Forensic Analysis of an Intrusion

Project Type: DFIR / Incident Investigation

Prepared by: Niknaz Sadehvandi
Role: Founder & Cybersecurity Consultant
Organization: NS Cybersecurity
Date: December 2022

Objective

The objective of this project was to perform a forensic investigation of a simulated system intrusion to identify indicators of compromise, persistence mechanisms, and evidence of data exfiltration. The assessment focused on reconstructing attacker activity through log analysis and Windows artifact examination to support incident response and remediation decision-making.

Tools & Technologies

- Windows Operating System
- IIS Web Server Logs
- Windows Event Logs
- Autoruns (Sysinternals)
- File System Analysis
- Scheduled Task Inspection
- DFIR Investigation Methodology

Technical Steps Performed

1. Log Review & Initial Triage

- Collected and reviewed IIS web server logs to identify abnormal access patterns.
- Examined timestamps, request paths, and client activity associated with suspicious behavior.

2. Persistence Mechanism Analysis

- Inspected Windows startup folders and autorun locations using Autoruns.
- Identified unauthorized startup entries indicating persistence attempts.

3. Scheduled Task Investigation

- Reviewed scheduled tasks for abnormal or unauthorized execution.
- Correlated task execution with observed log activity and file creation times.

4. Exfiltration Evidence Review

- Analyzed logs and system artifacts for indicators of outbound data transfer.
- Identified suspicious network activity consistent with data exfiltration behavior.

5. Timeline Reconstruction

- Correlated logs, persistence artifacts, and execution events.
- Reconstructed an intrusion timeline detailing attacker actions and system impact.

Findings

- IIS logs revealed abnormal access patterns indicative of malicious activity.
- Persistence mechanisms were identified via unauthorized startup artifacts.
- Scheduled tasks were leveraged to maintain attacker access.
- Evidence supported outbound data exfiltration attempts.
- Multiple artifacts corroborated a confirmed system compromise.

Outcome

- Successfully reconstructed a timeline of the simulated intrusion.
- Confirmed compromise involving persistence and data exfiltration techniques.
- Produced DFIR-ready documentation suitable for incident escalation and remediation.
- Demonstrated practical forensic investigation skills aligned with real-world DFIR workflows.

Evidence

- Forensic screenshots and artifact views
- Log excerpts supporting intrusion activity
- Full investigation report

