Ransomware Re-Revisited

Dain Couch, AOC Chief IT Security Officer
Sharon Blount-Baker, Crawford County Circuit Clerk
Carrie Kilgore, Crawford County Chief Deputy Circuit Clerk

Where we were

Where we are

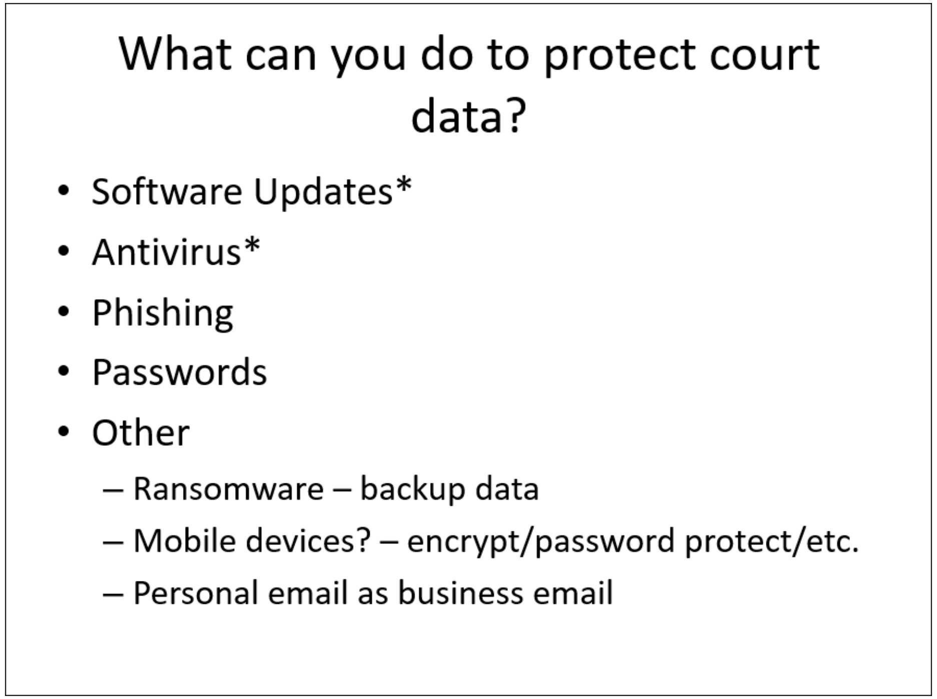
Resources and Mitigation

AOCs

Crawford County Ransomware

2014

Securing Court Information



What can you do to protect court data?

- Software Updates*
- Antivirus*
- Phishing
- Passwords
- Other
  - – Ransomware – backup data
  - – Mobile devices? – encrypt/password protect/etc.
  - – Personal email as business email

Largely single computers

1 bitcoin ransom – about $300

Now

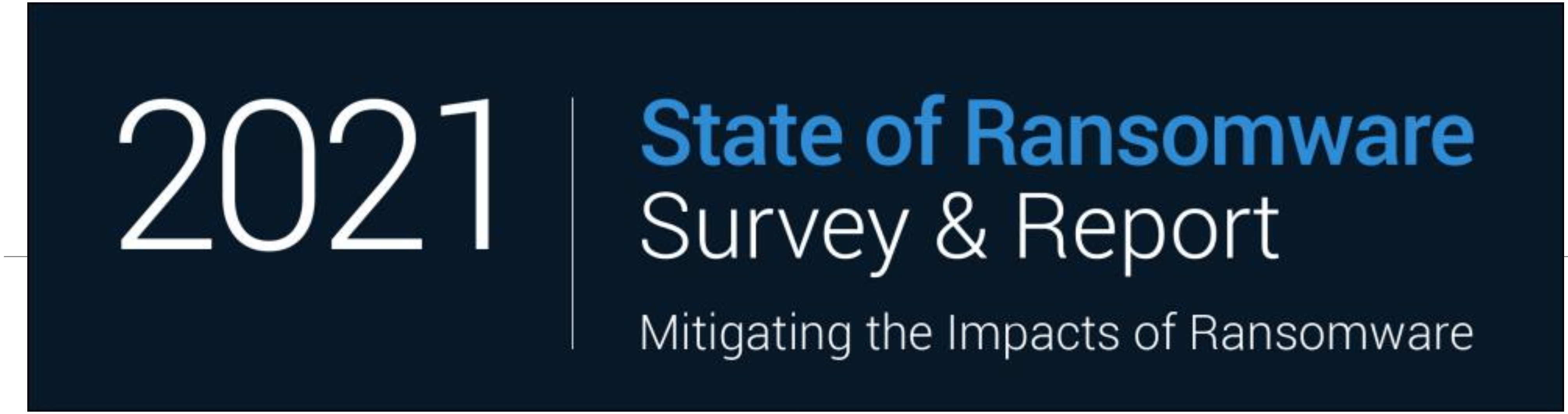
Ransomware is a billion-dollar industry.

