Incident Response Case Report

Analyst: Alexander T. Ramos
Date: October 05, 2025
Incident Title: Phishing Attack Leading to Credential Theft and Malware Execution
Severity: High
Status: Resolved

1. Executive Summary

On October 4, 2025, the SOC detected suspicious PowerShell activity on a corporate Windows endpoint. Subsequent investigation revealed a phishing email containing a malicious attachment that downloaded a credential-stealing malware variant identified as AgentTesla. Swift containment actions prevented lateral movement and data exfiltration. The incident was contained and eradicated within five hours, with no evidence of compromise to sensitive data.

2. Incident Timeline

Time (PST)	Event
09:13 AM	Splunk SIEM alert triggered for base64-encoded PowerShell execution.
09:20 AM	Analyst confirmed correlation between email logs and affected endpoint.
09:32 AM	EDR isolated endpoint from the network.
09:50 AM	Firewall and proxy blocks applied to malicious IP and domain.
11:00 AM	Malware sample analyzed and identified as AgentTesla.
1:15 PM	Endpoint reimaged and user credentials reset.
2:00 PM	Incident closed following post-remediation verification.

3. Affected Systems

Hostname	Role	Impact
WIN10-ENG-JSMITH	User workstation	Compromised (malware infection, credential theft

4. Indicators of Compromise (IOCs)

Type	Indicator	Description
Domain	microsoft-update-checks.com	Fake Microsoft update domain hosting malware.
IP Address	45.199.200.32	Known C2 server for AgentTesla.
File Hash	6acb82e2f92e3...	Hash of malware executable.

5. Response Actions

Containment: Isolated endpoint, disabled account, and blocked malicious IP/domain.
Eradication: Removed malware, patched systems, and reset PowerShell execution policy.
Recovery: Reimaged device, restored approved data, and validated clean system state.

6. Impact Assessment

Data Loss	None detected
Systems Affected	1 endpoint
Business Impact	Minimal downtime (under 5 hours)
User Impact	Temporary credential reset required

7. Lessons Learned

- Increase phishing simulation frequency for end-user awareness.
- Add real-time alerts for base64-encoded PowerShell activity.
- Automate IOC blocking via SIEM–EDR integration.
- Improve incident documentation templates for rapid reporting.

8. Conclusion

The rapid identification, containment, and remediation of this incident demonstrate effective SOC procedures and adherence to NIST 800-61 response principles. The organization’s quick response prevented further compromise and reinforced readiness for future threats.

Prepared by: Alexander T. Ramos – Cybersecurity Analyst