LMG SECURITY

New Trends in Cyber Incident Response and Forensics

Matt Durrin
IR Technical Lead
LMG Security

Sherri Davidoff
CEO
LMG Security

Who Are We?

New Book!

Ransomware Response

Sherri Davidoff

Founder & CEO, LMG Security

Training: Black Hat, FDIC, ABA, & more

“Alien” from “Breaking & Entering”

NEW BOOK! “Data Breaches”

Matt Durrin

Incident Response Technical Lead

Black Hat Instructor

Research & Development

Evil, sometimes.

LMG SECURITY

LMG SECURITY

New Trends in Cyber Incident Response and Forensics

Matt Durrin
IR Technical Lead
LMG Security

Sherri Davidoff
CEO
LMG Security

REvil ransomware hits US nuclear weapons contractor

By Lawrence Abrams

The Register®

{* SECURITY *}

The latest REvil ransomware victim? Sol Oriens. Oh, a US

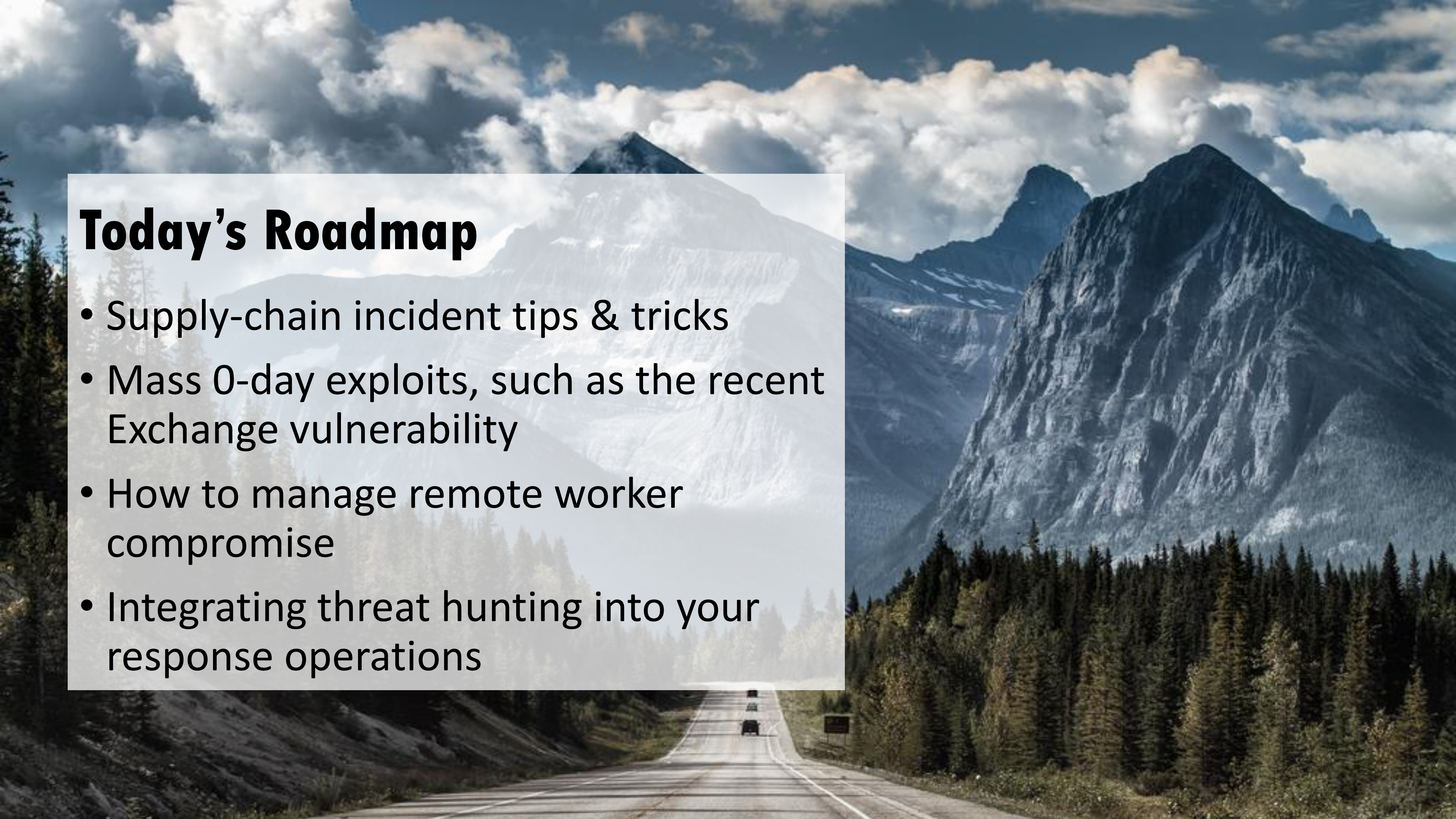
weapons contractor

aims 'no current indication' top-

vas plundered

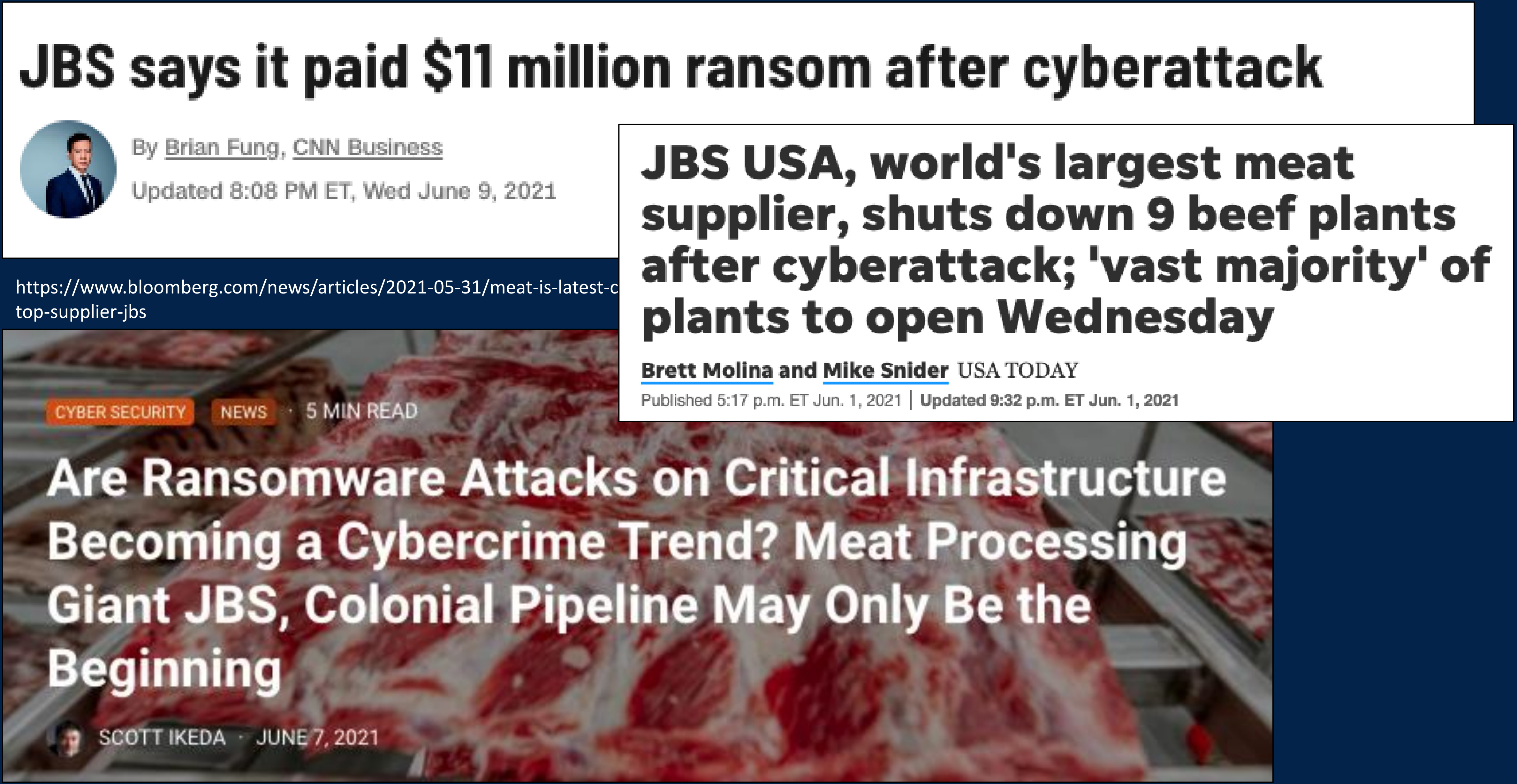
JBS and Colonial Pipeline hacks highlight how large food and energy companies have become prime targets

- Industry consolidation has created a single point of failure for major food and energy companies as hackers seek the largest payouts possible
- Any downtime for large companies critical to food and energy supplies could cost millions of dollars, increasing the likelihood they will meet demands



Today’s Roadmap

- Supply-chain incident tips & tricks
- Mass 0-day exploits, such as the recent Exchange vulnerability
- How to manage remote worker compromise
- Integrating threat hunting into your response operations



JBS says it paid $11 million ransom after cyberattack

By Brian Fung, CNN Business

Updated 8:08 PM ET, Wed June 9, 2021

JBS USA, world's largest meat supplier, shuts down 9 beef plants after cyberattack; 'vast majority' of plants to open Wednesday

Brett Molina and Mike Snider USA TODAY

Published 5:17 p.m. ET Jun. 1, 2021 | Updated 9:32 p.m. ET Jun. 1, 2021

CYBER SECURITY NEWS · 5 MIN READ

Are Ransomware Attacks on Critical Infrastructure Becoming a Cybercrime Trend? Meat Processing Giant JBS, Colonial Pipeline May Only Be the Beginning

SCOTT IKEDA · JUNE 7, 2021

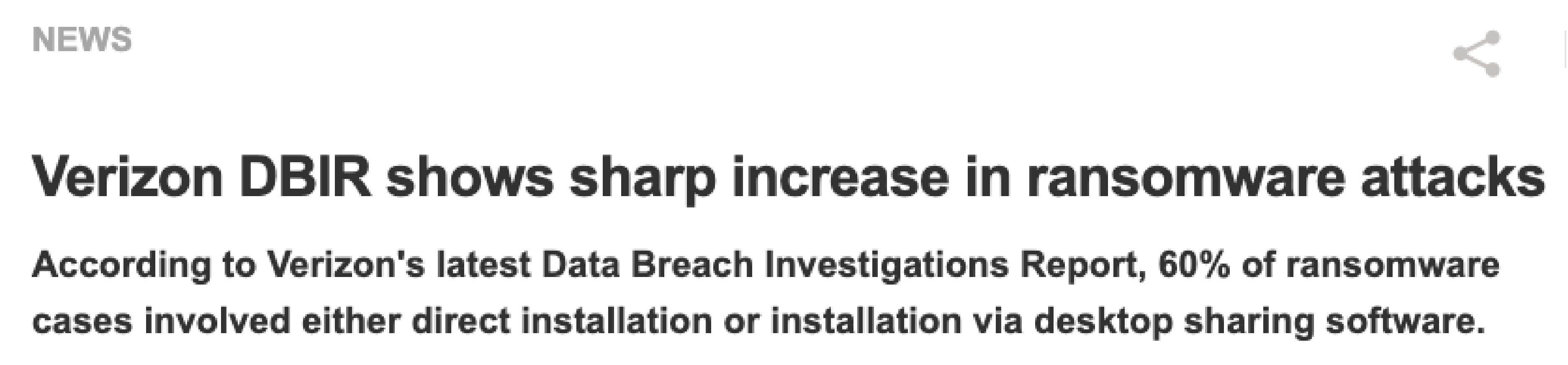
https://www.bloomberg.com/news/articles/2021-05-31/meat-is-latest-c
top-supplier-jbs

https://www.cnn.com/2021/06/09/busin
attack-11-million/index.html

https://www.usatoday.com/story/money/shopping/2021/06/01/jbs-cyberattack-worlds-largest-meat-supplier-closes-5-beef-plants/7493850002/

https://www.cpomagazine.com/cyber-security/are-ransomware-attacks-on-critical-infrastructure-
becoming-a-cybercrime-trend-meat-processing-giant-jbs-colonial-pipeline-may-only-be-the-beginning/

Ransomware Attacks

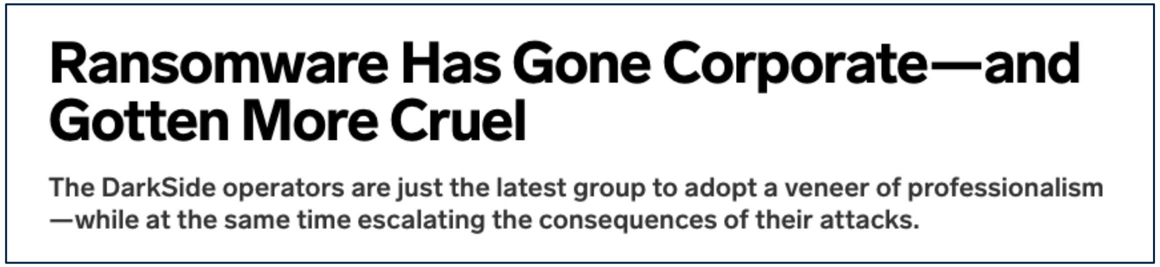


NEWS

Verizon DBIR shows sharp increase in ransomware attacks

According to Verizon's latest Data Breach Investigations Report, 60% of ransomware cases involved either direct installation or installation via desktop sharing software.

Alexander Culafi, News Writer

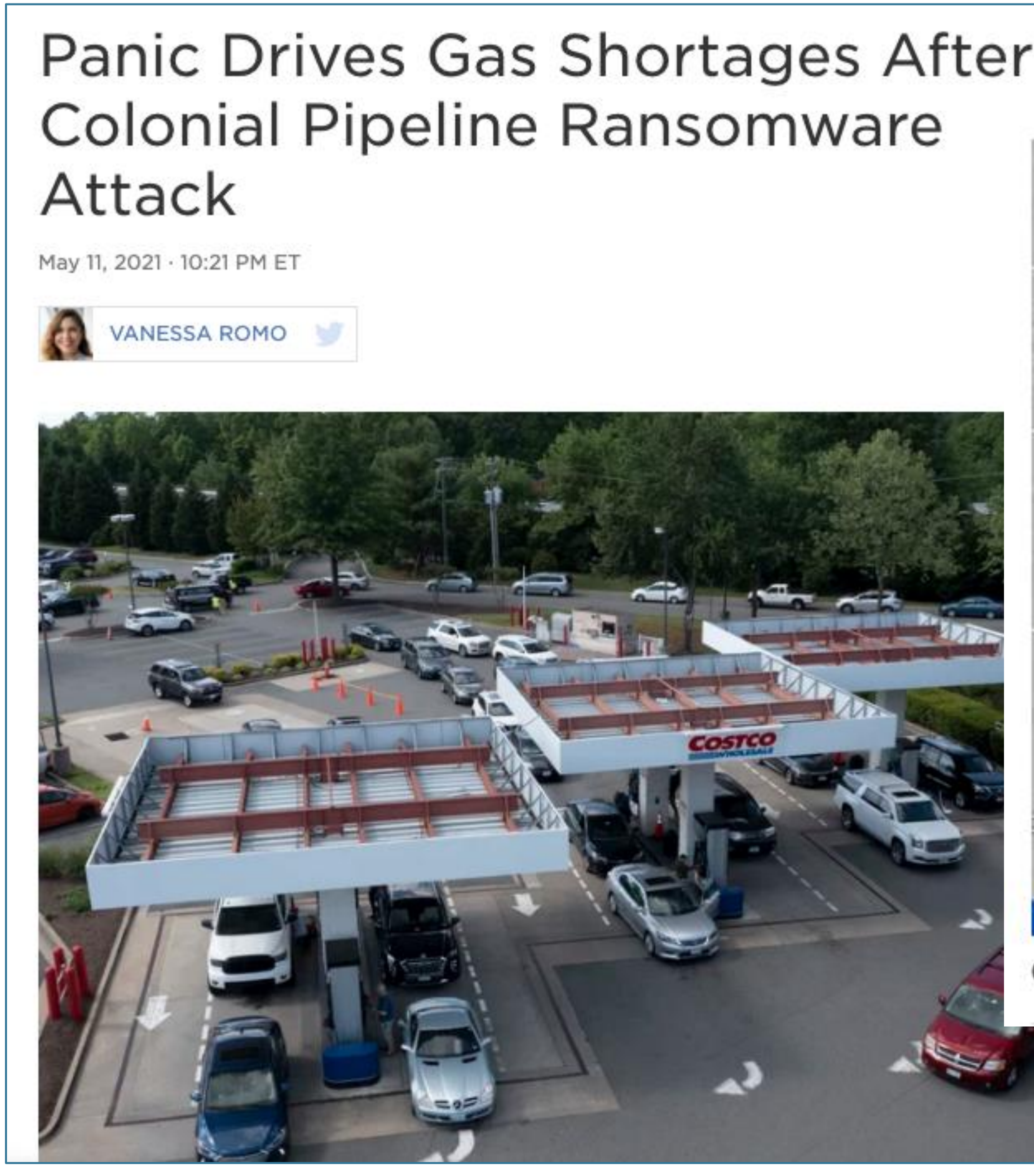


Ransomware Has Gone Corporate—and Gotten More Cruel

The DarkSide operators are just the latest group to adopt a veneer of professionalism —while at the same time escalating the consequences of their attacks.

erizon-DBIR-shows-sharp-increase-in-ransomware-attacks

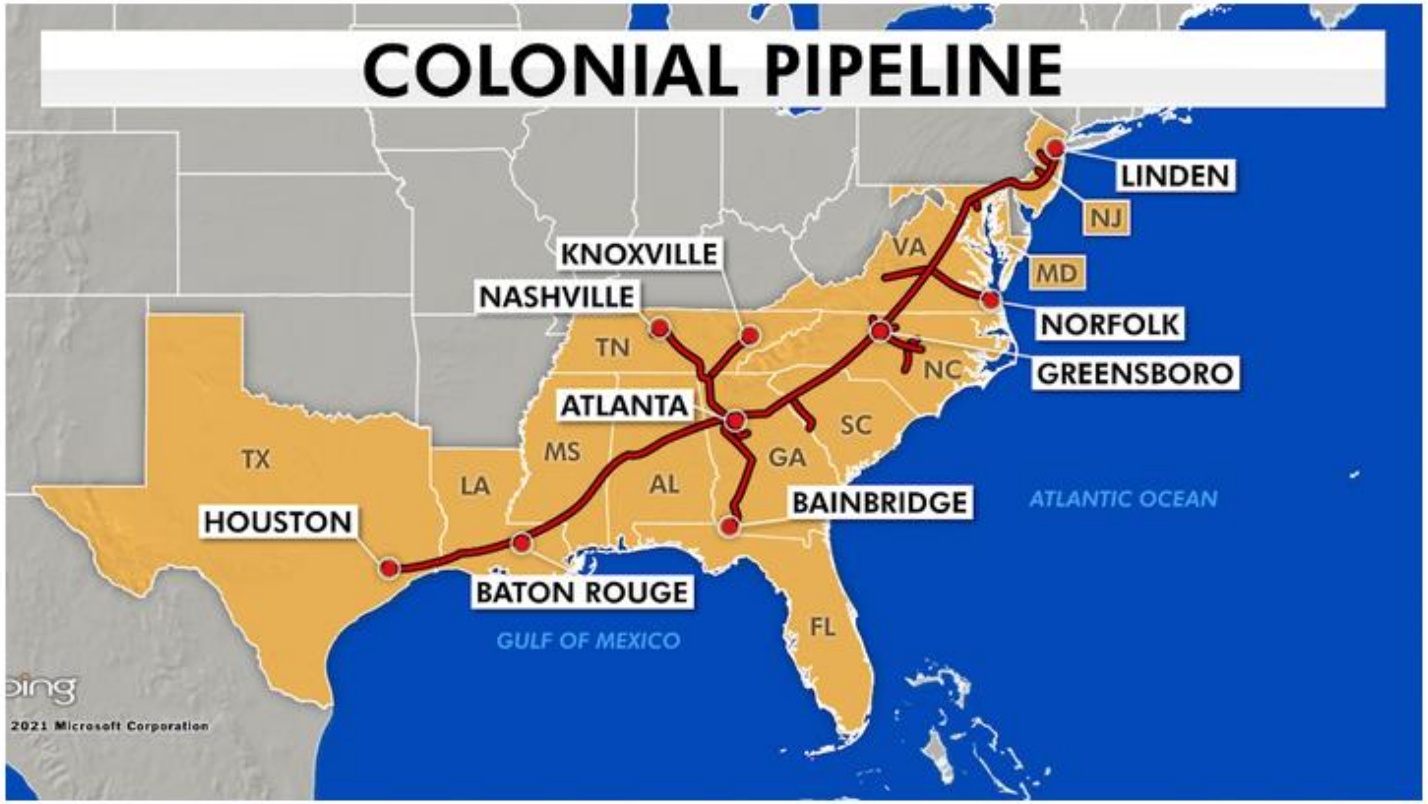
Colonial Pipeline Attack



Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack

May 11, 2021 · 10:21 PM ET

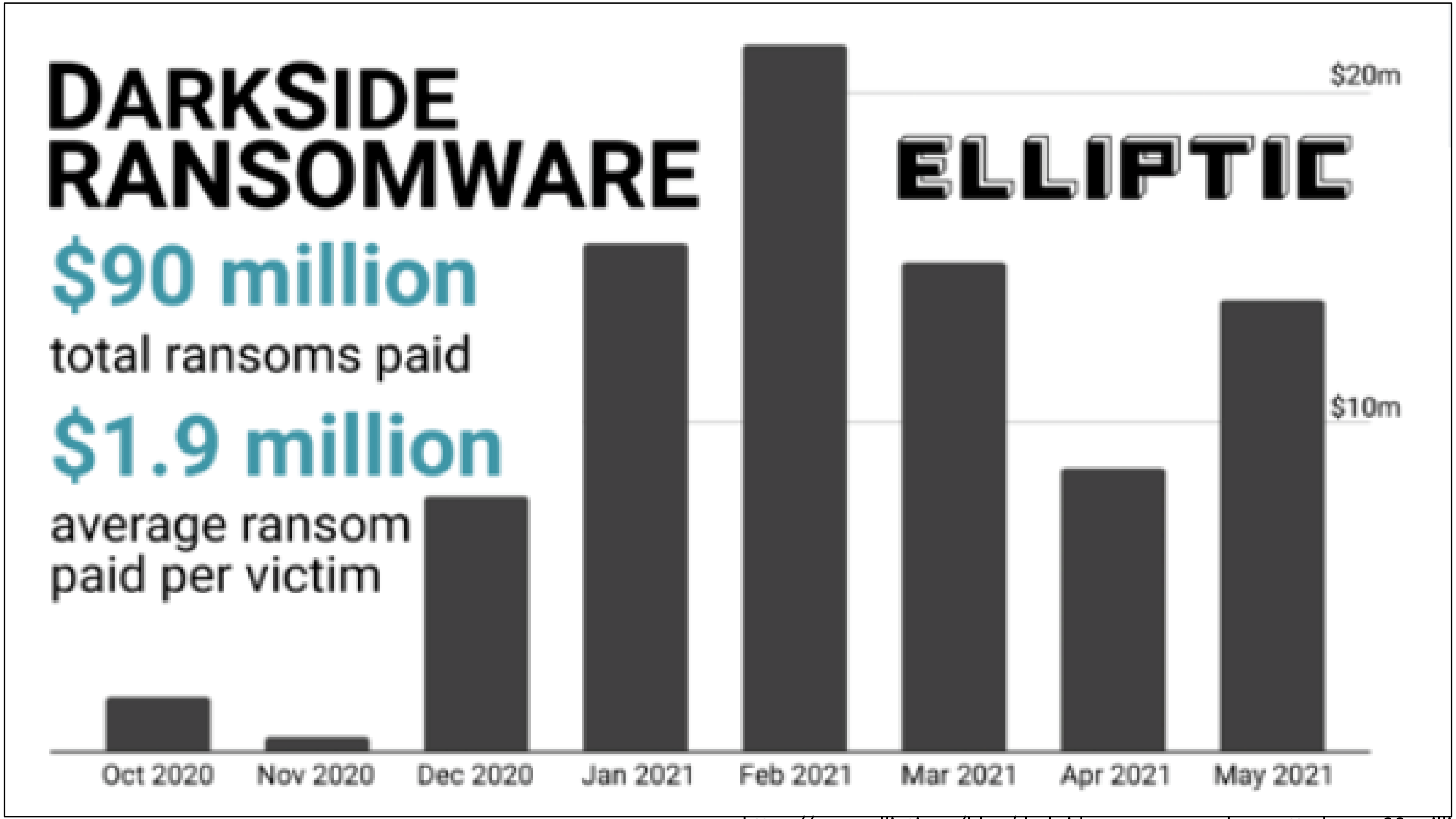
VANESSA ROMO



Colonial Pipeline stretches along the East Coast. (Fox News)