Shifted from individual machines to network breach, lateral movement, exfiltration.

- Double Extortion
- Triple Extortion

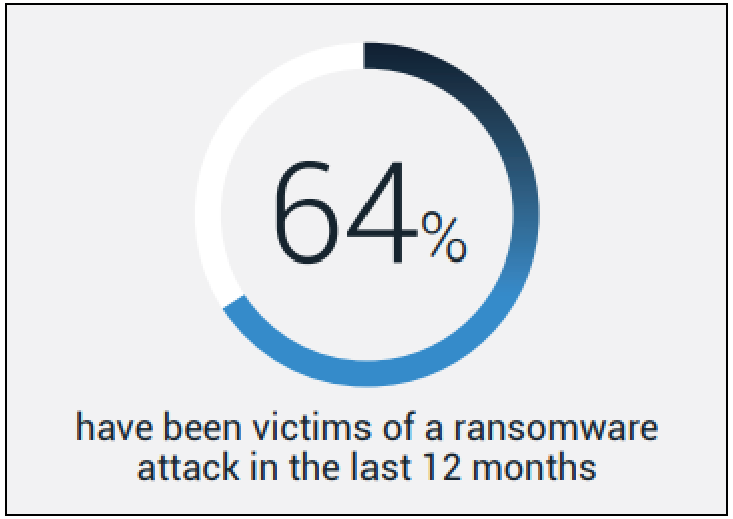
Cybersecurity focus/talk has shifted from prevention to recovery to RESILIENCE.

“Failing gracefully and recovering quickly”



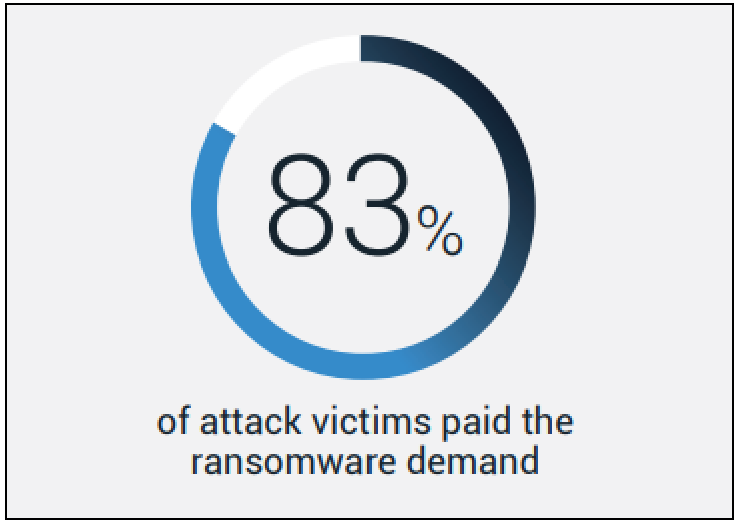
2021 State of Ransomware Survey & Report

Mitigating the Impacts of Ransomware



64%

have been victims of a ransomware attack in the last 12 months



83%

of attack victims paid the ransomware demand

thycotic. Centrify

https://thycotic.com/resources/ransomware-survey-and-report-2021/

$925,162

*Average ransomware payment as seen by Palo Alto response team

https://www.paloaltonetworks.com/blog/2022/06/average-ransomware-payment-update/#:~:text=The%20numbers%20are%20startling%3A%20The,rose%2071%25%20from%20last%20year

