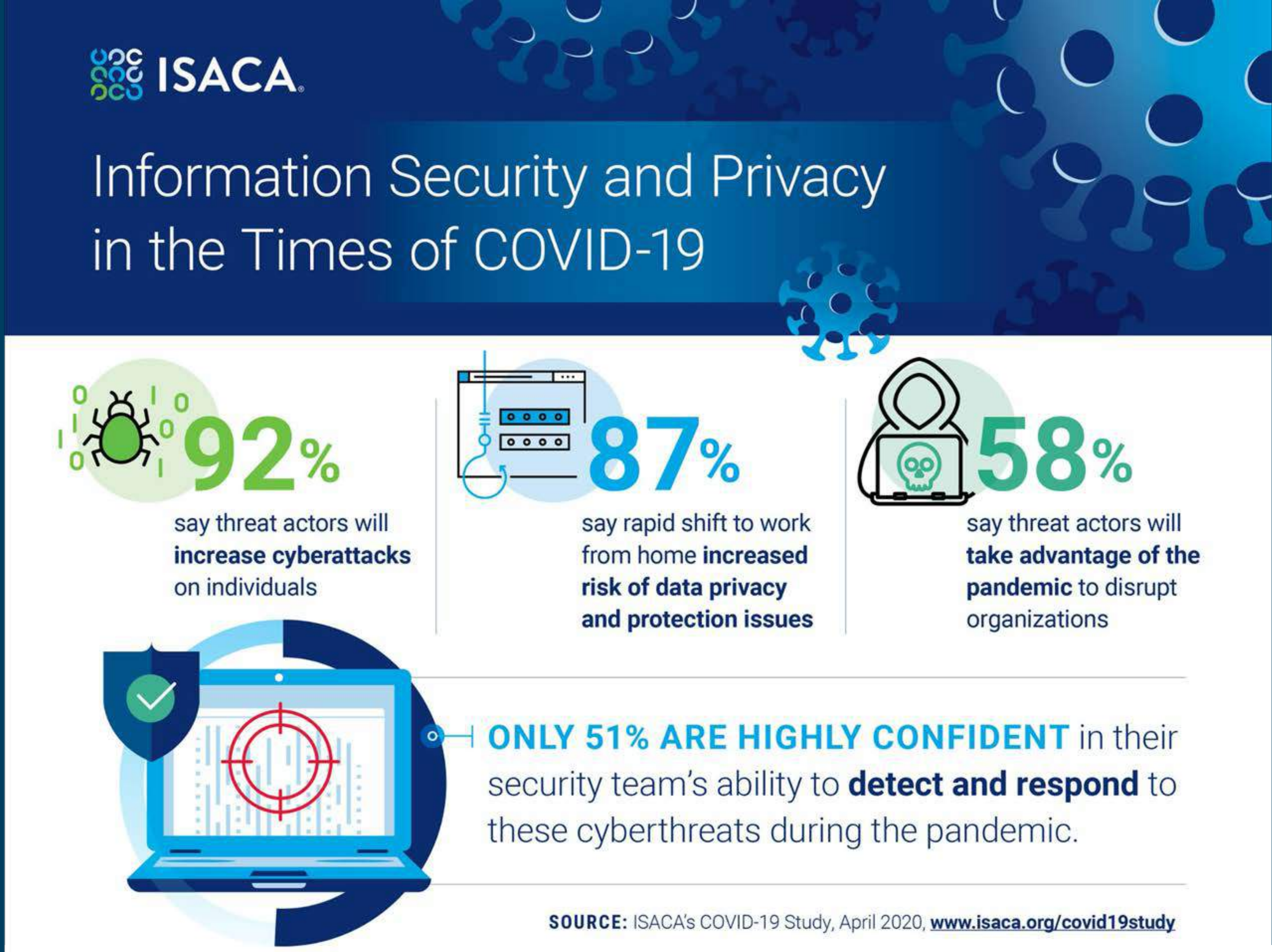
BUT: it is not anywhere near the levels that some figures would suggest

DNS Abuse in the Age of CoViD-19: CTI-League’s View

Most Companies Were Rushed into Pandemic Operations

Yet 25,000+ CVEs (vulnerabilities) reported by September

(Previous record 16,500+ in 2018)



