How to act / react correctly, negotiating with hackers

1. Overview of how we find ourselves in this situation.

2. Quick Run-through of a real-life incident with internal focus

3. Discoveries with my clients and work with professional K&R incident handlers and Room42

4. Current state of art ransomware incident handling with focus of 'being a good client' for professional incident handlers

https://www.linkedin.com/in/kpatrickwheeler

Today's Three 'Hats':

1. Security Architecture Domain Chief: Payments & Anti-Fraud
2. CISO
3. Educator

https://www.cyberwayfinder.com/ CWF

1. Reframing Our Point Of View

"You never once mentioned ***my*** customer"

Cyber Criminality: Skiddies to Nazguls

14-Year-Old Japanese Boy Arrested for Creating Ransomware

Tuesday, June 06, 2017 Wang Wei

Japanese authorities have arrested a 14-year-old boy in Osaka, a prefecture and large port city, for allegedly creating and distributing a ransomware malware.

CWF

… kittens, bears, pandas, african princes and how they operate …

Global Financial: Hostage Finances

So who's fault is it?

Part I

German Steel Mills: Destruction Operations / Infra

German Steel Mill Attack (2014)

German Still Mill Control System Compromise

Event: This attack comes on the heels of the German BSI report Die Lage der IT-Sicherheit in Deutschland 2014 released earlier this month revealing the cyber attack at a German steel mill in which the attackers gained access to the control system for the production facility.

Impact: This resulted in massive physical damage when the attack prevented a normal system shutdown from occurring.

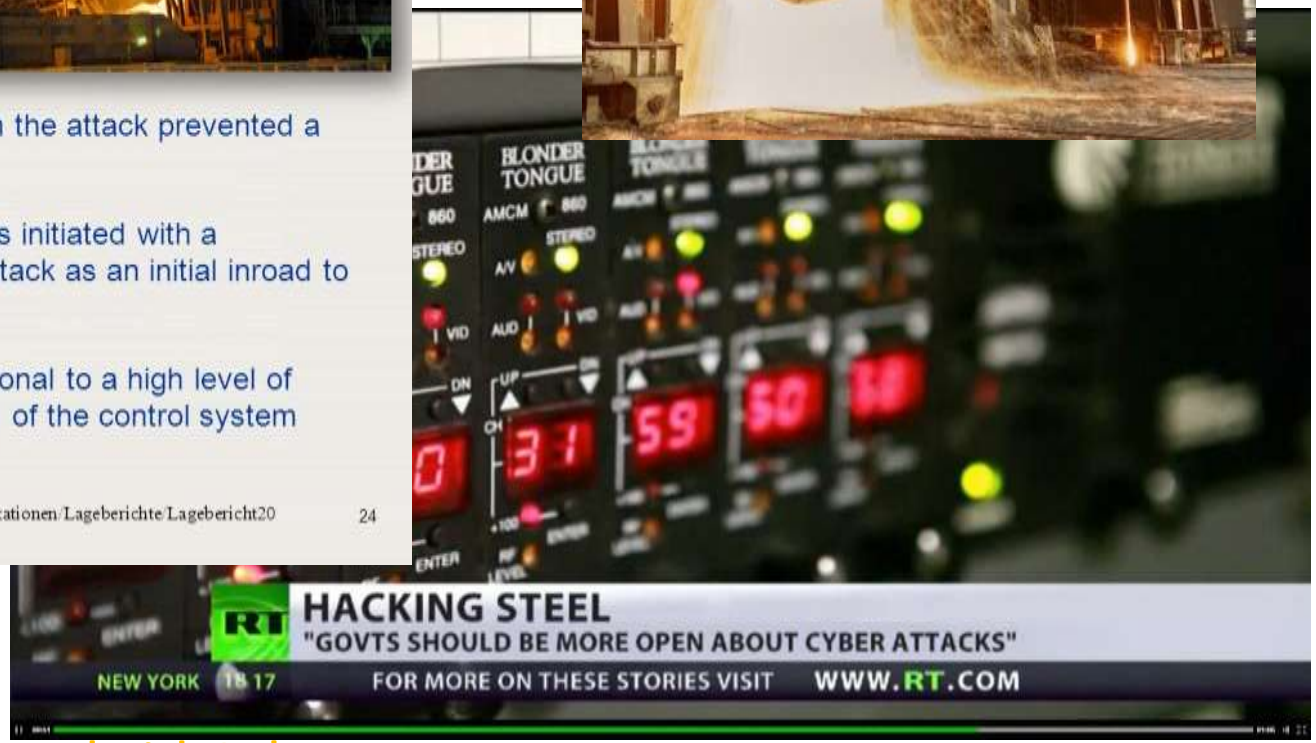
Specifics: The report indicates that the compromise was initiated with a sophisticated "spear phishing" and social engineering attack as an initial inroad to gain access to the control systems.

The report further indicates that the attacks had in additional to a high level of knowledge of IT Security, but also a good understanding of the control system operations.

IAEA

Ref:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

24



Geographically Disintermediated Hybrid Cyber-War:

