GitHub - francisck/DanderSpritz_docs: The goal of this project is to examine, reverse, and document the different modules available in the Equation Group's DanderSpritz post-exploitation framework leaked by the ShadowBrokers

By francisck

Archived: 2026-04-05 14:46:02 UTC

DanderSpirtz documentation

The goal of this project is to document the different capabilities and functionality of the DanderSpirtz post-exploitation framework / application by examining the contents of the "resources" folder included in the ShadowBrokers leak and doing live testing of the system.

Note: This repository does **not** contain all of the FuzzBunch code, exploits, binaries, etc. The repository *only* contains the files found in the *Windows/Resources/* directory included in the leak.

This repository alone is not enough to run DanderSpritz.

If you're interested in viewing the entire contents of the leak use this repo:

EQGRP_Lost_in_Translation

Python bytecode has been decompiled

The original ShadowBrokers leak had most of the python scripts compiled into optimized bytecode (.pyo). In order to make this reversing / documentation effort easier I've decompiled the code and uploaded the "raw" python code to this repository

The original python bytecode files have been left intact

Resource Codenames and capabilities

The sub-directories in the "Resources" directory contain different modules which are used by DanderSpirtz to provide capabilities such as packet capture, memory dumps, etc.

Below are the codenames that correspond to the different modules and the potential capabilities based on examining the python code, comments, XML, available "command" txt files

Folder	Code Name	Description / Functionality
DSky	***Darkskyline***	PacketCapture tool
DaPu	***DarkPulsar***	Appears to be a legacy implant, similar to PeddleCheap but older
Darkskyline	***DarkSkyline***	Contains tools to parse and filter traffic captured by DarkSkyline
DeMI	***DecibelMinute***	Appears to interact with KillSuit to install, configure, and uninstall it

Folder	Code Name	Description / Functionality
Df	***DoubleFeature***	Generates a log & report about the types of tools that could be deployed on the target. A lot of tools mention that *doublefeature* is the only way to confirm their existence
DmGZ	***DoormanGauze***	DoormanGauze is a kernel level network driver that appears to bypass the standard Windows TCP/IP stack
Dsz	***DanderSpritz***	Several DanderSpritz specific files such as command descriptions (in XML), and several scripts with DSS (Debug script interface?) / DSI extensions?. They seem to be scripts run by DanderSpritz
Ep	***ExpandingPulley***	Listening Post developed in 2001 and abandoned in 2008. Predecessor to DanderSpritz
ExternalLibraries	N/A	Well..
FlAv	***FlewAvenue***	Appears related to DoormanGauze (based on FlAv/scripts/_FlewAvenue.txt)
GRDO	***GreaterDoctor***	Appears to parse / process from GreaterSurgeon (based on GRDO/Tools/i386/GreaterSurgeon_postProcess.py & analyzeMFT.py)
GROK	??	Appears to be a keylogger (based on Ops/PyScripts/overseer/plugins/keylogger.py)
GRcl	??	Appears to dump memory from a specific process (based on GRcl/Commands/CommandLine/ProcessMemory_Command.xml)
GaTh	***GangsterTheif***	Appears to parse data gathered by GreaterDoctor to identify other (malicious) software that may be installed persistently (based on GaTh/Commands/CommandLine/GrDo_ProcessScanner_Command.xml)
GeZU	***GreaterSurgeon***	Appears to dump memory (based on GeZu/Commands/CommandLine/GeZu_KernelMemory_Command.xml)
Gui	N/A	Resources used by the DanderSpirtz GUI
LegacyWindowsExploits	N/A	Well..
Ops	N/A	Contains a lot of awesome tools and python / dss scripts used by DanderSpritz. Deserves a lot of investigation. includes tools to gather data from Chrome, Skype, Firefox (ripper) and gather information about the machine / environment (survey)
Pfree	***Passfreely***	Oracle implant that bypasses auth for oracle databases
PaCU	***PaperCut***	Allows you to perform operations on file handles opened by other processes
Pc	***PeddleCheap***	The main implant (loaded via DoublePulsar) that performs all of these actions and communciates with the C2 (DanderSpirtz)

Folder	Code Name	Description / Functionality
Pc2.2	***PeddleCheap***	Resources for PeddleCheap including different DLLs / configs to call back to the C2
Python	N/A	Python Libraries / resources being used
ScRe	??	Interacts with SQL databases (based on ScRe/Commands/CommandLine/Sql_Command.xml)
StLa	***Strangeland***	Keylogger (based on StLa/Tools/i386-winnt/strangeland.xsl)
Tasking	N/A	Handles the collection "tasks" that DanderSpritz has requested on the same (collection of windows, network data, etc)
TeDi	***TerritorialDispute***	A plugin used to determine what other (malicious) software may be persistently installed (based on TeDi/PyScripts/sigs.py). Appears to be used to identify other nation states also
Utbu	***UtilityBurst***	Appears to be a mechanism for persistence via a driver install *unsure* (based on UtBu/Scripts/Include/_UtilityBurstFunctions.dsi)
ZBng	***ZippyBang***	Looking at this quickly, it appears to be the NSA's version of Mimikatz. It can duplicate tokens (Kerberos tokens?) and "remote execute commands" as well as logon as users (based on files in ZBng/Commands/CommandLine)
