

Cyber Threat Brief

March 2020

Ilene Klein, CISSP, CISM, CIPP/US
Arizona Cybersecurity Program Coordinator

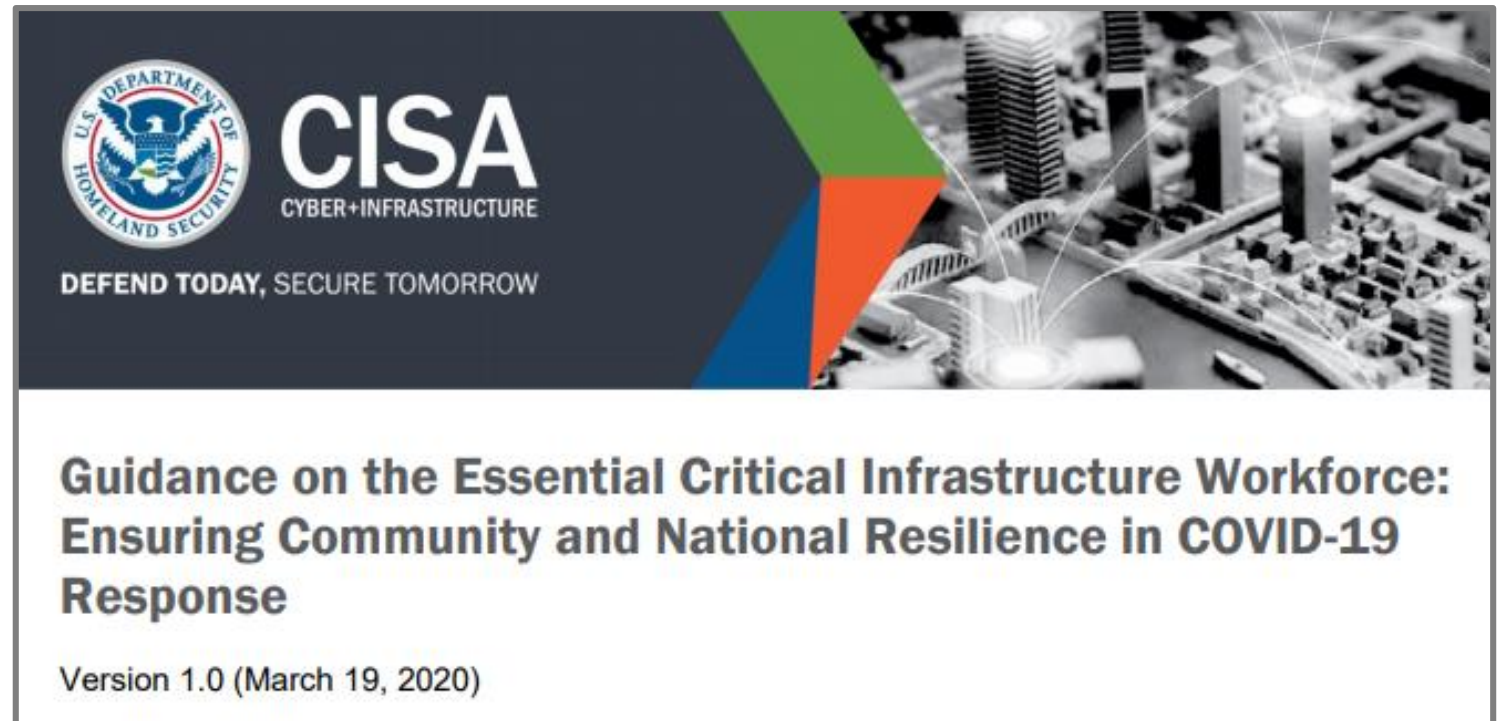


Why Cybersecurity Matters in the Time of Pandemic

- A heightened dependency on digital infrastructure raises the cost of failure
- Broad-based cyberattacks could cause widespread infrastructure failures that take entire communities or cities offline, obstructing healthcare providers, public systems and networks
- Cybercrime exploits fear and uncertainty
- More time online could lead to riskier behavior
 - For example, users could fall for “free” access to obscure websites or pirated shows, opening the door to likely malware and attacks
- Source: World Economic Forum

We're Critical per DHS CISA

- Workers responding to cyber incidents involving critical infrastructure, including medical facilities, SLTT governments and federal facilities, energy and utilities, and banks and financial institutions, and other critical infrastructure categories and personnel



CURRENT THREATS



Threat Vector – Bored People

- What do people do when bored and stuck at home?
- Learn new skills – hacking!
- Find new online friends – hackers or new Anonymous!
- Act on grudges or campaign for social/ideological reasons – DDOS!
- Try to “earn” money – scamming or extorting people!

Health and Human Services Hack (1/2)

- 3/15: U.S. Health and Human Services Department suffered a cyber attack on its computer system Sunday night
 - HHS realized that there had been a cyber intrusion and false information was circulating
 - The hack involved overloading the HHS servers with millions of hits over several hours (no info provided about intrusion)
- The National Security Council tweeted just before midnight
 - “Text message rumors of a national #quarantine are FAKE. There is no national lockdown. @CDCgov has and will continue to post the latest guidance on #COVID19.”
- Administration officials assume that it was a hostile foreign actor, but there is no definitive proof at this time

Was It Really an Attack? (2/2)

- HHS “experienced an unusual number of scans”
- Security researchers reported that on a scale of 1-10, the incident was about a 2
 - “Signs pointed, at most, to a failed distributed denial-of-service attack”
 - “My sources at several DDoS mitigation services said they haven’t seen an attack aimed at the site. Instead, this looks like a spike of legitimate traffic aimed at a website of interest to the general public”

Fake COVID-19 Case Map (Old News from 3/12)

- Phish and online ads promoted link to fake COVID-19 global case map that mimics the John Hopkins University map
- Website downloads AZOrult to the victim's device
 - Malware is an information-stealing Trojan that can download additional malware and exfiltrate data, such as financial information, chat sessions, login credentials, browsing history, and more



Make Sure...

- ***Attackers are actively scanning ports 3389 (RDP) and 445 (SMB)***
- Make sure ports 3389 (RDP) and 445 (SMB) are closed!
 - Use Shodan to search
- And use multi-factor authentication
- Organizations are opening them to allow for easier remote access and file access