ISACA

Information Security and Privacy in the Times of COVID-19

92% say threat actors will **increase cyberattacks** on individuals

87% say rapid shift to work from home **increased risk of data privacy and protection issues**

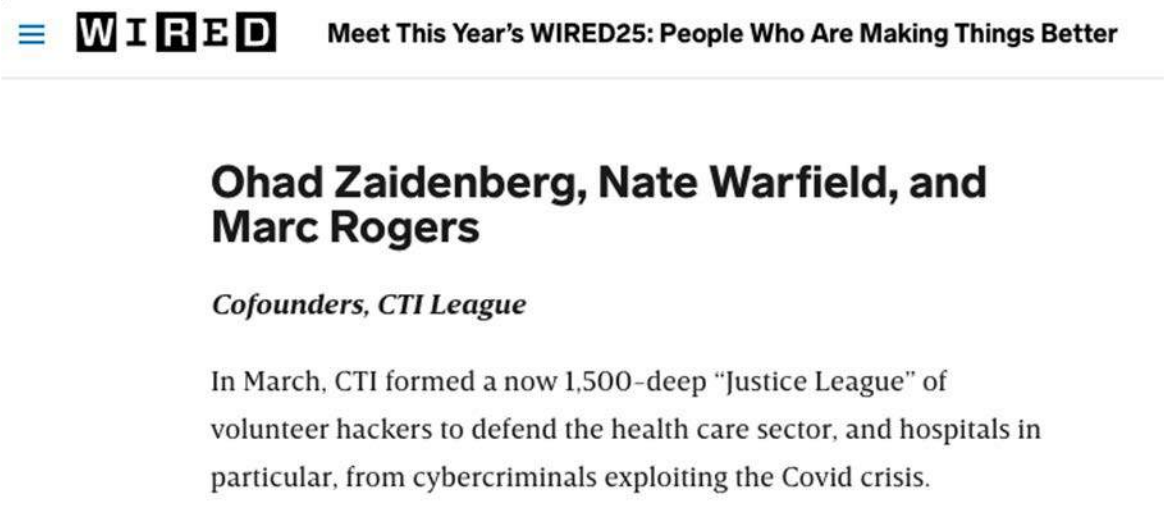
58% say threat actors will **take advantage of the pandemic** to disrupt organizations

ONLY 51% ARE HIGHLY CONFIDENT in their security team's ability to **detect and respond** to these cyberthreats during the pandemic.

SOURCE: ISACA's COVID-19 Study, April 2020, www.isaca.org/covid19study

The CTI league

- A globally distributed team, for a globally distributed problem.
- Defending the medical industry is hard.
- >70% of medical facilities in the US are small with no dedicated security resources.
- If large institutions are struggling to keep up with patching what hope do we have with smaller ones?
- Attackers are smart enough to target weaker linked organizations first.



Meet This Year's WIRED25: People Who Are Making Things Better

Ohad Zaidenberg, Nate Warfield, and Marc Rogers

Cofounders, CTI League

In March, CTI formed a now 1,500-deep "Justice League" of volunteer hackers to defend the health care sector, and hospitals in particular, from cybercriminals exploiting the Covid crisis.