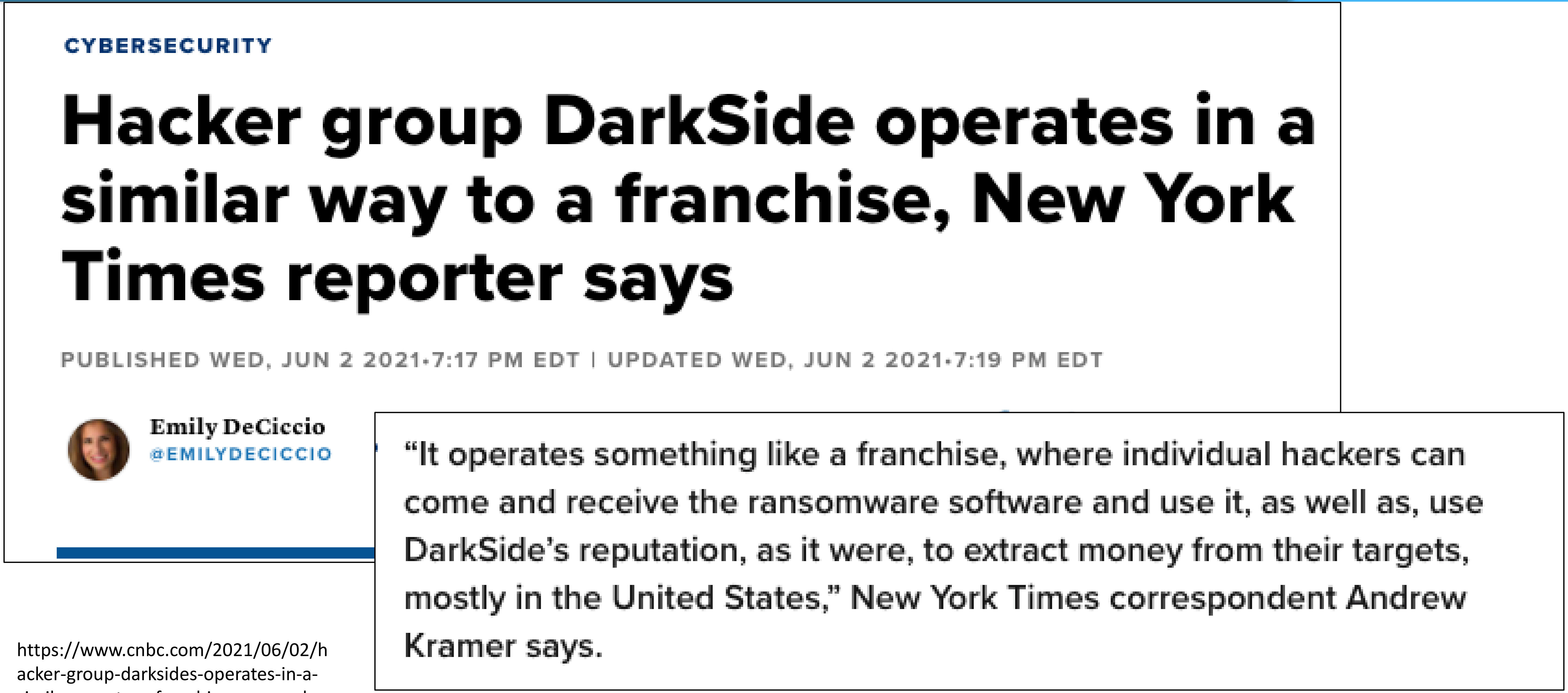
ess.com/energy/colonial-pipeline-shutdown

Who Were the Hackers?



https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin

Ransomware as a Franchise



CYBERSECURITY

Hacker group DarkSide operates in a similar way to a franchise, New York Times reporter says

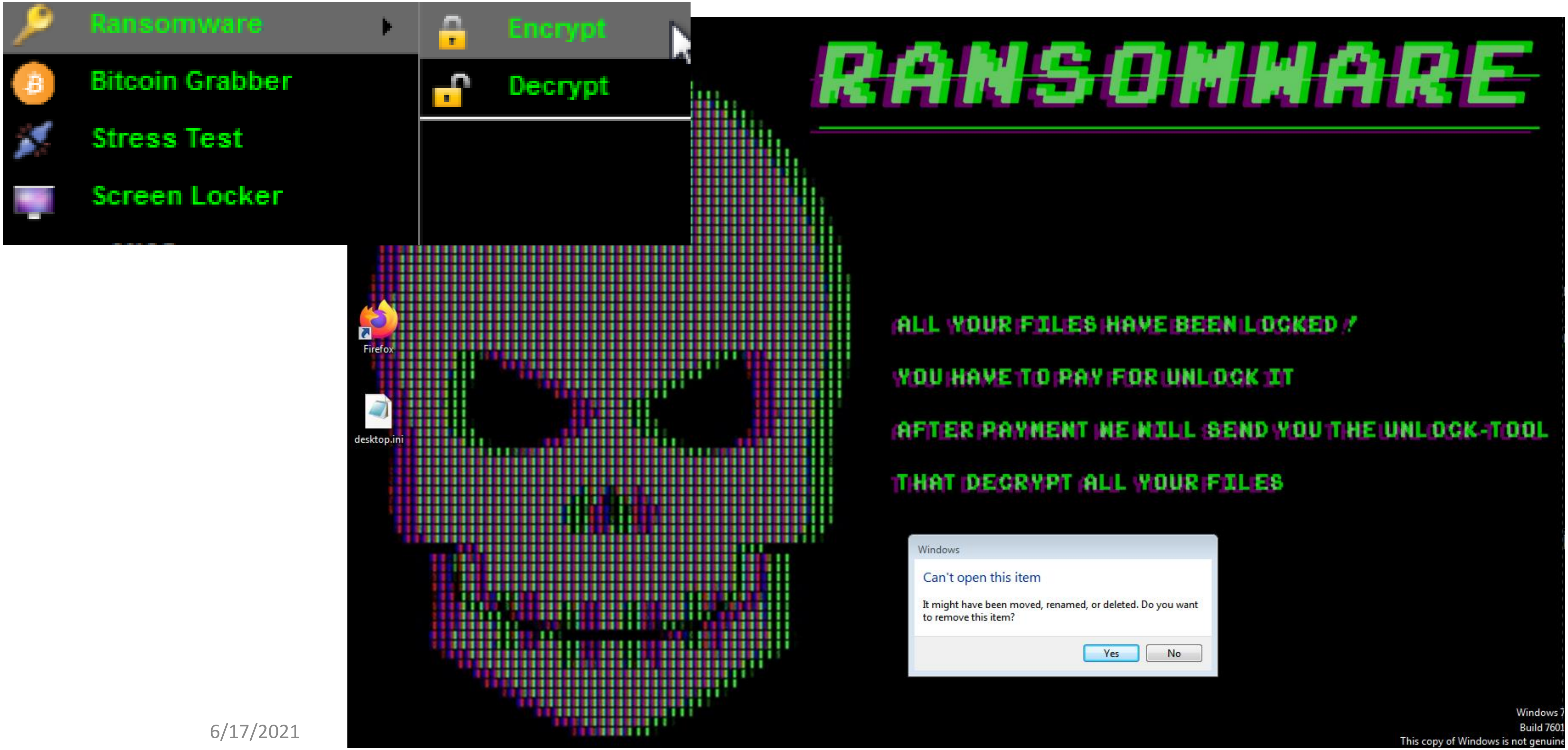
PUBLISHED WED, JUN 2 2021•7:17 PM EDT | UPDATED WED, JUN 2 2021•7:19 PM EDT

Emily DeCiccio
@EMILYDECICCIO

"It operates something like a franchise, where individual hackers can come and receive the ransomware software and use it, as well as, use DarkSide's reputation, as it were, to extract money from their targets, mostly in the United States," New York Times correspondent Andrew Kramer says.

https://www.cnbc.com/2021/06/02/hacker-group-darksides-operates-in-a-similar-way-to-a-franchise-new-york-times-reporter-says.html

Point-and-Click Ransomware



ALL YOUR FILES HAVE BEEN LOCKED !

YOU HAVE TO PAY FOR UNLOCK IT

AFTER PAYMENT WE WILL SEND YOU THE UNLOCK-TOOL

THAT DECRYPT ALL YOUR FILES

Windows

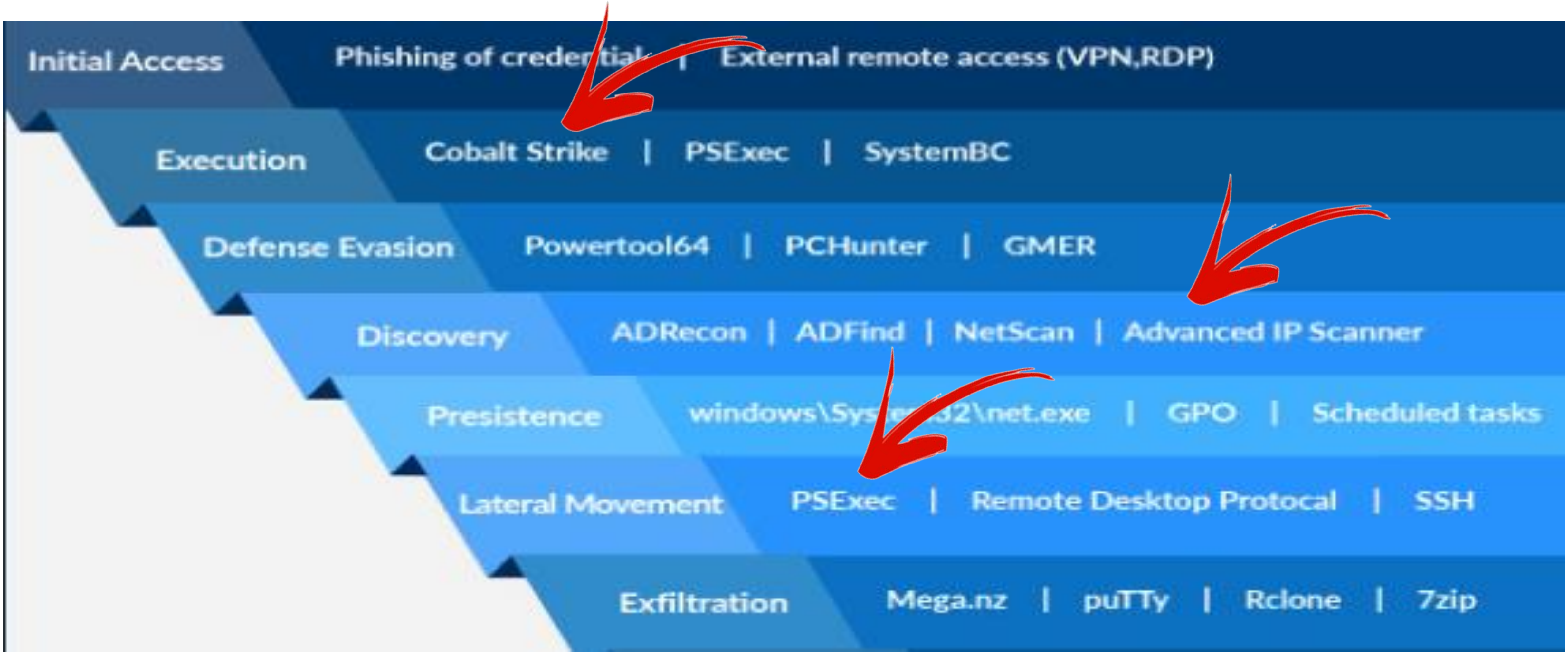
Can't open this item

It might have been moved, renamed, or deleted. Do you want to remove this item?

Yes No

Windows 7
Build 7601
This copy of Windows is not genuine

Darkside’s Methodology



Initial Access	Phishing of credentials | External remote access (VPN,RDP)
Execution	Cobalt Strike | PSExec | SystemBC
Defense Evasion	Powertool64 | PCHunter | GMER
Discovery	ADRecon | ADFind | NetScan | Advanced IP Scanner
Presistence	windows\System32\net.exe | GPO | Scheduled tasks
Lateral Movement	PSExec | Remote Desktop Protocal | SSH
Exfiltration	Mega.nz | puTTy | Rclone | 7zip

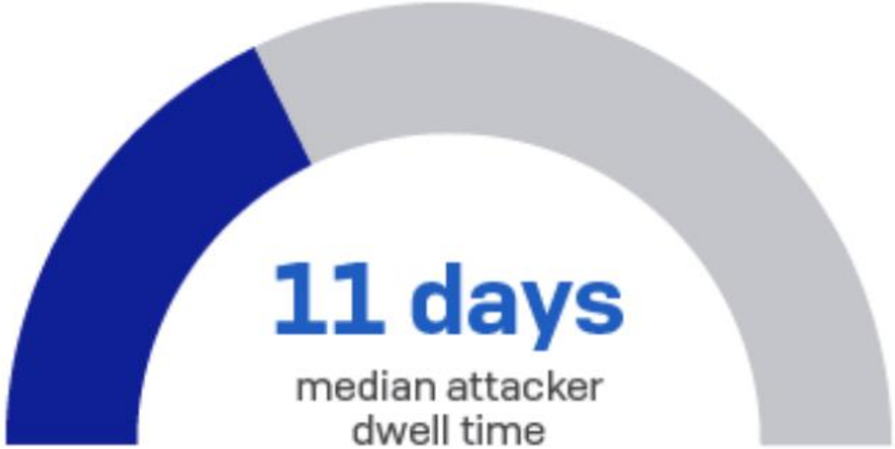
https://twitter.com/cyberwarfarelab/status/1393961644657569797/photo/1

Legitimate Tools, Criminal Use

“Nearly 60% of PowerShell exploits employ Cobalt Strike, and some 12% of attacks use a combination of Cobalt Strike and Microsoft Windows tools PowerShell and PsExec.”

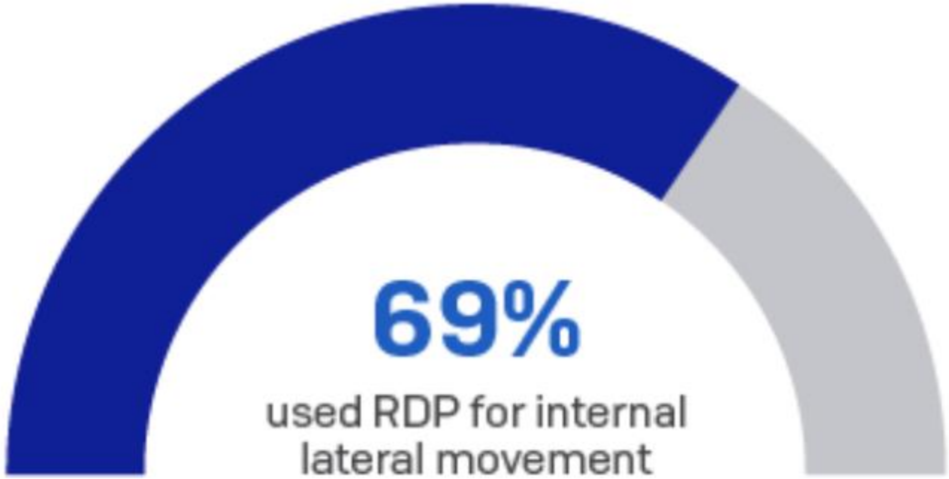
https://www.darkreading.com/attacks-breaches/cobalt-strike-becomes-a-preferred-hacking-tool-by-cybercrime-apt-groups/d/d-id/1341073

The Attackers Lurk…



11 days

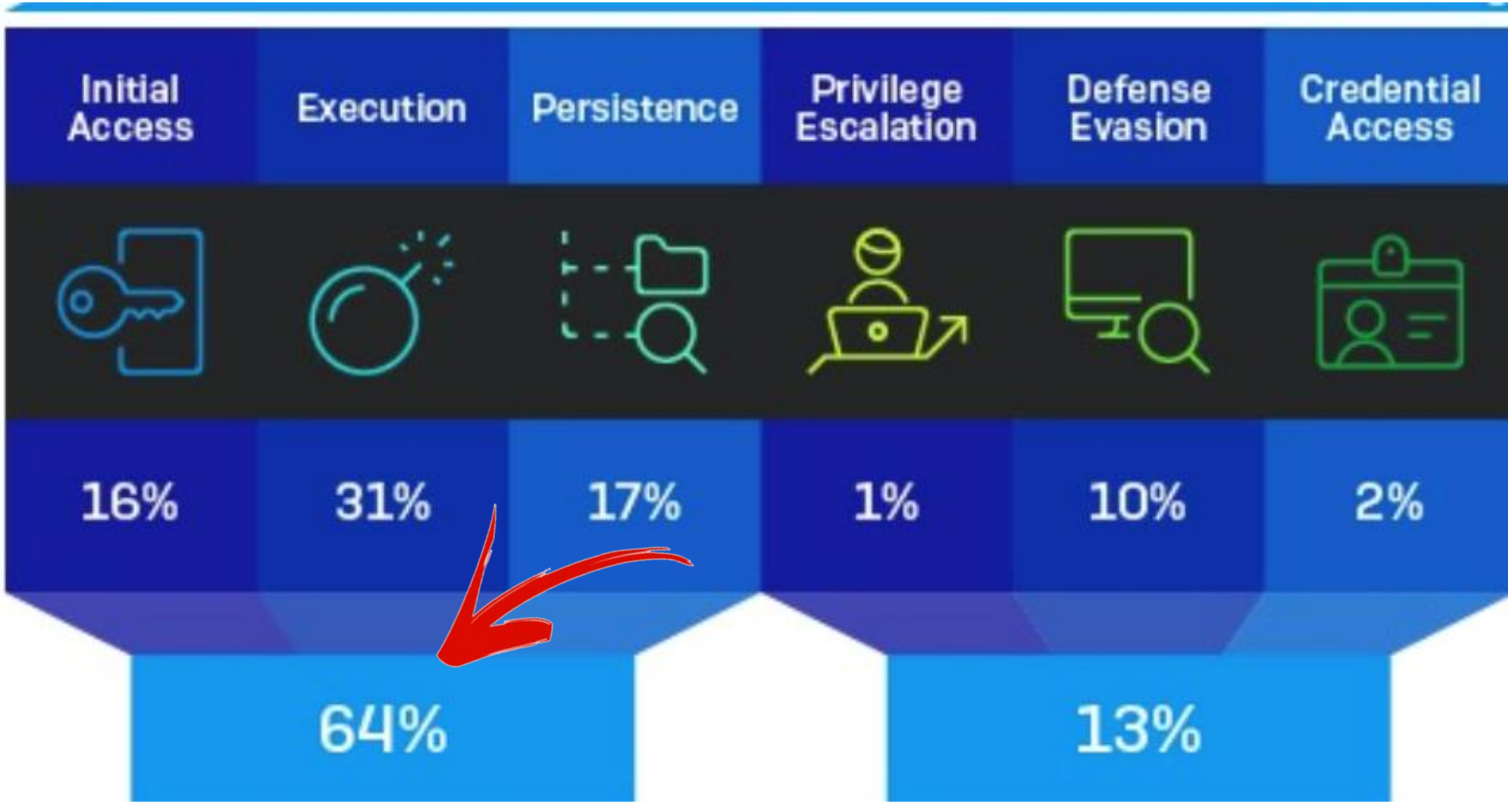
median attacker dwell time



69%

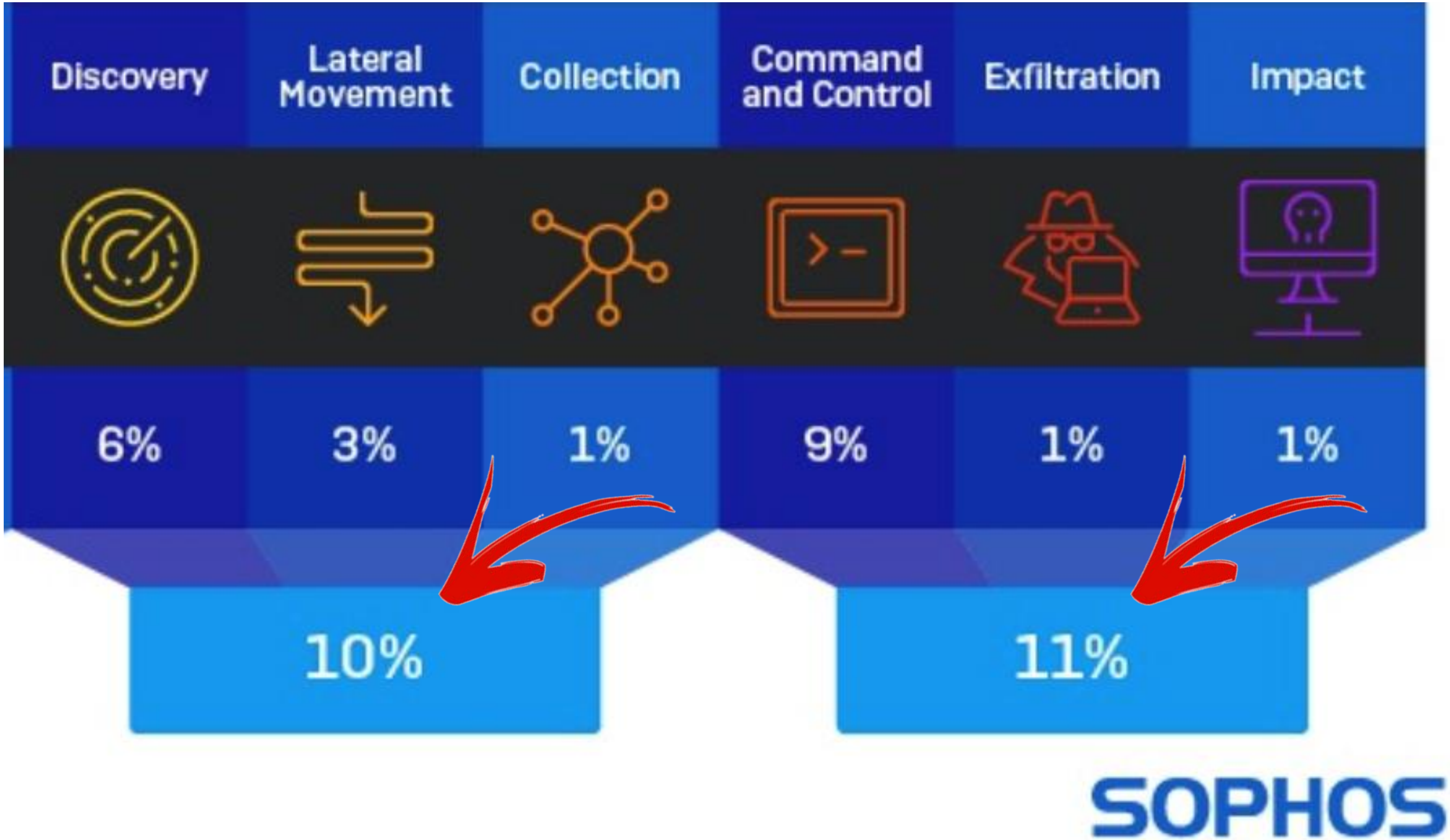
used RDP for internal lateral movement

What are the Attackers Doing?



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
16%	31%	17%	1%	10%	2%
64%			13%		

What are the Attackers Doing?



Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
6%	3%	1%	9%	1%	1%

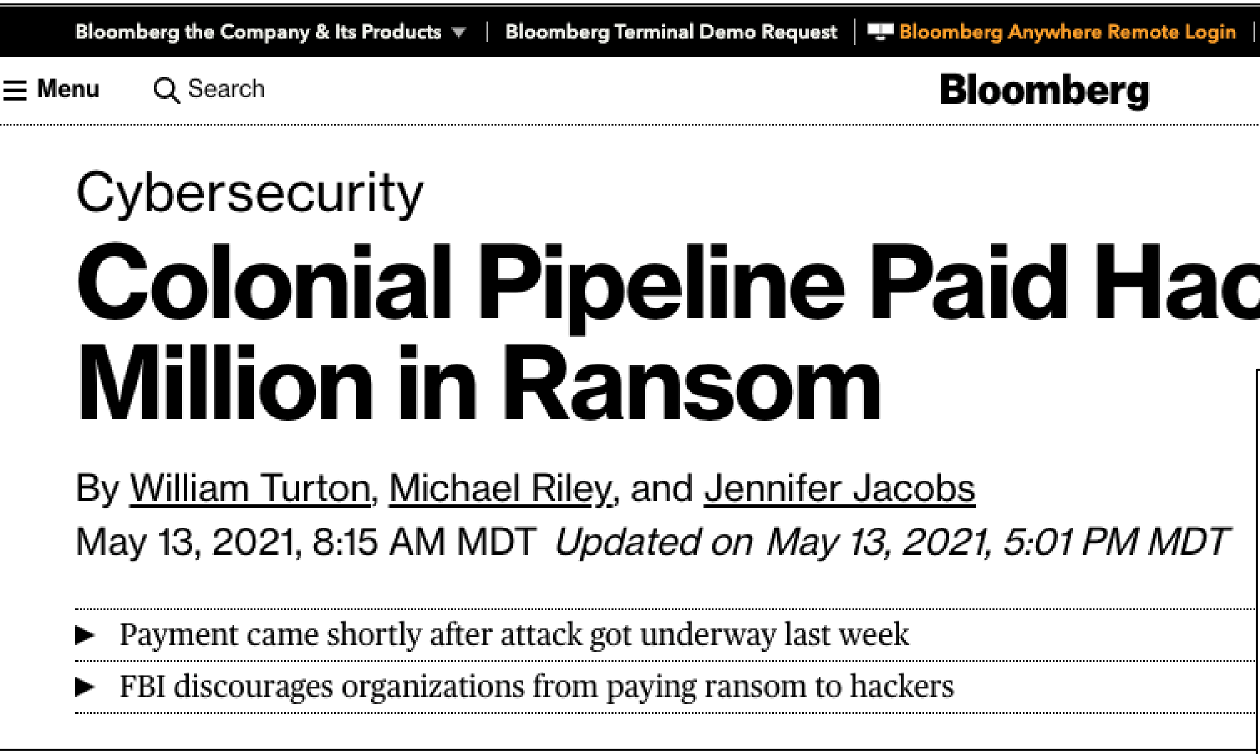
10%

11%

Threat Hunting

- Proactive, human-driven
- Specialized tools
- Search for subtle indicators of compromise
- Find and eradicate persistent threats
- Prevent repeat ransomware infections

Colonial Pipeline Paid the Ransom



Bloomberg the Company & Its Products ▾ | Bloomberg Terminal Demo Request | Bloomberg Anywhere Remote Login | Bloomberg Customer Support
☰ Menu
Search
Bloomberg
Sign In

Cybersecurity

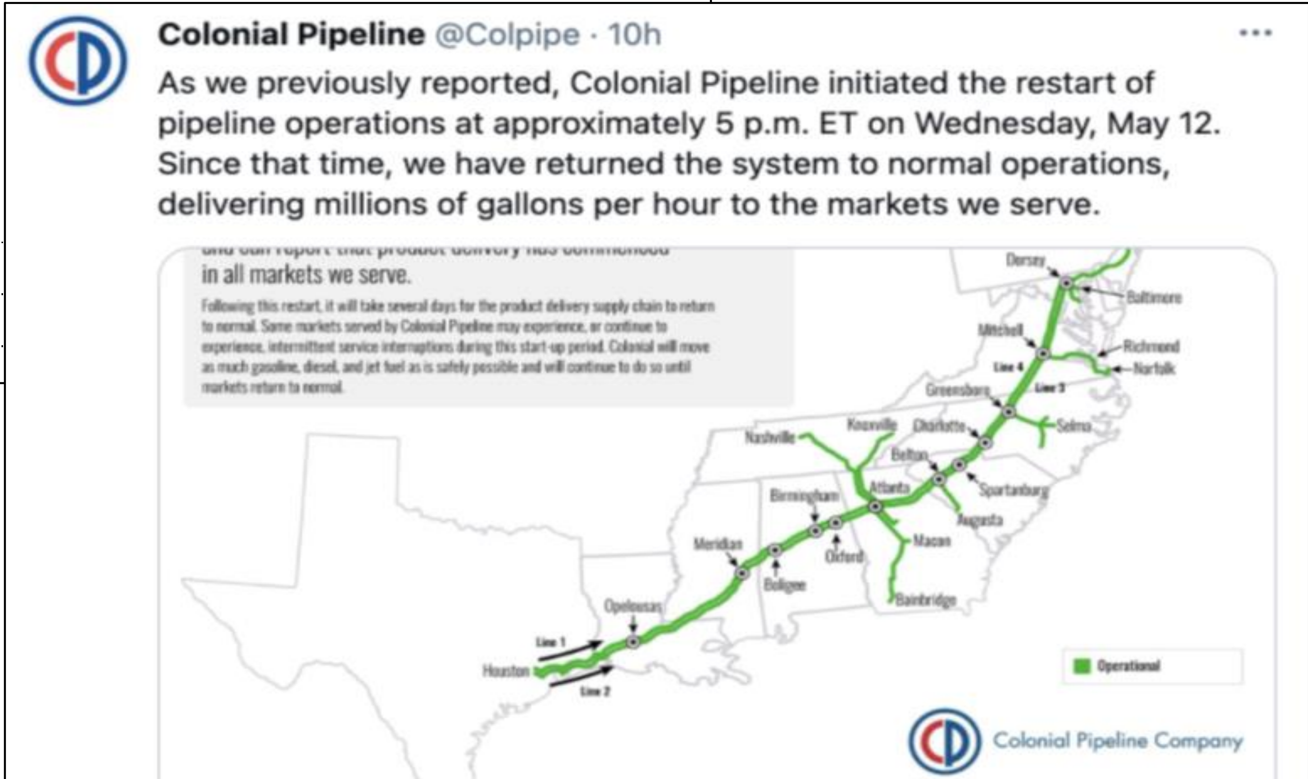
Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom

By William Turton, Michael Riley, and Jennifer Jacobs

May 13, 2021, 8:15 AM MDT *Updated on May 13, 2021, 5:01 PM MDT*

- Payment came shortly after attack got underway last week
- FBI discourages organizations from paying ransom to hackers

https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom



Colonial Pipeline @Colpipe · 10h

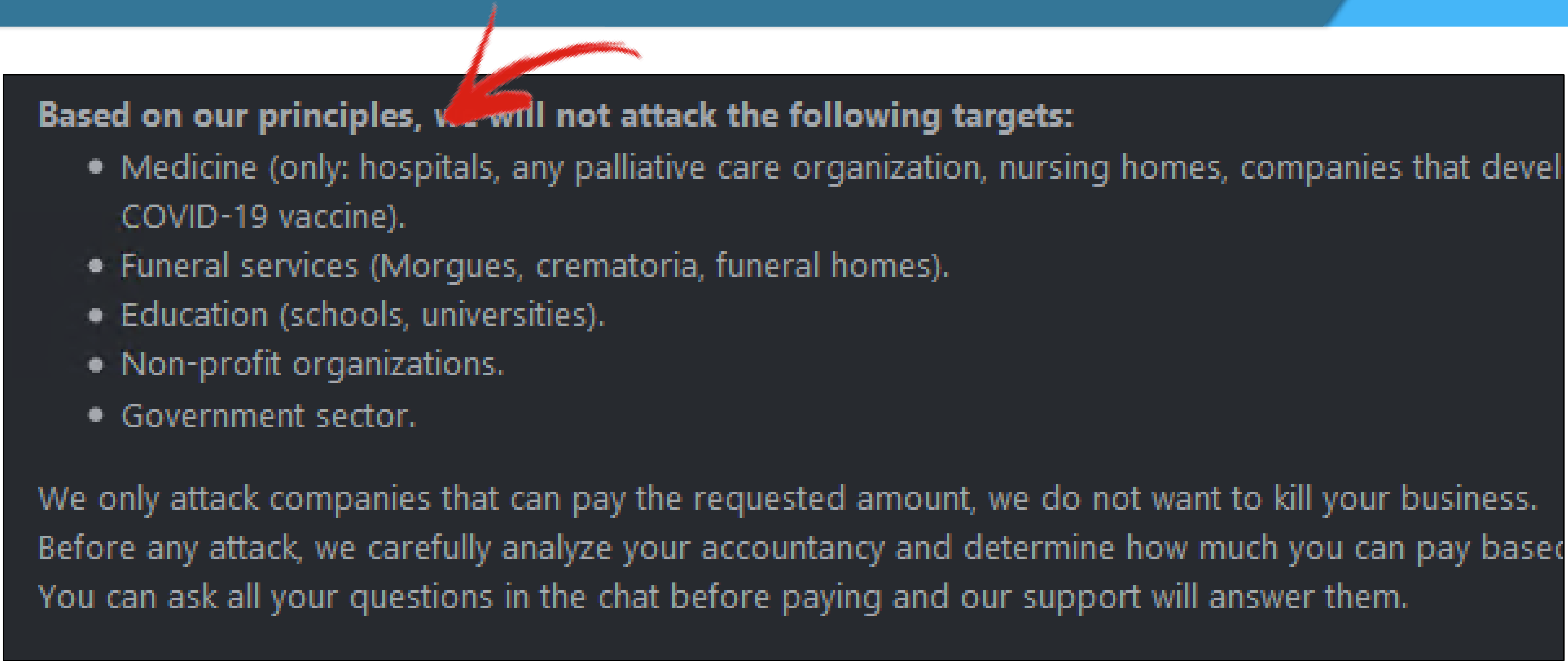
As we previously reported, Colonial Pipeline initiated the restart of pipeline operations at approximately 5 p.m. ET on Wednesday, May 12. Since that time, we have returned the system to normal operations, delivering millions of gallons per hour to the markets we serve.

and can report that product delivery has commenced in all markets we serve.

Following this restart, it will take several days for the product delivery supply chain to return to normal. Some markets served by Colonial Pipeline may experience, or continue to experience, intermittent service interruptions during this start-up period. Colonial will move as much gasoline, diesel, and jet fuel as is safely possible and will continue to do so until markets return to normal.

https://medium.com/cloud-security/colonial-pipeline-hack-4486d16f2957

Hackers with Morals?



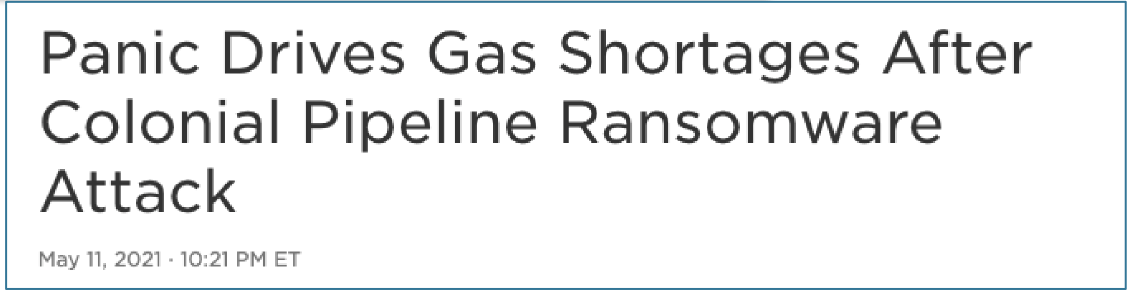
Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that devel COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay basec
You can ask all your questions in the chat before paying and our support will answer them.

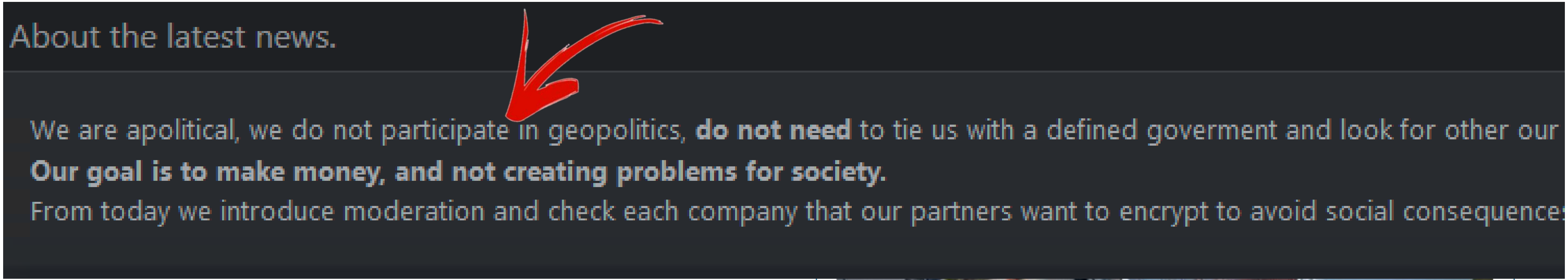
Problems in Paradise

DarkSide Leaks



Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack

May 11, 2021 · 10:21 PM ET



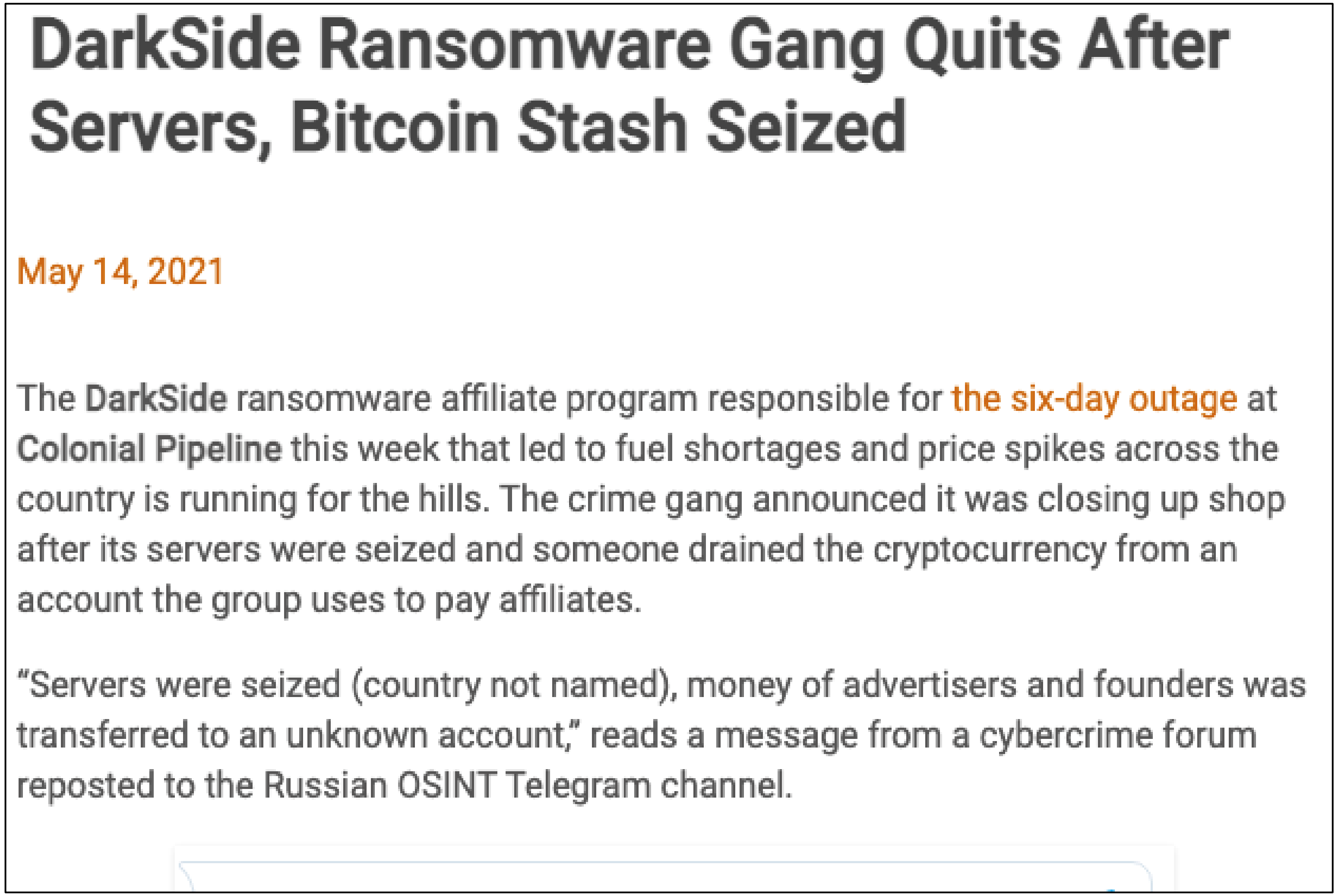
About the latest news.

We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined goverment and look for other our

Our goal is to make money, and not creating problems for society.

From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequence

…Trouble on the Darkside



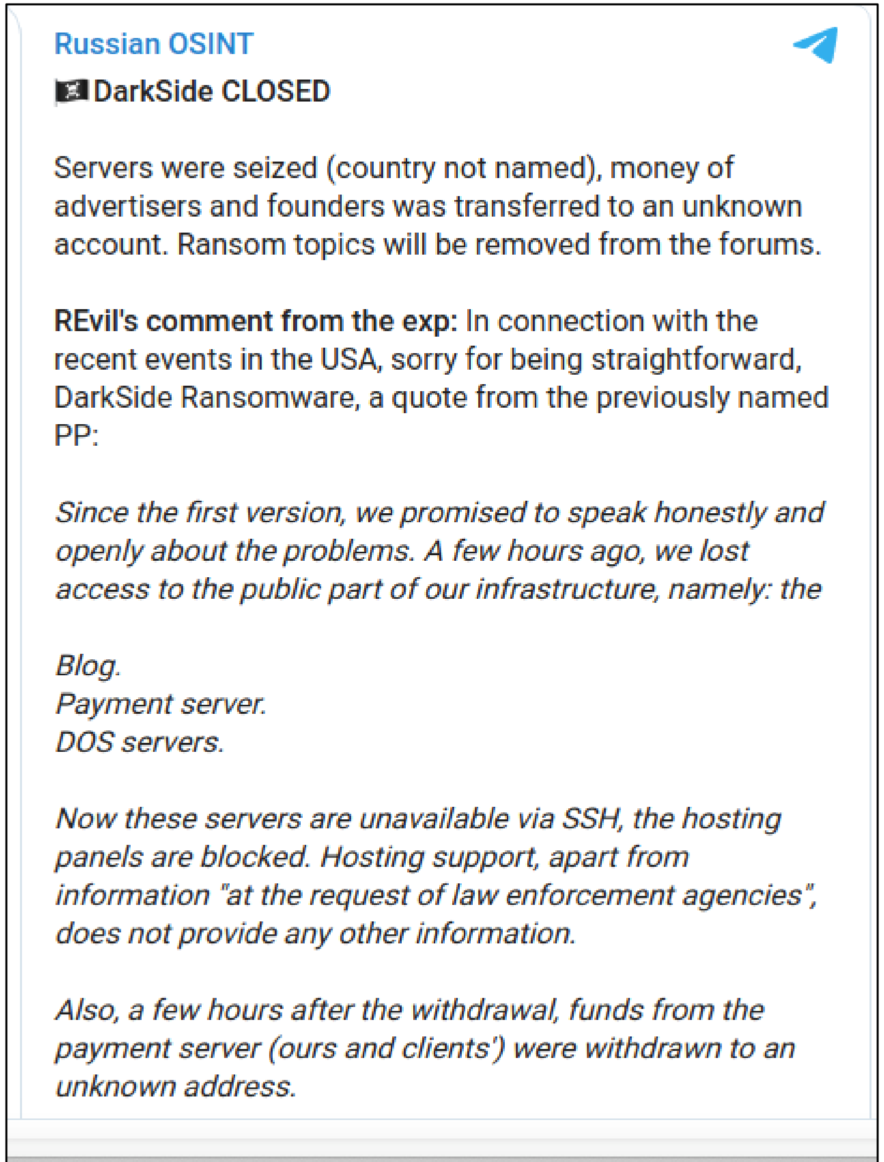
DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized

May 14, 2021

The **DarkSide** ransomware affiliate program responsible for the six-day outage at **Colonial Pipeline** this week that led to fuel shortages and price spikes across the country is running for the hills. The crime gang announced it was closing up shop after its servers were seized and someone drained the cryptocurrency from an account the group uses to pay affiliates.

"Servers were seized (country not named), money of advertisers and founders was transferred to an unknown account," reads a message from a cybercrime forum reposted to the Russian OSINT Telegram channel.

https://krebsonsecurity.com/2021/05/darkside-ransomware-gang-quits-after-servers-bitcoin-stash-seized/



Russian OSINT

🏴‍☠️DarkSide CLOSED

Servers were seized (country not named), money of advertisers and founders was transferred to an unknown account. Ransom topics will be removed from the forums.

REvil's comment from the exp: In connection with the recent events in the USA, sorry for being straightforward, DarkSide Ransomware, a quote from the previously named PP:

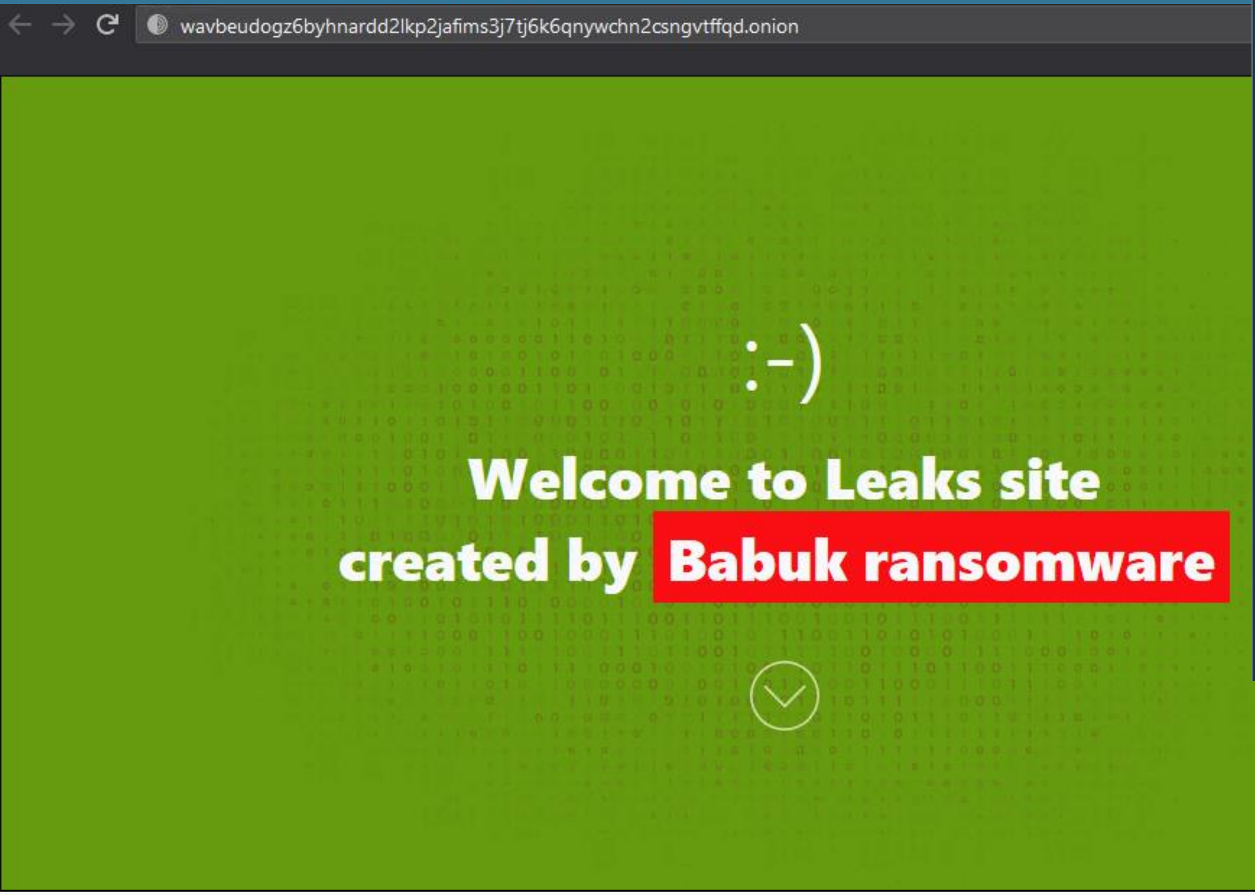
Since the first version, we promised to speak honestly and openly about the problems. A few hours ago, we lost access to the public part of our infrastructure, namely: the

Blog.
Payment server.
DOS servers.

Now these servers are unavailable via SSH, the hosting panels are blocked. Hosting support, apart from information "at the request of law enforcement agencies", does not provide any other information.

Also, a few hours after the withdrawal, funds from the payment server (ours and clients') were withdrawn to an unknown address.

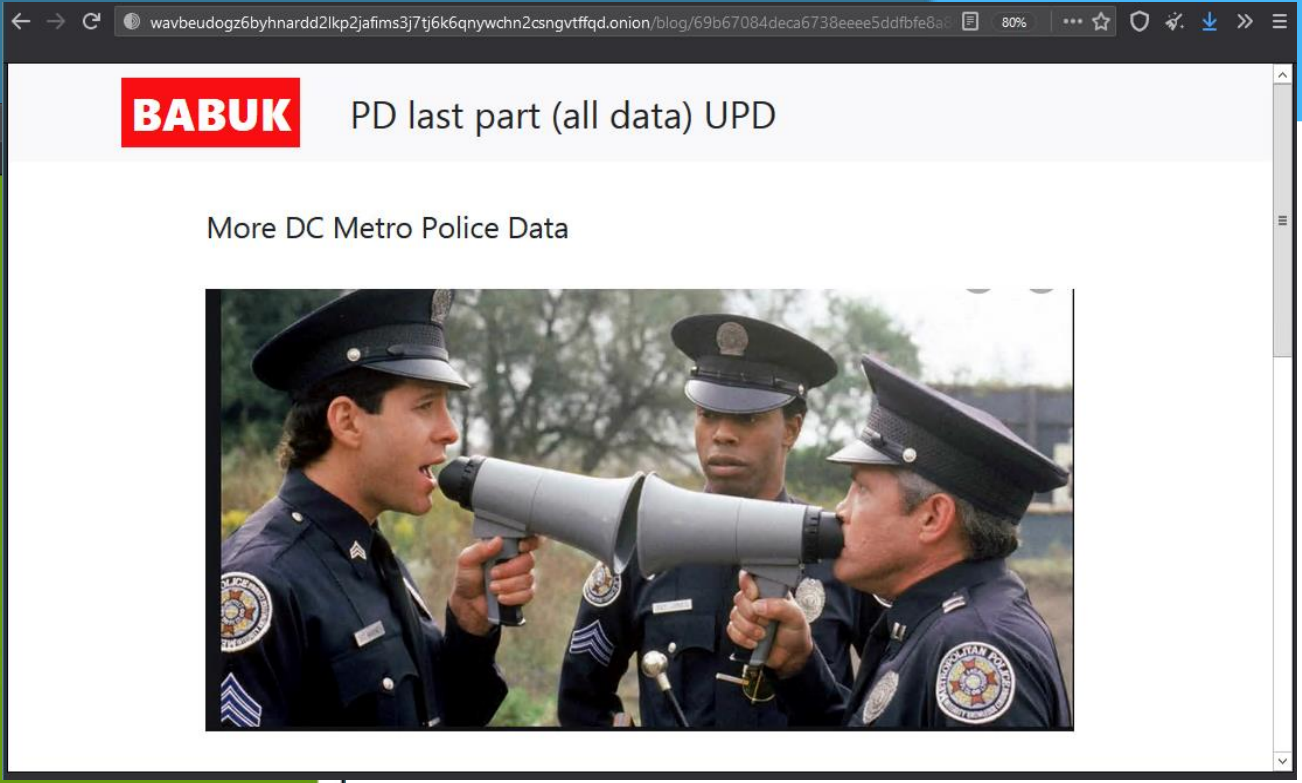
Criminals Overreach…



wavbeudogz6byhnardd2lkp2jafims3j7tj6k6qnywchn2csngvtffqd.onion

:-)

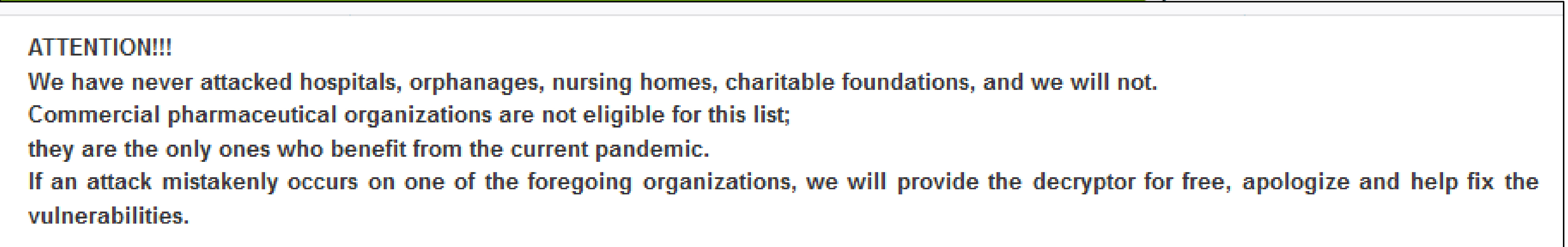
Welcome to Leaks site created by Babuk ransomware



wavbeudogz6byhnardd2lkp2jafims3j7tj6k6qnywchn2csngvtffqd.onion/blog/69b67084deca6738eeee5ddfbfe8a

BABUK PD last part (all data) UPD

More DC Metro Police Data



ATTENTION!!!

