Malware Download and Incident Response Plan

Talal Ahmed | Team Lambda

This report outlines the end-to-end process of setting up a malware analysis environment, executing a Zeus malware sample, and developing a subsequent Incident Response (IR) plan based on industry standards.

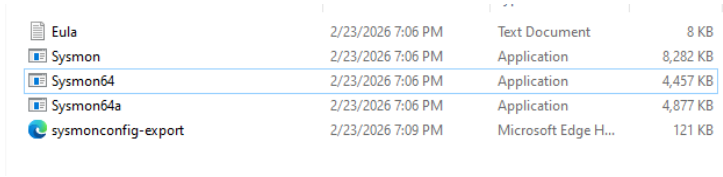
Environment Setup & Malware Download

The objective was to create a controlled environment to observe malware behavior while maintaining network-level and host-level monitoring.

Preparation Steps

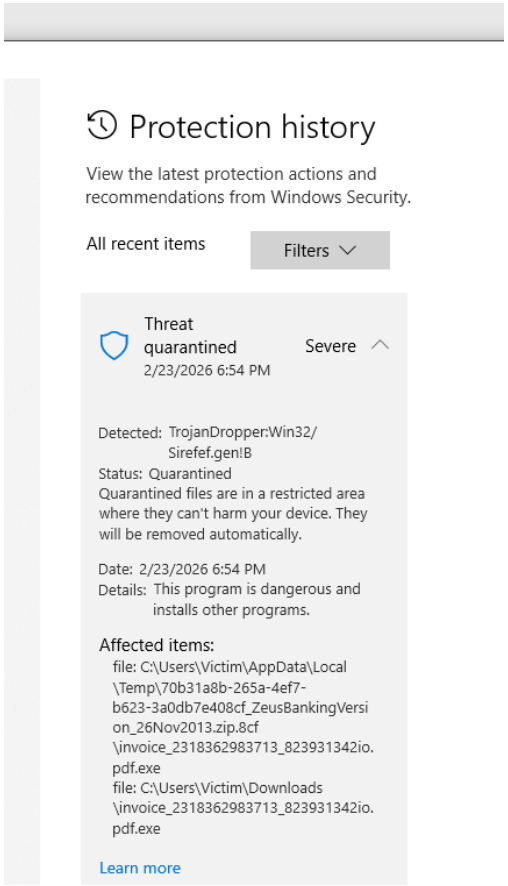
- **Virtual Machine (VM) Deployment**: A Windows 10 VM was provisioned as the target "victim" machine.
- **Network Security**: The VM was placed behind an active pfSense firewall to monitor and log all outbound/inbound traffic.
- **Wazuh Agent Installation**: The Wazuh agent was installed via PowerShell and pointed to the Wazuh Manager at 192.168.164.2 to ensure real-time log collection.
- **Sysmon Integration**: Sysmon was installed and configured using a customized config (e.g., SwiftOnSecurity) to provide deep visibility into process creations and network connections.

```
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.2-1.msi -OutFile
$env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.164.2' WAZUH_AGENT_NAME='w10'
PS C:\Windows\system32> NET START wazuh
The Wazuh service is starting.
The Wazuh service was started successfully.
```

