

The New Threat Landscape in a Post Pandemic World



The future of hacking: COVID work and who they target



August 14, 2020

Bill DeLisi

Amid COVID-19, hackers play on people's fear of malware disguised as legitimate software.

1 2 3 4 5 6 7 8 9 10 11 12

COVID-19
Infra-structure
Ransomware
Malware
Phishing
Hacking
DDOS
Fake Email
Zoom Bomb

Subjects Contact

Subjects Tech Lifestyle & Health Policy & Public Interest People & Culture

Cybersecurity Experts Report: 4,000 Cyberattacks Since COVID-19 Pandemic

and law enforcement report 800% surge.

SHARE THIS ARTICLE



NewsWire -- The global pandemic has seen a huge rise in people working from home, being more digitally connected than ever. There are plenty of good things that have come out of bad as well. One of the biggest issues is that cyberattacks have skyrocketed during the pandemic. Cloud. Cybercriminals have taken this opportunity to up their attacks, both in the cloud and on the ground. Here's what you need to know about the rise in cyberattacks during the COVID-19 pandemic of

WiCyS 2021 CONFERENCE PANEL

The New Threat Landscape in a Post Pandemic World

September 10th, 2021 @ 12:00pm MDT



Priyam Biswas
Intel
@amipri



Awalin Sopan
Sophos
@awalisopan



Abhilasha
Bhargav-Spantzel
Microsoft
@spantzel



Michele Myauo
Microsoft



Reshma
Shahabuddin
Sophos

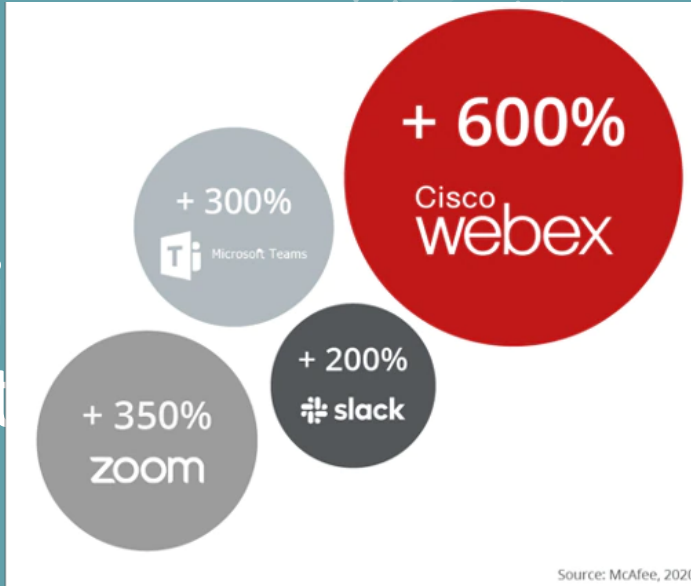


#WiCyS2021

Motivation



Maj Fact



Extended
Dependency on
Telework

High Demand for
Information

Stress and anxiety
originating from
economic and
overall uncertainty

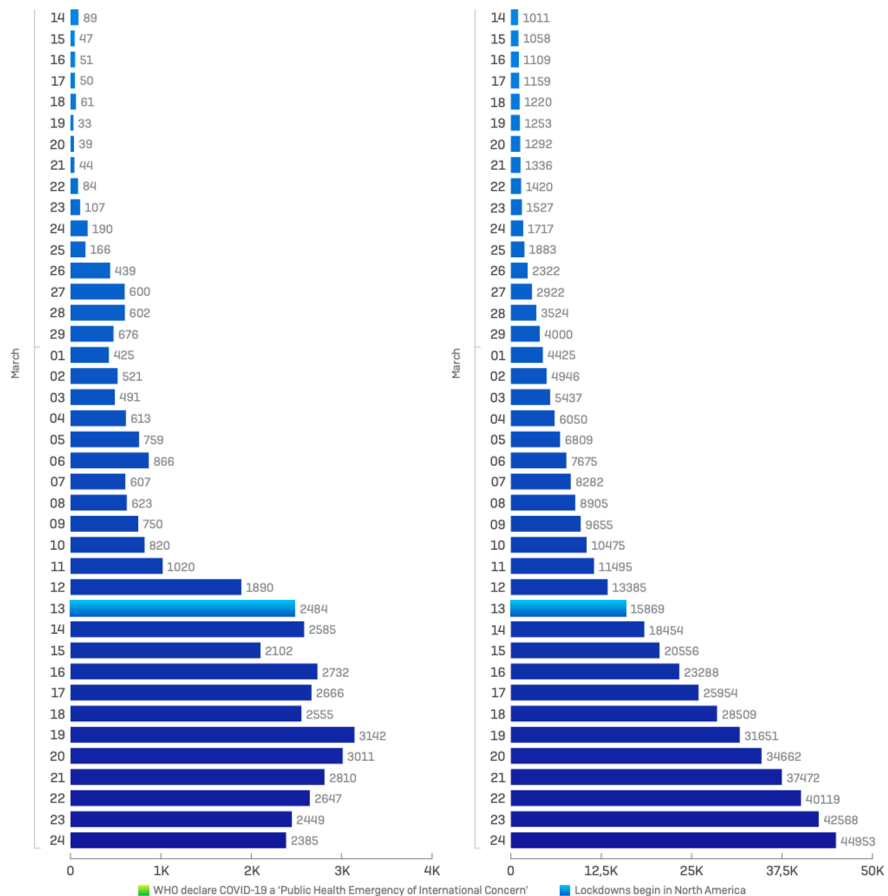


Fig.17. Throughout the early months of the COVID-19 crisis, people registered thousands of domains and licensed at least that many TLS certificates per day, whose names contained the string "COVID-19" or "corona". Source: SophosLabs.

