

# Cybersecurity Incident Response Framework

Investigating a Conti ransomware Incident



- **Purpose of the Project:**

To develop a robust incident response framework.

- **What we will focus on :**

- Overview of cybersecurity concepts and threats.
- Create a Detailed incident response plan.
  - system hardening, secure architecture, and access control measures.
  - develop a Playbook to help handling various types of incident
- Simulation of cybersecurity incident of Conti Ransomware.
- Applying the created IR plan in into incident
- Writing Response documentation including containment, eradication, and recovery steps.

# Who We Are

We are a dedicated **third-party incident response team** specializing in **comprehensive cybersecurity services**.

- **Our Services Include:**

- **Incident Investigation:** Analyzing the breach, understanding the attack vector, and assessing impact.
- **Containment and Eradication:** Implementing measures to contain the incident and eliminate threats.
- **Recovery:** Assisting with system restoration and ensuring vulnerabilities are addressed.
- **Threat Intelligence:** Providing insights into emerging threats and post-incident reporting.
- **Training and Preparedness:** Offering training sessions for staff to prevent future incidents.

- **Current Focus:**

We are currently investigating a ransomware incident affecting the company, ensuring a swift and effective response to minimize damage and restore operations.

- **Tools and Techniques for the project:**
  - **Our Incident response plan is based on**
    - NIST Cybersecurity Framework
    - Cyber kill chain Framework
  - **For incident simulation we will use tryhackme.com website**
    - Discuss the Conti ransomware walkthrough
    - Use Splunk SIEM to investigate the attack
  - **We used some references in our project**
    - CompTIA Security+
    - Certified Information Systems Security Professional (CISSP):
    - OWASP (Open Web Application Security Project):
    - NIST (National Institute of Standards and Technology):
    - CERT (Computer Emergency Response Team):

- **What is cybersecurity?**

- Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

- **What is information security?**

- Information security (sometimes referred to as InfoSec) covers the tools and processes that organizations use to protect information.
- This includes policy settings that prevent unauthorized people from accessing business or personal information it also protect data at rest , motion and use.

# Communications Security: CIA

Information security deals with protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

## CIA Triad

The CIA triad consists of three components of information security:

- **Confidentiality** - Only authorized individuals, entities, or processes can access sensitive information.
- **Integrity** - This refers to the protection of data from unauthorized alteration.
- **Availability** - Authorized users must have uninterrupted access to the network resources and data that they require.



# Threat, Vulnerability, and Risk

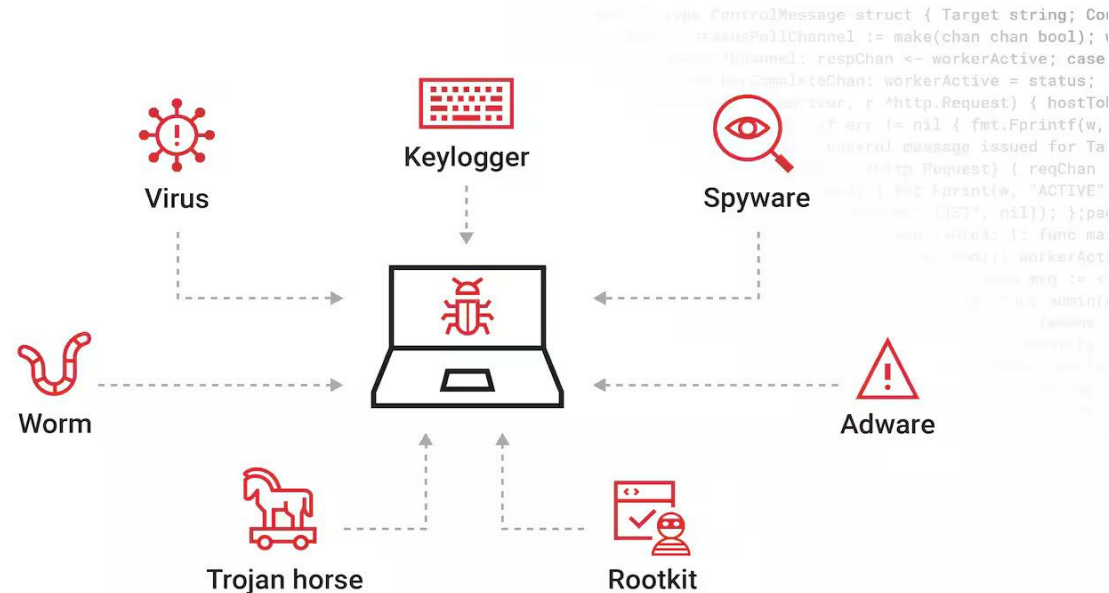
- Attackers want to access our assets such as data and other intellectual property, servers, computers, smart phones, tablets, and so on.

TERM	EXPLANATION
Threat	A potential danger to an asset such as data or the network itself.
Vulnerability	A weakness in a system or its design that could be exploited by a threat.
Attack Surface	An attack surface is the total sum of the vulnerabilities in a given system that are accessible to an attacker. The attack surface describes different points where an attacker could get into a system, and where they could get data out of the system.
Exploit	The mechanism that is used to leverage a vulnerability to compromise an asset. Exploits may be remote or local. A remote exploit is one that works over the network without any prior access to the target system. In a local exploit, the threat actor has some type of user or administrative access to the end system. It does not necessarily mean that the attacker has physical access to the end system.
Risk	The likelihood that a particular threat will exploit a particular vulnerability of an asset and result in an undesirable consequence.



