

Investigate a Malware-infected System Logs and Report Findings and Solutions

Logs and Evidence Collected

Analysis of Collected System Logs

1. Windows Event Logs

- **Security Logs:**
 - **Event ID 4672:** Special privileges assigned to a new logon.
 - **User:** UnknownUser
 - **Privilege:** SeAssignPrimaryTokenPrivilege (privilege escalation indicator)
 - **Event ID 4776:** Failed credential validation for account.
 - **User:** SYSTEM
 - **Source IP:** 198.51.100.10
 - Suggests possible brute-force or credential stuffing attempt.
- **Application Logs:**
 - **Event ID 1015:** explorer.exe faulted due to injected.dll.
 - This indicates **DLL injection**, a common malware technique.
- **System Logs:**
 - **Event ID 7034:** Windows Update Service terminated unexpectedly.
 - Attackers often disable updates to prevent patching of vulnerabilities.

2. Firewall and Network Logs

- **Outbound Connections:**
 - From 192.168.50.23 to:
 - 203.0.113.5 on port 22 (SSH)

- **192.0.2.89** on **port 9090 (suspicious custom port)**
- These connections were **allowed** — possibly malware exfiltrating data or creating reverse shells.
- **Unauthorized Access Attempt:**
 - Source IP: **198.51.100.10**, Destination IP: **192.168.50.23**
 - Action: **Blocked**
 - Reason: **Multiple failed authentication attempts**
 - Likely part of a brute-force or lateral movement attempt.

3. Antivirus / Endpoint Protection Logs

- **Detected Threat:**
 - **Worm.Autorun.Script** in **C:\Users\Guest\Documents\hidden.vbs**
 - Detection Method: **Behavior Analysis**
 - **Action Taken:** Suspended
- **System Scan Report:**
 - Threats Detected:
 - **C:\ProgramData\startup.bat** → Trojan Downloader
 - **C:\Users\Guest\Documents\hidden.vbs** → Worm
 - **Action Taken:** Quarantined
 - Status: Further Investigation Required

Summary of Indicators of Compromise (IoCs)

Indicator of Compromise	Description	Evidence
explorer.exe → injected.dll	DLL injection attack	Application Log Event ID 1015

startup.bat	Trojan downloader on system	Antivirus Scan
hidden.vbs	Worm infection	Detected Threat + Scan
IP: 198.51.100.10	Repeated unauthorized access	Security Log & Firewall Log
Event ID 4672	Privileged logon by unknown user	Security Log
Disabled updates	Likely persistence technique	System Log Event ID 7034
Outbound to 203.0.113.5:22, 192.0.2.89:9090	Suspicious external communication	Firewall Logs

Indicators of Compromise (IOCs) Identified

1. Unauthorized Process Execution

- **Executable Launched:** C:\Users\Public\startup\autorun.vbs
- **Parent Process:** wscript.exe spawned by explorer.exe
- **Command Line:** wscript.exe hidden.vbs
- **Behavior:**
 - Scheduled to run at user logon via HKCU\Software\Microsoft\Windows\CurrentVersion\Run
 - **Unusual** for average users to run .vbs scripts directly unless configured by malware

Conclusion: This is **unauthorized/suspicious**. hidden.vbs is a known technique for stealthy malware execution.

2. Suspicious Outbound Network Connections

- **Source IP:** 192.168.50.23
- **Outbound Destinations:**

- 203.0.113.5:22 – Outbound SSH
- 192.0.2.89:9090 – Uncommon port
- **Process:** Connection initiated by `svchost.exe` (normally benign, often abused)
- **Flags:**
 - These are **non-corporate external IPs**
 - `svchost.exe` is not expected to initiate outbound SSH sessions

Conclusion: These are **likely Command and Control (C2)** or **data exfiltration** attempts.

3. ❌ Failed Remote Login Attempts

- **Event ID:** 4776
- **Target Account:** `SYSTEM`
- **Source:** IP address `198.51.100.10`
- **Authentication Package:** NTLM
- **Failure Code:** 0xC000006A (wrong password)

Conclusion: Indicates a **remote brute-force login attempt** from an **unauthorized external address**.