…'Economic' Influence Operations

CWF

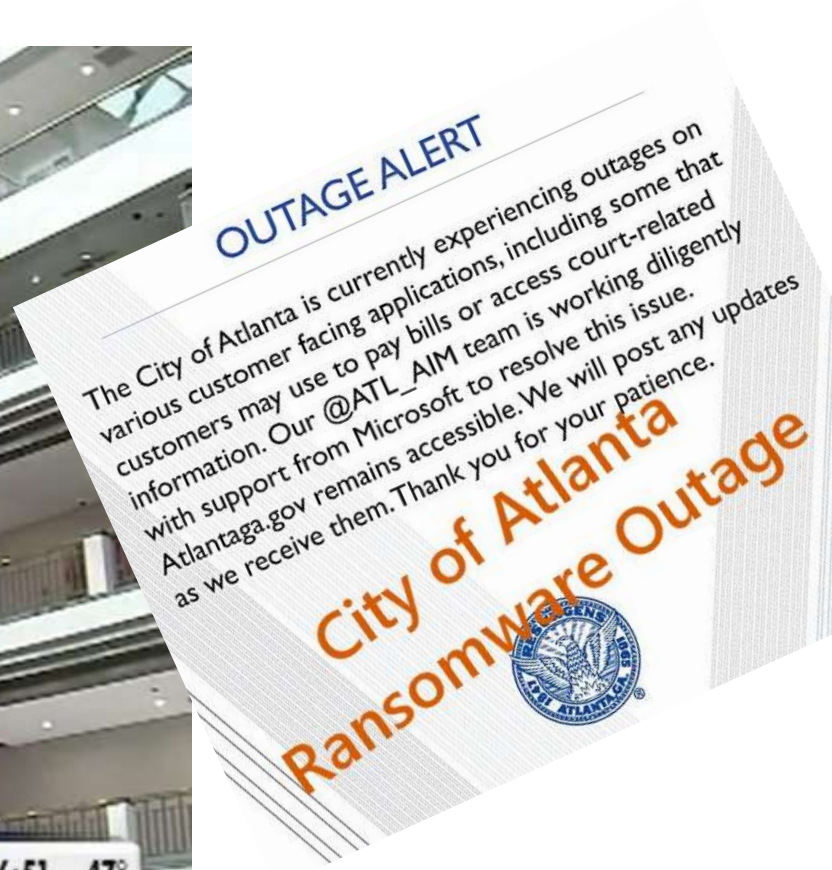
The Nation States: Hybrid warfare

Geographically Disintermediated Hybrid Cyber-War:

…Kinetic Response to Cyber Operations

CWF

United States City of Atlanta: Hostage Citizens



Geographically Disintermediated Hybrid Cyber-War:

…'False Flag' ransom attacks

CWF

Global Software Supply Chain: Destruction Technology of TRUST

not

Geographically Disintermediated Hybrid Cyber-War:

…we can all be Collateral Damage

CWF

Country-Wide Assault: ‘Messaging’

Geographically Disintermediated Hybrid Cyber-War:

…’False Flag’ ransom attacks

Costa Rica declares state of emergency over ransomware attack

Hackers crippled computer networks across multiple government agencies, including the Finance Ministry.

CWF

Retail Robbery, The ABC's: Addicts, Bikers & Carders

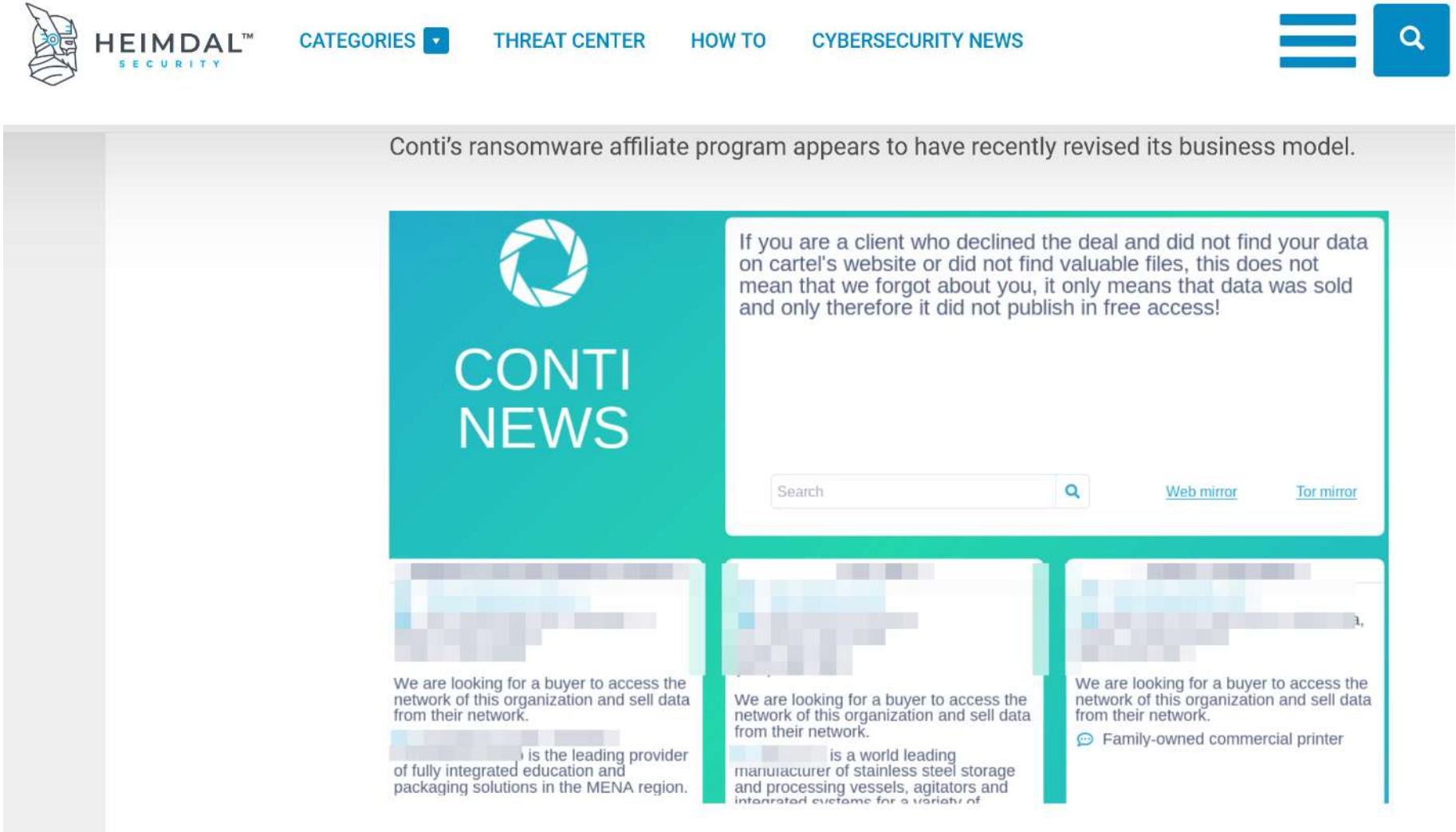
CWF

The Corporates: Office Park Industrialization

Your Enterprise / Business Model's 'Hidden' Competition

Our Enterprises are now operating in an 'Adversarial Business Climate'

