SOC189- VBScript Suspicious Behavior Detected

Contents

1. Incident Summary

- **Event ID:** 139
- **Date/Time:** April 20, 2023, 09:42 AM
- **Rule Name:** SOC189 - VBScript Suspicious Behavior Detected
- **Alert Type:** Malware
- **Severity Level:** Medium
- **Incident Responder:** Silas Gachie
- **MITRE ATT&CK Technique:**
  - T1547: Persistence - Boot or Logon Autostart Execution

---

2. Incident Description

- **Overview:**
  On April 20, 2023, at 09:42 AM, an alert was triggered by the SOC monitoring system. The rule SOC189 flagged suspicious behavior linked to a VBScript, which has been associated with malware execution or persistence mechanisms. This incident correlates with MITRE ATT&CK technique **T1547**—specifically focusing on **Boot or Logon Autostart Execution** used to establish persistence on the affected system.
- **Affected System(s):**
  - Hostname: David
  - IP Address: 172.16.17.31
  - Operating System: Windows 10

---

3. Investigation Summary

- **Detection Method:**
- **Behavior Details:**
  - Path: "C:\Windows\System32\WScript.exe" "C:\Users\LetsDefend\Downloads\Purchase_Order\Purchase_Order.xls.vbs"
  - Actions: Contacts 2 domains and 1 host, downloads malware on the system and installs hooking the running process at startup
- **Indicators of Compromise (IOCs):**

  103.47.144.80
  1c546a6548beda639640ebfbb52abd5f6013c33500172cfccf0e8716c96bb196

chongme.33.publicvm.com

---

4. Mitigation Steps

- **Immediate Actions Taken:**
  - Suspicious script terminated.
  - Registry keys reverted.
  - System isolated from the network.
- **Next Steps:**
  - Full system malware scan.
  - Analyze the script in a sandbox.
  - User awareness training.

---

5. Recommendations

- Disable unnecessary VBScript execution.
- Monitor system startup and registry modifications.
- Regularly update and patch systems.
- Implement phishing prevention measures.

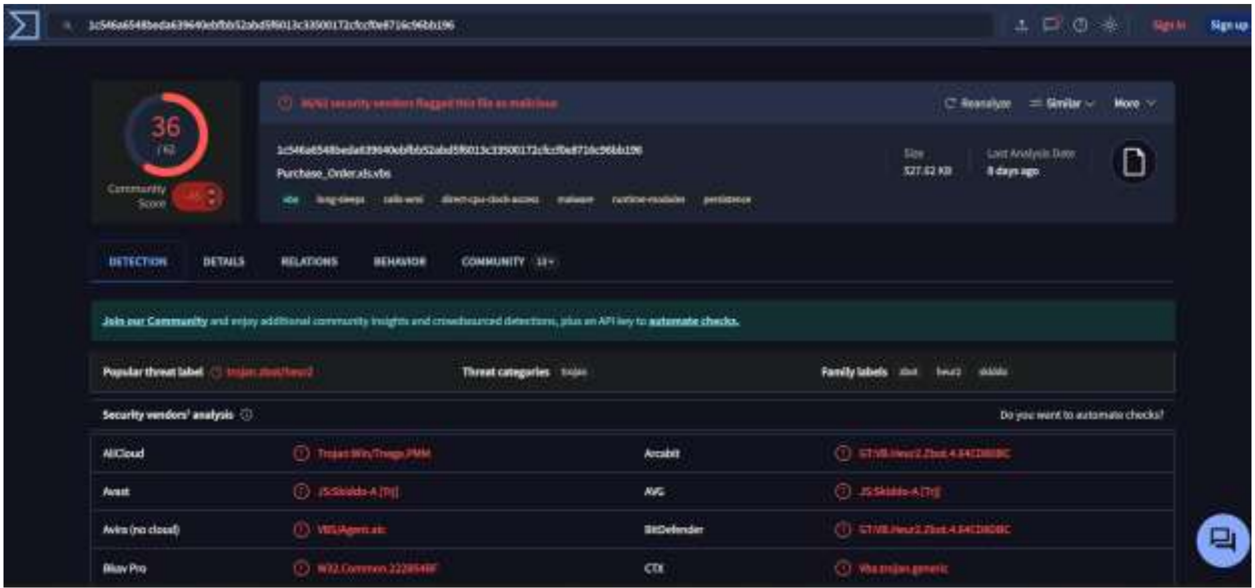
---

6. Conclusion

- **Status:** Resolved
- **Follow-up Actions:** Incident investigation will continue to confirm root cause and determine if any additional systems were compromised. Further analysis of the malicious script in a controlled environment is recommended.

