



# INCIDENT RESPONSE FRAMEWORK

A complete incident response framework including planning, execution, and review based on various cybersecurity principles

## Prepared by:

*Mohamed Samir Helmy*

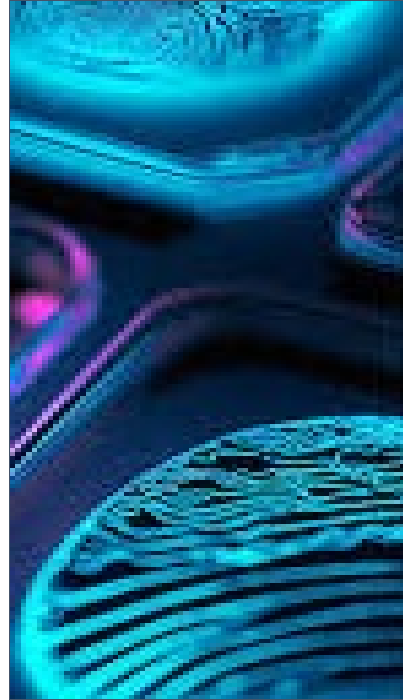
*Mahmoud badr abdelhamid*

*Mohamed mohsen gamal*

*Mohamed Soudi Yousef*

*Menna mohamed salman*

*Mohammad Hesham Mohammad*



Conti Ransomware  
Incident Response

## **Basic cybersecurity concepts**

### **What is Cybersecurity:**

Cybersecurity is primarily concerned with protecting digital assets from malicious attacks that originate in cyberspace. It involves safeguarding computer systems, networks, and data from unauthorized access, theft, damage, or disruption. Cybersecurity professionals focus on preventing, detecting, and responding to cyber threats such as:

**Malware:** Viruses, worms, trojans, ransomware, and spyware.

**Phishing:** Attempts to deceive individuals into revealing sensitive information.

**Denial of Service (DoS) attacks:** Overwhelming a system or network to prevent legitimate users from accessing it.

**Social engineering:** Manipulating people to divulge confidential information or perform actions that compromise security.

**Data breaches:** Unauthorized access to sensitive data.

### **What is Information Security:**

Information security is a broader field that encompasses the protection of information assets in all forms, including physical, digital, and analog. It focuses on ensuring the confidentiality, integrity, and availability (CIA) of information. Information security professionals address threats that can come from various sources, such as:

**Physical security:** Protecting physical assets like hardware, data centers, and paper records.

**Operational security:** Implementing policies and procedures to prevent unauthorized access and data breaches.

**Technical security:** Using technological controls to protect information systems.

### **The CIA Triad: Confidentiality, Integrity, and Availability**

The CIA Triad is a fundamental security model that outlines the three core objectives of information security:

**Confidentiality:** Ensuring that information is accessible only to authorized individuals. This prevents unauthorized disclosure or access to sensitive data.

**Integrity:** Maintaining the accuracy and completeness of information. This protects against unauthorized modifications or alterations to data.

**Availability:** Ensuring that authorized users can access information when they need it. This prevents interruptions or disruptions to services.

These three principles work together to protect information assets and maintain the security of systems.

### **What is Hashing:**

Hashing is a one-way function that transforms data into a fixed-length string called a hash value. The hash value is unique to the original data, meaning that even a slight change in the data will result in a completely different hash value.

### **Key characteristics of hashing:**

One-way: It's impossible to reverse the process and recover the original data from the hash value.

Fixed length: The hash value is always the same size, regardless of the input data.

Unique: Different data inputs will produce different hash values.

Common uses of hashing:

Password storage: Hashing passwords before storing them makes it difficult for attackers to recover the original passwords even if the database is compromised.

Data integrity: Comparing the hash value of a file with a previously stored hash value can verify if the file has been modified.

Digital signatures: Hashing a document and then encrypting the hash value with a private key creates a digital signature that can be used to verify the authenticity and integrity of the document.

### **What is Encryption:**

Encryption is a process that transforms data into a scrambled format that is unintelligible to unauthorized parties. This process requires a cryptographic key to encrypt and decrypt the data.

## Key characteristics of encryption:

**Reversible:** The original data can be recovered from the encrypted data using the correct decryption key.

**Variable length:** The encrypted data may be larger or smaller than the original data.

**Secure:** A strong encryption algorithm and a securely managed key are essential for protecting the encrypted data.

## Common uses of encryption:

**Data transmission:** Encrypting data before transmitting it over a network prevents unauthorized interception and access.

**Data storage:** Encrypting data at rest protects it from unauthorized access even if the storage device is compromised.

**Secure communication:** Encryption is used to protect sensitive information exchanged over communication channels

Difference between hashing and encryption:

Hashing	Encryption
One-way	Reversible
Data integrity, password storage, digital signatures	Data confidentiality, secure communication
No key required	Requires a key for encryption and decryption

# **Common cybersecurity terminologies**

## **Threat**

A potential danger to an asset such as data or the network itself

## **Vulnerabilities**

A vulnerability is a weakness or flaw in a system or application that can be exploited by an attacker to gain unauthorized access or control. Vulnerabilities can arise from various factors, including programming errors, design flaws, and configuration mistakes. Examples of vulnerabilities include buffer overflows, SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

## **Attack Surface**

An attack surface refers to the parts of a system or application that are exposed to potential attacks. It encompasses the entry points through which an attacker can exploit vulnerabilities. The attack surface can include network interfaces, web applications, APIs, and physical access points.

## **Exploits**

An exploit is a piece of code or technique that takes advantage of a vulnerability to compromise a system or application. Exploits can be used to gain unauthorized access, steal data, or disrupt services. Attackers often develop and share exploits to target specific vulnerabilities.

## **Risk**

Risk is the potential for a threat to exploit a vulnerability and cause harm or damage. It is typically assessed by considering the likelihood of an attack occurring and the potential impact of such an attack. Risk management involves identifying, assessing, and mitigating risks to protect systems and data.

## **Key Relationships to Risk:**

**Vulnerability:** A weakness in a system or application.

**Attack Surface:** The parts of a system exposed to attacks.

**Exploit:** Code or technique that leverages a vulnerability.

**Threat:** A potential attacker or malicious event.

**Risk:** The likelihood and potential impact of a threat exploiting a vulnerability.

### **Example:**

**Vulnerability:** A SQL injection vulnerability in a web application.

**Attack Surface:** The web application's input forms.

**Exploit:** A malicious SQL query that can be injected into the application to execute unauthorized commands.

**Threat:** A malicious actor with knowledge of the vulnerability.

**Risk:** The potential for the attacker to steal sensitive data or disrupt the application's functionality.

## **Risk Management and Risk Management Strategy**

### **What is a risk management**

Risk management is the process of identifying, assessing, and mitigating risks to protect assets and achieve organizational objectives. It involves evaluating potential threats and vulnerabilities, assessing their likelihood and impact, and developing strategies to reduce or eliminate them.

Risk management strategy outlines the specific approach and methods an organization will use to manage risks. It typically includes:

**Risk identification:** Identifying potential threats and vulnerabilities.

**Risk assessment:** Evaluating the likelihood and impact of each risk.

**Risk response:** Developing strategies to mitigate, avoid, transfer, or accept risks.

**Risk monitoring and control:** Continuously monitoring risks and taking corrective actions as needed.

# Types of Malwares

Malware, short for malicious software, is any software designed to harm or damage computer systems or networks. There are many different types of malware, each with its own unique characteristics and objectives. Some common types of malware include:

**Viruses:** Self-replicating programs that attach themselves to other files and execute when the infected file is run.

**Worms:** Self-propagating programs that spread across networks without requiring human intervention.

**Trojans:** Malicious programs disguised as legitimate software.

**Ransomware:** Malware that encrypts or locks files, demanding a ransom payment for decryption or access.

**Spyware:** Software that secretly monitors a user's activities and collects personal information.

**Adware:** Software that displays unwanted advertisements.

**Rootkits:** Malware that hides itself deep within a system's operating system.

**Bots:** Malicious programs that can be controlled remotely by an attacker.

**Phishing:** Emails or messages designed to trick users into revealing sensitive information.

Fileless Malware:

**Living Off the Land (LOL) Binaries:** Malware that leverages legitimate system tools and binaries to execute malicious actions.

**Memory-Based Malware:** Malware that primarily resides in system memory, making it difficult to detect and remove.

**Mobile Malware:**

**SMS Trojans:** Malware that intercepts and sends text messages without the user's knowledge.

**Mobile Spyware:** Malware that secretly monitors a user's mobile device activities and collects personal information.

**Fake Apps:** Malicious apps disguised as legitimate ones.

## **Targeted Malware:**

**Nation-State Malware:** Malware developed by governments for espionage or sabotage purposes.

**Supply Chain Attacks:** Attacks targeting software supply chains to compromise multiple systems.

## **Cryptojacking Malware:**

**Cryptomining Malware:** Malware that secretly uses a system's resources to mine cryptocurrency.

## **Polymorphic Malware:**

**Metamorphic Malware:** Malware that constantly changes its code to evade detection.

**Polymorphic Malware:** Malware that changes its form but maintains its functionality.

**Bootkit:** Malware that infects a system's boot sector, allowing it to execute before the operating system loads.

**Keylogger:** Malware that records keystrokes to steal sensitive information.

**Clicker:** Malware that generates fake clicks on advertisements or links.

**Spam:** Unsolicited emails, often containing malicious links or attachments.

## **Common Network Attacks**

### **Man-in-the-Middle (MitM) Attacks**

A MitM attack occurs when an attacker intercepts communications between two parties, potentially altering or eavesdropping on the data. This can be achieved through various techniques, such as setting up a rogue Wi-Fi access point or exploiting vulnerabilities in encryption protocols.

### **Buffer Overflow Attacks**

A buffer overflow attack exploits a vulnerability in a program that allows an attacker to write data beyond the allocated memory buffer. This can lead to the execution of malicious code, gaining unauthorized access, or causing the program to crash.



## **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks**

DoS and DDoS attacks aim to overwhelm a system or network with excessive traffic, making it unavailable to legitimate users. A DoS attack originates from a single source, while a DDoS attack involves multiple compromised systems (bots) working together to launch attacks.

## **ICMP (Internet Control Message Protocol) Attacks**

ICMP is used for network diagnostics and error reporting. ICMP attacks exploit vulnerabilities in ICMP implementations to disrupt network services or gather information. Examples include ICMP flood attacks and ICMP ping of death attacks.

## **Amplification and Reflection Attacks**

Amplification and reflection attacks exploit the amplification factor of certain protocols to launch large-scale DoS attacks. The attacker sends crafted requests to vulnerable servers, which respond with much larger replies, overwhelming the target. Examples include DNS amplification attacks and NTP amplification attacks.

## **Address Spoofing Attacks**

Address spoofing involves disguising the source IP address of a packet to hide the attacker's identity. This can be used to launch attacks without being traced or to bypass security measures.

## **TCP (Transmission Control Protocol) Attacks**

TCP is a reliable connection-oriented protocol used for most internet traffic. TCP attacks exploit vulnerabilities in TCP implementations, such as TCP SYN flood attacks, which aim to exhaust a server's resources by sending a large number of SYN packets without completing the three-way handshake.

## **Other Common Network and Web Attacks**

### **SQL Injection Attacks**

SQL injection attacks exploit vulnerabilities in web applications that allow an attacker to inject malicious SQL code into a database query. This can be used to steal sensitive data, modify or delete records, or even gain unauthorized access to the database.

**Real-life example:** In 2016, a SQL injection vulnerability in the WordPress plugin "WP Statistics" allowed attackers to gain full control of websites, stealing user data and installing malware.