# Malware definition

- Malware is a code or software designed to damage, disrupt, steal, or do illegitimate action on data, hosts, or networks.
- The three most common types of malware are **Virus**, **Worm**, and **Trojan horse**.





# Malware types

Malware Type	Description
Virus	Attaches to legitimate programs or files and spreads when the infected file is executed.
Worm	Self-replicates and spreads across networks without user interaction.
Trojan	Disguises itself as legitimate software but contains malicious code to perform unauthorized actions.
Spyware	Secretly monitors and collects user information, often for surveillance or data theft.
Adware	Displays unwanted advertisements on the user's device, often slowing down performance.
Ransomware	Encrypts files or locks users out of their system until a ransom is paid.
Rootkit	Grants attackers administrative-level control over a system while remaining hidden.

# Ransomware

- Ransomware is a malware that denies access to the infected computer system or its data.
- Ransomware frequently uses an encryption algorithm to encrypt system files and data.
- Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns.
- Social engineering is also used, when cybercriminals pretending to be security technicians
- make random calls at homes and persuade users to connect to a website that downloads ransomware to the user's computer



# WannaCry Ransomware



# Overview of Conti Ransomware

- **What is Conti Ransomware?**

Conti is a highly sophisticated ransomware strain first identified in early 2020, known for its rapid deployment and extensive use of double extortion tactics, where data is both encrypted and threatened with public release.

- **Key Characteristics:**

**Targeted Attacks:** Primarily focuses on high-value targets, including enterprises and critical infrastructure.

**Speed and Efficiency:** Capable of encrypting thousands of files in a matter of minutes.

**Communication:** Operates as a Ransomware-as-a-Service (RaaS), allowing affiliates to conduct attacks while the Conti group manages the backend.

**Notable Incidents:** in 2021, Conti attacked the Irish Health Service, disrupting healthcare services and leading to significant financial losses.

- **Attack Vector:**

- Often gains initial access through phishing emails, exploiting vulnerabilities, or using Remote Desktop Protocol (RDP).

# Common Network Attacks

Attack Type	Description
Man-in-the-Middle Attack	Attacker intercepts and potentially alters communication between two parties.
Buffer Overflow Attack	Exploits a system by overloading a buffer to execute malicious code.
DoS Attack	Denies legitimate users access to a resource by overwhelming the system with traffic.
DDoS Attack	Similar to DoS but launched from multiple compromised devices to flood a target.
ICMP Attack	Exploits ICMP protocol (Ping) to overwhelm the target with echo requests.

# Introduction to Network Discovery

- Definition:
  - Network discovery is the process of identifying devices, services, resources, and vulnerabilities on a network.
- Importance:
  - Provides visibility into network assets and vulnerabilities.  
Essential for security assessments, vulnerability management, and compliance.
  - Helps in network planning, management, and optimization.

# Key Network Discovery Techniques

## 1.Active Scanning

- 1.Description: Sends packets to various IP addresses to discover devices and open ports.
2. Tools: Nmap, Angry IP Scanner

## 2.Passive Scanning

- 1.Description: Monitors network traffic to identify devices and services without active probing.
2. Tools: Wireshark, PRTG Network Monitor