CTI LEAGUE

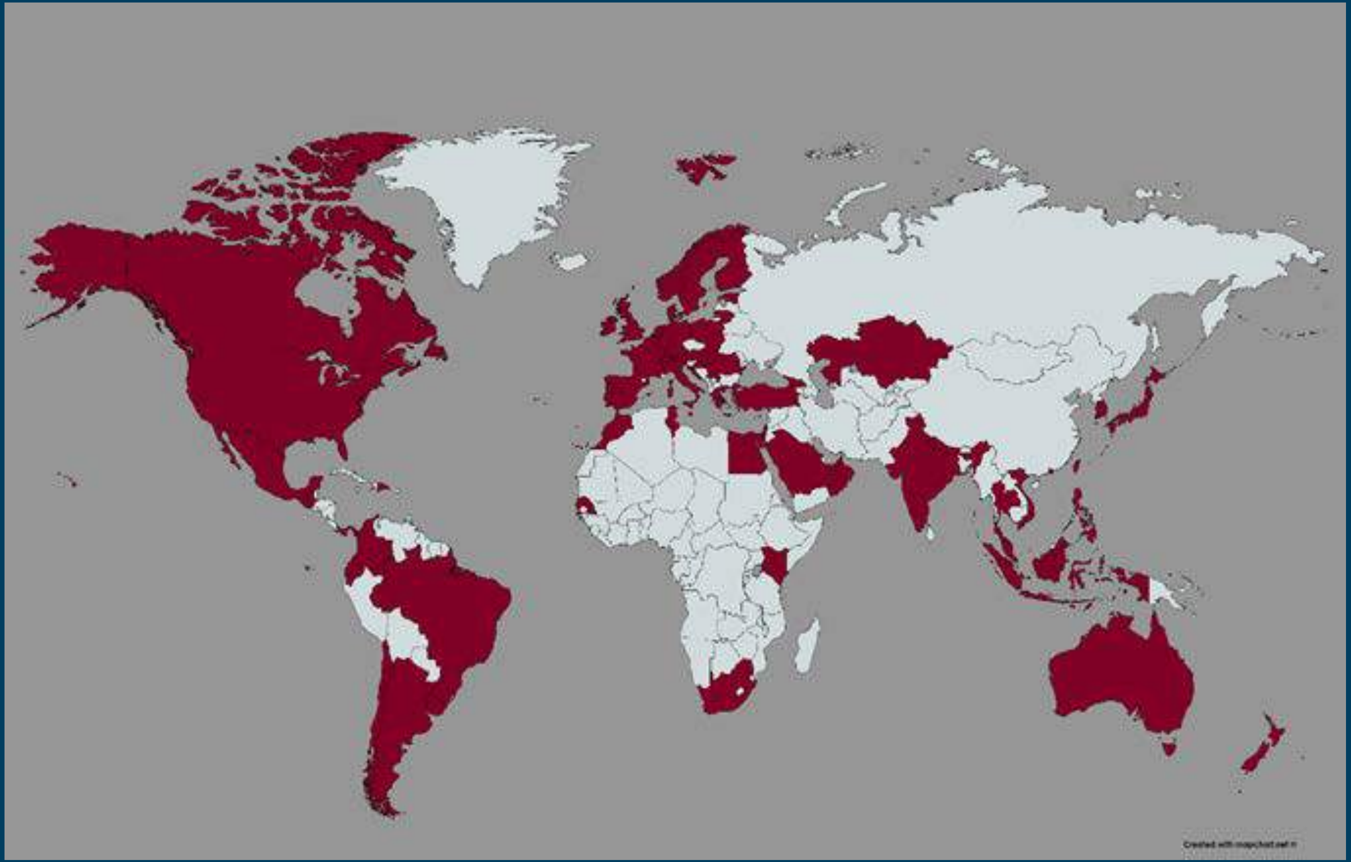
https://CTI-League.com

CTI-League demographics

- The CTI-League is a cross-industry, volunteer org co-founded by Marc Rogers, VP Cybersecurity at Okta

- 1500+ members cover 80 countries and 22 timezones
  - 10% from GOV/LEO worldwide
  - 6% from national CERT’s
  - 7% medical and health sector
  - 77% Infosec