### **Cross-Site Scripting (XSS) Attacks**

XSS attacks occur when malicious code is injected into a web page and executed by the user's browser. This can be used to steal cookies, redirect users to malicious websites, or execute arbitrary JavaScript code.

**Real-life example:** In 2018, a cross-site scripting vulnerability in the Magento e-commerce platform allowed attackers to steal customer credit card information.

### **Cross-Site Request Forgery (CSRF) Attacks**

CSRF attacks trick a user's browser into performing unauthorized actions on their behalf. This can be used to hijack user sessions, change passwords, or make unauthorized purchases.

**Real-life example:** In 2017, a CSRF vulnerability in the Drupal content management system allowed attackers to execute arbitrary code on websites, potentially leading to data breaches or website defacement.

### **Zero-Day Attacks**

Zero-day attacks exploit vulnerabilities that are unknown to the software vendor and have not been patched. These attacks are particularly dangerous because they can be difficult to defend against until a patch is released.

**Real-life example:** In 2017, the WannaCry ransomware attack exploited a zero-day vulnerability in Microsoft's SMB protocol to infect hundreds of thousands of computers worldwide.

### **Phishing Attacks**

Phishing attacks involve sending fraudulent emails or messages designed to trick users into revealing sensitive information or clicking on malicious links.

**Real-life example:** In 2022, a phishing campaign targeting healthcare organizations successfully stole patient data from multiple hospitals.

### **Supply Chain Attacks**

Supply chain attacks target third-party vendors or suppliers to gain access to an organization's systems. This can be achieved through compromised software, compromised credentials, or physical access to supply chain facilities.

**Real-life example:** In 2021, the SolarWinds supply chain attack involved the compromise of a software update for SolarWinds Orion network monitoring software, allowing attackers to infiltrate numerous government and private sector organizations.

## **Physical Security Threats**

Physical security threats can include unauthorized access to facilities, data centers, or equipment. This can lead to data theft, equipment damage, or disruptions to services.

**Real-life example:** In 2021, a group of hackers broke into a data center in Sweden and stole servers containing sensitive data.

These are just a few examples of other common network and web attacks. It's important for organizations to be aware of these threats and implement appropriate security measures to protect their systems and data.

## **Password Spraying Attacks**

Password spraying involves attempting to log in to multiple accounts using a common password. This can be used to identify weak passwords or compromised credentials.

**Real-life example:** In 2021, a password spraying attack was used to compromise millions of LinkedIn accounts.

## **Privilege Escalation Attacks**

Privilege escalation attacks aim to gain higher-level privileges within a system or network. This can be achieved through exploiting vulnerabilities or exploiting misconfigurations.

**Real-life example:** In 2022, a privilege escalation vulnerability in the Microsoft Exchange Server software allowed attackers to gain unauthorized access to email accounts and other systems.

## **Clickjacking Attacks**

Clickjacking attacks involve tricking users into clicking on hidden links or buttons that perform unintended actions. This can be used to steal sensitive information or hijack user sessions.

**Real-life example:** In 2018, a clickjacking attack was used to redirect users to malicious websites.

## **Watering Hole Attacks**

Watering hole attacks target specific groups or organizations by compromising websites or applications they frequently visit.

**Real-life example:** In 2013, a watering hole attack targeted the websites of **Tibetan advocacy groups** to infect visitors with malware.

## Internet of Things (IoT) Attacks

IoT attacks target devices connected to the internet, such as smart home devices, industrial control systems, and medical devices. These attacks can be used to disrupt services, steal data, or launch other attacks.

**Real-life example:** In 2016, the Mirai botnet, which was composed of millions of compromised IoT devices, was used to launch a massive DDoS attack on Dyn, a major DNS provider.

These are just a few more examples of common network and web attacks. It's important for organizations to be aware of these threats and implement appropriate security measures to protect their systems and data.

## Network Discovery

Network discovery is the process of identifying and mapping devices, networks, and services within a given network environment. It is a crucial step in network security assessments, vulnerability scanning, and incident response. There are several techniques and tools available for network discovery, each with its own advantages and limitations.

### Passive Network Discovery

Passive network discovery involves monitoring network traffic without sending any probes or requests. This technique is less likely to trigger alarms or detection mechanisms, but it may not be able to discover stealthy devices or networks.

### Tools:

- **Wireshark:** A popular open-source packet analyzer that can capture and analyze network traffic.
- **Tcpdump:** A command-line packet analyzer for Unix-like systems.
- **Ntop:** A network traffic monitoring tool that provides real-time statistics and visualizations.

**Example:** By analyzing network traffic, it is possible to identify the IP addresses of active devices, the protocols they are using, and the services they are offering.

## Active Network Discovery

Active network discovery involves sending probes or requests to network devices to elicit responses. This technique can provide more comprehensive information but may trigger alarms or detection mechanisms.

### Tools:

- **Ping:** A network utility used to test connectivity to a device by sending ICMP echo requests.
- **Traceroute:** A network utility used to trace the path that packets take to reach a destination.
- **Nmap:** A powerful network scanning tool that can discover hosts, services, and vulnerabilities.
- **Nessus:** A vulnerability scanner that can also be used for network discovery.
- **OpenVAS:** A vulnerability scanner that includes network discovery capabilities.

**Example:** By sending ping requests to a range of IP addresses, it is possible to identify active devices on the network. Traceroute can be used to determine the path that packets take to reach a specific destination, revealing intermediate devices and network segments.

## Network Discovery Techniques Based on Protocols

- **ARP (Address Resolution Protocol) Spoofing:** This technique involves sending forged ARP replies to associate a malicious device with a legitimate IP address, allowing the attacker to intercept traffic.
- **DNS (Domain Name System) Spoofing:** This technique involves redirecting DNS queries to malicious servers, allowing the attacker to control which websites users access.
- **DHCP (Dynamic Host Configuration Protocol) Snooping:** This technique involves monitoring DHCP traffic to identify unauthorized DHCP servers or clients.
- **SNMP (Simple Network Management Protocol):** This protocol is used to manage network devices. By exploiting vulnerabilities in SNMP implementations, attackers can gain unauthorized access to devices.
- **ICMP (Internet Control Message Protocol):** is a network layer protocol used for sending error messages and control information between devices on an IP network. It can also be used for network discovery.
  - **ICMP Echo Request:**
    - A device sends an ICMP echo request to another device.
    - If the target device is reachable, it responds with an ICMP echo reply.
    - If the target device is unreachable, it sends an ICMP destination unreachable message.

### ICMP Timestamp Request:

- A device sends an ICMP timestamp request to another device.

- The target device responds with an ICMP timestamp reply, including the current timestamp.
- This can be used to determine the round-trip time (RTT) between the devices.

### **ICMP Address Mask Request:**

- A device sends an ICMP address mask request to another device.
- The target device responds with an ICMP address mask reply, indicating its subnet mask.

### **ICMP Router Advertisement:**

- Routers can send ICMP router advertisements to announce their presence and configuration information to other devices on the network.

### **ICMP Router Solicitation:**

- A device can send an ICMP router solicitation to request router advertisements.

**Example:** By sending ICMP echo requests to a range of IP addresses, it is possible to identify active devices on the network. Traceroute can be used to determine the path that packets take to reach a specific destination, revealing intermediate devices and network segments.

## **Specialized Network Discovery Techniques**

- **Wireless Network Discovery:** This involves identifying and analyzing wireless networks and devices. Tools such as Aircrack-ng and Kismet can be used for this purpose.
- **Darknet Discovery:** This involves identifying and analyzing networks that are not connected to the public internet. Tools such as Shodan and Censys can be used for this purpose.
- **Deep Packet Inspection (DPI):** This technique involves analyzing the contents of network packets to identify specific applications, protocols, and data types.

# **NIST framework phases of incident response**

## **Phase 1: Preparation**

### **1. Incident Response Plan (IRP):**

**Roles and Responsibilities:** Clearly define the roles and responsibilities of individuals involved in the incident response process, including incident responders, security analysts, system administrators, and management.

**Communication Protocols:** Establish communication channels and procedures for reporting, escalating, and coordinating incident response activities.

**Escalation Procedures:** Define guidelines for escalating incidents to appropriate levels of management based on severity and potential impact.

**Recovery Strategies:** Develop plans for restoring systems and data to their pre-incident state, including backup procedures, disaster recovery plans, and contingency planning.

### **2. Training and Awareness:**

**Regular Training:** Conduct regular training sessions to educate employees about security best practices, incident recognition, and reporting procedures.

**Awareness Campaigns:** Create awareness campaigns to promote a security-conscious culture within the organization.

**Phishing Simulations:** Conduct phishing simulations to test employees' ability to identify and report suspicious emails or messages.

### **3. Tools and Technologies:**

**SIEM Solutions:** Implement a SIEM solution to collect, analyze, and correlate security events from various sources.

**IDS/IPS:** Deploy intrusion detection and prevention systems to monitor network traffic for suspicious activity.

**Firewall:** Configure a firewall to control network traffic and protect against unauthorized access.

**Antivirus and Anti-Malware:** Use antivirus and anti-malware software to detect and remove malicious code.

**Data Loss Prevention (DLP):** Implement DLP solutions to prevent sensitive data from being exfiltrated.

#### **4. Partnerships:**

**Law Enforcement:** Establish relationships with local law enforcement agencies to coordinate incident response efforts and report criminal activities.

**Cybersecurity Experts:** Develop partnerships with external cybersecurity experts or consultants who can provide specialized assistance during incidents.

**Industry Associations:** Participate in industry associations or forums to share information and best practices with other organizations.

### **Phase 2: Detection and Analysis**

#### **1. Monitoring and Logging:**

**Real-time Monitoring:** Continuously monitor network traffic, system logs, and security events for anomalies or suspicious activity.

**Alerting:** Configure alerts to notify security personnel of critical events or potential incidents.

**Centralized Logging:** Centralize logs from various systems and devices for easier analysis and correlation.

#### **2. Threat Intelligence:**

**Threat Feeds:** Subscribe to threat intelligence feeds to stay informed about emerging threats and vulnerabilities.

**Intelligence Analysis:** Analyze threat intelligence data to identify potential risks and assess their impact on the organization.

#### **3. Incident Identification:**

**Baseline Analysis:** Establish a baseline of normal system behavior to detect deviations that may indicate an incident.

**Anomaly Detection:** Use anomaly detection techniques to identify unusual patterns or activities.

**Alert Triage:** Prioritize alerts based on severity and potential impact.

#### **4. Analysis:**

**Digital Forensics:** Conduct a forensic investigation to gather evidence and determine the root cause of the incident.



**Incident Timeline:** Create a timeline of events to understand the sequence of actions and identify the attacker's methods.

**Impact Assessment:** Assess the potential impact of the incident on the organization's operations, reputation, and financial standing

### **Phase 3: Containment, Eradication, and Recovery**

#### **1. Containment:**

- **Isolation:** Isolate affected systems or networks to prevent further spread of the incident.
- **Network Segmentation:** Implement network segmentation to limit the impact of the incident.
- **Disabling Services:** Disable unnecessary services or applications to reduce the attack surface.

#### **2. Eradication:**

- **Removal of Malware:** Remove any malicious code or malware from affected systems.
- **Patching Vulnerabilities:** Apply security patches and updates to address known vulnerabilities.
- **Configuration Changes:** Modify system configurations to prevent future attacks.

#### **3. Recovery:**

- **Data Restoration:** Restore data from backups or alternative sources.
- **System Restoration:** Restore affected systems to their pre-incident state.
- **Business Continuity:** Implement business continuity plans to minimize disruption and maintain operations.