## 3.Network Mapping

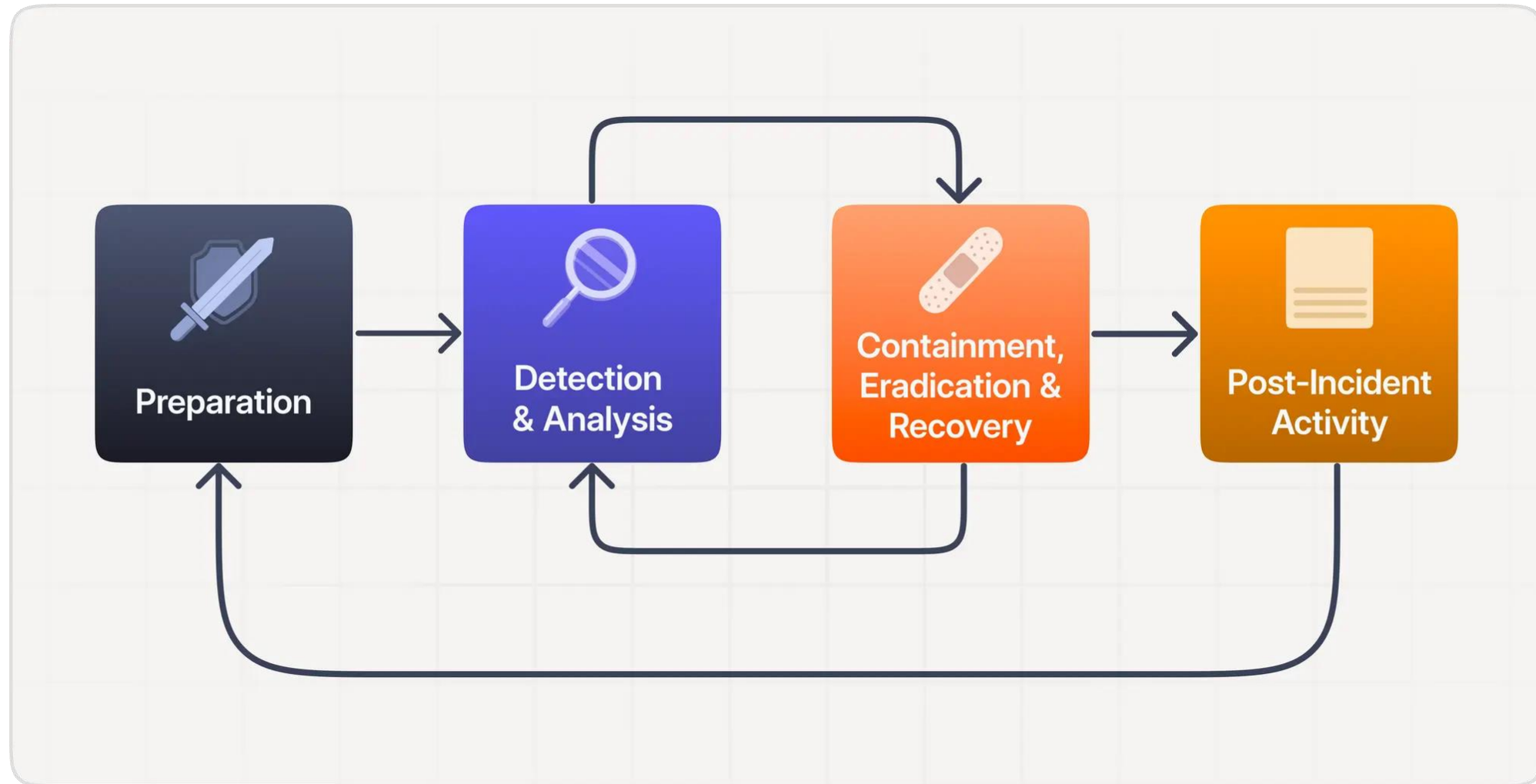
- 1.Description: Creates a visual representation of the network topology to identify potential vulnerabilities.
2. Tools: SolarWinds Network Topology Mapper

# Network Discovery Role in Incident Response

- **Initial Assessment:** Quickly identifies affected devices and the scope of the incident.
- **Forensic Analysis:** Helps trace back the attack path and understand the impact.
- **Vulnerability Assessment:** Facilitates identifying unpatched systems and vulnerable services during a response.
- **Continuous Monitoring:** Regularly use network discovery techniques to stay ahead of threats.
- **Integration with SIEM:** Incorporate findings into Security Information and Event Management (SIEM) systems for better incident response.
- **Documentation:** Keep detailed records of network configurations and changes for forensic readiness.