Surprise! – Growth in Phishing Attacks

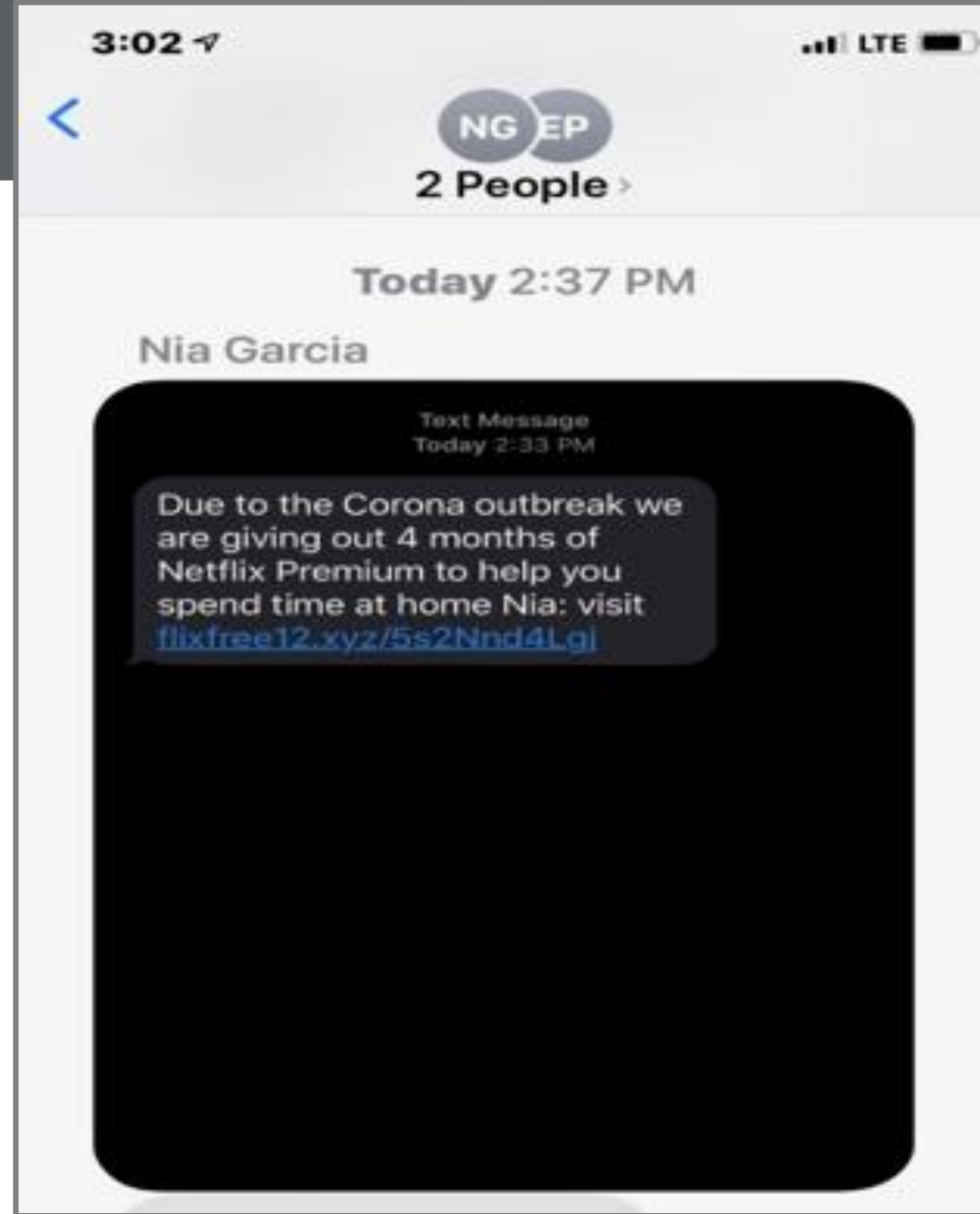
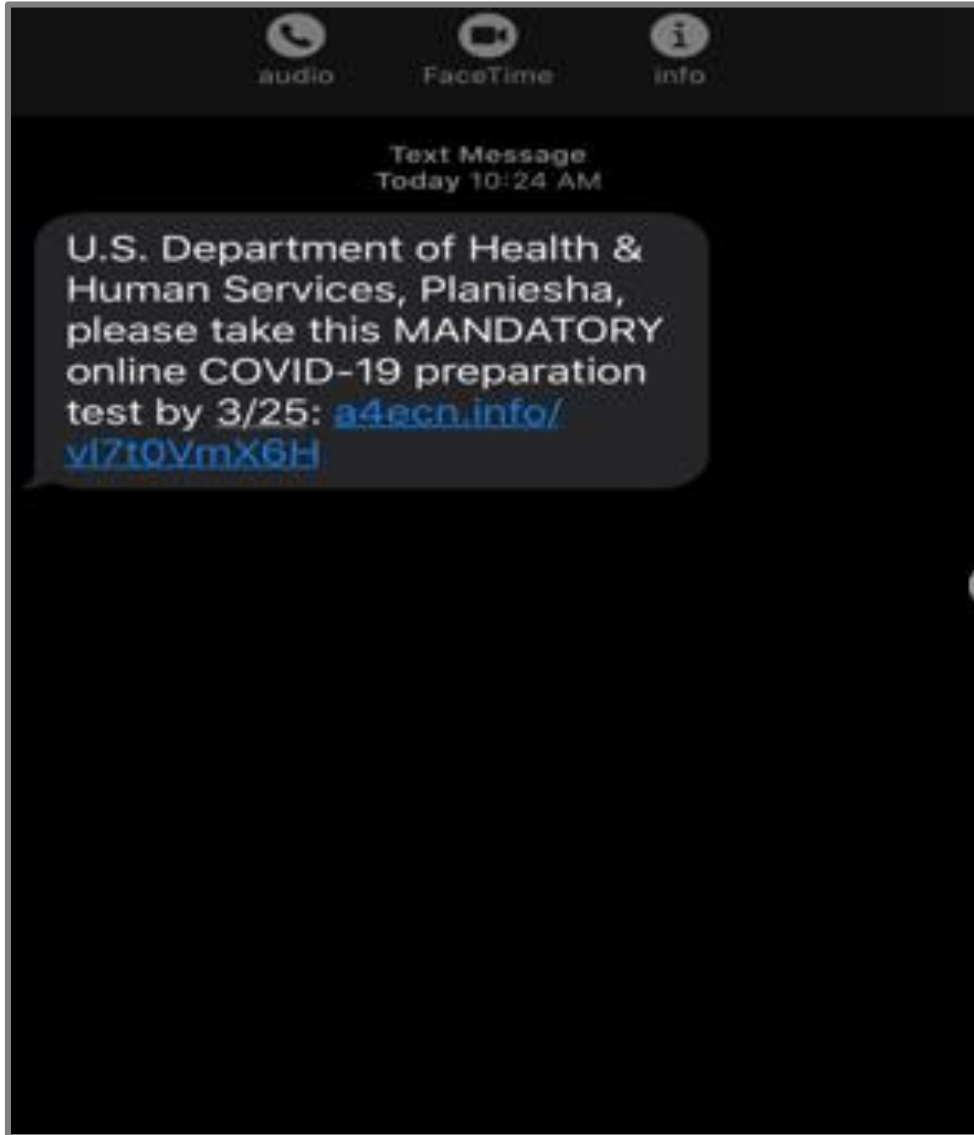
- 72% = Growth in phishing attack from January to March
 - Key terms = “reset password” or “business continuity” that create fear
- Also, increased risk of fake sites that replicate popular teleconferencing platforms
 - With domain names that may be off by only one letter
- Source: Cybersecurity firm, RedMarlin

Current COVID-19 Phish Campaigns





Smishing – Rec'd 3/23-24



FTC's Coronavirus Scam Warnings

- **Public health scams**
 - Messages that claim to be from the Centers for Disease Control (CDC), World Health Organization (WHO), or other public health offices
- **Government check scams**
 - Financial help for businesses available thanks to federal relief
- **Business email scams**
 - Financial transactions, like expedited orders, cancelled deals, and refunds, that are not that unusual due to coronavirus
- **IT scams**
 - Calls or messages supposedly from tech staff asking for a password or directing the recipient to download software

Sextortion with a COVID-19 Twist

- Sextortion scammers are adding the COVID-19 pandemic as a tool to scare and extort money from victims
- New version threatens to infect victims' families with the SARS-CoV-2 virus if the extortion demands are not met
 - Plus reveal “dirty secrets”
- eMail subject = [YOUR NAME] : [YOUR PASSWORD]
 - To get recipients to open the email
- Victims must send \$4,000 worth of Bitcoin to the attackers to prevent further harm