### **Phase 4: Post-Incident Activity**

#### **1. Review and Evaluation:**

- **Incident Analysis:** Conduct a detailed analysis of the incident to identify root causes, weaknesses, and lessons learned.
- **Effectiveness Assessment:** Evaluate the effectiveness of the incident response process and identify areas for improvement.

#### **2. Updates and Improvements:**

- **IRP Revision:** Update the IRP to reflect the lessons learned from the incident.
- **Security Policies:** Review and update security policies and procedures to address identified vulnerabilities.

- **Training and Awareness:** Enhance training and awareness programs to improve employee preparedness.

### **3. Communication:**

- **Internal Communication:** Communicate the incident and its resolution to employees and stakeholders.
- **External Communication:** If necessary, communicate with customers, partners, or regulatory agencies about the incident.

### **4. Continuous Improvement:**

- **Security Posture Assessment:** Conduct regular security assessments to identify and address vulnerabilities.
- **Threat Intelligence Monitoring:** Stay informed about emerging threats and adjust security measures accordingly.
- **Incident Response Drills:** Conduct regular incident response drills to test preparedness and identify areas for improvement.

## **Phases of cyber kill chain attack**

### **1. Reconnaissance:**

- **Open-Source Intelligence:**
  - Searching social media for employee information or company announcements.
  - Analyzing company websites for vulnerabilities or outdated software.
  - Using search engines to find publicly available information about the target's systems and networks.
- **Technical Reconnaissance:**
  - Scanning networks for open ports or vulnerable services.
  - Using vulnerability scanners to identify weaknesses in systems and applications.
  - Analyzing DNS records to gather information about the target's infrastructure.

## 2. Weaponization

- **Creating Malware:**
  - Developing custom malware to exploit specific vulnerabilities.
  - Using existing malware tools and frameworks to create malicious code.
- **Selecting Delivery Methods:**
  - Phishing emails with malicious attachments or links.
  - Exploiting vulnerabilities in web applications or software.
  - Using social engineering techniques to trick victims into clicking on malicious content.

## 3. Delivery

- **Phishing Emails:**
  - Sending emails that appear to be from legitimate sources, often containing malicious attachments or links.
  - Using social engineering techniques to trick victims into clicking on malicious content.
- **Exploit Kits:**
  - Using exploit kits to automatically scan for vulnerabilities in websites and deliver malicious payloads to visitors.
- **Malicious Websites:**
  - Creating malicious websites that contain malicious code or redirect users to malicious content.

## 4. Exploitation

- **Exploiting Vulnerabilities:**
  - Using known vulnerabilities in software or operating systems to gain unauthorized access.
  - Exploiting misconfigurations or weak passwords.
- **Installing Malware:**
  - Installing malware on the compromised system to maintain persistent access and gather information.
  - Using rootkits or backdoors to hide malicious activity.

## 5. Installation

- **Establishing Foothold:**

- Creating system accounts or modifying existing accounts to gain unauthorized access.
- Installing persistence mechanisms to maintain access even if the initial entry point is compromised.

- **Installing Backdoors:**

- Installing backdoors or hidden tools to maintain access to the compromised system.
- Using remote administration tools to control the compromised system.

## 6. Command and Control

- **Establishing Communication:**

- Using command and control servers or infrastructure to communicate with the compromised system.
- Using encryption or tunneling techniques to hide communication.

- **Issuing Commands:**

- Issuing commands to the compromised system to gather information, steal data, or launch further attacks.
- Using remote administration tools to control the compromised system.

## 7. Actions on Objectives

- **Data Exfiltration:**

- Stealing sensitive data, such as customer information, intellectual property, or financial data.
- Using encryption or compression to obfuscate stolen data.

- **Lateral Movement:**

- Moving laterally within the network to compromise additional systems or gain access to sensitive data.
- Using compromised credentials or vulnerabilities to access other systems.

- **Disruption:**

- Disrupting operations by deleting data, modifying systems, or launching denial-of-service attacks.

## **Incident Response Documentation of Conti malware incident :**

### **Phase 1 - Preparation**

In the **Preparation Phase**, the goal is to ensure that all necessary tools, processes, and procedures are in place so that your organization is ready to handle potential incidents like the one involving the Conti ransomware. This phase is critical because it lays the foundation for effective incident response and minimizes the impact of attacks when they occur.

#### **1. Objectives of the Preparation Phase**

- **Establish and maintain an incident response policy** that outlines the roles and responsibilities of the incident response team (IRT).
- **Ensure infrastructure is secured** by employing the right tools for continuous monitoring, logging, and vulnerability assessment.
- **Train and educate staff** to recognize early warning signs of attacks (e.g., phishing emails) and to respond quickly to incidents.
- **Create and maintain a communication plan** for notifying key stakeholders during an incident.
- **Test the incident response plan** periodically through simulated attacks (e.g., penetration testing, red teaming).

#### **2. Tools and Platforms Used in Preparation**

For a strong defense and readiness for incidents like the Conti ransomware, your organization should be utilizing the following tools:

##### **2.1 Splunk: Security Information and Event Management (SIEM)**

Splunk provides comprehensive monitoring and logging capabilities, making it a key tool in detecting anomalies in your infrastructure.

- **Purpose:**
  - Centralized log management.
  - Real-time monitoring and analysis of logs from multiple sources (e.g., firewalls, servers, endpoints).
  - Alerting and reporting on suspicious activities or known indicators of compromise (IOCs).

- **Preparation Steps:**
  - **Log Collection and Aggregation:** Ensure that all critical infrastructure components, including the Exchange server, are sending logs to Splunk.
  - **Create Dashboards:** Develop custom Splunk dashboards to track real-time events such as failed login attempts, file modifications, process creations, and new user creations.
  - **Correlate Events:** Configure Splunk to correlate Sysmon logs, which will detect malicious behavior, like the creation of suspicious files (e.g., the ransomware dropper).
  - **Alerts:** Set up alerting for known IOCs related to ransomware (e.g., unusual file extensions, PowerShell commands, privilege escalation activities).
- **Sample Log Sources to Monitor in Splunk:**
  - **Sysmon Logs:** Detailed information on file creation, process creation, and network connections.
  - **Windows Event Logs:** To track authentication failures, user account changes, and administrative actions.
  - **Network Traffic Logs:** Monitoring of incoming/outgoing traffic, especially abnormal traffic patterns indicative of command-and-control (C2) connections.

## 2.2 Kali Linux: Offensive Security Platform

Kali Linux, a powerful penetration testing operating system, plays a crucial role in incident preparation and regular security assessments.

- **Purpose:**
  - Conduct penetration testing to identify vulnerabilities in critical infrastructure.
  - Perform network scans and exploit vulnerabilities to evaluate the security posture.
  - Simulate attack scenarios and train response teams.
- **Preparation Steps:**
  - **Penetration Testing:** Perform regular penetration tests on servers (including Exchange) and external-facing services using tools like **Nmap** for port scanning, **Metasploit** for exploit testing, and **Burp Suite** for web vulnerabilities.
  - **Training:** Conduct red team vs. blue team exercises where a simulated attack is launched from the Kali machine, and the incident response team reacts in real-time.
  - **IOCs Simulation:** Test defenses by simulating known Conti ransomware behaviors, such as PowerShell-based user creation or file modifications.
- **Tools to Use on Kali Linux:**
  - **Nmap:** Network scanning and port discovery.
  - **Metasploit:** Exploit known vulnerabilities and assess the ability of security controls to detect and block exploits.
  - **Wireshark:** Packet analysis for detecting abnormal network behavior.

## 2.3 Nessus Vulnerability Scanner

Nessus is one of the most commonly used tools for vulnerability scanning and remediation.

- **Purpose:**
  - Conduct vulnerability assessments to ensure all systems are patched and not susceptible to known exploits (e.g., CVE-2020-0796, CVE-2018-13374, and CVE-2018-13379).
  - Regularly scan for misconfigurations, outdated software, and potential security weaknesses.
- **Preparation Steps:**
  - **Regular Vulnerability Scanning:** Ensure that all systems, including the Exchange server, are regularly scanned using Nessus to detect vulnerabilities.
  - **Automated Reports:** Set up automated reports that highlight vulnerabilities needing immediate attention, especially in critical systems like Exchange.
  - **Patch Management:** Based on Nessus scan results, ensure there's a process in place to apply patches quickly to vulnerable systems.
- **Types of Vulnerabilities to Scan For:**
  - **Unpatched CVEs:** Critical vulnerabilities associated with the operating system, applications, and network services.
  - **Weak Configurations:** For example, weak password policies, disabled firewalls, or improperly configured permissions.
  - **Exposure to Exploits:** Especially vulnerabilities that ransomware like Conti would exploit (e.g., ProxyShell or ProxyLogon vulnerabilities in Exchange).

## 3. Key Preparation Strategies

### 3.1 Incident Response Team (IRT) Designation

- **Define Roles:** Each member of the incident response team should have clearly defined roles. For example:
  - **Incident Commander:** Oversees the response process and communicates with upper management.
  - **Forensics Specialist:** Investigates how the attacker gained access and collects evidence.
  - **Network Security Engineer:** Responsible for monitoring network traffic and isolating affected systems.
- **Key Personnel:** Ensure there is a designated point of contact for each critical component (e.g., email server, networking team, legal and compliance).

### 3.2 Documentation and Playbooks

- **Incident Response Playbooks:** Create and maintain detailed incident response playbooks for ransomware attacks, which should include:
  - Steps to take upon detection of ransomware, including system isolation, file triage, and communication protocols.
  - Methods to retrieve logs from Splunk and investigate suspicious events like file creation (Sysmon Event ID 11).
  - Actions to mitigate ransomware spread, including disconnecting infected hosts from the network and blocking malicious IP addresses.
- **Checklists:** Ensure the incident response plan includes checklists for:
  - Isolating affected systems.
  - Taking system snapshots for forensics.
  - Restoring affected systems from clean backups.

## 4. Logging and Monitoring

### 4.1 Key Log Types to Collect and Monitor

- **Authentication Logs:** Identify failed or suspicious login attempts, especially to critical servers like the Exchange system.
- **Process Creation Logs:** Monitor Sysmon Event ID 1 (Process Creation) and Event ID 11 (File Creation) for suspicious activities like the execution of cmd.exe or powershell.exe from unusual directories.
- **Network Logs:** Use Splunk to monitor inbound and outbound network traffic for unusual communication patterns, particularly for known malicious IP addresses or C2 servers.
- **Privilege Escalation Logs:** Watch for actions like the creation of new users or privilege escalation (e.g., net user /add commands).

## 5. Testing and Simulation

- **Conduct Simulated Ransomware Attacks:** Using Kali Linux, simulate common ransomware behaviors (e.g., encryption of files, creation of ransom notes, lateral movement) and measure the speed and effectiveness of detection and response.
- **Red Teaming Exercises:** Test how the organization responds to an actual attack scenario. Use Nessus to identify and exploit vulnerabilities, and see how quickly the blue team reacts.
- **Patch Testing:** Before applying patches from Nessus scans, test them in a controlled environment to ensure they don't cause downtime or other issues.



## 6. Communication Plan

- **Internal Communication:** Prepare a secure method of communication that can be used during an incident, especially if email services are compromised (e.g., Slack, Signal).
- **External Communication:** Have templates ready for informing customers and stakeholders of any incidents, ensuring compliance with regulations like GDPR.

## 7. Conclusion

A well-prepared organization is better equipped to handle incidents like Conti ransomware effectively. Using tools like Splunk for monitoring, Kali Linux for testing, and Nessus for vulnerability scanning ensures that defenses are in place and the incident response team is ready to react quickly.

