CYBERCRANE

WHAT YOU DON’T KNOW BUT SHOULD

Contact: Charles.Andrews.CSO@gmail.com

Worlds #1 Security Influencer

Cyber Global Expert

Retired Chief of Police/TX Master Peace Officer Reserve

Retired Global CSO (Chief Security Officer)

World Crime Prevention Certified/Expert

Yellowstone/6666 Ranch Wanna Be'

Award Winning Cyber Veteran

Global Cyber Strategic Advisor

Former Deputy CISO for all of Texas

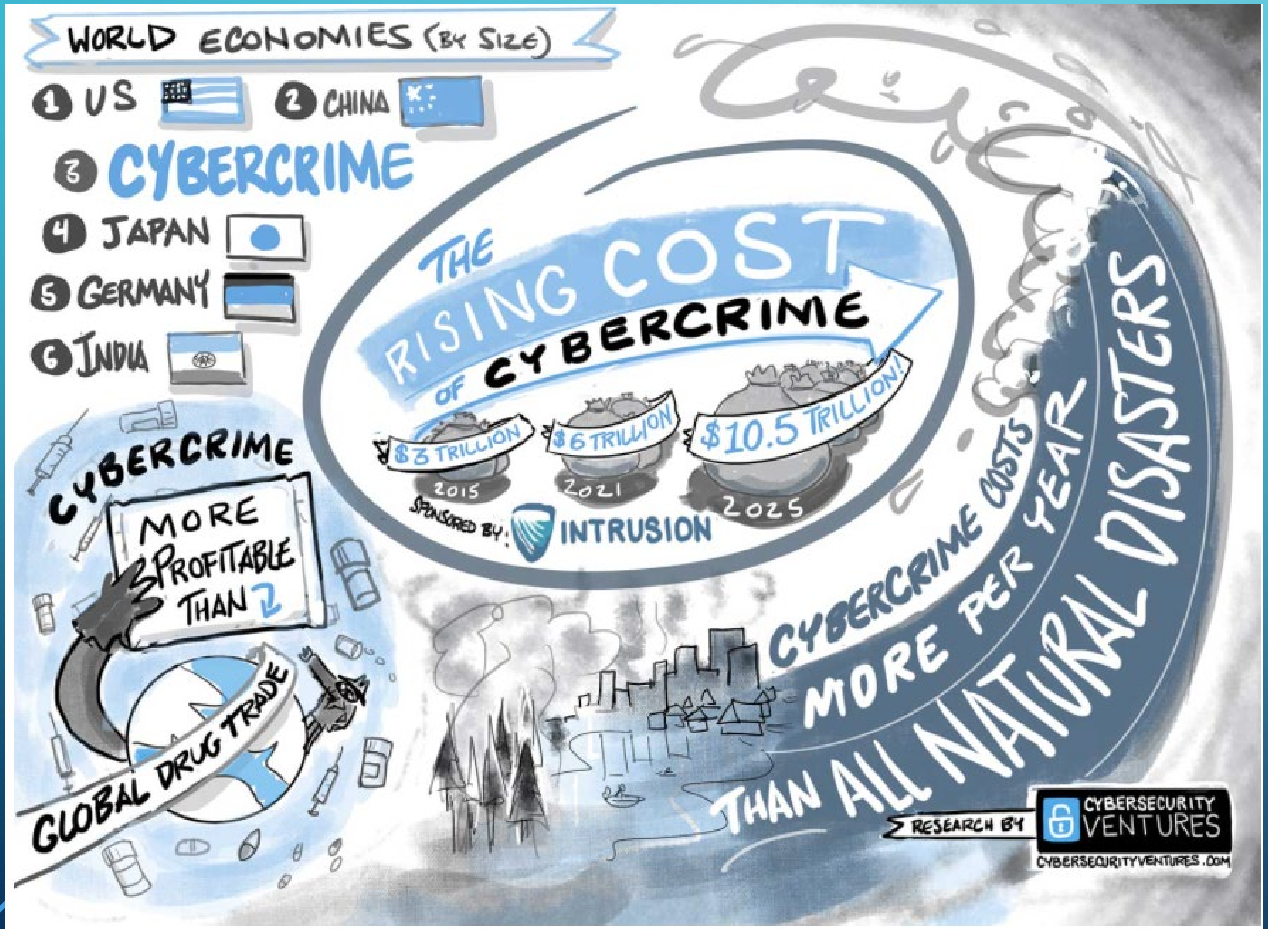
Commander for the Largest Cyberattack on Local Government in US History