4. 🛑 Terminated Security Services

- **Event ID:** 7034
- **Service Name:** `wuauserv` (Windows Update)
- **Termination Type:** Unexpected crash

Conclusion: Disabling the update service is a known **persistence tactic** used by malware to **prevent patching** and **avoid detection**.

IOC Category	Details	Why Suspicious
Unauthorized Process Exec	wscript.exe hidden.vbs from explorer.exe	Likely part of malware (autorun worm or trojan)
Suspicious Network Activity	Outbound to 203.0.113.5:22 & 192.0.2.89:9090 via svchost.exe	Indicative of remote C2 channel or exfiltration
Failed Remote Logins	Multiple Event 4776 failures from IP 198.51.100.10 targeting SYSTEM	Brute-force attempt from unknown remote host
Security Services Terminated	Event 7034: Windows Update Service unexpectedly stopped	Prevents patching and AV signature updates

A summary of findings and analysis

 Incident Report: Suspicious Activity Detected on Host

Date of Detection: June 28, 2025

Reported By: Security Operations Analyst


Host IP: 192.168.50.23

Username: (Redacted for privacy)

Operating System: Windows 10

Incident Status: Under Investigation

Severity: High

 Table of Indicators of Compromise (IoCs)

Indicator of Compromise (IoC)	Description	Evidence Collected
Unauthorized Script Execution	A Visual Basic Script (hidden.vbs) executed at logon via wscript.exe.	- C:\Users\Public\startup\autorun.vbs - Parent: explorer.exe - Command: wscript.exe hidden.vbs
Suspicious Outbound Connections	Unusual outbound traffic to external IPs and ports not associated with normal ops.	- svchost.exe connecting to 203.0.113.5:22 and 192.0.2.89:9090 - Host IP: 192.168.50.23
Failed Remote Login Attempts	Multiple NTLM authentication failures from a non-local IP address.	- Event ID 4776 - Target: SYSTEM - Source IP: 198.51.100.10 - Failure Code: 0xC000006A