## Detailed Documentation of the Detection and Analysis Phase of Incident Response

### Phase -2: Detection and Analysis

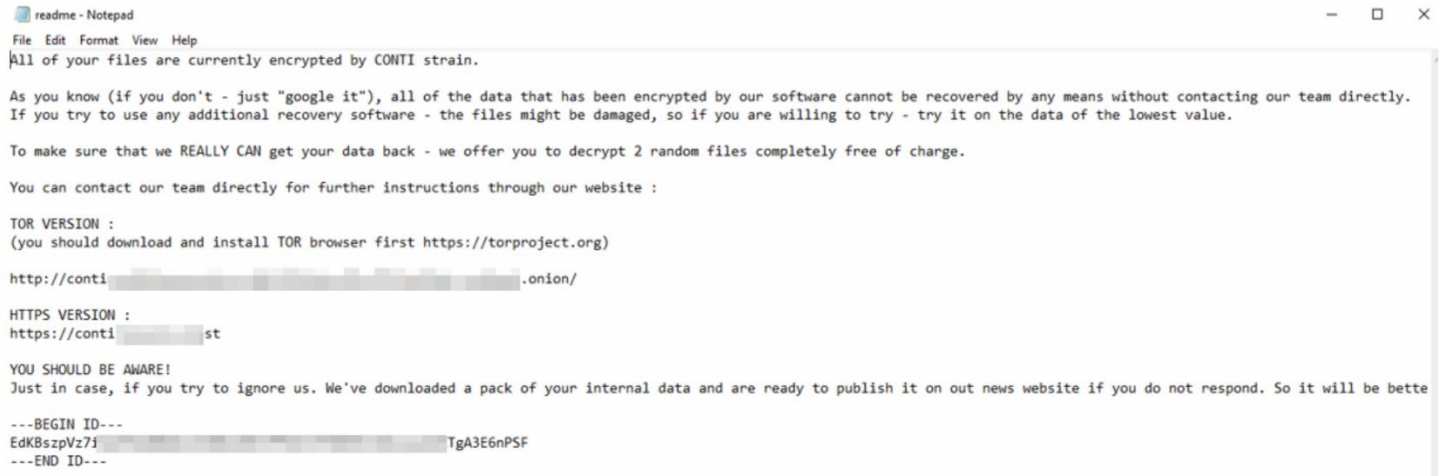
In this phase of incident response, the goal is to thoroughly detect and analyze malicious activities to understand the scope of the attack and determine appropriate actions for containment and eradication. In the case of the Conti ransomware attack on the Exchange Server as described in the write-up, detection primarily involved analyzing system logs using Splunk, a popular Security Information and Event Management (SIEM) tool.

This documentation will explore the Indicators of Compromise (IOCs), detail the attack phases using the Cyber Kill Chain, and provide a systematic analysis of the ransomware attack scenario where the Conti malware was delivered through a phishing attack.

# 1. Overview of the Incident

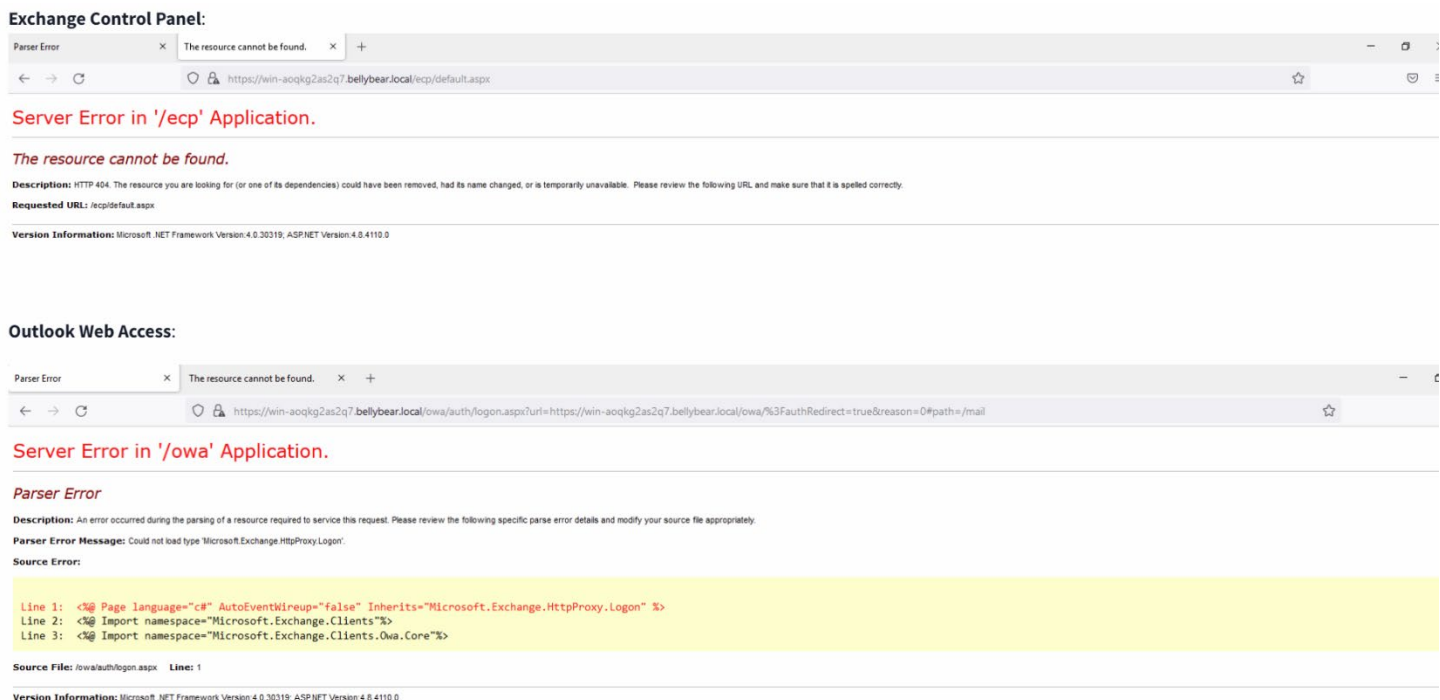
Some employees of the company reported being unable to log in to **Outlook**, and the Exchange admin also reported issues accessing the Exchange Admin Center. During initial triage, suspicious ransom notes were discovered on the Exchange server.

Below is a screenshot of the ransomware note.



There also Below are the error messages that the Exchange admin and employees see when they try to access anything related to Exchange or Outlook.

Below is a screenshot of the error



The **Splunk** platform was utilized to investigate this situation and identify the ransomware.

## 2. Indicators of Compromise (IOCs)

IOCs are forensic artifacts of an intrusion that can be used to detect or identify malicious activities within an organization's systems. Below are the IOCs related to the Conti ransomware attack found during the analysis:

File Path of Ransomware Executable:

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

This was identified as the location of the ransomware executable, a critical IOC for detecting where the malware was placed.

New Search									
Index= sourcetype=winEventlog:Microsoft-Windows-System/Operational * .exe									
debug CurrentDirectory CommandLine Image Hashes ParentCommandLine ParentImage _time									
5 events (before 10/19/24 10:05:35.000 AM) No Event Sampling									
Events Patterns Statistics (5) Visualization									
20 Per Page Format Preview									
CurrentDirectory	CommandLine	Image	Hashes	ParentCommandLine	ParentImage	Time			
C:\Windows\System32\	"C:\Program Files\Windows Defender\WinDefend.exe" SignatureUpdateService -ScheduleJob -HttpDownload -RestrictPrivileges -Revoke	C:\Program Files\Windows Defender\WinDefend.exe	MD5-280836881E89E833C0CA8D1A8395_5HA256-81F35A8001A2966305748CA9579E7F532844A8B02C68F85124D939F6899_1PFWASHFFAE1E26343119C480178379C863F	"C:\Program Files\Windows Defender\WinDefend.exe" SignatureUpdateService -ScheduleJob -HttpDownload -RestrictPrivileges	C:\Program Files\Windows Defender\WinDefend.exe	2021-09-08 13:08			
C:\Users\Administrator\Documents\	cmd.exe	C:\Users\Administrator\Documents\cmd.exe	MD5-290C7DFB01E50CEA9E19DA81A781AF2C_5HA256-53B1C182F41A77C38E57083E57539453F7A8F87F4896B1F9CA22_1PFWASHFFAE1E26343119C480178379C863F	C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe	2021-09-08 13:05			

## MD5 Hash of the Ransomware: 290C7DFB01E50CEA9E19DA81A781AF2C

The MD5 hash of the **cmd.exe** executable is another IOC that helps identify this specific instance of the Conti ransomware.

from virus total search of file hash we see that the file is malicious and the ransomware called **conti ransomware**.

64  
172  
Community Score

64/72 security vendors flagged this file as malicious

53b1c1b2f41a7fc300e97d036e57539453f7a8f87f4896b1f9ca22  
53b1c1b2f41a7fc300e97d036e57539453f7a8f87f4896b1f9ca22.bin

Size 190.0 KB  
Last Analysis Date 16 days ago

perex runtime-modules detect-debug-environment direct-cpu-clock-access long-sleeps calls-wmi cve-2014-3331 exploit

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY (27)

Crowdsourced YARA rules

Matches rule Windows\_Ransomware\_Conti\_89f3b6fa from ruleset Windows\_Ransomware\_Conti at https://github.com/elastic/protectio... by Elastic Security

Matches rule Windows\_Ransomware\_Conti\_89f3b6fa from ruleset Windows\_Ransomware\_Conti at https://github.com/elastic/protectio... by Elastic Security

Matches rule win\_conti\_auto from ruleset win\_conti\_auto at https://malpedia.caad.fkie.fraunhofer.de/ by Felix Blistein - yara-signatur at cocacoding dot com

Matches rule Conti from ruleset Conti at https://github.com/kevoreilly/CAPEv2 by kevoreilly

Matches rule Conti from ruleset Conti at https://github.com/kevoreilly/CAPEv2 by kevoreilly

Crowdsourced Sigma Rules

CRITICAL 0 HIGH 1 MEDIUM 0 LOW 0

Matches rule Uncommon File Created in Office Startup Folder by frack113, Nasreddine Bencherchali (Nexttron Systems) at Sigma Integrated Rule Set (GitHub)

Crowdsourced IDS rules

HIGH 0 MEDIUM 3 LOW 3 INFO 0

Matches rule PROTOCOL DNS SPOOF every response with TTL of 1 min. and no authority at Snort registered user ruleset

## File created by cmd.exe ransomware in multiple path:

**Event ID 11** is associated with file creation activities. This Sysmon Event ID is crucial for detecting when and where the ransomware executable was created.

## File called readme.txt Saved to Multiple Locations:

This ransom note was distributed across various folders, another clear **indicator of compromise**.