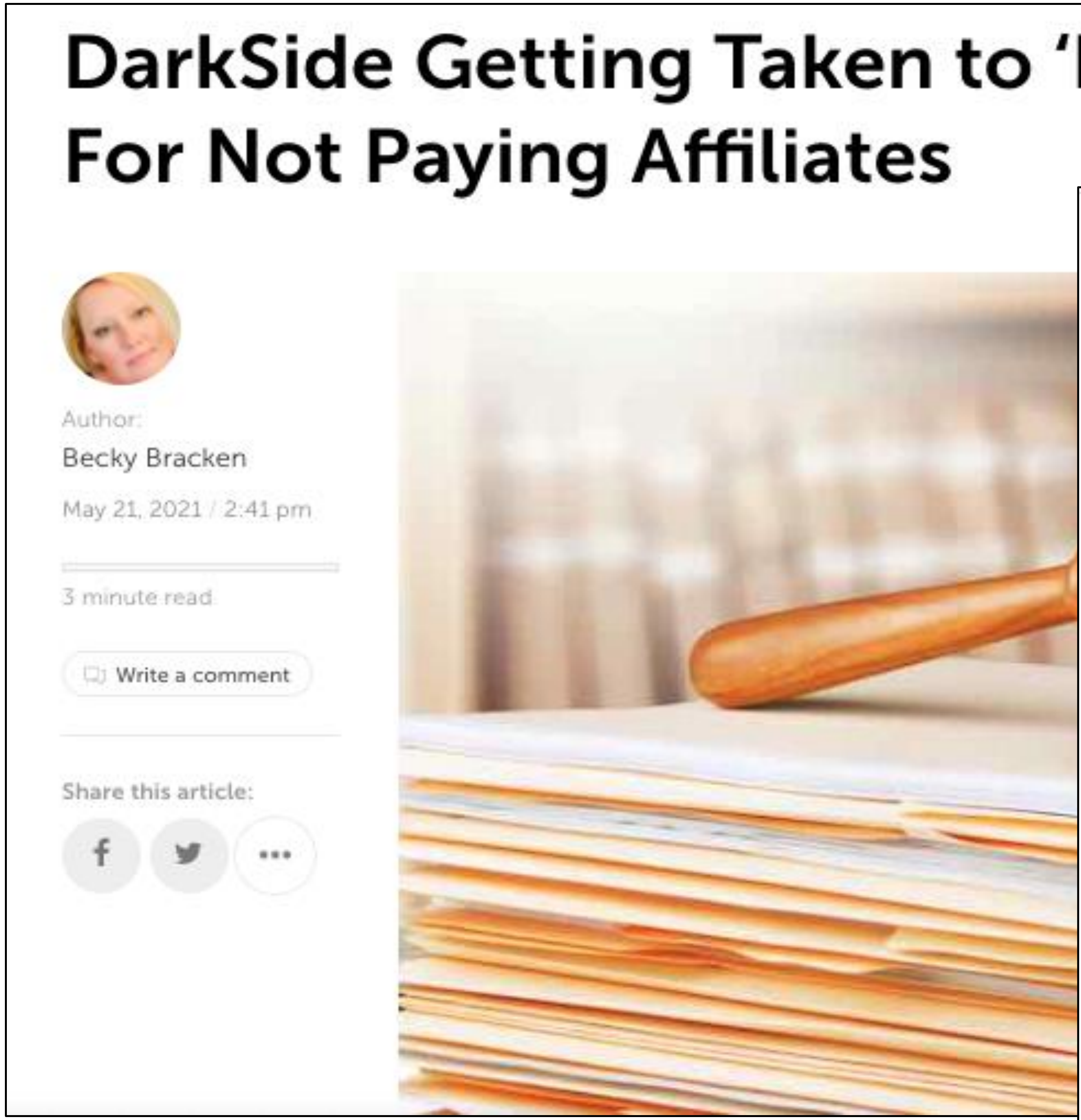
We have never attacked hospitals, orphanages, nursing homes, charitable foundations, and we will not.

Commercial pharmaceutical organizations are not eligible for this list;

they are the only ones who benefit from the current pandemic.

If an attack mistakenly occurs on one of the foregoing organizations, we will provide the decryptor for free, apologize and help fix the vulnerabilities.

Darkside On Trial



DarkSide Getting Taken to 'Hackers' Court' For Not Paying Affiliates

Author:
Becky Bracken

May 21, 2021 / 2:41 pm

3 minute read

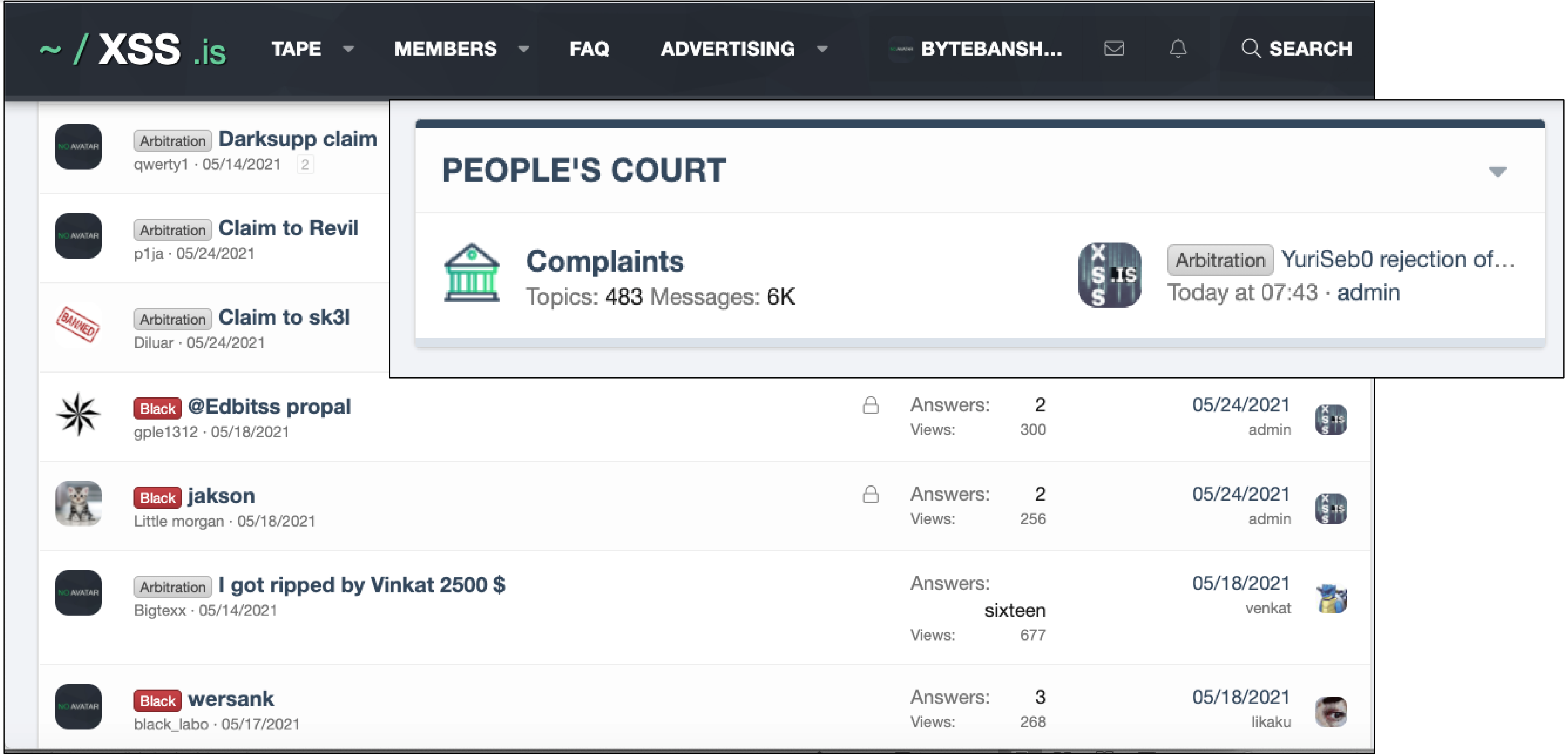
DarkSide partners demand their promised share of the ransoms

13:54 / May 21, 2021

The partners have made a claim for bitcoins stored on a hacker forum.

https://threatpost.com/darkside-hackers-court-paying-affiliates/166393/

XSS.is: The Russian Hacker Court



Arbitration Darksupp claim
qwerty1 · 05/14/2021 2

Arbitration Claim to Revil
p1ja · 05/24/2021

Arbitration Claim to sk3l
Diluar · 05/24/2021

PEOPLE'S COURT

Complaints
Topics: 483 Messages: 6K

Arbitration YuriSeb0 rejection of...
Today at 07:43 · admin

Black @Edbitss propal
gple1312 · 05/18/2021
Answers: 2
Views: 300
05/24/2021
admin

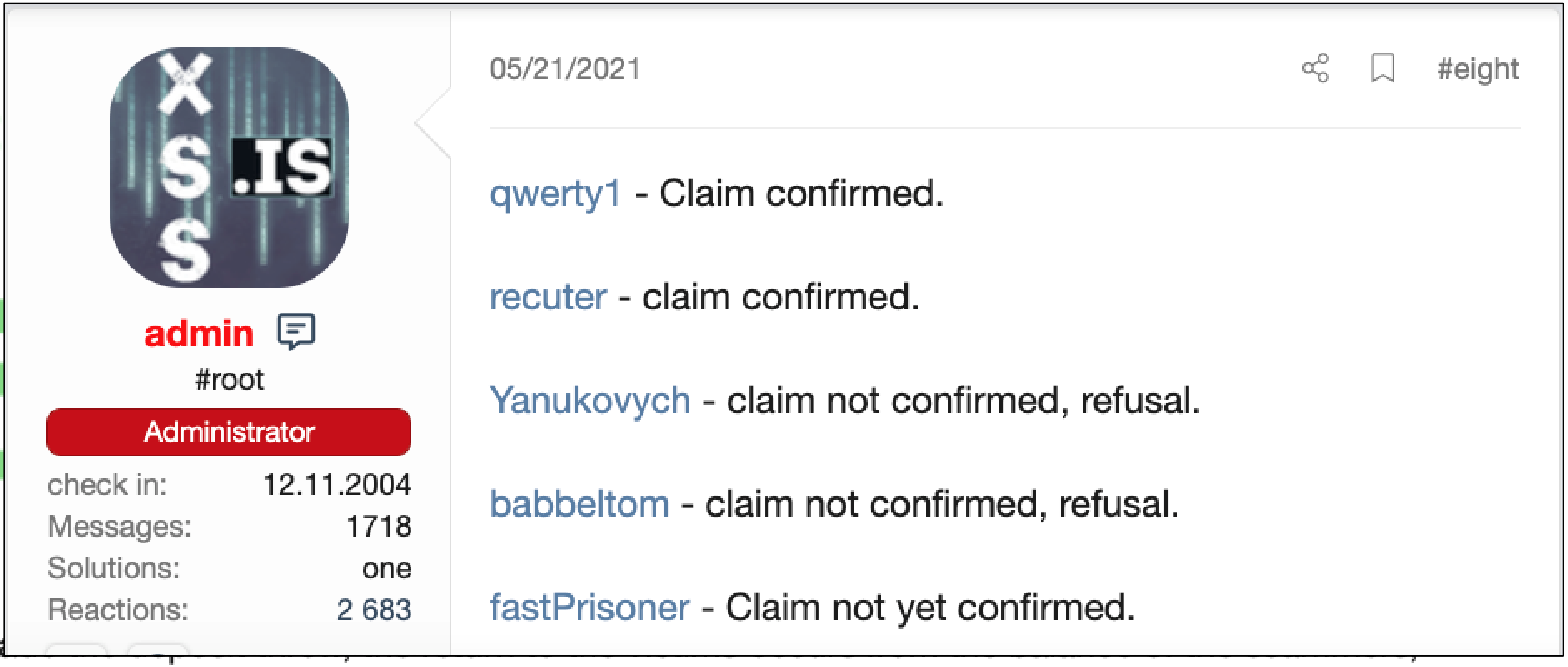
Black jakson
Little morgan · 05/18/2021
Answers: 2
Views: 256
05/24/2021
admin

Arbitration I got ripped by Vinkat 2500 $
Bigtexx · 05/14/2021
Answers: sixteen
Views: 677
05/18/2021
venkat

Black wersank
black_labo · 05/17/2021
Answers: 3
Views: 268
05/18/2021
likaku

Escrow Rules for XSS.is

Deposit HERE . Depositing and withdrawing a deposit is automated.



05/21/2021

#eight

admin

#root

Administrator

check in: 12.11.2004
Messages: 1718
Solutions: one
Reactions: 2 683

qwerty1 - Claim confirmed.

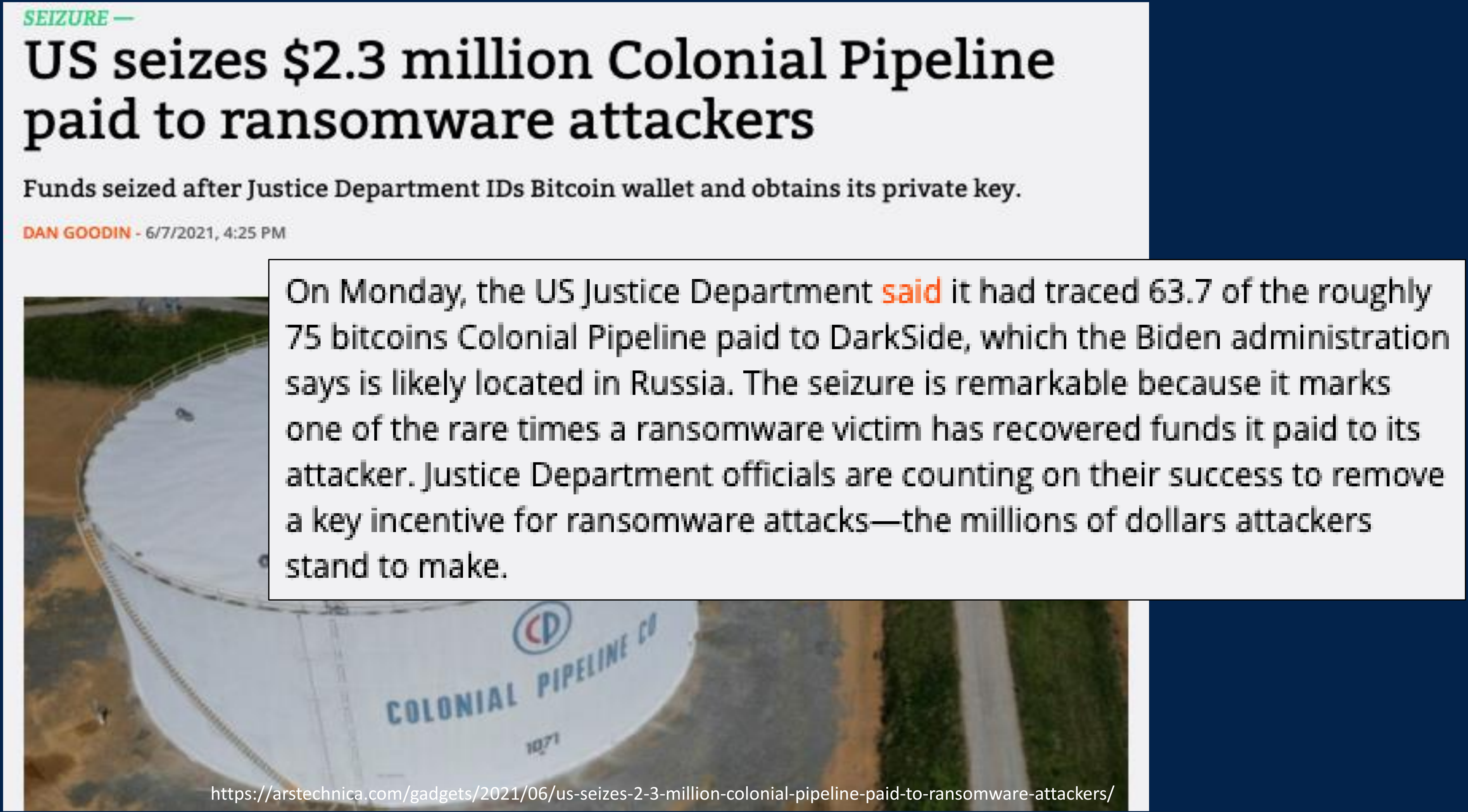
recuter - claim confirmed.

Yanukovych - claim not confirmed, refusal.

babbeltom - claim not confirmed, refusal.

fastPrisoner - Claim not yet confirmed.

- If the user who ma
dividing proportionally between the victims in a% ratio. Consideration of the return process takes place directly in black, within 7 days. Exclusively the administrator (arbitrator) deals with the consideration and payment;



SEIZURE —

US seizes $2.3 million Colonial Pipeline paid to ransomware attackers

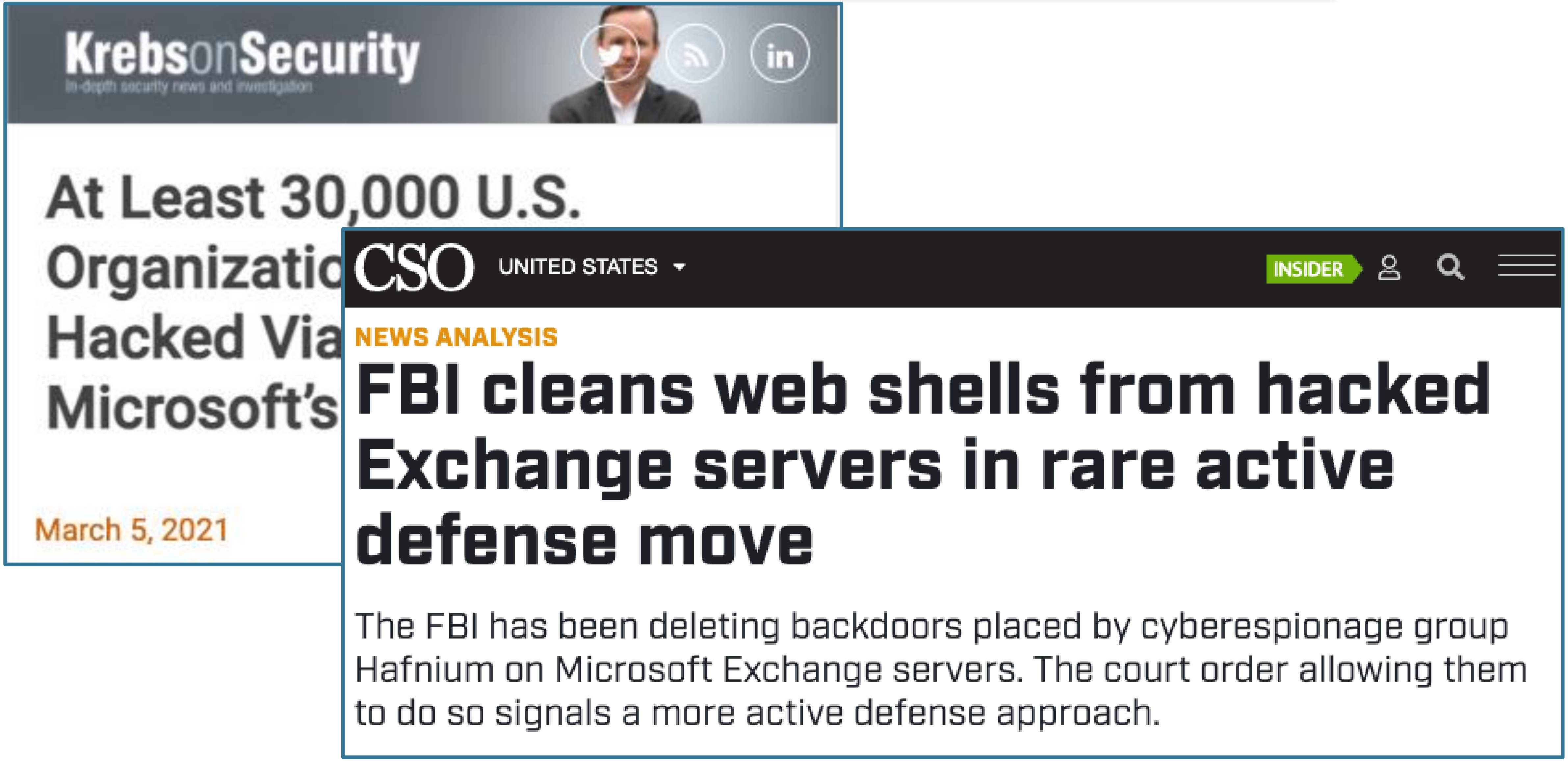
Funds seized after Justice Department IDs Bitcoin wallet and obtains its private key.

DAN GOODIN - 6/7/2021, 4:25 PM

On Monday, the US Justice Department said it had traced 63.7 of the roughly 75 bitcoins Colonial Pipeline paid to DarkSide, which the Biden administration says is likely located in Russia. The seizure is remarkable because it marks one of the rare times a ransomware victim has recovered funds it paid to its attacker. Justice Department officials are counting on their success to remove a key incentive for ransomware attacks—the millions of dollars attackers stand to make.

https://arstechnica.com/gadgets/2021/06/us-seizes-2-3-million-colonial-pipeline-paid-to-ransomware-attackers/

Law Enforcement Intervention



KrebsonSecurity

In-depth security news and investigation

At Least 30,000 U.S. Organizatio Hacked Via Microsoft's

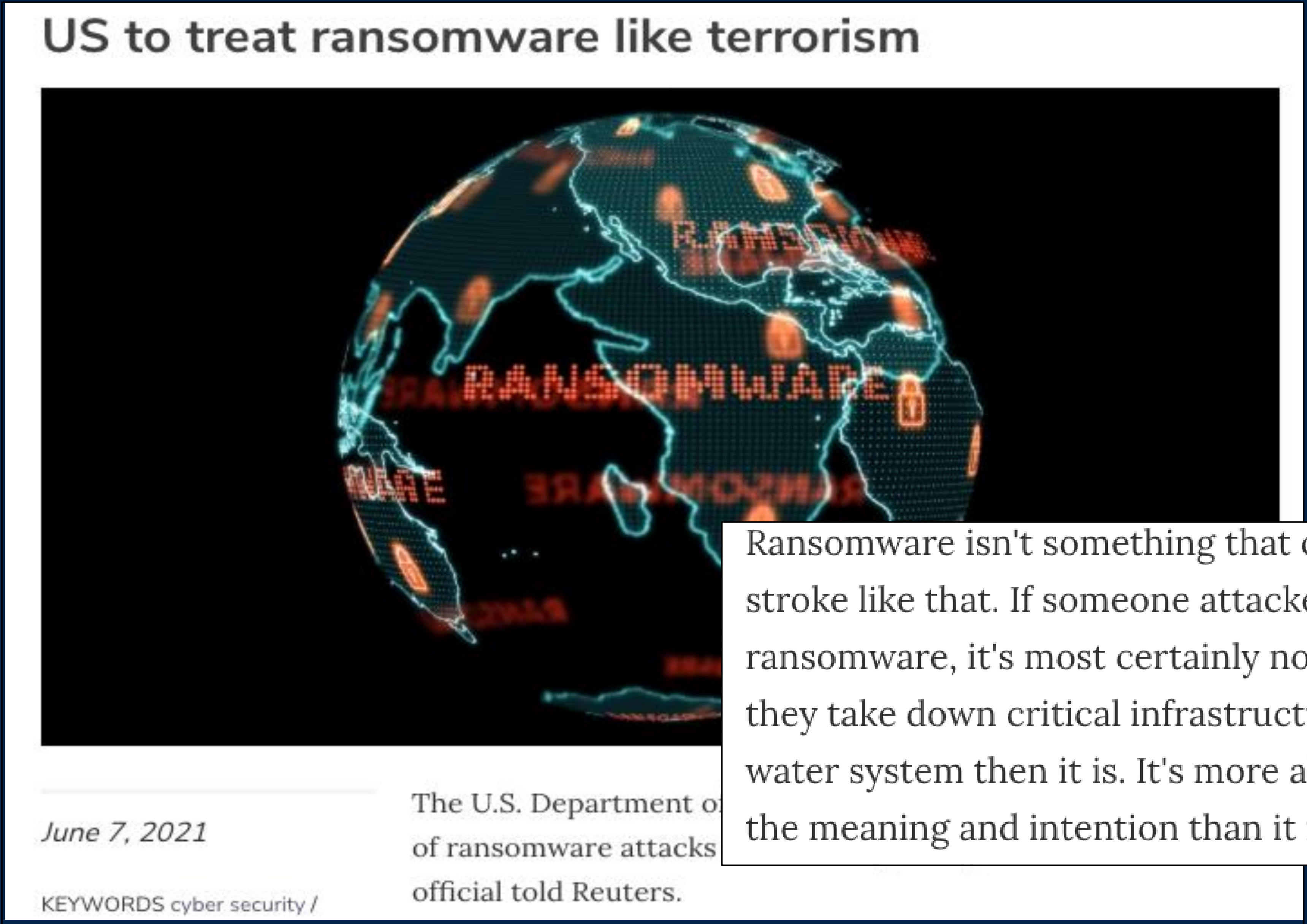
March 5, 2021

CSO UNITED STATES

NEWS ANALYSIS

FBI cleans web shells from hacked Exchange servers in rare active defense move

The FBI has been deleting backdoors placed by cyberespionage group Hafnium on Microsoft Exchange servers. The court order allowing them to do so signals a more active defense approach.



