PESU Center for
Information Security,
Forensics and
Cyber Resilience

Welcome to

PES University

Ring Road Campus, Bengaluru

PESU Center for
Information Security,
Forensics and
Cyber Resilience

Applied Cryptography

UE22CS342AA4

Prof. Prasad Honnavalli, Prof. Indu R, Dr. Swetha & Dr. Geetha

Lecture 28

Emergency Exit

Assembly Point

Washroom

No Chatting

Phones on silent

No Sleeping

Disclaimer

- *This presentation is purely educational.*
- *The views expressed by the presenter is not representation of any organization.*
- *The views are based on professional experience of the presenter and no liability is accepted by the presenter in the event of any potential or perceived losses resulting from this presentation.*

A Note on Security

☞ In this course, you will be exposed to information about security problems and vulnerabilities with computing systems and networks.

☞ To be clear, you are not to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network without the express consent of the owner.

☞ In particular, you will comply with all my instructions when doing the labs.

- My instructions are in consonance with applicable laws of India and PES University policies.
- If in any doubt, please consult your professor!

☞ Any violation is at **YOUR RISK!**
And may result in severe consequences.

Ransomware Attack at Colonial Pipeline

The case

- ☞ Issues relating to cybersecurity raised by the Colonial Pipeline ransomware attack are not unique:
  - ● But the scope and publicity of the attack makes it stand out.

- ☞ The case explores the intersection of technical and managerial aspects of cybersecurity issues with added focus on Ransomware payment and response to a highly publicized event impacting the public at large.

Objectives

- ☞ Understand how data encryption works and understand how adversaries use this technique for malicious purposes
  - ● such as Ransomware and Data Destruction.
  - ● Denial of Service
- ☞ Understand their use cases - Financial or State Actors
- ☞ Understand how to detect and how to defend against attacks using Data Encryption.

Outcomes

☞ Apply MITRE ATT&CK framework i.e. the Tactics, Techniques and Common Knowledge to analyse the Ransomware attacks on various OS platforms, in particular **T1486**

☞ Analyze the critical and central role of Cryptography and misuse/dual use of legitimate system calls to avoid detection by Malicious actors

☞ Apply the Framework to prepare organizations to respond to Cyber Incidents

☞ Understand the Role of stakeholder and senior leadership in dealing with Ransomware attacks

What is relationship of Ransomware and Cybersecurity?

☞ What is Cryptography?

☞ What is relation of Ransomware and Cryptography?

☞ How does Encryption facilitate ransomware?

☞ Why is access to “the key” so critical?

MITRE ATT&CK

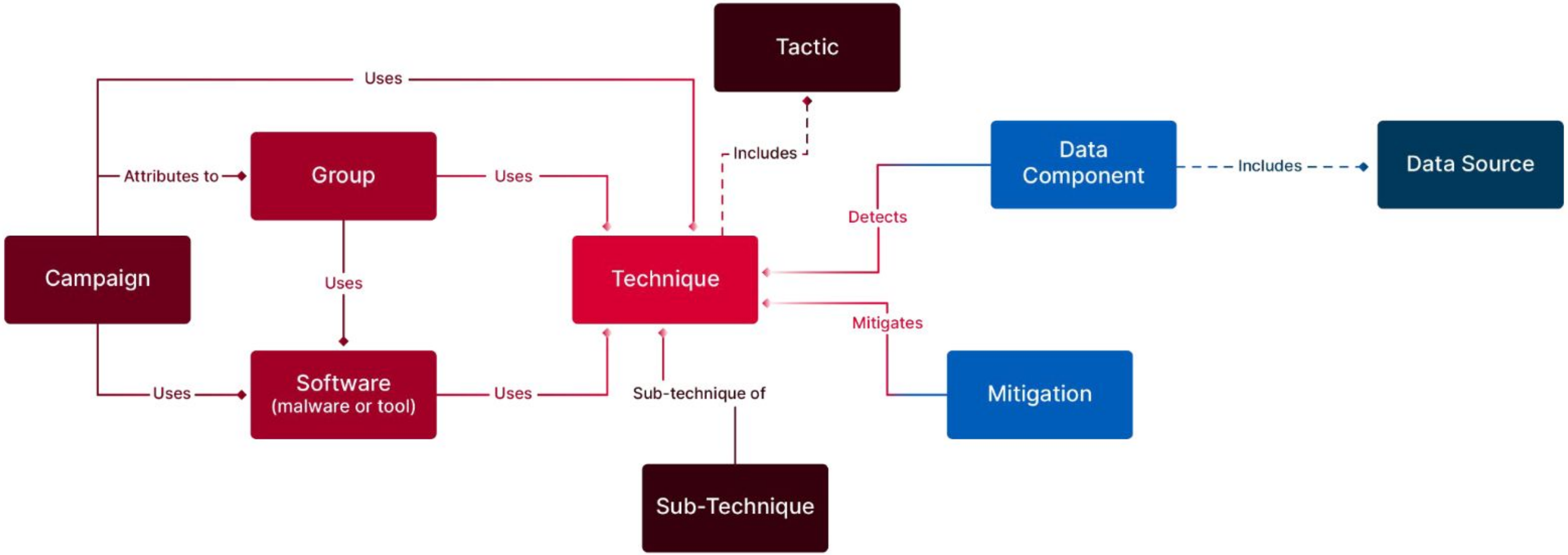
Adversarial **T**actics, **T**echniques **&** **C**ommon **K**nowledge

MITRE ATT&CK

https://attack.mitre.org/matrices/enterprise/.

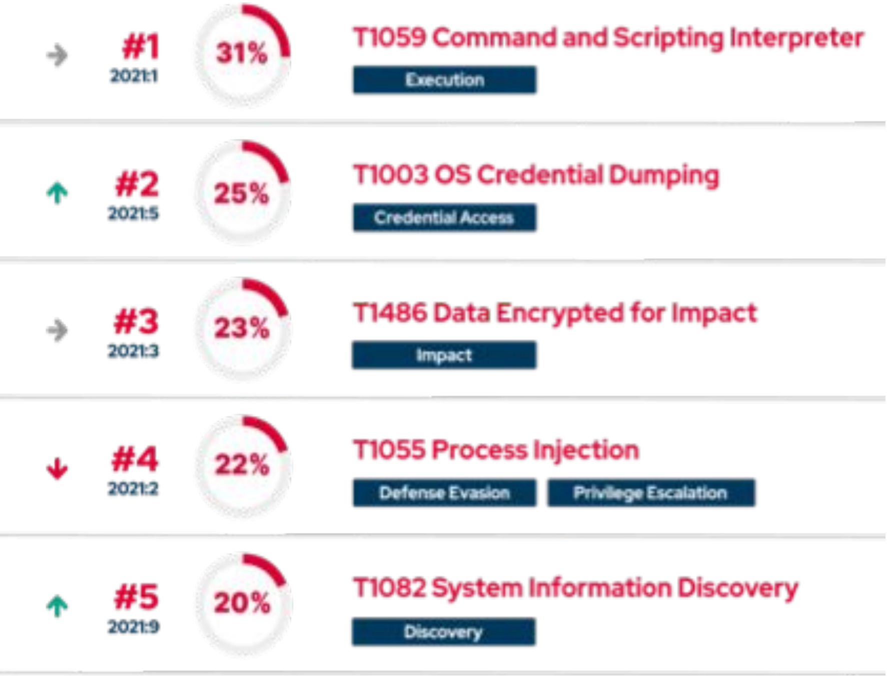
The Top 10 Most Prevalent MITRE ATT&CK Techniques Used by Adversaries

The MITRE ATT&CK Framework



- ☞ In the life-cycle of their attacks, cyber threat groups use ATT&CK "Techniques" to achieve their goals which are classified as "Tactics" in the framework.
- ☞ The MITRE ATT&CK identifies certain malware or tools to execute adversaries' techniques as "Software".
- ☞ As a comprehensive knowledge base, the MITRE ATT&CK framework provides valuable information about each technique and how to mitigate with "Mitigation" and "Data Source".

Top 10 MITRE ATT&CK Techniques

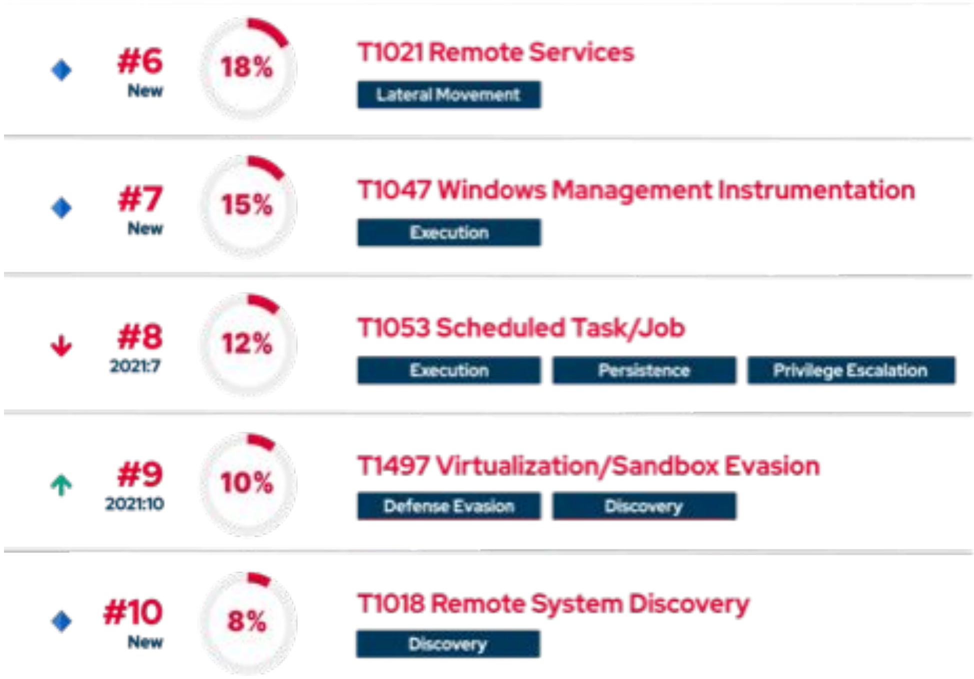


→	#1 2021:1	31%	T1059 Command and Scripting Interpreter	Execution
↑	#2 2021:5	25%	T1003 OS Credential Dumping	Credential Access
→	#3 2021:3	23%	T1486 Data Encrypted for Impact	Impact
↓	#4 2021:2	22%	T1055 Process Injection	Defense Evasion Privilege Escalation
↑	#5 2021:9	20%	T1082 System Information Discovery	Discovery

Highlighting Lateral Movement of Adversaries

- The most significant insight from this year's report is that attackers are increasingly leveraging malware to perform Lateral Movement.
- Lateral Movement is a tactic that attackers use to move from one compromised system in a network to another, helping them to further their objectives.

Top 10 MITRE ATT&CK Techniques



◆	#6 New	18%	T1021 Remote Services	Lateral Movement
◆	#7 New	15%	T1047 Windows Management Instrumentation	Execution
↓	#8 2021:7	12%	T1053 Scheduled Task/Job	Execution Persistence Privilege Escalation
↑	#9 2021:10	10%	T1497 Virtualization/Sandbox Evasion	Defense Evasion Discovery
◆	#10 New	8%	T1018 Remote System Discovery	Discovery

Lateral Movement on the Rise:

Attackers Utilize New as well as Tried and Tested Techniques

☞ Attackers are increasingly using techniques to perform Lateral Movement, a tactic to move from one compromised system in a network to another.

- Command and Scripting Interpreter and OS Credential Dumping, are widely used
- New techniques are used such as Remote Services, Remote System Discovery
- To discover remote systems, execute commands on remote systems, and obtain account credentials.

Abuse of Remote Discovery and Access:

Attackers Leverage Windows, Linux, and macOS Built-in Tools

☞ Remote System Discovery and Remote Services

- These techniques involve abusing built-in tools and protocols in operating systems, such as net, ping, RDP, SSH, and WinRM for malicious purposes.

- This allows attackers to gather information about targets, including Windows, Linux, and macOS systems in a compromised network, and move laterally throughout the network without being detected by security controls.

- This trend indicates that attackers are increasingly utilizing legitimate remote discovery and access tools and services.

Uncovering the Dark Side of Legitimate Tools:

Adversaries Are Weaponizing Legitimate Software in Cyberattacks

☞ Adversaries prefer using legitimate tools over custom-developed ones.

- This is highlighted by the most common technique, T1059 Command and Scripting Interpreter, which involves the abuse of legitimate interpreters such as PowerShell, AppleScript, and Unix shells to execute arbitrary commands.

- Other examples of legitimate tools that are commonly abused by adversaries include utilities for OS Credential Dumping, System Information Discovery, Remote Services, WMI, Scheduled Task/Job, and Remote System Discovery.

