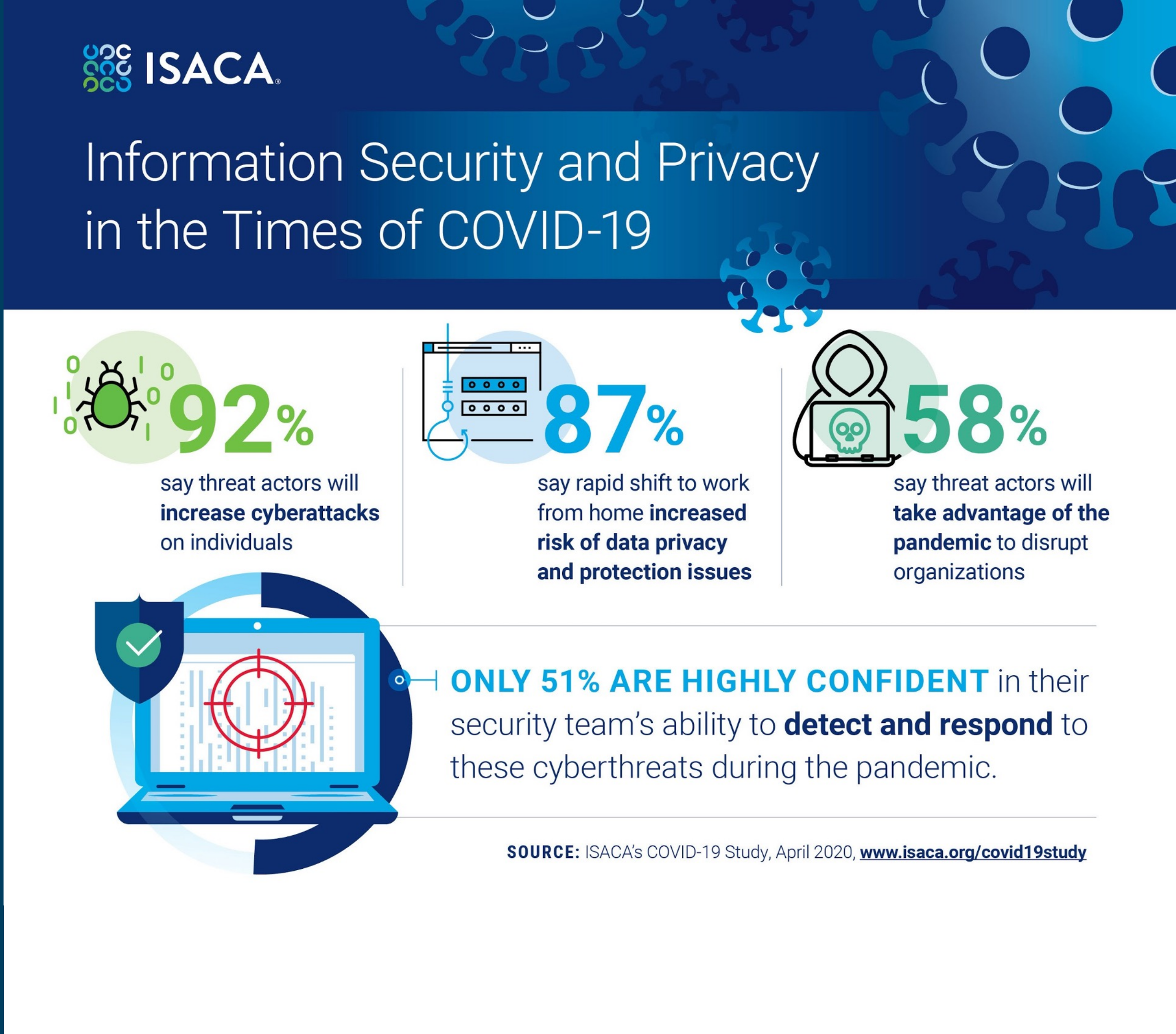
Most Companies Were Rushed into Pandemic Operations