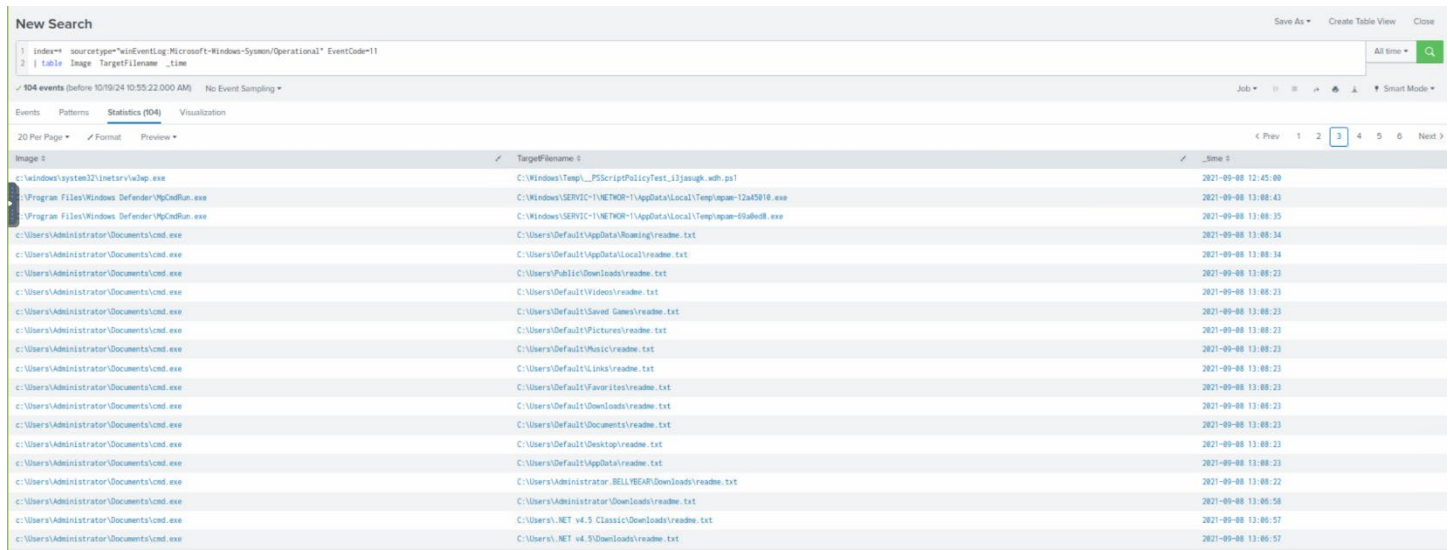
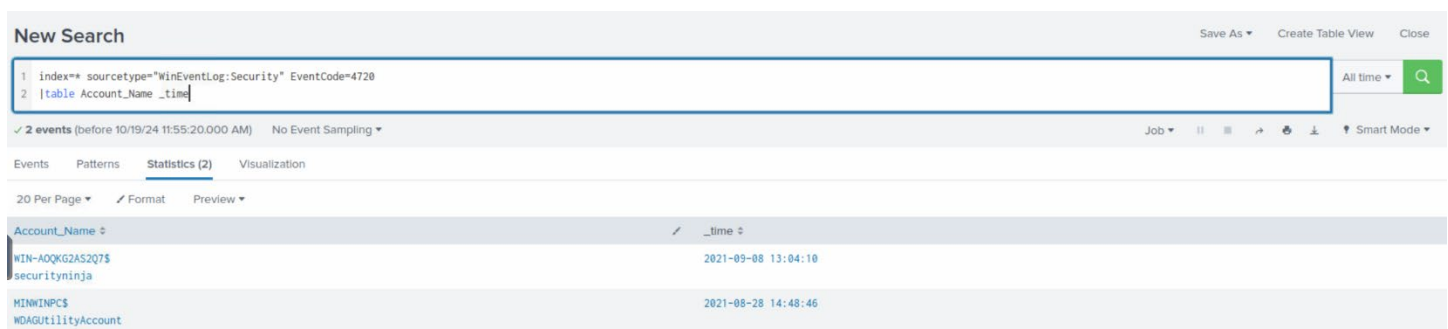


Image	TargetFilename	_time
C:\Windows\system32\inetres\iexp.exe	C:\Windows\Temp\PScriptPolicyTest_12jaugk.wdh.ps1	2021-09-08 12:45:00
C:\Program Files\Windows Defender\mpcmdrun.exe	C:\Windows\SYSTEM32\NETSH\Local\Temp\open-12a5018.exe	2021-09-08 13:08:43
C:\Program Files\Windows Defender\mpcmdrun.exe	C:\Windows\SYSTEM32\NETSH\Local\Temp\open-60abed.exe	2021-09-08 13:08:35
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\AppData\Roaming\readme.txt	2021-09-08 13:08:34
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\AppData\Local\readme.txt	2021-09-08 13:08:34
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Public\Downloads\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Videos\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Saved Games\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Pictures\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Music\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Links\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Favorites\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Downloads\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Documents\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\Desktop\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Default\AppData\readme.txt	2021-09-08 13:08:23
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Administrator\BELLBEDI\Downloads\readme.txt	2021-09-08 13:08:22
C:\Users\Administrator\Documents\cmd.exe	C:\Users\Administrator\Downloads\readme.txt	2021-09-08 13:06:58
C:\Users\Administrator\Documents\cmd.exe	C:\Users\NET v4.5 Classic\Downloads\readme.txt	2021-09-08 13:06:57
C:\Users\Administrator\Documents\cmd.exe	C:\Users\NET v4.5\Downloads\readme.txt	2021-09-08 13:06:57

## A user is created called securityninja:

We will use the following query to find any malicious user created with **eventcode=4720** user creation event in sysmon



Account_Name	_time
WIN-AQKG2AS2Q7\$ securityninja	2021-09-08 13:04:10
MINKNPC\$ WDAGUtilityAccount	2021-08-28 14:48:46

Only two events is shown, One of them is service account called **WDAGUtilityAccount** we will skip that, but the other event we will see the account name created called **secuirtyninja** We want to extract more information and know what the command created

that account so we will use Sysmon because sysmon logs all commands



Web Shell Deployed:

i3gfPctK1c2x.aspx

A malicious web shell was deployed via the compromised Exchange Server, an additional IOC that signals post-exploitation activities.

1 index=\* sourcetype=iis cs\_method=POST

2 | dedup cs\_uri\_stem

3 | table cs\_uri\_stem c\_port s\_ip s\_port \_time

All time

15 events (before 10/19/24 12:27:59.000 PM) No Event Sampling

Job Visualization

Events Patterns Statistics (15) Visualization

20 Per Page Format Preview

cs_uri_stem	c_port	s_ip	s_port	_time
/ecp/DOI/DOIService.svc/GetList		fe80::50c7:e3a5:fed7:dc19%5	443	2021-09-08 13:07:45
/api/emsdb/		fe80::50c7:e3a5:fed7:dc19%5	443	2021-09-08 13:07:25
/powershell		fe80::50c7:e3a5:fed7:dc19%5	80	2021-09-08 13:07:06
/OWA/auth.owa		127.0.0.1	443	2021-09-08 13:05:06
/Microsoft-Server-ActiveSync/default.eas		:::1	443	2021-09-08 13:05:00
/owa/ev.owa2		fe80::50c7:e3a5:fed7:dc19%5	443	2021-09-08 13:04:08
/autodiscover/autodiscover.json		10.10.10.6	443	2021-09-08 12:52:11
/owa/auth/i3gfPctK1c2x.aspx		10.10.10.6	443	2021-09-08 12:51:50
/owa/service.svc		fe80::50c7:e3a5:fed7:dc19%5	443	2021-09-08 12:51:32
/owa/pl11.ashx		fe80::50c7:e3a5:fed7:dc19%5	443	2021-09-08 12:47:55
/owa/sessiondata.ashx		fe80::50c7:e3a5:fed7:dc19%5	443	2021-09-08 12:47:54
/owa/auth.owa		fe80::50c7:e3a5:fed7:dc19%5	443	2021-09-08 12:47:48

File permission changed on Web Shell:

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

This command highlights how the attacker executed the web shell,  
The command removes read only from the file allowing attacker to do further steps in the attack.

New Search

Save As Create Table View Close

1 index=\* sourcetype="WinEventLog:Microsoft-Windows-Sysmon/Operational" \*.aspx

2 | table CurrentDirectory CommandLine Image Hashes ParentCommandLine ParentImage EventCode \_time

All time

1 event (before 10/19/24 12:11:16.000 PM) No Event Sampling

Job Visualization

Events Patterns Statistics (1) Visualization

20 Per Page Format Preview

Image	Hashes	ParentCommandLine	ParentImage	EventCode	_time
C:\Windows \System32 \attrib.exe	MD5=3A536CC896D9C6CA2C2EE4C21CCA1DFA,SHA256=B101350BCEE773B7E777596138B3C28FBF1D79A13C2C8783575A9D893D52E6,IMPHASH=2CB38FE7D8F223D9DA50B7CBA9B95A6D	C:\Windows \system32\cmd.exe	C:\Windows \System32 \cmd.exe	1	2021-09-08 12:52:09

## **Exploited CVEs:**

After search the web of Conti ransomware we reached out that the ransomware use these three exploits in the system

CVE-2020-0796 (SMBGhost) , CVE-2018-13374 ,CVE-2018-13379

These vulnerabilities were exploited in the attack, further indicators of how the attacker gained unauthorized access to the network.

## **3. Attack Analysis mapping Using the Cyber Kill Chain**

The Cyber Kill Chain is a framework for understanding the stages of a cyber attack, from initial reconnaissance to full compromise. Here's a breakdown of the attack phases in this scenario, assuming the Conti ransomware was delivered via phishing, and the Exchange Server was exposed to the internet.

### **Phase 1: Reconnaissance**

The attacker likely started with reconnaissance by scanning the target organization's public-facing Exchange Server, which was published on the internet without any security restrictions. The attacker may have discovered known vulnerabilities in the server and identified it as a viable target for exploitation.

### **Phase 2: Weaponization**

In this phase, the attacker crafted a phishing email containing a malicious attachment or link designed to exploit a vulnerability in the Exchange server. The attacker weaponized the Conti ransomware and possibly other malware tools for initial access.

### **Phase 3: Delivery**

The attack was delivered through phishing, where a malicious email was sent to employees. When the recipient opened the attachment or clicked the link, it exploited the Exchange Server via one of the known CVEs, such as CVE-2020-0796 (SMBGhost) or CVE-2018-13379, allowing the malware to be installed.

## **Phase 4: Exploitation**

After successful delivery, the ransomware exploited the vulnerabilities on the Exchange Server. CVE-2020-0796, a critical vulnerability in Microsoft's SMB protocol, was likely leveraged to spread across the internal network, while CVE-2018-13374 and CVE-2018-13379 provided additional avenues for gaining deeper access into the infrastructure.

## **Phase 5: Installation**

The attacker used the cmd.exe file to execute malicious commands, including placing a ransomware executable on the Exchange Server (c:\Users\Administrator\Documents\cmd.exe). The web shell (i3gfPctK1c2x.aspx) was also installed on the server to maintain remote access to the compromised system.

## **Phase 6: Command and Control (C2)**

The attacker established command and control by adding a new user (securityninja) to the compromised system using the command net user /add securityninja hardToHack123\$. This gave the attacker the ability to maintain persistent access and control over the Exchange server.

## **Phase 7: Actions on Objectives**

In the final phase, the attacker performed various malicious activities, including:

Migrating processes to PowerShell and unsecapp.exe for persistence.

Dumping system hashes using lsass.exe for credential theft.

Executing the ransomware payload, encrypting files, and dropping ransom notes (readme.txt).

Utilizing the web shell to further exploit the compromised Exchange server.

## **4. Conclusion and Recommendations**

Based on the detection and analysis phase, it is evident that the attack utilized multiple known vulnerabilities and post-exploitation techniques to infiltrate the network, deploy ransomware, and maintain persistence. The lack of security restrictions on the publicly exposed Exchange server was a critical factor that facilitated the attack.



## Key Recommendations:

**Patch Vulnerabilities:** Immediately apply patches to address CVE-2020-0796, CVE-2018-13374, and CVE-2018-13379 across all affected systems.

**Implement Email Filtering and Anti-Phishing Measures:** Strengthen defenses against phishing emails to prevent malware delivery via social engineering attacks.

**Network Segmentation:** Ensure that critical services like Exchange are not exposed directly to the internet without appropriate protections such as firewalls, VPNs, and multi-factor authentication (MFA).

**Monitor for IOCs:** Use Splunk or similar SIEM tools to continuously monitor for known IOCs, including suspicious process activity, command-line executions, and MD5 hash signatures.