Ransomware Remains Rife:

Data Encryption is a Top Threat

- ☞ Data Encrypted for Impact has maintained its position as the third most commonly used technique by adversaries.
- ☞ This technique, exhibited by nearly a quarter of all malware analyzed, encrypts files and highlights the ongoing threat of ransomware to organizations.

Malware Continues to Evolve Rapidly:

The Rise of Multi-faceted Tactics in Cyber Attacks

- ☞ On average, malware uses 11 different TTPs (Tactics, Techniques and Procedures).
- ☞ One-third of malware (32%) leverages more than 20 TTPs, and
- ☞ One-tenth of malware employs more than 30 TTPs.
- ☞ Malware developers behind these attacks are highly sophisticated.
  - They have likely invested significant resources into researching and developing a wide range of techniques for evading detection and compromising systems.

T1486. Data Encrypted for Impact

☞ Adversaries utilize advanced encryption algorithms to render their victim's data useless.

☞ In ransomware attacks, adversaries hold the decryption key for ransom with the hopes of financial gain.

☞ The pattern in the infamous ransomware attacks shows that adversaries use multiple encryption algorithms for speed, security, and efficiency.

T1486. Data Encrypted for Impact

☞ In order to efficiently carry out ransomware attacks, threat actors will often utilize symmetric encryption, which allows for faster encryption and exfiltration of the victim's files.

☞ Although symmetric encryption is faster and more efficient, it has two main limitations:

☞ **Key distribution problem:**

- The encryption key is the only thing that ensures privacy in symmetric encryption, and the secrecy of the encryption key is paramount for the confidentiality of the encrypted data.
- If the encryption key is revealed to a third party while in transit or on disk, encrypted files can be decrypted easily.
- Therefore, distributing the encryption key is a challenge that ransomware operators need to overcome.

T1486. Data Encrypted for Impact

☞ **Key management problem:**

- Using different encryption keys for different encryption operations is a common best practice for symmetric encryption.
- However, this practice creates a key management problem as the number of encryption keys grows for each encryption operation.
- For ransomware, threat actors must create different encryption keys for each infected host and keep all the keys secret; otherwise, victims can decrypt all the data using the revealed key.

☞ Ransomware operators use asymmetric encryption to solve symmetric encryption's key distribution and management problems.

- Although slower than its alternative, asymmetric encryption allows ransomware operators to leave their public key in the infected hosts without worry since victims cannot decrypt their files without the private key.

T1486. Data Encrypted for Impact

- ☞ In a typical ransomware attack, ransomware payload encrypts files with a symmetric encryption algorithm using a secret key.
- ☞ Then, the payload encrypts the secret key with a public key that is custom created for the infected host.
- ☞ This combined use of both encryption algorithms is called the **hybrid encryption approach**.
- ☞ It helps ransomware operators to leverage the fast encryption performance of symmetric encryption while using the strong security of asymmetric algorithms.

Symmetric encryption:

☞ Symmetric encryption algorithms use the same key for encryption and decryption processes. This key is also known as the secret key.

☞ AES, Blowfish, ChaCha20, DES, 3DES, and Salsa20 are some popular examples of symmetric algorithms.

☞ Symmetric Encryption – Advantages

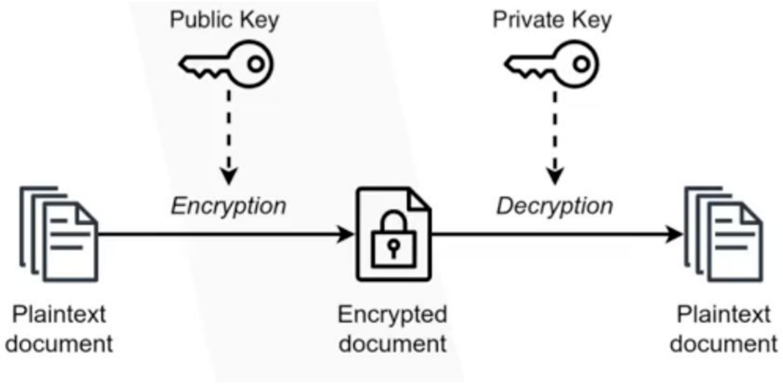
- Is faster
- Suited for bulk encryption
- Requires less storage space

☞ Symmetric Encryption – Disadvantages

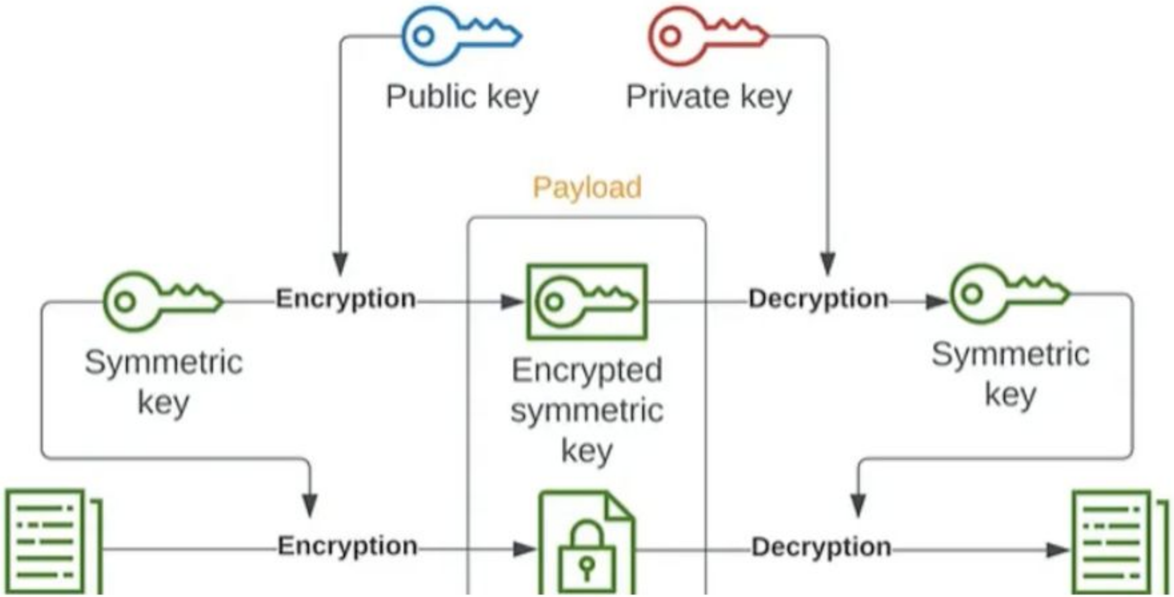
- Key distribution problem
- Key management problem

Asymmetric encryption:

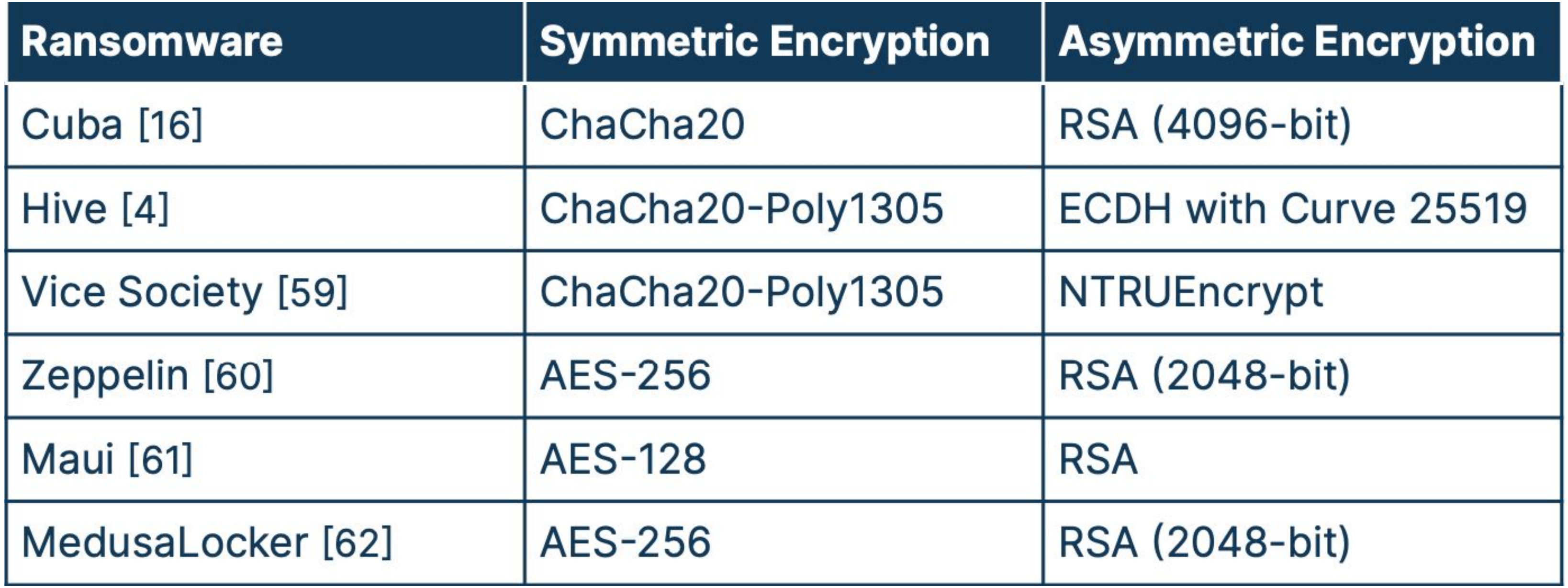
- ☞ Asymmetric encryption algorithms use a key pair called public and private keys for encryption and decryption, respectively.
- ☞ These algorithms are also known as public key encryption. RSA, ECDH, and ECDSA are popular asymmetric encryption algorithms.
- ☞ Asymmetric Encryption – Advantages
  - Solves Key distribution problem
  - Solves Key management problem
  - Hence considered to offer higher level of security
- ☞ Asymmetric Encryption – Disadvantages
  - Slower than symmetric encryption
  - Requires more storage space



Hybrid Encryption



Encryption algorithms used by ransomware



Ransomware	Symmetric Encryption	Asymmetric Encryption
Cuba [16]	ChaCha20	RSA (4096-bit)
Hive [4]	ChaCha20-Poly1305	ECDH with Curve 25519
Vice Society [59]	ChaCha20-Poly1305	NTRUEncrypt
Zeppelin [60]	AES-256	RSA (2048-bit)
Maui [61]	AES-128	RSA
MedusaLocker [62]	AES-256	RSA (2048-bit)

Source: CISA Alerts 2022

Data Destruction - wiper malware

☞ Data destruction attacks aim to render the files useless as quickly as possible

☞ Adversaries often employ symmetric encryption algorithms to achieve this goal

☞ Let's take a look at Hermetic Wiper malware as an example.

- In February of 2022, Russian state sponsored threat actors targeted Ukrainian critical infrastructure with a wiper malware called Hermetic Wiper.
- This malware makes any infected Windows system in operable by encrypting and corrupting the Master Boot Record.
- After a successful Hermetic Wiper attack, infected systems cannot reboot and are effectively rendered useless.

☞ During its attack, Hermetic Wiper also encrypts any file under user directories and log files to prevent incident response teams from recovering any user data or e vidence of the attack.