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

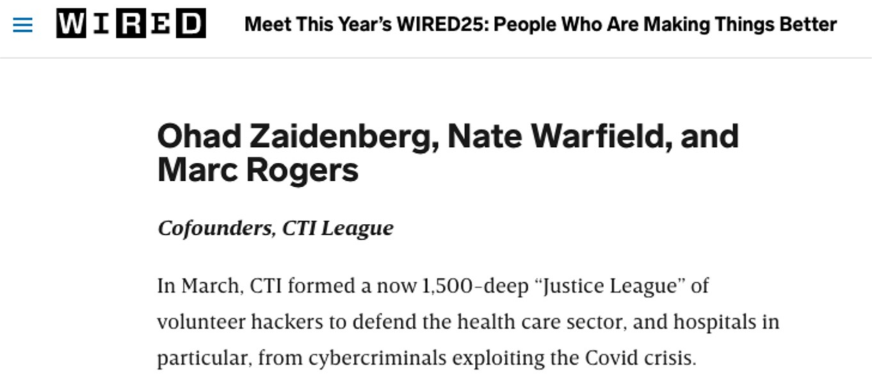
ONLY 51% ARE HIGHLY CONFIDENT in their security team's ability to **detect and respond** to these cyberthreats during the pandemic.

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

© Okta and/or its affiliates. All rights reserved. Okta Confidential

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.



≡
WIRED
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

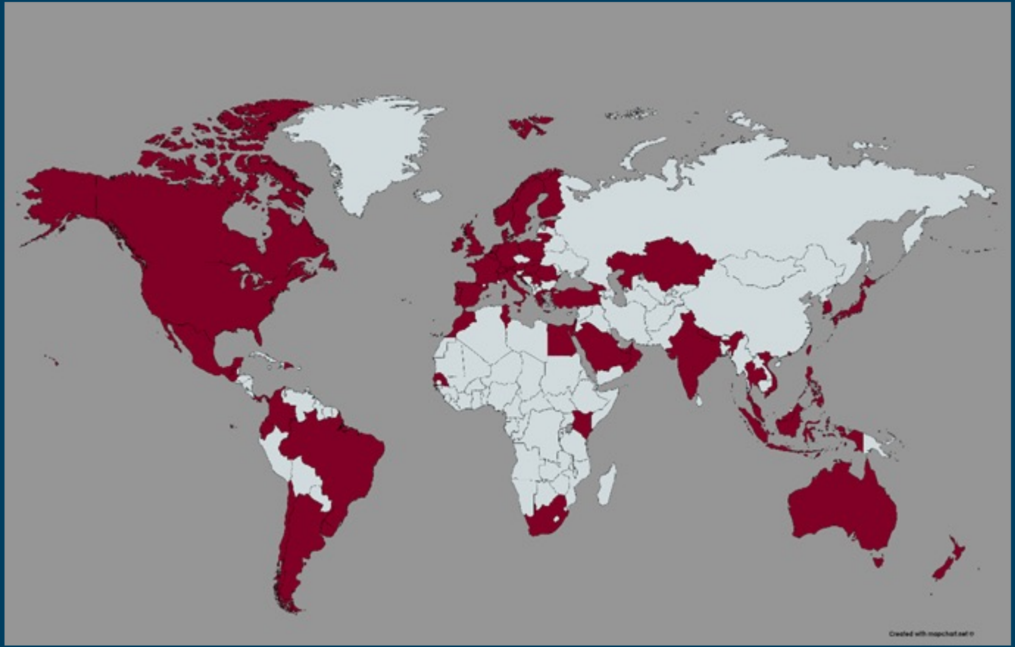
© Okta and/or its affiliates. All rights reserved. Okta Confidential