US to treat ransomware like terrorism

June 7, 2021

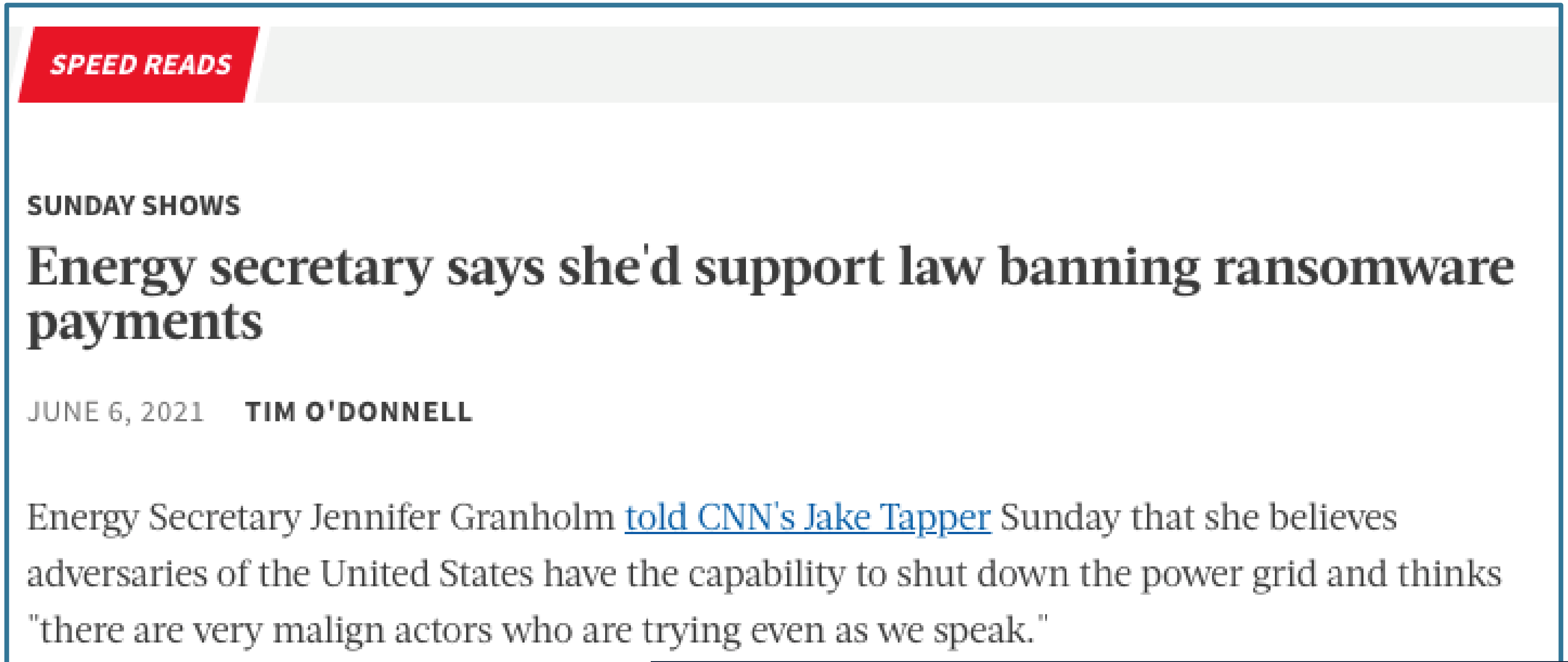
The U.S. Department o
of ransomware attacks
official told Reuters.

KEYWORDS cyber security /

Ransomware isn't something that can be labeled with a broad stroke like that. If someone attacked a small dental office with ransomware, it's most certainly not an act of terrorism. However, if they take down critical infrastructure such as an oil pipeline or water system then it is. It's more about the target of the attack and the meaning and intention than it is about the type of attack.

https://www.securitymagazine.com/articles/95366-us-to-treat-ransomware-like-terrorism

Nuclear Option



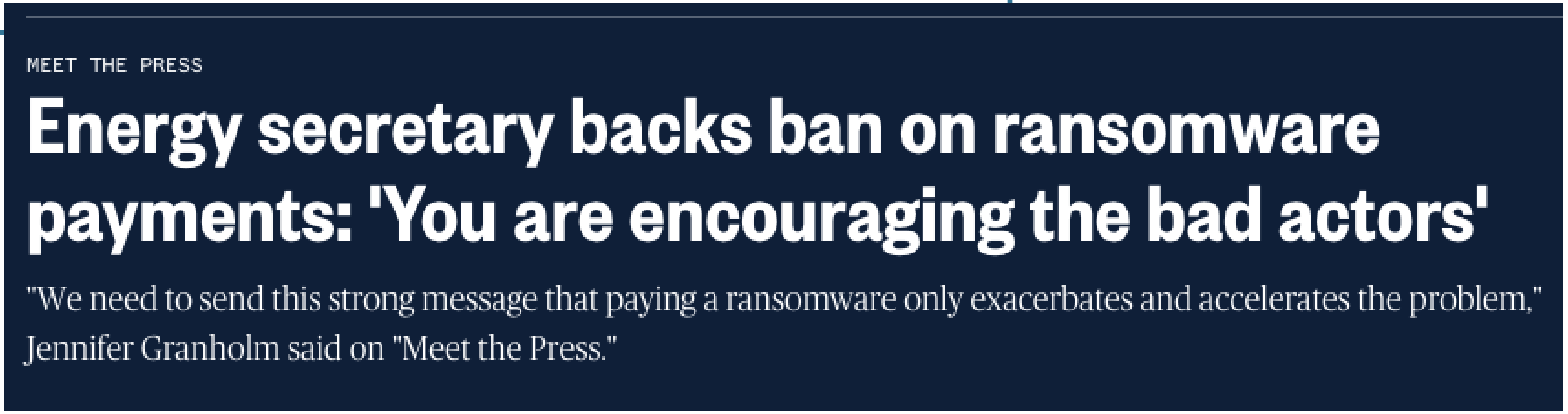
SPEED READS

SUNDAY SHOWS

Energy secretary says she'd support law banning ransomware payments

JUNE 6, 2021 **TIM O'DONNELL**

Energy Secretary Jennifer Granholm told CNN's Jake Tapper Sunday that she believes adversaries of the United States have the capability to shut down the power grid and thinks "there are very malign actors who are trying even as we speak."

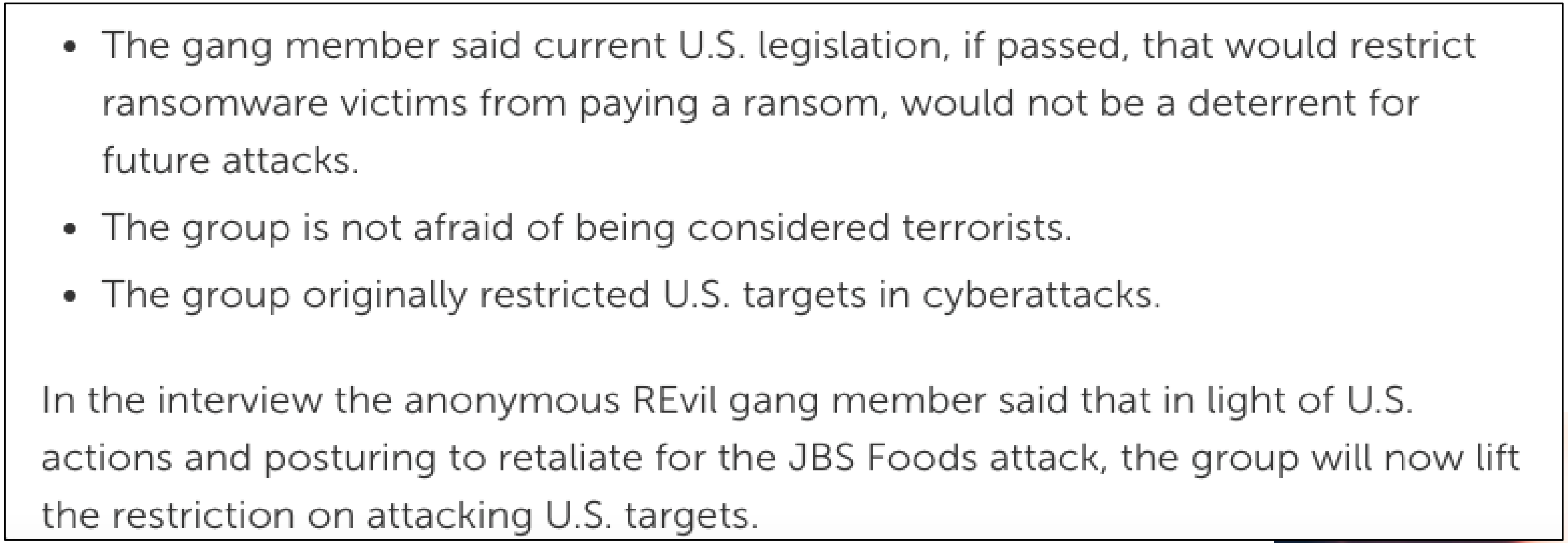


MEET THE PRESS

Energy secretary backs ban on ransomware payments: 'You are encouraging the bad actors'

"We need to send this strong message that paying a ransomware only exacerbates and accelerates the problem," Jennifer Granholm said on "Meet the Press."

Criminals are "Undeterred"

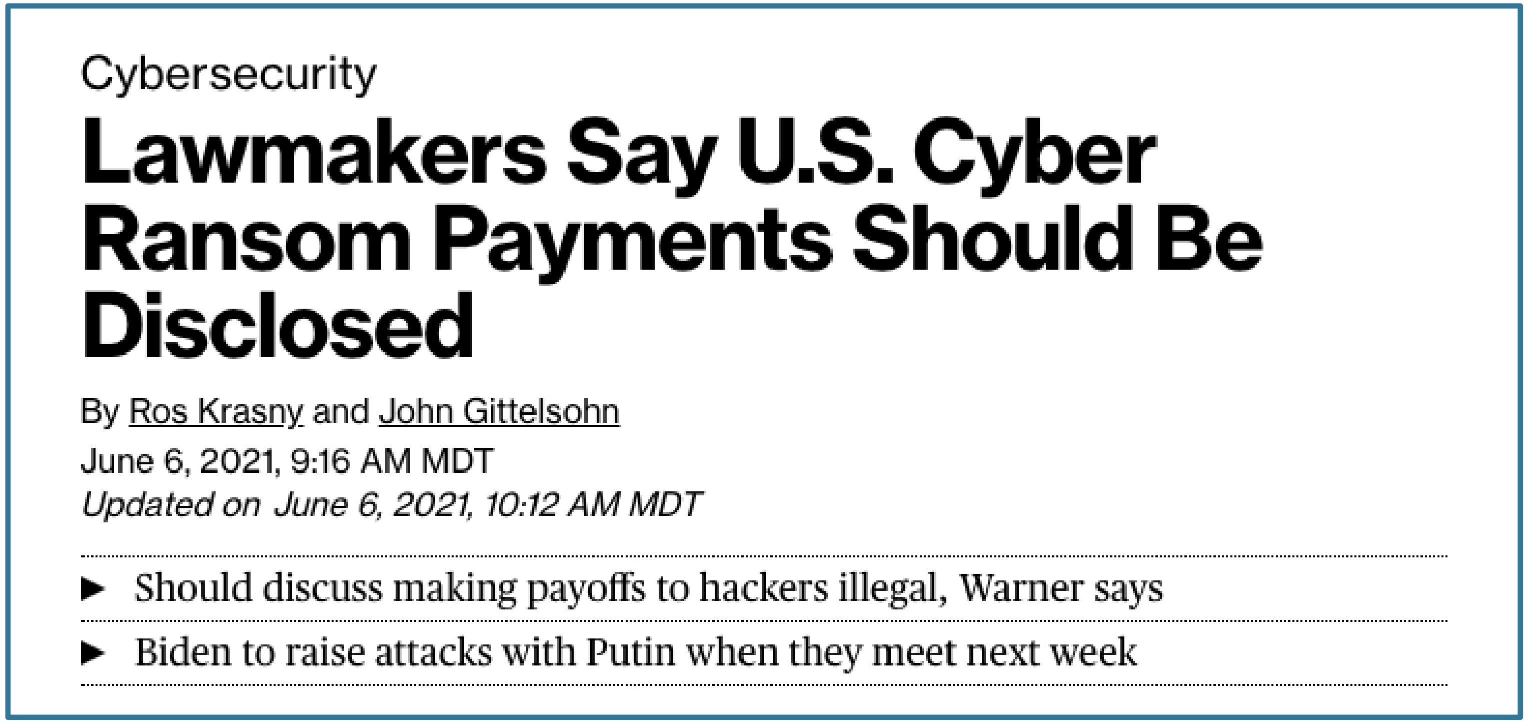


- The gang member said current U.S. legislation, if passed, that would restrict ransomware victims from paying a ransom, would not be a deterrent for future attacks.
- The group is not afraid of being considered terrorists.
- The group originally restricted U.S. targets in cyberattacks.

In the interview the anonymous REvil gang member said that in light of U.S. actions and posturing to retaliate for the JBS Foods attack, the group will now lift the restriction on attacking U.S. targets.

https://threatpost.com/revil-spill-details-us-attacks/166669/

Potential Policy Shift



Cybersecurity

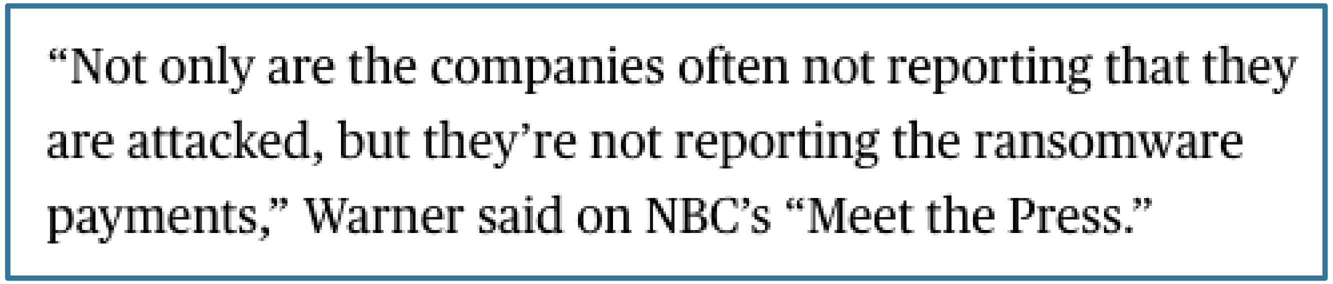
Lawmakers Say U.S. Cyber Ransom Payments Should Be Disclosed

By Ros Krasny and John Gittelsohn

June 6, 2021, 9:16 AM MDT

Updated on June 6, 2021, 10:12 AM MDT

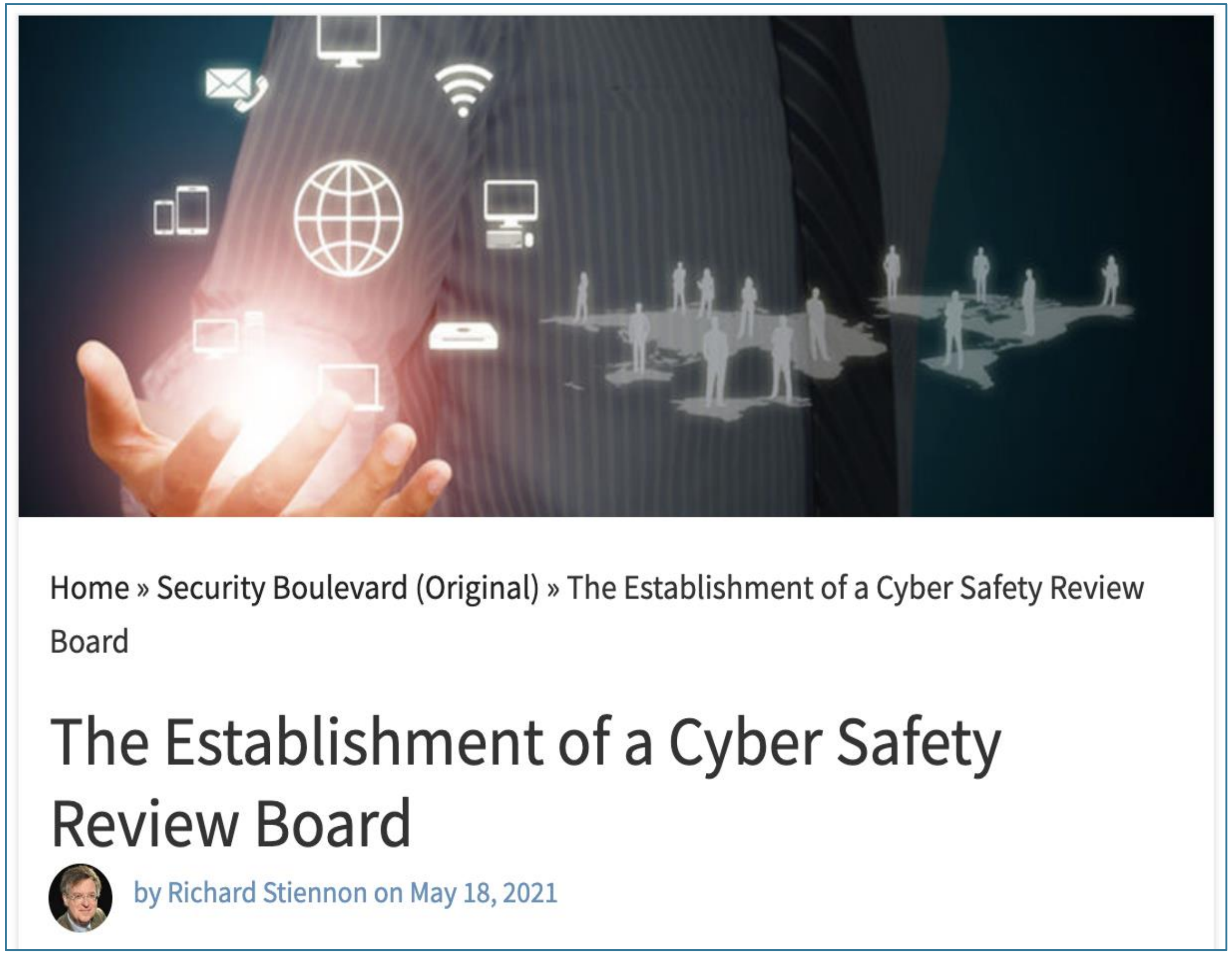
- Should discuss making payoffs to hackers illegal, Warner says
- Biden to raise attacks with Putin when they meet next week



"Not only are the companies often not reporting that they are attacked, but they're not reporting the ransomware payments," Warner said on NBC's "Meet the Press."

https://www.bloomberg.com/news/articles/2021-06-06/lawmakers-say-u-s-cyber-ransom-payments-should-be-disclosed

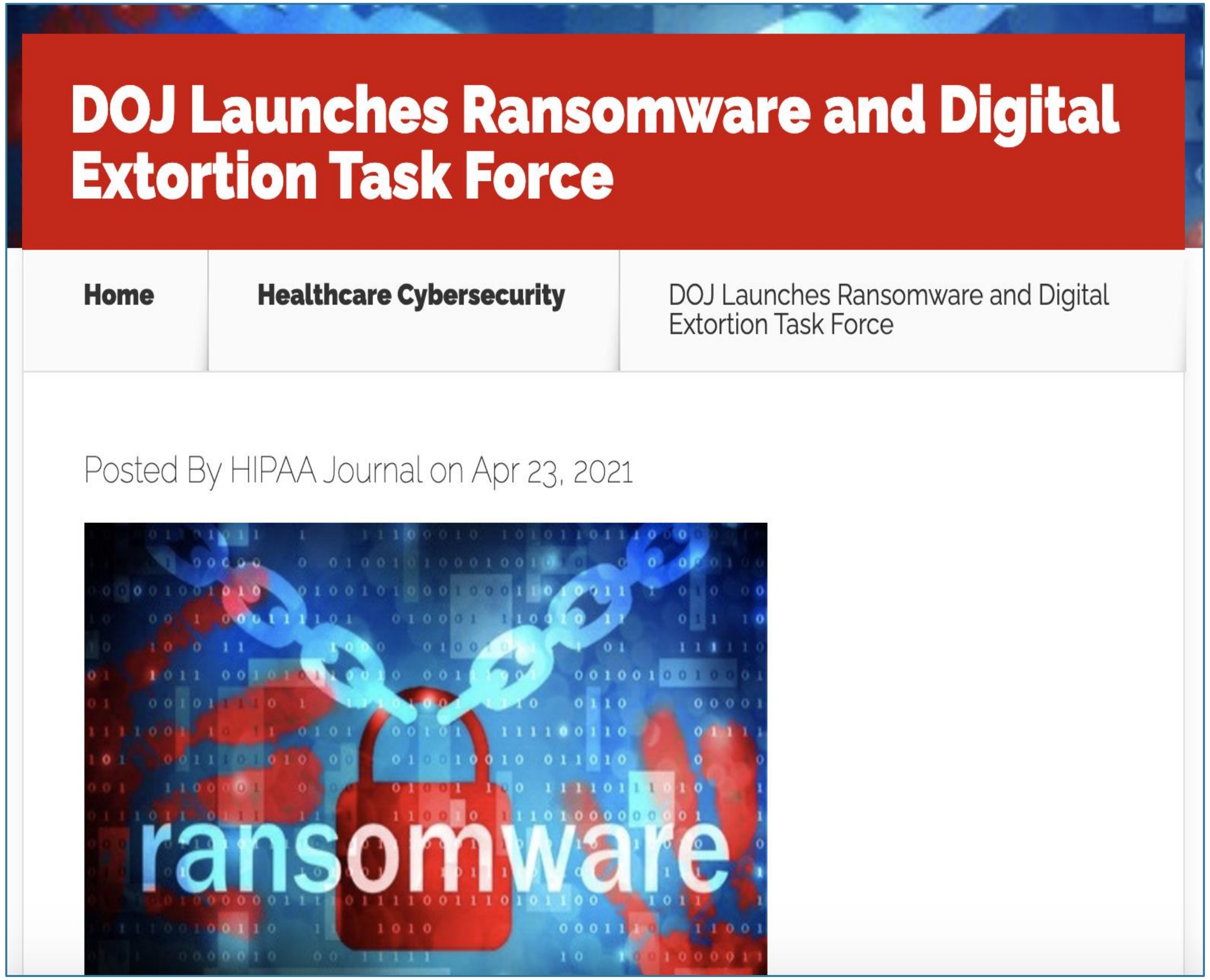
Increased Government Oversight



Home » Security Boulevard (Original) » The Establishment of a Cyber Safety Review Board

The Establishment of a Cyber Safety Review Board

by Richard Stiennon on May 18, 2021

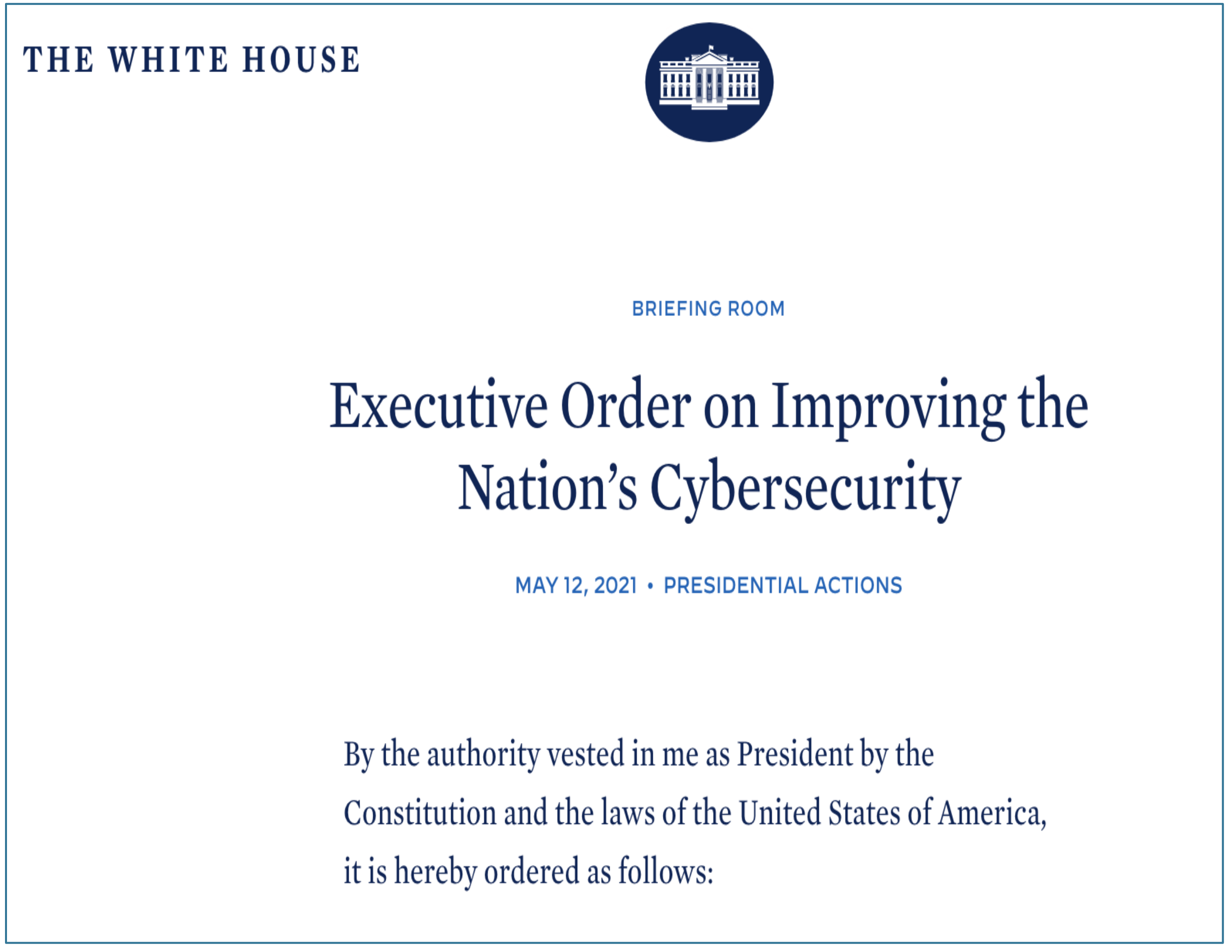


DOJ Launches Ransomware and Digital Extortion Task Force

Home | Healthcare Cybersecurity | DOJ Launches Ransomware and Digital Extortion Task Force