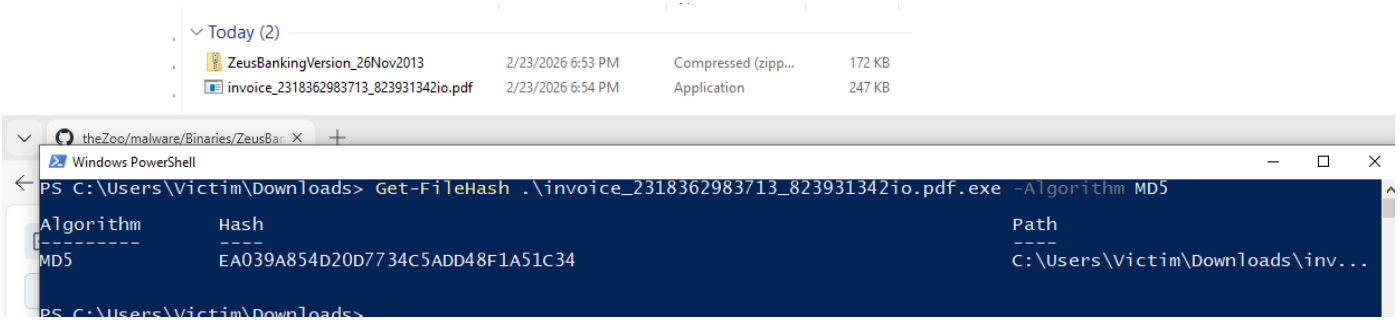


Malware Acquisition

- **Source**: The malware was sourced from "The Zoo" (a reputable malware repository).
- **Defender Configuration**: Initial download attempts were automatically blocked and quarantined by Windows Defender, which identified the file as TrojanDropper:Win32/Sirefef.gen!B. To proceed with the analysis, Windows Defender real-time protection was temporarily disabled.



- **File Details**:
  - **Name**: invoice_2318362983713_823931342io.pdf.exe
  - **MD5 Hash**: EA039A854D20B7734C5ADD48F1A51C34



Detection and Observation

Once executed, the malware's activity was captured across multiple monitoring platforms.

pfSense Monitoring

The pfSense firewall logged several "Deny" actions (marked with a red **X**) as the malware attempted to reach external command-and-control (C2) servers.

- **Target IPs**: 2.16.158.58 and 2.16.158.81 on port **443**.
- **Protocol**: TCP.