New Attack: Zoom-Bombing

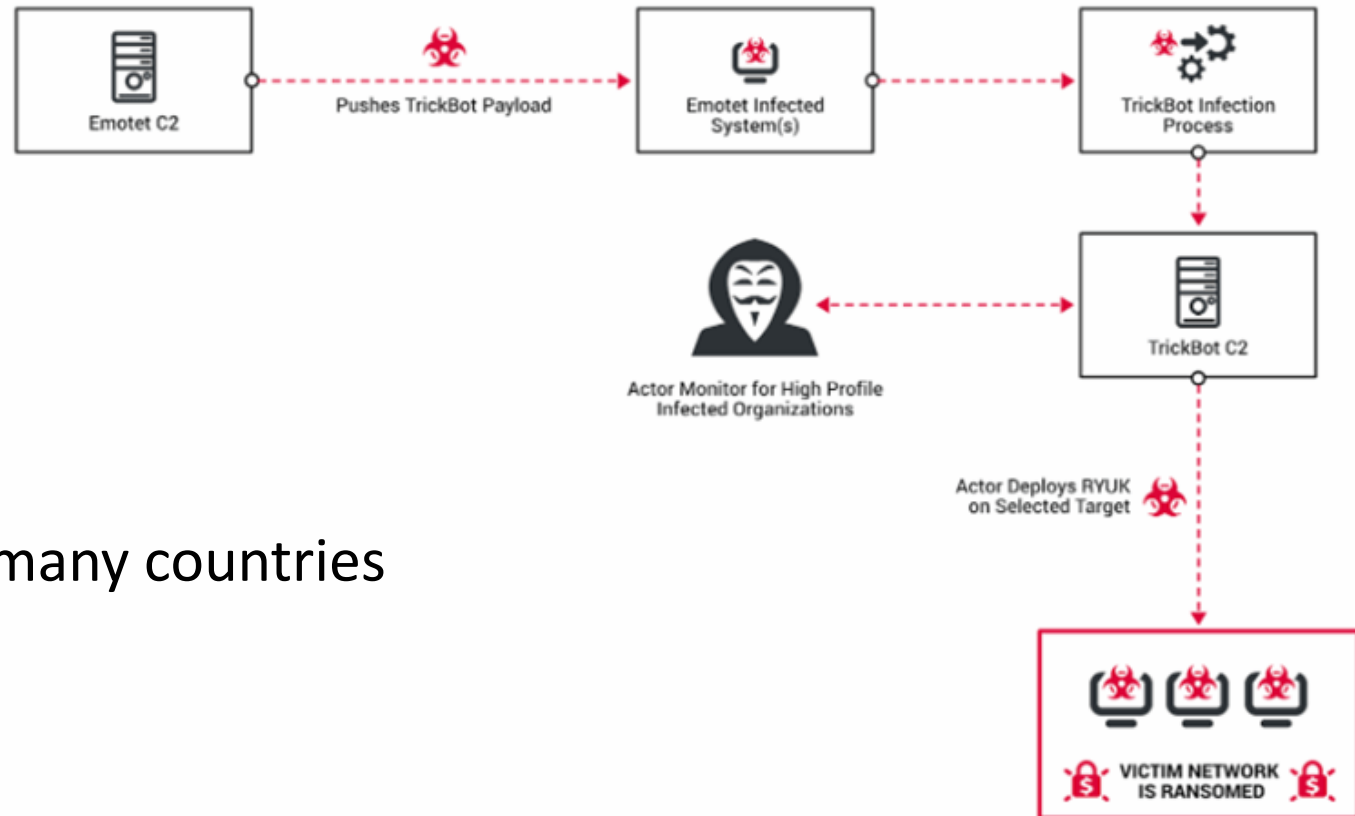
- Definition: Gate-crashing Zoom meetings to display porn or violent images
 - Sharing your meeting link on social media or other public forums makes your event public which allows anybody with the link to join the meeting
- Don't post meeting details on public sites
- Use Zoom host controls to control meeting
 - Allow only signed-in users to join
 - Lock the meeting
 - Prevent removed participants from rejoining
 - Turn off file transfer, annotation, screen sharing, video...
 - Mute participants
 - Disable private chat

Ransomware Attackers Prefer Off Hours

- 76% = Ransomware infections (triggering the encryption process) in the enterprise sector that occur outside working hours
 - 49% = Attacks taking place during nighttime over the weekdays
 - 27% = Attacks taking place over the weekend
- Why? Most companies don't have IT staff working those shifts, and if they do, they are most likely short-handed
- 3 days = Time threat actors wait ***after the initial breach*** before deploying ransomware (in 75% of all ransomware incidents)
- Source: FireEye, based on dozens of ransomware incident response investigations from 2017 to 2019

Ransomware Hitting Hospitals

- (Some) attackers are continuing to target healthcare sector – taking advantage of critical need for systems
- There are reports of using the Emotet-TrickBot-Ryuk tactic that was widely used last year
 - Now targeting hospitals in many countries



Maze Team official press release. March 18 2020

Due to situation with incoming global economy crisis and virus pandemic, our Team decided to help commercial organizations as much as possible. We are starting exclusive discounts season for everyone who have faced our product. Discounts are offered for both decrypting files and deleting of the leaked data. To get the discounts our partners should contact us using the chat or our news resource.

In case of agreement all the info will be deleted and decryptors will be provided.

The offer applies to both new partners and the «archived» ones. We are always open for cooperation and communication.

We also stop all activity versus all kinds of medical organizations until the stabilization of the situation with virus

Operators behind Maze ransomware announce they will refrain from targeting healthcare and medical organizations in light of COVID-19 coronavirus: Blog Photo via Twitter.

Um, Gee, Thanks, DoppelPaymer

- Per DoppelPaymer operators
- “we always try to avoid hospitals, nursing homes ... we always do not touch 911 (only occasionally is possible or due to misconfig in their network) ... if we do it by mistake – we'll decrypt for free”

Yea, But Maze Still Extorts Victims

- March 14: Maze operators attack Hammersmith Medicines Research
 - A British company that previously tested the Ebola vaccine and is on standby to perform the medical trials on any COVID-19 vaccine
- Maze operators stole data from victim and then published it online to get them to pay the ransom demanded
 - Victim “repelled” ransomware attack and quickly restored all their functions
 - Data stolen included details of people who participated in testing trials between eight and 20 years previously
 - Maze operators published samples of data on the dark web

Ransomware Attack = Data Breach

- All ransomware attacks now must be considered data breaches
- More ransomware families are publishing stolen data of their victims who choose not to pay
 - CLOP
 - DoppelPaymer
 - Maze
 - Nefilim
 - Nemty
 - Sekhmet
 - Sodinokibi/Revil

Bandwidth Will Probably Be an Issue

- Reports of AT&T and Verizon having capacity issues in Arizona
- Why? Too many people streaming media and working from home
 - 40% = Rise in mobile traffic on AT&T
 - 22% = Rise in Verizon's wireless and fiber broadband service
 - 100% = Rise in Wi-Fi calls
 - 300% = Rise in remote-conferencing programs like Zoom and Skype
 - 400% = Rise in video games
- Telecom providers are working to increase capacity

Senators Ask ISPs to Increase Capacity

- U.S. Senator Mark R. Warner (D-VA) and 17 other senators sent a letter to the CEOs of eight major ISPs calling on them to take steps to accommodate the unprecedented reliance on telepresence services
 - Why? Increased telework, online education, telehealth, and remote support services
 - ISPs include AT&T, CenturyLink, Charter Communications, Comcast, Cox Communications, Sprint, T-Mobile, and Verizon
- Senators asked companies to suspend restrictions and fees, and provide free or at-cost broadband options for students

Internet Capacity?

- The Federal Communications Commission granted T-Mobile temporary access to spectrum in the 600MHz band that's owned by other licensees
 - To help prevent congestion in cellular data networks
- FCC also granted Verizon and AT&T temporary access to more airwaves.

Internet Capacity?