The Criminal Syndicates: FaaS – Fraud as a Service



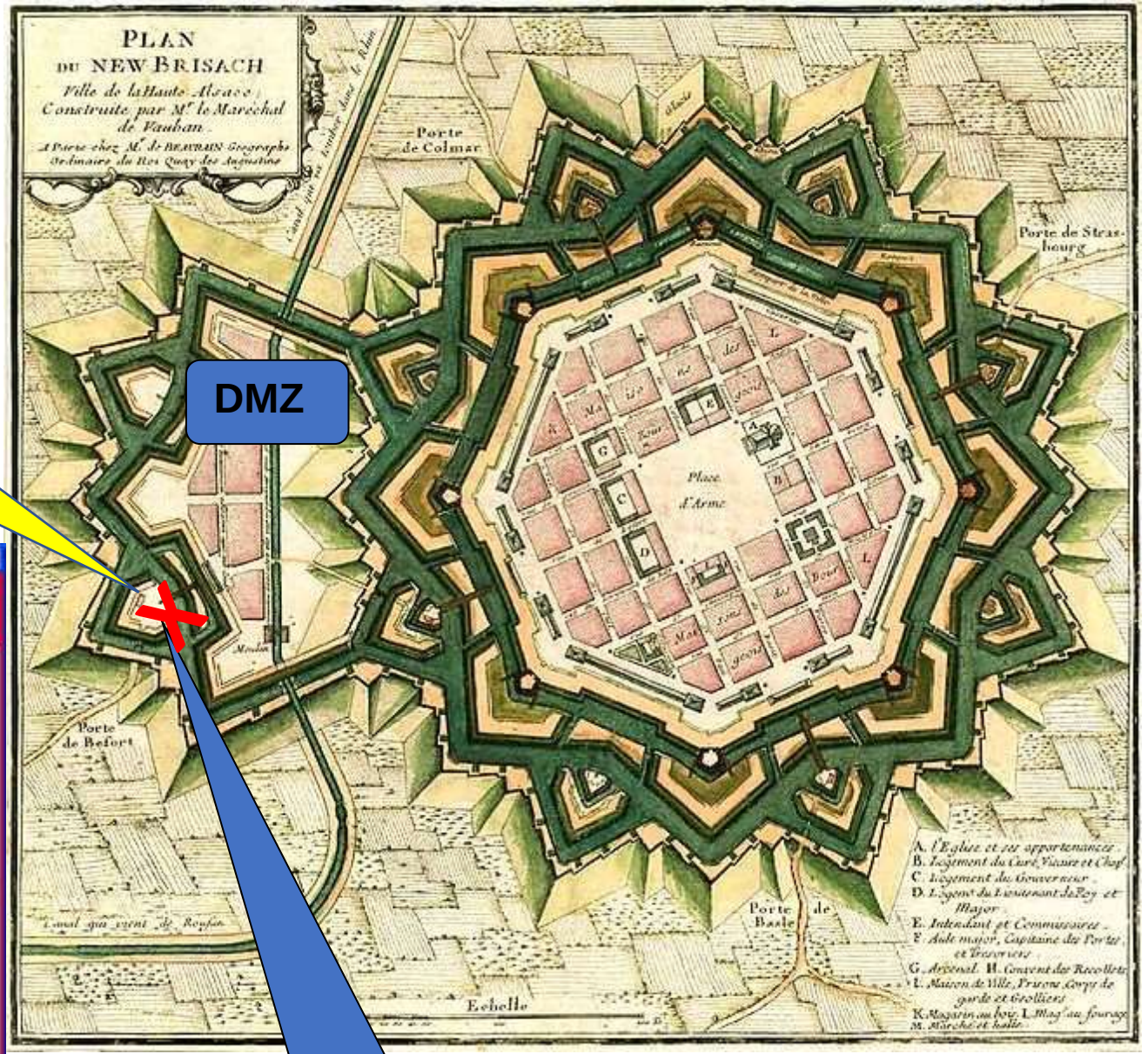
Your Enterprise / Business Model's 'Hidden' Competition …

Is innovating faster than you are …

CWF

The Nation States: and their cyber armed forces

2. CryptoLocker Attack



DMZ

Web Browsing Platform

" It was not me "

A Rude Email …

From: Long Established Business Partner
<ChiefOfRisk@ExceedinglyPrivate.com>

To: Contact Center Operative Name1,
Contact Center Operative Name2,
Contact Center Operative Name3,
Contact Center Operative Name4,
Client Support Generic Mailbox,
Customer Relationship PRIMARY Name1
Customer Relationship SECONDARY Name2

Subject: balance verification

Data for balance verification.
<<verificationfile.zip>>

Jenny's perfect day and three perfect things…

Jenny Ericson · 1st

https://www.linkedin.com/in/jenny-ericson-473662106/

…and a rude reaction

CWF

(EDC)2

Every-Day-Catella & Every-Day-Carry

Phish-Phighter (Anti-Spam/Malware Champion), Capellen, Luxembourg, Europe

In recognition of being the first to call-out and to do everything right when we received some very nasty and targeted malware attacks ... coupled with being that **single–point–of–heroism** when stuff really needs to go right ! This is to appreciate:

Jenny Ericson

For **Shining a Light!**

In recognition for shining a bright light into our processes, the shadowy landscape and recesses within our environment and ensuring our PCI compliance is a bright and shining thing ...