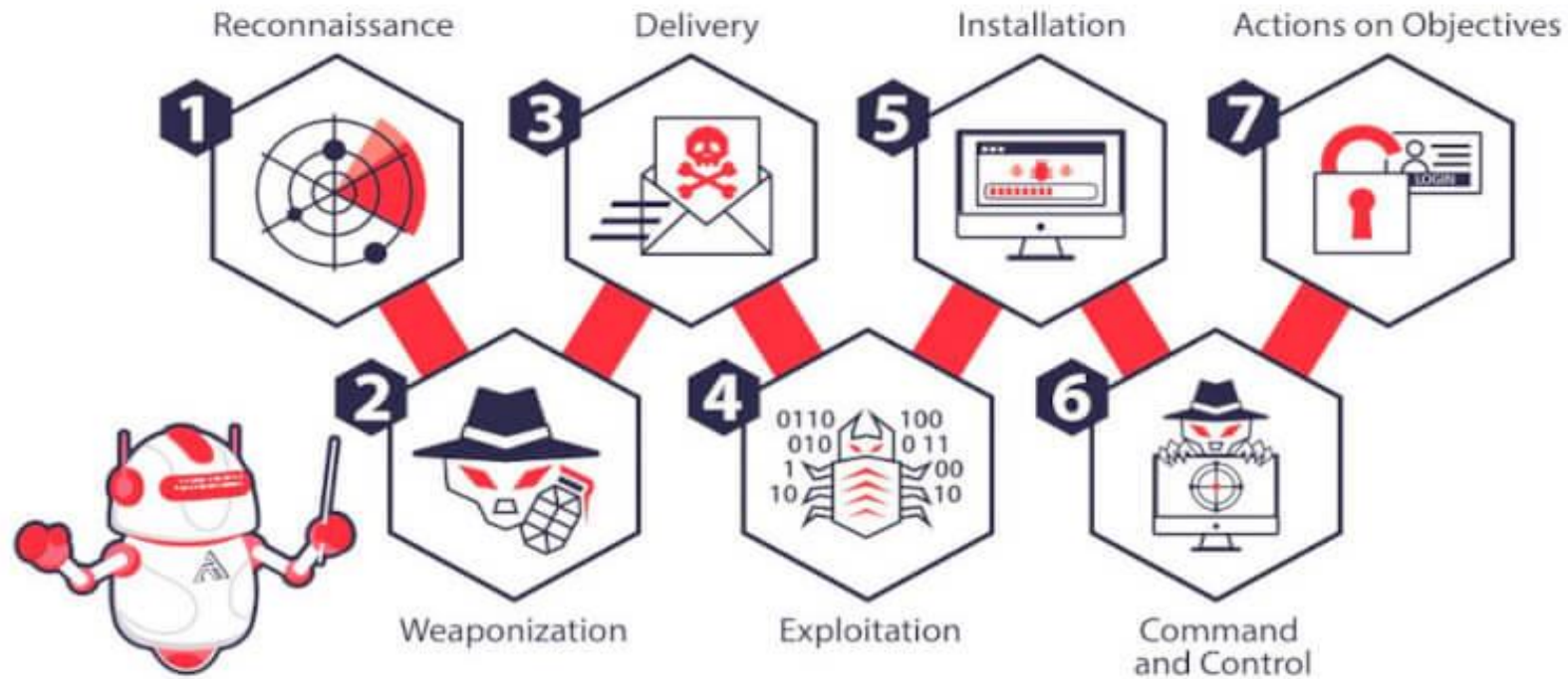


# Phases of Incident Response



# Cyber kill chain phases

## THE CYBER KILL CHAIN





# Incident Response Plan (IRP): Preparation and Implementation

An introduction to the key elements and steps involved in preparing and implementing an effective Incident Response Plan to address security incidents and breaches.

# Roles and Responsibilities



## Incident Responders

Responsible for coordinating the immediate response to the incident, including containment, investigation, and mitigation efforts.



## Security Analysts

Responsible for analyzing security data, identifying threats, and providing recommendations to improve security posture.



## System Administrators

Responsible for maintaining and securing the systems and infrastructure involved in the incident, and providing technical support to the incident response team.



## Management

Responsible for providing direction, resources, and decision-making authority to the incident response team, as well as communicating with stakeholders.

Clearly defining the roles and responsibilities of each individual involved in the incident response process is crucial for an effective and coordinated response.

# Communication Protocols



## Reporting Procedures

Establish clear guidelines for how to report security incidents, including designated points of contact, communication channels, and required information.



## Escalation Matrix

Develop an escalation matrix to determine when and how to elevate incident response activities to higher levels of management or specialized teams.



## Coordination Mechanisms

Implement coordination mechanisms, such as regular meetings, shared documentation, and communication tools, to ensure a cohesive and collaborative incident response effort.



## Incident Response Plan

Integrate incident response activities into a comprehensive plan that outlines the overall process, roles and responsibilities, and decision-making frameworks.

Effective communication protocols are essential for a successful and coordinated incident response. By establishing clear reporting procedures, escalation mechanisms, and coordination processes, organizations can enhance their ability to detect, respond to, and mitigate security incidents in a timely and effective manner.



# Escalation Procedures

- **Define Incident Severity Levels**

Establish a clear classification system to categorize incidents based on factors such as impact, urgency, and potential consequences. This could include levels ranging from low-impact/low-priority to high-impact/critical.

- **Establish Notification Thresholds**

Determine the specific criteria that would trigger the escalation of an incident to the next level of management, such as the number of users affected, the business function disrupted, or the estimated financial or reputational impact.

- **Identify Escalation Contacts**

Maintain a up-to-date directory of key stakeholders and decision-makers who should be notified in the event of an escalated incident, along with their contact information and preferred communication channels.

- **Outline Escalation Workflow**

Document the step-by-step process for how incidents should be escalated, including who is responsible for initiating the escalation, the required approvals or authorizations, and the expected timeline for response and resolution.

- **Establish Communication Protocols**

Define clear guidelines for how information about escalated incidents should be communicated, including the frequency of updates, the level of detail to be provided, and the preferred communication methods (e.g., email, conference calls, status reports).

# Recovery Strategies



## Backup Procedures

Regularly backup critical data, systems, and configurations to secure off-site or cloud-based storage locations.



## Disaster Recovery Plans

Establish comprehensive disaster recovery plans to ensure seamless restoration of systems and data in the event of an incident.



## Contingency Planning

Develop detailed contingency plans to address various failure scenarios, including hardware/software failures, natural disasters, and cyber-attacks.



## Restoration Strategies

Outline step-by-step procedures for restoring systems and data from backups, ensuring a timely and effective recovery process.

By implementing robust recovery strategies, organizations can minimize the impact of incidents and ensure the continuity of their critical operations.

# Regular Training



## Educate Employees

Conduct training sessions to educate about security best practices, such as identifying phishing attempts, creating strong passwords, and safely handling sensitive information.



## Incident Recognition

Train employees to recognize signs of security incidents, such as suspicious emails, unauthorized access attempts, or unusual system behavior, and how to properly report them.



## Reporting Procedures

Ensure employees understand the established reporting procedures for security incidents, including whom to notify and how to escalate issues to the appropriate personnel.

Regular training is essential for maintaining a strong security culture within the organization. By educating employees on security best practices, incident recognition, and reporting procedures, you can empower them to be the first line of defense against cyber threats.



# Awareness Campaigns



## Regular Security Awareness Training

Conduct frequent training sessions to educate employees on best practices, common threats, and role in maintaining a secure environment.



## Phishing Simulation Exercises

Simulate phishing attacks to assess employee preparedness and identify areas for improvement in spotting suspicious emails.



## Informative Posters and Newsletters

Display posters and distribute newsletters highlighting security tips, policies, and incident reporting procedures.



## Security Awareness Contests

Organize contests and challenges to engage employees and reinforce security-conscious behaviors, such as password management or device locking.