- CTI League mission: To protect the healthcare sector during the pandemic



Created with mapchart.net ©

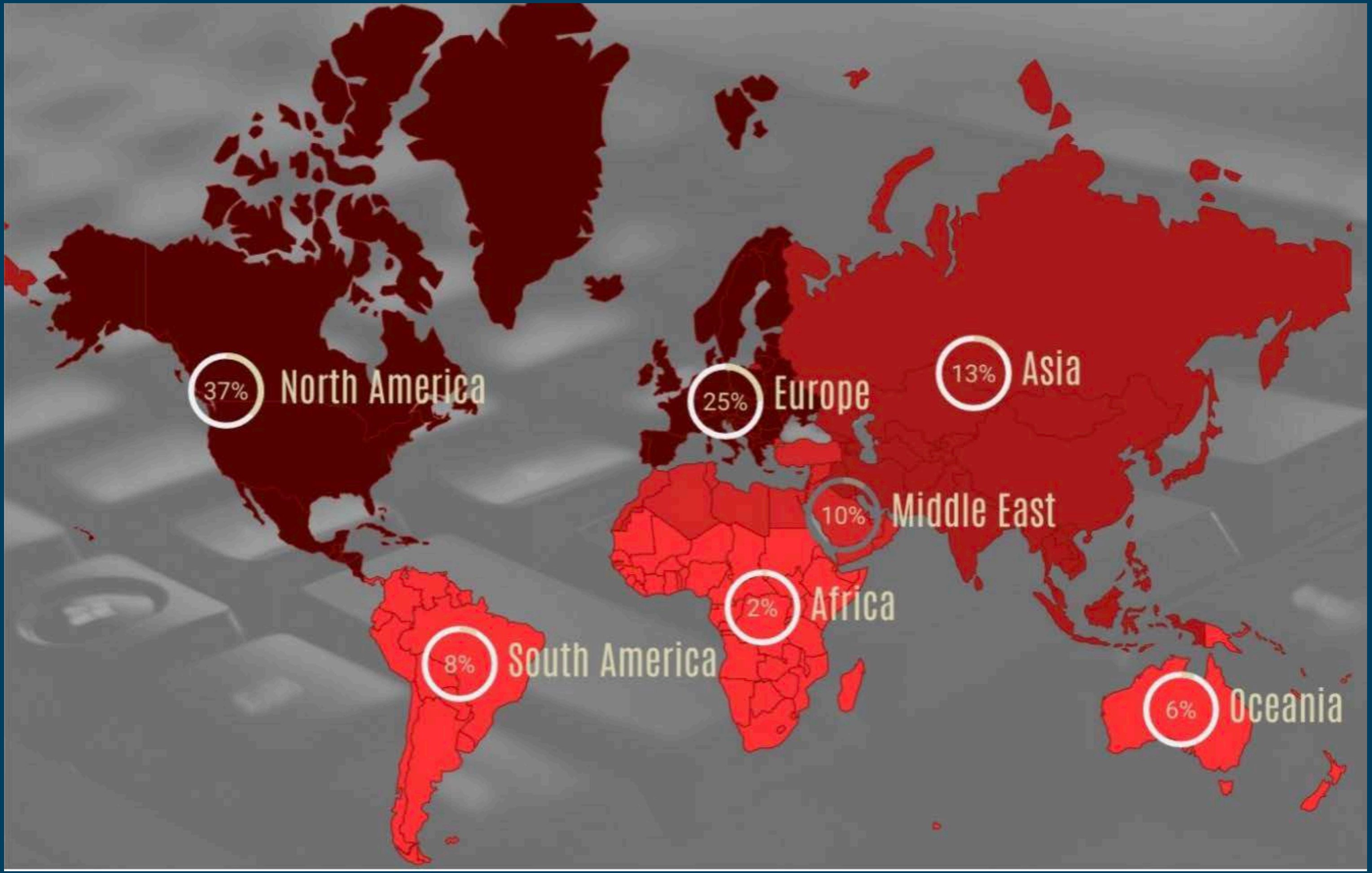
Globally Threat Landscape.

More than half of attacks against healthcare organizations originate from US and EU countries.

Origination does not equal attribution.

Many campaigns have complex infrastructure established globally in advance.

Attacks against healthcare organizations are a global problem.



Source: Upcoming CTI League darknet report.

Collaboration

Much of What is Being Found, Exploited is **Old**

Results:
Medical Vulnerabilities Triaged by CTI-League in 1st Month

Total vulnerabilities detected in one month: 2,000+ found in high risk medical organizations

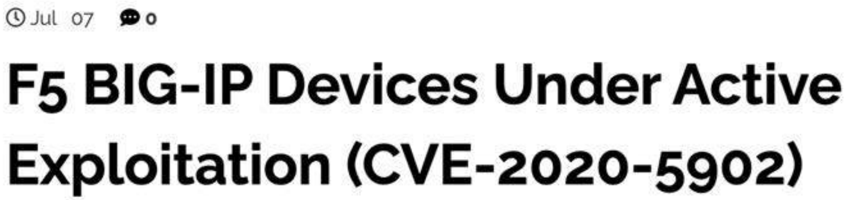
Sample of Vulnerabilities detected in just one week:

RCE vulnerability – 22
BlueKeep vulnerability – 2
SMBv3 open ports – 2
Citrix Gateway servers – 21
Less prioritized CVE vulnerabilities – 5
Exposed Xero Universal Viewer instances – 3

Data from CTI-League Report, March 2020

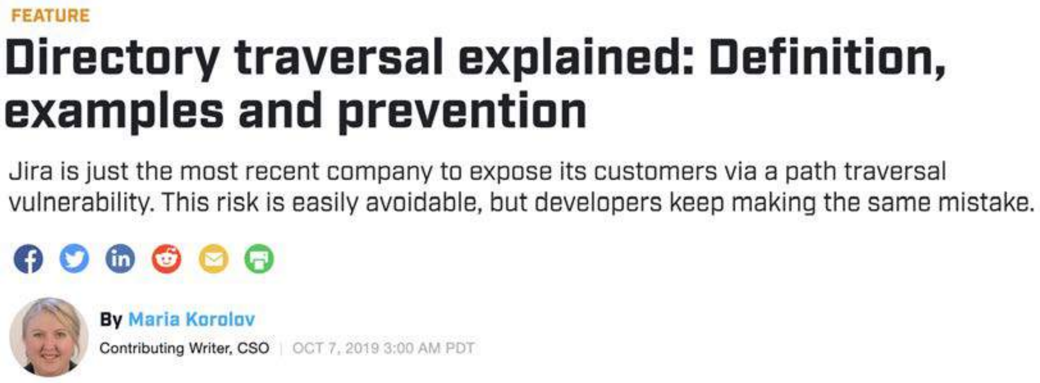
However, we also need to learn from past mistakes.

- 2020 has seen some of the simplest critical exploits released since **1990**.
  - Ex: Same directory traversal methodology resulted in CITRIX, and F5 critical vulnerabilities.
- Worse, many initial assessments have been inaccurate
- Organizations large and small are failing to keep up with volume of patches



Jul 07 0

F5 BIG-IP Devices Under Active Exploitation (CVE-2020-5902)

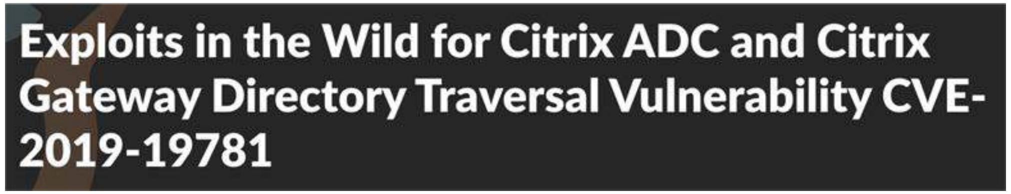


FEATURE

Directory traversal explained: Definition, examples and prevention

Jira is just the most recent company to expose its customers via a path traversal vulnerability. This risk is easily avoidable, but developers keep making the same mistake.

By Maria Korolov
Contributing Writer, CSO | OCT 7, 2019 3:00 AM PDT



Exploits in the Wild for Citrix ADC and Citrix Gateway Directory Traversal Vulnerability CVE-2019-19781