---

7. Attachments



1c546a6548beda639640ebfbb52abd5f6013c33500172cfccf0e8716c96bb196

36 / 62

Community Score

36/62 security vendors flagged this file as malicious

Reanalyze · Similar · More

1c546a6548beda639640ebfbb52abd5f6013c33500172cfccf0e8716c96bb196

Purchase_Order.xls.vbs

vbs · long-sleeps · calls-wmi · direct-cpu-clock-access · malware · runtime-modules · persistence

Size: 527.62 KB

Last Analysis Date: 8 days ago

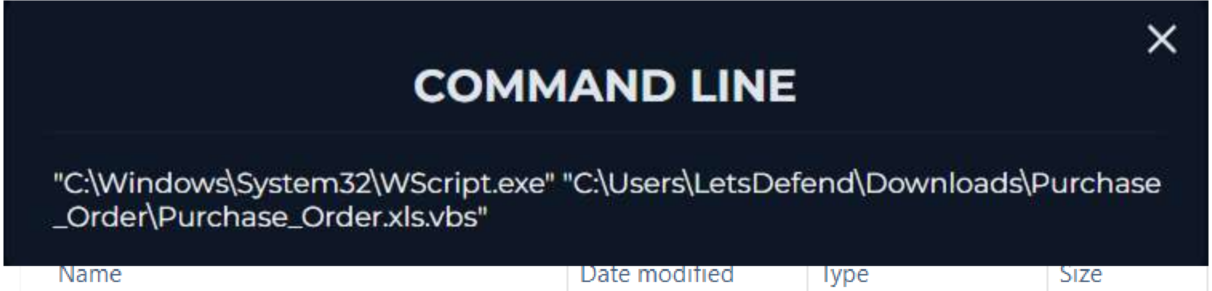
DETECTION · DETAILS · RELATIONS · BEHAVIOR · COMMUNITY 13+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.zbot/heur2 · Threat categories: trojan · Family labels: zbot · heur2 · skiddo

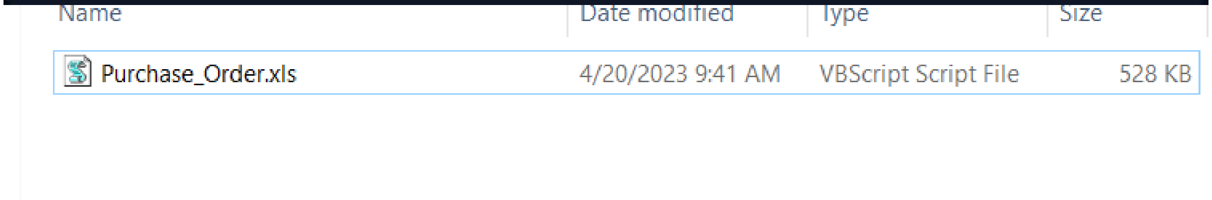
Security vendors' analysis · Do you want to automate checks?

AliCloud	Trojan:Win/Tnega.PMM	Arcabit	GT:VB.Heur2.Zbot.4.E4CD8DBC
Avast	JS:Skiddo-A [Trj]	AVG	JS:Skiddo-A [Trj]
Avira (no cloud)	VBS/Agent.aic	BitDefender	GT:VB.Heur2.Zbot.4.E4CD8DBC
Bkav Pro	W32.Common.22285A8F	CTX	Vbs.trojan.generic