Resilience

Prevention – much the same as it ever was

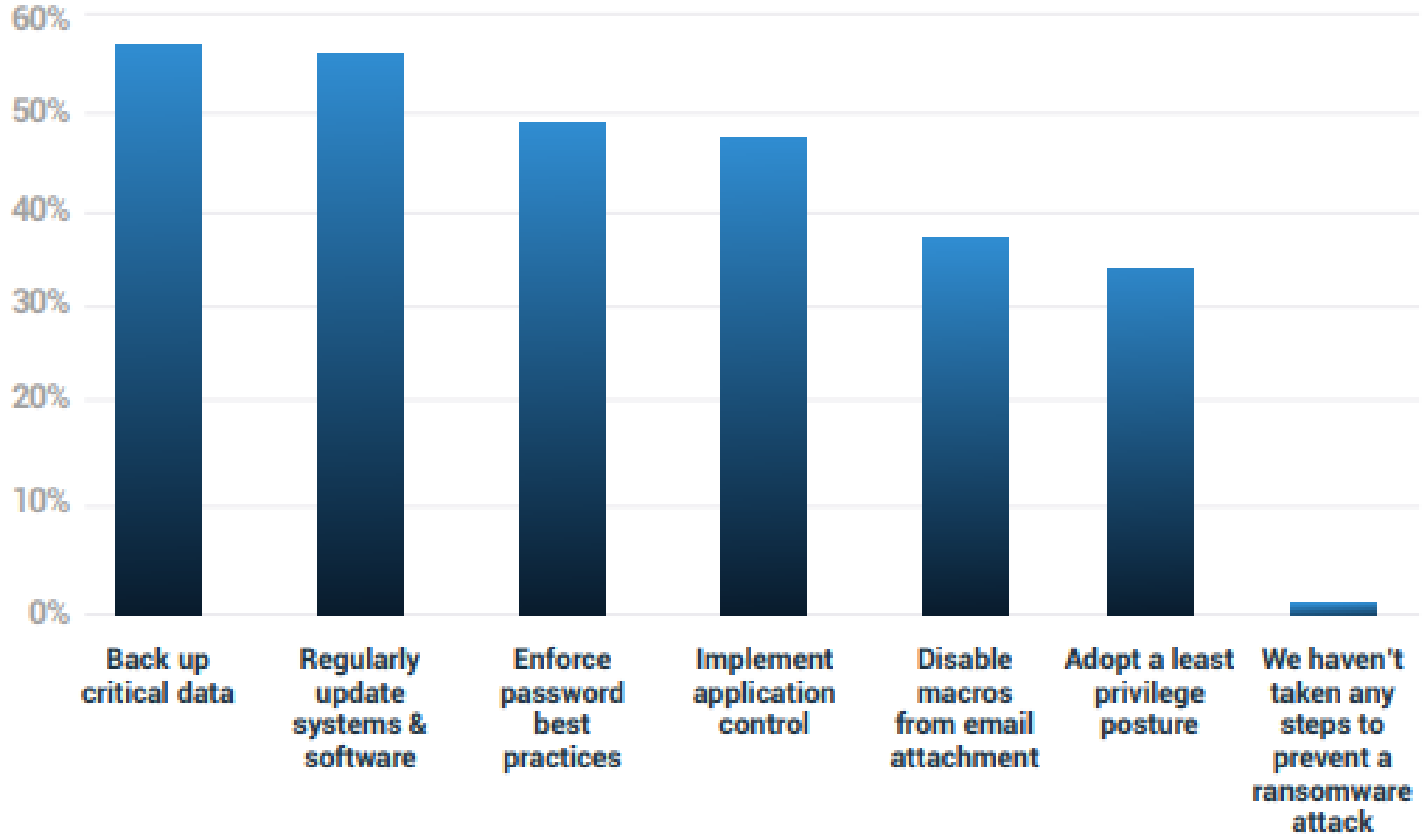
Recovery – also much the same as it ever was

Are you improving?

Is incident response to cybersecurity events included in your COOP?

- Do you have a plan?
- Have you trained on it?
- Have you exercised it?

What, if any, steps have you taken to prevent a ransomware attack? (Tick all that apply)



Resources

Multi State Information Sharing and Analysis Center (MS-ISAC) https://www.cisecurity.org/ms-isac

- Free services and products. Become a member! https://learn.cisecurity.org/ms-isac-registration

Cybersecurity & Infrastructure Security Agency (CISA) https://cisa.gov

- Stop Ransomware https://www.cisa.gov/stopransomware

National Center for State Courts https://ncsc.org (search on “cybersecurity”)

- Cybersecurity Basics for Courts https://www.ncsc.org/__data/assets/pdf_file/0014/15251/cybersecurity-2020-01-06.pdf

No More Ransom https://nomoreransom.org

- Prevention advice, identification and decryption tools

CISA Short list of Ransomware Mitigations

CISA recommends the following precautions to protect users against the threat of ransomware:

Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.