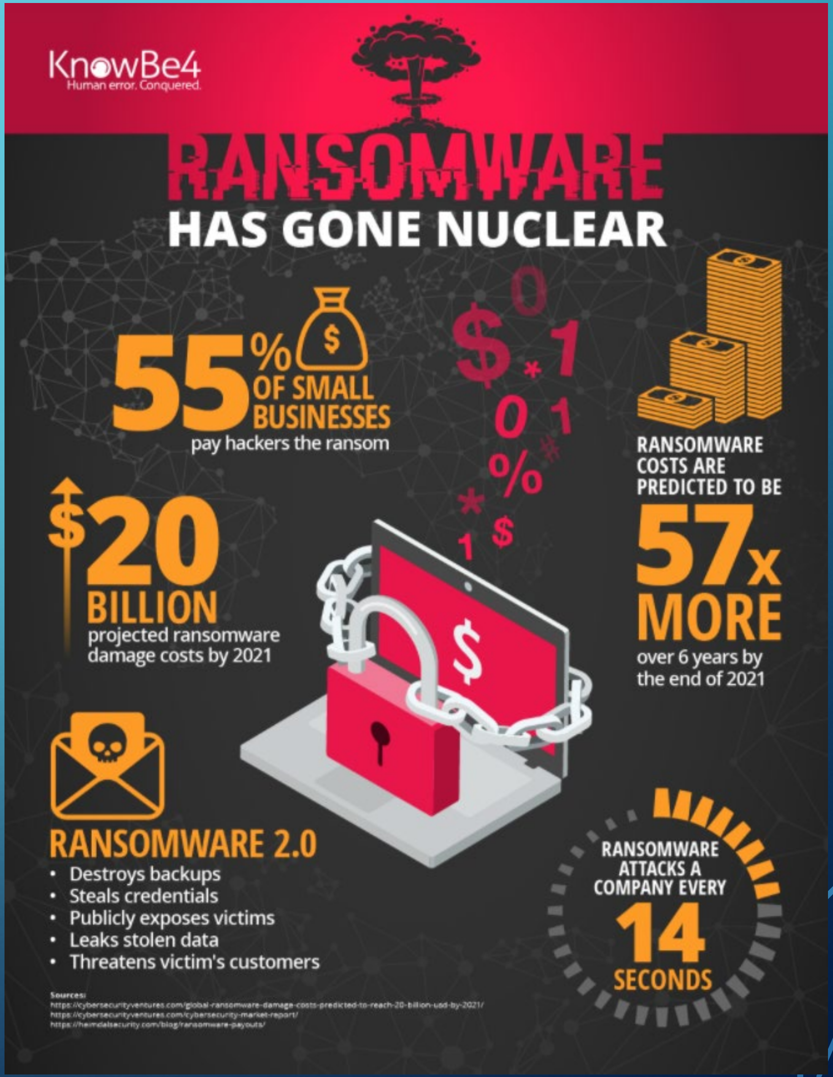
Director of Research for DF and Cyber at SHSU, eat em up kats

From a Texas town of 196 people

THE TOASTER IS THREATENING TO BURN THE HOUSE DOWN IF WE DON'T FEED IT SOME CRYPTO!

THE STATE OF CYBERSECURITY HOW BAD IS IT OUT THERE?