Termination of Windows Update service - Event ID 7034
Security Services (**wuauserv**) unexpectedly - Service: **wuauserv**
terminated. - Status: Unexpected Termination

```
MINGW64/c/logs
HNSIGNATURES MINGW64 /c/logs
$ mkdir -p /c/logs
HNSIGNATURES MINGW64 /c/logs
$ mkdir -p /c/logs/windows_events
mkdir -p /c/logs/firewall_network
mkdir -p /c/logs/antivirus
HNSIGNATURES MINGW64 /c/logs
$ touch /c/logs/windows_events/system.log
touch /c/logs/windows_events/application.log
touch /c/logs/windows_events/security.log
HNSIGNATURES MINGW64 /c/logs
$ touch /c/logs/firewall_network/firewall.log
touch /c/logs/firewall_network/network.log
touch /c/logs/firewall_network/connection_attempts.log
HNSIGNATURES MINGW64 /c/logs
$ touch /c/logs/antivirus/scan_report.log
touch /c/logs/antivirus/quarantine.log
touch /c/logs/antivirus/realtime_protection.log
HNSIGNATURES MINGW64 /c/logs
$ cat >> /c/logs/windows_events/security.log <<EOF
> Event ID: 4672 - Special Privilege Assigned to New Logon
User: UnknownUser
Privilege: SeAssignPrimaryTokenPrivilege
Event ID: 4776 - The computer attempted to validate the credentials for an account
User: SYSTEM
Source IP: 198.51.100.10
> EOF
HNSIGNATURES MINGW64 /c/logs
$ cat /c/logs/windows_events/security.log
Event ID: 4672 - Special Privilege Assigned to New Logon
User: UnknownUser
Privilege: SeAssignPrimaryTokenPrivilege
Event ID: 4776 - The computer attempted to validate the credentials for an account
User: SYSTEM
Source IP: 198.51.100.10
HNSIGNATURES MINGW64 /c/logs
$ cat >> /c/logs/windows_events/application.log <<EOF
> Event ID: 1015 - Application Error
Application Name: explorer.exe
> EOF
```

```
MINGW64/c/logs
HNSIGNATURES MINGW64 /c/logs
$ cat >> /c/logs/firewall_network/firewall.log <<EOF
> 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
Timestamp: 2024-04-01 14:50:30
Source IP: 192.168.50.23
Destination IP: 192.0.2.89
Port: 9090
Protocol: TCP
Status: ALLOWED
> EOF
HNSIGNATURES MINGW64 /c/logs
$ cat /c/logs/windows_events/firewall.log
cat: /c/logs/windows_events/firewall.log: No such file or directory
HNSIGNATURES MINGW64 /c/logs
$ cat /c/logs/firewall_network/firewall.log
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
Timestamp: 2024-04-01 14:50:30
Source IP: 192.168.50.23
Destination IP: 192.0.2.89
Port: 9090
Protocol: TCP
Status: ALLOWED
HNSIGNATURES MINGW64 /c/logs
$ cat >> /c/logs/firewall_network/connection_attempts.log <<EOF
> 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
> EOF
HNSIGNATURES MINGW64 /c/logs
$ cat /c/logs/firewall_network/connection_attempts.log
Timestamp: 2024-04-01 15:12:00
Source IP: 198.51.100.10
```

```
MINGW64/c/logs
HNSIGNATURES MINGW64 /c/logs
$ cat >> /c/logs/windows_events/security.log <<EOF
> Event ID: 4672 - Special Privilege Assigned to New Logon
User: UnknownUser
Privilege: SeAssignPrimaryTokenPrivilege
Event ID: 4776 - The computer attempted to validate the credentials for an account
User: SYSTEM
Source IP: 198.51.100.10
> EOF
HNSIGNATURES MINGW64 /c/logs
$ cat /c/logs/windows_events/security.log
Event ID: 4672 - Special Privilege Assigned to New Logon
User: UnknownUser
Privilege: SeAssignPrimaryTokenPrivilege
Event ID: 4776 - The computer attempted to validate the credentials for an account
User: SYSTEM
Source IP: 198.51.100.10
HNSIGNATURES MINGW64 /c/logs
$ cat >> /c/logs/windows_events/application.log <<EOF
> Event ID: 1015 - Application Error
Application Name: explorer.exe
Faulting Module: injected.dll
> EOF
HNSIGNATURES MINGW64 /c/logs
$ cat /c/logs/windows_events/application.log
Event ID: 1015 - Application Error
Application Name: explorer.exe
Faulting Module: injected.dll
HNSIGNATURES MINGW64 /c/logs
$ cat >> /c/logs/windows_events/system.log <<EOF
> Event ID: 7034 - Service Control Manager
Service: Windows Update Service Terminated Unexpectedly
> EOF
HNSIGNATURES MINGW64 /c/logs
$ cat /c/logs/windows_events/system.log
Event ID: 7034 - Service Control Manager
Service: Windows Update Service Terminated Unexpectedly
HNSIGNATURES MINGW64 /c/logs
$
```

```
MINGW64/c/logs
Action: BLOCKED
Reason: Multiple failed authentication attempts
> EOF

HIPSIGNATURES MINGW64 /c/logs
$ cat /c/logs/firewall/network/connection_attempts.log
Timestamp: 2024-04-01 15:12:00
Source IP: 192.0.2.100
Destination IP: 192.168.50.23
Action: BLOCKED
Reason: Multiple failed authentication attempts
> EOF

HIPSIGNATURES MINGW64 /c/logs
$ cat >> /c/logs/antivirus/scan_report.log <<EOF
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
> EOF

HIPSIGNATURES MINGW64 /c/logs
$ cat /c/logs/antivirus/scan_report.log
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
> EOF

HIPSIGNATURES MINGW64 /c/logs
$ cat >> /c/logs/antivirus/quarantine.log <<EOF
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
> EOF

HIPSIGNATURES MINGW64 /c/logs
$ cat /c/logs/antivirus/quarantine.log
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
> EOF

HIPSIGNATURES MINGW64 /c/logs
$ |
```

```
MINGW64/c/logs
HIPSIGNATURES MINGW64 /c/logs
$ cat > /c/logs/ioc_analyzer.sh << 'EOF'
#!/bin/bash
echo "===== ANALYZING WINDOWS EVENT LOGS ====="
# Unauthorized privilege assignment
grep -i "Event ID: 4672" /c/logs/windows_events/security.log && echo "[!] Privilege escalation attempt detected."
# Failed logins
grep -i "Event ID: 4776" /c/logs/windows_events/security.log && echo "[!] Failed credential validation attempt."
# Suspicious module injection
grep -i "Injected.dll" /c/logs/windows_events/application.log && echo "[!] Possible code injection detected."
# Security service terminated
grep -i "7045" /c/logs/windows_events/system.log | grep -i "Terminated" && echo "[!] Security or critical service terminated unexpectedly."
echo -e "\n===== ANALYZING FIREWALL & NETWORK LOGS ====="
# Suspicious outbound connections
grep -E "203\.\d\.\d\.\d" /c/logs/firewall_network/firewall.log && echo "[!] Suspicious external IP communication detected."
echo -e "\n===== IOC SCAN COMPLETE ====="
HIPSIGNATURES MINGW64 /c/logs
$ |
```

```
MINGW64/c/logs
===== ANALYZING WINDOWS EVENT LOGS =====
Event ID: 4672 - Special Privilege Assigned to New Logon
[!] Privilege escalation attempt detected.
Event ID: 4776 - The computer attempted to validate the credentials for an account
[!] Failed credential validation attempt.
Faulting Module: injected.dll
[!] Possible code injection detected.
===== ANALYZING FIREWALL & NETWORK LOGS =====
Destination IP: 203.0.113.5
Destination IP: 192.0.2.89
[!] Suspicious external IP communication detected.
Reason: Multiple failed authentication attempts
[!] Repeated failed login attempts detected.
===== ANALYZING ANTIVIRUS LOGS =====
/c/logs/antivirus/quarantine.log: C:\ProgramData\startup.bat (Trojan Downloader)
/c/logs/antivirus/quarantine.log: C:\Users\Guest\Documents\hidden.vbs (Worm)
/c/logs/antivirus/quarantine.log: Action Taken: Quarantined, Further Investigation Required
/c/logs/antivirus/scan_report.log: Threat Name: Worm.Autorun.Script
/c/logs/antivirus/scan_report.log: Action Taken: Suspended
[!] Malware activity recorded.
===== IOC SCAN COMPLETE =====
HIPSIGNATURES MINGW64 /c/logs
$ ls /c/logs
antivirus firewall_network ioc_analyzer.sh windows_events
HIPSIGNATURES MINGW64 /c/logs
$ |
```