- 3/19: The European Union has asked Netflix to slow its download speeds in order to reduce network bandwidth now that millions of people have committed to staying home
 - Netflix uses “adaptive streaming” which automatically adjusts picture quality based on a network’s capacity
 - They also distribute hubs of its content on servers worldwide so shows can be delivered locally rather than all steaming from one central source

SAFETY NET UK internet capacity could be RATIONED to prioritise ‘critical’ apps and websites, experts reveal

[Sean Keach](#), Digital Technology and Science Editor
23 Mar 2020, 13:56 | Updated: 23 Mar 2020, 18:34

Never Let a Good Incident Go to Waste

- Per DHS, terrorists are exploiting COVID-19 pandemic to incite violence
 - March 19: ISIS issued its weekly *al-Naba* newsletter, which contained calls for attacks in Western countries against strained healthcare systems
 - White supremacist extremists have called for infected individuals to intentionally spread COVID-19 in diverse neighborhoods and in religious institutions such as mosques and synagogues
 - Other social media users are sharing and discussing perceived threats associated with the US Government response to the outbreak, specifically tied to social media rumors and fears of martial law and gun confiscation

Some of the COVID-19-Related Nation State Attacks

- Many state-sponsored threat actors are using coronavirus lures to distribute malware
 - Chinese APTs: Vicious Panda, Mustang Panda
 - North Korean APTs: Kimsuky
 - Russian APTs: Hades group (believed to have ties with APT28), TA542 (Emotet)
 - Pakistan APT36: Crimson RAT
 - Other APTs: Sweed (Lokibot)

BlackWater Abuses Cloudflare Workers for C2 Communication

- New backdoor malware called BlackWater pretends to be COVID-19 information (filename = Important - COVID-19.rar)
 - It abuses Cloudflare Workers as an interface to the malware's command and control (C2) server
 - Cloudflare Workers are JavaScript programs that run directly on Cloudflare's edge so that they can interact with connections from remote web clients
- Using a Cloudflare Worker rather than connecting directly to the C2 makes it harder for security software to block IP traffic without blocking all of Cloudflare's Worker infrastructure
 - Cloudflare is a web-infrastructure and website-security company

Social Engineering Remote Workers

- Attackers are creating fake LinkedIn profiles or “padding” their profiles saying they worked at companies
 - “Hey – I worked at your company too!”
- Goal = Connect with targets for scams or compromise
- Attackers are targeting HR due to hiring surges and layoffs
 - Sending malicious attachments (resumes)
 - Scamming (BEC – send my paycheck to new account)

Disinformation Campaigns

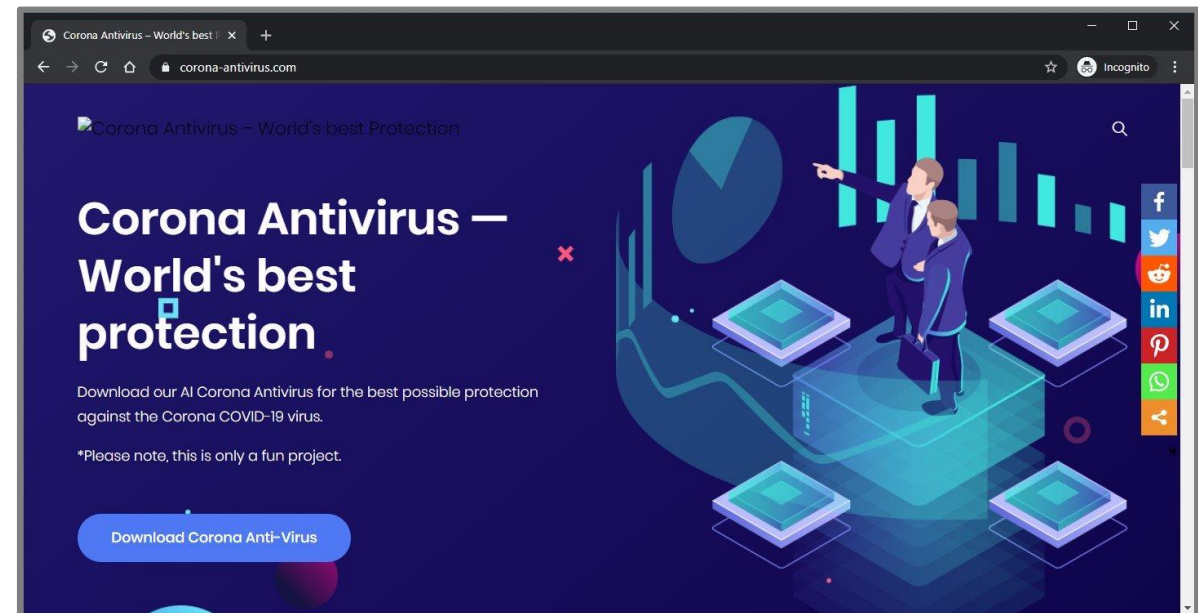
- Russia and China are conducting coronavirus disinformation campaigns
- Russian campaign is designed to undermine the EU's efforts to disseminate factual information on the Covid-19 pandemic
 - Campaign is being conducted in multiple languages
 - The Kremlin has reportedly denied any involvement
- Chinese campaign is about whether the coronavirus actually originated in China

Hackers Hijack Routers' DNS to Spread Malicious App

- Hackers are hijacking routers' DNS settings so that web browsers display alerts for a fake COVID-19 information app
 - User's web browser opens on its own and displays a message prompting them to download a "COVID-19 Inform App" allegedly from the World Health Organization (WHO)
 - Download actually installs Oski information-stealing malware
- Alerts are caused by an attack that changed the DNS servers configured on their home D-Link or Linksys routers to use DNS servers operated by the attackers
- It's unknown how the attackers are gaining access to the routers – maybe weak router passwords?

Now There's Fake Coronavirus Antivirus

- The two sites are promoting fake coronavirus-themed AV software
 - *antivirus-covid19[.]site* found by Malwarebytes (since taken down)
 - *corona-antivirus[.]com* found by MalwareHunterTeam
- They distribute a malicious payload that will infect the target's computer with the BlackNET RAT and add it to a botnet



CYBER WARFARE, POLITICS, AND LEGISLATION



Russia Wants to “Take Whole Nations Offline”

- Hacker group “Digital Revolution” released documents describing a procurement order from Russia’s Federal Security Service (FSB)
- Purpose: Develop “Fronton” software that would enable cyberattacks using infected Internet-of-Things (IoT) devices
- Malware would infect any smart device to build a botnet
- Then use the botnet to DDOS the servers responsible for the stability of online services and the Internet itself in entire countries