Posted By HIPAA Journal on Apr 23, 2021

New Executive Order



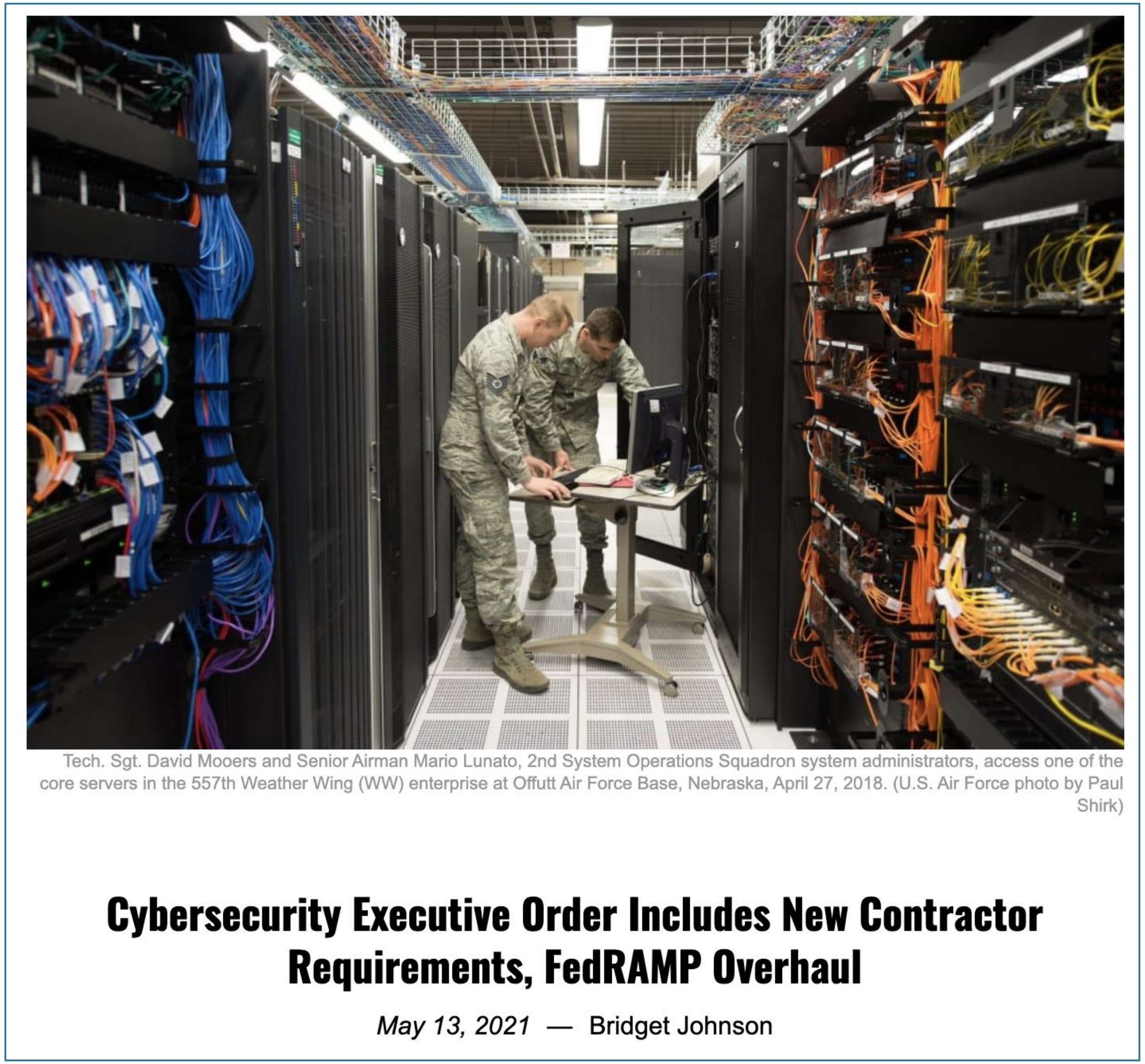
THE WHITE HOUSE

BRIEFING ROOM

Executive Order on Improving the Nation’s Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:



Tech. Sgt. David Mooers and Senior Airman Mario Lunato, 2nd System Operations Squadron system administrators, access one of the core servers in the 557th Weather Wing (WW) enterprise at Offutt Air Force Base, Nebraska, April 27, 2018. (U.S. Air Force photo by Paul Shirk)

Cybersecurity Executive Order Includes New Contractor Requirements, FedRAMP Overhaul

May 13, 2021 — Bridget Johnson

Supplier Cybersecurity & Response

- Improve software supply chain Security
- Increase information sharing capabilities
- Modernize and implement stronger cybersecurity requirements for suppliers
- Default contractual requirements
- Improve supplier detection capabilities
- Formalize supplier response policies

Software Bill of Materials (SBOM)

- Provide SBOMs for all products in use
- Maintain supply chain and code integrity with automated tools
- Frequent checks for vulnerabilities
- Participate in a vulnerability disclosure program
- Maintain up-to-date data on code, components, and controls for both primary and third-party software for each application
- Audit and enforce controls

Software Bill of Materials Required by 2021 Cyber Security Executive Order

May 14, 2021

Supplier Attacks

Russian SolarWinds Hackers Target 150 Organizations in New Attack

By Rob Lever for AFP
May 28, 2021

The SolarWinds attack has been connected to Russian state-backed hackers.

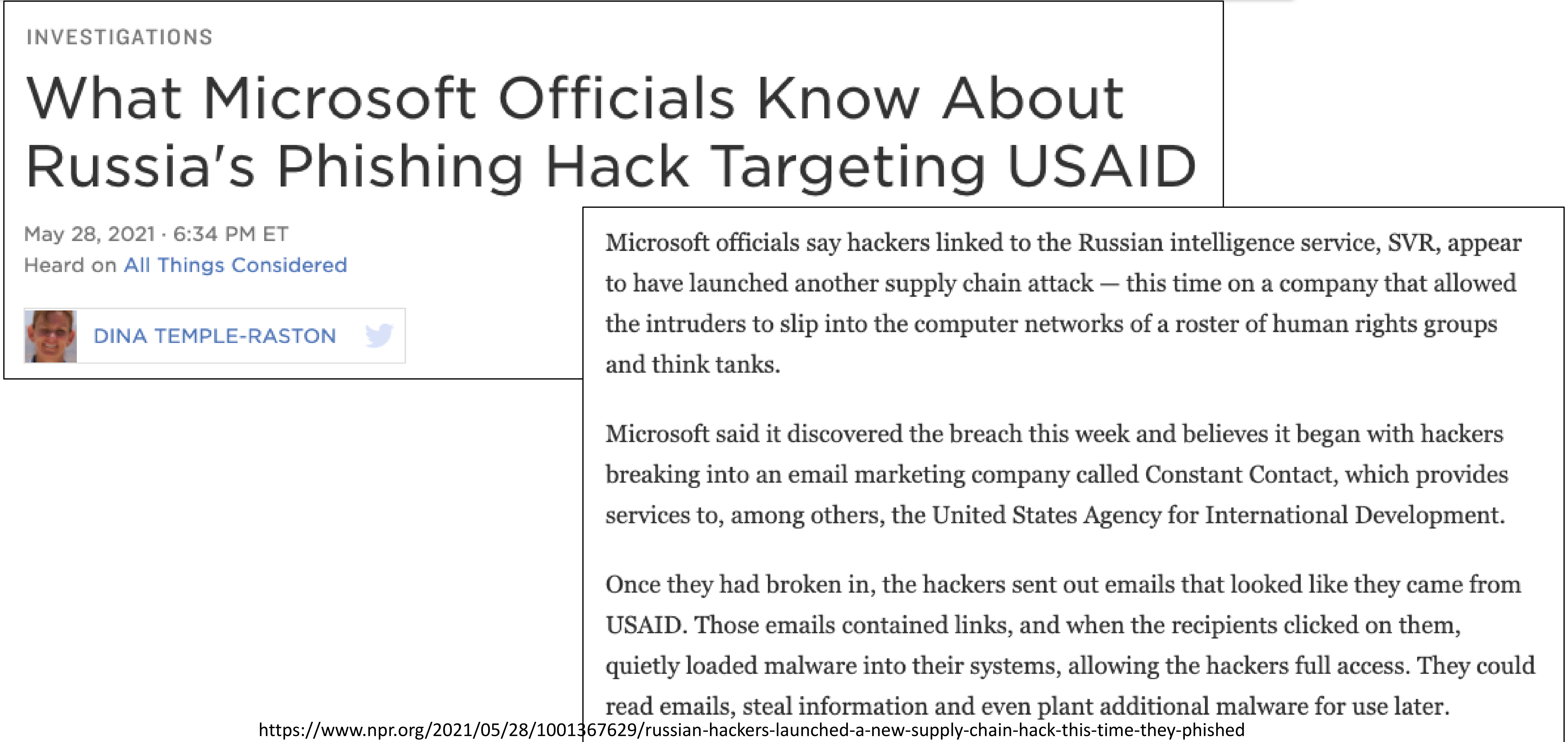
Christopher Schimer / Flickr (CC BY-SA 2.0)

The Moscow Times
INDEPENDENT NEWS FROM RUSSIA

The state-backed Russian group behind a massive hacking campaign revealed last year has re-emerged with a series of attacks on government agencies, think tanks, consultants and other organizations, according to officials and researchers.

https://www.themoscowtimes.com/2021/05/28/russian-solarwinds-hackers-target-150-organizations-in-new-attack-a74047

Solar Winds Update



INVESTIGATIONS

What Microsoft Officials Know About Russia's Phishing Hack Targeting USAID

May 28, 2021 · 6:34 PM ET

Heard on All Things Considered

DINA TEMPLE-RASTON

Microsoft officials say hackers linked to the Russian intelligence service, SVR, appear to have launched another supply chain attack — this time on a company that allowed the intruders to slip into the computer networks of a roster of human rights groups and think tanks.

Microsoft said it discovered the breach this week and believes it began with hackers breaking into an email marketing company called Constant Contact, which provides services to, among others, the United States Agency for International Development.

Once they had broken in, the hackers sent out emails that looked like they came from USAID. Those emails contained links, and when the recipients clicked on them, quietly loaded malware into their systems, allowing the hackers full access. They could read emails, steal information and even plant additional malware for use later.

https://www.npr.org/2021/05/28/1001367629/russian-hackers-launched-a-new-supply-chain-hack-this-time-they-phished

Adapt Your Response Processes

- Stay Up to Date on legislation & regulations
- Include suppliers/contractors
- Check your cloud logs/evidence
- Prepare for LE involvement
- Monitor your high risk scenarios
- Understand your insurance coverage
- Include remote workers/contractors

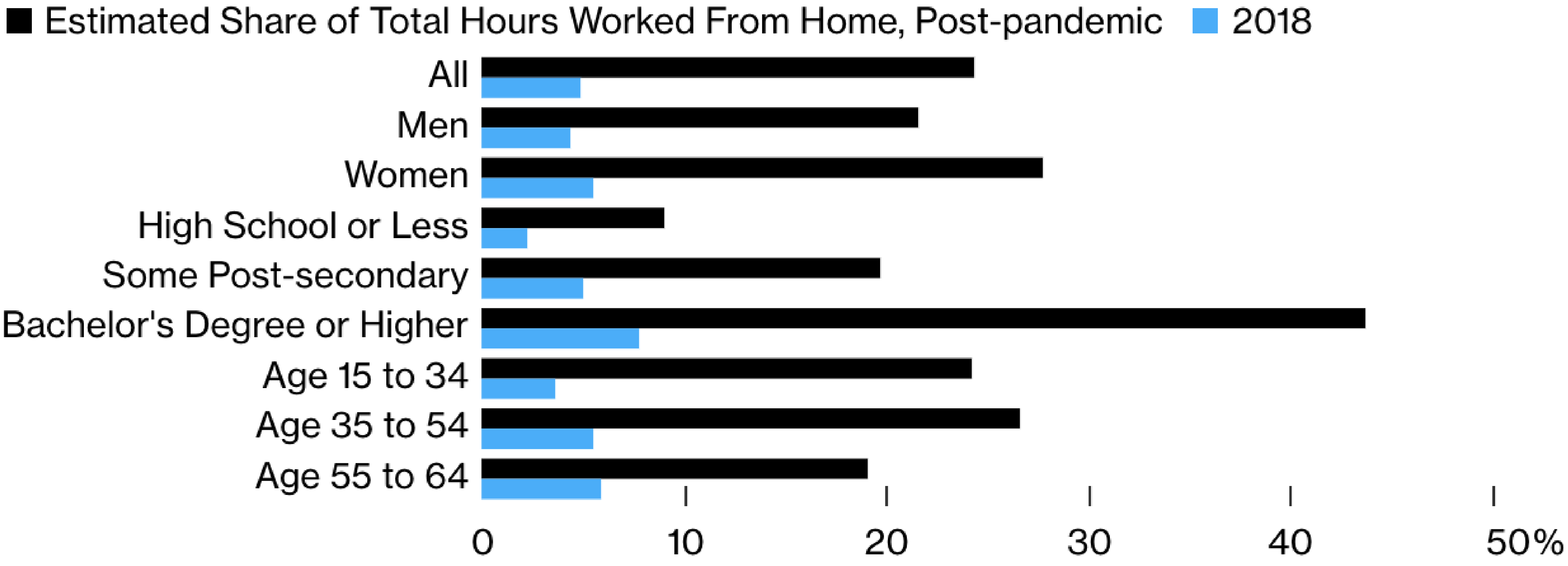
Case: Response w/ Remote Workforce

- Professional services firm
- ~50 employees
- ~300 contractors
- Remote access w/ VPN
- Policy against using personal devices
- …but everybody did it

Remote Workers

Out of Office

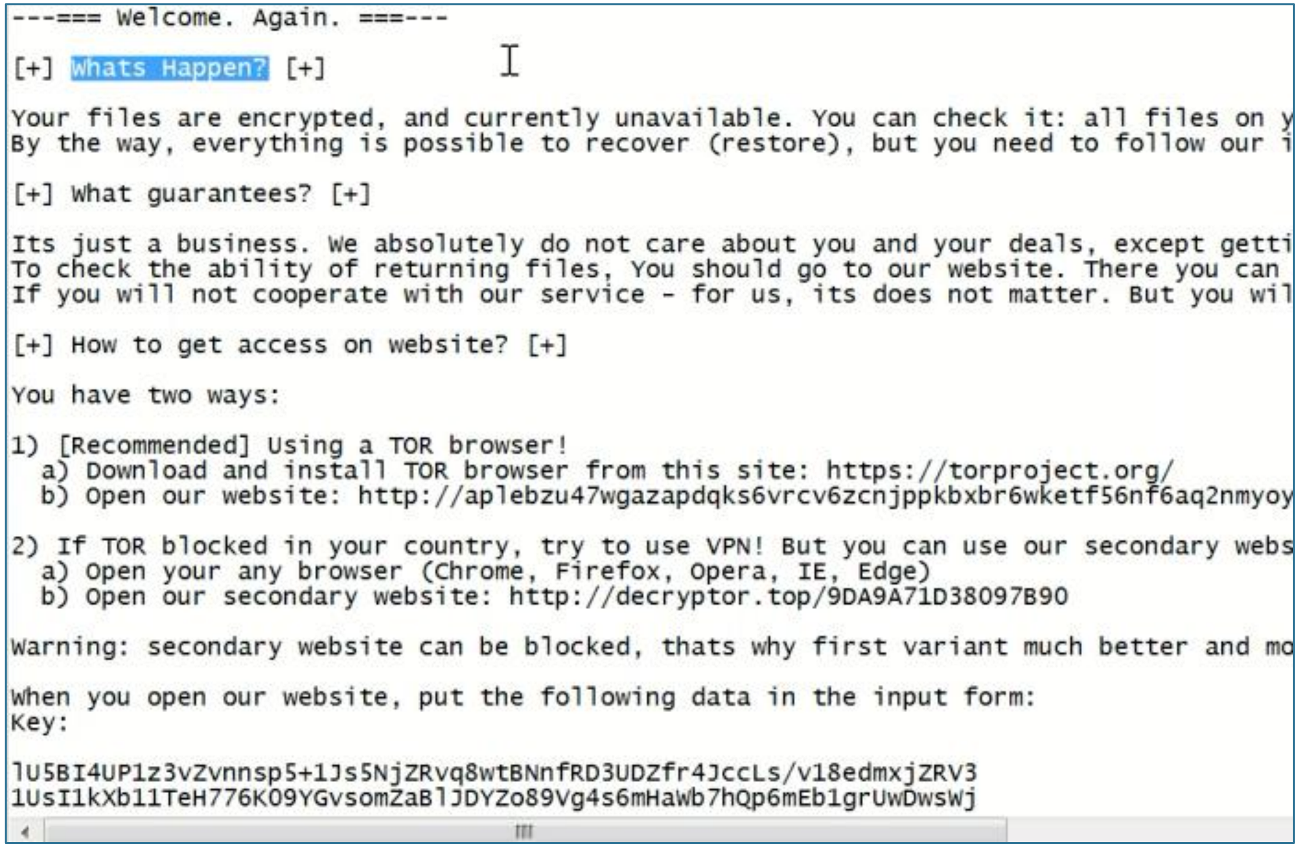
Nearly a quarter of hours worked could be remote after the pandemic



Source: Statistics Canada

Ransomware Strikes!

- Monday morning - employees arrive
- Web servers, databases and production systems are all offline
- Ransom notes on the screens
  - Print-bombed the ransom note, too
- VPN is down



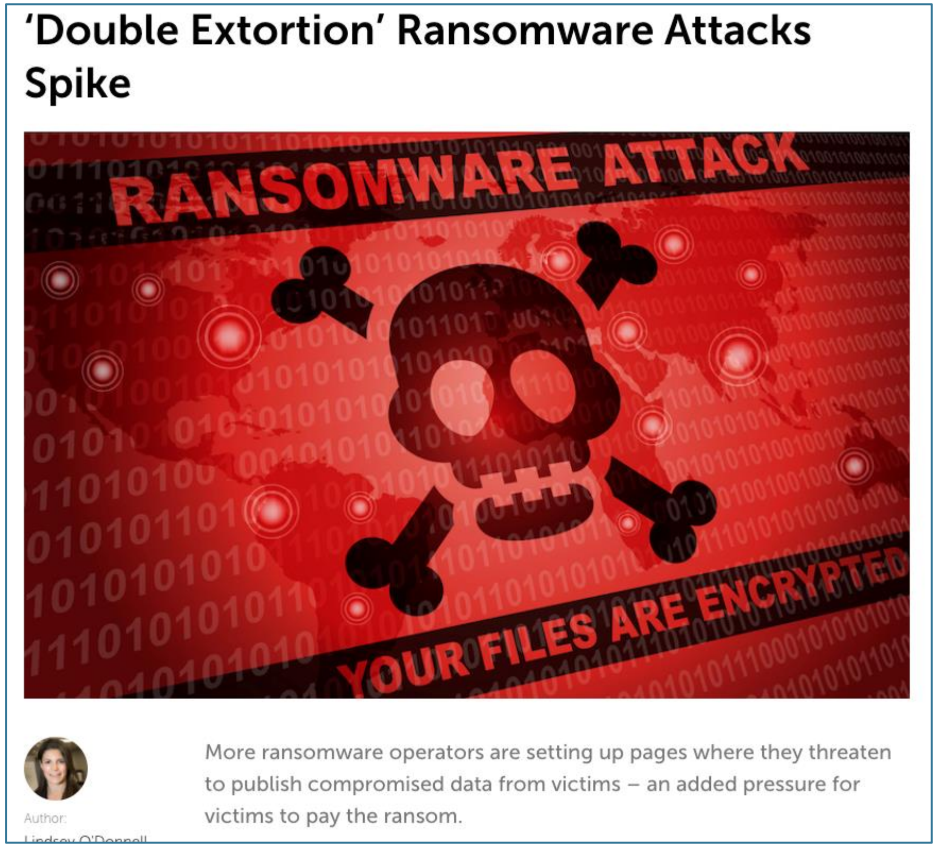
```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on y
By the way, everything is possible to recover (restore), but you need to follow our i

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals, except getti
To check the ability of returning files, You should go to our website. There you can
If you will not cooperate with our service - for us, its does not matter. But you wil

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoy

2) If TOR blocked in your country, try to use VPN! But you can use our secondary webs
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://decryptor.top/9DA9A71D38097B90

Warning: secondary website can be blocked, thats why first variant much better and mo

When you open our website, put the following data in the input form:
Key:

lU5BI4UP1z3vZvnnsp5+1Js5NjZRvq8wtBNnfRD3UDZfr4JccLs/v18edmxjZRV3
1UsI1kXb11TeH776K09YGvsomZaBlJDYZo89Vg4s6mHaWb7hQp6mEb1grUwDwsWj
```

Data is Gone! (Forever?)

- Primary data servers encrypted
- Backups are fully encrypted too (unrecoverable)
- Key operational data was unrecoverable
  - Financial data
  - Employee records
  - Vendor data
  - Intellectual property

Threats to Publicly Leak Data

RANSOM DEMAND: $1,200,000



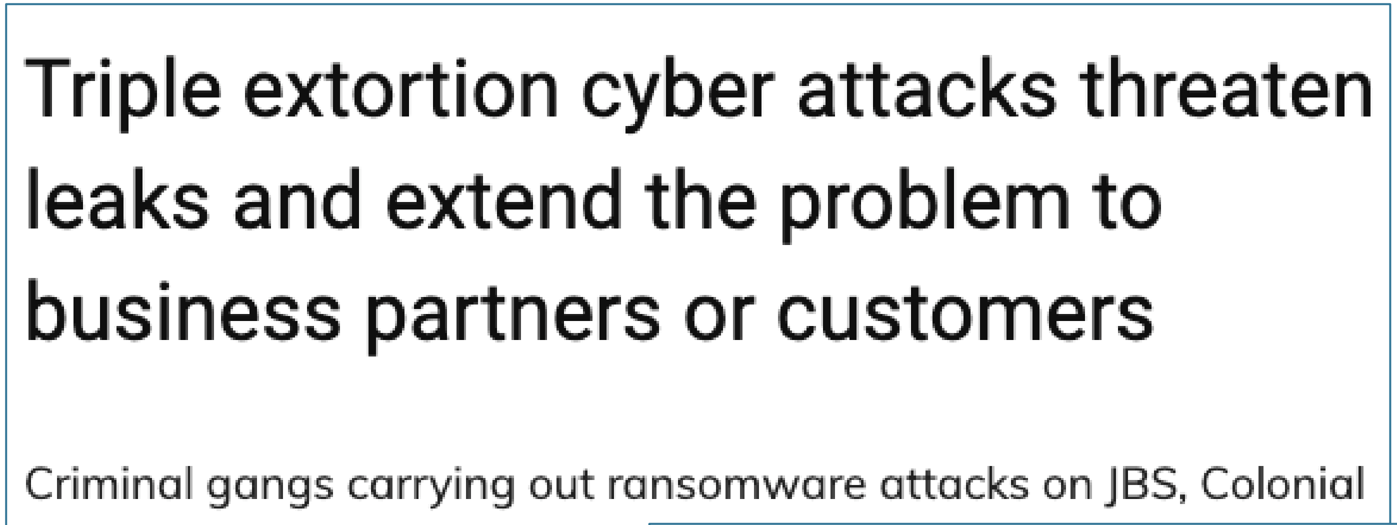
'Double Extortion' Ransomware Attacks Spike

Author:
Lindsey O'Donnell

More ransomware operators are setting up pages where they threaten to publish compromised data from victims – an added pressure for victims to pay the ransom.