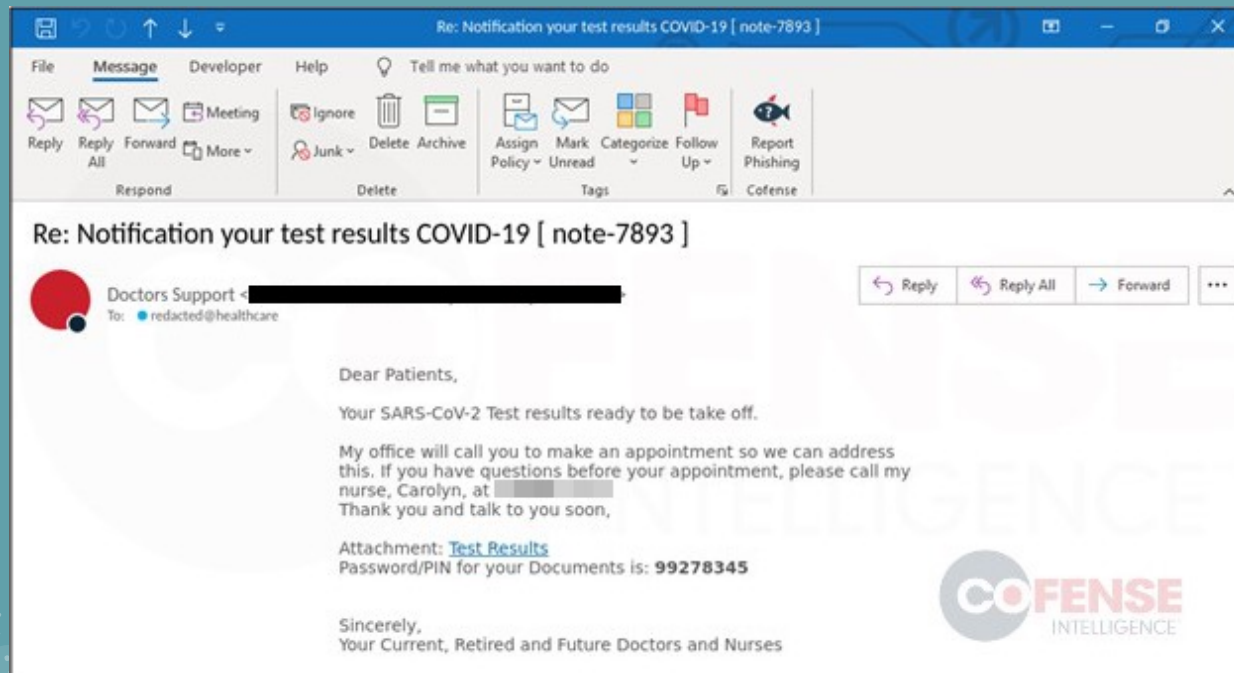
SOPHOSlabs

Major Trends

Fake Information

portal

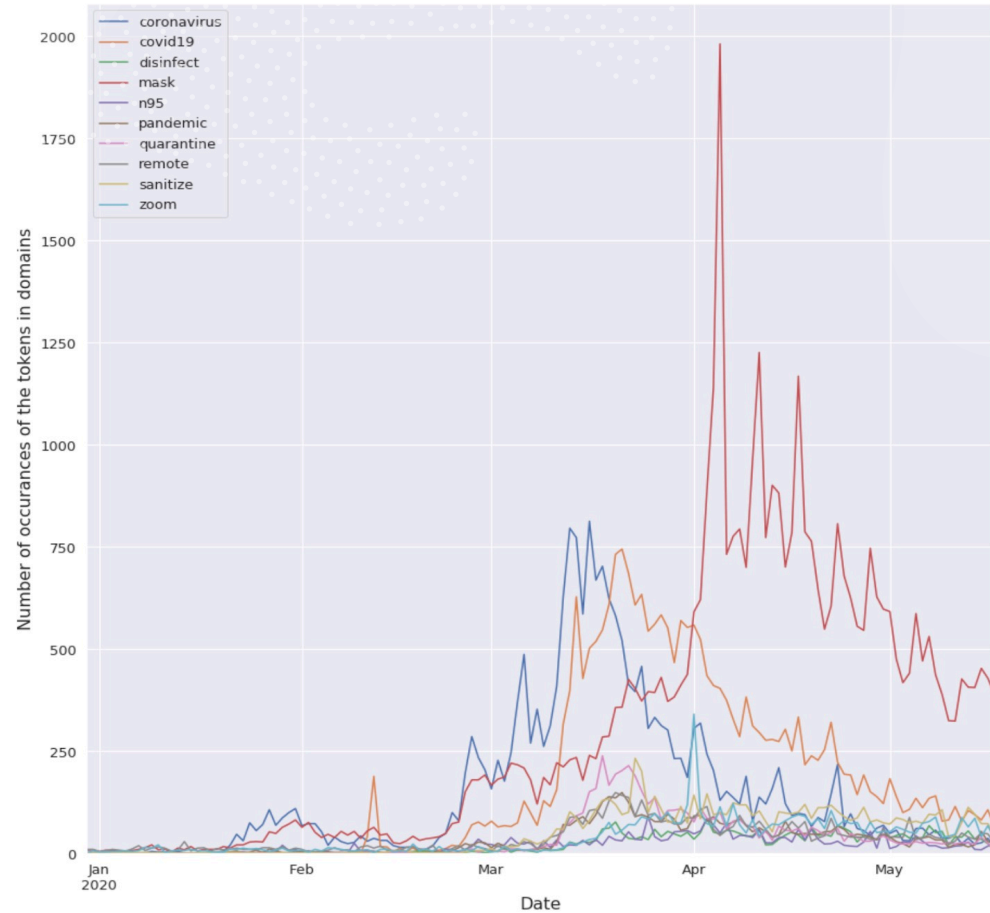
Major Trends Phishing Scams



Phishing Scams Related to the Pandemic

- Get Vaccinated Now Scams
- Paying for Appointment Scam
- False Contact Tracing Scams
- Assistance from “Big Name” Company Scams
- New Treatment or Breakthrough Scams