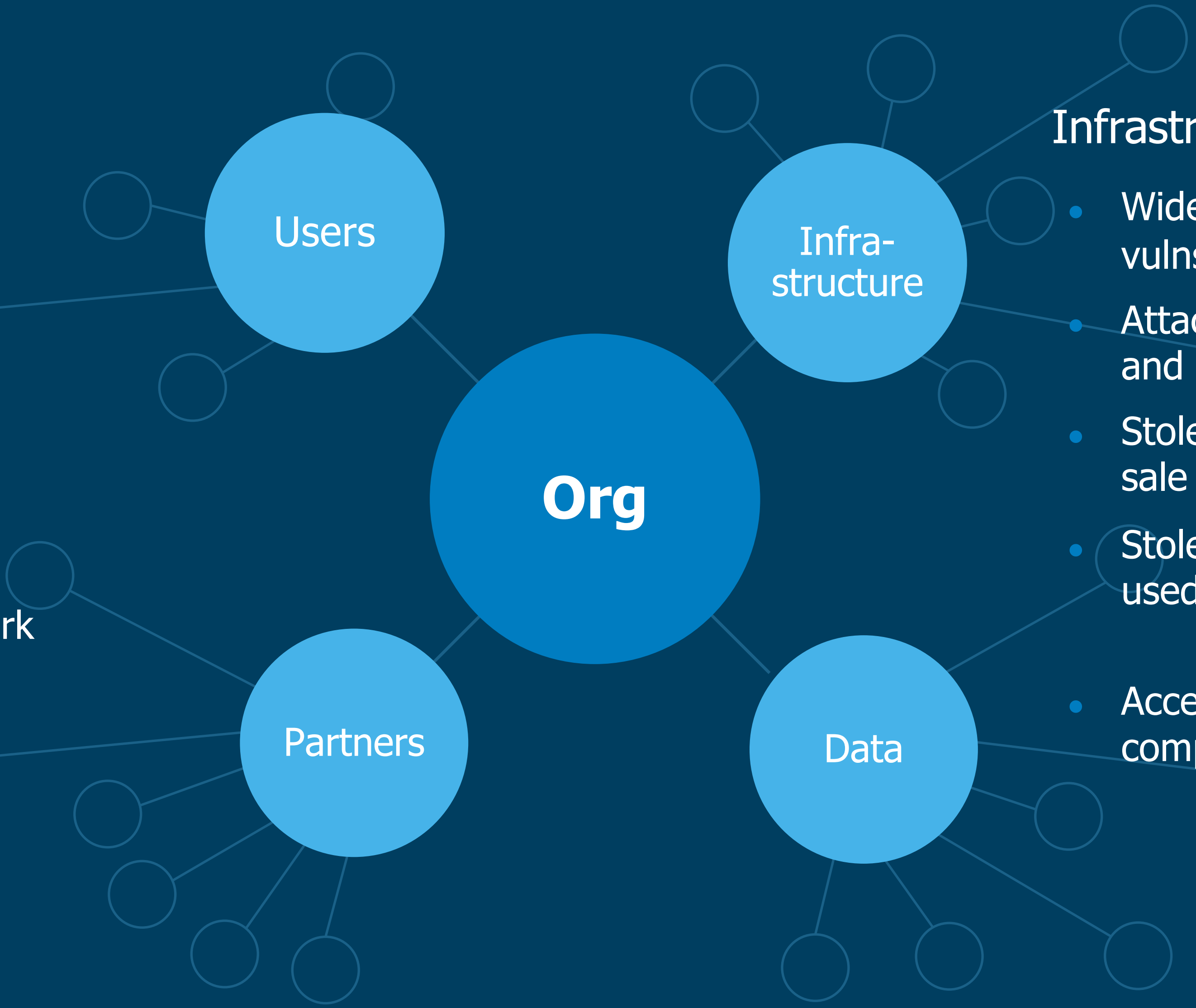
Broad Spectrum of Threats with a Broad Spectrum of Goals

Individual Employees

- Account and identity theft
- Internal tool compromise

Partners

- Attackers routinely "work the chain of trust" attacking smaller organizations as a way into larger ones



Infrastructure + Data

- Wide use of infrastructure vulns against medical facilities
- Attackers are after Data, IP and Access
- Stolen data routinely found for sale on darkweb
- Stolen accounts are sold or used to enrich other forms of attacks
- Access to compromised companies sold for bitcoin