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



© Okta and/or its affiliates. All rights reserved. Okta Confidential

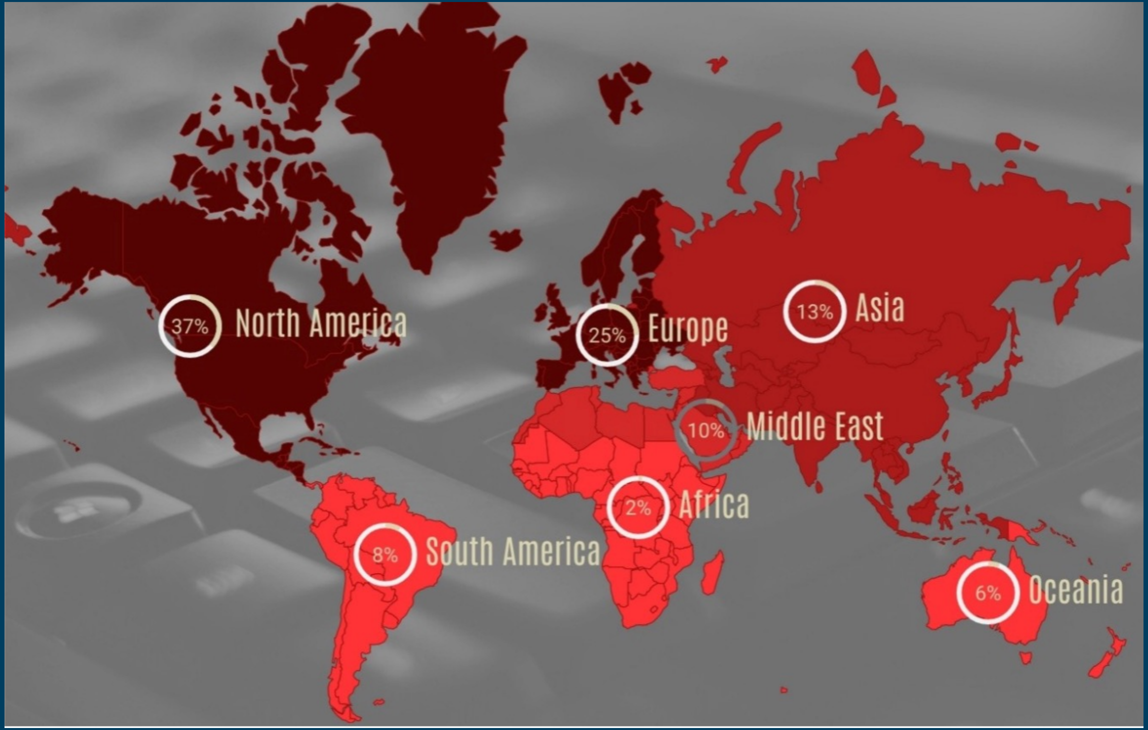
Globally Threat Landscape.

More than half of attacks against healthcare organizations actually originate from the 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: CTI League darknet report.

© Okta and/or its affiliates. All rights reserved. Okta Confidential

Collaboration

© Okta and/or its affiliates. All rights reserved. Okta Confidential

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:

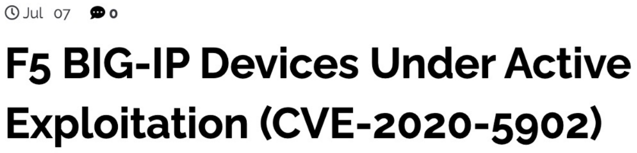
RCE vulnerability – 22
BlueKeep vulnerability – 2
SMBv3 open ports – 2
Citrix Gateway servers – 21
Less prioritized CVE vulnerabilities – 5
Exposed Xero Universal Viewer instances – 3

Data from CTI-League Report, March 2020

© Okta and/or its affiliates. All rights reserved. Okta Confidential

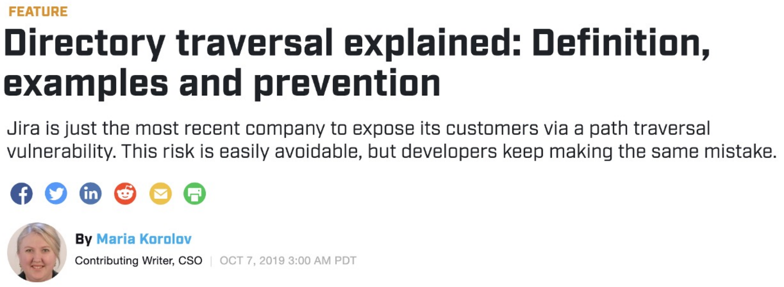
However, we also need to learn from past mistakes.

- 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)