Congratulations and with sincere appreciation:

Timo Nurminen,
Managing Director

K.Patrick Wheeler,
Chief Information Security Officer

Samia Beladjellali,
Catella Operations Manager

CWF

The Front Line in Cybersecurity has Shifted … paraphrasing Caleb Barlow[ref] :

Companies are not prepared for a destructive attack. As an industry we primarily focus on data loss and privacy as the key metric for concern. We are often ignoring the reconnaissance prior to a destructive attack. A destructive attack is an all-of-business response that will test the resiliency of your business and we need to shift our focus to better understand this threat. If you need cardiac surgery you want a specialist and not a general practitioner. The same is true when it is your business having a "cardiac episode" from a breach. There is no tool, product or machine learning during a major incident like a hyper-skilled specialist practitioner. Crisis decision making is a skill you did not learn in business school and you cannot learn it from a book. It is a skill that has to be practiced. Learn about OODA loops, Commanders Intent and build your runbooks.

"Nothing is more deadly in a large security incident than your own organizational structure."

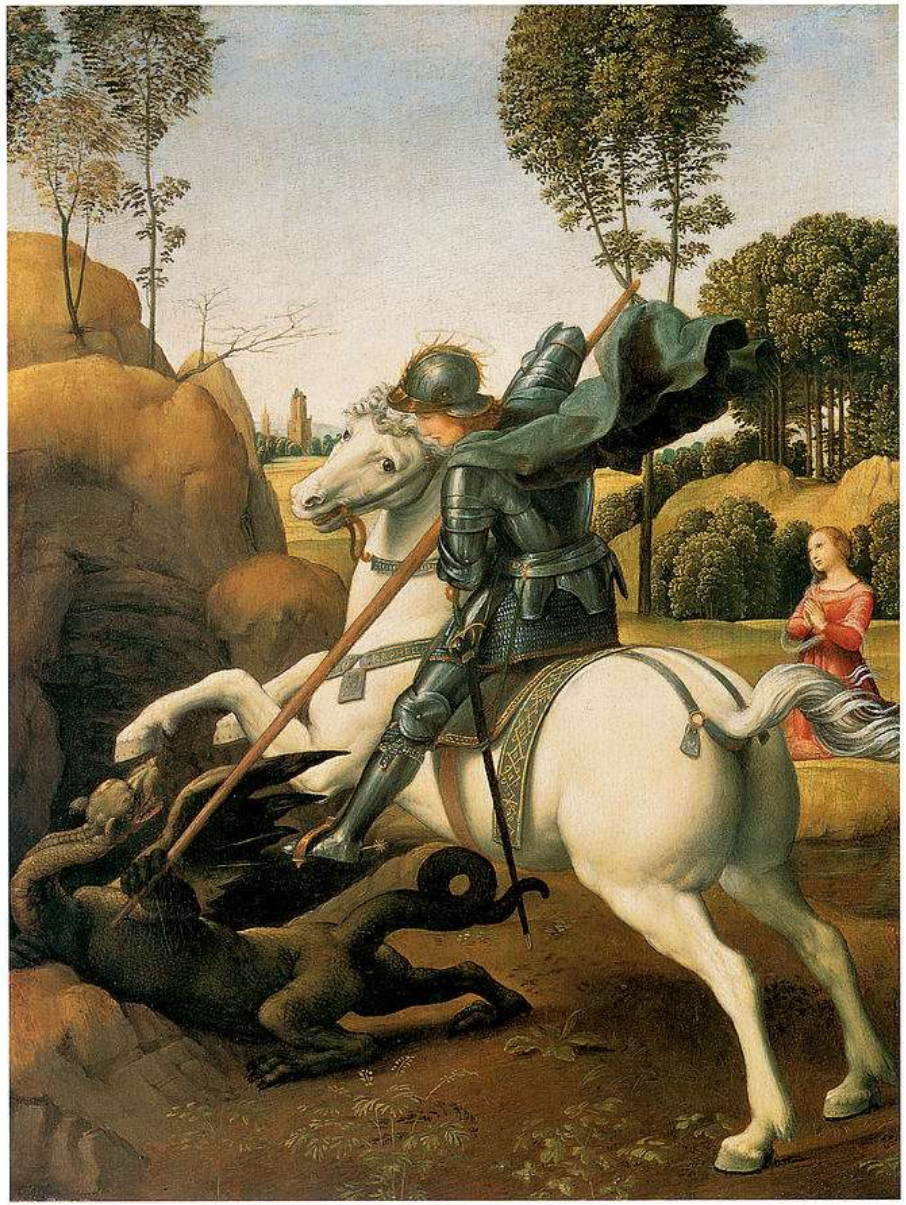
You are up against a human adversary and the only want to beat them is to make decisions faster with the people you have in the room. Not making a decision is a decision. Can you assemble the team you need in minutes (not hours) and any time day or night? Crisis communication is an art form. Do you know how to communicate with your team, investors, key customers when primary systems are down? Do you know what you would say in advance? Words matter and they can make all the difference.

CWF

3. St. George, Cybersecurity & Criminals

Right Things
Right Reasons

Right Things
Wrong Reasons



Wrong Things
Right Reasons

Wrong Things
Wrong Reasons

“…never pay!”

FBI has exemption to arrange payments to hostage-takers: U.S. sources

Mark Hosenball

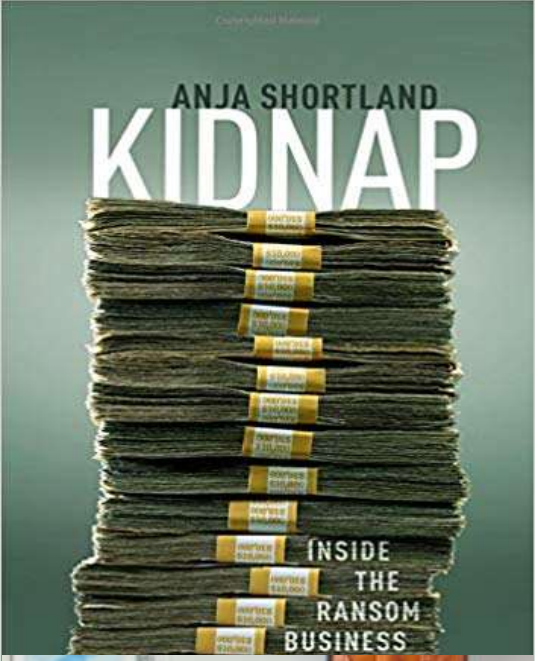
4 MIN READ

WASHINGTON (Reuters) - While U.S. policy bans federal officials from doing business with kidnappers, the FBI for years has used a secret exemption to government rules to communicate with hostage-takers and sometimes send money to them, U.S. government sources said.