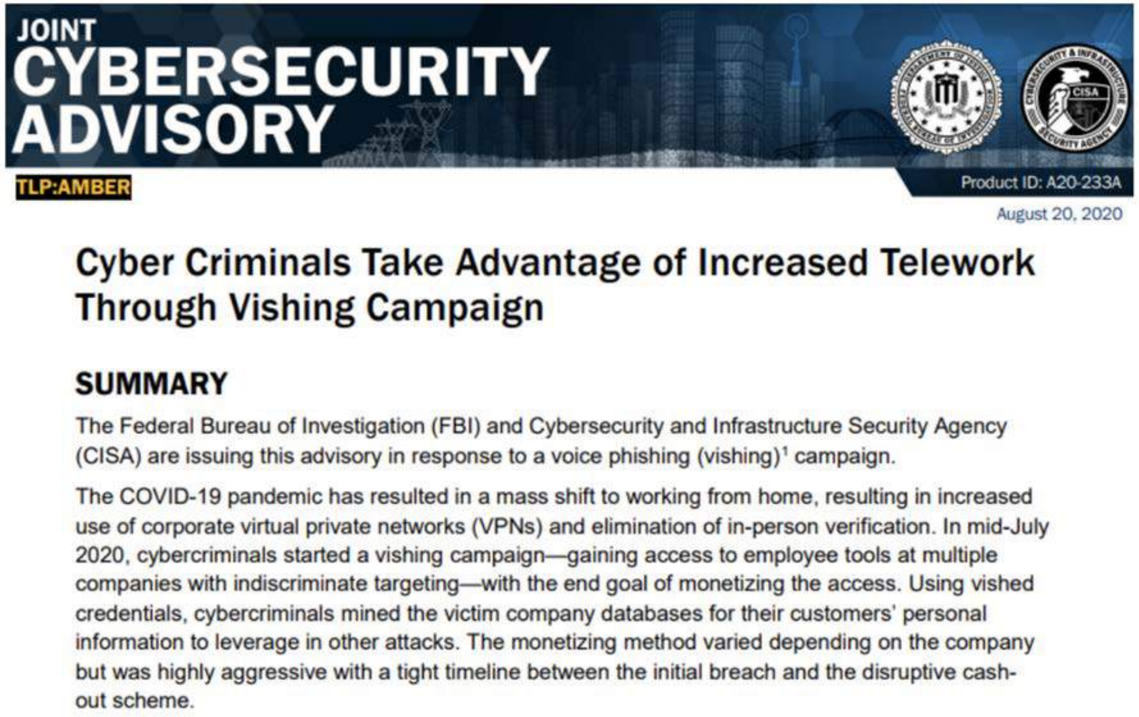
Simplest Attacks Are the Most Effective

Isolation leaves employees vulnerable

Major vishing and phishing campaigns on-going

Simple vector: sophisticated execution

People are primary targets in 2020



JOINT CYBERSECURITY ADVISORY

TLP:AMBER

Product ID: A20-233A

August 20, 2020

Cyber Criminals Take Advantage of Increased Telework Through Vishing Campaign

SUMMARY

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are issuing this advisory in response to a voice phishing (vishing)[1] campaign.

The COVID-19 pandemic has resulted in a mass shift to working from home, resulting in increased use of corporate virtual private networks (VPNs) and elimination of in-person verification. In mid-July 2020, cybercriminals started a vishing campaign—gaining access to employee tools at multiple companies with indiscriminate targeting—with the end goal of monetizing the access. Using vished credentials, cybercriminals mined the victim company databases for their customers' personal information to leverage in other attacks. The monetizing method varied depending on the company but was highly aggressive with a tight timeline between the initial breach and the disruptive cash-out scheme.

Results: Domain Takedowns (March 19 – April 14)

Total Takedowns: 2,833

Takedowns by Country:

- Malicious Internet Domains – 2,818
- United Kingdom Institution Impersonators – 2
- Canada Institution Impersonators – 4
- European Union Institution impersonators – 1
- Denmark Institution impersonators – 1
- Morocco Institution impersonators – 1
- Brazil Institution Impersonators – 1

Final Thoughts

Don’t let siloes remain a major challenge:

Stronger together.

OSINT
Yourself and your organization.

Know what’s out there.

Prioritize patching

2020 is challenge, but we have the tools.
We need to use them together: Collaboration

Engage with ICANN

Thank You and Questions

Visit us at **icann.org**
Email: email@icann.org

- @icann
- facebook.com/icannorg
- youtube.com/icannnews
- flickr.com/icann
- linkedin/company/icann
- slideshare/icannpresentations
- soundcloud/icann