Never click on links or open attachments in unsolicited emails.

Back up data on a regular basis. Keep it on a separate device and store it offline.

Follow safe practices when using devices that connect to the Internet. Read Good Security Habits for additional details.

- Password Security
- Public networks and Wi-Fi
- Suspicious Emails
- Patching

https://www.cisa.gov/stopransomware/ransomware-faqs

It’s not if, it’s when.

May/June 2021

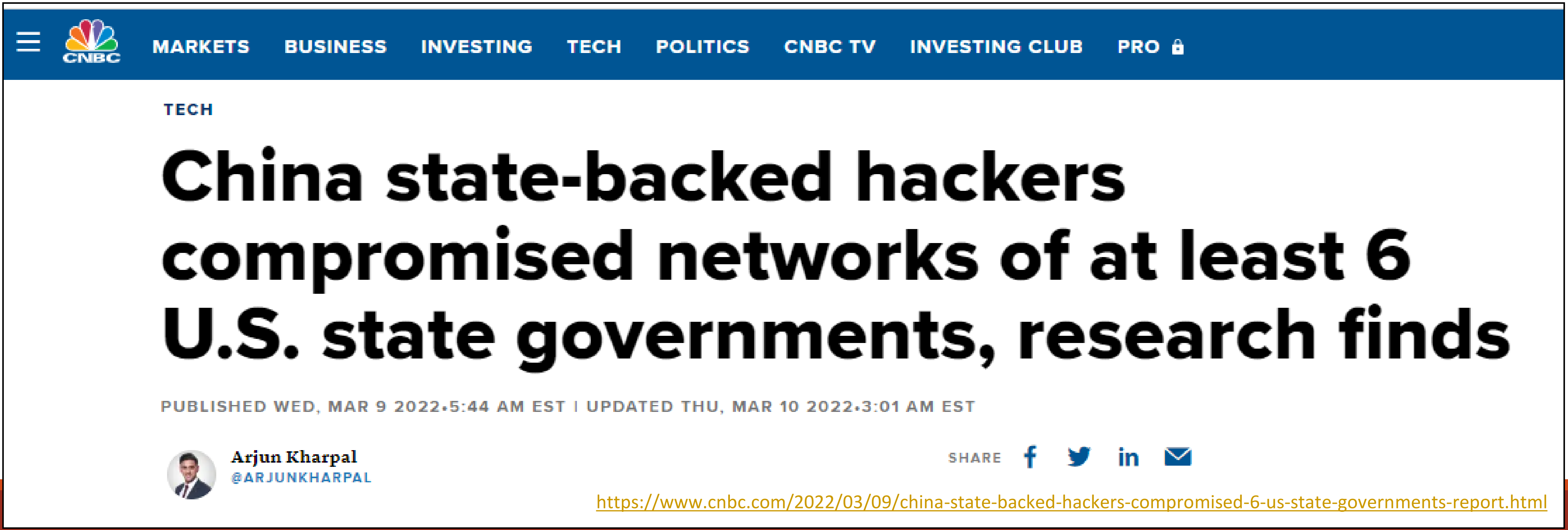
APT 41 Intrusion

AOC

May/June 2021

APT 41 Intrusion

In MS-ISAC releases and the media



TECH

China state-backed hackers compromised networks of at least 6 U.S. state governments, research finds