By implementing a comprehensive awareness campaign, the organization can cultivate a security-conscious culture, empower employees to be vigilant, and reduce the risk of security breaches.

# Phishing Simulations



## Assess employee awareness

Evaluate how well employees can identify phishing attempts and report suspicious emails or messages.



## Customize scenarios

Design phishing simulation campaigns that mimic real-world threats and tactics used by cybercriminals.



## Track and analyze results

Monitor employee responses, identify training gaps, and measure the effectiveness of your phishing simulations.



## Provide feedback and

Offer educational resources and guidance to help employees improve their ability to recognize and report phishing attempts.

Conducting regular phishing simulations is a critical component of a comprehensive cybersecurity strategy, helping to strengthen employee vigilance and organizational resilience against phishing attacks.

# Security Technologies

- **Security Information and Event Management (SIEM)**

Centralized platform to collect, analyze, and correlate security-related data from various sources to detect, investigate, and respond to security incidents.

- **Intrusion Detection/Prevention System (IDS/IPS)**

Monitors network traffic to identify and prevent suspicious activity, such as unauthorized access attempts, malware infections, and cyber attacks.

- **Firewall**

Establishes a barrier between a trusted, internal network and an untrusted, external network, controlling and monitoring incoming and outgoing traffic based on predefined security rules.

- **Antivirus Software**

Detects, prevents, and removes malware, such as viruses, worms, and Trojans, to protect your systems and data from unauthorized access and damage.

- **Data Loss Prevention (DLP) Solution**

Monitors, detects, and prevents the unauthorized access, use, or transmission of sensitive or confidential data, ensuring data security and regulatory compliance.

# Partnerships



## Law Enforcement Collaboration

Establish communication channels with local, state, and federal law enforcement agencies to facilitate timely incident reporting and coordinate response efforts.



## Cybersecurity Expert Networking

Engage with cybersecurity experts, such as incident response teams and threat intelligence analysts, to share threat information and best practices for prevention and mitigation.



## Industry Association Engagement

Participate in industry-specific associations and forums to collaborate with peers, stay informed emerging threats, and collectively develop strategies to address common security challenges.

By fostering partnerships across law enforcement, cybersecurity experts, and industry associations, organizations can build a comprehensive and coordinated approach to incident response, leveraging shared knowledge and resources to enhance their overall cybersecurity posture.

# Service Outage!



readme - Notepad

File Edit Format View Help

All of your files are currently encrypted by CONTI strain.

As you know (if you don't - just "google it"), all of the data that has been encrypted by our software cannot be recovered by any means without contacting our team directly. If you try to use any additional recovery software - the files might be damaged, so if you are willing to try - try it on the data of the lowest value.

To make sure that we REALLY CAN get your data back - we offer you to decrypt 2 random files completely free of charge.

You can contact our team directly for further instructions through our website :

TOR VERSION :

(you should download and install TOR browser first <https://torproject.org>)

<http://conti>

HTTPS VERSION :

<https://conti>

YOU SHOULD BE AWARE!

Just in case, if you try to ignore us. We've downloaded a p

---BEGIN ID---

EdKBszpVz7i

---END ID---

TgA3E

Parser Error

The resource cannot be found.

← → ↻

<https://win-aoqkg2as2q7.bellybear.local/owa/auth/login.aspx?url=https://win-aoqkg2as2q7.bellybear.local/owa/%3FauthRedirect=true&reason=0#path=/mail>

Server Error in '/owa' Application.

Parser Error

Description: An error occurred during the parsing of a resource required to service this request. Please review the following specific parse error details and modify your source file appropriately.

Parser Error Message: Could not load type 'Microsoft.Exchange.HttpProxy.Logon'.

Source Error:

Line 1: <%@ Page language="c#" AutoEventWireup="false" Inherits="Microsoft.Exchange.HttpProxy.Logon" %>  
Line 2: <%@ Import namespace="Microsoft.Exchange.Clients"%>  
Line 3: <%@ Import namespace="Microsoft.Exchange.Clients.Owa.Cone"%>

Source File: /owa/auth/login.aspx Line: 1

Version Information: Microsoft .NET Framework Version:4.0.30319; ASP.NET Version:4.8.4110.0

# Conti\_ransomware\_note.txt

```
1 index=* sourcetype="winEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=11 *.txt
2 | table Image TargetFilename _time
```

Image ↕	TargetFilename ↕
c:\Users\Administrator\Documents\cmd.exe	C:\Users\Public\Downloads\readme.txt
c:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Videos\readme.txt
c:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Saved Games\readme.txt
c:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Pictures\readme.txt
c:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Music\readme.txt
c:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Links\readme.txt
c:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Favorites\readme.txt