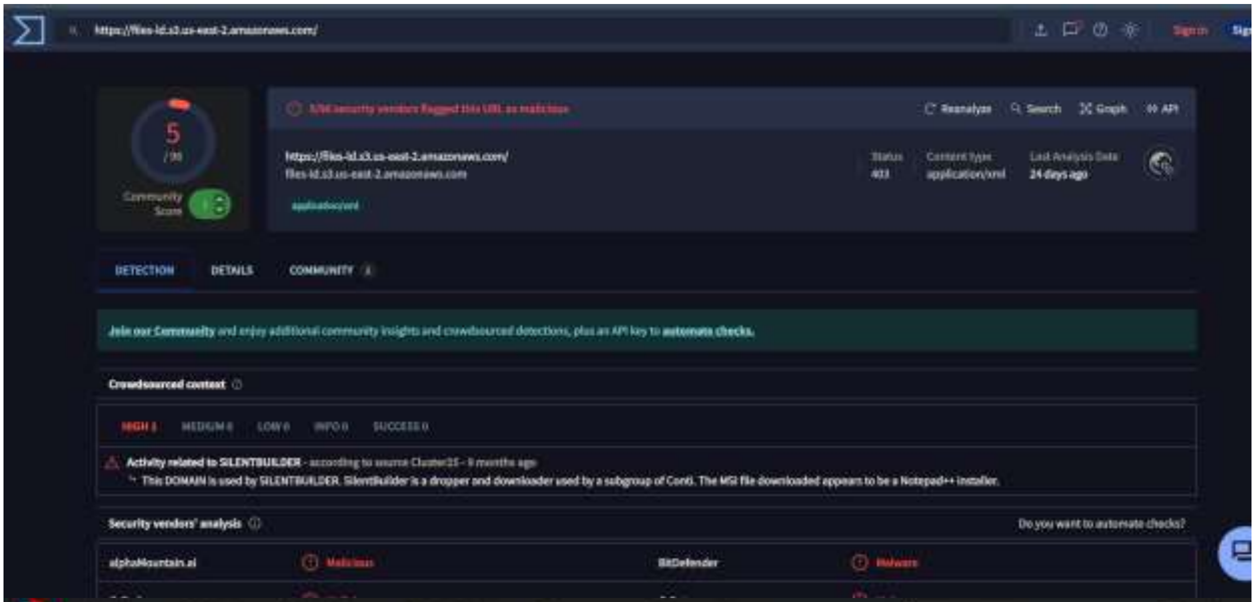


COMMAND LINE

```
"C:\Windows\System32\WScript.exe" "C:\Users\LetsDefend\Downloads\Purchase_Order\Purchase_Order.xls.vbs"
```



Name	Date modified	Type	Size
Purchase_Order.xls	4/20/2023 9:41 AM	VBScript Script File	528 KB



5/96 security vendors flagged this URL as malicious

https://files-ld.s3.us-east-2.amazonaws.com/
files-ld.s3.us-east-2.amazonaws.com
application/xml

Status: 403
Content type: application/xml
Last Analysis Date: 24 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Crowdsourced context

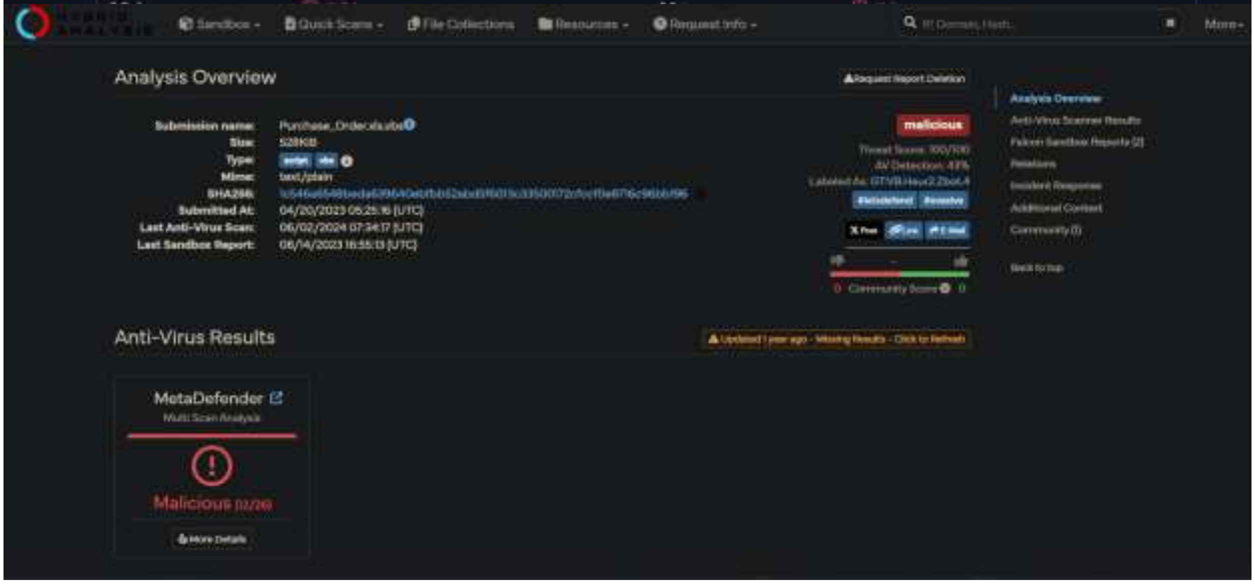
HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

Activity related to SILENTBUILDER - according to source Cluster25 - 9 months ago
This DOMAIN is used by SILENTBUILDER. SilentBuilder is a dropper and downloader used by a subgroup of Conti. The MSI file downloaded appears to be a Notepad++ installer.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Malware



Analysis Overview

Submission name:	Purchase_Order.xls.vbs
Size:	528KiB
Type:	script vbs
Mime:	text/plain
SHA256:	[illegible]
Submitted At:	04/20/2023 06:25:16 (UTC)
Last Anti-Virus Scan:	06/02/2024 07:34:17 (UTC)
Last Sandbox Report:	06/14/2023 16:55:13 (UTC)

malicious
Threat Score: 100/100
AV Detection: 43%
Labeled As: GT:VB.Heur2.Zbot.4
#bitdefender #evasive

0 Community Score 0

Analysis Overview
Anti-Virus Scanner Results
Falcon Sandbox Reports (2)
Relations
Incident Response
Additional Context
Community (0)
Back to top

Anti-Virus Results

Updated 1 year ago - Missing Results - Click to Refresh

MetaDefender
Multi Scan Analysis
Malicious 12/26