**Cybersecurity Incident Investigation Report**

**Executive Summary**

This report documents a comprehensive malware investigation conducted on April 1, 2024, following reports of unusual system behavior including slow performance, pop-up ads, and unauthorized connections to external IP addresses. The investigation revealed multiple indicators of compromise (IoCs) across system logs, network traffic, and endpoint protection systems.

**1. Log Analysis and Evidence Collection**

**Windows Event Logs (Security)**

**Event ID 4672 - Special Privilege Assignment**

* **User:** UnknownUser
* **Privilege:** SeAssignPrimaryTokenPrivilege
* **Analysis:** Unauthorized privilege escalation detected for unknown user account

**Event ID 4776 - Credential Validation Attempt**

* **User:** SYSTEM
* **Source IP:** 198.51.100.10
* **Analysis:** Failed authentication attempt from external IP address

**Application Logs**

**Event ID 1015 - Application Error**

* **Application:** explorer.exe
* **Faulting Module:** injected.dll
* **Analysis:** Critical system process (Windows Explorer) compromised by malicious DLL injection

**System Logs**

**Event ID 7034 - Service Control Manager**

* **Service:** Windows Update Service
* **Status:** Terminated Unexpectedly
* **Analysis:** Essential Windows service disrupted, potentially by malware

**Firewall and Network Logs**

**Outbound Connections Analysis:**

**Connection 1:**

* **Timestamp:** 2024-04-01 14:45:00
* **Source IP:** 192.168.50.23
* **Destination IP:** 203.0.113.5
* **Port:** 22
* **Protocol:** TCP
* **Status:** ALLOWED

**Connection 2:**

* **Timestamp:** 2024-04-01 14:50:30
* **Source IP:** 192.168.50.23
* **Destination IP:** 192.0.2.89
* **Port:** 9000
* **Protocol:** TCP
* **Status:** ALLOWED

**Unauthorized Access Attempt:**

* **Timestamp:** 2024-04-01 15:12:00
* **Source IP:** 198.51.100.10
* **Destination IP:** 192.168.50.23
* **Action:** BLOCKED
* **Reason:** Multiple failed authentication attempts

**Antivirus/Endpoint Protection Logs**

**Detected Threats:**

* **Timestamp:** 2024-04-01 15:30:00
* **Threat Name:** Worm.Autorun.Script
* **File Path:** C:\Users\Guest\Documents\hidden.vbs
* **Action Taken:** Suspended
* **Detection Method:** Behavior Analysis

**System Scan Report:**

* **Timestamp:** 2024-04-01 16:00:00
* **Total Files Scanned:** 200,000
* **Threats Detected:** 2
  + C:\ProgramData\startup.bat (Trojan Downloader)
  + C:\Users\Guest\Documents\hidden.vbs (Worm)
* **Action Taken:** Quarantined, Further Investigation Required

**2. Indicators of Compromise (IoCs)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Indicator Type** | **Value** | **Description** | **Evidence Source** |
| **Unauthorized Process Execution** | explorer.exe with injected.dll | Windows Explorer compromised by DLL injection | Application Logs |
| **Suspicious Outbound Connections** | 203.0.113.5:22, 192.0.2.89:9000 | Unauthorized external communications | Firewall Logs |
| **Failed Remote Login Attempts** | Source IP: 198.51.100.10 | Multiple failed authentication attempts | Security Logs |
| **Terminated Security Service** | Windows Update Service | Critical service unexpectedly terminated | System Logs |
| **Malicious Files** | startup.bat, hidden.vbs | Trojan downloader and worm detected | Antivirus Logs |
| **Privilege Escalation** | UnknownUser account | Unauthorized user granted special privileges | Security Logs |

**3. Investigation Summary**

**What Happened?**

The system was compromised by a multi-stage malware attack that began with a Trojan downloader (startup.bat) which subsequently downloaded and executed additional malicious payloads including a worm script (hidden.vbs). The malware performed DLL injection into the Windows Explorer process, established unauthorized network connections, and attempted to escalate privileges through an unknown user account.

**What Was Found?**

* **Primary Infection Vector:** Trojan downloader in startup directory
* **Secondary Payload:** Autorun worm script with network propagation capabilities
* **System Compromise:** DLL injection into critical Windows processes
* **Network Activity:** Unauthorized outbound connections to suspicious IP addresses
* **Privilege Escalation:** Creation of unknown user account with special privileges
* **Service Disruption:** Windows Update service terminated, potentially to prevent security updates

**What Is the Impact?**

* **Confidentiality:** Potential data exfiltration through unauthorized network connections
* **Integrity:** System files and processes compromised through DLL injection
* **Availability:** Critical Windows services disrupted, system performance degraded
* **Security Posture:** Firewall bypassed, endpoint protection partially evaded
* **Business Operations:** User productivity impacted by pop-up ads and slow performance

**4. Recommended Remediation Steps**

**Immediate Actions (0-24 hours)**

1. **Isolate the infected machine** from the network to prevent lateral movement
2. **Terminate all unauthorized processes** and remove injected DLLs
3. **Block identified malicious IP addresses** (203.0.113.5, 192.0.2.89, 198.51.100.10) at firewall level
4. **Remove or disable the UnknownUser account** and audit all privilege assignments
5. **Quarantine and delete identified malware files** (startup.bat, hidden.vbs)

**Short-term Actions (1-7 days)**

1. **Perform full system restoration** from clean backup or complete OS reinstallation
2. **Update all security patches** and restart Windows Update service
3. **Conduct comprehensive malware scan** on all network-connected devices
4. **Reset all user passwords** and implement multi-factor authentication
5. **Review and update firewall rules** to block unauthorized outbound connections

**Long-term Actions (1-4 weeks)**

1. **Implement enhanced endpoint detection and response** (EDR) solutions
2. **Conduct security awareness training** for all employees
3. **Establish network segmentation** to limit malware spread
4. **Deploy application whitelisting** to prevent unauthorized executable files
5. **Implement continuous monitoring** for similar IoCs across the environment

**Preventive Measures**

1. **Regular security assessments** and penetration testing
2. **Email security gateway** to block malicious attachments
3. **Web content filtering** to prevent access to malicious websites
4. **Backup and recovery procedures** with offline backup storage
5. **Incident response plan** with defined roles and procedures

**5. Lessons Learned**

1. **Detection Gap:** The initial Trojan downloader evaded detection for an unknown period, indicating a need for improved behavioral analysis
2. **Network Monitoring:** Unauthorized outbound connections should trigger immediate alerts
3. **Privilege Management:** Unknown user accounts with special privileges require immediate investigation
4. **Service Monitoring:** Critical Windows services should be monitored for unexpected termination
5. **User Education:** Additional training needed on identifying and avoiding malicious software

**Conclusion**

This incident represents a sophisticated multi-stage malware attack that successfully compromised system integrity and established unauthorized network communications. The combination of Trojan downloaders, worm propagation, DLL injection, and privilege escalation indicates an advanced persistent threat. Immediate remediation steps have been implemented, and long-term security improvements are recommended to prevent similar incidents.

The investigation confirms that the unusual system behavior reported by the employee was indeed indicative of malware infection, validating the importance of user reporting in early threat detection.