Analysis Summary

The presence of **unauthorized script execution**, **external network connections** via system processes like **svchost.exe**, and **multiple failed login attempts** indicate that the host may be

compromised by a remote attacker. The unexpected shutdown of security services suggests deliberate attempts to evade detection and maintain persistence.

A summary of findings and analysis



Investigation Summary



What Happened

A potentially malicious script (**hidden.vbs**) was executed during user login, initiating unauthorized activity on the host system. The host began communicating with unknown external IP addresses over suspicious ports and exhibited signs of attempted remote access. Core system services, including a key security service, were found to be unexpectedly terminated.



What Was Found

- **Unauthorized Script Execution:** A Visual Basic script (**hidden.vbs**) was auto-executed using **wscript.exe** via a startup folder entry.
- **Suspicious Outbound Connections:** System processes like **svchost.exe** were observed communicating with external IP addresses not associated with normal operations, including one over SSH (port 22) and another on a high port (9090).
- **Failed Remote Logins:** Numerous NTLM authentication failures originated from a remote IP, indicating potential brute-force or credential stuffing attempts.
- **Security Service Terminated:** The Windows Update service (**wuauserv**) was unexpectedly shut down, indicating possible tampering or an attempt to disable system defenses.



Impact

- **System Compromise Likely:** The execution of an unauthorized script and external communications suggest initial access may have been achieved.
- **Security Posture Degraded:** Termination of security services like Windows Update exposes the system to further vulnerabilities and patch delays.
- **Risk of Lateral Movement:** If attacker access is confirmed, there's a high risk of pivoting to other systems on the network.
- **Data Exfiltration Possible:** Outbound connections could facilitate the transfer of sensitive information outside the organization's control.



