Investigating a Suspicious osk.exe Using Sysmon, Splunk, FortiGate UTM, Suricata, and OSINT

Overview

In this lab, I investigated an unexpected executable tied to a suspicious registry related finding. The objective was to confirm whether osk.exe was legitimate, identify where it executed from, scope network behavior, extract indicators, and validate the likely malware family using log evidence plus targeted OSINT.

SOC handoff summary

Classification: Security incident, suspected masquerading and malicious outbound activity
Severity: High
Confidence: High
Affected asset: we8105desk.waynecorpinc.local
User context: bob.smith
Internal IP: 192.168.250.100
Key artifacts: Non standard osk.exe execution path, high volume outbound connections, SHA256 hash, vendor labeling from VirusTotal and FortiGate
Primary IOCs
File path: C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming{35ACA89F-933F-6A5D-2776-A3589FB99832}\osk.exe
SHA256: 37397F8D8E4B3731749094D7B7CD2CF56CACB12DD69E0131F07DD78DFF6F262B
Network: destination ports 6892 and 80, 16384 unique destination IPs on port 6892

Environment and data sources

I worked from a lab host with Splunk as the SIEM and multiple security telemetry sources. The investigation used these datasets.

- Sysmon logs ingested into Splunk, Windows event XML
- FortiGate Unified Threat Management logs for web and threat categorization
- Suricata alerts for network detection context
- OSINT for binary validation and malware identification, VirusTotal

Investigation workflow

I used a fast triage flow. Establish a known good baseline, verify execution evidence, scope behavior, then cross validate findings across independent telemetry sources.

Step 1. OSINT baseline validation of osk.exe

osk.exe is associated with the Windows On Screen Keyboard feature. A legitimate osk.exe should normally exist at:
C:\Windows\System32\osk.exe

This provided a clean baseline. If osk.exe executed from a user profile or roaming directory, it would be immediately suspicious and consistent with masquerading.

Step 2. Confirm execution path using Sysmon in Splunk
I filtered to Sysmon events in Splunk and searched for osk.exe, then focused on Sysmon process creation telemetry to extract the exact execution path.
Key finding. The observed osk.exe was running from a user roaming directory, not from System32, which strongly indicates masquerading.
Suspicious full path identified
C:\Users\bob.smith.WAYNECORPINC\AppData\Roaming{35ACA89F-933F-6A5D-2776-A3589FB99832}\osk.exe

Step 3. Confirm the host, user, and internal source IP
After confirming the suspicious path, I tied execution to a specific host, user, and internal IP. This anchors the rest of the pivots and keeps the investigation reproducible.
Confirmed execution context
Host: we8105desk.waynecorpinc.local
Internal IP: 192.168.250.100
User: bob.smith

Step 4. Identify network behavior and scope of impact
Next, I moved from execution evidence to network behavior using Sysmon network activity and confirmed scope by counting unique destination IPs for the most active port.
Key network findings
Destination ports: 6892, 80
Unique destination IP addresses on port 6892: 16384
This level of outbound fan out is a major indicator of automation and suspicious activity. A legitimate accessibility tool would not typically generate outbound connections to thousands of unique internet hosts.

Step 5. Extract and validate the file hash
To support OSINT enrichment and malware identification, I extracted the SHA256 for the suspicious binary and validated formatting before using it externally.
Suspicious osk.exe SHA256
37397F8D8E4B3731749094D7B7CD2CF56CACB12DD69E0131F07DD78DFF6F262B

Step 6. OSINT enrichment with VirusTotal
Using the SHA256 hash, I searched VirusTotal and reviewed detection results to identify the likely malware family. The detection naming indicated Cerber.

Step 7. FortiGate UTM correlation for malware labeling

To cross validate with vendor classification from a separate telemetry source, I pivoted into FortiGate UTM logs for category and name mapping.

FortiGate results

Malware category: Botnet

Malware name: Cerber.Botnet

Step 8. Suricata alert validation for HTTP connection

Finally, I reviewed Suricata alerts to validate network detection context for the HTTP connection on destination port 80. This provided additional detection support that defenders can operationalize in a SOC workflow.