Data Destruction - wiper malware

- In 2022, the Russian invasion of Ukraine brought attention to the fact that state-sponsored threat actors also utilize encryption for nefarious purposes, such as destroying victims' data or distracting them from the actual attack.
- This serves as a reminder that encryption is not only prevalent in ransomware attacks but can also be weaponized by state actors.
- In data destruction attacks, adversaries irreversibly encrypt files with keyless encryption techniques and leave their victims without a way to decrypt their files.
- Here are some of the recent wiper malware examples:
  - RuRansom
  - WhisperGate
  - HermeticWiper
  - MeteorExpress
  - Exmatter

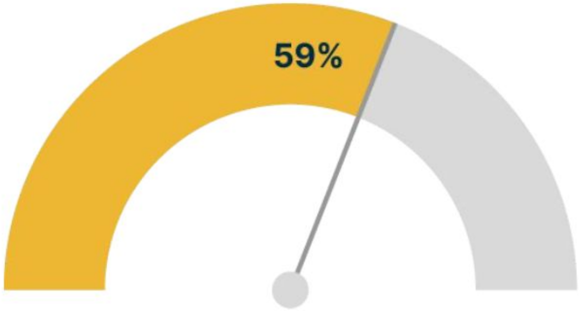
Security teams can monitor these API functions for ransomware detection

- ☞ Built-in Windows APIs allow users to utilize both symmetric and asymmetric encryption algorithms such as DES, 3DES, RC2, RC4, and RSA.
- ☞ Adversaries abuse this feature in their data encryption operations.
- ☞ For example, BlueSky and Nefilim abuse Microsoft's Enhanced Cryptographic Provider to import cryptographic keys and encrypt data with the following API functions.
  - Initializing and connecting to the cryptographic service provider: CryptAcquireContext
  - Calculating the hash of the plain text key: CryptCreateHash, CryptHashData
  - Creating the session key: CryptDeriveKey
  - Encrypt data: CryptEncrypt
  - Clear tracks: CryptDestroyHash, CryptDestroyKey, CryptReleaseContext
  - Ransomware operators often query unique information to generate a unique identifier for infected hosts. Unique identifiers allow them to track infected hosts and encryption/decryption processes. For example, Zeppelin ransomware queries the MachineGUID value from the following registry key, as it is a unique identifier for each Windows host.
- ☞ Registry: "HKLM\SOFTWARE\Microsoft\Cryptography" Key: "MachineGUID"

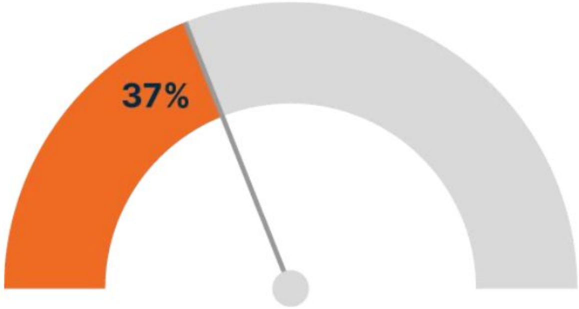
The State of Threat Exposure Management

Threat exposure management programs

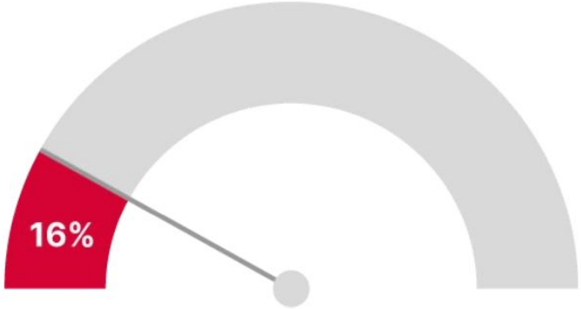
- On average security teams can only prevent just over half of all attacks (59%).
- Detection scores are even lower.
- Companies are only logging 1 in 3 successful attacks (37%) and
- Creating alerts for less than 1 in 6 (16%).



Only 59% of attacks were prevented



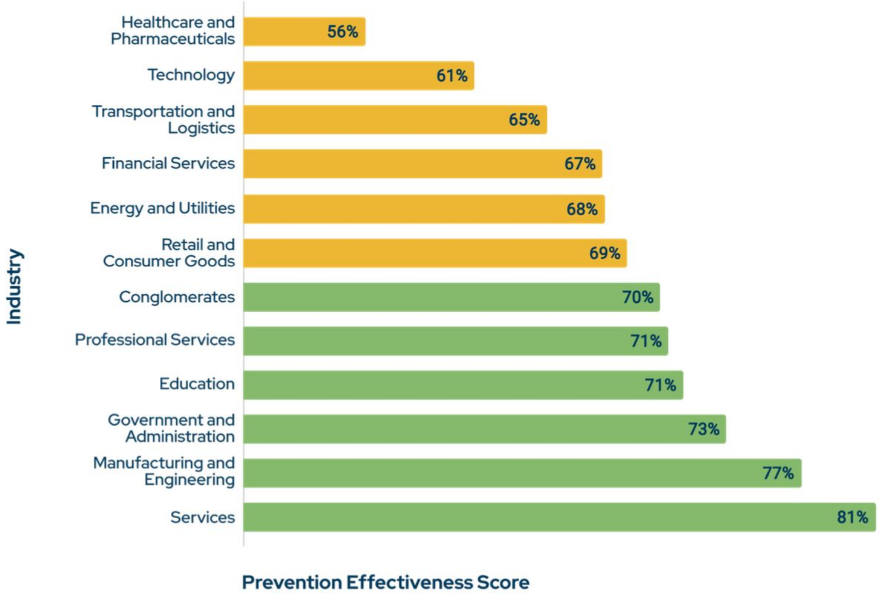
Only 37% of attacks were logged



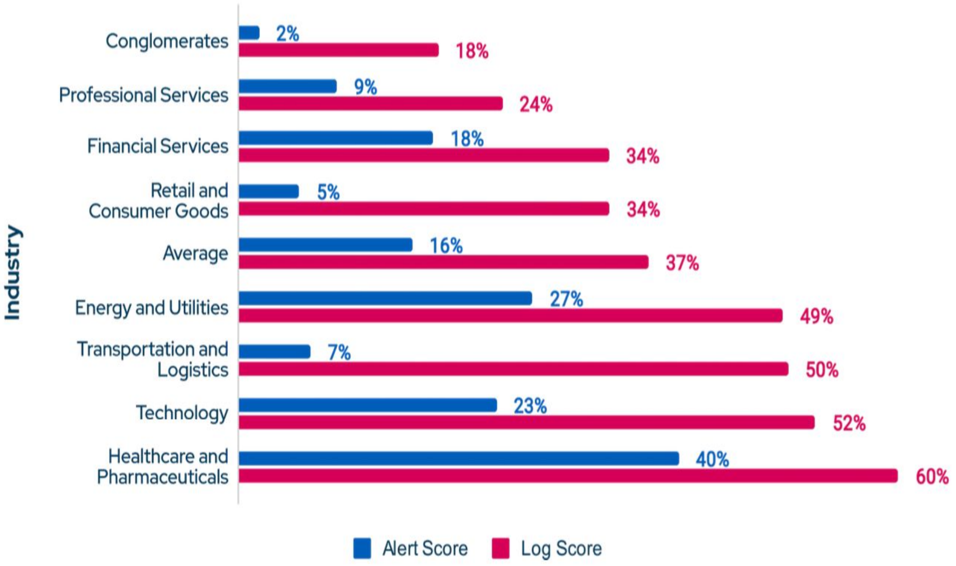
Only 16% of attacks triggered alerts

State of Industry

Prevention Effectiveness Score by Industry



Log Score and Alert Score by Industry



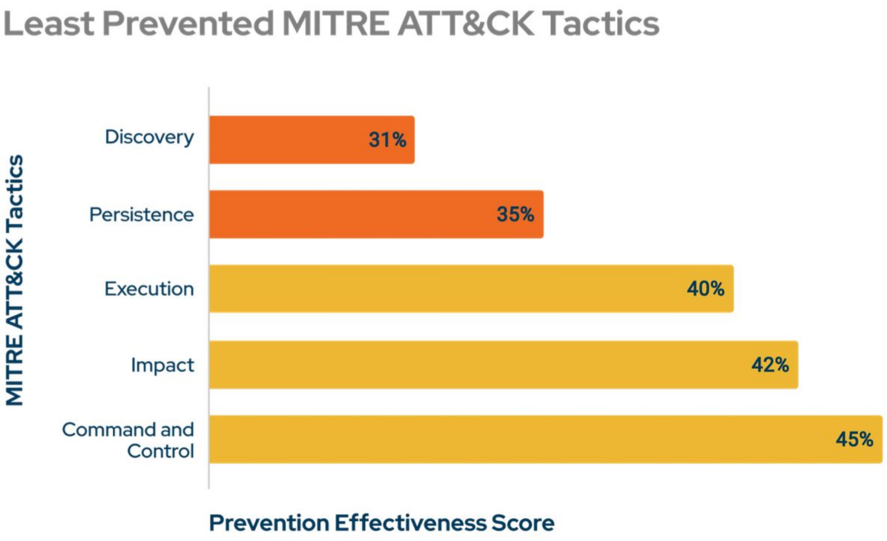
Least Prevented MTRE ATT&CK Tactics

☞ Inability to defend against the impact and command and control tactics

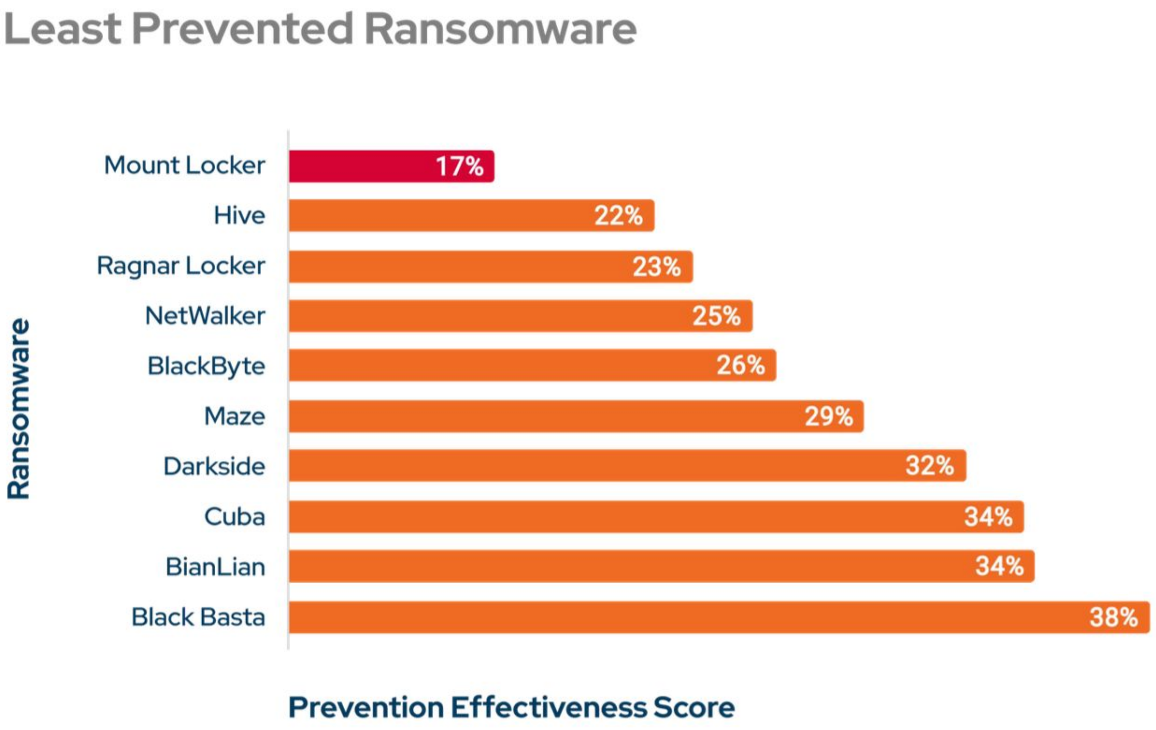
☞ Essentially, cybercriminals can cause significant disruption, including but not limited to data destruction, encryption, and manipulation, system downtime, financial loss, and tarnished reputation.

- Prevent initial system intrusion as well as tighten controls that prevent an intruder from executing actions that could directly impact their business.

- Preclude malicious actors from communicating with compromised systems to extract data, command malicious software, or control system functions.



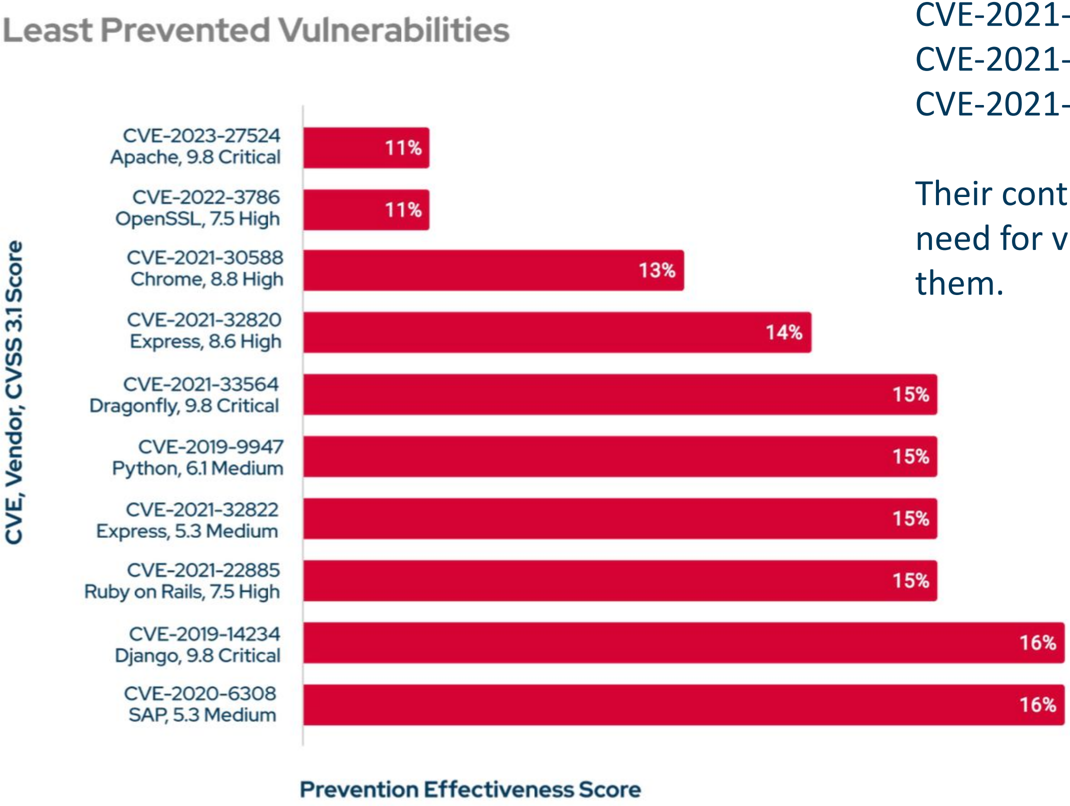
Spotlight on Ransomware Attacks



NetWalker, Maze, and Darkside varieties,

are infamous for their highprofile attacks.

