🛡️ Incident Response Plan: Malware Infection in Simulated Network

📅 Date of Report:

June 19, 2025

👤 Author:

Derek Santos Carwin — SOC Analyst (Student Project)

🧠 1. Description of the Security Incident

On **June 18, 2025, at 14:32 EST**, a suspicious outbound HTTP request was detected from a **Windows 10 host (10.0.2.15)** to an unfamiliar domain: `malware-dropper.example.net`. The file downloaded was a suspicious executable named `invoice_viewer.exe`.

The host was identified as a virtual machine in our isolated lab network. The activity was detected through **Zeek HTTP logs** and triggered a **malware alert in Security Onion's Suricata engine**.

🔍 2. Method for Detecting the Incident

Detection was achieved using the following tools:

Tool	Detection Method
Zeek (Bro)	Detected anomalous HTTP request to suspicious domain
Suricata	Generated IDS alert: `ET MALWARE Possible Malware Download`
Wireshark	Confirmed download of `.exe` payload
Kibana Dashboard	Alert spike for "high severity" malware detections

Indicator of Compromise (IOC):

- Destination IP: `185.101.93.77`
- Domain: `malware-dropper.example.net`
- File: `invoice_viewer.exe`
- File Hash (SHA256): `7b9f9a0a8a4e4d98988bb6ce622b97386c75cf125ae87621213bc2b16727a21f`

🚧 3. Containment Strategy

Immediate Containment Actions:

- Isolated the infected host (`10.0.2.15`) from the network using the hypervisor.
- Disabled outbound internet access from all lab hosts pending investigation.
- Logged the attack source IP into the local blocklist.

Future Prevention Measures:

- Implemented egress filtering to restrict HTTP traffic to known trusted domains.
- Added Suricata rule to trigger alerts for future access to known-malware domains.

🧹 4. Eradication Steps

- Removed the malicious file from the affected host.
- Cleared temporary directories for suspicious residual files.
- Performed deep antivirus scans using **Windows Defender Offline** and **ClamAV**.

Additional Steps:

- Reverted the VM to a clean snapshot (dated June 15, 2025).
- Reviewed Zeek `conn.log` and `files.log` to ensure no other hosts downloaded the malware.

♻️ 5. Recovery Steps

- Reconnected the cleaned host to the lab network under observation.
- Re-enabled internet access with firewall restrictions in place.

- Validated system logs and performance baseline metrics for stability.
- Conducted final log review for lateral movement attempts — none detected.

🧩 6. Identified Attack Type

Attack Category: Malware Infection
Vector: HTTP download of malicious executable from a compromised website
Attack Type: Remote Access Trojan (suspected)

📈 7. Timeline of the Incident

Time (EST)	Event
14:32	Host `10.0.2.15` requested `invoice_viewer.exe`
14:33	Suricata triggered malware alert
14:35	SOC alert escalated to Tier 1 Analyst
14:40	Host isolated and internet blocked
14:50	File removed, full scan initiated
15:15	Snapshot restored, host recovered
15:30	Firewall rules updated, monitoring continued

📌 8. Summary of Key Indicators & Tools

Component	Details
Affected Host	Windows 10 VM (`10.0.2.15`)
IOC – File	`invoice_viewer.exe`
IOC – IP	`185.101.93.77`
Detection Tools	Zeek, Suricata, Wireshark, Kibana

Response Tools	VM Snapshot, Antivirus, Blocklists

✅ 9. Lessons Learned

- **Early detection is critical** — tools like Zeek and Suricata provided timely alerts.
- Need to **limit outbound HTTP requests** in lab environments.
- Reinforced importance of **regular VM snapshots** and system isolation techniques.

Comprehensive Security Policy

For: "We Originated Cyber Security" Project & Environments

1. Purpose

The purpose of this policy is to establish and maintain a secure environment for monitoring, capturing, and analyzing network traffic in order to identify threats and protect digital assets. It outlines security requirements, responsibilities, and procedures to minimize cybersecurity risks.

---

2. Scope

This policy applies to all individuals accessing the project environment, including:

- Students and Trainees
- SOC Analysts and Cybersecurity Professionals
- Instructors and Supervisors
- Organization Employees and Contractors

It covers:

- Network traffic analysis systems
- Monitoring tools (e.g., Wireshark, Nmap)
- Data storage and transmission
- Endpoints and devices connected to the network
- User access and authentication

---

3. Roles and Responsibilities

Role	Responsibilities
SOC Analyst	Monitor and respond to security incidents, follow documentation protocols
Instructor/Manager	Oversee operations, enforce policy compliance, conduct training
Users (Trainees, Students)	Follow guidelines, use tools responsibly, report anomalies
IT Support	Ensure system security, patch updates, manage user access

---

4. Acceptable Use Policy (AUP)

- Use project tools and systems only for educational or authorized professional purposes.
- Do not attempt to access, share, or analyze unauthorized or personal data.
- Do not launch offensive security techniques (e.g., attacks) without written permission.
- All activity must align with ethical and legal standards (e.g., no malware distribution, no unauthorized packet sniffing on live environments).