Scam Token Trends

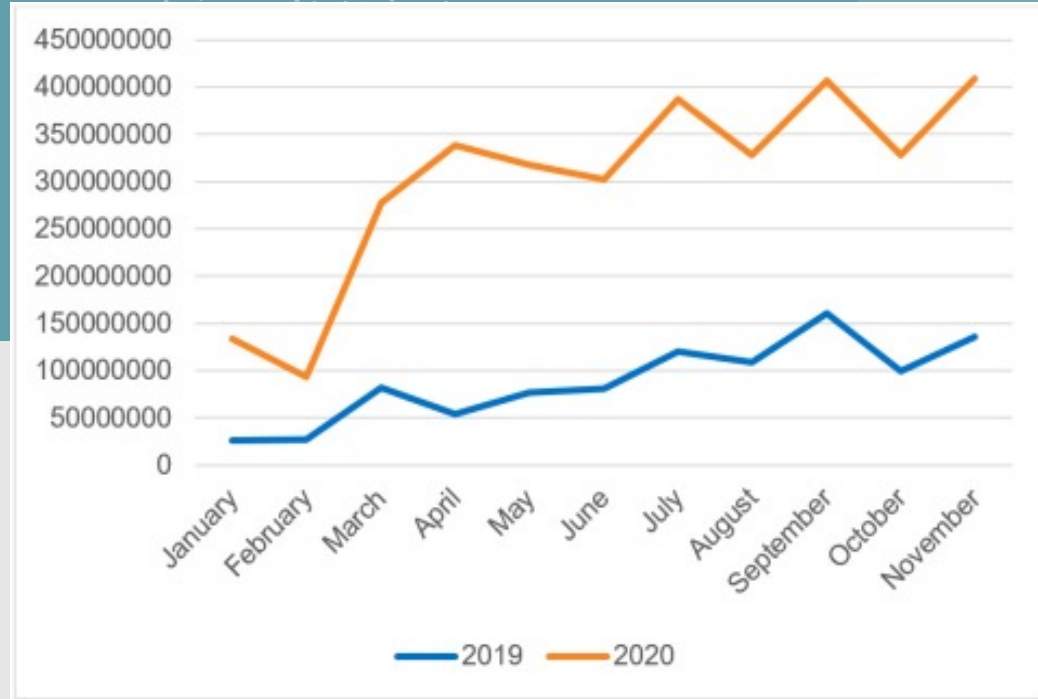


(Source: Tamas Voros, Sophos)

- Phishing scams in Supply Chain

Most popular Attack

- Brute force attack against RDP protocol



Human Factors



Poll

How has the pandemic changed your day to day life?



Poll created by speaker, Awalyn Sopan

Your answer:

a lot

Poll Results

50 Answers

- Working remote
- Started working remotely and multi tasking from home
- just less travel; otherwise, no change
- A bit.
- Able to reduce my use of my car & take advantage of career and educational opportunities remotely
- Working from home you miss the bonding of face to face time with co-workers.
- More prayerful, thankful and grateful!
- I get to sleep later and no traffic on my way to my home office.
- The covid 19 lbs. Working out became non-existent and more time at home meant being closer to family.

- I have learned to slow down and stop trying to multitask
- no
- Am home much more
- I now prefer days off during the week than the actual weekend, to avoid crowds and busy hours.
- Had to work harder on productivity. Sometimes I found it harder to focus.
- At home more so more hours in my day.
- Besides being moved to 100% telework, I find my quality of life has actually drastically improved.
- It has been more flexible. I'm able to take care of my job, my family, mental and physical health.
- Wfh is great!
- Much more casual
- I sit way too much! I've put an alarm on to move around.
- Remote work more acceptable
- it made almost everything boring, as I was confined to not meeting people
- Truthfully it's mostly impacted my social life and not my work life since I was/am remote.
- Focus my time on what really matters: Family and health
- I've become more aware.
- it's tripled my work as a teacher teaching remotely.

- Ability to work from home with the exception of having to go into the office for exceptions
- Lost my IT job. Have been upskilling & networking to find my entry into Cybersecurity ever since.
- A little
- Not much. I'm a hermit
- More diligent about taking personal time.
- Flexible work schedule
- Relocated to another city, permanent WFH.
- It has created stress
- I get to wear a mask like a superhero (or villain)
- Validated the importance of time not being spent on commuting
- I work way more
- Enforcing Adaptive behaviour
- Yes I'm more tired
- a lot
- stay inside
- Stay at home more, WFH as much as possible, bought hardware to practice at home
- Yes
- I am more comfortable in anonymity
- I am working remotely, thanks to the pandemic. I have more time with my daughter.



Human Aspect of the Change

Fast digital transformation without any proper training

People are more vulnerable to cyber attacks



Attack on
Healthcare Industry

**The healthcare sector alone lost over \$20 billion
in impacted revenue, lawsuits, and ransom paid in
2020**

Schools Struggling to Stay Open Get Hit by Ransomware Attacks

Districts around the U.S. are fighting a wave of increasingly aggressive hackers, who are publicly posting sensitive student information

rooks of the Athens Independent School District in Texas.