Last 500 Firewall Log Entries. (Maximum 500) Pause

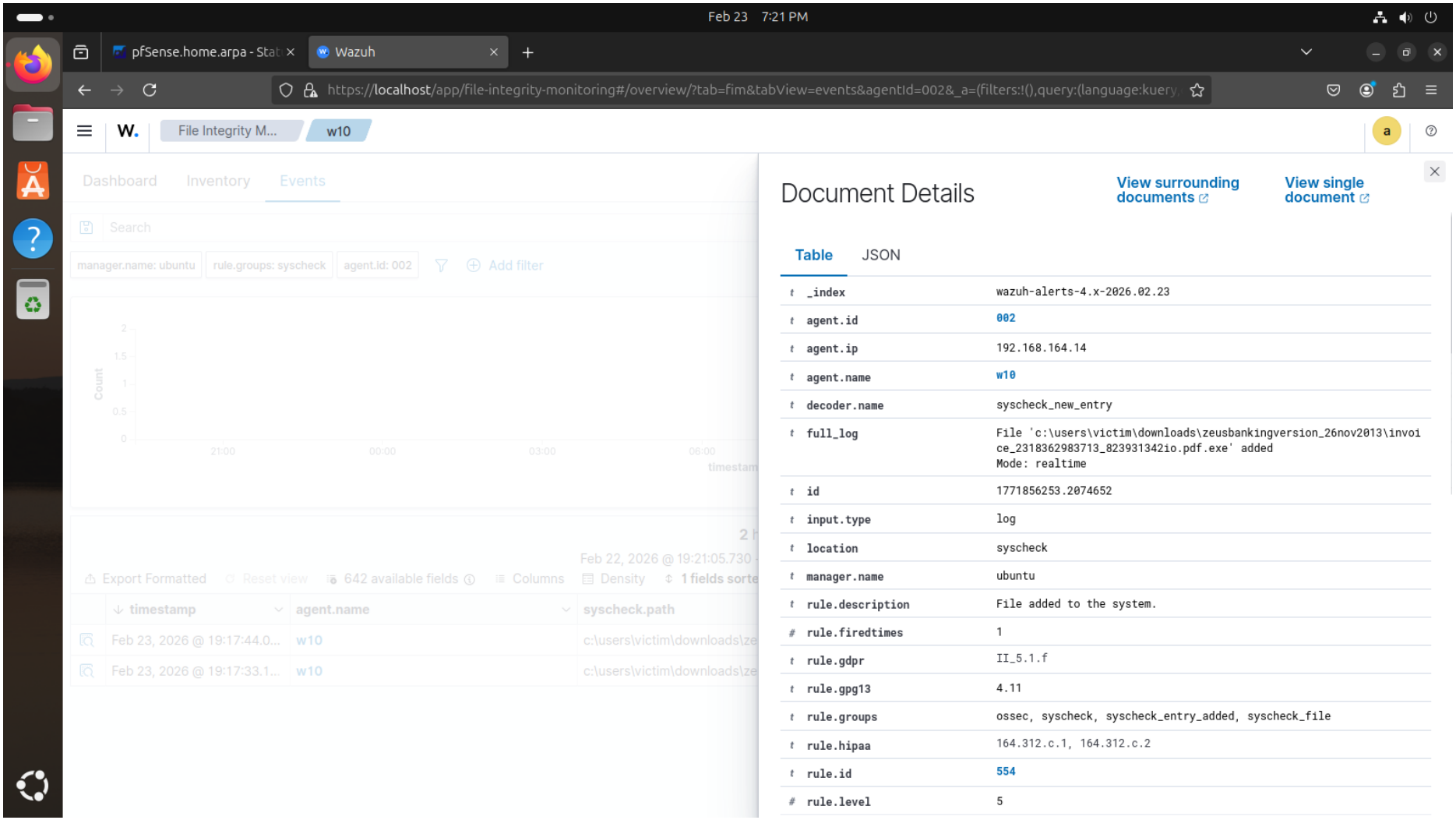
Action	Time	Interface	Source	Destination	Protocol
✕	Feb 23 19:41:36	WAN	192.168.170.1:138	192.168.170.255:138	UDP
✕	Feb 23 19:33:18	LAN	192.168.164.14:49927	2.16.158.58:443	TCP:RA
✕	Feb 23 19:33:04	LAN	192.168.164.14:49927	2.16.158.58:443	TCP:FA
✕	Feb 23 19:32:57	LAN	192.168.164.14:49927	2.16.158.58:443	TCP:FA
✕	Feb 23 19:32:53	LAN	192.168.164.14:49927	2.16.158.58:443	TCP:FA
✕	Feb 23 19:32:51	LAN	192.168.164.14:49927	2.16.158.58:443	TCP:FA
✕	Feb 23 19:32:50	LAN	192.168.164.14:49927	2.16.158.58:443	TCP:FA
✕	Feb 23 19:32:50	LAN	192.168.164.14:49927	2.16.158.58:443	TCP:FA
✕	Feb 23 19:29:35	WAN	192.168.170.1:138	192.168.170.255:138	UDP
✕	Feb 23 19:17:34	WAN	192.168.170.1:138	192.168.170.255:138	UDP
✕	Feb 23 19:10:35	LAN	192.168.164.14:49709	2.16.158.81:443	TCP:RA
✕	Feb 23 19:10:28	LAN	192.168.164.14:49687	2.16.158.58:443	TCP:RA
✕	Feb 23 19:10:22	LAN	192.168.164.14:49709	2.16.158.81:443	TCP:FA
✕	Feb 23 19:10:19	LAN	192.168.164.14:49687	2.16.158.58:443	TCP:FA
✕	Feb 23 19:10:16	LAN	192.168.164.14:49709	2.16.158.81:443	TCP:FA
✕	Feb 23 19:10:14	LAN	192.168.164.14:49687	2.16.158.58:443	TCP:FA