**Incident Response Planning:** Ensure that an effective incident response plan is in place to quickly detect, analyze, and respond to ransomware attacks

## Phase -3 Containment

The **containment phase** is a critical part of the **incident response lifecycle**. It occurs after the detection and analysis phase and is essential for preventing the attacker from causing further damage, spreading the attack, or stealing more sensitive information. The primary goal of this phase is to limit the impact of the security incident, maintain the availability of services, and ensure the threat is contained before moving to eradication and recovery.

In this documentation, we'll provide a step-by-step process for containing the Conti ransomware incident described previously. Since the malware was delivered via phishing and the compromised Exchange Server was exposed to the internet without restrictions, containment requires both immediate and long-term actions to halt further damage, protect critical assets, and ensure minimal disruption.

### 1. Overview of the Containment Phase

The **containment phase** involves a mix of short-term actions to immediately stop the spread of the ransomware, and long-term strategies that prevent the attacker from re-establishing control over the compromised systems. Key objectives during this phase include:

- **Isolating affected systems** from the rest of the network to prevent lateral movement.
- **Preserving evidence** for further investigation while limiting further damage.
- **Blocking attacker communication channels** such as command and control (C2) servers.
- **Maintaining business continuity** as much as possible by keeping critical services operational.

## 2. Types of Containment Strategies

There are generally two types of containment strategies in incident response:

- **Short-term (immediate) containment:** Quick actions aimed at stopping the spread of the attack in the short term.
- **Long-term containment:** Actions that involve more thorough steps to ensure systems are fully protected from further compromise, often implemented before full system recovery or reinstallation.

In this scenario involving the Conti ransomware, both short-term and long-term containment measures are necessary.

## 3. Short-Term Containment Actions

Short-term containment focuses on **quickly isolating affected systems** and stopping any active processes that are contributing to the attack or ransomware encryption.

### Step 1: Isolate Infected Systems

#### 1. Disconnect the Exchange Server from the network:

- Immediately isolate the compromised Exchange Server by disconnecting it from the network or placing it in a quarantine VLAN. This prevents further lateral movement of the ransomware and stops external communication with command-and-control (C2) servers.

Rationale: In the case of ransomware like Conti, stopping network connectivity is essential to prevent the encryption process from spreading to other critical systems. Isolation will also stop the ransomware from sending any stolen data to the attacker's C2 infrastructure.

#### 2. Isolate affected workstations:

- Identify any endpoints or workstations that show signs of infection, particularly those where phishing emails were opened. These systems should also be disconnected from the network.

### Step 2: Block Malicious IPs and Domains

#### 1. Use firewall rules to block communication to known malicious IP addresses and domains related to the attack:

- Based on threat intelligence and IOCs identified during the detection phase, configure firewalls, proxies, and intrusion prevention systems (IPS) to block connections to the attacker's C2 infrastructure.

Rationale: Conti ransomware often communicates with external C2 servers for encryption keys and data exfiltration. Blocking these communications can prevent the attacker from proceeding further with the attack.

**2. Disable outbound traffic from infected systems:**

- In addition to blocking known malicious addresses, ensure that all outbound connections from compromised systems are blocked, especially from the Exchange Server.

**Step 3: Stop the Ransomware Process**

**1. Kill the ransomware process on infected machines:**

- Use administrative tools (e.g., task manager, PowerShell, or third-party endpoint detection and response (EDR) tools) to terminate malicious processes like cmd.exe or powershell.exe that are running the ransomware.

**2. Disable unauthorized accounts created by the attacker:**

- As identified in the detection phase, the attacker created a user securityninja. Immediately disable this account, remove its privileges, and audit any other unauthorized accounts.

**Step 4: Apply Temporary Security Controls**

**1. Disable unnecessary services on the Exchange Server:**

- Temporarily disable vulnerable services such as SMB (Server Message Block) and other services that could be exploited until further patching and configuration are completed.

**2. Implement network segmentation:**

- If possible, segment critical systems from other parts of the network. Ensure that only essential communication flows between systems are allowed to limit the spread of the infection.

**Step 5: Preserve Evidence**

**1. Capture forensic images:**

- Take snapshots or forensic images of compromised systems for later analysis. This will ensure that evidence is preserved before any cleanup or eradication takes place. Forensic images can be critical in identifying how the attacker gained access, what systems were affected, and what data may have been exfiltrated.

**2. Document all containment actions:**

- Keep a detailed log of all containment actions taken. This documentation is vital for post-incident analysis and may be necessary if the organization needs to comply with legal requirements or insurance claims related to the incident.

## 4. Long-Term Containment Actions

Long-term containment focuses on ensuring that attackers cannot regain access to the environment and that vulnerabilities are addressed before full restoration of services.

### Step 1: Patch Vulnerabilities

1. **Patch all affected systems** to prevent re-exploitation of vulnerabilities:
  - Immediately apply patches for known vulnerabilities, particularly those exploited by Conti, such as **CVE-2020-0796** (SMBGhost) and **CVE-2018-13379** (Fortinet VPN). Ensure the Exchange Server is updated with the latest security patches.

Rationale: The initial exploitation vector was likely due to unpatched vulnerabilities in the exposed Exchange Server. Patching these vulnerabilities is critical to prevent re-entry by the attacker.

### Step 2: Disable Unnecessary Internet Exposure

1. **Restrict public access to critical services:**
  - Ensure that the Exchange Server is no longer directly exposed to the internet without proper protection. Implementing a firewall or VPN for external access is recommended to prevent unauthorized connections from outside the network.
2. **Review access controls:**
  - Review and update access control lists (ACLs) to ensure that only authorized personnel can access critical services. Enforce least privilege principles, requiring multi-factor authentication (MFA) for all administrative access.

### Step 3: Remove Persistence Mechanisms

1. **Remove the web shell (i3gfPctK1c2x.aspx):**
  - Identify and remove the malicious web shell installed on the Exchange Server, along with any other scripts or backdoors that could allow the attacker to regain access to the system.
2. **Monitor for persistence mechanisms:**
  - Using Splunk or EDR tools, continue monitoring for any persistence mechanisms, such as rogue user accounts, scheduled tasks, or registry changes, that could allow the attacker to re-enter the system.

### Step 4: Conduct Full System Scans

1. **Run full anti-malware scans:**
  - Perform thorough scans of all systems using up-to-date anti-virus and endpoint detection tools to identify and remove any remaining malware or ransomware files.
2. **Harden the environment:**

- Apply security best practices such as disabling unused ports, restricting administrative access, and improving logging and monitoring. Ensure that logging is centralized and monitored in real-time for quicker detection of future incidents.

## Step 5: Strengthen User Awareness

### 1. **Conduct security awareness training:**

- Since phishing was the initial delivery method of the ransomware, it is critical to conduct phishing awareness training across the organization. Educate users on recognizing malicious emails, safe email practices, and reporting suspicious activity.

### 2. **Implement stronger email filtering:**

- Enhance email security with stricter filtering policies to block malicious attachments and links. Deploy technologies like DMARC, SPF, and DKIM to mitigate phishing risks.

## Step 6: Audit User Accounts and Passwords

### 1. **Force password changes for all accounts:**

- As the attacker likely dumped system hashes and created unauthorized accounts, enforce password resets for all users, especially those with administrative access.

### 2. **Implement strong password policies:**

- Use complex password requirements and encourage the use of password managers. Enable MFA for all users to minimize the impact of future phishing or credential theft attacks.

## 5. Conclusion

The containment phase plays a pivotal role in ensuring that the attacker is stopped from causing further damage, the ransomware is prevented from spreading, and business operations are maintained as much as possible. By combining immediate actions like isolating systems and blocking C2 communication with longer-term strategies such as patching, removing persistence mechanisms, and strengthening security controls, organizations can effectively contain ransomware attacks like Conti.

After containment is achieved, the next steps involve moving to the **eradication and recovery phases**, where systems are cleaned, vulnerabilities are addressed, and business continuity is fully restored.

## Key Recommendations for Future Prevention:

- Implement network segmentation to limit ransomware spread.
- Patch critical vulnerabilities regularly and in a timely manner.
- Secure public-facing services like Exchange with firewalls, VPNs, and MFA.
- Conduct regular security awareness training focused on phishing prevention.
- Monitor for and respond to IOCs in real-time with SIEM and EDR solutions.

## Phase-4 Eradication

The **eradication phase** of incident response is where the root cause of the security incident is identified and removed from the environment. The primary goal of this phase is to ensure that the malicious elements of the attack—whether malware, backdoors, compromised user accounts, or misconfigurations—are fully eradicated so that attackers cannot re-establish control or continue their activities.

Based on the TryHackMe Conti ransomware lab write-up you provided, this documentation outlines the eradication phase, focusing on actions taken to eliminate the Conti ransomware and associated attacker footholds in the network. We'll assume that the ransomware was delivered through phishing and that the Exchange Server was exposed on the internet without sufficient restrictions. Any missing inputs or assumed information will be incorporated as needed.

### 1. Overview of the Eradication Phase

The eradication phase involves a thorough cleaning of compromised systems, ensuring that all traces of the attacker's presence are eliminated. This includes:

- **Removing malicious files and artifacts** such as ransomware binaries, web shells, and other malware components.
- **Eliminating persistence mechanisms** like rogue user accounts, scheduled tasks, or registry keys.
- **Patching vulnerabilities** and misconfigurations that allowed the initial attack vector.
- **Verifying that all attacker footholds** are fully removed before restoring systems.

## 2. Steps to Eradicate Conti Ransomware from the Environment

### Step 1: Remove the Ransomware Files

#### 1.1 Identifying Conti Ransomware Artifacts

- **Search for the ransomware binary (cmd.exe)** that was identified during the detection and analysis phase, which was found in a non-standard location: C:\Users\Administrator\Documents\cmd.exe.
- **Locate and remove any related files**, such as the ransomware note (readme.txt), that was saved across multiple folder locations.
  - Action: Use antivirus and endpoint detection and response (EDR) tools to **scan the entire system** for ransomware binaries, including other possible infected files that could have been renamed or moved to different directories.
  - Assumption: The malware may have dropped additional payloads in different locations on the system (e.g., temp folders, system directories).

#### 1.2 MD5 Hash Verification

- As per the TryHackMe write-up, the MD5 hash of the ransomware was identified as 290C7DFB01E50CEA9E19DA81A781AF2C.
  - **Use this hash** to search for any additional copies of the ransomware across the network by conducting a thorough file hash scan.

#### 1.3 Removing the Web Shell

- The attacker deployed a web shell (i3gfPctK1c2x.aspx) on the Exchange Server, as noted during the detection phase. This web shell must be removed.
  - Action: Perform a **full scan of all web directories** on the Exchange Server (e.g., the OWA folder where the shell was found: C\$\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\i3gfPctK1c2x.aspx) and ensure that all unauthorized files are removed.
  - **Search for other web shells** or backdoors that may have been deployed by the attacker to maintain access to the system.

### Step 2: Eliminate Persistence Mechanisms

#### 2.1 Disable Unauthorized User Accounts

- The attacker created a new user account (securityninja) as part of the compromise, which must be removed.
  - Action: **Identify and disable all unauthorized user accounts**, especially those created by the attacker. Cross-reference this against existing user lists to ensure no additional rogue accounts were added.

- **Review administrative privileges** on all compromised systems and revert any changes that granted elevated privileges to unauthorized users.

## 2.2 Remove Scheduled Tasks

- Attackers frequently use **scheduled tasks** to persist on the system even after the malware is removed.
  - Action: Use forensic tools or PowerShell commands to **list all scheduled tasks** on the compromised system. Look for any suspicious tasks set to run malicious commands or processes, especially ones related to the cmd.exe or powershell.exe binaries the attacker used.
  - **Delete any suspicious scheduled tasks** that are tied to the attack.