WORLD ECONOMIES (BY SIZE)
1 US
2 CHINA
3 CYBERCRIME
4 JAPAN
5 GERMANY
6 INDIA
THE RISING COST OF CYBERCRIME
$3 TRILLION
2015
$6 TRILLION
2021
$10.5 TRILLION!
2025
SPONSORED BY: INTRUSION
CYBERCRIME MORE PROFITABLE THAN
GLOBAL DRUG TRADE
CYBERCRIME COSTS MORE PER YEAR THAN ALL NATURAL DISASTERS
RESEARCH BY CYBERSECURITY VENTURES
CYBERSECURITYVENTURES.COM



RANSOMWARE HAS GONE NUCLEAR

55% OF SMALL BUSINESSES pay hackers the ransom

$20 BILLION projected ransomware damage costs by 2021

RANSOMWARE COSTS ARE PREDICTED TO BE 57x MORE over 6 years by the end of 2021

RANSOMWARE 2.0

- Destroys backups
- Steals credentials
- Publicly exposes victims
- Leaks stolen data
- Threatens victim's customers

RANSOMWARE ATTACKS A COMPANY EVERY 14 SECONDS

Sources:
https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
https://cybersecurityventures.com/cybersecurity-market-report/
https://heimdalsecurity.com/blog/ransomware-payouts/

CONSTRUCTION INDUSTRY IS RIGHT IN THE THICK OF IT AND BEING ACTIVELY TARGETED

THESE ARE A CONCERN FOR EVERYONE

PEOPLE

They want your employees' personal info

PROJECTS

They want you competitive advantage and intellectual property

FINANCES

They want your financial information so they can steal your money

THESE ARE CONCERNS SPECIFIC TO THE CRANE INDUSTRY

DRAWINGS AND PLANS

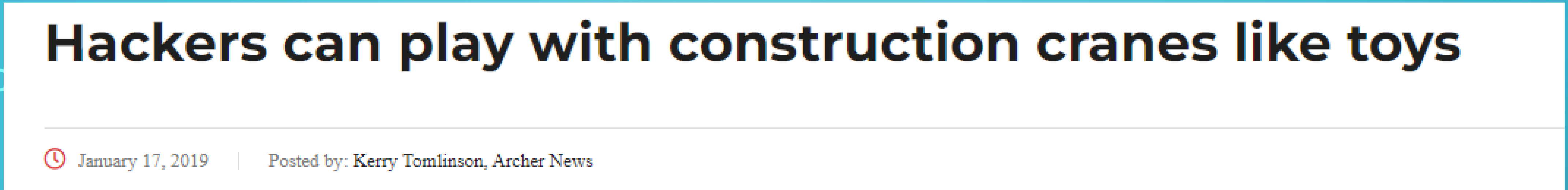
Why design things themselves when they can just take yours?

PLANNING AND LOGISTICS

If they can compromise your logistics and supply chain, they can ruin you or hold you hostage

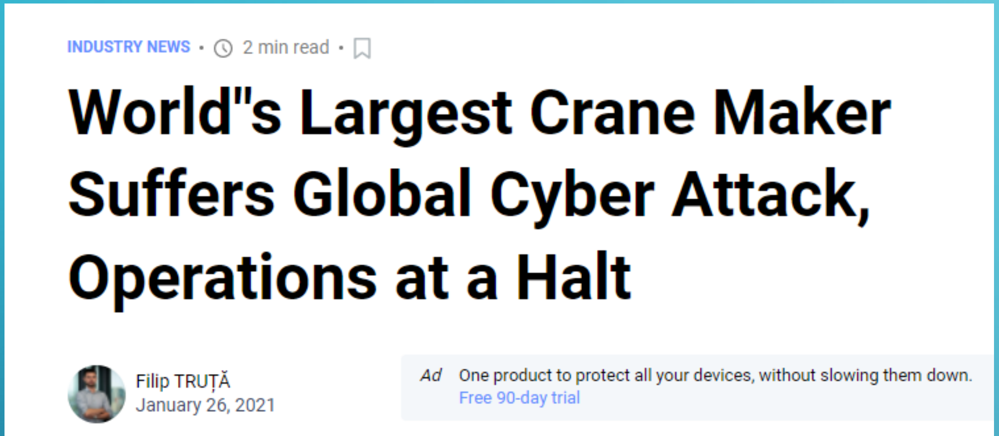
SYSTEMS AND EQUIPMENT

This is where it gets real bad, they compromise your systems and hold your data hostage, or worse yet, they compromise your equipment and get people killed.