Management

Cyber

Security Enterprise Services

Security Leadership and Management

Logical Security

Security & Business Resilience

Security Education & Training

Cyber Security News

Education: K-12

Now ransomware is inundating public school systems

May 11, 2021

Robert R. Ackerman Jr.

KEYWORDS cyber security / k-12 security / ransomware / risk management

Order Reprints



Almost every American adult knows that cyberattacks and breaches are ubiquitous and have primarily targeted companies and government entities. They might even know that the single most common breach these days is ransomware, a malicious process by which hackers dismantle computer systems and don't fix them until a ransom is paid.

Few, however, are aware that ransomware is targeting a new set of highly vulnerable victims en masse. In recent months, the majority of successful ransomware attacks have struck K-12 schools nationwide, casting a whole new light on the number of Americans highly susceptible to a cyberattack.

By [Tawnell D. Hobbs](#) | Photographs by Justin Clemons for The Wall Street Journal

Nov. 13, 2020 9:52 am ET

SHARE TEXT

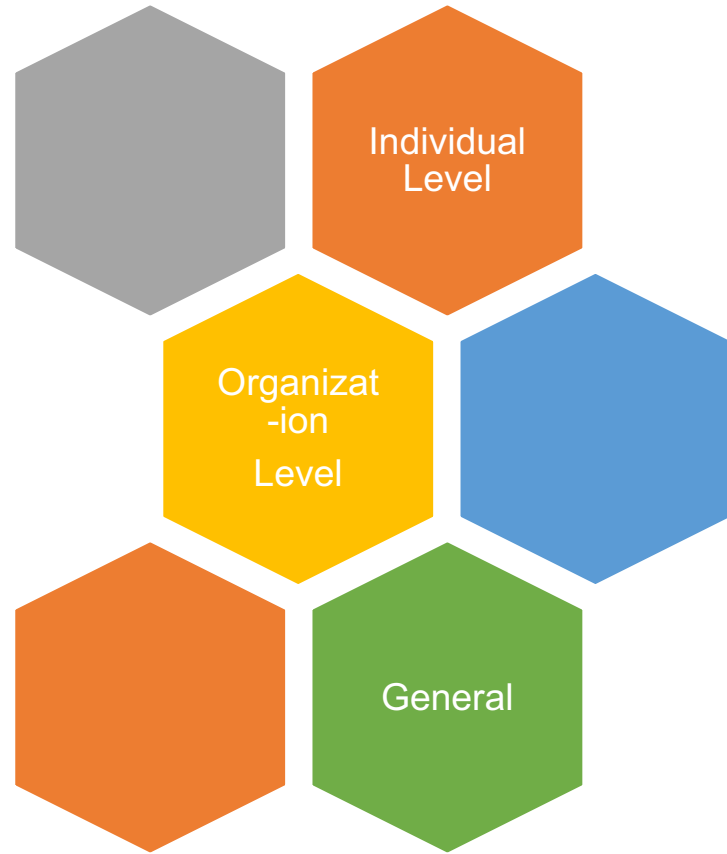
172 RESP

Zero Trust Architecture

Michele Myauo, PhD
*Microsoft Azure Global Cybersecurity,
Principal Engineering Manager*



Solutions?



Individual Level

1

Think twice
before clicking
any link

2

Ensure all the
updates

3

Use anti-virus
and anti-
malware

Company Level



REMOTE ACCESS
INFRASTRUCTURE



ACCESS CONTROL
AND MULTI-FACTOR
AUTHENTICATION



PERIODICAL
TESTING/TRAINING

General

Mass
awareness



Improved cyber
threat
monitoring



Come out of the
“security as
granted” culture



Key Takeaway

- Pro-active
- Active threat monitoring
- Mandatory training for all ages

THANK YOU & Questions



<https://giphy.com/gifs/dccomics-fierce-lets-do-this-dcsuperherogirls-SScSc0nO2tezJNQC21>



Priyam Biswas
@amipri



Awalin Sopan
@awalisopan



Abhilasha
Bhargav-Spantzel
@spantzel



Michele Myauo



Reshma
Shahabuddin