Under a directive issued by President George W. Bush in 2002, the FBI can engage with suspected kidnappers, including on financial transactions, when the bureau has reason to believe it would be useful for an investigation or intelligence gathering.

The rules apply to both criminal situations inside the United States and international incidents such as kidnappings, two sources familiar with the rules said.

Global Hostage Negotiators and Critical Incident Handlers



CWF

Part II

Cyber ‘hostage’ situation
Cyber ‘critical incident’ handling

Public Forum & CWF Private Training Session cyber incident ‘negotiation’

Deep Dive Innovation & Design Think Incident Pivot

CWF

cyber escape room
cyber attack simulation
cyber range exercise

c3 Cybersecurity Competence Center LUXEMBOURG

https://room42.lu/

CWF

Cyber Critical Incident Handling

CWF

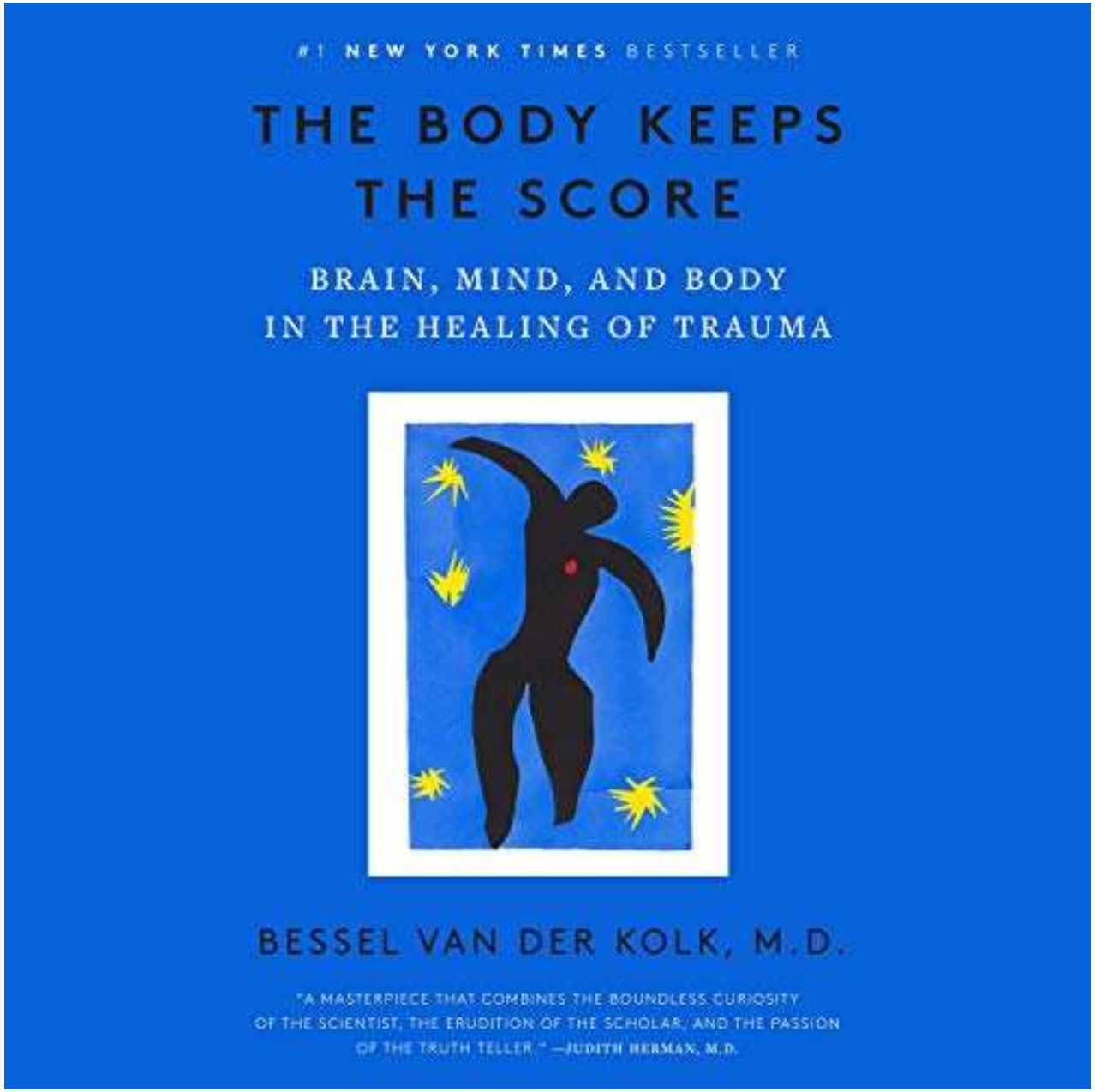
Part III


"I've learned that people will forget what you said, people will forget what you did, but people will never forget how you made them feel."
Dr Maya Angelou