Hackers can play with construction cranes like toys

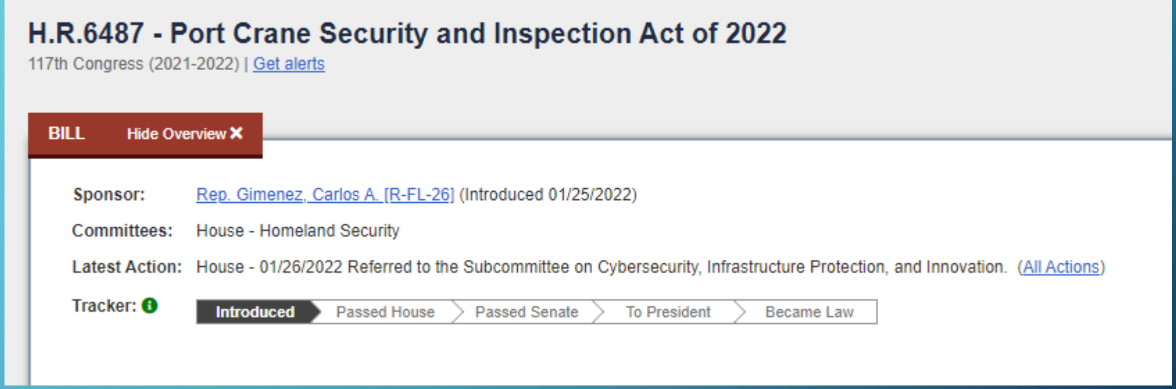
January 17, 2019 | Posted by: Kerry Tomlinson, Archer News



INDUSTRY NEWS • 2 min read •

World"s Largest Crane Maker Suffers Global Cyber Attack, Operations at a Halt

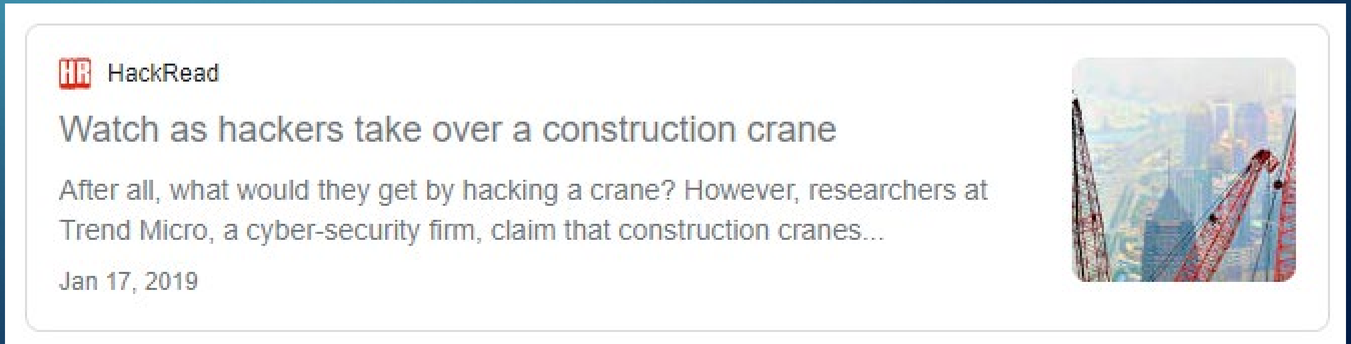
Filip TRUȚĂ
January 26, 2021



H.R.6487 - Port Crane Security and Inspection Act of 2022

117th Congress (2021-2022) | Get alerts

Sponsor:	Rep. Gimenez, Carlos A. [R-FL-26] (Introduced 01/25/2022)
Committees:	House - Homeland Security
Latest Action:	House - 01/26/2022 Referred to the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation. (All Actions)
Tracker:	Introduced > Passed House > Passed Senate > To President > Became Law



HackRead

Watch as hackers take over a construction crane

After all, what would they get by hacking a crane? However, researchers at Trend Micro, a cyber-security firm, claim that construction cranes...