TOOLS AND RESOURCES





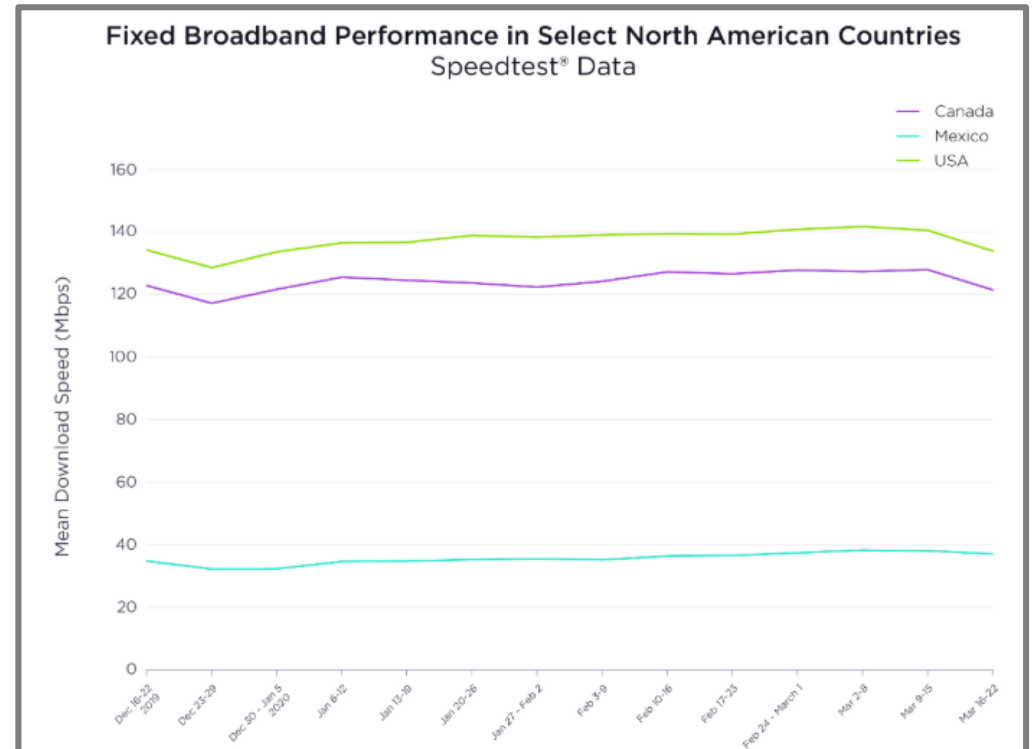
COVID-19 Domains

- List of 4,000 URLs associated with COVID-19
 - You might find possible typosquatting instances for your organization
- <https://pastebin.com/raw/QhPPTJXs>

```
2020coronavirus.org
99coronavirus.com
acoronaviruscure.com
alarmacoronavirus.surgever.com
*.anticoronavirus.cloud
anticoronavirus.cz
anticoronaviruskit.com
*.anticoronavirustienda.com
api.coronavirusstop.org
ashevillecoronavirus.com
brasilsemcoronavirus.com.br
*.californiacoronaviruslaw.com
canepicworkfromhomeduetocoronavirusyet.com
casosdecoronavirus.com
celebswithcoronavirus.com
checktoncoronavirus.fr
cleancoronavirus.com
combat-coronavirus.com
*.comsobreviviralcoronavirus.com
contraelcoronavirusajedrez.com
coronavirus19forum.iphonetechstore.com
coronavirus2019.info
*.coronavirus-ahora.com
coronavirusandchill.com
coronavirus.benkyou.com.br
coronavirus.bolivia.bo
coronavirusbuy.com
coronavirus-calculator.com
coronaviruscallcenter.com
coronavirus.caravanasosito.com
```

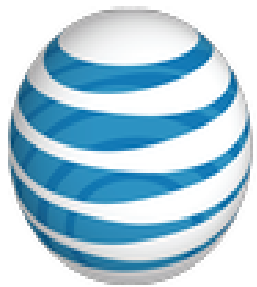
Ookla's Global Internet Performance Tracker

- Tracks COVID-19'S impact on global internet performance
- <https://www.speedtest.net/insights/blog/tracking-covid-19-impact-global-internet-performance/#north-america>



Down Detector

- <https://downdetector.com/>
- Real-time problem and outage monitoring for internet services



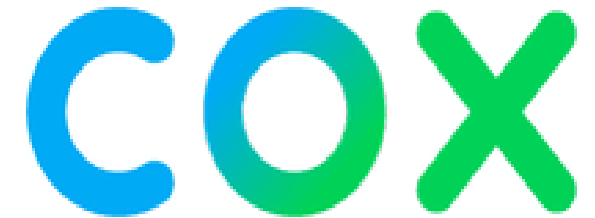
at&t

AT&T



CenturyLink™

CenturyLink

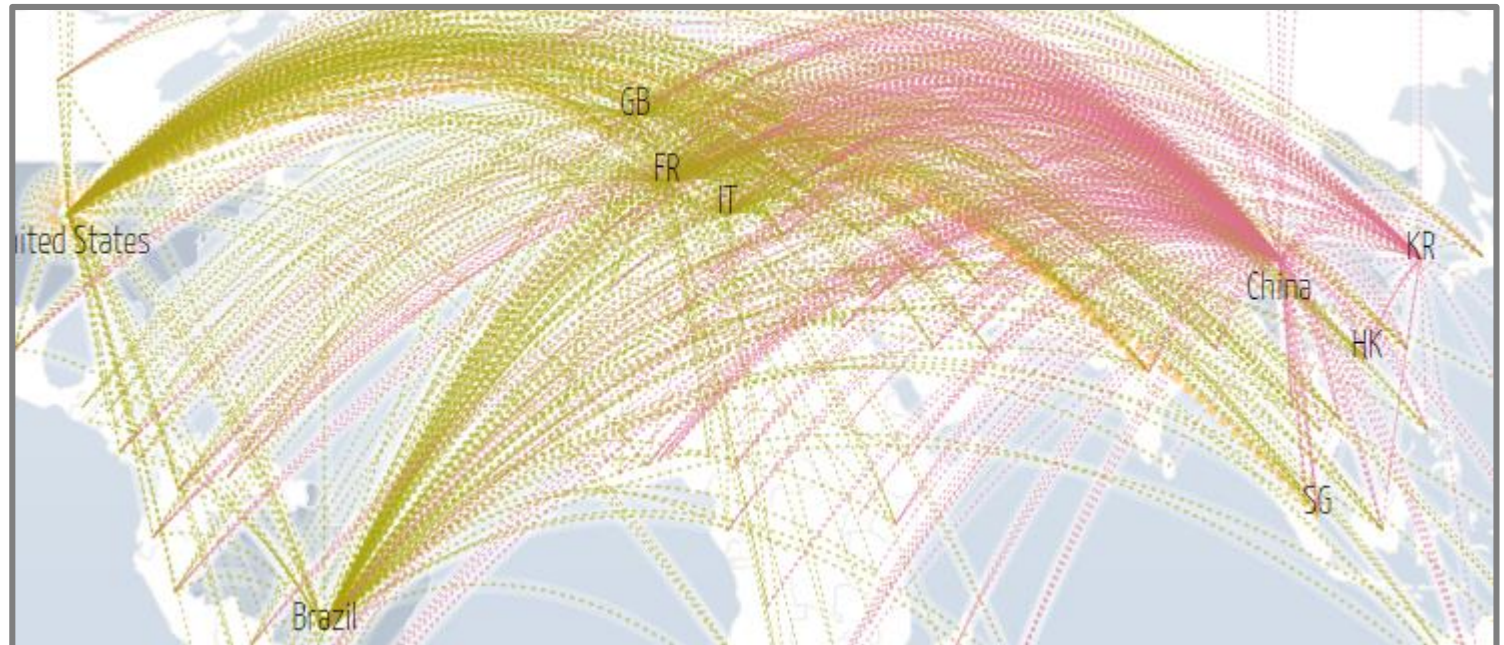


Cox



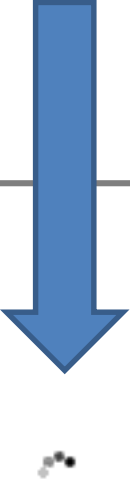
Digital Attack Maps

- <https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18345&view=map>
- More maps: <https://norse-corp.com/map/>