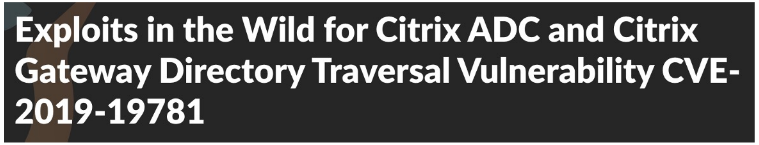
FEATURE

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

© Okta and/or its affiliates. All rights reserved. Okta Confidential

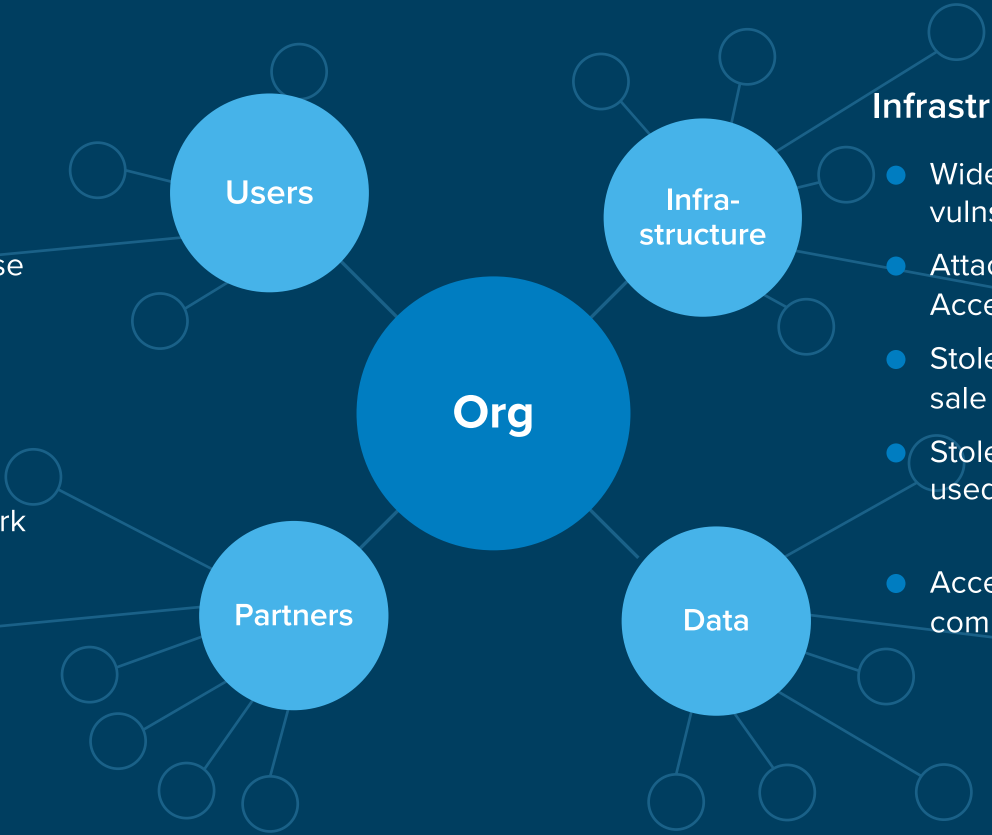
Broad Spectrum of Threats with a Broad Spectrum of Goals

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

© Okta and/or its affiliates. All rights reserved. Okta Confidential

Simplest Attacks Are the Most Effective

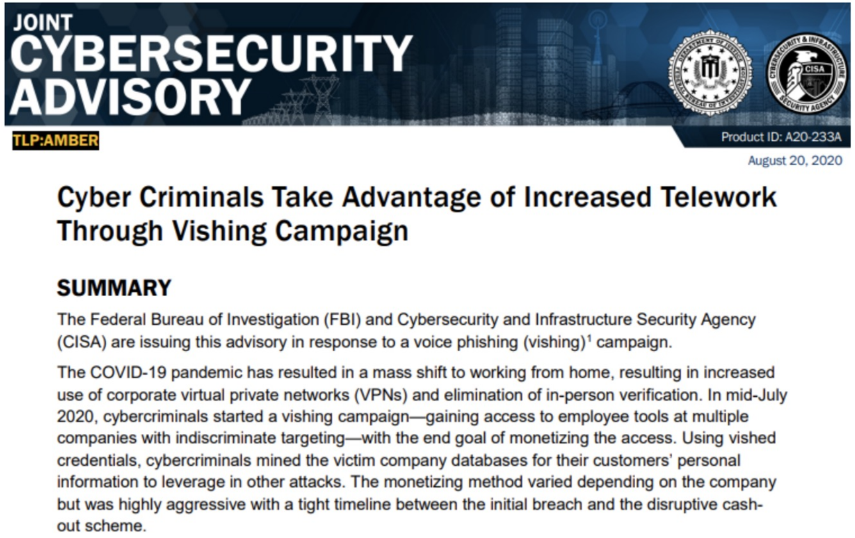
Isolation leaves employees vulnerable

Major vishing and phishing campaigns on-going

Simple vector: sophisticated execution

© Okta and/or its affiliates. All rights reserved. Okta Confidential

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.

© Okta and/or its affiliates. All rights reserved. Okta Confidential

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

© Okta and/or its affiliates. All rights reserved. Okta Confidential

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

© Okta and/or its affiliates. All rights reserved. Okta Confidential