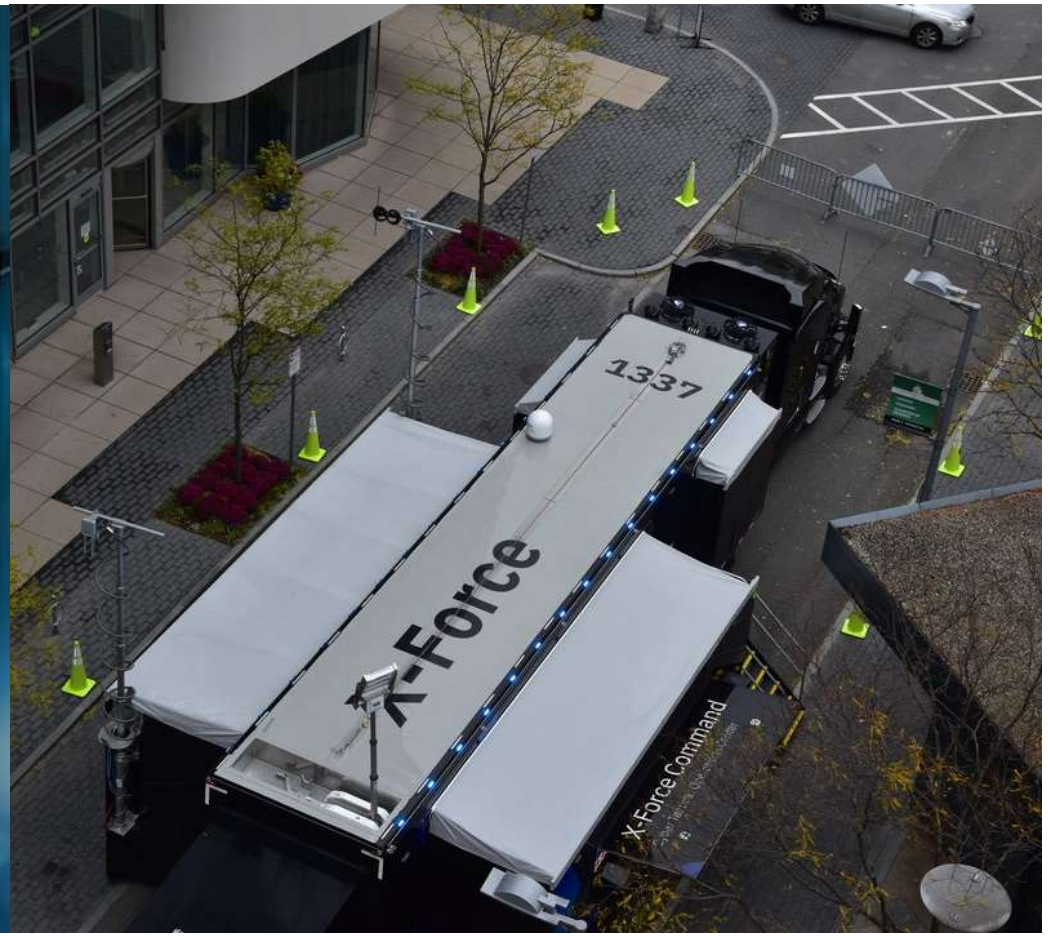
A ‘new’ muscle memory

CWF

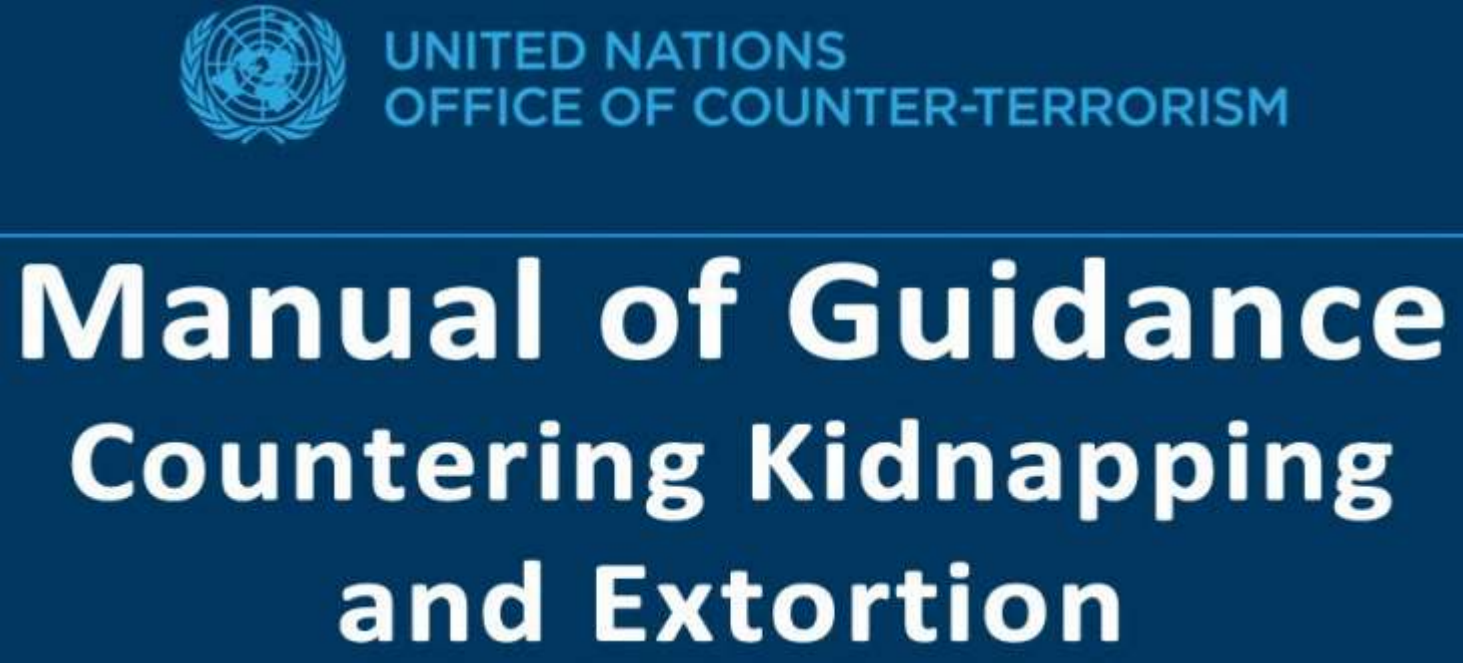
Cyber ‘Trauma’



Two examples of ‘trauma’ inducement



CWF



12.2 Recovered hostage

Once a hostage is recovered, the lead officer must give consideration to the following:

- Immediate medical care
- Operational hot debriefing (lessons learned review held immediately after the recovery)
- Removing the hostage(s) to a secure location away from to the media, if possible
- Specialist psychological support for the hostage(s)
- Crime scene management at any identified stronghold or other location where the hostage may have been kept
- Appointing a family liaison officer to support the released hostage
- Witness protection assessment, particularly if the case is related to a criminal vendetta
- Developing a strategy to interview and debrief the hostage

An important question for the hot debriefing of the hostage or hostages could be whether or not they had seen or heard any other potential hostages being held at the same location at the same time.