Outcome and determination

This investigation confirmed a masquerading binary. The executable name matched a legitimate Windows component, but the execution path proved it was not the legitimate System32 binary. Host telemetry and network behavior showed high volume outbound activity, and OSINT plus FortiGate threat labeling aligned on Cerber family naming, with FortiGate categorizing it as botnet activity. Based on the evidence, I treated this as a high severity security incident requiring containment and follow up scoping.

Recommended response actions, production safe guidance

Containment

- Isolate the host from the network pending triage completion
- Block the file hash and the suspicious roaming path execution pattern in endpoint controls where available
- Apply an egress control or temporary block for suspicious outbound patterns tied to this host, especially high fan out behavior

Eradication and recovery

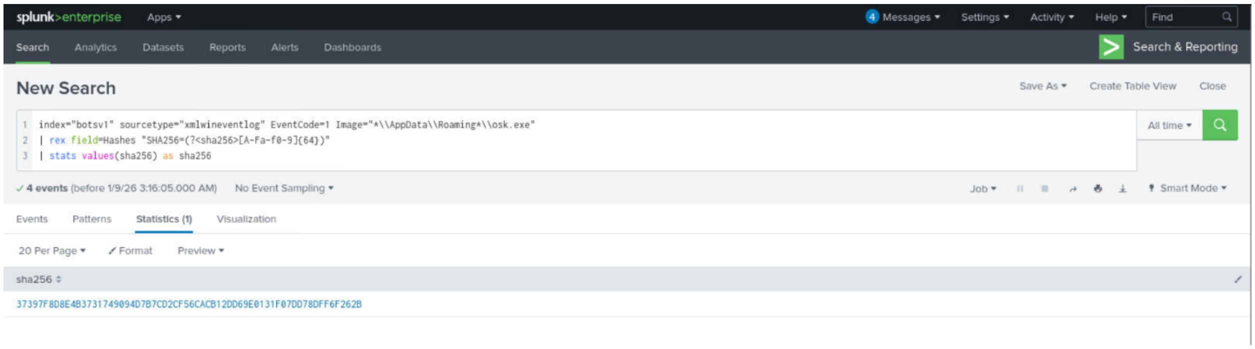
- Remove the malicious binary and any associated persistence mechanisms discovered during continued triage
- Reset credentials for the affected user if credential exposure is suspected
- Validate system integrity and reimage if policy and evidence warrant it

Detection and hunting

- Hunt across endpoints for execution of osk.exe outside C:\Windows\System32\osk.exe
- Hunt for the SHA256 across telemetry, plus the roaming GUID style path pattern
- Add monitoring for unusual outbound fan out on non standard ports, including counts of unique destinations per host over short windows

Skills demonstrated

- Baseline validation using OSINT for known good Windows binaries and expected file paths
- SIEM hunting using Sysmon telemetry to confirm execution and associated network activity
- Scoping impact using quantitative pivots, including unique destination IP counting
- IOC extraction and validation using SHA256 hashing for external enrichment
- Cross correlation across endpoint logs, firewall threat logs, and IDS alerts
- Evidence based malware identification using VirusTotal detection naming and FortiGate threat labeling.