PUBLISHED WED, MAR 9 2022•5:44 AM EST | UPDATED THU, MAR 10 2022•3:01 AM EST

Arjun Kharpal
@ARJUNKHARPAL

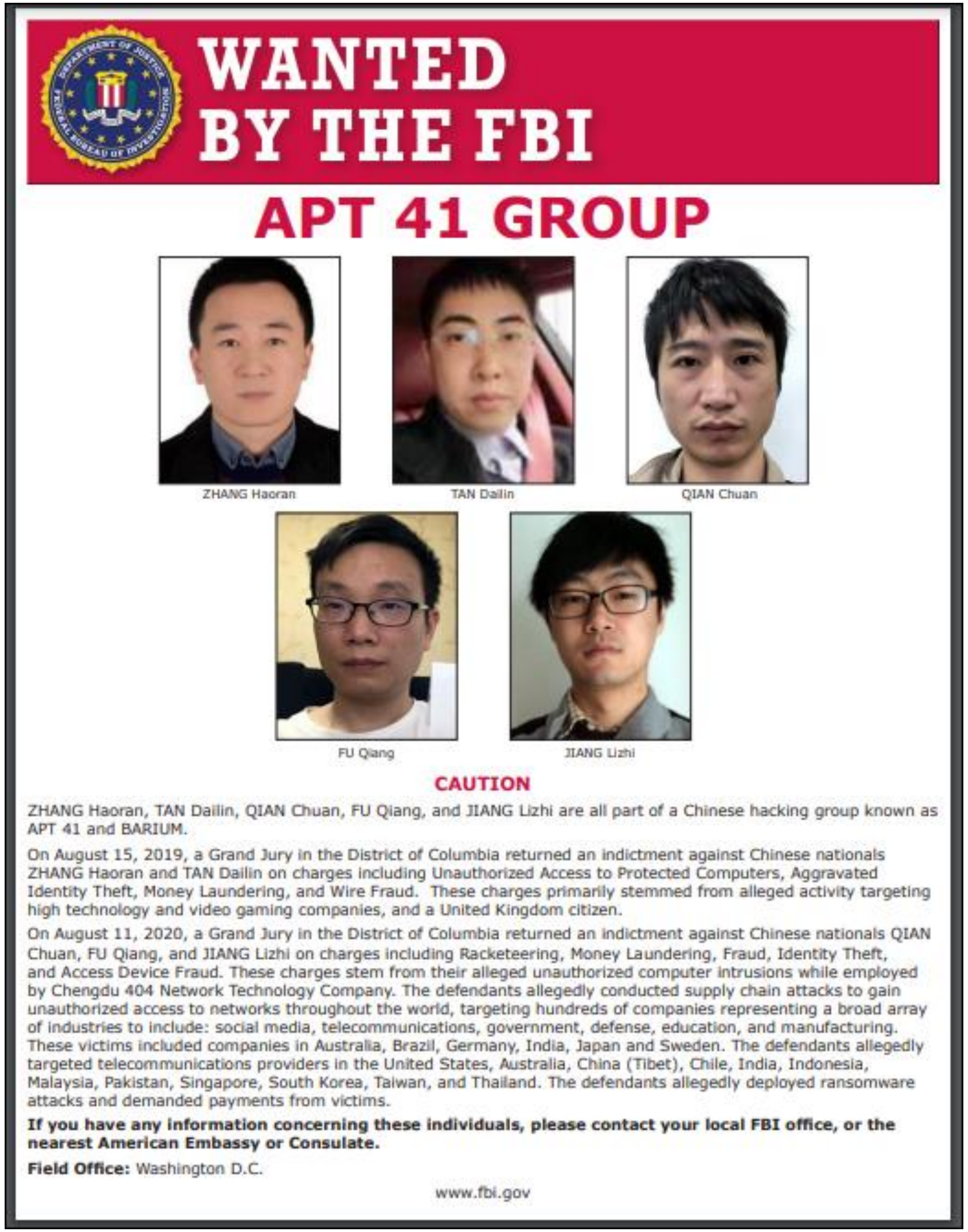
https://www.cnbc.com/2022/03/09/china-state-backed-hackers-compromised-6-us-state-governments-report.html

APT 41 Group

Indicted by DC Grand Juries in 2019 and 2020 for Unauthorized Access to Protected Computers, Aggravated Identity Theft, Racketeering, Money laundering, Fraud, Identity Theft, Access Device Fraud.

Ransomware attacks included in their arsenal/techniques.

https://www.fbi.gov/wanted/cyber



WANTED BY THE FBI

APT 41 GROUP

ZHANG Haoran

TAN Dailin

QIAN Chuan

FU Qiang

JIANG Lizhi

CAUTION

ZHANG Haoran, TAN Dailin, QIAN Chuan, FU Qiang, and JIANG Lizhi are all part of a Chinese hacking group known as APT 41 and BARIUM.

On August 15, 2019, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals ZHANG Haoran and TAN Dailin on charges including Unauthorized Access to Protected Computers, Aggravated Identity Theft, Money Laundering, and Wire Fraud. These charges primarily stemmed from alleged activity targeting high technology and video gaming companies, and a United Kingdom citizen.