## 2.3 Review Registry Keys for Persistence

- In some cases, attackers modify the **Windows registry** to establish persistence.
  - Action: Perform a **registry scan** for persistence mechanisms, especially under keys such as HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run.
  - Remove any entries that launch malware or unauthorized applications on system startup.

## Step 3: Patch Vulnerabilities

### 3.1 Patch the Exchange Server

- The Exchange Server was exposed on the internet without restrictions, and the attacker exploited known vulnerabilities. Based on external research, we know that the Conti ransomware exploited vulnerabilities such as **CVE-2020-0796** (SMBGhost) and **CVE-2018-13379** (Fortinet VPN).
  - Action: Ensure that the **Exchange Server is fully patched** with the latest security updates, including all critical and security patches from Microsoft.
  - **Disable or restrict public access** to the Exchange Server unless absolutely necessary. Implement stronger access control measures, such as VPN-based access and multi-factor authentication (MFA).

### 3.2 Patch Other Affected Systems

- **Apply patches** to all affected endpoints and servers across the organization, focusing on known vulnerabilities exploited by Conti ransomware.
  - Assumption: Other systems in the network could be affected by vulnerabilities that the ransomware might exploit (e.g., outdated software or OS versions).
  - **Use vulnerability scanners** to identify unpatched systems and apply security fixes as needed.



## Step 4: Ensure the Integrity of System Files

### 4.1 Run System Integrity Checks

- After removing the ransomware, it is important to verify that the system's core files have not been tampered with.
  - Action: Use tools like **System File Checker (SFC)** or **Windows File Integrity** to perform checks on critical system files and replace any corrupted or compromised files.
  - **Verify the integrity of the Exchange Server** to ensure no modifications have been made to system files that would allow the attacker to re-enter the environment.

### 4.2 Reinstall Critical Services (if needed)

- If the compromise is extensive or critical system files have been severely impacted, it may be necessary to **reinstall the Exchange Server** and other critical services from known good backups.
  - Action: Perform a **clean reinstallation** of the Exchange Server software if system integrity cannot be guaranteed.

## Step 5: Remove Malicious Processes

### 5.1 Identify Malicious Processes

- As detected during the analysis phase, the attacker used the powershell.exe and wbem\unsecapp.exe processes to maintain persistence and migrate processes for lateral movement.
  - Action: Review process logs and **identify any lingering malicious processes** that were used during the attack. Use tools such as **Process Explorer** or **Sysinternals** to kill any suspicious processes.
  - **Monitor system memory and running processes** for signs of malicious activity, particularly those related to the migration to lsass.exe and the dumping of system hashes.

### 5.2 Remove Any Malicious Services

- **Check for malicious services** that may have been installed by the attacker to maintain persistence, such as unauthorized services that execute commands or malware on startup.
  - Action: List all services running on the compromised systems and remove or disable any services that are not recognized or necessary for system operation.

## Step 6: Verify No Further Compromise

### 6.1 Conduct Full-Scale Scans

- After the initial eradication efforts, **run a full-scale anti-malware scan** across all systems to ensure no traces of the ransomware or attacker footholds remain.
  - Action: Use enterprise-level antivirus and endpoint protection solutions (such as **EDR** or **XDR**) to thoroughly scan for any remaining malicious files, processes, or artifacts across the environment.

### 6.2 Monitor for Indicators of Compromise (IOCs)

- Continue to **monitor the network and systems for IOCs** related to the Conti ransomware, such as:
  - MD5 hash 290C7DFB01E50CEA9E19DA81A781AF2C (associated with the ransomware binary).
  - The cmd.exe and powershell.exe processes used by the attacker.
  - Any traffic attempting to connect to known Conti command-and-control (C2) servers.
  - Suspicious account creation or privilege escalations, especially involving user accounts like securityninja.

## Step 7: Harden the Environment

### 7.1 Enhance Network Security

- **Apply network segmentation** to restrict lateral movement within the environment. Critical systems like the Exchange Server should be isolated from other parts of the network, and only essential traffic should be allowed.
- **Enable logging and monitoring** for all critical systems, including those exposed to the internet. Ensure that security tools like **SIEM** (Security Information and Event Management) are monitoring logs for suspicious activity in real-time.

### 7.2 Strengthen Endpoint Protection

- **Deploy endpoint protection and response solutions (EDR)** across all workstations and servers to monitor for any signs of compromise in real-time. Configure these tools to alert security teams of suspicious behavior, such as ransomware-like file encryption, unauthorized process execution, or data exfiltration.

### 7.3 Enforce Strong Authentication and Access Control

- **Implement multi-factor authentication (MFA)** on all critical systems, particularly for administrative accounts.

- **Review and enforce least privilege access** to ensure that users only have the permissions necessary to perform their jobs. This limits the damage that could occur if a user account is compromised.

## Conclusion

The eradication phase ensures that all malicious artifacts related to the Conti ransomware attack are thoroughly removed, vulnerabilities are patched, and persistence mechanisms are eliminated. The primary focus is on ensuring that the attacker cannot regain access or continue their activities, paving the way for safe system recovery.

Once the eradication phase is complete, the incident response team can proceed to the **recovery phase**, where systems are fully restored, services are brought back online, and the organization moves towards full operational capacity.

## Detailed Documentation of the Recovery Phase in Incident Response

The **recovery phase** of incident response is the process of restoring affected systems and operations to normal while ensuring that the environment is secure from future attacks. It involves carefully bringing systems back online, verifying that they are free of any malicious software or configurations, and implementing changes to prevent recurrence.

Based on the TryHackMe Conti ransomware scenario you provided, the ransomware was delivered via phishing, and an Exchange Server was exposed to the internet without sufficient protection. We will assume that the Exchange Server is critical for the organization's email services, and the business continuity relies on its full restoration. This documentation outlines the steps to recover from the Conti ransomware attack, incorporating lessons learned and industry best practices.

### 1. Phase-4 Recovery

The recovery phase focuses on ensuring that:

- **All systems are restored** to their pre-attack state.
- **Operational continuity** is reestablished while keeping business disruptions to a minimum.
- **Confidence in the environment** is regained by ensuring no further compromise is present.
- **Improved security controls** are implemented to prevent future incidents.

## 2. Key Recovery Objectives

- **Restore services** (e.g., email and other critical systems) while ensuring that all systems are clean of ransomware.
- **Monitor systems** closely for signs of any recurring malicious activity.
- **Implement preventative measures**, such as patching vulnerabilities and hardening systems, to avoid a repeat incident.
- **Communicate with stakeholders** to provide updates on system status, recovery progress, and long-term mitigation efforts.

## 3. Steps to Recover from the Conti Ransomware Attack

### Step 1: System Restoration

#### 1.1 Restore from Known Good Backups

- **Identify backups** of critical systems, including the Exchange Server, that were taken before the ransomware infection occurred.
  - Assumption: Backups were regularly made and stored offline or in a secure, isolated environment that was not affected by the ransomware.
  - Action: Verify that these backups are clean by scanning them with updated antivirus and endpoint detection and response (EDR) tools before proceeding with restoration.
  - Best Practice: Ensure that backups are encrypted and stored in multiple locations to prevent their corruption by ransomware.

#### 1.2 Rebuild Compromised Systems

- For severely compromised systems (such as the Exchange Server), it may be safer to **rebuild the systems from scratch** rather than risk leaving remnants of malware.
  - **Perform a clean reinstallation** of operating systems and services on compromised machines.
  - **Reconfigure the Exchange Server** by reinstalling and reapplying service packs and updates, rather than restoring from an infected state.
  - Action: Use known-good installation media to rebuild the system and ensure all configuration files are set to their correct, secure state.

#### 1.3 Restore User Data and Services

- Once systems are rebuilt and deemed clean, restore user data from **pre-infection backups**.
  - Action: Gradually bring user services (e.g., email) back online in stages, verifying functionality and security after each step.
  - Assumption: Email services such as Outlook were affected by the Exchange Server compromise. These should be restored by **migrating data from backup systems** or **recovering email data** from clients who may have cached messages.

## 1.4 Validate the Restoration Process

- After the restoration is complete, **verify the integrity** of all restored data and services.
  - Action: Test the restored system functionality thoroughly, checking the Exchange Server, user email accounts, system stability, and configuration settings.
  - **Verify security controls**, such as firewalls and intrusion detection systems, are properly configured and functioning as expected.

## Step 2: Ensure the Environment Is Secure

### 2.1 Reconfigure Network and Access Controls

- **Harden access to the Exchange Server** to prevent a recurrence of the attack, as the server was initially exposed to the internet without restrictions.
  - Action: Implement **firewall rules**, access control lists (ACLs), and **virtual private networks (VPNs)** to restrict public access to the Exchange Server.
  - **Require multi-factor authentication (MFA)** for all users accessing critical systems.
  - Best Practice: Apply the principle of least privilege (POLP) to limit access to critical systems and ensure that only authorized users have access.

### 2.2 Apply Security Patches

- Based on the known vulnerabilities (CVE-2020-0796, CVE-2018-13374, CVE-2018-13379) exploited in this attack, ensure that all affected systems are **patched and updated**.
  - Action: Patch not only the Exchange Server but also other systems that may have been vulnerable due to outdated software.
  - Assumption: Other systems in the network may have been at risk or exploited during the attack, so ensure that **system-wide patching** is applied.

### 2.3 Monitor for Residual Malicious Activity

- After systems are restored and patched, **continuously monitor** for any signs of reinfection or persistence by the attacker.
  - Action: Implement **continuous monitoring** with security information and event management (SIEM) tools to detect anomalies such as unusual login attempts, new malware, or ransomware-like behavior.
  - Ensure that **Sysmon and Splunk logs** are configured to capture file creation events, suspicious PowerShell executions, or any suspicious process migrations (e.g., related to powershell.exe or cmd.exe used in the original attack).
  - Best Practice: Use threat intelligence services to monitor for Indicators of Compromise (IOCs) related to Conti ransomware and apply threat detection rules across the network.

## Step 3: Validate Business Operations and User Accounts

### 3.1 Restore User Access

- After ensuring that systems are clean, **gradually restore user access** to critical services such as email and file-sharing.
  - Action: Validate that all **affected user accounts** (including those impacted by ransomware) have secure, functioning credentials. Any compromised accounts, such as the unauthorized user securityninja, must be disabled or deleted.
  - Reset all **user passwords** and ensure the use of **strong authentication methods** such as MFA to prevent attackers from using stolen credentials.

### 3.2 Restore Normal Operations

- Test the functionality of **all key systems and services** to ensure they are working properly before fully resuming business operations.
  - Action: Run test transactions, initiate communications, and ensure employees can access systems normally without issues.
  - Perform **system performance checks** to ensure the Exchange Server and other restored services are running at optimal levels.

## Step 4: Implement Long-Term Mitigation

### 4.1 Review and Update Incident Response Plans

- Based on the findings from the incident, **update the organization's incident response (IR) plan** to address any gaps or delays observed during the response process.
  - Action: Perform a **post-incident review** and document lessons learned from the attack, including how the ransomware was able to penetrate the environment, which systems were vulnerable, and the steps taken to recover.
  - Ensure that the organization is prepared for future attacks, focusing on **detection, analysis, and containment procedures**.

### 4.2 Implement Enhanced Security Measures

- **Strengthen email security** to reduce the risk of phishing attacks (which was the assumed delivery method of the Conti ransomware).
  - Action: Implement **email filtering**, anti-phishing solutions, and user training to recognize and avoid phishing attempts.
  - Deploy **anti-ransomware measures** such as file integrity monitoring, email scanning, and attachment filtering.
  - Apply **endpoint detection and response (EDR)** solutions to monitor user workstations and servers for malicious activity.