Spotlight on Software Vulnerabilities


Least Prevented Vulnerabilities

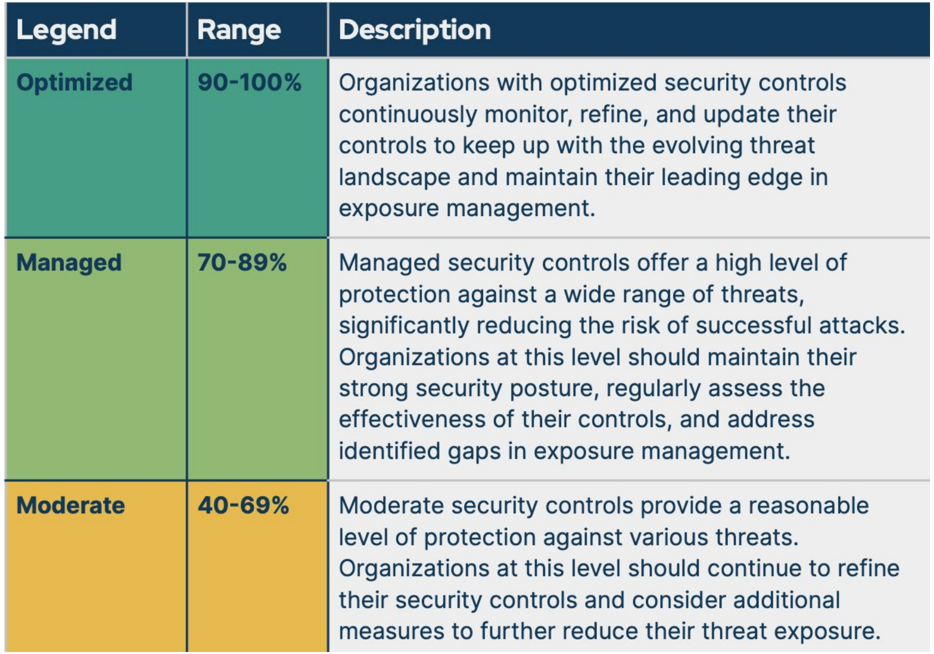
CVE-2021-30588 (affecting Chrome's JavaScript Engine), CVE-2021-33564 (affecting Linux distributions), CVE-2021-22885 (impacting Ruby on Rails).

Their continued exploitability underscores the ongoing need for vulnerability managers to prioritize patching them.

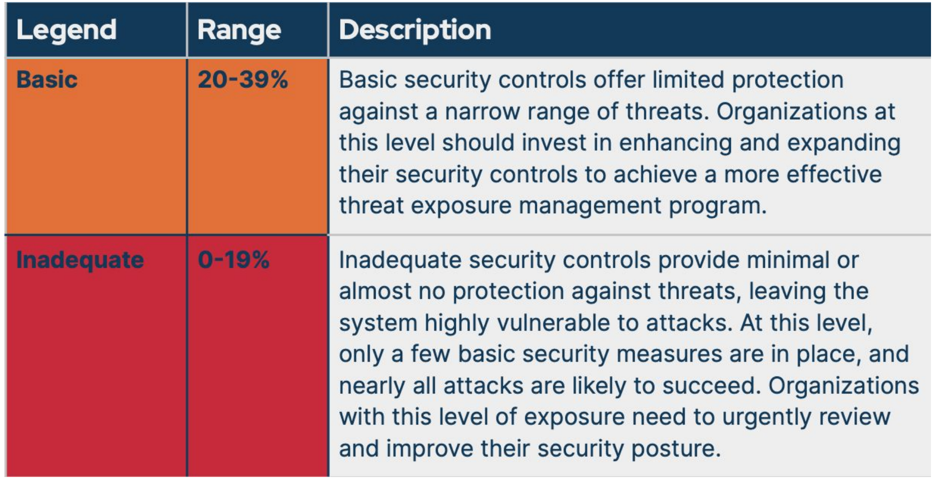
The presence of CVE-2019-9947 and CVE-2019-14234, both now 4 years old, highlights the fact that vulnerabilities can pose long-term security risks.

Timely identification and remediation of vulnerabilities is essential, even in older systems.

Maturity Model



Legend	Range	Description
Optimized	90-100%	Organizations with optimized security controls continuously monitor, refine, and update their controls to keep up with the evolving threat landscape and maintain their leading edge in exposure management.
Managed	70-89%	Managed security controls offer a high level of protection against a wide range of threats, significantly reducing the risk of successful attacks. Organizations at this level should maintain their strong security posture, regularly assess the effectiveness of their controls, and address identified gaps in exposure management.
Moderate	40-69%	Moderate security controls provide a reasonable level of protection against various threats. Organizations at this level should continue to refine their security controls and consider additional measures to further reduce their threat exposure.



Legend	Range	Description
Basic	20-39%	Basic security controls offer limited protection against a narrow range of threats. Organizations at this level should invest in enhancing and expanding their security controls to achieve a more effective threat exposure management program.
Inadequate	0-19%	Inadequate security controls provide minimal or almost no protection against threats, leaving the system highly vulnerable to attacks. At this level, only a few basic security measures are in place, and nearly all attacks are likely to succeed. Organizations with this level of exposure need to urgently review and improve their security posture.

About Colonial Pipeline

About - Colonial Pipeline

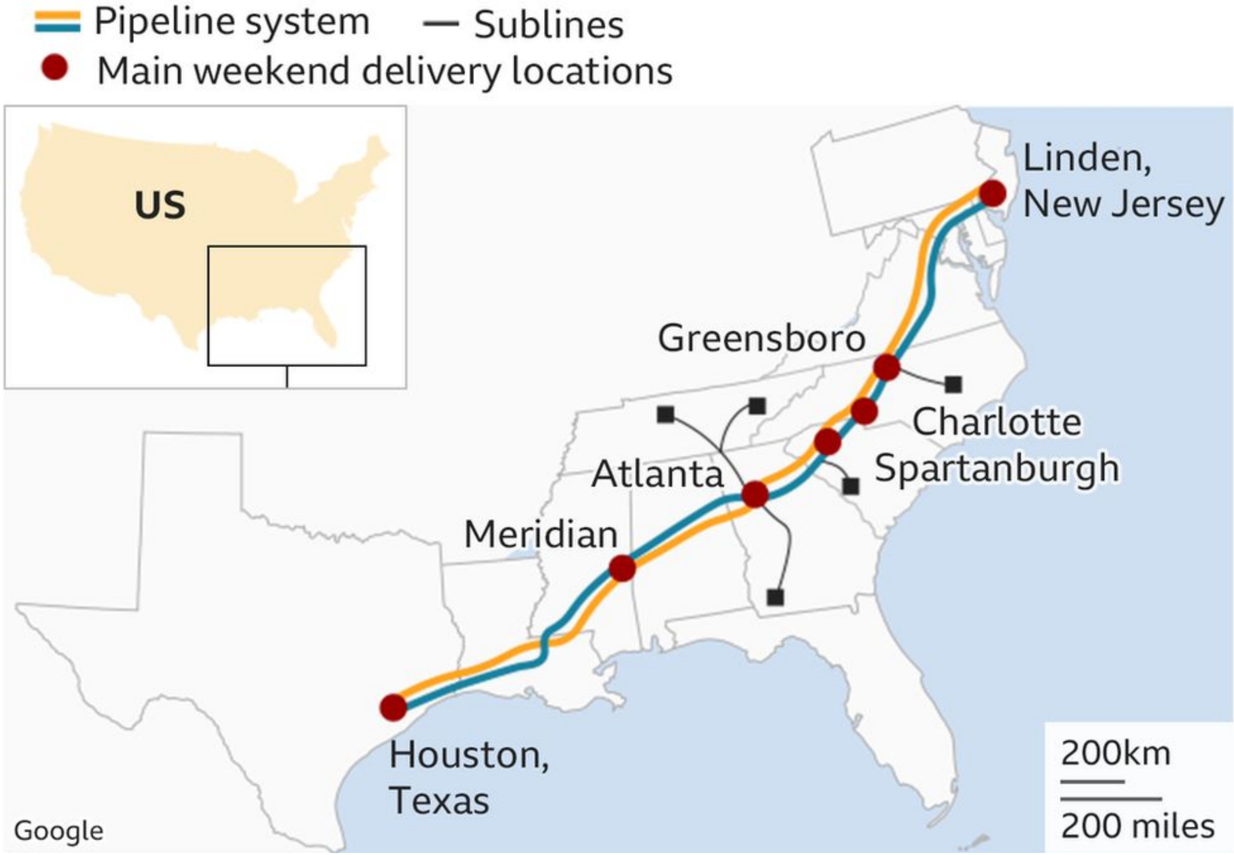
COLONIAL PIPELINE CO.

Colonial Pipeline <u>**5,500 mi (8,850 KM)**</u>

A little more than half (<u>51%</u>) of the world's total oil and gas pipelines by length are in the Americas and the Colonial Pipeline is the longest in the world.

- ☞ Colonial transports various grades of gasoline, diesel fuel, home heating oil, jet fuel, and fuels
- ☞ Colonial transports approximately 45 percent of all fuel consumed on the East Coast,
- ☞ Provides refined products to more than 50 million Americans.
- ☞ Supplies fuels for the U.S. military through a pipeline system.

Colonial Pipeline



The Colonial pipeline consists of 4 main lines and a number of branch lines.

- Line 1 - A 40 inch line moving 1.5 million barrels/day of gasoline from Houston to Greensboro, NC
- Line 2 - A 36 inch line moving 1.2 million barrels/day of middle distillates (diesel, heating oil, jet fuel) from Houston to Greensboro, NC
- Line 3 - An 885 thousand barrels/day line moving all products (gasoline, diesel, heating oil, jet fuel) from Greensboro, NC to Linden, NJ
- Line 4 - A 32 inch line moving 700 thousand barrels/day from Greensboro, NC to Baltimore
- Major spurs off the main lines include:
    - Atlanta to Southern Georgia
    - Atlanta to Tennessee (Chattanooga, Nashville, Knoxville)
    - Greensboro to Raleigh/Durham, NC
    - Mitchell (central Virginia) to Richmond, Norfolk, and Roanoke

The Colonial pipeline consists of 4 main lines and a number of branch lines.

☞ Colonial connects to a number of other pipelines that move product on through the Northeast, including:

- Laurel pipeline (Buckeye) - Connects in Philadelphia and moves product west through Pennsylvania to Pittsburgh
- IHT - Connects in Linden and moves product across the surrounding New York and New Jersey area
- Long Island pipeline (Buckeye) - Connects in Linden and moves product across Long Island
- Buckeye East System - Connects in Linden and moves product west to Eastern Pennsylvania, where there is a connection to the Laurel pipeline and lines moving north into Northeastern Pennsylvania and upstate New York

The Colonial pipeline consists of 4 main lines and a number of branch lines.

☞ Colonial batches can be either fungible between shippers (with standard specifications set by Colonial) or segregated for a specific shipper.

☞ Lines 1 and 2 have a minimum batch size of 75 thousand barrels, while lines 3 and 4 have a minimum of 25 thousand barrels.

☞ Colonial schedules batches in 5-day cycles (72 each year). The mix of products and grades in each cycle will vary with changes in market demand.

☞ The pipeline is frequently operating at capacity requiring Colonial to allocate space to shippers. Allocated volumes for shippers with an established history (regular shippers) are based on historical shipped volumes.

☞ 5% of space is allocated to all new shippers (without necessary shipping history to be regular shippers), which is then assigned to individual shippers by lottery. There is an active market for trading shipping space on the line.