On August 11, 2020, a Grand Jury in the District of Columbia returned an indictment against Chinese nationals QIAN Chuan, FU Qiang, and JIANG Lizhi on charges including Racketeering, Money Laundering, Fraud, Identity Theft, and Access Device Fraud. These charges stem from their alleged unauthorized computer intrusions while employed by Chengdu 404 Network Technology Company. The defendants allegedly conducted supply chain attacks to gain unauthorized access to networks throughout the world, targeting hundreds of companies representing a broad array of industries to include: social media, telecommunications, government, defense, education, and manufacturing. These victims included companies in Australia, Brazil, Germany, India, Japan and Sweden. The defendants allegedly targeted telecommunications providers in the United States, Australia, China (Tibet), Chile, India, Indonesia, Malaysia, Pakistan, Singapore, South Korea, Taiwan, and Thailand. The defendants allegedly deployed ransomware attacks and demanded payments from victims.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Washington D.C.

www.fbi.gov

Root cause unknown – log4j?

Server was segmented from the rest of the network – no lateral movement.

Other AOCs

Kentucky – Twice (2014, 2019)

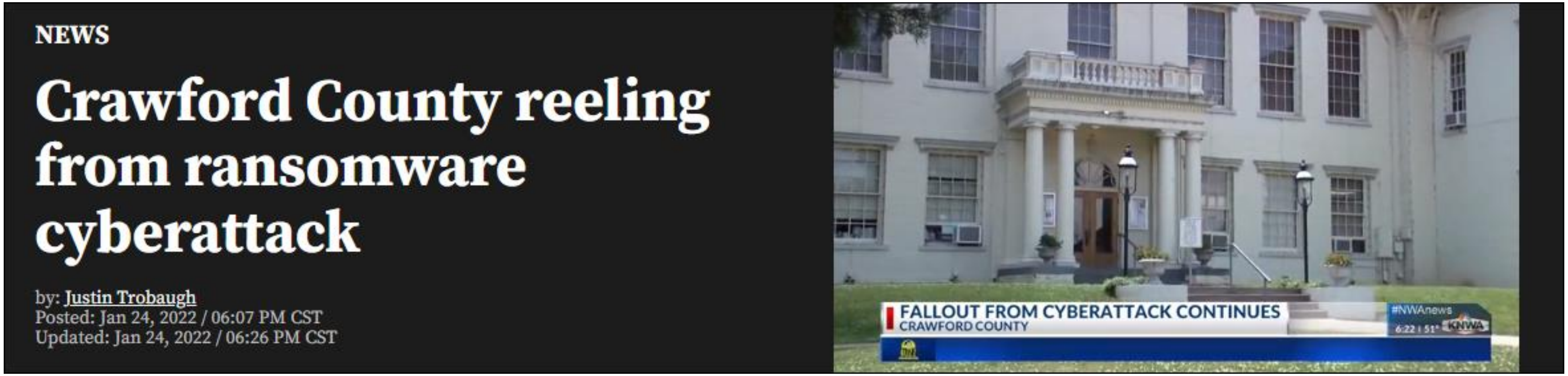
Georgia (2019)

Texas (2020)

Alaska (2021)

Kentucky recording: https://cdm16501.contentdm.oclc.org/digital/collection/tech/id/978

Texas and Alaska recording from NCSC Webinars https://vimeo.com/683293406 (requires free vimeo account)