Wazuh & Sysmon Analysis

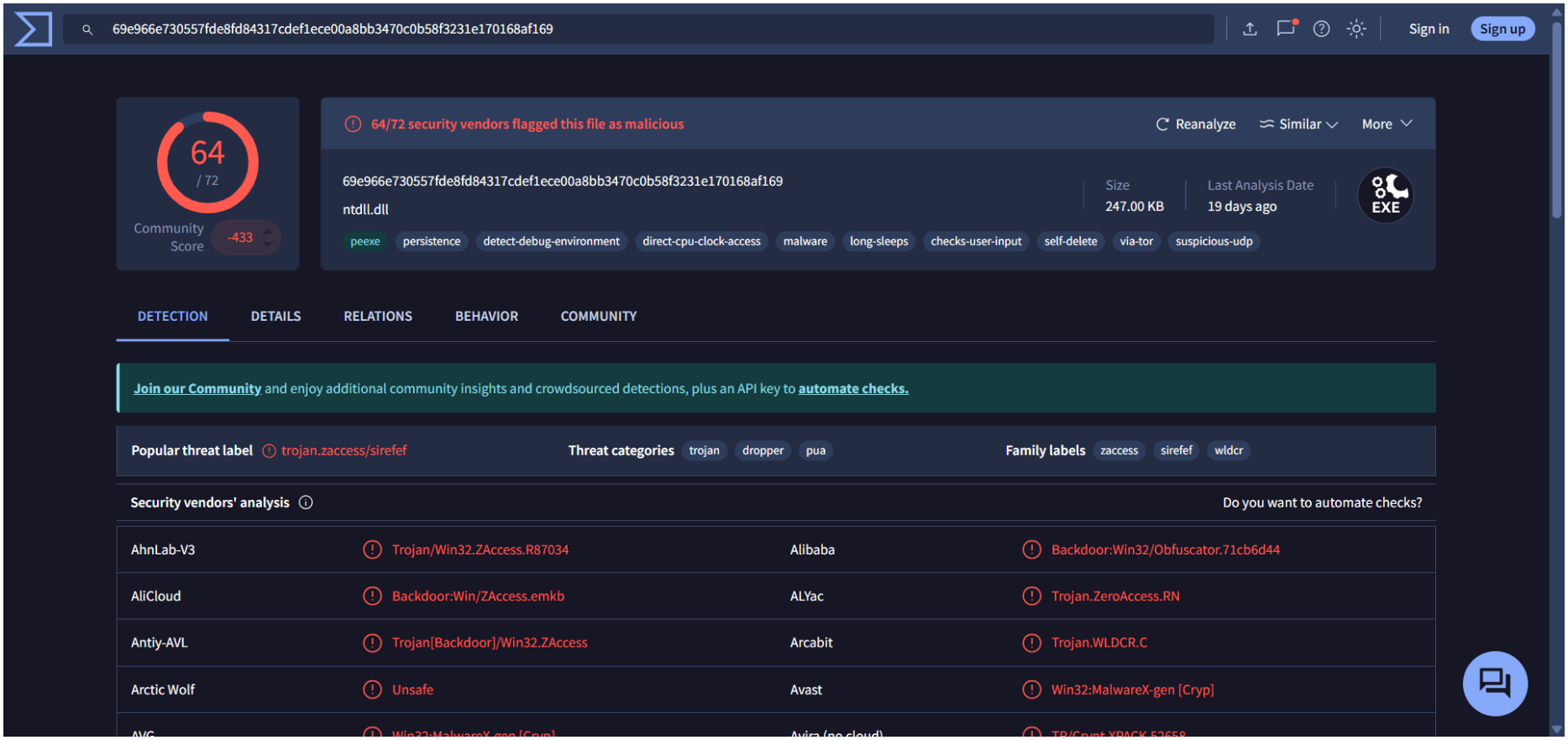
Wazuh's dashboard highlighted several critical Indicators of Attack (IOAs):

- **Rule 554**: "File added to the system" flagged the initial placement of the executable.
- **Rule 92213**: "Executable file dropped in folder commonly used by malware".
- **Rule 92052**: "Windows command prompt started by an abnormal process," indicating the malware was attempting to execute shell commands.

timestamp	agent.name	rule.description	rule.level	rule.id
Feb 23, 2026 @ 19:17:44.0...	w10	File deleted.	7	553
Feb 23, 2026 @ 19:17:43.3...	w10	Windows command prompt started by an abnormal process	4	92052
Feb 23, 2026 @ 19:17:40.9...	w10	Executable file dropped in folder commonly used by malware	15	92213
Feb 23, 2026 @ 19:17:40.9...	w10	Executable file dropped in folder commonly used by malware	15	92213
Feb 23, 2026 @ 19:17:33.1...	w10	File added to the system.	5	554



Looking up the hash on VirusTotal yields this result.


