WildFire Analysis Report

1 File Information

File Type	PE
File Signer	
SHA-256	c58158f7bc2caef28a0bc5f10e0536daf841a32bf9ed05c52d7a0576346080e5
SHA-1	f7bdf39ddada9268518d087a56dee3256da54ead
MD5	4e8c629221da743086cd0af905d6f6d2
File Size	55296bytes
First Seen Timestamp	2019-10-07 04:35:46 UTC
Verdict	**Malware**
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections set to both writable and executable

Standard sections are set to either writable or executable. PE files with sections set to both writable and executable are likely packed or obfuscated.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

Last section is executable

In standard PE files the execute flag is reserved for the first section. Use of the execute flag in the last section may indicate a packed or obfuscated file.

First section is writable

In standard PE files the write flag is reserved for sections after the first. Use of the write flag in the first section may indicate a packed or obfuscated file.

3 Dynamic Analysis

3.1. VM1 (Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007)

3.1.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior	Severity
This is a WildFire test sample WildFire test samples exercise the capabilities of the WildFire analysis engine for purposes of testing.	▮▮▮▮▮▮▮▮▮▮
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	▮▯▯▯▯▯▯▯▯▯
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	▮▯▯▯▯▯▯▯▯▯

3.1.2. Network Activity

No network data available.

3.1.3. Host Activity

Process Activity

Process Name - sample.exe

(command: c:\documents and settings\administrator\sample.exe)

Registry Activity

Registry Key	Value	Action
HKEY_LOCAL_MACHINE\Software\PaloAlto		Create
\REGISTRY\MACHINE\SOFTWARE\PaloAlto\PanCar	1	Set

Event Timeline

1	Created Process c:\documents and settings\administrator\sample.exe
2	Set key \REGISTRY\MACHINE\SOFTWARE\PaloAlto\PanCar to value 1

3.2. VM2 (Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010)

3.2.1. Behavioral Summary

This sample was found to be **malware** on this virtual machine.

Behavior	Severity
This is a WildFire test sample WildFire test samples exercise the capabilities of the WildFire analysis engine for purposes of testing.	▮▮▮▮▮▮▮▮▮▮
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	▮▯▯▯▯▯▯▯▯▯

Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	▮▯▯▯▯▯▯▯▯▯

3.2.2. Network Activity

No network data available.

3.2.3. Host Activity

Process Activity

Process Name - sample.exe

(command: C:\Users\Administrator\sample.exe)

Registry Activity

Registry Key	Value	Action
HKEY_LOCAL_MACHINE\Software\PaloAlto		Create
\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\PaloAlto\PanCar	1	Set

Event Timeline

1 Created Process C:\Users\Administrator\sample.exe

2 Set key \REGISTRY\MACHINE\SOFTWARE\Wow6432Node\PaloAlto\PanCar to value 1