---

5. Access Control

- Users must be authenticated using strong passwords and, if possible, multi-factor authentication (MFA).
- Access is granted based on the principle of least privilege (PoLP).
- Role-based access controls (RBAC) must be implemented to ensure appropriate permissions.
- User accounts are reviewed regularly and revoked when no longer needed.

---

6. Network Monitoring & Logging

- All network traffic must be captured within the controlled lab or simulation environments.
- Logs must be collected, encrypted, and retained for a minimum of 90 days.
- Suspicious behavior or unauthorized access attempts must be reported and investigated immediately.

---

7. Tool Usage & System Configuration

- Only approved tools (e.g., Wireshark, Nmap) are permitted.
- Tools must be kept up to date and securely configured.
- No cracked, pirated, or unverified third-party tools may be installed or used.

---

8. Data Protection

- Sensitive data (e.g., IP logs, captured packets) must be stored securely with encryption.
- Data transmission should use encrypted protocols (e.g., HTTPS, SSH).
- Access to project data should be logged and auditable.

---

9. Incident Response Plan

- All users must be trained in identifying and reporting incidents.
- Incidents should be reported to the designated SOC lead or instructor within **1 hour**.
- Response steps include:
    - Logging the incident
    - Containing the threat
    - Analyzing the root cause
    - Remediating and restoring operations
    - Documenting findings and improvements

---

10. Policy Review and Updates

- This policy is reviewed **biannually** or after any major incident.
- All users must re-sign acknowledgment after any update.
- Suggestions for improvement should be submitted to the policy lead or instructor.