A Timeline of the Colonial Pipeline Attack

- ☞ May 6, 2021: Malicious actors launch an attack, stealing 100GB data, locking computers, and requesting a ransom.
- ☞ May 7, 2021: Colonial Pipeline pays the ransom.
- ☞ May 8, 2021: Colonial Pipeline publicly announces attack, then shuts off servers and some pipelines.
- ☞ May 9, 2021: Colonial Pipeline makes a 2nd public announcement, discussing its system restart plans.
- ☞ May 10, 2021: The FBI confirms DarkSide ransomware caused the attack, and Colonial Pipeline releases two more statements around its restoration process.
- ☞ May 11, 2021: Federal agencies release an advisory describing DarkSide ransomware and mitigation strategies while Colonial Pipelines releases a statement around fuel shipping.
- ☞ May 12, 2021: Colonial Pipeline restores operations and announces fuel delivery timelines, amidst people "panic buying" gasoline.

Colonial Pipeline

Analysis

How did Colonial handle the crisis?

- ☞ What is the crisis?
- ☞ How was the incident detected?
- ☞ Who was the first responder?
- ☞ Did Colonial have an incident response playbook?
- ☞ Was the playbook effective in the actual incident?
- ☞ How and who made the decision to escalate?

Some Questions – Incident detection and Response

- ☞ Who detected the incident at Colonial
- ☞ Who was the first responder?
- ☞ How did Colonial employees know that they should escalate this situation?
- ☞ And how did they know who to escalate to?
- ☞ How does the first responder determine if this is an incident of magnitude?
- ☞ Who at Colonial made the decision to declare this as an incident of magnitude?

Some Questions - Teams

- ☞ How did Colonial organize the response team?
- ☞ Constitution of IR team
  - IR Playbook?
  - Who are the members?
  - What role does each member play?
- ☞ What factors are considered in team composition?
- ☞ Where and how did Colonial response team get together? In person or virtual?
- ☞ When you primary Business / IT systems are down, how do you communicate with various stakeholders?

During the Incident

- ☞ Containment
- ☞ Backup and Recovery
- ☞ Should you pay Ransom?
- ☞ Notify Law enforcement

Response during the Cyber Incident

- ☞ Containment
- ☞ Assessment and Analysis
- ☞ Backup and Recovery
- ☞ Should we pay the Ransom?
- ☞ Inform Law Enforcement/Govt agencies
- ☞ Communicate with Stakeholders
- ☞ Review and Improve

Incidence Response

☞ Constitution of IR team

- Who are the members?
- What role does each member play?
- How do the members communicate?
- IR Playbook?

Was Colonial crisis communication practices appropriate?

☞ Identify key stakeholders

☞ Assess the situation

☞ Develop a clear and concise message

☞ Communicate promptly and regularly

☞ Be transparent

☞ Be prepared for Media Questions

☞ Consider use of outside resources

How should organizations prevent and prepare for Cyber attacks?

- ☞ Backup regularly and validate
- ☞ Keep software and systems updated
- ☞ Train Employees
- ☞ Implement End point protection
- ☞ Use Network Segmentation
- ☞ Conduct Cyber attack simulations
- ☞ Have a validated Response Plan
- ☞ Consider Cybersecurity Insurance

What was the executives’ role during the attack?

- ☞ Coordination and communication
- ☞ Decision Making
- ☞ Resource Allocation
- ☞ Post attack assessment and improvement

Do you agree with Colonial’s decision to pay ransom?

☞ Pros

- Quick Resolution
- Access to Decryption keys
- Price of NOT paying may be higher
- Sharing of vulnerability

☞ Cons

- No guarantee of receiving decryption keys
- No guarantee of protection of sensitive information
- Slow decryption process/time
- Encourages further attacks
- Legal Implications

During the Incident

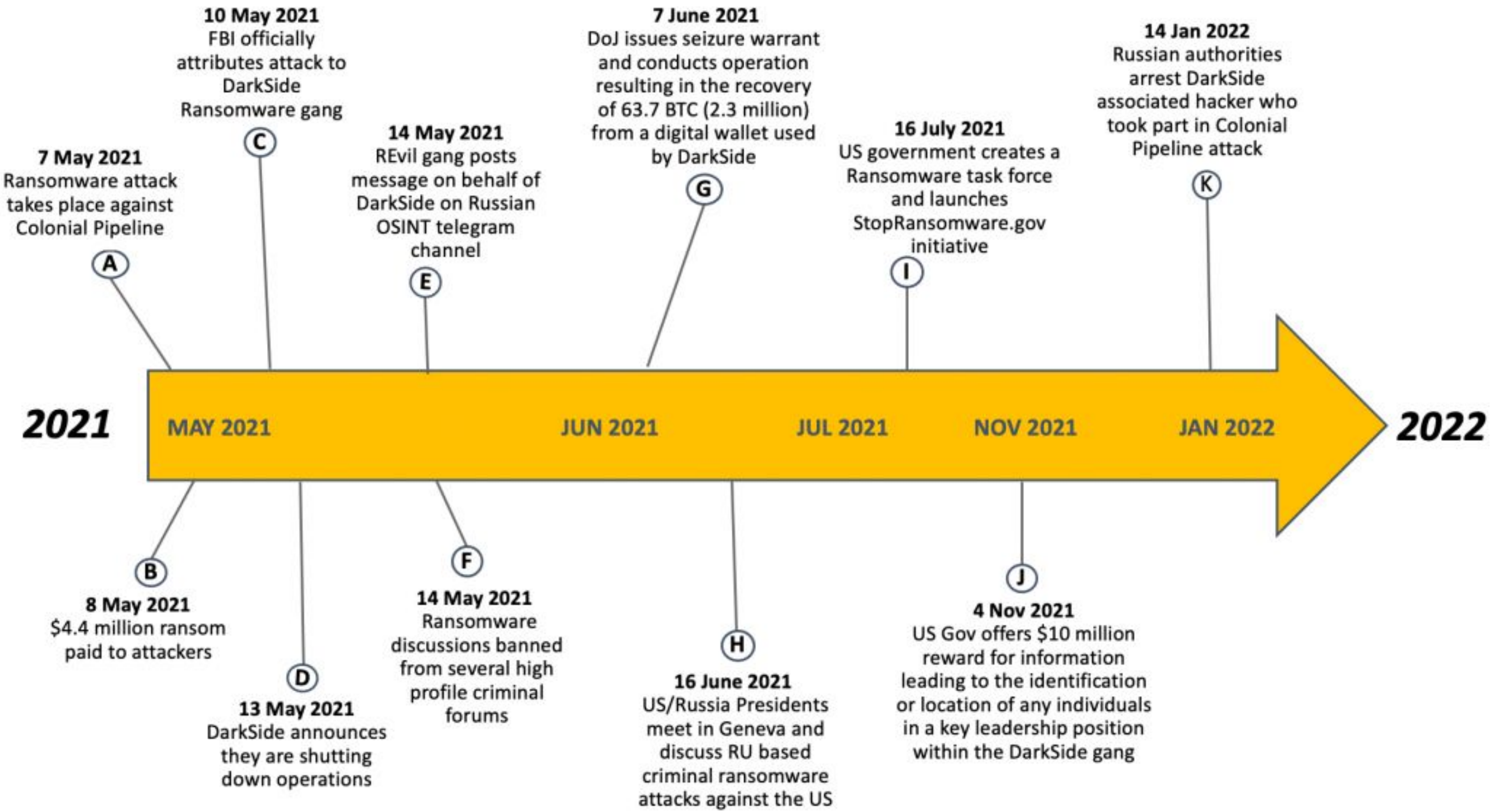
☞ Communicate with Stakeholders

- Identify key stakeholders
- Clear and concise message
- Regular updates
- Media updates
- External support

Prevention

- ☞ Validated Backups
- ☞ Software and systems updated
- ☞ Security patches applied
- ☞ Training
- ☞ End Point protection
- ☞ Segmentation of Network

One Year on..



A — **7 May 2021** Ransomware attack takes place against Colonial Pipeline

B — **8 May 2021** $4.4 million ransom paid to attackers

C — **10 May 2021** FBI officially attributes attack to DarkSide Ransomware gang

D — **13 May 2021** DarkSide announces they are shutting down operations

E — **14 May 2021** REvil gang posts message on behalf of DarkSide on Russian OSINT telegram channel

F — **14 May 2021** Ransomware discussions banned from several high profile criminal forums

G — **7 June 2021** DoJ issues seizure warrant and conducts operation resulting in the recovery of 63.7 BTC (2.3 million) from a digital wallet used by DarkSide

H — **16 June 2021** US/Russia Presidents meet in Geneva and discuss RU based criminal ransomware attacks against the US

I — **16 July 2021** US government creates a Ransomware task force and launches StopRansomware.gov initiative

J — **4 Nov 2021** US Gov offers $10 million reward for information leading to the identification or location of any individuals in a key leadership position within the DarkSide gang

K — **14 Jan 2022** Russian authorities arrest DarkSide associated hacker who took part in Colonial Pipeline attack

Impact of the Attack

- US Government declares a regional emergency declaration for 17 states and Washington, D.C., to keep fuel supply lines open on May 9

- On May 10, Georgia Governor Brian Kemp declared a state of emergency, and temporarily waived collection of the state's taxes on motor fuels (diesel and gasoline).

- In response to panic buying in the Southeast, U.S. Transportation Secretary Pete Buttigieg and U.S. Energy Secretary Jennifer Granholm on May 12 both cautioned against gasoline hoarding, reiterating that the United States was undergoing a "supply crunch" rather than a gas shortage.

- On May 12, the U.S. Consumer Product Safety Commission advised people to "not fill plastic bags with gasoline" or to use any containers not meant for fuel.

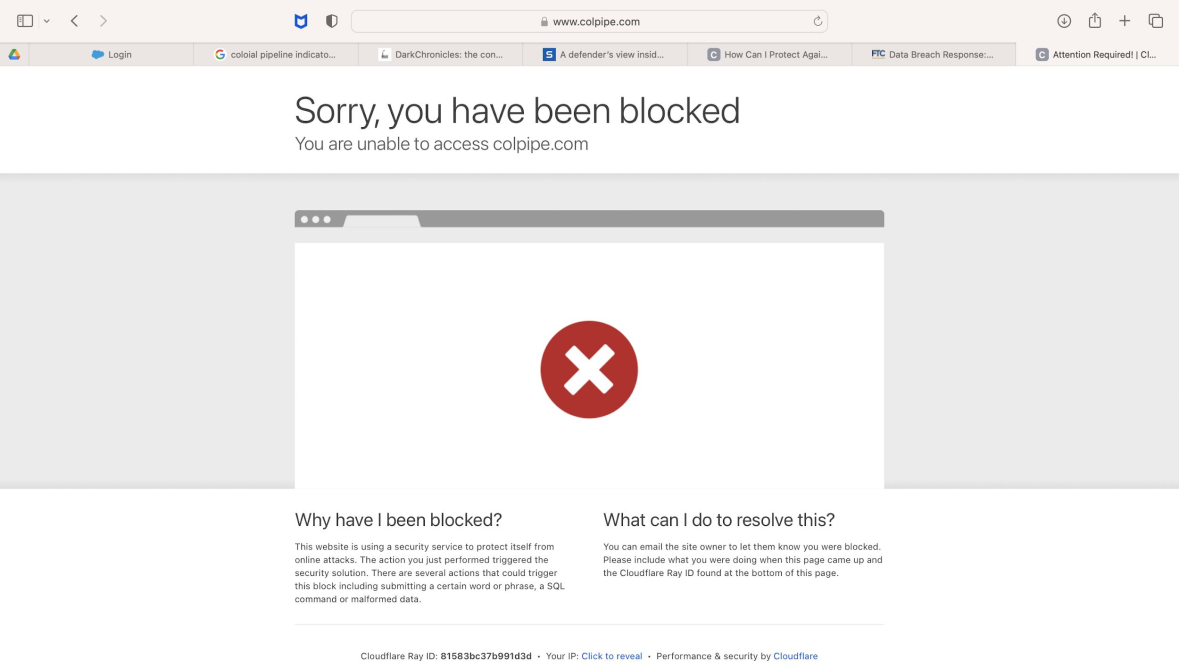
Source: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

Impact of the Attack

- Biden signed Executive Order 14028 on May 12, increasing software security standards for sales to the government, tighten detection and security on existing systems, improve information sharing and training, establish a Cyber Safety Review Board, and improve incident response.
- The United States Department of Justice also convened a cybersecurity task force to increase prosecutions.
- The Department of State issued a statement that a $10,000,000 reward would be given out in case of information leading to the arrest of DarkSide members.

Source: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

Access Blocked !


www.colpipe.com
Login
coloial pipeline indicato...
DarkChronicles: the con...
A defender's view insid...
How Can I Protect Agai...
Data Breach Response:...
Attention Required! | Cl...