Jan 17, 2019

https://www.hackread.com/watch-as-hackers-take-over-construction-crane/

I DON'T KNOW ANYTHING ABOUT CYBER! WHAT CAN WE DO?!

FOCUS ON THE BUSINESS

No one understands your business better than you

Understand what could hurt the most if it got taken out

Approach cyber like any other business problem

FIND TRUSTED PARTNERS

There are a lot of people out there who claim to do this

Find people who understand your business and speak your language

IT'S ALL BUSINESS RISK

Finance systems

Crane operations

Downtime

Intellectual Property

Logistics

Anything that can affect the bottom line and touches technology in anyway

"You run the crane business, let your partner take care of your cyber", #1 Security Influencer

COMPANY PROFILES TOO ROUGH TO WRITE DOWN

WILL CYBER INSURANCE COVER ME?

Cyber insurance is a new field with bad math

They will ask you if and how you are protecting everything in your environment

When you have an incident, they will look for any reason to not pay

When they do pay, it is usually to the bad guys and does not cover your own recovery

LET'S TALK RANSOMWARE: SCARY STUFF

COMPROMISE

They know who you are

They know how to get in

They map your environment

They break your backups first

ENCRYPTION

They steal your data

Then they make your system unusable

If your backups are no good, you are a sitting duck

EXTORTION

They charge you for access to your own data

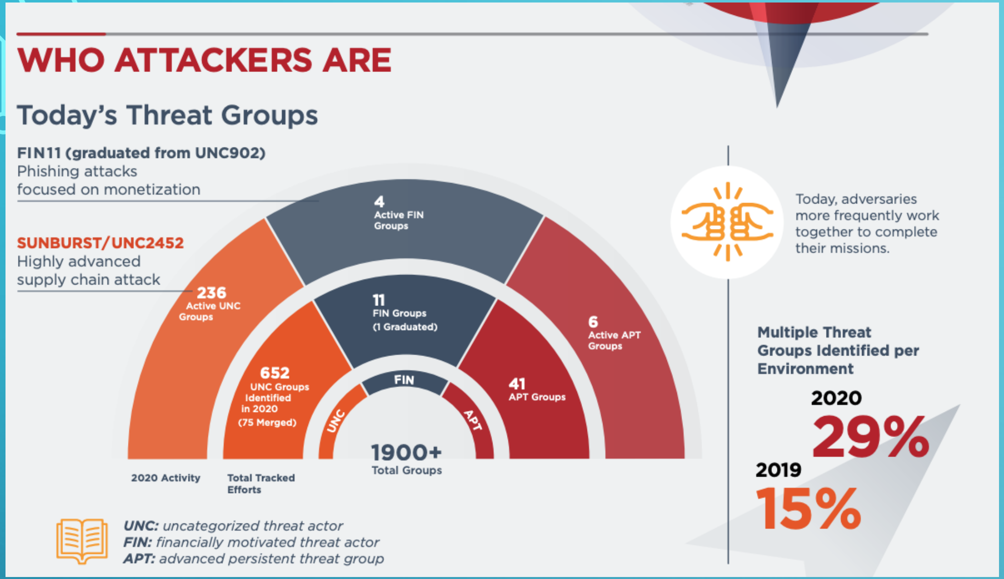
Millions of dollars in crypto currency

If you won't pay, they publish or auction your information on the dark web

If you get hit once, you can expect to get hit again, and sooner than later.
They keep track of the soft targets and sell/share that info to each other: Who you gonna call?