PDF Name:
Digital_Forensics_Project3_Forensic_Analysis_of_an_Intrusion.pdf

Portfolio Status

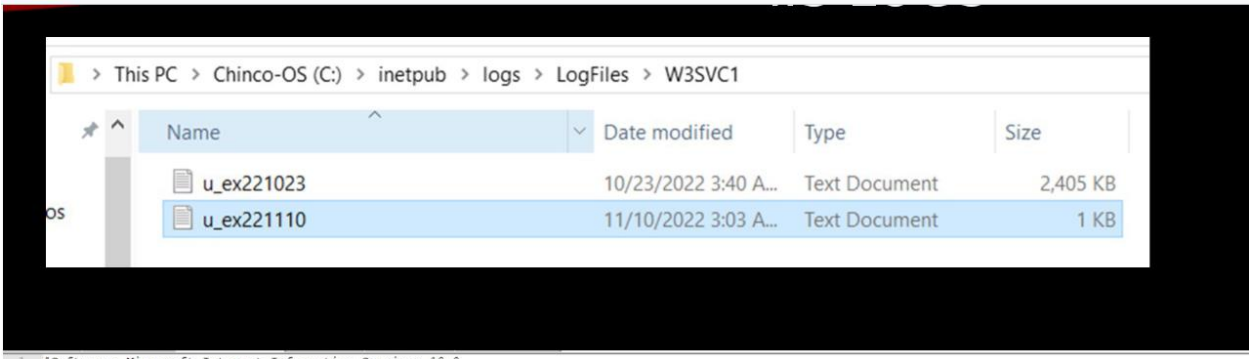
Project Status: Completed

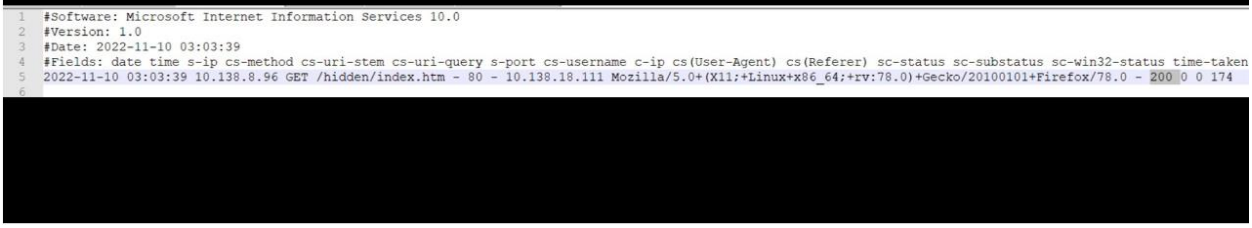
Evidence:

- IIS log analysis
- Startup and scheduled task artifacts
- Timeline reconstruction documentation

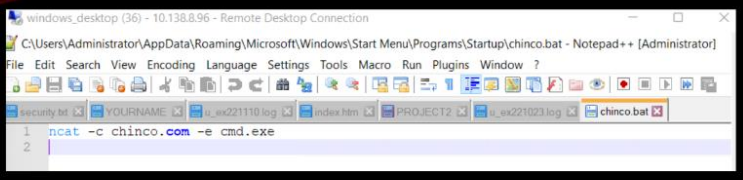
LOGS

- During the investigation what was found in the logs.

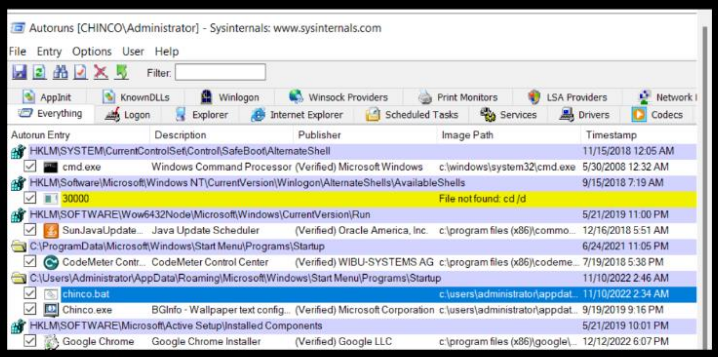




AUTORUNS AND/OR THE STARTUP FOLDER

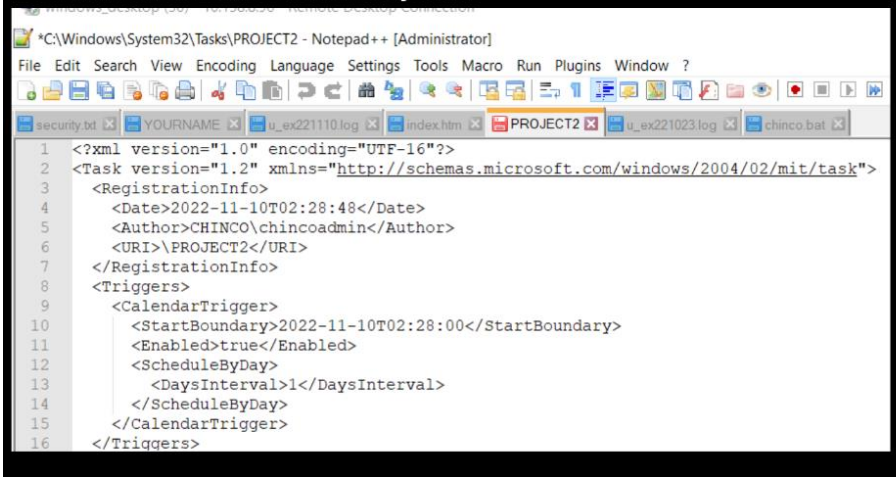


- Where is the folder located?



SCHEDULED TASKS

- What is a scheduled task? (project 2)
- Where is the folder located?
- What does the Task likely do?



THE GOLDEN NUGGET - EXFILTRATION