Sorry, you have been blocked

You are unable to access colpipe.com

Why have I been blocked?

This website is using a security service to protect itself from online attacks. The action you just performed triggered the security solution. There are several actions that could trigger this block including submitting a certain word or phrase, a SQL command or malformed data.

What can I do to resolve this?

You can email the site owner to let them know you were blocked. Please include what you were doing when this page came up and the Cloudflare Ray ID found at the bottom of this page.

Cloudflare Ray ID: 81583bc37b991d3d • Your IP: Click to reveal • Performance & security by Cloudflare

About Darkside

How the DarkSide Ransomware Works

☞ Stage One

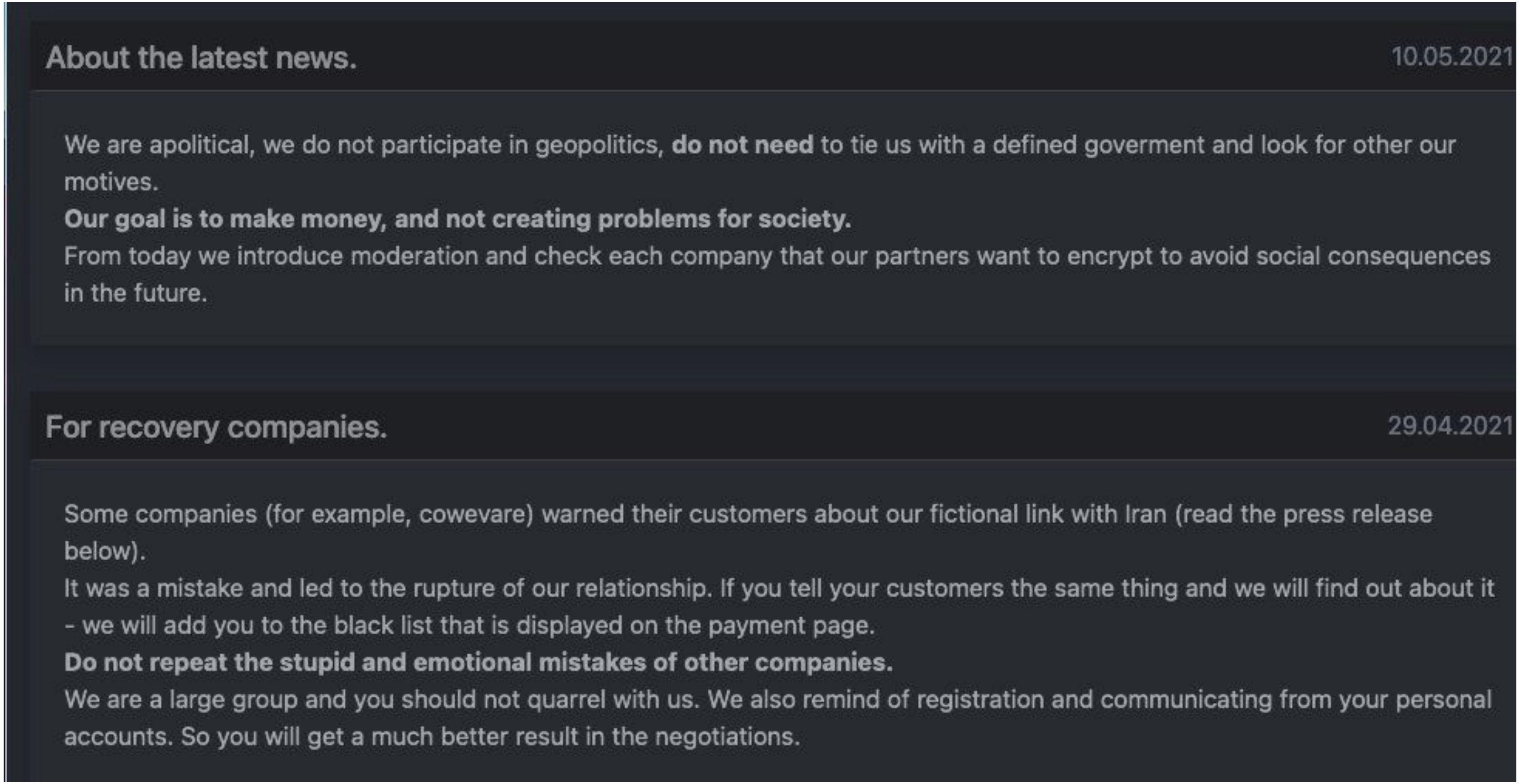
- Initial compromise - attackers gain access to a device, masquerading as a legitimate user so that they can install the malicious code on the compromised endpoint. Research indicates that cybercriminals do this in three ways:

  1. Brute force password attack
  2. Phishing attacks with malicious links
  3. CVE-2021-20016, a SQL-injection vulnerability against an organization’s Virtual Private Network (VPN) infrastructure

☞ Stage Two

- Escalate privileges to gain access to sensitive information.
- Finally, they encrypt business-critical processes, request a ransom, show “proof of life” over the exfiltrated data, and decrypt everything only after the target pays them.

We are good people, all we want is the money



About the latest news.

10.05.2021

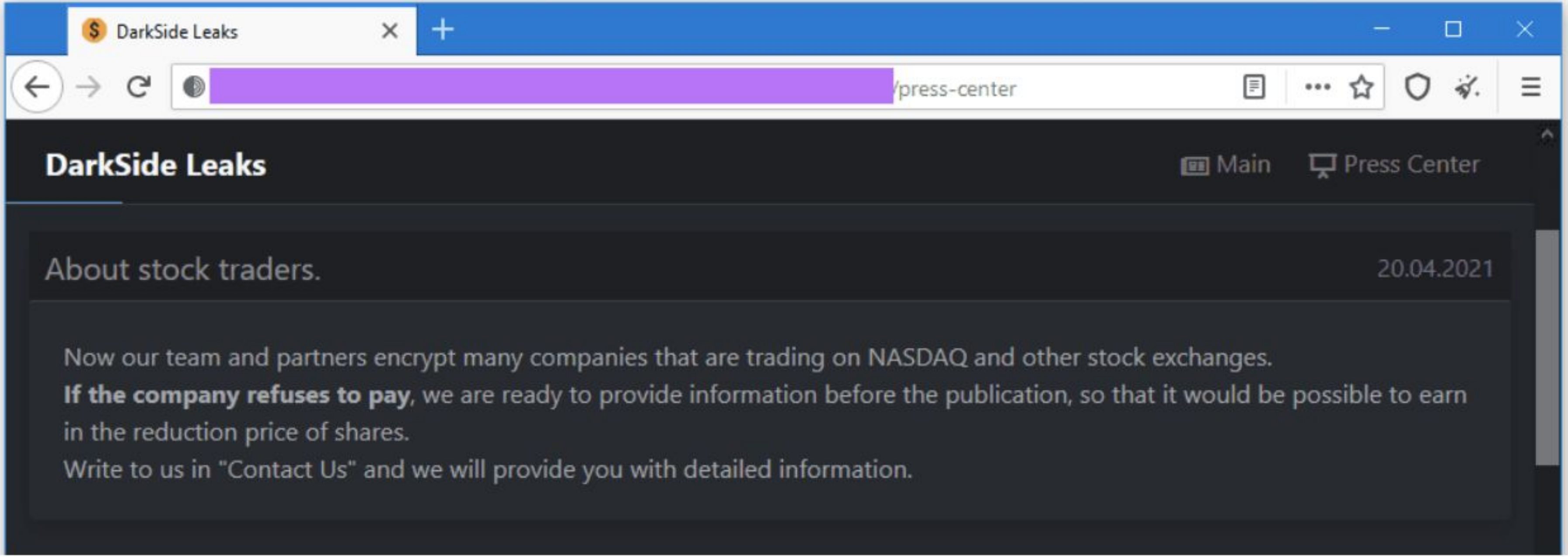
We are apolitical, we do not participate in geopolitics, **do not need** to tie us with a defined goverment and look for other our motives.
Our goal is to make money, and not creating problems for society.
From today we introduce moderation and check each company that our partners want to encrypt to avoid social consequences in the future.

For recovery companies.

29.04.2021

Some companies (for example, cowevare) warned their customers about our fictional link with Iran (read the press release below).
It was a mistake and led to the rupture of our relationship. If you tell your customers the same thing and we will find out about it - we will add you to the black list that is displayed on the payment page.
Do not repeat the stupid and emotional mistakes of other companies.
We are a large group and you should not quarrel with us. We also remind of registration and communicating from your personal accounts. So you will get a much better result in the negotiations.

Extortion

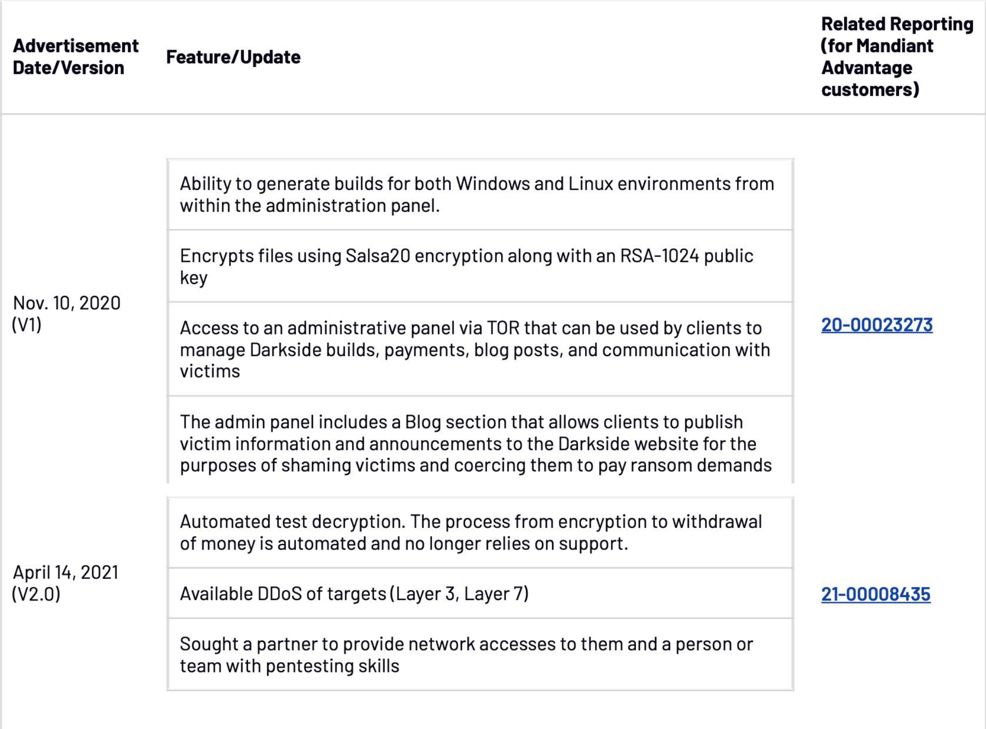


About stock traders. 20.04.2021

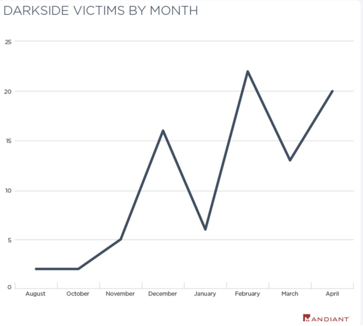
Now our team and partners encrypt many companies that are trading on NASDAQ and other stock exchanges.
If the company refuses to pay, we are ready to provide information before the publication, so that it would be possible to earn in the reduction price of shares.
Write to us in "Contact Us" and we will provide you with detailed information.

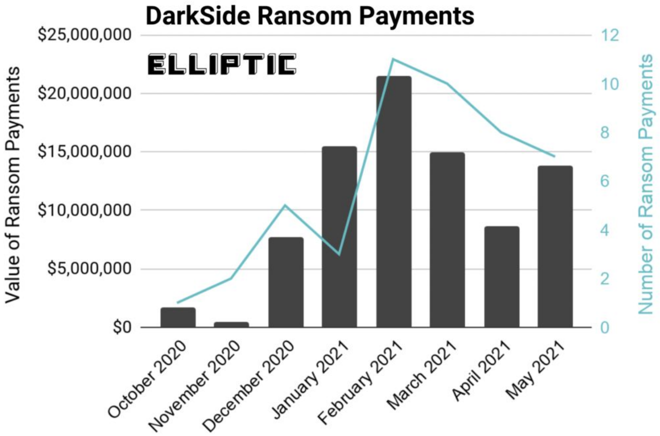
About DARKSIDE

DARKSIDE ransomware operates as a ransomware-as- a-service (RaaS) wherein profit is shared between its owners and partners, or affiliates, who provide access to organizations and deploy the ransomware.