Down Detector Example

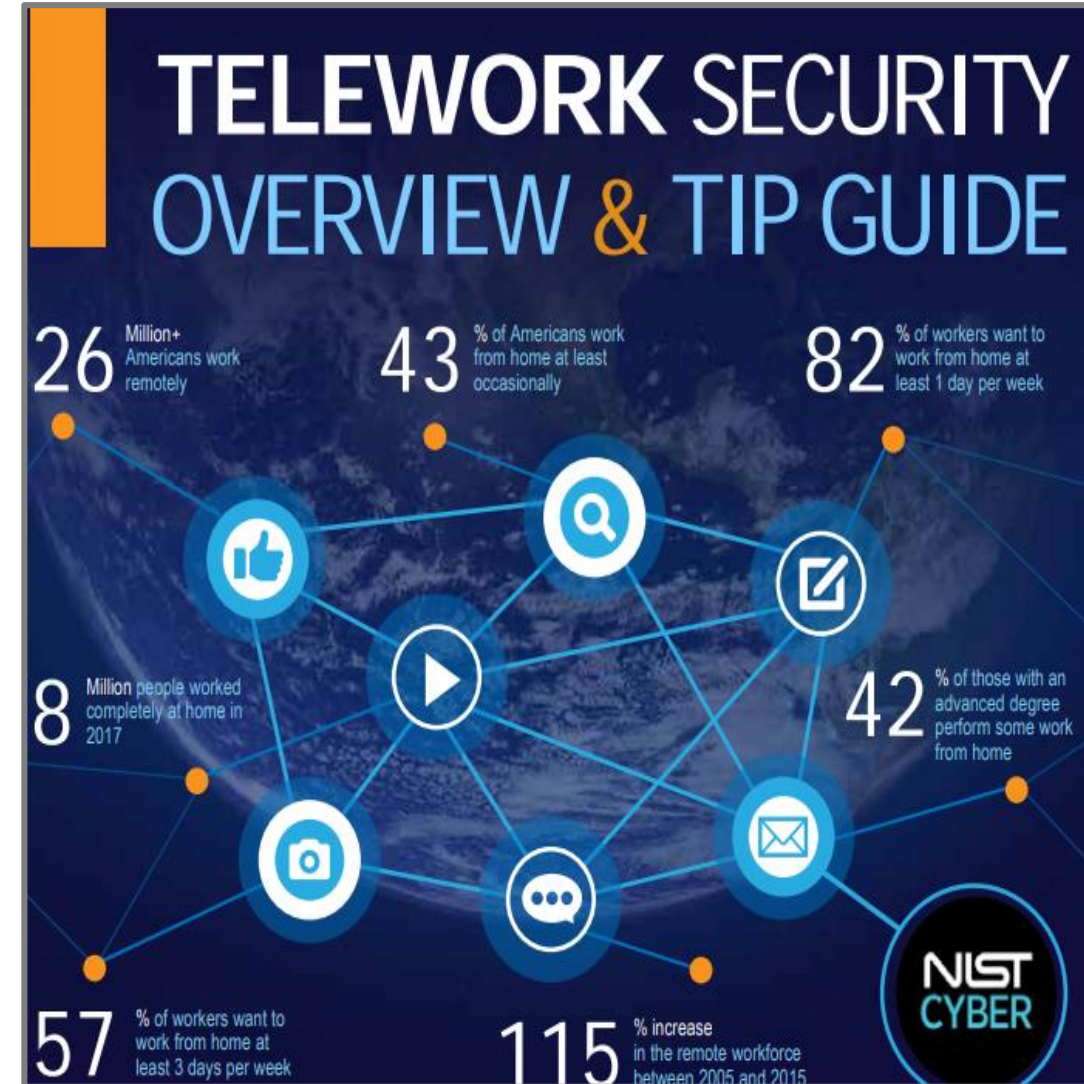
- Um, I use Cox and screen wouldn't load (3/24, 11:25am)



Cox Phoenix problems last 24 hours

NIST Telework Tips

- Infographic
- <https://www.nist.gov/system/files/documents/2020/03/18/Telework%20Overview%20and%20Tips.pdf>



- <https://csrc.nist.gov/>

Telework Cybersecurity

(Updated March 24, 2020)

Today, many employees choose to telework (also known as 'telecommuting'). Teleworking is the ability of an organization's employees, contractors, business partners, vendors, and other users to perform work from locations other than the organization's facilities. While an important work option at this time, it also brings some cybersecurity risks to organizations that can be understood and managed.

To help with this, NIST offers the following resources--primarily NIST Special Publications (SP):

- **Telework:**

- *For Organizations:*

- [*ITL Bulletin: Security for Enterprise Telework, Remote Access, and Bring Your Own Device \(BYOD\) Solutions*](#);
- [*Guide to Enterprise Telework, Remote Access, and Bring Your Own Device \(BYOD\) Security*](#) (SP 800-46 Rev. 2).

- *For Telworkers:*

- [*Telework Security Basics*](#) (blog post) and [*Telework Security Overview and Tip Guide*](#) (graphic);
- [*Preventing Eavesdropping and Protecting Privacy on Virtual Meetings*](#) (blog post) and [*Tips for Securing Conference Calls*](#) (graphic);
- [*User's Guide to Telework and Bring Your Own Device \(BYOD\) Security*](#) (SP 800-114 Rev. 1).

- <https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf>

ITL BULLETIN

ITL BULLETIN MARCH 2020

**Security for Enterprise Telework, Remote Access, and
Bring Your Own Device (BYOD) Solutions**

NIST Conference Call Security

- Infographic
- <https://www.nist.gov/system/files/documents/2020/03/17/Conference%20Call%20Security%20Graphic.pdf>



Free Access to PassiveTotal

- For anyone looking to do more research on COVID-19 attacks, RiskIQ is providing an ongoing list of newly observed infrastructure (not necessarily malicious) and offering 30 days of access to PassiveTotal
-
- <https://twitter.com/RiskIQ/status/1239619032933748738>

Has That IP Been Compromised?

- Team Cymru is offering free access to a portal that will allow the lookup of 50 IP addresses at a time to identify the geographic location of the host and to identify if it has been identified as compromised in the last 30 days via their various detections
- <https://reputation.team-cymru.com/>

Coronavirus-themed Domains

- DomainTools is offering a free listing of coronavirus-themed domains they are seeing registered, with a 70 percent or higher risk score associated with it
 - The list is updated daily around 16:00 Pacific Time
- <https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats>

SANS Free Security Training

- Cyber Aces: Free online video series that teaches the fundamentals “in flash”
- <https://www.cyberaces.org/>



The screenshot shows the SANS Cyber Aces website. The header features the SANS logo, the text 'CYBER ACES' with a star icon, and the binary sequence '01100110101011'. Navigation links for 'Courses', 'About', and 'Contact' are visible. A blue button labeled 'TUTORIALS' is prominent. The main content area has a dark background with binary code and the text 'Your gateway to cybersecurity skills and careers.' Below this, a blue headline reads 'The best online security courses. Free.' The footer text states: 'SANS Cyber Aces Online is an online course that teaches the core concepts needed to assess, and protect information security systems. The course was developed by SANS, the most'



Free DMARC Bootcamp – Beginning May 4




- Global Cyber Alliance (GCA) is offering a new installment of its DMARC Bootcamp
 - Five weeks of online technical training focused on what DMARC is and how to implement it
- <https://bootcamp.globalcyberalliance.org/dmarc-bootcamp-2020>

Malware Analysis Class

- Univ of Cincinnati CompSci/Engineering Department made their graduate level Malware Analysis class public
- <https://class.malware.re/>

MalwareBazaar

- A project from abuse.ch
- Goal = Share malware samples with the infosec community, AV vendors, and threat intelligence providers
- <https://bazaar.abuse.ch/>

Dateadded (UTC)	SHA256 hash	Type	Signature	Tags
2020-03-27 15:58:55	b9a9208aafc5b7d73bf9af9ced0b9be8d77a0a4b952391e15b61325ad3be3d9f	<input type="checkbox"/> exe	Gozi	Gozi 
2020-03-27 15:36:49	f95099f59ee1cd2f4b432c8698da05d7517c17d122ee3682900e9ee107574561	<input type="checkbox"/> exe	GuLoader	exe GuLoader 
2020-03-27 14:29:04	776c7ce560ca7459a622d906f61ceba94e541898731d00cf2b14ba2b06037d74	<input type="checkbox"/> exe	HawkEye	exe HawkEye 

ASU Online Classes (Some Free)

- <https://asuforyou.asu.edu/>

Options for every learner, at any age.