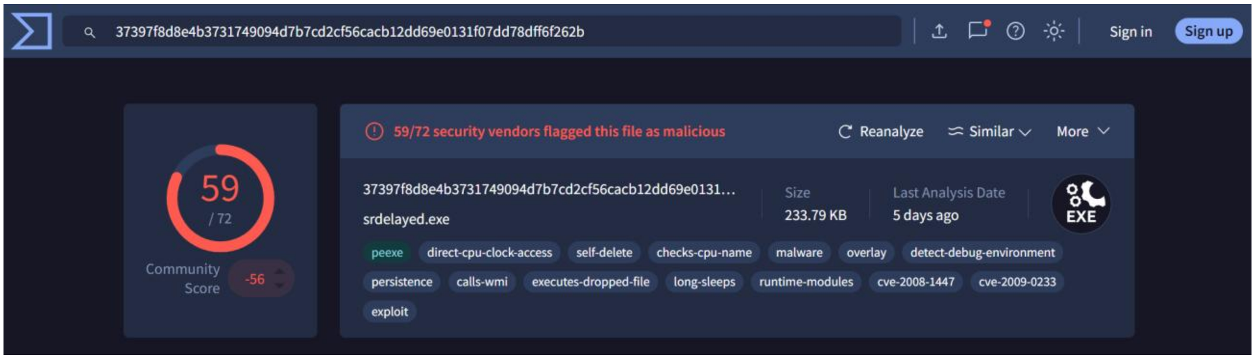


New Search

```
index="botsv1" sourcetype="xmlwineventlog" EventCode=1 Image="*\\AppData\\Roaming*\\osk.exe"
| rex field=Hashes "SHA256=(?<sha256>[A-Fa-f0-9]{64})"
| stats values(sha256) as sha256
```

✓ 4 events (before 1/9/26 3:16:05.000 AM) No Event Sampling ▾

sha256
37397F8D8E4B3731749094D7B7CD2CF56CACB12DD69E0131F07DD78DFF6F262B



37397f8d8e4b3731749094d7b7cd2cf56cacb12dd69e0131f07dd78dff6f262b

59 / 72

Community Score -56

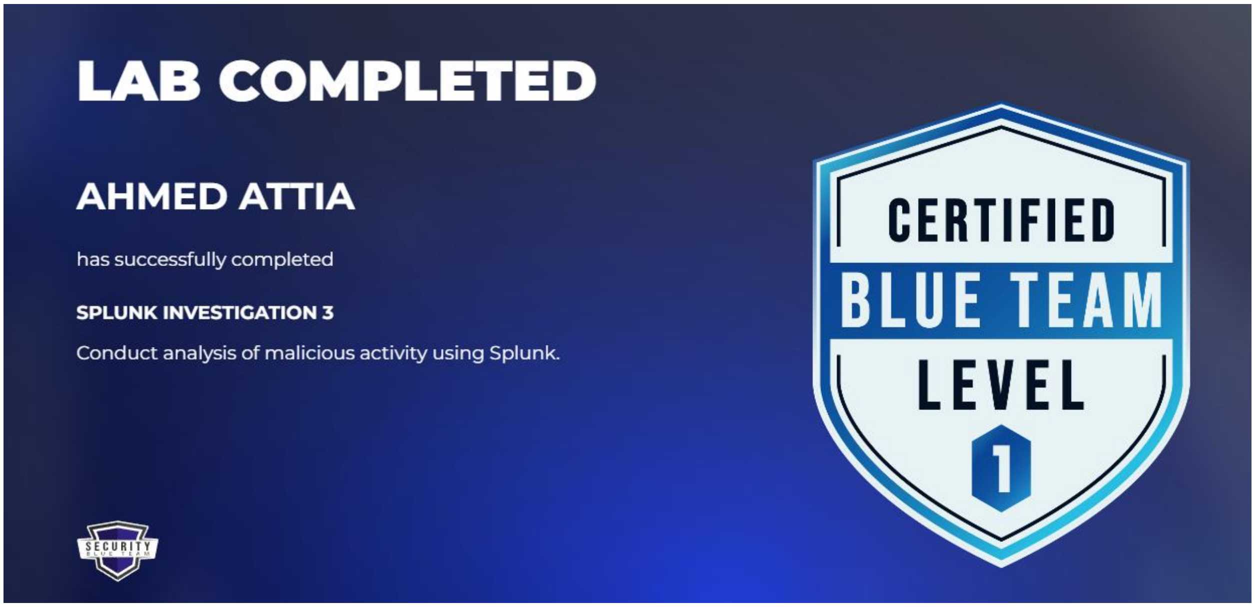
59/72 security vendors flagged this file as malicious

37397f8d8e4b3731749094d7b7cd2cf56cacb12dd69e0131...
srdelayed.exe

Size 233.79 KB

Last Analysis Date 5 days ago

peexe direct-cpu-clock-access self-delete checks-cpu-name malware overlay detect-debug-environment persistence calls-wmi executes-dropped-file long-sleeps runtime-modules cve-2008-1447 cve-2009-0233 exploit


CERTIFIED
BLUE TEAM
LEVEL
1
SECURITY BLUE TEAM

LAB COMPLETED

AHMED ATTIA

has successfully completed

SPLUNK INVESTIGATION 3

Conduct analysis of malicious activity using Splunk.