Advertisement Date/Version	Feature/Update	Related Reporting (for Mandiant Advantage customers)
Nov. 10, 2020 (V1)	Ability to generate builds for both Windows and Linux environments from within the administration panel.	20-00023273
	Encrypts files using Salsa20 encryption along with an RSA-1024 public key	
	Access to an administrative panel via TOR that can be used by clients to manage Darkside builds, payments, blog posts, and communication with victims	
	The admin panel includes a Blog section that allows clients to publish victim information and announcements to the Darkside website for the purposes of shaming victims and coercing them to pay ransom demands	
April 14, 2021 (V2.0)	Automated test decryption. The process from encryption to withdrawal of money is automated and no longer relies on support.	21-00008435
	Available DDoS of targets (Layer 3, Layer 7)	
	Sought a partner to provide network accesses to them and a person or team with pentesting skills	

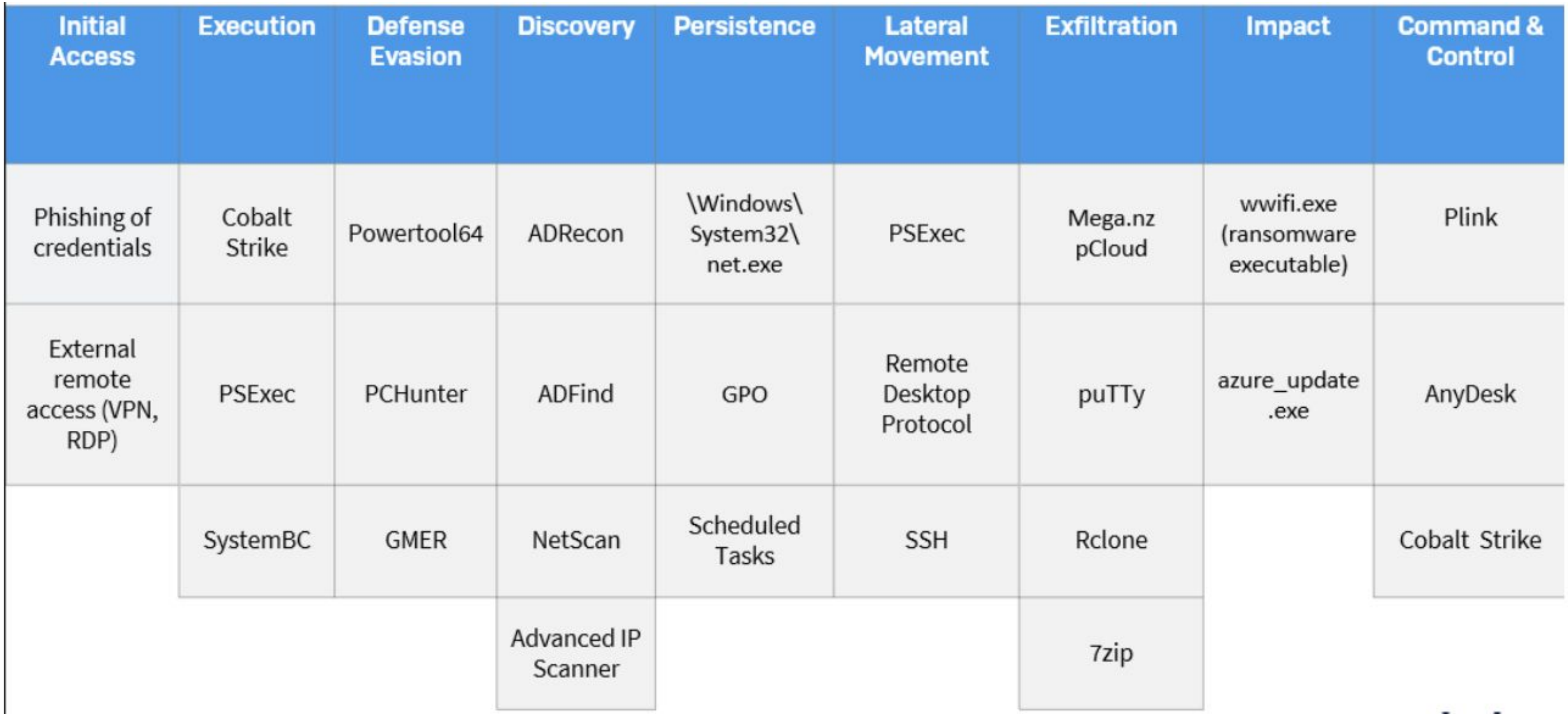




Extortion

- ☞ The Darkside crew believes that the negative impact of having a traded company's name listed on its website would be enough to cause its stock price to fall and for a crooked trader to make a profit.
- ☞ "DarkSide becomes the first ransomware variant to make it formal."
- ☞ This approach is just the latest in a long list of techniques that ransomware gangs have been adding to their extortion arsenals.
- ☞ Other gangs have previously used:
  - cold-calls to threaten victims that were preparing to restore data from backups
  - tried making personal threats against the executives responsible for approving the ransom payment
  - threatened to notify business partners
  - threatened companies with DDoS attacks
  - threatened companies that they'd notify journalists about their security breaches
  - threatened to notify privacy watchdog agencies about a breach so the company can get fined
  - and even sent emails to a victim's clients, asking the customers to put pressure on the company to pay its ransom demand and avoid having the customers' data leaked online

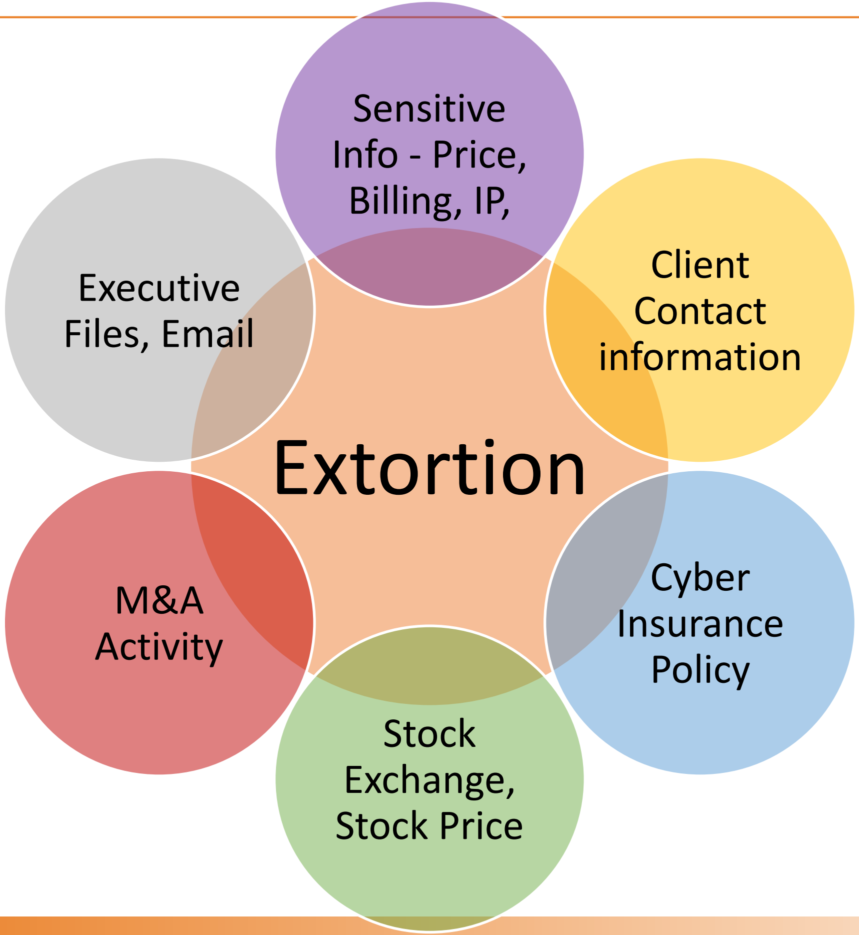
DARKSIDE Ransomware tools



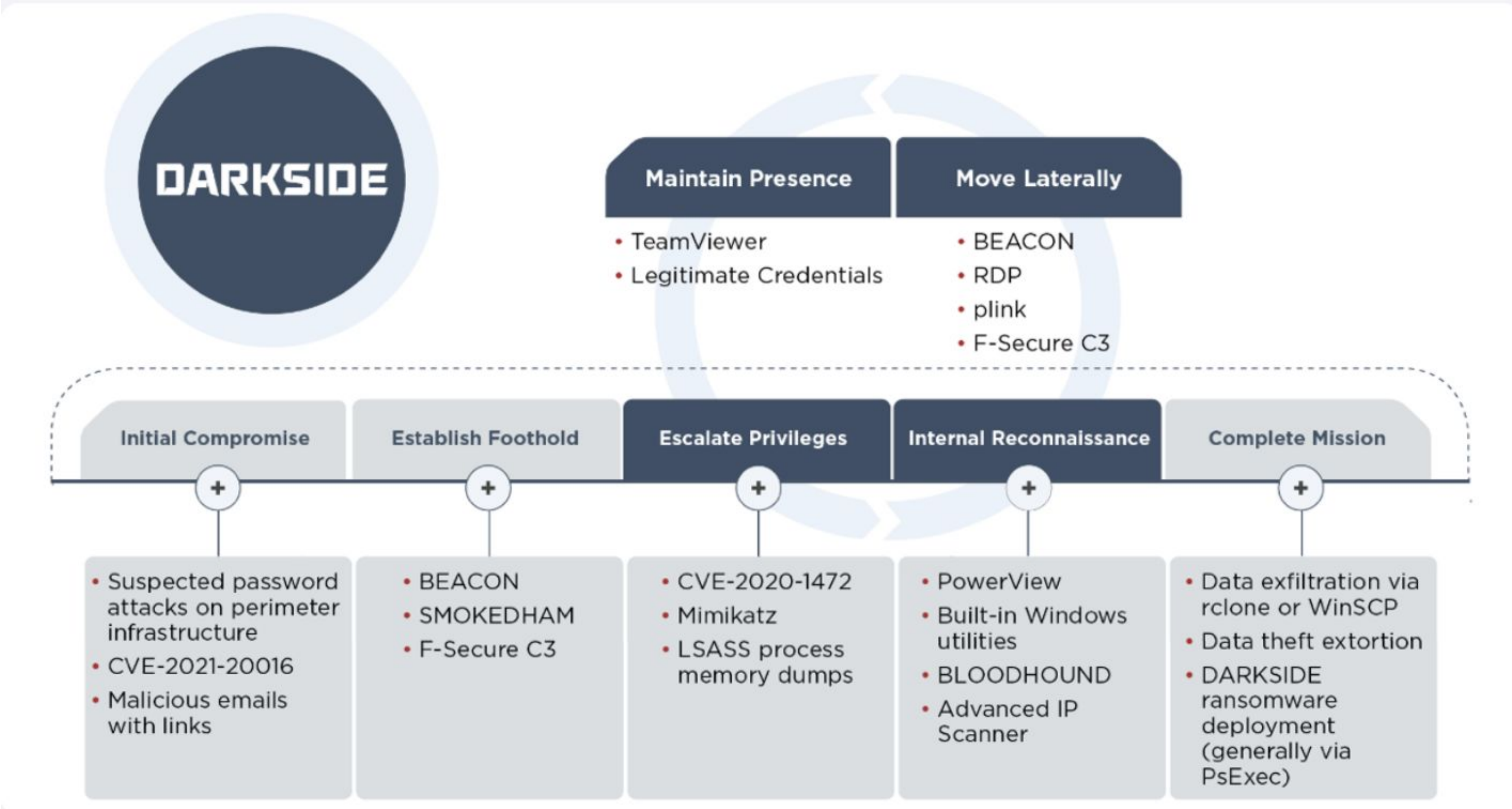
Initial Access	Execution	Defense Evasion	Discovery	Persistence	Lateral Movement	Exfiltration	Impact	Command & Control
Phishing of credentials	Cobalt Strike	Powertool64	ADRecon	\Windows\System32\net.exe	PSExec	Mega.nz pCloud	wwifi.exe (ransomware executable)	Plink
External remote access (VPN, RDP)	PSExec	PCHunter	ADFind	GPO	Remote Desktop Protocol	puTTy	azure_update.exe	AnyDesk
	SystemBC	GMER	NetScan	Scheduled Tasks	SSH	Rclone		Cobalt Strike
			Advanced IP Scanner			7zip		

Source Sophos

Extortion Ecosystem


Sensitive Info - Price, Billing, IP,
Client Contact information
Executive Files, Email
Extortion
M&A Activity
Cyber Insurance Policy
Stock Exchange, Stock Price