ASU for **You**




List of Cyber Resources

- An organized list of resources including tools, blog-posts and how-to tutorials
- <https://github.com/scspcommunity/Cyber-Sec-Resources>

- Basics of Web & Network
- Books
- CTF Walkthroughs
- Data Protection
- Exploit Development
- How-To Tutorials
- Interview Questions
- Linux Basics
- Misc Content By SCSP
- Mobile Application Security
- Online Practice Labs
- Programming Resources
- Resources and Writeups
- SCSP Presentations
- SIEM Solutions

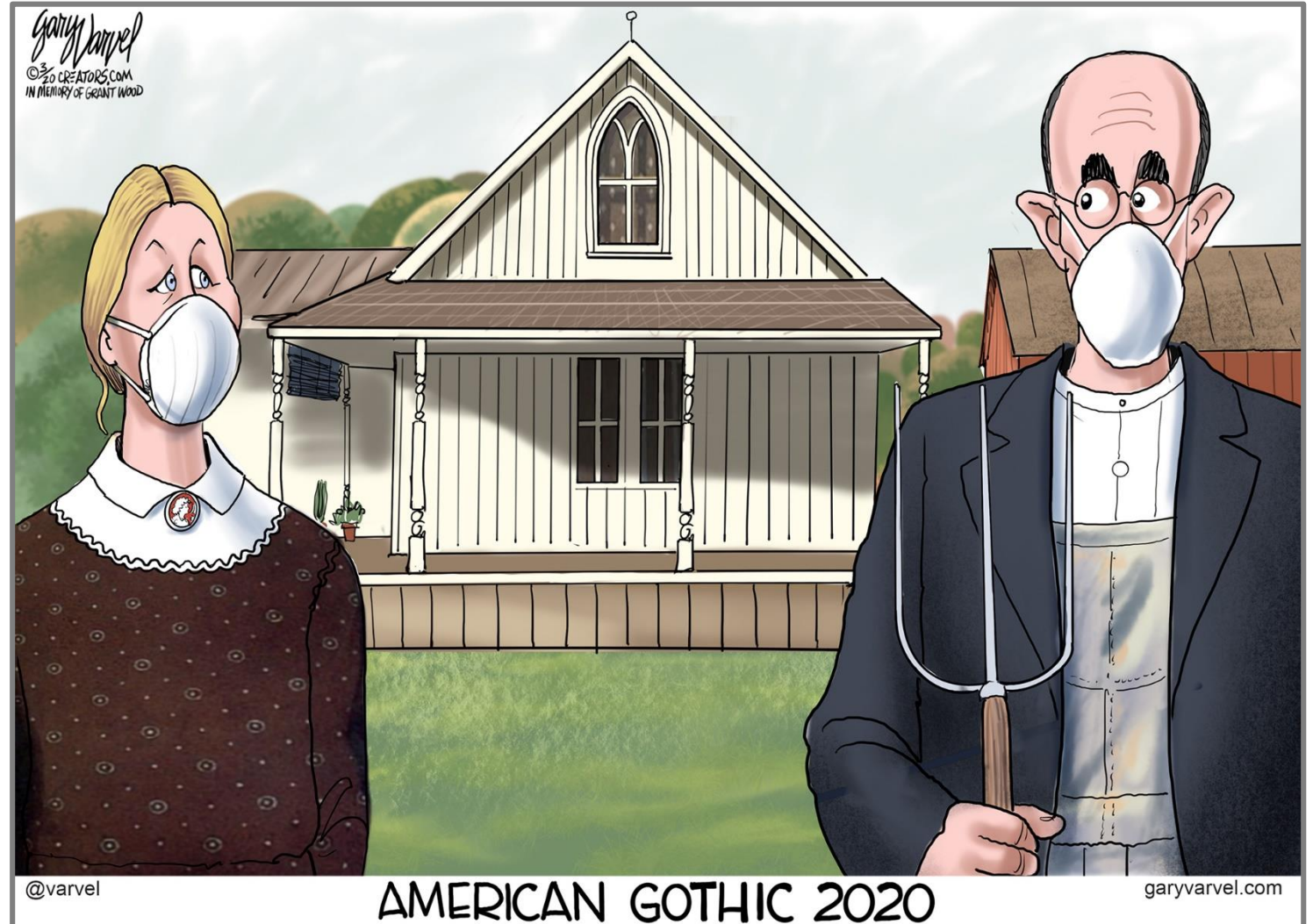
List of Bad Cyber Actors

- https://rsf.org/sites/default/files/a4_predateur-en_final.pdf




Force Name	Country	Count	Flag	Methods used	Known targets
FORCE 47	Vietnam	176/180*		Methods used: "Reinformation" campaigns on social media.	Known targets: Run by the Ministry of Public Security, this army of 10,000 cyber-soldiers combats online "abuses" and " reactionary forces ", meaning those opposed to the government. After a deadly incident in Dong Tam on 9 January, in which the actions of the police were widely criticized, Force 47 flooded social media with forced confessions in which individuals said they had made petrol bombs and other weapons in order to attack the police.
THE SAUDI ELECTRONIC BRIGADE	Saudi Arabia	172/180*		Methods used: Spreading false information and hate messages.	Known targets: Created by Saud Al-Qahtani when he was an adviser to the Crown Prince, this network of pro-regime trolls and bots currently produces more than 2,500 tweets a day, above all promoting the content of the conservative satellite TV news channel Saudi 24. It has also been responsible for spreading sectarian and antisemitic messages and conspiracy theories about Jamal Khashoggi, the Saudi journalist whose murder Al-Qahtani was clearly one of the instigators.

STUPID AND FUN STUFF



Police Ask Criminals Not to Commit Crimes



SLC Police Dept. 

@slcpd



Due to the confirmed case of [#COVID-19](#) from community spread, SLCPD is asking all criminal activities/nefarious behavior to cease until further notice. We appreciate your anticipated cooperation in halting crime & thank criminals in advance. [#SocialDistancingNow](#) [#behaveyourself](#)



Struthers Police Department

about 2 weeks ago



Due to the coronavirus, the police department is asking that all criminal activities stop until further notice. Thank you for your anticipated cooperation in the matter. We will update you when we deem it's appropriate to proceed with yo bad selves.