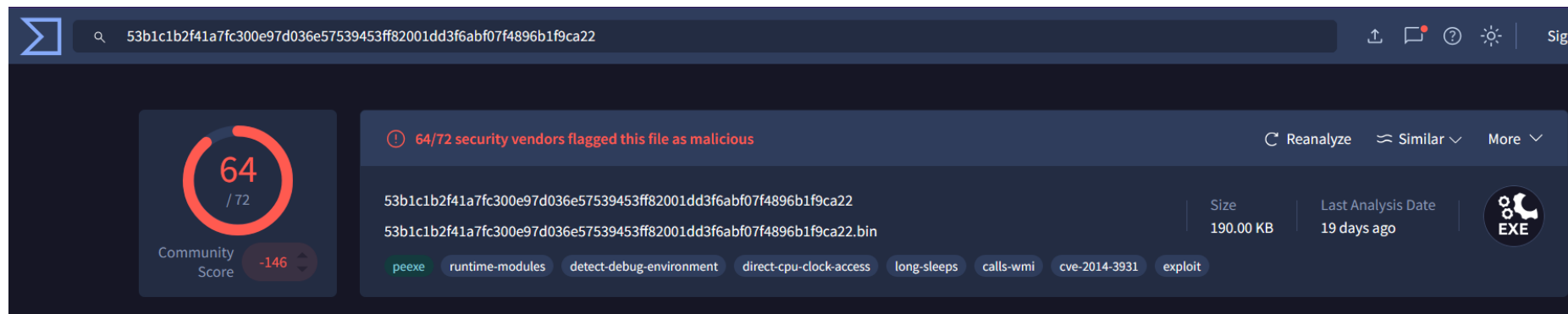
# Ransomware ?!

- Splunk Query:

```
1 index=* sourcetype="winEventLog:Microsoft-Windows-Sysmon/Operational" *.exe
2 | dedup CurrentDirectory
3 | table CurrentDirectory CommandLine Image Hashes ParentCommandLine ParentImage _time
```

c:\Users\Administrator\Documents\ cmd.exe

C:\Users\Administrator  
\Documents\cmd.exe



The screenshot shows the VirusTotal interface for a file with SHA256 hash 53b1c1b2f41a7fc300e97d036e57539453ff82001dd3f6abf07f4896b1f9ca22. The file is identified as 53b1c1b2f41a7fc300e97d036e57539453ff82001dd3f6abf07f4896b1f9ca22.bin, with a size of 190.00 KB and analyzed 19 days ago. A red warning icon indicates that 64 out of 72 security vendors flagged the file as malicious. The Community Score is 64/72, with a score of -146. The file is categorized as EXE. Various tags are listed below the file name, including peexe, runtime-modules, detect-debug-environment, direct-cpu-clock-access, long-sleeps, calls-wmi, cve-2014-3931, and exploit.

53b1c1b2f41a7fc300e97d036e57539453ff82001dd3f6abf07f4896b1f9ca22

Size: 190.00 KB | Last Analysis Date: 19 days ago

64/72 security vendors flagged this file as malicious

Community Score: 64 / 72 (-146)

peexe runtime-modules detect-debug-environment direct-cpu-clock-access long-sleeps calls-wmi cve-2014-3931 exploit

# New user creation !!!

## New Search

```
1 index=* sourcetype="WinEventLog:Security" EventCode=4720
2 |table Account_Name _time
```

✓ **2 events** (before 10/21/24 2:20:57.000 PM) No Event Sampling ▼

Events Patterns **Statistics (2)** Visualization

100 Per Page ▼ ✎ Format Preview ▼

Account\_Name ⇅

WIN-A00KG2AS207\$

securityninja

MINWINPC\$

WDAGUtilityAccount



# Assigning the new user to interesting groups


```
1 index=* sourcetype="winEventLog:Microsoft-Windows-Sysmon/Operational" securityninja
2 | table CommandLine _time Image ParentCommandLine ParentImage
```

✓ 6 events (before 10/21/24 2:24:42.000 PM) No Event Sampling ▼

Events Patterns **Statistics (6)** Visualization

100 Per Page ▼ / Format Preview ▼

CommandLine ↕	_time ↕
C:\Windows\system32\net1 localgroup "Remote Desktop Users" "securityninja" /add	2021-09-08 13:04:11
net localgroup "Remote Desktop Users" "securityninja" /add	2021-09-08 13:04:11
C:\Windows\system32\net1 localgroup administrators securityninja /add	2021-09-08 13:04:10
net localgroup administrators securityninja /add	2021-09-08 13:04:10
C:\Windows\system32\net1 user /add securityninja hardToHack123\$	2021-09-08 13:04:10
net user /add securityninja hardToHack123\$	2021-09-08 13:04:10



# Privilege Escalation !!!

## CreateRemoteThread

```
1 index=* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=8
2 | table SourceImage TargetImage _time
```

✓ 2 events (before 10/21/24 2:31:42.000 PM) No Event Sampling ▼

Events Patterns **Statistics (2)** Visualization

100 Per Page ▼ / Format Preview ▼

SourceImage ↕	TargetImage ↕
C:\Windows\System32\wbem\unsecapp.exe	C:\Windows\System32\lsass.exe
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Windows\System32\wbem\unsecapp.exe

# What is **lsass.exe** ?

- Managing user logins and logouts
- Authenticating users and services
- Handling password changes and password policies
- Contains the password of users in hash format

# Why migrating to **lsass.exe** ?

- **Elevated Privileges:** higher privilege
- **Persistence:** less likely to be terminated
- **Stealth:** hiding within a legitimate system process
- **Access to Credentials:** ability to access and steal stored credentials
- **Lateral Movement:** using the harvested credentials
- **Data Exfiltration:** send sensitive back to the attacker

# Conti uses Web Shell ?!

```
1 index=* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" *.aspx
2 | table CurrentDirectory CommandLine Image ParentCommandLine ParentImage _time
```