RANSOMWARE FIGURES

THERE WERE AN ESTIMATED 185 MILLION RANSOMWARE ATTACKS GLOBALLY IN 2020



WHO ATTACKERS ARE

Today's Threat Groups

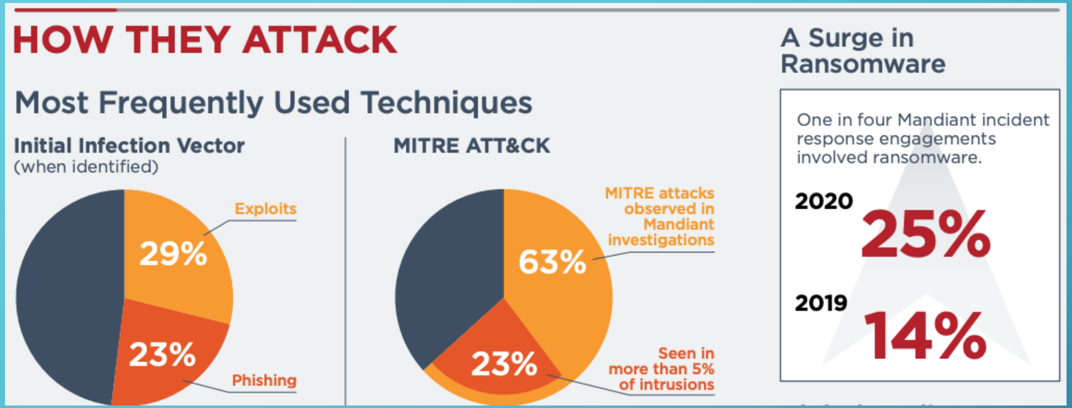
FIN11 (graduated from UNC902)
Phishing attacks
focused on monetization

SUNBURST/UNC2452
Highly advanced
supply chain attack

Today, adversaries more frequently work together to complete their missions.

Multiple Threat Groups Identified per Environment

UNC: *uncategorized threat actor*
FIN: *financially motivated threat actor*
APT: *advanced persistent threat group*

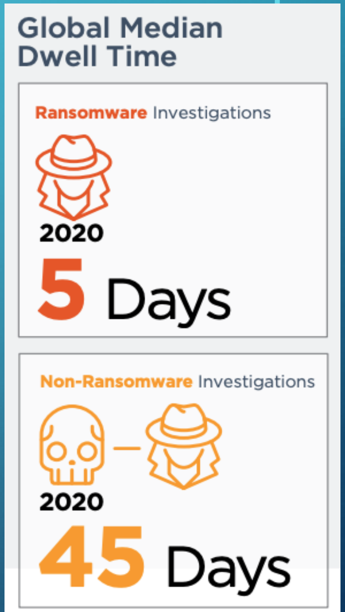


HOW THEY ATTACK

Most Frequently Used Techniques

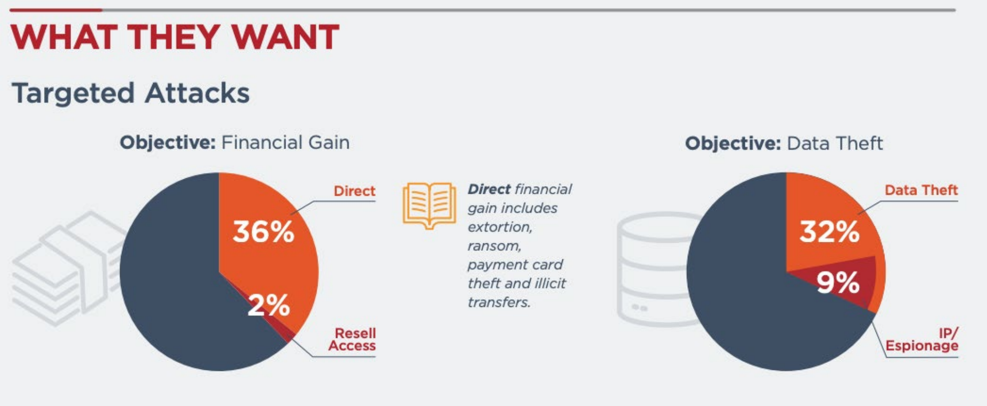
A Surge in Ransomware

One in four Mandiant incident response engagements involved ransomware.