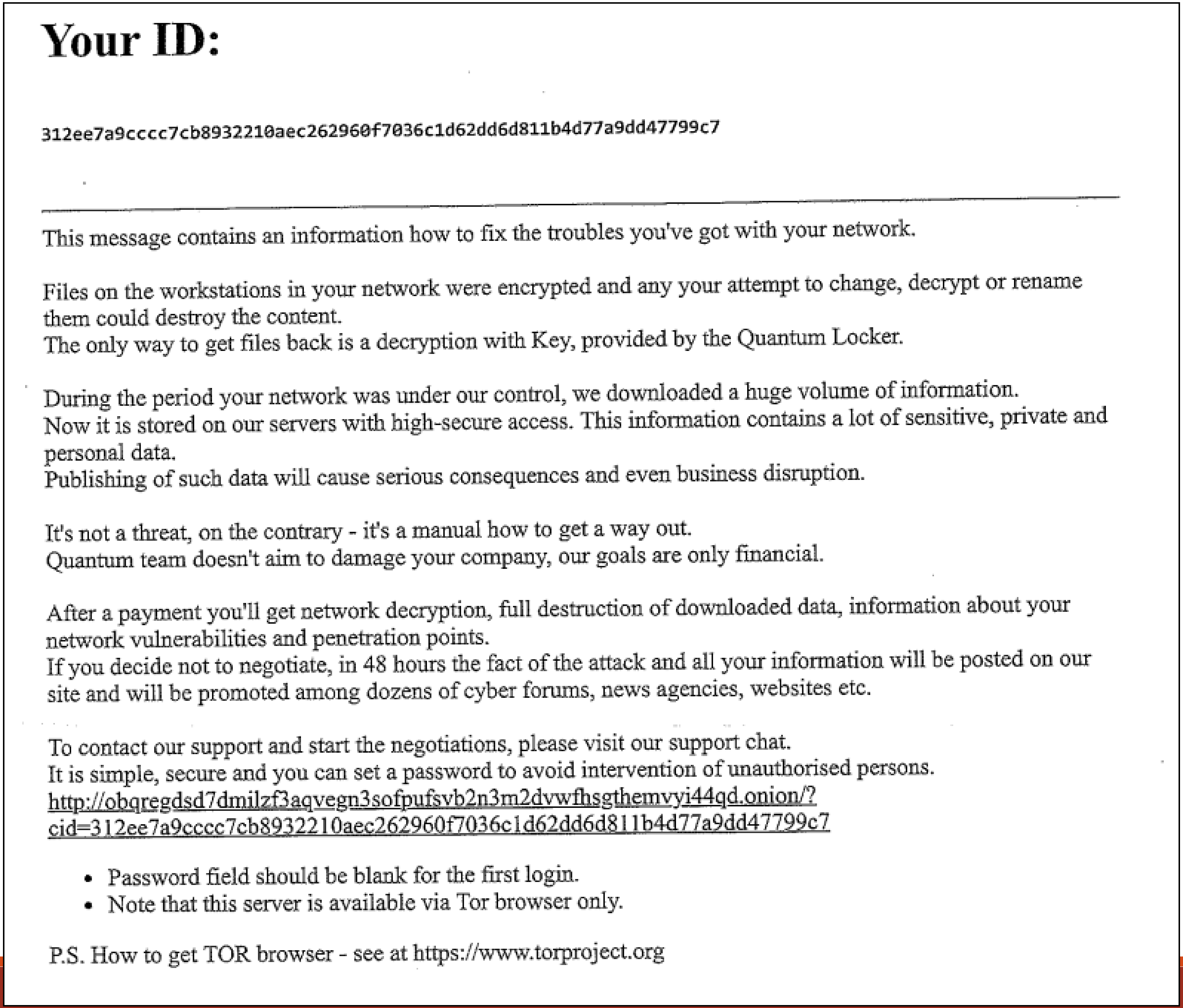


NEWS

Crawford County reeling from ransomware cyberattack

by: Justin Trobaugh
Posted: Jan 24, 2022 / 06:07 PM CST
Updated: Jan 24, 2022 / 06:26 PM CST

https://www.nwahomepage.com/news/crawford-county-reeling-from-ransomware-cyberattack/



Your ID:

312ee7a9cccc7cb8932210aec262960f7036c1d62dd6d811b4d77a9dd47799c7

This message contains an information how to fix the troubles you've got with your network.

Files on the workstations in your network were encrypted and any your attempt to change, decrypt or rename them could destroy the content.
The only way to get files back is a decryption with Key, provided by the Quantum Locker.

During the period your network was under our control, we downloaded a huge volume of information.
Now it is stored on our servers with high-secure access. This information contains a lot of sensitive, private and personal data.
Publishing of such data will cause serious consequences and even business disruption.