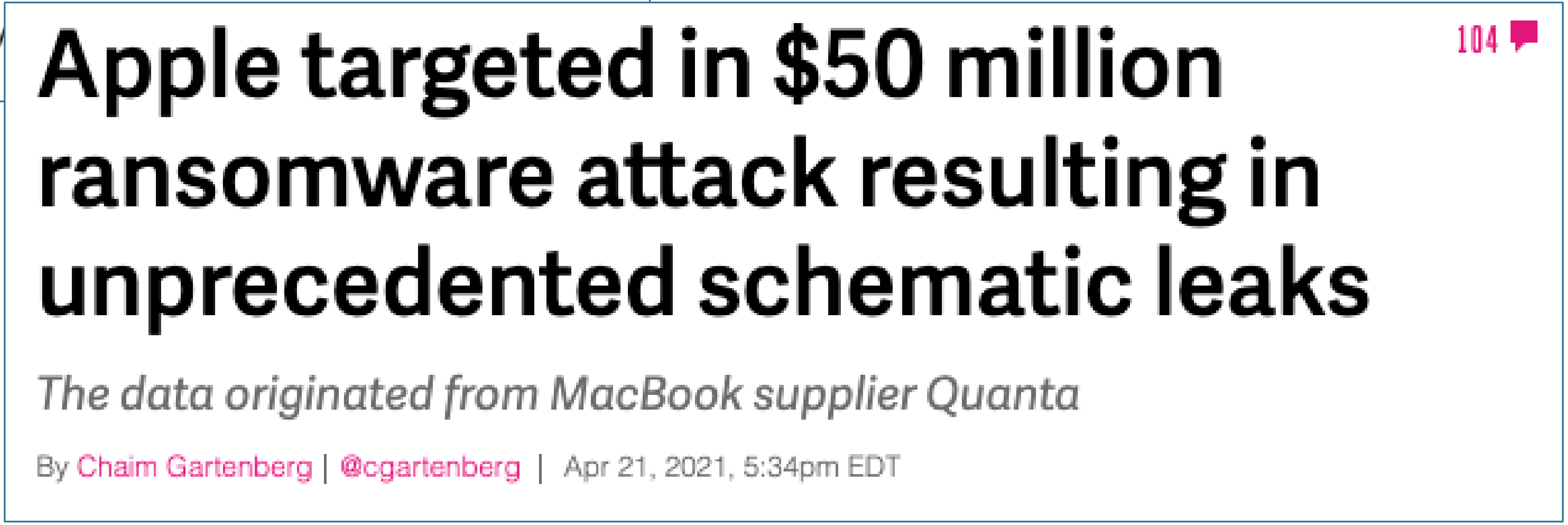
Today: 77% of all ransomware cases involve data theft

Triple Extortion



Triple extortion cyber attacks threaten leaks and extend the problem to business partners or customers

Criminal gangs carrying out ransomware attacks on JBS, Colonial Pipeline and others have a nev



104

Apple targeted in $50 million ransomware attack resulting in unprecedented schematic leaks

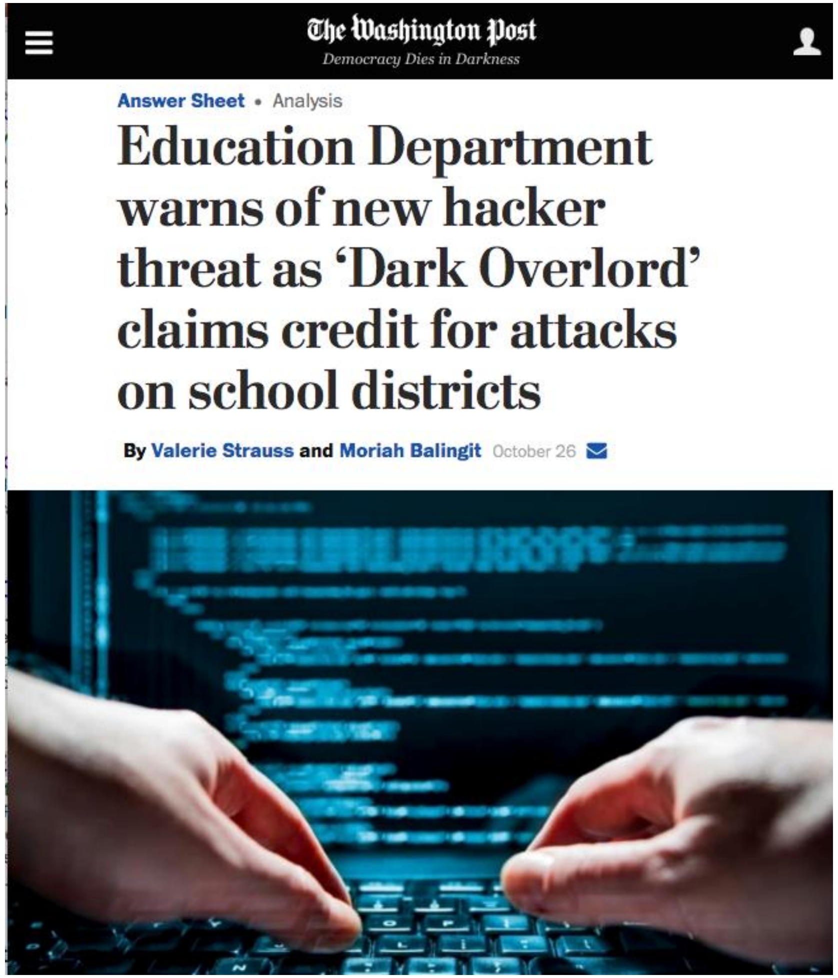
The data originated from MacBook supplier Quanta

By Chaim Gartenberg | @cgartenberg | Apr 21, 2021, 5:34pm EDT

https://granthshala.com/hackers-behind-jbs-ransomware-have-new-extortion-tactic/

Not Really New…

- Flashback to 2016: TheDarkOverlord
- Schools, hospitals, any org
- Threatens community members
- Parents, students
- Text messages
- Phone calls



The Washington Post

Democracy Dies in Darkness

Answer Sheet • Analysis

Education Department warns of new hacker threat as 'Dark Overlord' claims credit for attacks on school districts

By Valerie Strauss and Moriah Balingit October 26

Happy Blog!

Ransomware gang asks $42m from NY law firm, threatens to leak dirt on Trump

The REvil ransomware gang published last night 2.4 GB of Lady Gaga's legal documents.

By Catalin Cimpanu for Zero Day | May 15, 2020 -- 19:13 GMT (12:13 PDT) | To

Papa don't breach: Contracts, personal info on Madonna, Lady Gaga, Elton John, others swiped in celeb law firm 'hack'

Miscreants threaten to leak 756GB of allegedly stolen paperwork

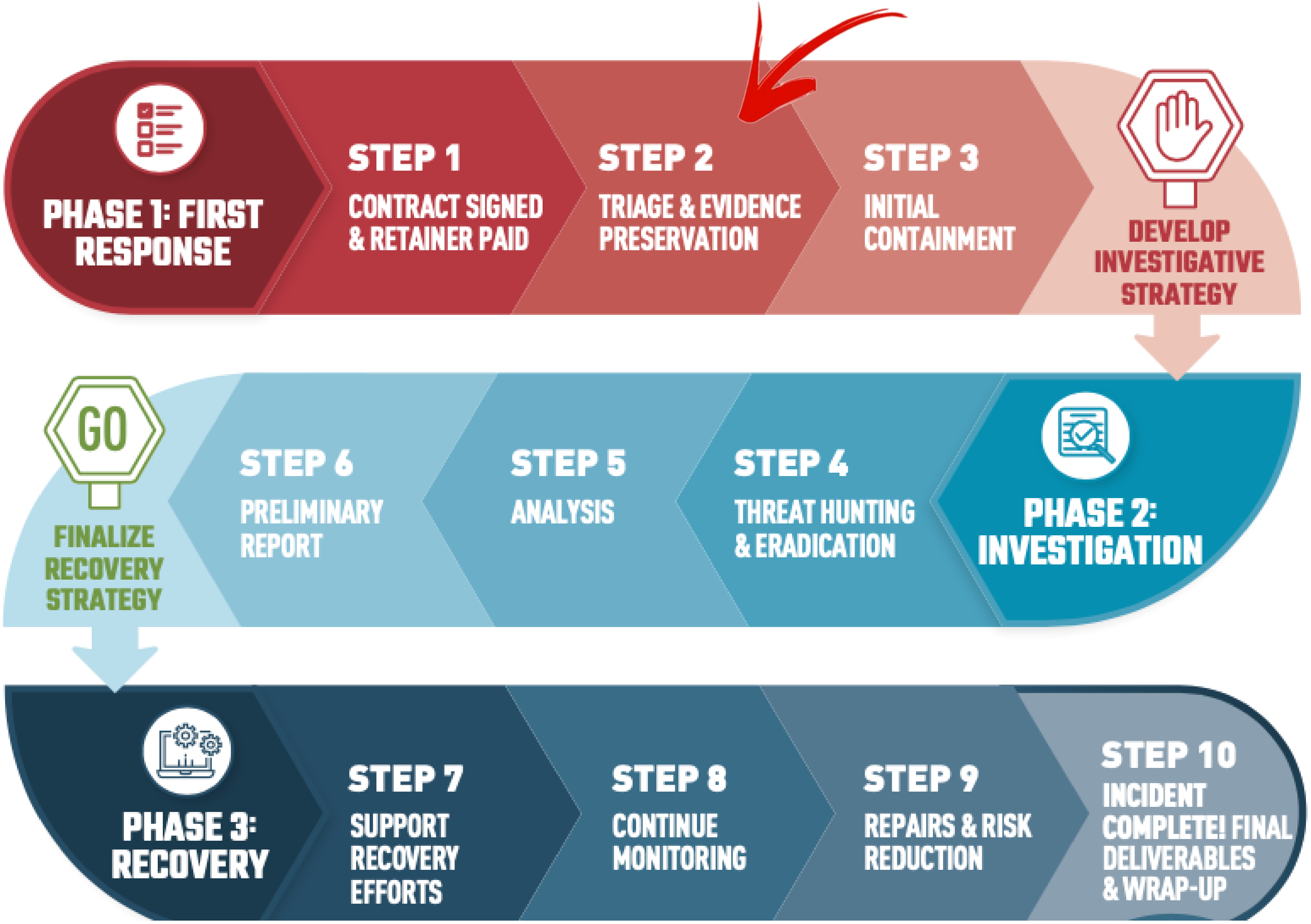
TUE 12 MAY 2020 // 01:43 UTC

23 GOT TIPS?

Shaun Nichols in San Francisco BIO EMAIL TWITTER SHARE ▼

Who's Involved?

- IT
- Insurance
- Outside Attorneys
- Forensics (LMG)



PHASE 1: FIRST RESPONSE

STEP 1
CONTRACT SIGNED & RETAINER PAID

STEP 2
TRIAGE & EVIDENCE PRESERVATION

STEP 3
INITIAL CONTAINMENT

DEVELOP INVESTIGATIVE STRATEGY

PHASE 2: INVESTIGATION

STEP 4
THREAT HUNTING & ERADICATION

STEP 5
ANALYSIS

STEP 6
PRELIMINARY REPORT

GO

FINALIZE RECOVERY STRATEGY

PHASE 3: RECOVERY

STEP 7
SUPPORT RECOVERY EFFORTS

STEP 8
CONTINUE MONITORING

STEP 9
REPAIRS & RISK REDUCTION

STEP 10
INCIDENT COMPLETE! FINAL DELIVERABLES & WRAP-UP

Triage

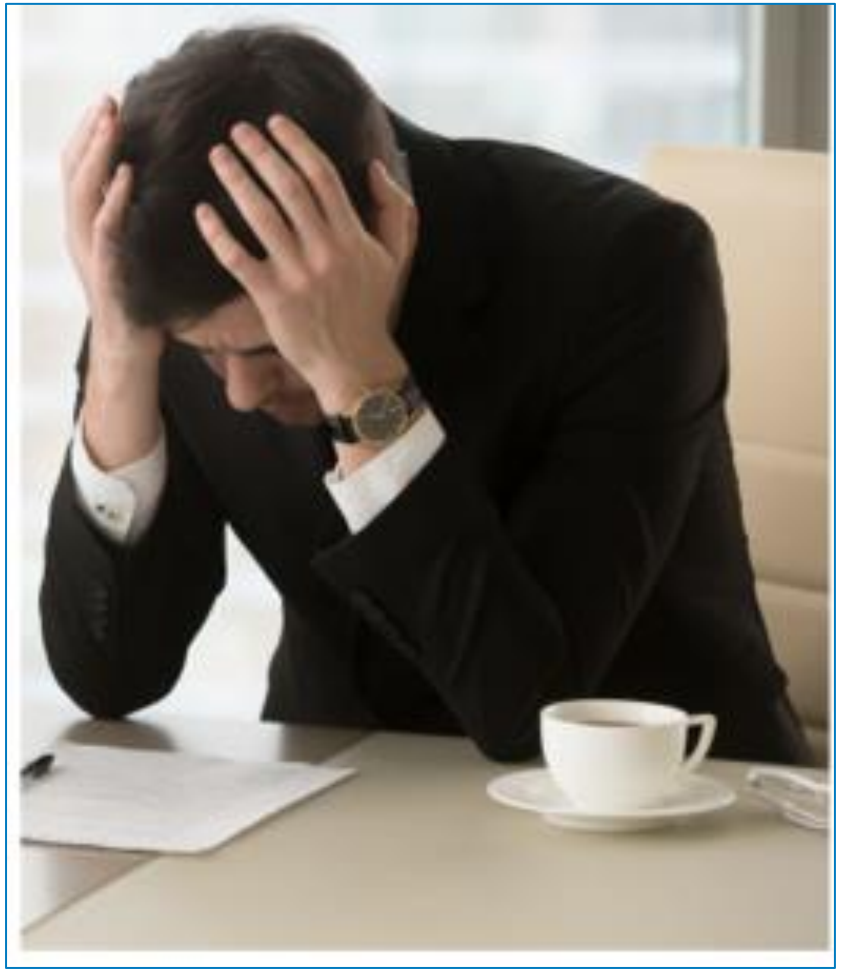
- Prioritize
- What
  systems are needed to operate?
- What information is at risk?
- Eradicate the threat
- Available resources
- Come up with a game plan

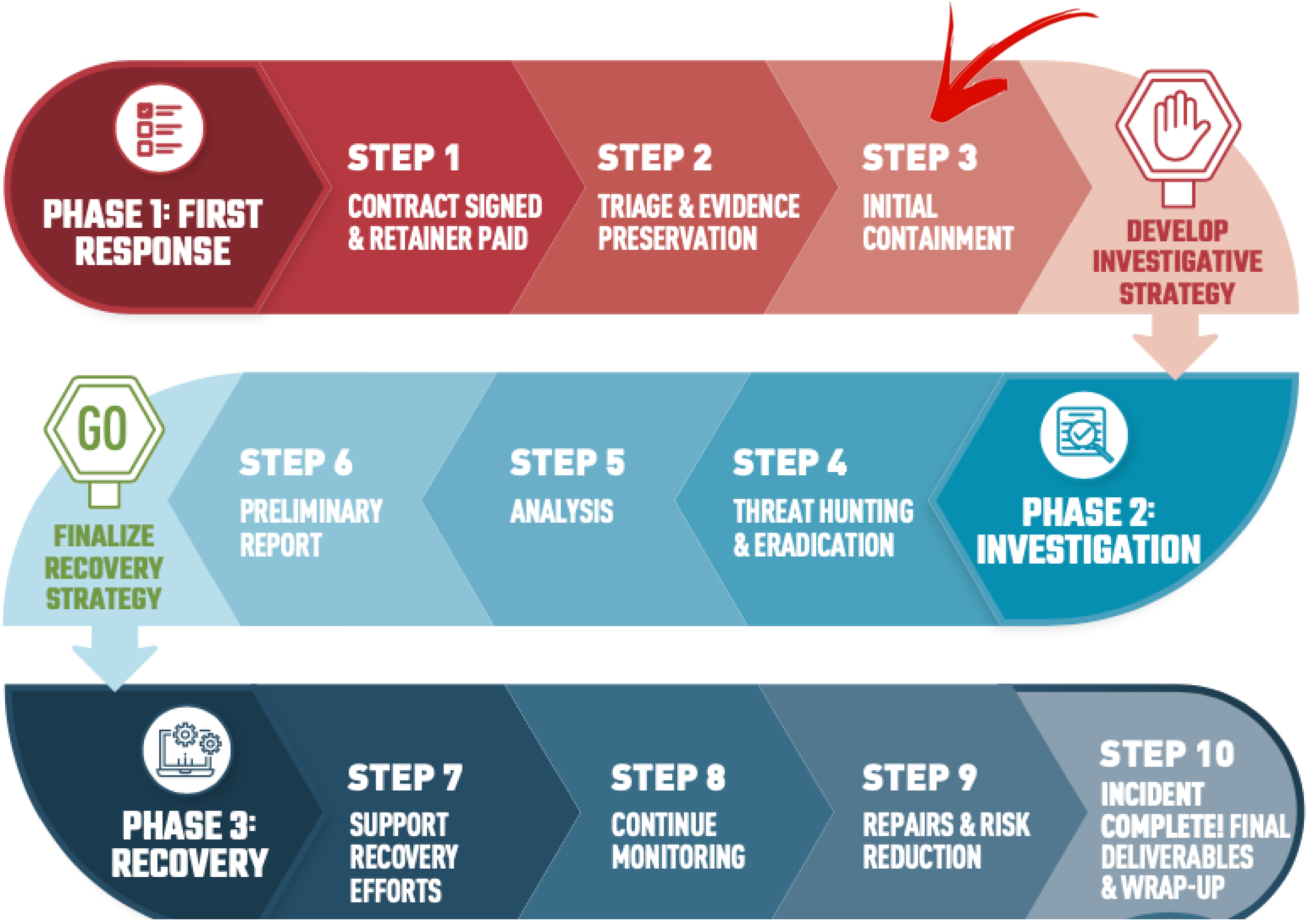
Why Preserve Evidence?

- Rule out a breach
- Understand what was affected
- Trace the attackers' footprints
- Avoid overnotification
- Digital evidence spoils easily!

Common Evidence Preservation Mistakes

1. Destroyed during recovery
   - Format & reinstall
2. Too late
   - Example: Email hacking case
3. Curiosity
   - Opening files, changing last access times





PHASE 1: FIRST RESPONSE

STEP 1
CONTRACT SIGNED & RETAINER PAID

STEP 2
TRIAGE & EVIDENCE PRESERVATION

STEP 3
INITIAL CONTAINMENT

DEVELOP INVESTIGATIVE STRATEGY

PHASE 2: INVESTIGATION

STEP 4
THREAT HUNTING & ERADICATION

STEP 5
ANALYSIS

STEP 6
PRELIMINARY REPORT

GO

FINALIZE RECOVERY STRATEGY

PHASE 3: RECOVERY

STEP 7
SUPPORT RECOVERY EFFORTS

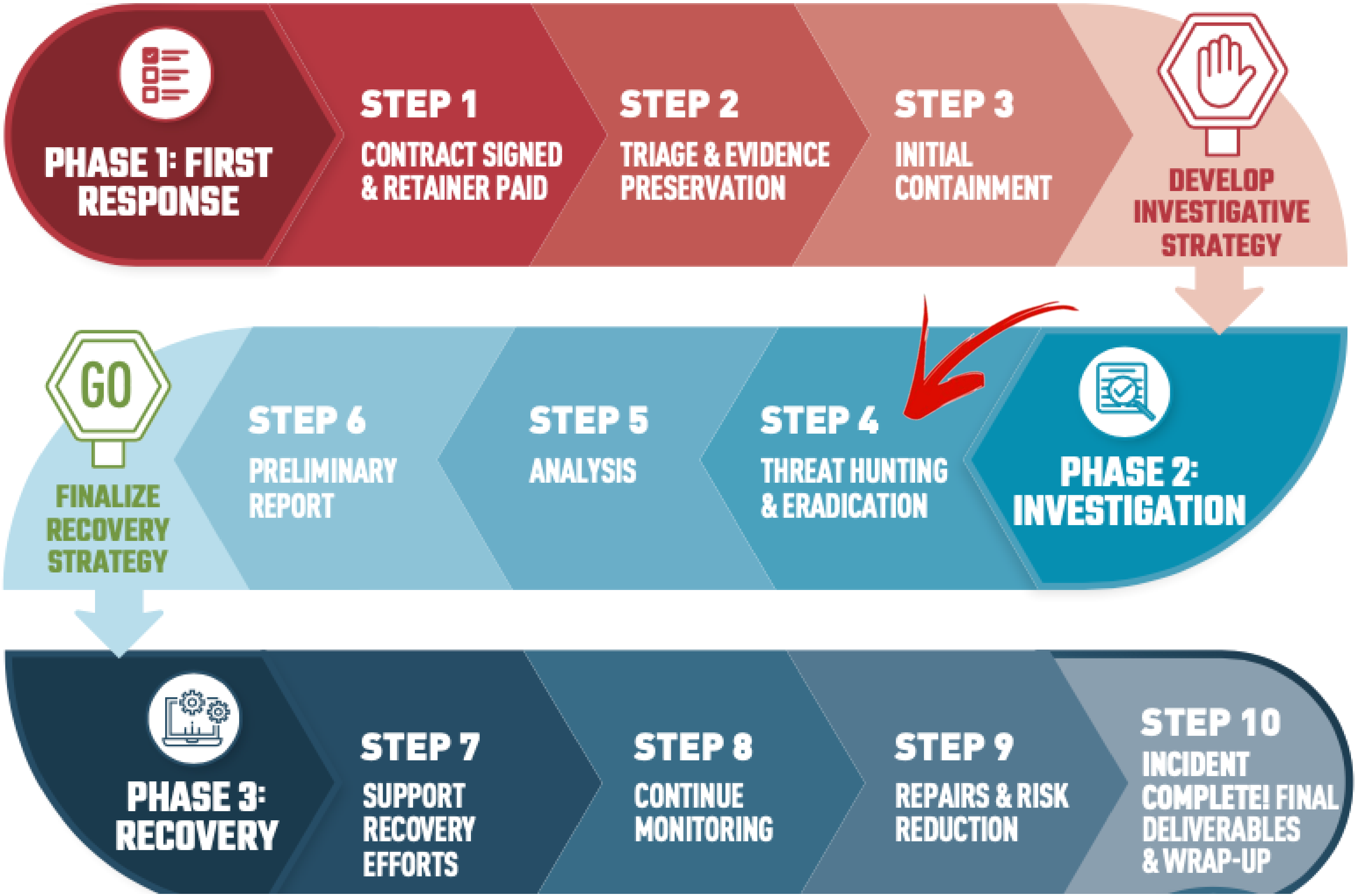
STEP 8
CONTINUE MONITORING

STEP 9
REPAIRS & RISK REDUCTION

STEP 10
INCIDENT COMPLETE! FINAL DELIVERABLES & WRAP-UP

Rapid Containment

- Kill all remote sessions
- Reset passwords IMMEDIATELY
- Disconnect VPN
- Disconnect primary servers from the network
- Configure secure remote access



PHASE 1: FIRST RESPONSE

STEP 1
CONTRACT SIGNED & RETAINER PAID

STEP 2
TRIAGE & EVIDENCE PRESERVATION

STEP 3
INITIAL CONTAINMENT

DEVELOP INVESTIGATIVE STRATEGY

PHASE 2: INVESTIGATION

STEP 4
THREAT HUNTING & ERADICATION

STEP 5
ANALYSIS

STEP 6
PRELIMINARY REPORT

GO

FINALIZE RECOVERY STRATEGY

PHASE 3: RECOVERY

STEP 7
SUPPORT RECOVERY EFFORTS

STEP 8
CONTINUE MONITORING

STEP 9
REPAIRS & RISK REDUCTION

STEP 10
INCIDENT COMPLETE! FINAL DELIVERABLES & WRAP-UP

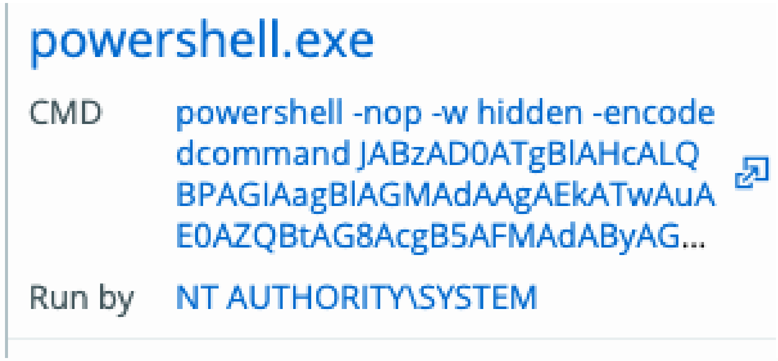
Working Backwards…

- Ransomware detonated at 2am Monday
- Pushed from the domain controller via PSEXEC
- RDP connected using a service account

Begin the Hunt

- Adversary was Egregor
- Cobalt Strike
- Ransomware Executables
- Malicious network traffic
- Encoded Powershell

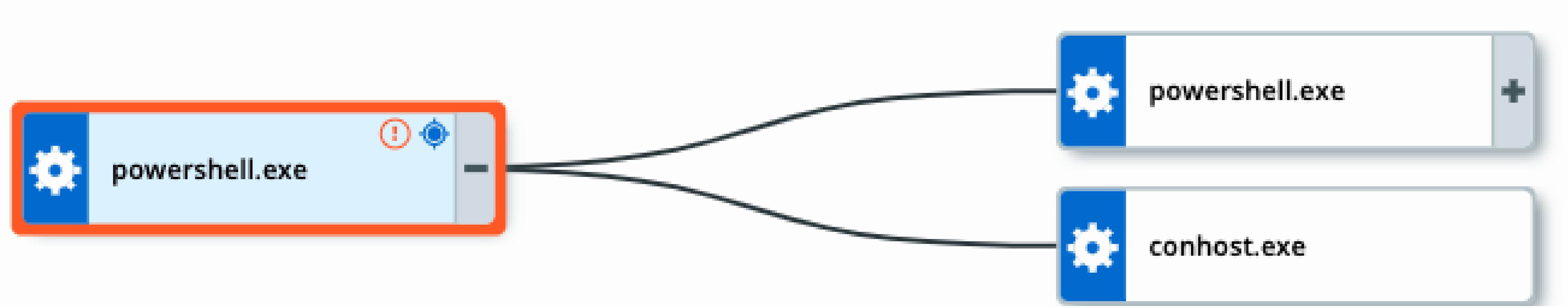
Finding Beacons



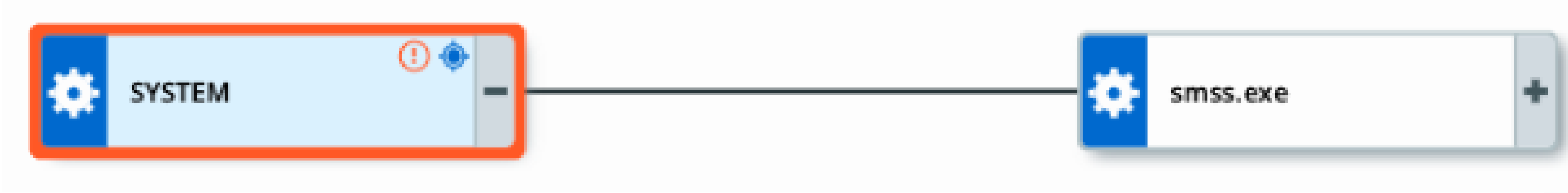
powershell.exe

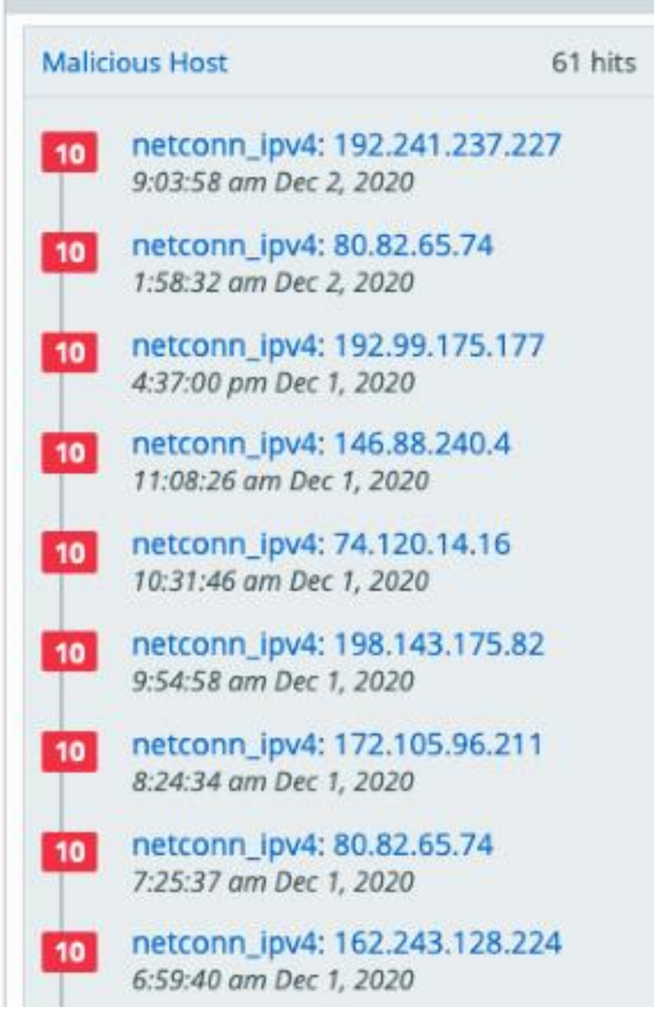
CMD powershell -nop -w hidden -encode
dcommand JABzAD0ATgBlAHcALQ
BPAGIAagBlAGMAdAAgAEkATwAuA
E0AZQBtAG8AcgB5AFMAdAByAG...