Sometimes the hostage, the victim and the family members affected will not need, want or initially request any post incident support. In addition to law enforcement support there are also international charitable organizations that have recognized family support groups, such as Hostage International.

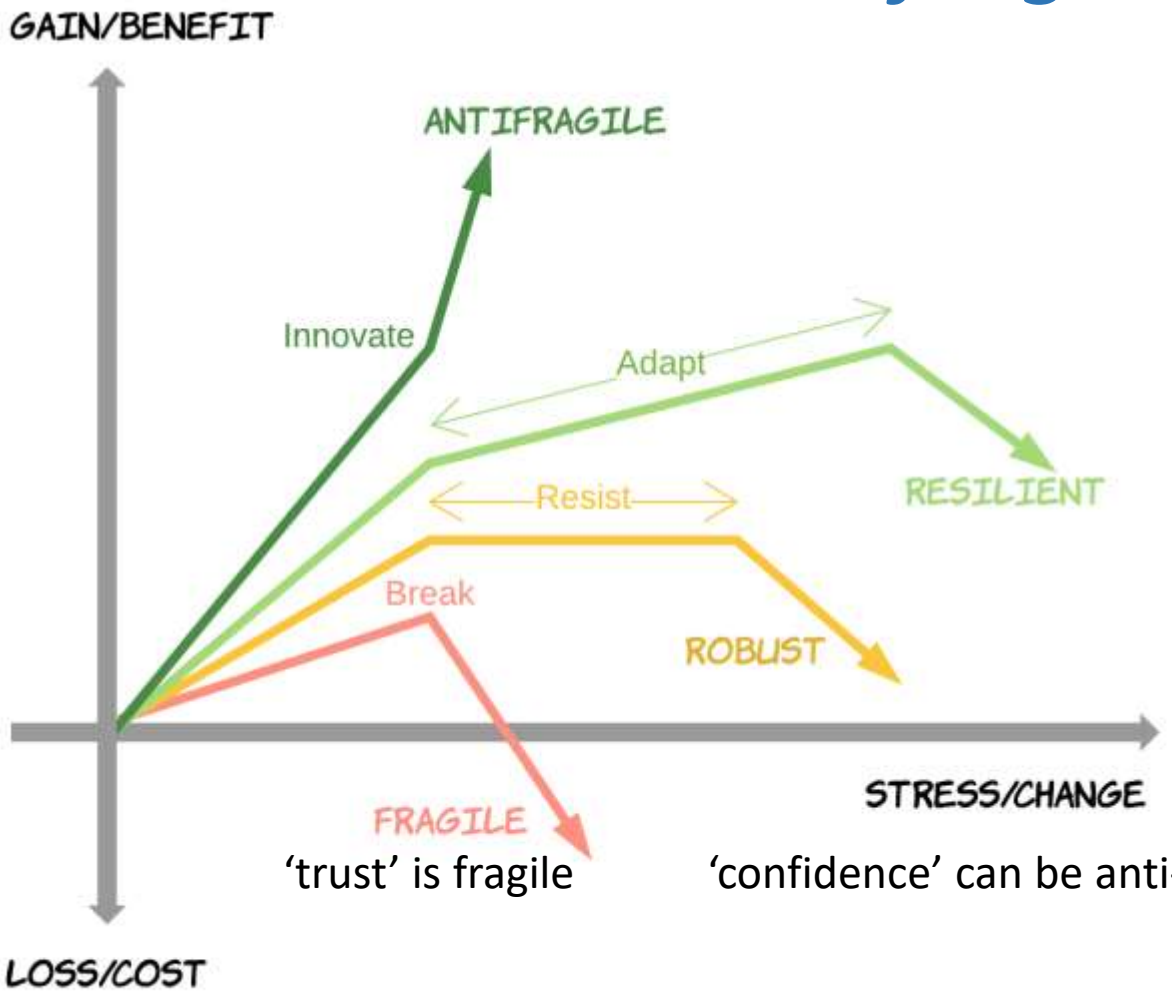
In addition, once released it is only natural that the hostage will want to be reunited with loved ones as soon as possible. … has to be managed with great sensitivity and in accordance with the wishes of all concerned, while being balanced with the needs of the prosecution

4. Look Where You Are Going …

What is our ‘Definition of Done’ for a Critically Destructive Cyber Incident?

antifragility

“… asked Duane, who retired from RSA…, at what point he considered RSA’s breach truly over: Was it the morning after he made the lonely decision to unplug a chunk of the company’s network? Or when the NSA, the FBI, Mandiant, and Northrop had wrapped up and left? “Our view was that the attack wasn’t ever over”



‘trust’ is fragile

‘confidence’ can be anti-fragile

Partners | About the Project | English

NO MORE RANSOM

Home | Crypto Sheriff | Ransomware: Q&A | Prevention Advice | Decryption Tools | Report a Crime

About the Project

Law enforcement and IT Security companies have joined forces to disrupt cybercriminal businesses with ransomware connections.

The "No More Ransom" website is an initiative by the National High Tech Crime Unit of the Netherlands' police, Europol's European Cybercrime Centre, Kaspersky and McAfee with the goal to help victims of ransomware retrieve their encrypted data without having to pay the criminals.