69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
Sign in
Sign up
64
/ 72
Community Score
-433
64/72 security vendors flagged this file as malicious
Reanalyze
Similar
More
69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
ntdll.dll
Size
247.00 KB
Last Analysis Date
19 days ago
EXE
peexe
persistence
detect-debug-environment
direct-cpu-clock-access
malware
long-sleeps
checks-user-input
self-delete
via-tor
suspicious-udp
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label
trojan.zaccess/sirefef
Threat categories
trojan
dropper
pua
Family labels
zaccess
sirefef
wldcr
Security vendors' analysis
Do you want to automate checks?
AhnLab-V3
Trojan/Win32.ZAccess.R87034
Alibaba
Backdoor:Win32/Obfuscator.71cb6d44
AliCloud
Backdoor:Win/ZAccess.emkb
ALYac
Trojan.ZeroAccess.RN
Antiy-AVL
Trojan[Backdoor]/Win32.ZAccess
Arcabit
Trojan.WLDCR.C
Arctic Wolf
Unsafe
Avast
Win32:MalwareX-gen [Cryp]

Incident Response Plan

Based on the observed Zeus variant, the following response plan is established:

1. Preparation

This phase focuses on the tools and configurations established before the incident occurred to ensure visibility.

- **Endpoint Monitoring:** Deployment of **Wazuh Agent** and **Sysmon** on the Windows 10 VM to capture process-level events.
- **Network Defense:** Configuration of a **pfSense firewall** to log and filter outbound traffic from the analysis VM.
- **Baseline Establishment:** Creating a known-good system state to compare against during analysis.

2. Detection and Analysis

This phase involves identifying the signs of an incident and determining its scope.

- **Alert Identification: Wazuh** triggered high-severity alerts for "Executable file dropped in folder commonly used by malware" (Rule 92213) and "Windows command prompt started by an abnormal process" (Rule 92052).
- **Log Correlation:** Correlation of **pfSense** logs showing blocked outbound TCP/443 traffic to IPs 2.16.158.58 and 2.16.158.81, indicating C2 (Command and Control) activity.
- **Malware Validation:** Validation of the file invoice_...pdf.exe via **MD5 hash** (EA039A854D20B7734C5ADD48F1A51C34) against threat intelligence, confirming it as **TrojanDropper:Win32/Sirefef.gen!B**.

3. Containment, Eradication, and Recovery

This phase focuses on stopping the spread, removing the threat, and restoring services.

- **Containment:**

  - **Short-term:** Isolation of the infected host (192.168.164.14) from the network via hypervisor settings to prevent further C2 communication.
  - **Long-term:** Implementation of firewall blocks on **pfSense** for the identified malicious IPs.
- **Eradication:**
  - **File Removal:** Deletion of the primary executable from the Downloads folder and cleanup of temporary files located in AppData\Local\Temp.
  - **Persistence Cleanup:** Scanning the registry for unauthorized run keys associated with the **Sirefef** variant.
- **Recovery:**
  - **Restoration:** Reverting the VM to a clean snapshot taken prior to the infection on Feb 23, 2026.
  - **Verification:** Performing follow-up scans with **Windows Defender** (reenabled) and monitoring **Wazuh** for recurring Rule 92052 alerts.

4. Post-Incident Activity

This phase focuses on improving the security posture to prevent future occurrences.

- **Incident Documentation:** Compiling all IOCs (IPs, MD5 hashes) and IOAs (abnormal process spawning) into a final report for the SOC team.
- **Policy Review:** Recommending a policy to block executable files from running directly from user-writable directories like Downloads.
- **Detection Improvement:** Creating custom **Wazuh** rules to specifically alert on the C2 IPs identified during this incident.

Conclusion

The successful execution and analysis of the **Zeus** malware sample within this controlled environment demonstrated the critical importance of a layered defense strategy. By integrating **pfSense** at the network perimeter and **Wazuh** with **Sysmon** at the endpoint level, we were able to achieve full visibility into the attack lifecycle.

Key takeaways from this exercise include:

- **Layered Visibility:** While **Windows Defender** initially blocked the threat, disabling it allowed us to see how secondary layers like **Wazuh** FIM and **Sysmon** process monitoring accurately flag malicious behaviors such as abnormal CMD execution and unauthorized file creation.
- **Network-Level Egress Control:** The **pfSense** logs proved vital in identifying blocked Command and Control (C2) attempts to external IPs (2.16.158.58), highlighting the role of firewalls in preventing data exfiltration even when a host is compromised.
- **Structured Response:** The development of the **Incident Response Plan** ensures that future detections follow a standardized process of containment, eradication, and recovery, ultimately reducing the organization's mean time to respond (MTTR).

This task confirms that through proper configuration and monitoring, security teams can effectively detect and neutralize sophisticated banking trojans before they achieve their objectives.