---

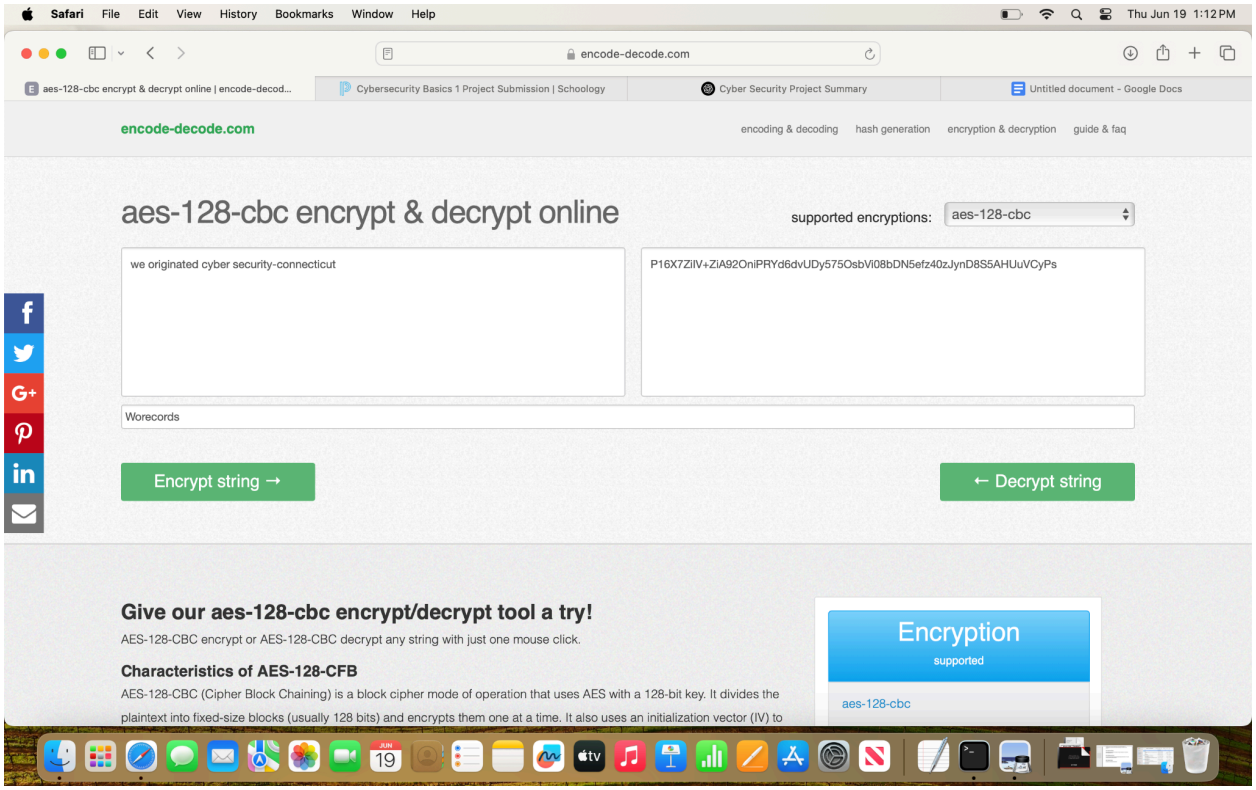
11. Compliance & Enforcement

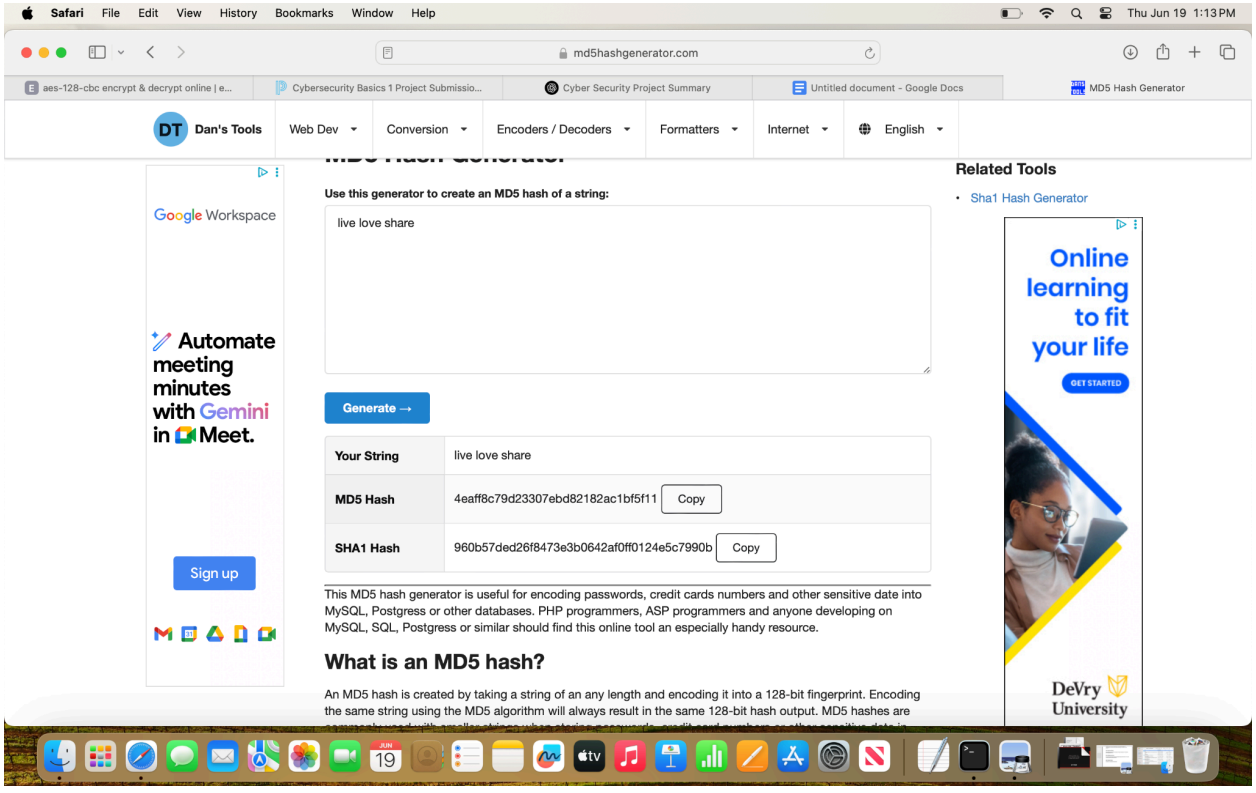
- Non-compliance may result in access suspension, disciplinary actions, or legal consequences.
- Violations of ethical or legal standards will be escalated to senior management or authorities if necessary.

Acknowledgment

By participating in the “We Originated Cyber Security” project, I acknowledge that I have read, understood, and agreed to comply with the security policy above.