An official website of the United States government Here's how you know

STOP RANSOMWARE

RESOURCES | NEWSROOM | ALERTS | REPORT RANSOMWARE | CISA.GOV

Stop Ransomware > Resources > Ransomware Guide

Resources

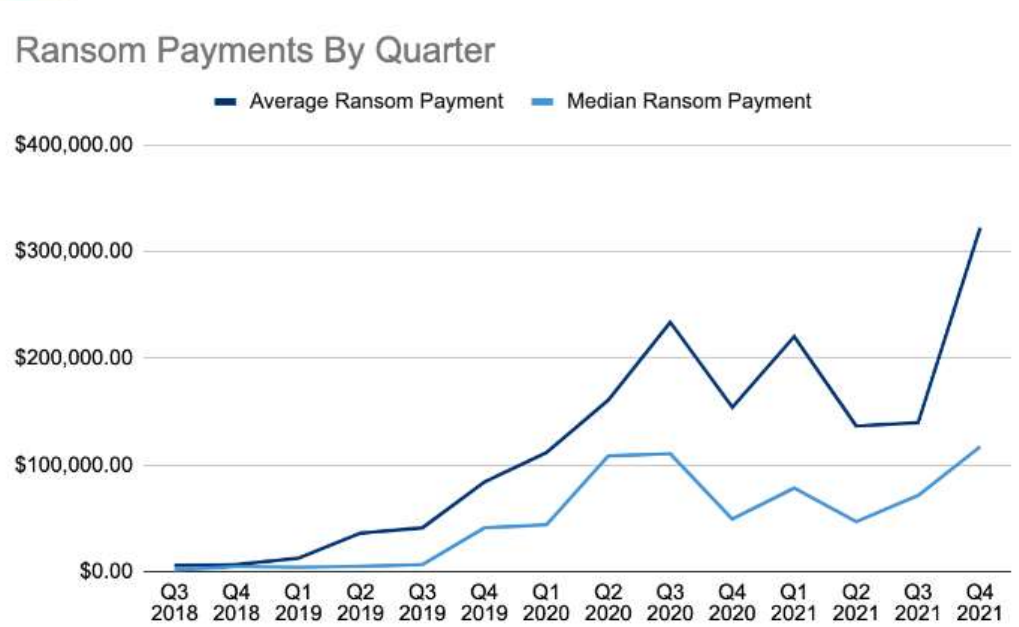
- Fact Sheets & Information
- Public Safety Emergency Communications Resources
- Ransomware 101
- Ransomware Guide

RANSOMWARE GUIDE

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems tha them unusable. Malicious actors then demand ransom in exchange for decryption. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) gove entities and critical infrastructure organizations.

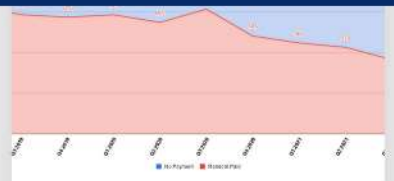
Ransomware incidents can severely impact business processes and leave organizations without the data they n operate and deliver mission-critical services. Malicious actors have adjusted their ransomware tactics over time include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly n shaming victims as secondary forms of extortion. The monetary value of ransom demands has also increas

CWF



COVEWARE

Coveware has been featured in the Forrester Ransomware Incident Response Report. Click here to read more.



Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting

Less Victims of Ransomware are Paying, even as Cybercriminals Shift from Big Game to Big Shame Hunting

Read More →

May 3, 2022

How the Russian/Ukraine war may lead to an explosion in Ransomware attacks

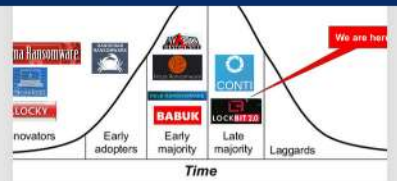
The long term impact of sanctions on Russian unemployment has the potential to increase the volume of future Ransomware attacks.

Read More →

Law enforcement pressure forces ransomware groups to refine tactics in Q4 2021

Ransomware as a service groups are shifting their tactics as enterprises become harder targets, and law enforcement pressure mounts.

Read More →



Ransomware as a Service Innovation Curve

As the Ransomware attacks continue, the direction and growth of the RaaS model is following a traditional innovation trajectory.

Read More →

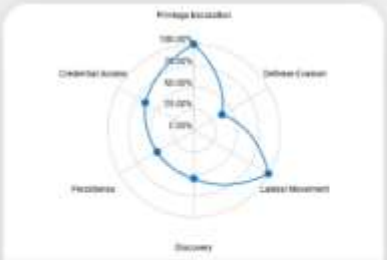
Jan 27, 2022

Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021

Ransomware attacks continued to proliferate in Q3 as governments and law enforcement ratchet up the pressure of the cyber extortion economy

Read More →

Oct 21, 2021



Q2 Ransom Payment Amounts Decline as Ransomware becomes a National Security Priority

Ransomware payment amounts declined in Q2 as several high profile attacks escalated the attention of the US government and law enforcement.

Read More →

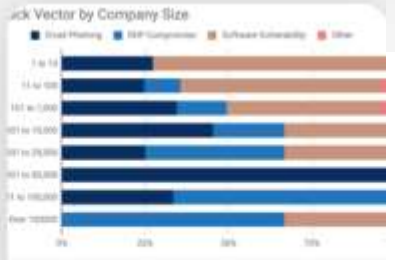
Jul 23, 2021

What We Can Learn From Ransomware Actor "Security Reports"

Ransomware Actors Explain in their Own Words How to Become an Expensive Target through security reports written to victims.

Read More →

Jun 24, 2021



Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound

Ransomware attacks continued to proliferate in Q1 2021 as several common but unpatched software vulnerabilities created a fresh supply of compromised network access to ransomware affiliates.

Read More →

Apr 26, 2021

Takeaway

Have Friends.

Many.