Attack Lifecycle – TTP throughout DARKSIDE



DARKSIDE

Maintain Presence

- TeamViewer
- Legitimate Credentials

Move Laterally

- BEACON
- RDP
- plink
- F-Secure C3

Initial Compromise

- Suspected password attacks on perimeter infrastructure
- CVE-2021-20016
- Malicious emails with links

Establish Foothold

- BEACON
- SMOKEDHAM
- F-Secure C3

Escalate Privileges

- CVE-2020-1472
- Mimikatz
- LSASS process memory dumps

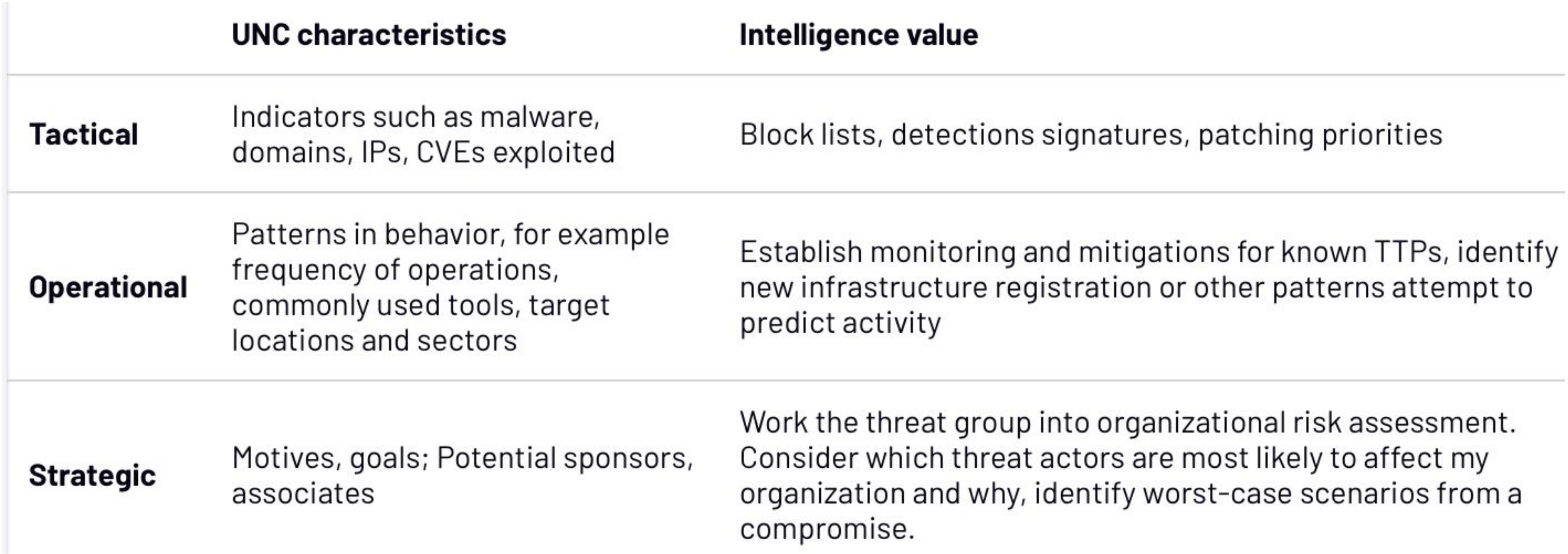
Internal Reconnaissance

- PowerView
- Built-in Windows utilities
- BLOODHOUND
- Advanced IP Scanner

Complete Mission

- Data exfiltration via rclone or WinSCP
- Data theft extortion
- DARKSIDE ransomware deployment (generally via PsExec)

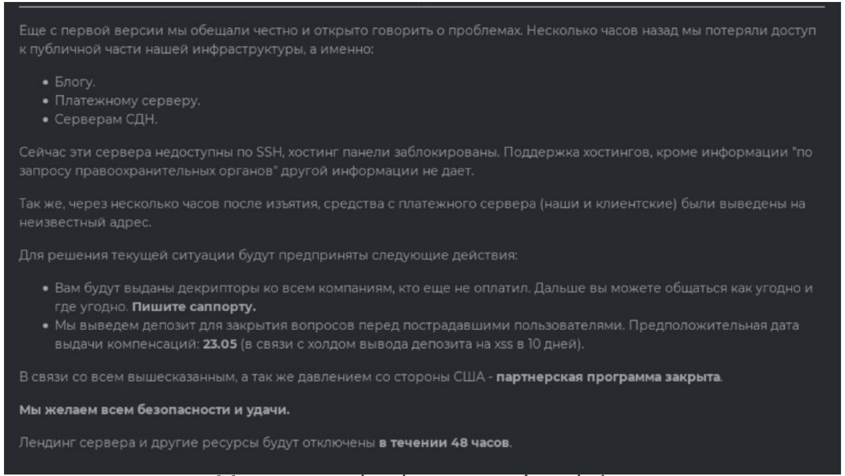
Attack Lifecycle



	UNC characteristics	Intelligence value
Tactical	Indicators such as malware, domains, IPs, CVEs exploited	Block lists, detections signatures, patching priorities
Operational	Patterns in behavior, for example frequency of operations, commonly used tools, target locations and sectors	Establish monitoring and mitigations for known TTPs, identify new infrastructure registration or other patterns attempt to predict activity
Strategic	Motives, goals; Potential sponsors, associates	Work the threat group into organizational risk assessment. Consider which threat actors are most likely to affect my organization and why, identify worst-case scenarios from a compromise.

Who won?

On May 14, DarkSide developers announced that they had lost access to part of their infrastructure, including their blog, payment server, and the CDN.



Еще с первой версии мы обещали честно и открыто говорить о проблемах. Несколько часов назад мы потеряли доступ к публичной части нашей инфраструктуры, а именно:

- Блогу.
- Платежному серверу.
- Серверам СДН.

Сейчас эти сервера недоступны по SSH, хостинг панели заблокированы. Поддержка хостингов, кроме информации "по запросу правоохранительных органов" другой информации не дает.

Так же, через несколько часов после изъятия, средства с платежного сервера (наши и клиентские) были выведены на неизвестный адрес.

Для решения текущей ситуации будут предприняты следующие действия:

- Вам будут выданы декрипторы ко всем компаниям, кто еще не оплатил. Дальше вы можете общаться как угодно и где угодно. **Пишите саппорту.**
- Мы выведем депозит для закрытия вопросов перед пострадавшими пользователями. Предположительная дата выдачи компенсаций: **23.05** (в связи с холдом вывода депозита на xss в 10 дней).

В связи со всем вышесказанным, а так же давлением со стороны США - **партнерская программа закрыта**.

Мы желаем всем безопасности и удачи.

Лендинг сервера и другие ресурсы будут отключены **в течении 48 часов**.

Message on the threat actor's website.

- Once again it has turned out that information security issues are relevant to villains, too. The successful (though, it turns out, not that brilliant) operation which involved stealing data, doing encryption and receiving ransom from Colonial Pipeline was not the end of the story.

- All the money, including their own money and “client” funds (apparently, the money of their affiliates) had been moved to an unknown address. They promised to pay compensation to their affiliates by May 23, 2021 from a previously made deposit payment and to provide all their affiliates with decryption utilities through their “technical support” channel.

- They also announced that the service and the affiliate program were discontinued.

This is likely the end of the DarkSide story.

If the affiliate program resumes its operation, it will probably be under a different name.

Ransomware Check list – Best Practices

Ransomware Response Checklist

Detection and Analysis

- ☞ Determine which systems were impacted, and immediately isolate them.
- ☞ Power down devices if you are unable to disconnect them from the network to avoid further spread of the ransomware infection.
- ☞ Triage impacted systems for restoration and recovery.
- ☞ Examine existing organizational detection or prevention systems (e.g., antivirus, EDR, IDS, Intrusion Prevention System) and logs.
- ☞ Confer with your team to develop and document an initial understanding of what has occurred based on initial analysis.
- ☞ Initiate threat hunting activities.

Ransomware Response Checklist

Reporting and Notification

☞ Trigger and initiate your IR playbook

- Incidence response plan as per approved playbook
  - Identify source and try to contain
- Communication plan,
- Inform stakeholders,
- Engage external resources,
- Notify agencies – law enforcement, others as necessary

Ransomware Response Checklist

Containment and Eradication

☞ If no initial mitigation actions appear possible

- Take a system image and memory capture of a sample of affected devices (e.g., workstations, servers, virtual servers, and cloud servers).
- Consult federal law enforcement, even if mitigation actions are possible, regarding possible decryptors available,
- Research trusted guidance
- Identify the systems and accounts involved in the initial breach and contain if feasable
- Conduct extended analysis to identify outside-in and inside-out persistence mechanisms.
- Rebuild systems based on prioritization of critical services
- Issue password resets for all affected systems and address any associated vulnerabilities and gaps in security or visibility
- The designated IT or IT security authority declares the ransomware incident over

Ransomware Response Checklist

Recovery and Post Incident Activity

- ☞ Reconnect systems and restore data from offline, encrypted backups based on a prioritization of critical services.
  - Take care not to re-infect clean systems during recovery.
  - For example, if a new Virtual Local Area Network (VLAN) has been created for recovery purposes, ensure only clean systems are added.
- ☞ Document lessons learned from the incident and associated response activities to inform updates to—and refine—organizational policies, plans, and procedures and guide future exercises of the same.
- ☞ Consider sharing lessons learned and relevant indicators of compromise with your sector ISAC to benefit others within the community.

Practices to avoid

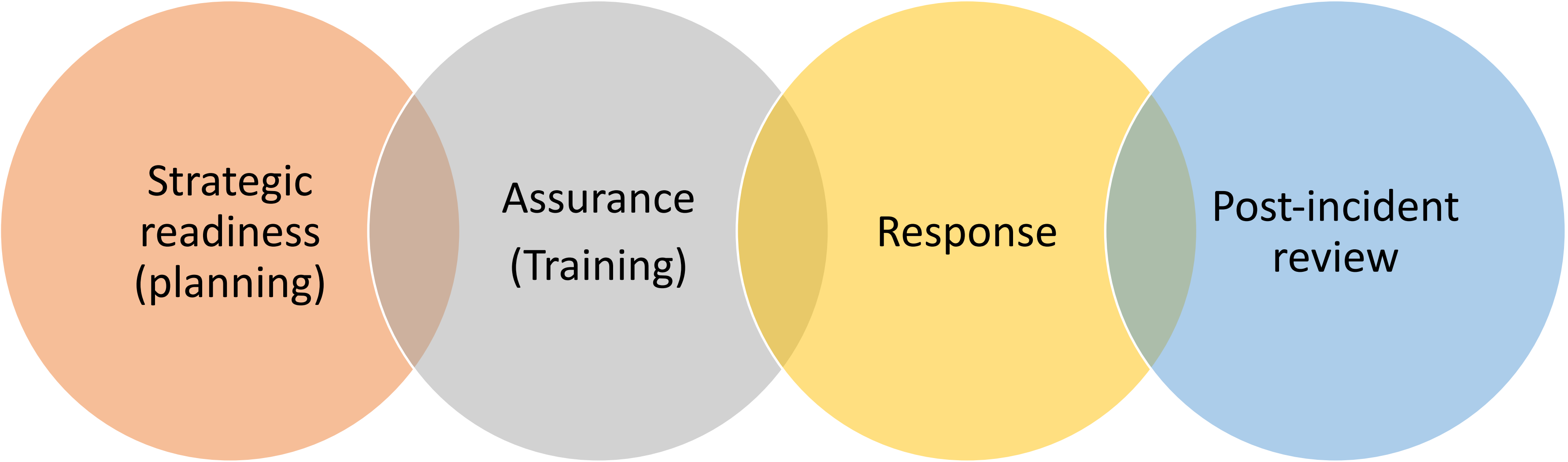
☞ Use of unsupported (or end-of-life) software is dangerous and significantly elevates risk.

☞ Use of known/fixed/default passwords and credentials significantly elevates risk.

☞ The use of single-factor authentication for remote or administrative access to systems is dangerous and significantly elevates risk

☞ All of the above is especially egregious in technologies accessible from the Internet.

4 Phases of Cybersecurity Crisis Communications



Strategic readiness (planning)

Assurance (Training)

Response

Post-incident review

Assignment Questions

- ☞ What is the role of cryptography in this crisis?
- ☞ Did Colonial handle the crisis appropriately?
- ☞ What did the company do well and what could it have done better? What other lessons have you learned from the incident?
- ☞ How should organizations manage the ever-increasing threat of data breaches?
- ☞ Do you agree with Blount’s decision to pay the ransom?
- ☞ In general, should organizations pay ransomware?

Thank you!

Follow us

isfcr.pesu

www.isfcr.pes.edu

ISFCR

PESU ISFCR

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES UNIVERSITY