Global Median Dwell Time

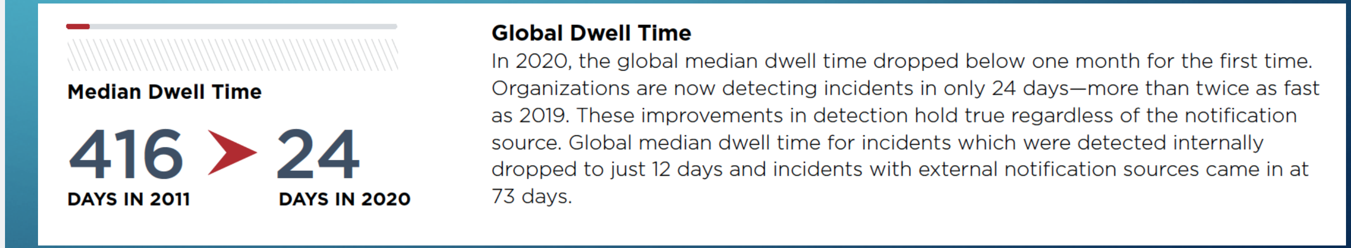
"Pervasive ransomware campaigns drove down the median dwell time as threat actors sought to capitalize on shifting trends in the workspace and a global crisis."



WHAT THEY WANT

Targeted Attacks

Direct *financial gain includes extortion, ransom, payment card theft and illicit transfers.*



Median Dwell Time

416 ➤ 24
DAYS IN 2011
DAYS IN 2020

Global Dwell Time

In 2020, the global median dwell time dropped below one month for the first time. Organizations are now detecting incidents in only 24 days—more than twice as fast as 2019. These improvements in detection hold true regardless of the notification source. Global median dwell time for incidents which were detected internally dropped to just 12 days and incidents with external notification sources came in at 73 days.

https://content.fireeye.com/m-trends/ig-m-trends-2021

FUTURE CONSIDERATIONS

REGULATIONS

Bills already introduced to congress

State legislature making reporting and protections mandatory

CRITICAL INFRASTRUCTURE

Construction relates to almost every critical infrastructure

Subjects the industry to potential regulation by association

Critical infrastructure is a massive target

GEO-POLITICS

One word: Russia

The time to start is now, get ahead while you can.

Planning and a focus on fundamentals are the only way to beat these guys. -Andy

PLANNING AND PREPARATION WITH INTENT THE ONLY WAY TO STAY AHEAD OF THE THREAT

- Fundamentals First
- Have a plan
- Practice makes perfect
- Focus on the business
- Ask questions from a business perspective
- Find a good partner who can connect your cyber needs to the bottom line
- Don’t buy the shiny toy, buy the right tool
- Trusted partners are critical when facing the unknown

There is no such thing as a shameless plug, its just a plug.

QUESTIONS?

Call this Texas Cyber Cowboy if you need to talk…

CHUCK ANDREWS
CLINT EASTWOOD
TEXAS CYBER COWBOY
HOW THE WWW WAS WON
FRIENDS OF CHUCK MEDIA GROUP PRESENTS SECURITY TALK NOW EPIC PICTURES
ANGIE ANDREWS STEVEN DORAN AS THE TRAIL BOSS JAMES BOND CHUCK NORRIS BRUCE WILLIS JOHN WAYNE ANONYMOUS RIFLEMAN
WRITTEN BY CHUCK NORRIS TEXAS RANGERS JAMES BOND DIRECTED BY CHUCK ANDREWS EXECUTIVE PRODUCER SADIE ANDREWS DIRECTOR OF PHOTOGRAPHY VIC CLARK PHOTOGRAPHY STORY BY RUSSIAN HACKERS
IN THEATERS SEPTEMBER 11

Charles.Andrews.CSO@gmail.com