## 4.3 Backup and Disaster Recovery

- Ensure that **backups are properly secured and maintained** so that future incidents can be recovered from quickly and effectively.
  - Action: Implement **regular backup schedules** and ensure that backups are stored securely offline or in a cloud-based solution that cannot be accessed by ransomware.
  - **Test disaster recovery plans** frequently to ensure that systems and data can be restored within an acceptable time frame during future incidents.

## Step 5: Monitor the Environment for Future Attacks

### 5.1 Ongoing Monitoring and Threat Intelligence

- **Monitor the environment** for any residual threats, including new malware variants or re-entry by the attackers.
  - Action: Use SIEM and other monitoring tools to **track suspicious behavior** in real-time and deploy threat intelligence services to **track Conti ransomware developments**.
  - **Share IOCs** with industry partners and information-sharing groups to stay ahead of evolving threats.

### 5.2 Validate System Hardening

- After restoring systems, ensure that **system hardening measures** (such as patch management, access control, and segmentation) remain in place and are regularly updated.
  - Action: Perform **regular security audits** and vulnerability scans to check for any new misconfigurations or weaknesses that could be exploited.

## 4. Final Verification and Communication

### 4.1 Conduct Final Verification Checks

- Perform final system integrity checks to ensure that **all malicious elements are removed**, and the system operates as expected.
  - Action: **Cross-check logs**, system metrics, and user activity reports to verify that no suspicious activity is present, and systems are running smoothly.

### 4.2 Communicate with Stakeholders

- **Notify internal and external stakeholders** about the successful completion of the recovery process.

- Action: Prepare a **final incident report** outlining the recovery steps, improvements made, and any additional long-term actions that will be taken to secure the environment

## Phase-5 Lesson-Learning

The **lesson-learning phase** is the final stage of the incident response process. It focuses on reviewing the incident, analyzing the effectiveness of the response, and making improvements to strengthen security and response strategies. This phase is critical for improving an organization's resilience and preparedness for future incidents.

Based on the **TryHackMe Conti ransomware scenario**, the ransomware was delivered via phishing, and the organization's Exchange Server was exposed to the internet without restrictions, allowing the attack to succeed. This documentation outlines the steps taken to review the incident, gather lessons learned, and implement improvements.

### 1. Overview of the Lesson-Learning Phase

The lesson-learning phase serves to:

- **Evaluate the incident response** and identify what worked well and what did not.
- **Document gaps** in the security controls and incident response plan (IRP).
- **Implement improvements** to security, processes, and policies.
- **Share knowledge** with internal and external stakeholders to prevent future incidents.

### 2. Key Goals of the Lesson-Learning Phase

- **Identify weaknesses** in the existing security architecture and response capabilities.
- **Document incident details** thoroughly for future reference and audit purposes.
- **Update incident response plans** based on findings and lessons learned.
- **Improve employee awareness** and security practices to prevent future attacks.
- **Share insights** and indicators of compromise (IOCs) with peers, industry groups, and security communities.



### 3. Steps in the Lesson-Learning Phase

#### Step 1: Conduct a Post-Incident Review Meeting

##### 1.1 Gather the Incident Response Team

- Assemble all stakeholders involved in the incident response process, including:
  - **Incident response team (IRT) members:** responsible for detection, analysis, containment, eradication, and recovery.
  - **IT personnel:** responsible for system restoration and patching.
  - **Security operations (SecOps) team:** for monitoring, detection, and threat intelligence.
  - **Legal and compliance teams:** for reporting, regulatory requirements, and data protection concerns.
  - **Management and business leaders:** for operational continuity and business decision-making.

##### 1.2 Document a Timeline of Events

- **Create a detailed timeline** of the attack from the initial compromise (phishing attack) to the final recovery.
  - Action: Use logs, monitoring data, and security reports to document every phase of the incident.
  - Ensure that the timeline includes when the attack started, when it was detected, how containment was achieved, and how the eradication and recovery phases were executed.

##### 1.3 Review Incident Response Performance

- Review how effectively the **incident response plan (IRP)** was executed.
  - Action: Identify the following:
    - **Was the phishing attack detected early?** (e.g., through SIEM alerts or user reporting).
    - **Was containment achieved quickly?** (Did the response team act swiftly to isolate the Exchange Server and prevent further spread?)
    - **Were communication protocols followed?** (Were stakeholders, including management and external parties, informed in a timely manner?)
    - **Was the eradication thorough?** (Was there any persistence or remnants of malware post-eradication?)

##### 1.4 Identify Gaps and Areas for Improvement

- **Analyze weaknesses** in the current security architecture and processes:
  - Action: Identify where the organization's **defense-in-depth model** failed:
    - The Exchange Server was exposed to the internet without sufficient restrictions.

- Phishing emails bypassed email security filters and led to user compromise.
- **User awareness training** may have been insufficient to recognize phishing attempts.
- **Assess gaps** in the incident response process:
  - Were detection and alerting systems tuned to detect this type of attack early enough?
  - Were containment and recovery efforts delayed due to a lack of predefined steps or coordination?
  - Was sufficient **logging and monitoring** in place to identify the full scope of the attack?

## Step 2: Document Lessons Learned

### 2.1 Review Attack Vectors and Vulnerabilities

- **Analyze the root cause** of the attack to prevent future occurrences:
  - The attack was initiated via a phishing email, which led to the execution of the Conti ransomware.
  - The Exchange Server was exposed without sufficient security controls, providing an easy target for the attackers.
  - **Lessons Learned:**
    - Implement more robust **email security filters** to detect and block phishing attempts.
    - Ensure that critical systems, such as the Exchange Server, are protected with **firewall rules, network segmentation, and multi-factor authentication (MFA)**.
    - Apply **regular patching** and ensure all internet-facing services are up to date with security patches (e.g., CVE-2020-0796).

### 2.2 Review Indicators of Compromise (IOCs)

- **Identify IOCs** discovered during the detection and eradication phases:
  - The ransomware created suspicious processes (e.g., powershell.exe executing commands related to downloading and running malware).
  - Unusual network traffic to external IPs associated with Conti command and control (C2) servers.
  - Newly created user accounts, such as net user securityninja /add, which were used for lateral movement.
  - **Lessons Learned:**
    - Ensure IOCs are integrated into **SIEM tools** and that alerts are configured to detect them.
    - Use **threat intelligence services** to regularly update the organization's knowledge of IOCs and ensure they are shared with other security teams.

## 2.3 Document the Incident's Impact

- **Evaluate the overall impact** of the attack:
  - How long were critical services (e.g., email via the Exchange Server) down?
  - What was the financial cost in terms of downtime, system recovery, and IT resources?
  - Were there any **data breaches** or loss of sensitive information?
  - **Lessons Learned:**
    - Document these metrics for future reference, especially if they need to be shared with **insurance providers** or for **regulatory compliance** reporting.
    - **Prepare reports** for management detailing the **business impact** and justification for any additional security investments.

## Step 3: Update Incident Response Plan (IRP) and Policies

### 3.1 Revise the Incident Response Plan

- **Update the IRP** based on the lessons learned from the attack.
  - Action: Revise procedures for:
    - **Phishing detection and mitigation:** Ensure better email filtering and faster response times to phishing reports.
    - **Exchange Server security:** Ensure critical servers are not exposed without adequate network restrictions and MFA.
    - **Containment and recovery processes:** Implement predefined steps for isolating compromised systems and faster recovery from backups.
  - **Test the updated IRP** with regular tabletop exercises and incident simulations.

### 3.2 Strengthen Security Policies

- **Revise security policies** to address identified weaknesses:
  - **Access controls:** Apply stricter controls on internet-facing servers, implementing MFA and VPNs for external access.
  - **User training:** Enhance user awareness programs with regular phishing simulations and training sessions to improve detection and response.
  - **Backup policies:** Ensure regular offline or secure cloud backups to mitigate the risk of ransomware infecting backup data.
  - **Patch management:** Implement stricter patch management policies, requiring regular vulnerability assessments and system patching.

## Step 4: Implement Long-Term Preventative Measures

### 4.1 Improve Monitoring and Detection

- **Enhance detection capabilities** to identify future attacks more quickly:

- Action: Integrate **SIEM tools** with updated IOCs from the Conti ransomware attack, and ensure alerts are configured for unusual behaviors.
- Deploy **endpoint detection and response (EDR)** solutions to monitor for suspicious activity like lateral movement, process migration, or ransomware-like behavior.
- Implement **anomaly-based detection** to identify suspicious patterns that might indicate a new attack.

## 4.2 Conduct Regular Security Audits

- **Schedule regular security audits** to verify that all critical systems are properly secured and maintained.
  - Action: Perform penetration testing and vulnerability assessments on **internet-facing services**, especially Exchange Servers.
  - Ensure that **firewalls, intrusion detection systems (IDS), and access control lists (ACLs)** are properly configured and maintained.

## 4.3 Continue Employee Security Awareness Training

- **Regularly train employees** to detect and respond to phishing attacks:
  - Action: Conduct **annual phishing simulations** to measure and improve user awareness.
  - Update training materials to cover **new phishing techniques** and ways attackers may attempt to bypass security controls.

## Step 5: Share Knowledge and Findings

### 5.1 Share Insights with External Stakeholders

- **Share lessons learned** with external parties, including:
  - **Peers in the industry** or security communities to improve collective defense.
  - **Government or regulatory bodies** (if required) to ensure compliance with data protection laws or cybersecurity regulations.
  - **Threat intelligence networks** to update them with new IOCs related to Conti ransomware.

### 5.2 Create Internal Reports for Stakeholders

- **Prepare comprehensive reports** for internal stakeholders, including management, IT leadership, and legal teams.
  - Action: Document the **full incident timeline**, lessons learned, and recommendations for long-term improvements.
  - Provide **financial impact assessments** and justifications for future security investments, such as improved backup solutions or advanced detection tools.

## 4. Conclusion

The **lesson-learning phase** is crucial to improving an organization's ability to respond to future incidents. By conducting thorough reviews, identifying gaps, and implementing stronger controls, the organization can reduce the likelihood of

## References:

National Institute of Standards and Technology (NIST): <https://www.nist.gov/>

International Organization for Standardization (ISO): <https://www.iso.org/home.html>

CompTIA Security+: <https://www.comptia.org/certifications/security>

Certified Information Systems Security Professional (CISSP):  
<https://www.isc2.org/certifications/cissp>

OWASP (Open Web Application Security Project): <https://www.owasp.org/>

NIST (National Institute of Standards and Technology): [<https://www.nist.gov/>](https://www.nist.gov/)

MITRE Corporation: <https://www.mitre.org/>

CERT (Computer Emergency Response Team): <https://www.cert.org/>

OWASP (Open Web Application Security Project): [<https://www.owasp.org/>](https://www.owasp.org/)

CISA (Cybersecurity and Infrastructure Security Agency): <https://www.cisa.gov/>

CERT (Computer Emergency Response Team): <https://www.cert.org/>

Cisco: <https://www.cisco.com/>

Symantec: <https://www.symantec.com/>

NIST (National Institute of Standards and Technology): [<https://www.nist.gov/>](https://www.nist.gov/)

CISA (Cybersecurity and Infrastructure Security Agency): <https://www.cisa.gov/>

OWASP (Open Web Application Security Project): [<https://www.owasp.org/>](https://www.owasp.org/)

Metasploit: <https://www.metasploit.com/>

Nessus: <https://www.tenable.com/products/nessus>

Nmap: <https://nmap.org/>

Wireshark: <https://www.wireshark.org/>

RFC 792: Internet Control Message Protocol (ICMP):  
<https://datatracker.ietf.org/doc/html/rfc792>