Run by NT AUTHORITY\SYSTEM



Malicious Network Communication




Malicious Host 61 hits

10 netconn_ipv4: 192.241.237.227
9:03:58 am Dec 2, 2020

10 netconn_ipv4: 80.82.65.74
1:58:32 am Dec 2, 2020

10 netconn_ipv4: 192.99.175.177
4:37:00 pm Dec 1, 2020

10 netconn_ipv4: 146.88.240.4
11:08:26 am Dec 1, 2020

10 netconn_ipv4: 74.120.14.16
10:31:46 am Dec 1, 2020

10 netconn_ipv4: 198.143.175.82
9:54:58 am Dec 1, 2020

10 netconn_ipv4: 172.105.96.211
8:24:34 am Dec 1, 2020

10 netconn_ipv4: 80.82.65.74
7:25:37 am Dec 1, 2020

10 netconn_ipv4: 162.243.128.224
6:59:40 am Dec 1, 2020

What About Remote Workers?

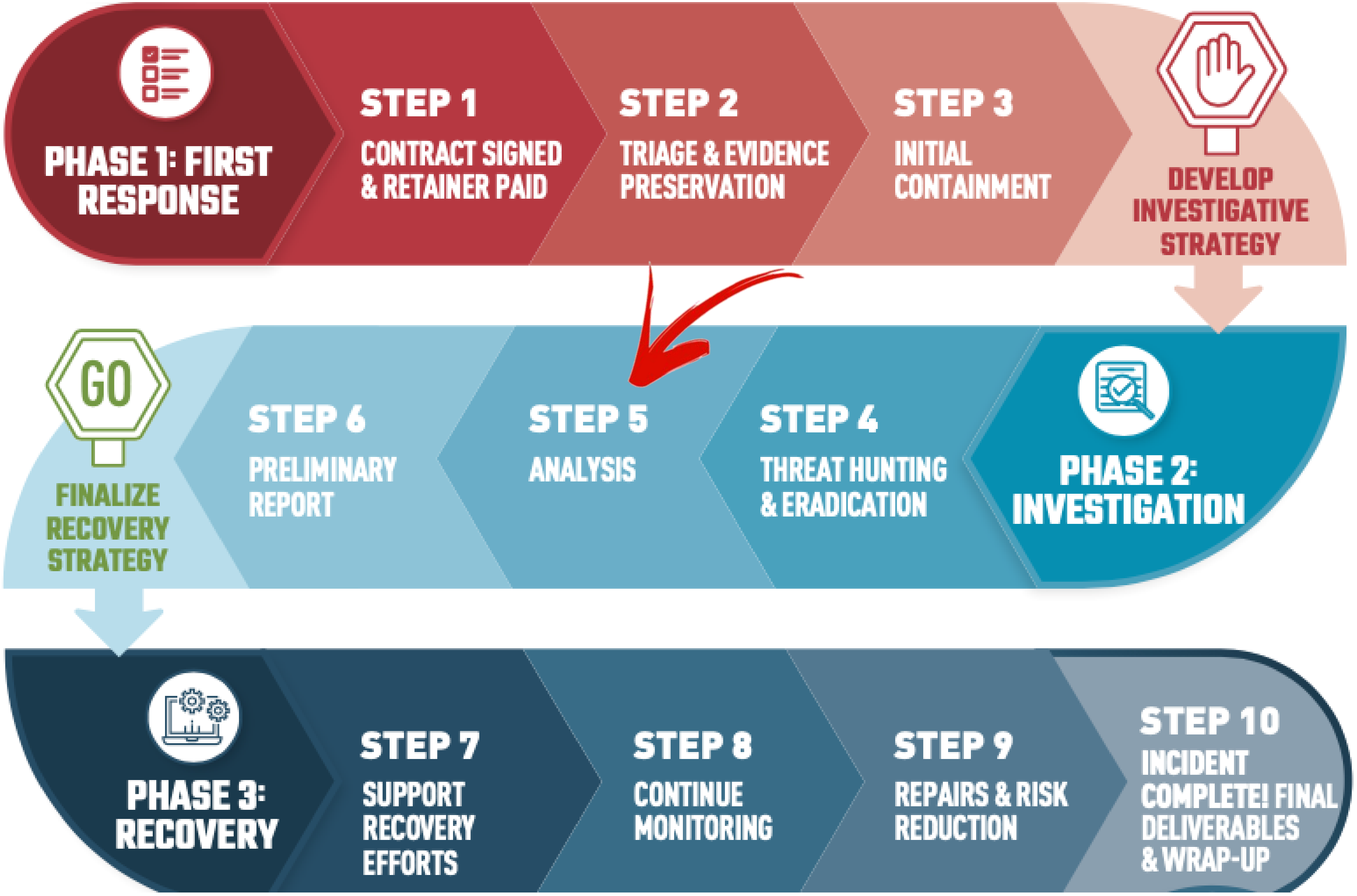
- Not connected…yet
- Infected systems
- Can’t find until reconnect
- No control over personal systems
- Global IP addresses (can’t just block Russia)

MacGyvered It

- Used Carbon Black
- Emailed installers to staff
- MUCH better ahead of time!
  - An ounce of prevention…

Visibility into Remote Workstations

- Centrally managed security software
- Both corp. & personal devices if used
- MDM Software
- Endpoint detection



PHASE 1: FIRST RESPONSE

STEP 1
CONTRACT SIGNED & RETAINER PAID

STEP 2
TRIAGE & EVIDENCE PRESERVATION

STEP 3
INITIAL CONTAINMENT

DEVELOP INVESTIGATIVE STRATEGY

PHASE 2: INVESTIGATION

STEP 4
THREAT HUNTING & ERADICATION

STEP 5
ANALYSIS

STEP 6
PRELIMINARY REPORT

FINALIZE RECOVERY STRATEGY

PHASE 3: RECOVERY

STEP 7
SUPPORT RECOVERY EFFORTS

STEP 8
CONTINUE MONITORING

STEP 9
REPAIRS & RISK REDUCTION

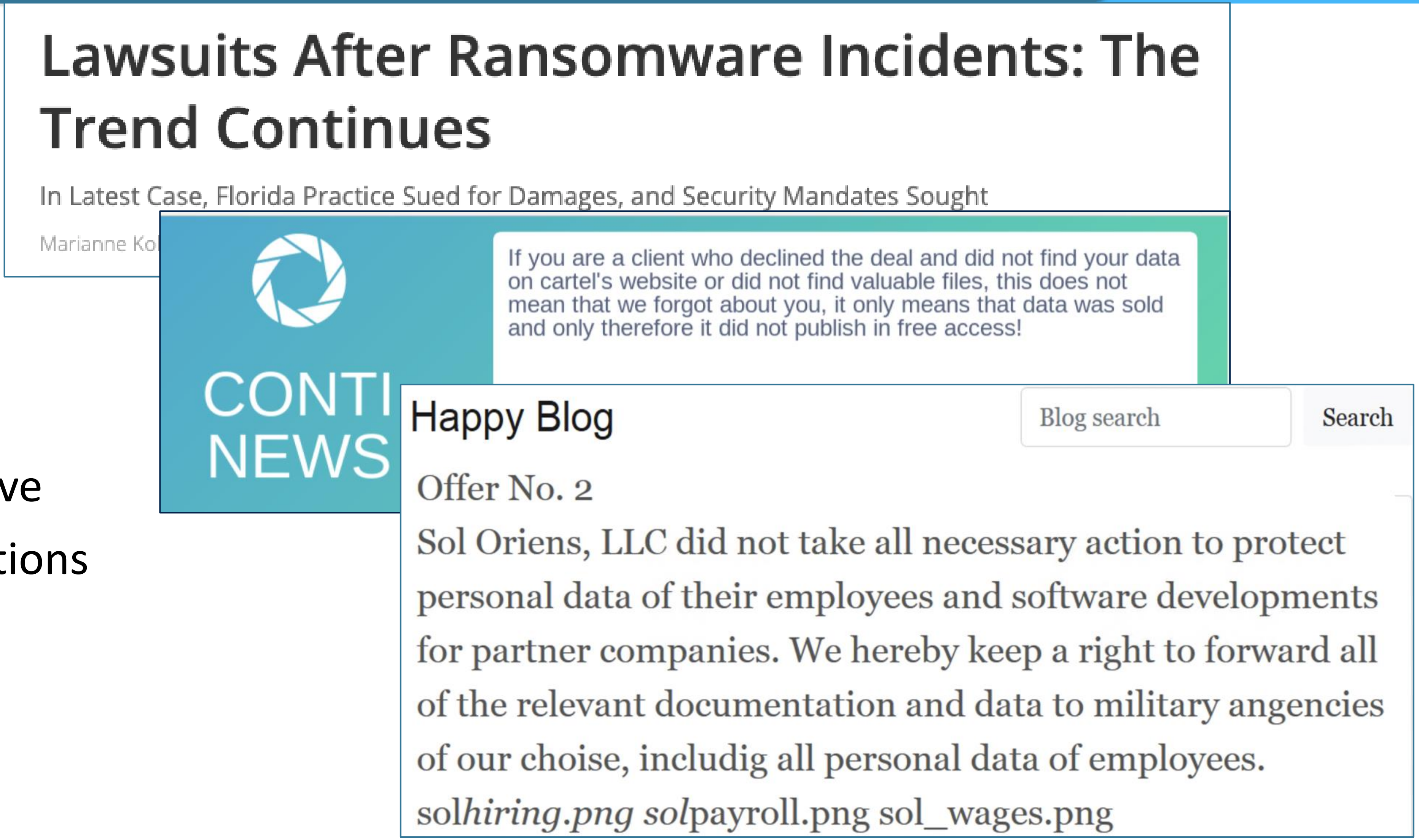
STEP 10
INCIDENT COMPLETE! FINAL DELIVERABLES & WRAP-UP

Risk of a Breach

- Financial
- Reputational
- Legal

You have to know:

- What data you have
- What laws/obligations apply



Lawsuits After Ransomware Incidents: The Trend Continues

In Latest Case, Florida Practice Sued for Damages, and Security Mandates Sought

Marianne Ko

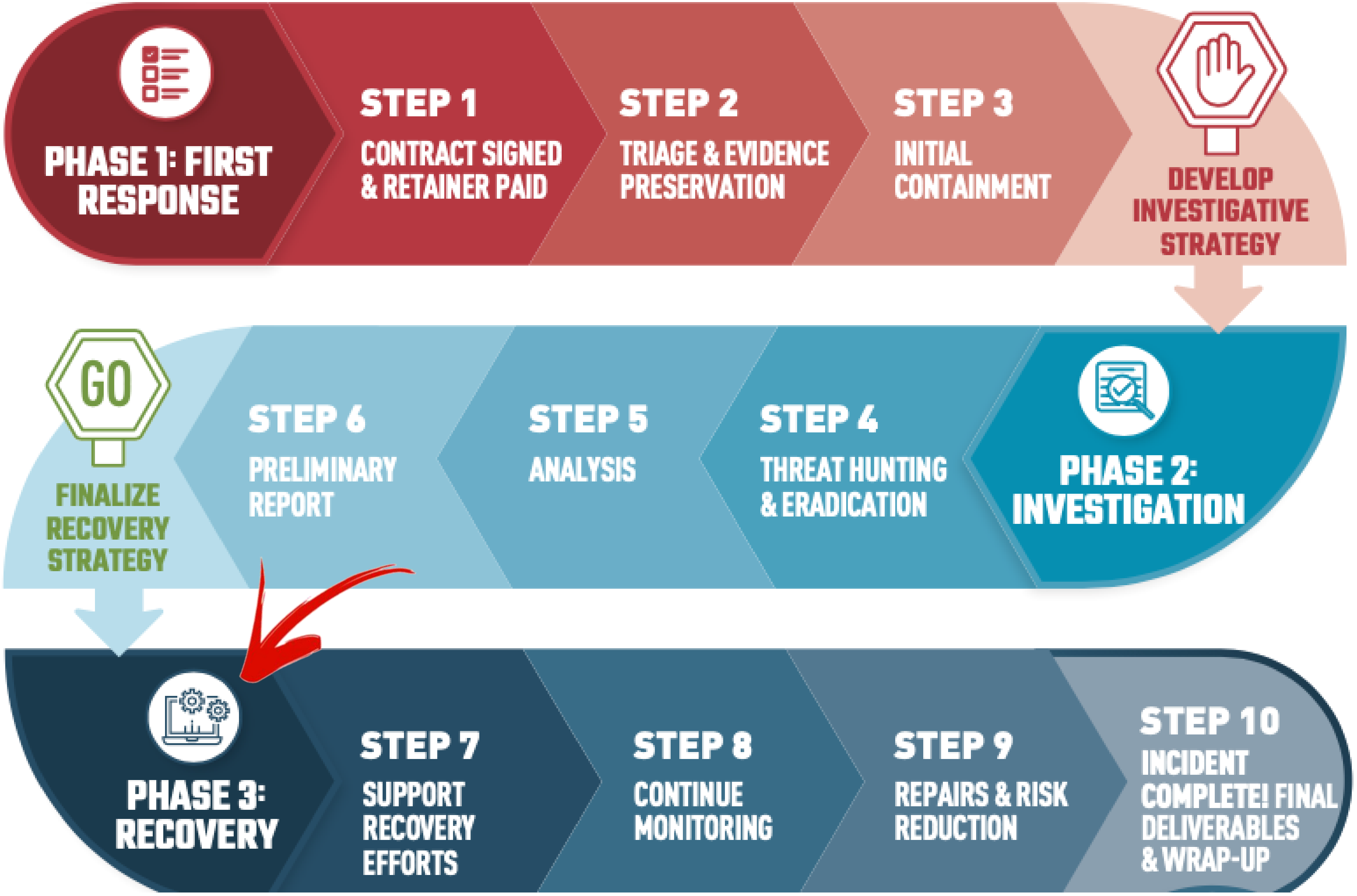
If you are a client who declined the deal and did not find your data on cartel's website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!

Happy Blog

Offer No. 2

Sol Oriens, LLC did not take all necessary action to protect personal data of their employees and software developments for partner companies. We hereby keep a right to forward all of the relevant documentation and data to military angencies of our choise, includig all personal data of employees.

sol*hiring.png sol*payroll.png sol_wages.png



PHASE 1: FIRST RESPONSE

STEP 1
CONTRACT SIGNED & RETAINER PAID

STEP 2
TRIAGE & EVIDENCE PRESERVATION

STEP 3
INITIAL CONTAINMENT

DEVELOP INVESTIGATIVE STRATEGY

PHASE 2: INVESTIGATION

STEP 4
THREAT HUNTING & ERADICATION

STEP 5
ANALYSIS

STEP 6
PRELIMINARY REPORT

GO

FINALIZE RECOVERY STRATEGY

PHASE 3: RECOVERY

STEP 7
SUPPORT RECOVERY EFFORTS

STEP 8
CONTINUE MONITORING

STEP 9
REPAIRS & RISK REDUCTION

STEP 10
INCIDENT COMPLETE! FINAL DELIVERABLES & WRAP-UP

Recovery & Restoration

- You must rebuild or clean all systems
- Antivirus helps but isn't perfect
- Monitor each system before putting back on the network
- Purchased a decryptor
- Test the decryptor (often infected)
- Doing it right takes time
  - Rushing = reinfection

Restoring Remote Access

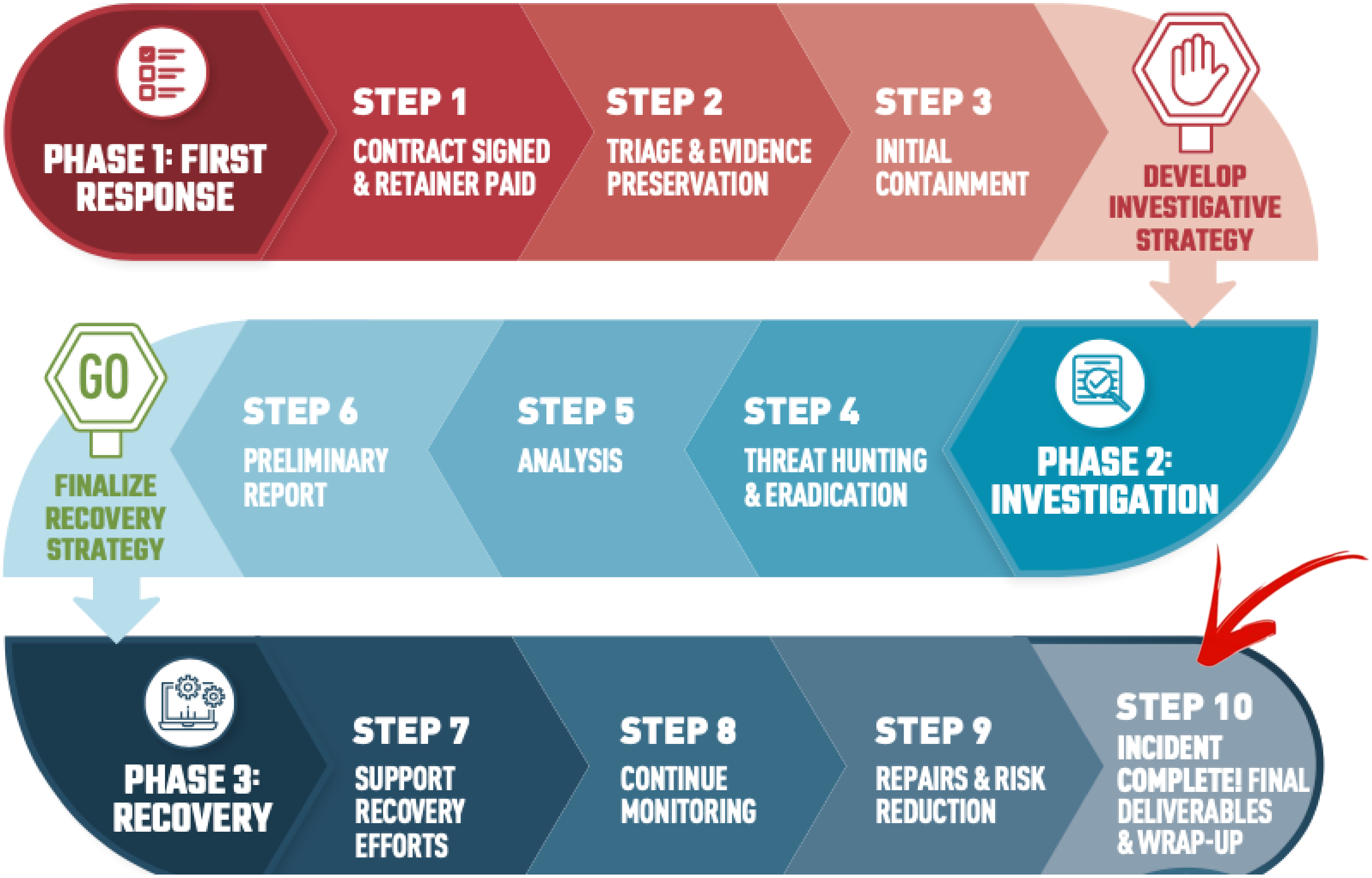
- Custom applications needed to be rebuilt
- Overseas contractors needed access
- Language barriers
- Whitelisting VPN traffic from geo-blocked areas
  - Russia
  - China
  - India
- Adjusted hours to accommodate time shifts

Your Response Needs to be FAST!

- What can slow it down?
- Communication problems
  - Language barrier between teams
- Lack of control over remote systems
- Lack of data inventory
  - What needs to be restored?
- Not knowing legal/contractual obligations
- Is it a potential breach?
- Lack of documented recovery plan

Create Response Resources in Advance

- Data Inventory
- Current List of Obligations
- Technical documentation
  - Network Map
  - Passwords
  - Dependencies
- Communications Plan
  - Out-of-band
  - After hours
  - Language



PHASE 1: FIRST RESPONSE

STEP 1
CONTRACT SIGNED & RETAINER PAID

STEP 2
TRIAGE & EVIDENCE PRESERVATION

STEP 3
INITIAL CONTAINMENT

DEVELOP INVESTIGATIVE STRATEGY

PHASE 2: INVESTIGATION

STEP 4
THREAT HUNTING & ERADICATION

STEP 5
ANALYSIS

STEP 6
PRELIMINARY REPORT

FINALIZE RECOVERY STRATEGY

PHASE 3: RECOVERY

STEP 7
SUPPORT RECOVERY EFFORTS

STEP 8
CONTINUE MONITORING

STEP 9
REPAIRS & RISK REDUCTION

STEP 10
INCIDENT COMPLETE! FINAL DELIVERABLES & WRAP-UP

Outcome

- Salesman who had been working remotely from home
- Personal computer
- Received a phishing email
- Computer became infected.
- VPN – dropped beacon & spread
- Paid $950,000
- Risk of a breach (investigation ongoing)

Conduct Response Training

- Educate onsite IT staff
- Evidence preservation & response basics
- SMBs/ non-profits
- Prevent evidence destruction
- Quick containment by first responders
- More support for widespread events

Tabletop Exercises

- Live simulated cyber events
  - Ransomware
  - BEC
  - Malware
  - Supply chain attacks & more
- Test processes, communications, etc.
- Clarify roles & responsibilities
- Align expectations & Identify gaps
- Fun & educational

Technical Training for First Responders

- NEW! On-Demand
- Cyber First Responder Class
- Ransomware Response
- Practical response training
  - Ransomware, cloud, malware & more
  - Evidence preservation, investigation, response
- Reduce risk for your organization
- Hands on labs! (Up to 80 hours or 90 days)

Now available on-demand:
https://www.LMGsecurity.com/RansomwareClass
https://www.LMGsecurity.com/CFR

Recap of Trends

- Ransomware Attacks & Demand $$
- Point & Click Ransomware Tools
- Hackers Use Legitimate Tools
- Law Enforcement Intervention
- Increased Gov Oversight
- Remote workers = new norm
- Triple extortion
- Risk of a Breach

Takeaways

- Threat Hunting is key
- Adapt Your Response Processes
- Visibility into Remote Workstations
- Create Response Resources in Advance
- Conduct Responder Training

Questions?

- Sherri Davidoff/ Matt Durrin
- training@LMGsecurity.com

@LMGSecurity

- Find us on LinkedIn

BREAKING BREACHES

Now available on-demand:
https://www.LMGsecurity.com/RansomwareClass
https://www.LMGsecurity.com/CFR