✓ 1 event (before 10/21/24 4:18:52.000 PM) No Event Sampling ▼

Events (1) Patterns **Statistics (1)** Visualization

100 Per Page ▼ / Format Preview ▼

CurrentDirectory ⚙ / CommandLine ⚙

c:\windows\system32 \inetsrv\	attrib.exe -r \\win-aoqkg2as2q7.bellybear.local\C\$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\i3gfPctK1c2x.aspx
----------------------------------	--

# Weaponizing a shell !

1 index=\* i3gfPctK1c2x.aspx All time 🔍

✓ 1 event (before 10/21/24 4:49:37.000 PM) No Event Sampling ▾ Job ▾ || ■ → 🖨️ ⬇️ ⚠️ Smart Mode ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 millisecond per column

List ▾ ✎ Format 20 Per Page ▾

< Hide Fields :≡ All Fields

SELECTED FIELDS  
a host 1  
a source 1  
a sourcetype 1

INTERESTING FIELDS  
a CommandLine 1  
a Company 1  
a ComputerName 1  
a CurrentDirectory 1  
a Description 1  
...

i	Time	Event
>	9/8/21 12:52:09.000 PM	... 24 lines omitted ... OriginalFileName: ATTRIB.EXE <b>CommandLine: attrib.exe -r \\.\win-aoqkg2as2q7.bellybear.local\C\$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\i3gfPctK1c2x.aspx</b> CurrentDirectory: c:\windows\system32\inetsrv\ User: NT AUTHORITY\SYSTEM ... 8 lines omitted ... ParentCommandLine: C:\Windows\system32\cmd.exe <a href="#">Show all 37 lines</a> host = WIN-AOQKG2AS2Q7 source = WinEventLog:Microsoft-Windows-Sysmon/Operational sourcetype = WinEventLog:Microsoft-Windows-Sysmon/Operational

# delivery !!



9/8/21 12:51:50.000 PM 2021-09-08 19:51:50 10.10.10.6 POST /owa/auth/i3gfPctK1c2x.aspx &CorrelationID=<empty>;&cafeReqId=e4f48fdc-0910-4b2e-9481-8802eee61b57;&encoding=; 443 - 10.10.10.2 Mozilla/5.0 - 200 0 0 54

Event Actions ▾

Type	<input checked="" type="checkbox"/>	Field	Value	Actions
Selected	<input checked="" type="checkbox"/>	host ▾	WIN-AOQKG2AS2Q7	▾
	<input checked="" type="checkbox"/>	source ▾	C:\inetpub\logs\LogFiles\W3SVC1\u_ex210908.log	▾
	<input checked="" type="checkbox"/>	sourcetype ▾	iis	▾
Event	<input type="checkbox"/>	CorrelationID ▾	<empty>	▾
	<input type="checkbox"/>	c_ip ▾	10.10.10.2	▾
	<input type="checkbox"/>	cafeReqId ▾	e4f48fdc-0910-4b2e-9481-8802eee61b57;	▾
	<input type="checkbox"/>	cs_User_Agent ▾	Mozilla/5.0	▾
	<input type="checkbox"/>	cs_method ▾	POST	▾
	<input type="checkbox"/>	cs_uri_query ▾	&CorrelationID=<empty>;&cafeReqId=e4f48fdc-0910-4b2e-9481-8802eee61b57;&encoding=;	▾
	<input type="checkbox"/>	cs_uri_stem ▾	/owa/auth/i3gfPctK1c2x.aspx	▾
	<input type="checkbox"/>	date ▾	2021-09-08	▾
	<input type="checkbox"/>	s_ip ▾	10.10.10.6	▾
	<input type="checkbox"/>	s_port ▾	443	▾
	<input type="checkbox"/>	sc_status ▾	200	▾
	<input type="checkbox"/>	sc_substatus ▾	0	▾
	<input type="checkbox"/>	sc_win32_status ▾	0	▾
	<input type="checkbox"/>	time ▾	19:51:50	▾
	<input type="checkbox"/>	time_taken ▾	54	▾

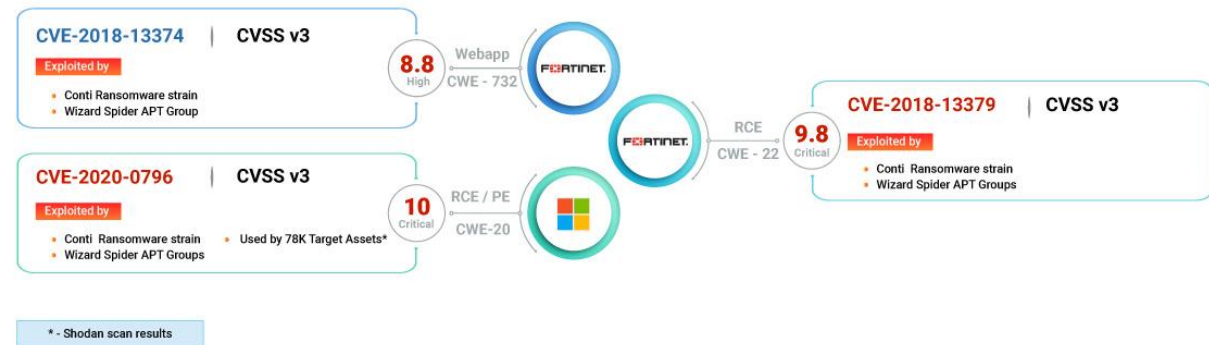
# Conti CVEs !

