Malware Analysis Report: INFO-Y-119

Detailed Investigation of sample_jan25.exe

Luca Volonterio

Brussels, January 24, 2025

1 Executive Summary

The analyzed sample, `sample_jan25.exe`, is a sophisticated backdoor designed for Windows XP environments. It utilizes multi-threading to separate installation, persistence, and Command and Control (CnC) communication tasks. Key features include a time-dependent Domain Generation Algorithm (DGA), polymorphic filename generation, and a hidden reverse shell.

2 Infection Indicators (IoCs)

2.1 Mutex and Persistence Flags

The malware uses a mutex to prevent multiple concurrent infections on the same host.

- **Full Name:** `\BaseNamedObjects\ShimCacheMutex`.
- **IoC Suitability:** Yes, this is a behavioral host-based IoC.
- **Explanation:** While it can be used to identify an active infection, analysts should note that malware often uses legitimate-sounding names to blend in with system operations.

2.2 Registry Indicators

The malware creates a dynamic and a static registry entry.

- **Dynamic Key:** Based on the computer name retrieved via `GetComputerNameA`, the malware generates a key following the pattern: `SOFTWARE\SysInternals%d\Snapshot%03d`. This is achieved by hashing the computer name into a seed used in a formatted string.
- **Persistence Value:** It creates the value `SGC07` under `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`.
- **IoC Suitability:** The `SGC07` value is a clear indicator of compromise as it is non-standard and persistent.

2.3 File System Indicators

- **Full Path:** the file is dropped in `C:\DocumentsandSettings\IEUser\LocalSettings\ApplicationData\SecurityUtility.exe`
- **Explanation:** The filename is generated by a function that randomly selects ”Professional” keywords (e.g., Security, Utility, Service) to mimic legitimate software.

3 Persistence Mechanisms

The malware ensures survival after reboot through two primary steps:

- **Self-Replication:** It copies itself from the initial path to the Application Data folder using CopyFileA.
- **Startup Execution:** It registers the copied executable in the Run registry key. This mechanism allows the malware to launch automatically upon user login.

4 Command and Control (CnC) Channel

4.1 Domain Generation Algorithm (DGA)

Analysis of the network thread reveals a DGA that selects domains based on the system month.

- **Seeding:** It calls GetSystemTime and applies a mask (wMonth & 3) to choose one of four encrypted seeds stored at 0x00409008.
- **Decryption:** The seeds are decrypted using a cyclic XOR algorithm (FUN_004021f0) with a static key located at 0x0040a044.
- **Identified Hostname:** For the current period, the resolved hostname is cloud.cylab.be.

4.2 Network Communication

The malware initializes the network subsystem using WSAStartup (version 2.2). After DNS resolution, it sends a ”welcome message” to the CnC server to establish the session.

5 Action on Target

5.1 Capabilities

The primary capability is providing the attacker with a fully interactive remote shell on the victim machine.

5.2 Implementation

The malware implements a reverse shell by:

1. Creating two anonymous pipes via CreatePipe.
2. Spawning a hidden cmd.exe process with its hStdInput, hStdOutput, and hStdError redirected to these pipes.
3. Bridging the pipes with the network socket: data received from the CnC is written to the command input, and the output of the command is read from the pipe and sent back to the CnC via send.

6 Conclusion

The sample sample_jan25.exe represents a classic persistent backdoor with evasion techniques such as DGA and randomized naming. Its ability to provide a hidden interactive shell makes it a high-risk threat to system integrity and data confidentiality.