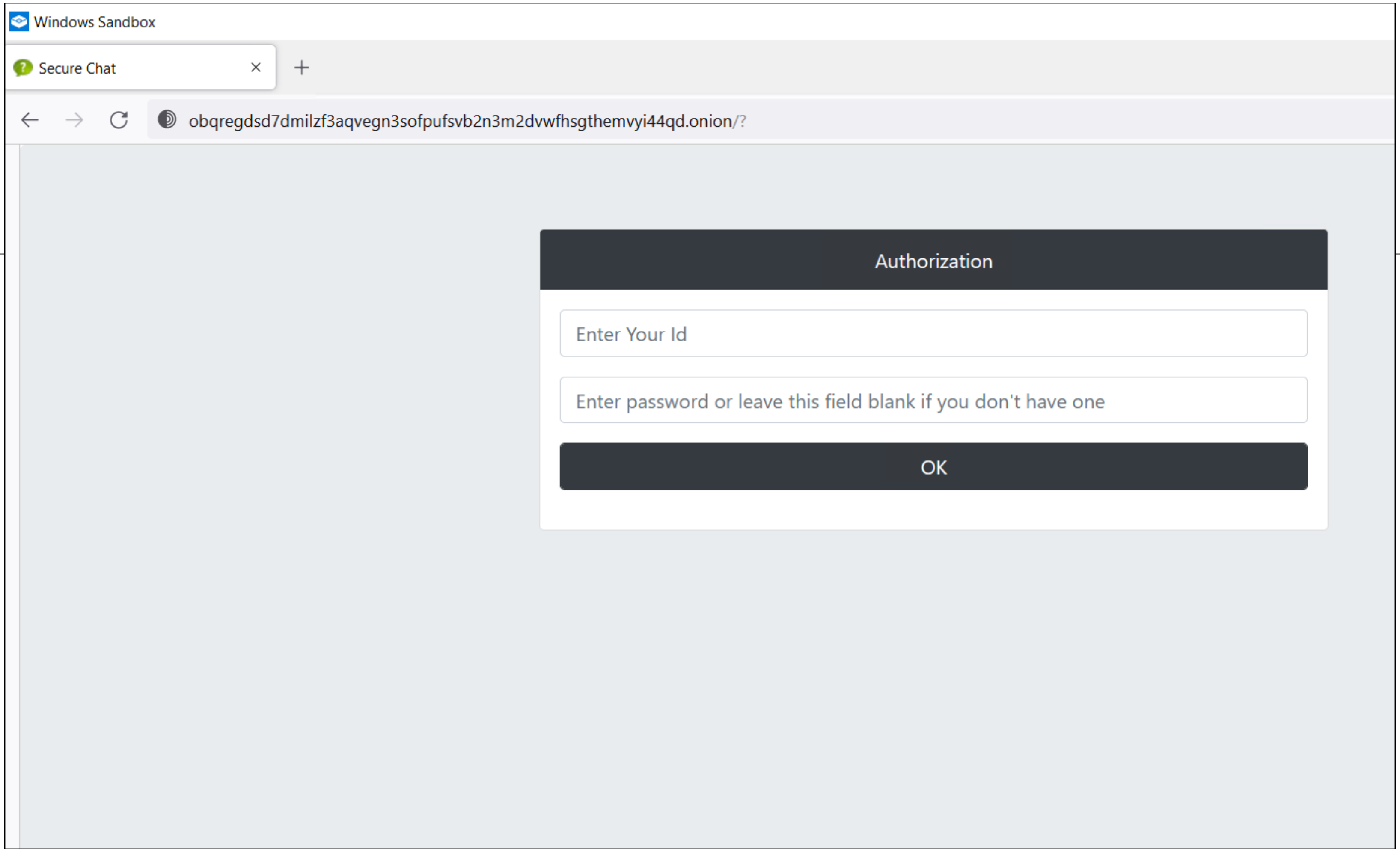
It's not a threat, on the contrary - it's a manual how to get a way out.
Quantum team doesn't aim to damage your company, our goals are only financial.

After a payment you'll get network decryption, full destruction of downloaded data, information about your network vulnerabilities and penetration points.
If you decide not to negotiate, in 48 hours the fact of the attack and all your information will be posted on our site and will be promoted among dozens of cyber forums, news agencies, websites etc.

To contact our support and start the negotiations, please visit our support chat.
It is simple, secure and you can set a password to avoid intervention of unauthorised persons.
http://obqregdsd7dmilzf3aqvegn3sofpufsvb2n3m2dvwfhsgthemvyi44qd.onion/?cid=312ee7a9cccc7cb8932210aec262960f7036c1d62dd6d811b4d77a9dd47799c7

- Password field should be blank for the first login.
- Note that this server is available via Tor browser only.

P.S. How to get TOR browser - see at https://www.torproject.org



obqregdsd7dmilzf3aqvegn3sofpufsvb2n3m2dvwfhsgthemvyi44qd.onion/?

Authorization

Enter Your Id

Enter password or leave this field blank if you don't have one

http://obqregdsd7dmilzf3aqvegn3sofpufsvb2n3m2dvwfhsgthemvyi44qd.onion

Questions?

Dain Couch dain.couch@arcourts.gov 501-410-1963