CVE-2020-0796: The attack showed lateral movement across systems, evidenced by the attacker migrating processes and escalating privileges using commands like: **net user /add** and **net localgroup administrators /add**

CVE-2018-13374 and CVE-2018-13379:  
The web shell (**i3gfPctK1c2x.aspx**)  
was deployed on the Exchange server  
through a vulnerability that enabled  
unauthorized file upload and execution.



## Vulnerabilities used by Conti Ransomware





# Post-Incident Overview

## Introduction

Outlines post-incident activities after the Conti ransomware attack. Goals: Review the incident, assess impact, document lessons, and improve future defenses.

## Objectives

- **Evaluate Response:** Identify strengths and weaknesses.
- **Document Findings:** Record key attack details and IOCs.
- **Identify Lessons:** Extract insights to enhance preparedness.
- **Strengthen Security:** Update policies and procedures.
- **Improve Training:** Educate staff on ransomware threats.



# Incident Timeline & Response

## - Incident Timeline

### Detection:

- **Date & Time:** Initial reports of Outlook and Exchange Admin Center access issues.
- **Indicators:** Ransom notes found on the Exchange server.

### Response Actions:

- Immediate isolation of affected systems.
- Notifications to key stakeholders; activated response protocols.

### Recovery:

- Restored services using clean backups and patched vulnerabilities.

## - Response Effectiveness

### Strengths:

- Rapid attack identification and system isolation.
- Effective team communication.

### Weaknesses:

- Delayed detection of the initial attack vector.
- Limited initial scope assessment led to extended recovery time.

# Incident Report & Findings

## Incident Overview

- **Type:** Conti Ransomware
- **Delivery:** Phishing email with malicious links exploiting Exchange Server vulnerabilities.

## Impact Assessment

- **Systems Affected:** Exchange Server, user workstations.
- **Data Loss:** Critical files potentially encrypted; ransom demands issued.
- **Downtime:** Email outage for approximately 72 hours.
- **Financial Impact:** Recovery costs, potential ransom, and reputational damage.

## Indicators of Compromise (IOCs)

- **File Path:** C:\Users\Administrator\Documents\cmd.exe
- **MD5 Hash:** 290C7DFB01E50CEA9E19DA81A781AF2C
- **File Names:** readme.txt; i3gfPctK1c2x.aspx

## Key Takeaways:



- **Regular Backups:** Ensure data recovery capabilities.
- **Timely Patching:** Keep systems updated to prevent exploitation.
- **Employee Training:** Continuous awareness on cybersecurity best practices.
- **Regular Security Assessments:** Conduct vulnerability assessments and penetration tests to identify risks proactively.
- **Threat Intelligence Integration:** Leverage real-time threat feeds to stay ahead of emerging threats.

# Detailed Lessons & Actions

## Phishing Threats

*Lesson:* Phishing email not identified promptly.

*Action:* Enhance email filtering and train users.

## Vulnerability Management

*Lesson:* Outdated patches led to exploited vulnerabilities.

*Action:* Enforce a regular patch management schedule.

## Incident Detection

*Lesson:* Reliance on user reports for detection.

*Action:* Improve monitoring with SIEM tools.

## Communication Protocols

*Lesson:* Communication during the incident was fragmented.

*Action:* Develop clear protocols with designated spokespeople.

## Response Time

*Lesson:* Response time was slower than expected.

*Action:* Conduct regular tabletop exercises to improve preparedness.

# Enhancing Security Measures

## Update Incident Response Plans

- Revise plans incorporating lessons learned.
- Ensure team contact details are current.
- Clearly define roles and responsibilities.

## Implement Technical Controls

- **Patch Vulnerabilities:** Apply patches to the Exchange Server.
- **Network Segmentation:** Isolate critical systems from less secure networks.
- **Access Controls:**
  - Implement Multi-Factor Authentication (MFA).
  - Audit user accounts for least privilege access.
- **Endpoint Protection:**
  - Deploy EDR solutions.
  - Ensure endpoints have updated antivirus software.

## Training & Continuous Monitoring

- **Employee Training:**
  - Conduct workshops on phishing and social engineering.
  - Update incident response training.
- **Continuous Monitoring:**
  - Utilize SIEM tools to monitor for IOCs.
  - Set alerts for unauthorized account creation and suspicious file changes.

# System Hardening

## Update and Patch Regularly

**Firmware Updates:** Ensure the firewall firmware is always up-to-date with the latest security patches.

**Regular Patching:** Apply patches promptly to address any vulnerabilities.

## Implement Advanced Features

### Intrusion Prevention Systems (IPS)

Use IPS to detect and block malicious activities.

**Application Layer Filtering:** Implement application layer filtering to inspect and control traffic based on application data.

## Regular Audits

Conduct regular audits of firewall logs to detect and respond to suspicious activities

## Configuration Changes for Firewalls

## Configure Rules and Policies

**Least Privilege:** Implement the principle of least privilege by allowing only necessary traffic.

**Deny by Default:** Set default policies to deny all traffic and explicitly allow only required services

## Enable Logging and Monitoring

**Detailed Logs** Enable detailed logging to monitor all traffic passing through the firewall.

