NAME: Rishita Shrimali INTERN-ID:292

Subject: Structured TTP Analysis for n.IGENERIC

# 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 potentially harmful malware identified as n.IGENERIC. 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 follows a logical attack chain from initial compromise to command and control communication, 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.  
  
The n.IGENERIC malware family often relies on deceptive methods to trick users into running the malicious payload. A common initial access vector is phishing emails carrying infected attachments.

Technique: T1566.001 - Phishing: Spearphishing Attachment

Procedure: The attacker crafts a targeted phishing email, disguising the malware as a legitimate file (e.g., 'ProjectUpdate\_2025.pdf.exe'). The file is disguised with a PDF icon to mislead users. When the user downloads and opens the file, the malware is introduced into the system.

Detection & Mitigation:  
• Monitor email gateways for suspicious attachments with double extensions.  
• Train employees to recognize phishing attempts.  
• Enable antivirus scanning of email attachments.

# 3. Tactic: Execution (TA0002)

Goal: To execute the malware payload on the victim machine.  
  
Technique 1: T1204.002 - User Execution: Malicious File  
The user is tricked into executing the n.IGENERIC file manually.  
  
Technique 2: T1059.001 - Command and Scripting Interpreter: PowerShell  
The malware may use PowerShell scripts to download additional payloads from attacker-controlled servers.

Detection & Mitigation:  
• Enable script block logging in PowerShell.  
• Restrict execution policies to signed scripts only.  
• Monitor for suspicious child processes spawned from email clients.

# 4. Tactic: Persistence (TA0003)

Goal: To ensure malware survives reboots and maintains control of the victim system.  
  
Technique: T1547.001 - Registry Run Keys / Startup Folder  
Procedure: The malware creates a registry entry or drops a copy of itself in the startup folder to re-execute on system boot.

Detection & Mitigation:  
• Monitor registry locations for unexpected entries.  
• Use Endpoint Detection and Response (EDR) solutions to alert on persistence attempts.  
• Limit user permissions to modify startup registry keys.

# 5. Tactic: Command and Control (TA0011)

Goal: To establish communication with the attacker's server for data exfiltration and instructions.  
  
Technique: T1071.001 - Application Layer Protocol: Web Protocols  
Procedure: The malware periodically sends HTTP/HTTPS requests to the Command and Control (C2) server to receive commands and exfiltrate stolen data.

Detection & Mitigation:  
• Monitor outbound traffic for beaconing behavior.  
• Use DNS and IP reputation services to block malicious domains.  
• Implement firewall rules to restrict unauthorized data transfer.

# 6. Summary of TTP Flow

|  |
| --- |
| Step Tactic Technique ID Description 1 Initial Access T1566.001 Phishing email with malicious executable attachment. 2 Execution T1204.002 User double-clicks the file, initiating the attack. 3 Execution T1059.001 Malware uses PowerShell to fetch additional payload. 4 Persistence T1547.001 Registry key or startup folder entry created. 5 Command & Control T1071.001 Malware communicates with remote server for instructions. |

# Appendix: Sample VirusTotal Analysis

File: ProjectUpdate\_2025.pdf.exe Scan Date: 2025-08-06 20:00 UTC  
  
Hashes:  
• MD5: a7d8cd98f00b204e9800998ecf8427e  
• SHA-1: ab39a3ee5e6b4b0d3255bfef95601890afd80709  
• SHA-256: 9a793335f52636a95369c3a39662c5141f492d6b966a6b7e492bccb907126xyz  
  
Detection:  
• Ratio: 58 / 70 (83% of engines detected this file as malicious)  
• Selected Vendor Detections:  
 - Microsoft: Trojan:Win32/n.IGENERIC  
 - Kaspersky: Trojan.Win32.Generic  
 - McAfee: Artemis!n.IGENERIC  
 - Sophos: Troj/n.IGEN-A  
  
Behavioral Analysis Summary (Sandbox):  
• Persistence: Creates a registry key to execute on startup.  
• Network: Connects to attacker-controlled C2 server over HTTP.  
• Process Activity: Spawns hidden PowerShell processes.  
• File System: Attempts to read and modify sensitive user files.