Name: _____
Date: _____


Safari File Edit View History Bookmarks Window Help
Thu Jun 19 1:12 PM
encode-decode.com
aes-128-cbc encrypt & decrypt online | encode-decod...
Cybersecurity Basics 1 Project Submission | Schoology
Cyber Security Project Summary
Untitled document - Google Docs
encode-decode.com
encoding & decoding
hash generation
encryption & decryption
guide & faq
aes-128-cbc encrypt & decrypt online
supported encryptions:
aes-128-cbc
we originated cyber security-connecticut
P16X7ZilV+ZiA92OniPRYd6dvUDy575OsbVi08bDN5efz40zJynD8S5AHUuVCyPs
Worecords
Encrypt string →
← Decrypt string
Give our aes-128-cbc encrypt/decrypt tool a try!
AES-128-CBC encrypt or AES-128-CBC decrypt any string with just one mouse click.
Characteristics of AES-128-CFB
AES-128-CBC (Cipher Block Chaining) is a block cipher mode of operation that uses AES with a 128-bit key. It divides the plaintext into fixed-size blocks (usually 128 bits) and encrypts them one at a time. It also uses an initialization vector (IV) to
Encryption
supported
aes-128-cbc


Safari File Edit View History Bookmarks Window Help
Thu Jun 19 1:13 PM
md5hashgenerator.com
aes-128-cbc encrypt & decrypt online | e...
Cybersecurity Basics 1 Project Submissio...
Cyber Security Project Summary
Untitled document - Google Docs
MD5 Hash Generator
DT Dan's Tools
Web Dev
Conversion
Encoders / Decoders
Formatters
Internet
English
Google Workspace
Automate meeting minutes with Gemini in Meet.
Sign up
Use this generator to create an MD5 hash of a string:
live love share
Generate →
Your String
live love share
MD5 Hash
4eaff8c79d23307ebd82182ac1bf5f11
Copy
SHA1 Hash
960b57ded26f8473e3b0642af0ff0124e5c7990b
Copy
This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive date into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL, Postgress or similar should find this online tool an especially handy resource.
What is an MD5 hash?
An MD5 hash is created by taking a string of an any length and encoding it into a 128-bit fingerprint. Encoding the same string using the MD5 algorithm will always result in the same 128-bit hash output. MD5 hashes are
Related Tools
Sha1 Hash Generator
Online learning to fit your life
GET STARTED
DeVry University

🔏 Legal and Ethical Compliance in Incident Response

Ensuring that all actions during an incident response adhere to legal and ethical standards is critical to maintaining the integrity of the organization, protecting users' rights, and avoiding legal liabilities. This section outlines the applicable laws, ethical responsibilities, and the specific ways our incident response plan upholds them.

⚖️ Relevant Laws and Regulations

1. Computer Fraud and Abuse Act (CFAA) – United States

- **What it covers**: Unauthorized access to or damage of protected computers and networks.
- **Why it matters**: During incident response, analysts may access sensitive systems or data. Any access must be authorized, even when investigating a potential breach.

2. General Data Protection Regulation (GDPR) – European Union *(Applies globally when handling EU citizens' data)*

- **What it covers**: Protection of personal data and privacy for individuals in the EU.
- **Why it matters**: If network monitoring captures personal data (e.g., IPs, email addresses), it must be handled lawfully, with consent, minimal exposure, and proper anonymization when required.

🧭 Ethical Considerations

✅ Privacy and Confidentiality

Incident responders often access confidential communications, personal information, or sensitive corporate data. Upholding trust means not using this access for personal gain, exposure, or surveillance beyond the scope of investigation.

🛡️ How Our Incident Response Plan Upholds Legal and Ethical Standards

Legal/Ethical Standard	Compliance in Plan

Authorized Access Only	Role-based access control ensures that only trained and approved personnel respond to incidents. Logs track all actions taken during an incident.
Data Privacy (GDPR)	Personal data is anonymized when possible, securely stored, and never shared beyond the incident response team. Notification procedures are in place if a breach involves EU data subjects.
Evidence Handling (Chain of Custody)	All evidence collected (logs, PCAPs) is documented, encrypted, and handled to preserve integrity—supporting legal admissibility.
Ethical Responsibility	All SOC analysts must sign a Code of Ethics emphasizing non-disclosure, privacy respect, and professional conduct.
Incident Reporting	Legal counsel is consulted when reporting breaches externally, ensuring correct regulatory compliance (e.g., GDPR 72-hour breach notification).

📄 Acknowledgment of Legal & Ethical Compliance

All project participants (students, analysts, instructors) must complete annual cybersecurity ethics training and sign acknowledgment forms confirming:

- Understanding of applicable laws
- Agreement to ethical guidelines
- Responsibility to report violations

✅ Summary

Our incident response plan embeds legal and ethical compliance through:

- Authorization protocols (CFAA)
- Data protection (GDPR)
- Respect for privacy and confidentiality
- Professional conduct and evidence handling