Recommended Remediation Actions

1. Isolate the Affected System

- **Immediately disconnect** the compromised host (192.168.50.23) from the network to prevent further lateral movement or data exfiltration.

2. Eradicate Malicious Artifacts

- Delete or quarantine the following:
 - C:\Users\Public\startup\autorun.vbs
 - C:\Users\Guest\Documents\hidden.vbs
 - Any associated scripts or scheduled tasks linked to malicious execution.
- Search the registry for persistence mechanisms (e.g., HKCU\Software\Microsoft\Windows\CurrentVersion\Run).

3. Reset Compromised Credentials

- Force password resets for all accounts that were targeted or used on the host.
- Ensure strong password policies and enable **account lockout policies** to prevent brute-force attempts.

4. Conduct Full System Scans

- Run a full antivirus/EDR scan using updated definitions.
- Use tools like **Windows Defender Offline**, **Malwarebytes**, or your enterprise EDR solution for in-depth scanning.

5. Review and Harden Network Rules

- Block outbound connections to:
 - 203.0.113.5
 - 192.0.2.89
- Implement **egress filtering** to restrict outbound traffic to approved destinations and ports.

6. Audit Other Systems

- Search for signs of lateral movement (e.g., WMI, PsExec, RDP connections).
- Check logs on other endpoints for:
 - Failed logins
 - Script execution
 - Unusual outbound traffic

7. Restore and Patch

- Reimage the affected system if necessary.
- Re-enable and ensure the integrity of the Windows Update service (**wuauserv**).
- Apply the latest OS and software patches across all systems.

8. Document and Report

- Log this incident in your internal ticketing or SIEM system.
- Retain all relevant forensic data (event logs, file hashes, timestamps, IPs) for future reference or external reporting if required.

9. User Awareness & Training

- Inform the affected user(s) of the incident.
- Provide training on recognizing phishing and malicious script behavior.

Lessons learned and preventive measures

Lessons Learned

1. **Weak Endpoint Defenses Were Exploited**

- The unauthorized script (**hidden.vbs**) executed without being blocked, indicating gaps in endpoint protection or policy enforcement.

2. **Lack of Outbound Traffic Controls**

- Malicious connections to external IPs were not restricted, allowing potential data exfiltration or C2 communication.

3. Inadequate Credential Protection

- Repeated failed logins suggest accounts were susceptible to brute-force attacks, possibly lacking account lockout policies or MFA.

4. Security Service Tampering Was Undetected

- The termination of Windows Update service went unnoticed until post-incident review, highlighting a monitoring gap.

5. No Early Detection or Alerting

- The indicators (suspicious process, logins, service failures) weren't flagged by existing monitoring tools, delaying response.
-

Preventive Measures

1. Implement Endpoint Protection & EDR

- Deploy enterprise-grade **Endpoint Detection and Response (EDR)** solutions.
- Enable script-blocking policies for unauthorized **.vbs**, **.bat**, and **.ps1** file execution.

2. Restrict Outbound Network Access

- Enforce **egress filtering** to restrict outbound traffic to only necessary IPs and ports.
- Block known malicious IPs and monitor traffic anomalies.

3. Harden User Authentication

- Enable **Multi-Factor Authentication (MFA)** for all remote access and privileged accounts.
- Configure **account lockout thresholds** to block brute-force attempts.

4. Patch Management and Integrity Checks

- Enforce regular patching of all endpoints and servers.

- Monitor and alert on changes to key services (e.g., Windows Update, AV).



5. Centralized Log Management

- Aggregate logs into a **SIEM** for real-time correlation and alerting.
- Set alerts for:
 - Failed login attempts
 - Unexpected service terminations
 - Suspicious process executions



6. User Awareness and Phishing Defense

- Conduct periodic security training focused on recognizing malicious links, attachments, and script behavior.
- Test users with simulated phishing exercises.



7. Routine Threat Hunting and Audits

- Perform regular internal threat hunts for anomalies (e.g., hidden scheduled tasks, suspicious startup items).
- Audit firewall and endpoint configurations quarterly.