 2.8K

 1.8K

 83K

 17.9K 8:24 AM - Mar 14, 2020



 7,533 people are talking about this

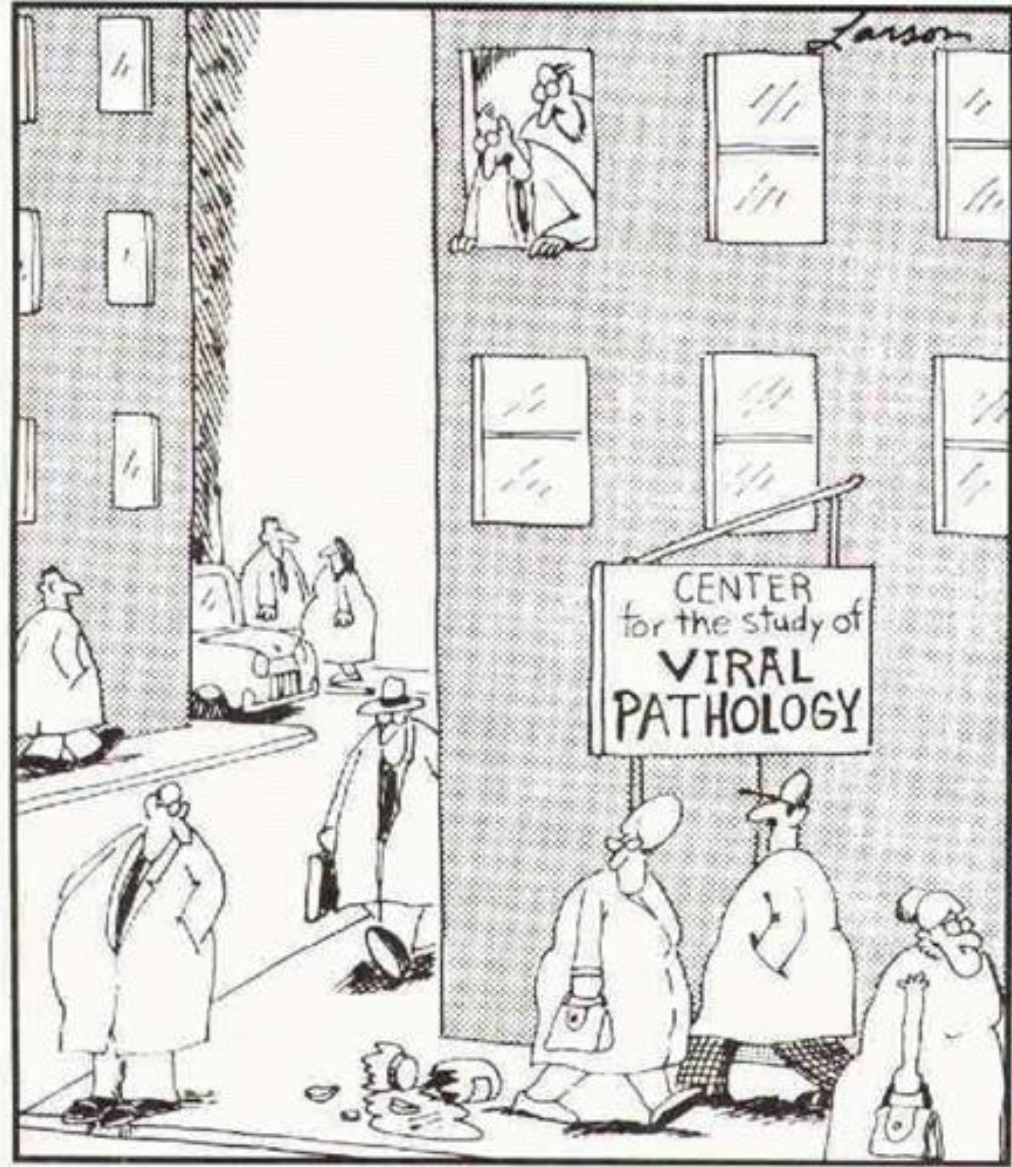




Pandemic Bingo

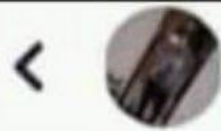


B	I	N	G	O
Put pants on before dialing in	Time losing all meaning	Wish you had been calling it “social distancing” all along	<i>Contagion</i> jokes	Family time now quantity over quality
Existential dread	Mornings suddenly enjoyable and full of possibility	Afraid of own hands	“Everything is fine” meme	Cadbury Mini Eggs for breakfast
Meetings losing all meaning	Unnatural longing for office birthday cake	FREE SPACE: Touching your face	Sudden everyone-is-talking-at-the-same-time-why	Pet time now constant and necessary
Full screen freeze with mouth wide open	Practical dread	Laugh to keep from freaking the fuck out	Your grandma was right, going for a walk is nice	Seeing co-workers’ bedrooms
Only hear every fifth word but get the gist	Me time now incredibly too much	Meaning losing all meaning	Full screen freeze but sound just keeps going as if it exists in a parallel functioning universe	Pound of bacon for lunch



"Uh-oh."

<http://go.to/funpic>



Brandon Mekish

Yesterday at 9:02 PM · 🧑🏻



So they really clothes school tomorrow



Like



Comment

😬 El Desalmado and 31 others



Sky Vitalene

They shirt it down 😬 16

20h Like Reply



Jayden Jack

That socks 😬 16

20h Like Reply

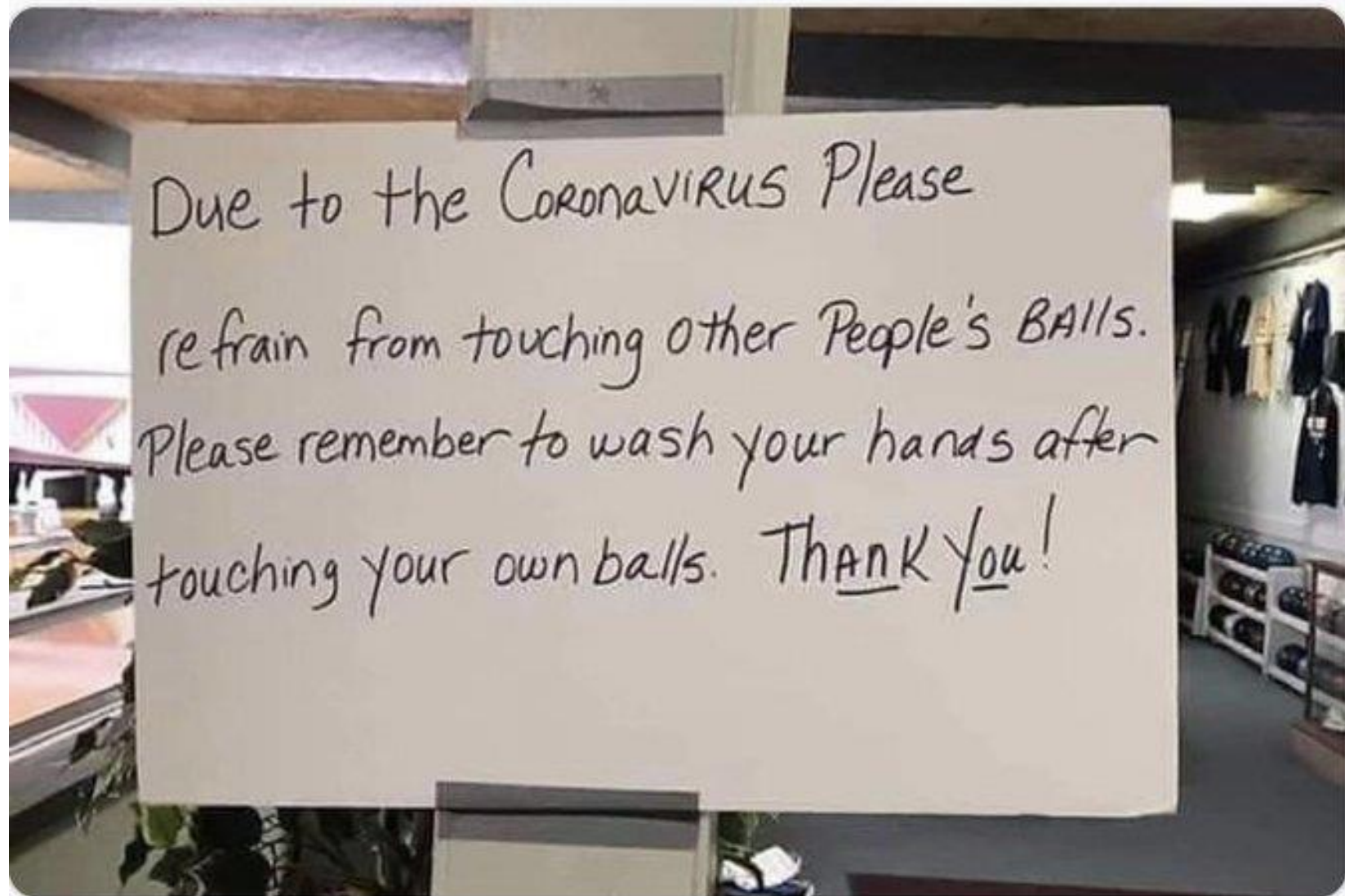


Karissa Dawn

i was underwear of this

19h Like Reply 😬 18

Seen at Bowling Alley



Thank You!

- Please provide feedback to ilene.klein@phoenix.gov
- Please take care of yourself!

