

Virtual Analyzer Report



Submission Context

Logged	2020-12-16 17:26:51
Submitter	Manual Submission
Type	Microsoft Cabinet file

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	Troj.Win32.TRX.XXPE50FFF039		
Exploited vulnerabilities	-		
Analyzed objects	Microsoft Cabinet file	1 - SWIFT_pdf.cab	EBF07DBD7FFCC37FA55DCBC69FE481C5CD7B2A63
	Windows 32-bit EXE file	1.1 - SWIFT_pdf.exe	0B84F126BF178A63E8602808D3833448757D276D

Analysis Environments

	Win2012_Office
Anti-security, self-preservation	✓
Autostart or other system reconfiguration	
Deception, social engineering	
File drop, download, sharing, or replication	
Hijack, redirection, or data theft	
Malformed, defective, or with known malware trails	✓
Process, service, or memory object change	✓
Rootkit, cloaking	
Suspicious network or messaging activity	

Win2012_Office

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	Troj.Win32.TRX.XXPE50FFF039
Exploited vulnerabilities	-
Network connection	No network

Object 1 - SWIFT_pdf.cab (Microsoft Cabinet file)

File name	SWIFT_pdf.cab
File type	Microsoft Cabinet file
SHA-1	EBF07DBD7FFCC37FA55DCBC69FE481C5CD7B2A63
SHA-256	7CBFCBF2B4080F8A8752C6D237D233A02950D05F46E17FCBB7103BB1E09F45C8
MD5	89D9310DD2AF77E3F8074F7CD853893E
Size	298636 byte(s)

Risk Level	Unrated
Detection	-
Exploited vulnerabilities	-

Object 1.1 - SWIFT_pdf.exe (Windows 32-bit EXE file)

File name	SWIFT_pdf.exe
File type	Windows 32-bit EXE file
SHA-1	0B84F126BF178A63E8602808D3833448757D276D
SHA-256	630A907CEFDD47F16078D2843D02AA7A9C1EA97A1BFC2CA66936B1D465BDB5C4
MD5	35EF28CE133203A879AEF9B624BB50A8
Size	306688 byte(s)

Risk Level	High risk
Detection	Troj.Win32.TRX.XXPE50FFF039
Exploited vulnerabilities	-
Threat Characteristics	Anti-security, self-preservation (1) Malformed, defective, or with known malware trails (2) Process, service, or memory object change (3)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1
Defense Evasion	Software Packing	Characteristics: 1

© ATT&CK™ is a trademark of The MITRE Corporation.

Notable Threat Characteristics

Anti-security, self-preservation (1)

Characteristic	Significance	Details
Uses suspicious packer		File Name: %WorkingDir%\SWIFT_pdf.exe Packer: UNKNOWN

Malformed, defective, or with known malware traits (2)

Characteristic	Significance	Details
Causes process to crash		Process ID: 1488 Image Path: SWIFT_pdf.exe
Detected as malware by Predictive Machine Learning		Detection Name: Troj.Win32.TRX.XXPE50FF039

Process, service, or memory object change (3)

Characteristic	Significance	Details
Creates process		Process ID: 1488 Image Path: %WorkingDir%\SWIFT_pdf.exe
Creates process		Process ID: 2512 Image Path: %WorkingDir%\SWIFT_pdf.exe Shell Command:
Resides in memory to evade detection		Injecting Process ID: 2512 Injected API: SetThreadContext Target Process ID: 1488 Target Image Path: %WorkingDir%\SWIFT_pdf.exe

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
www.bing.com	-	53	-	No risk	-	SWIFT_pdf.exe
go.microsoft.com	-	53	-	No risk	-	SWIFT_pdf.exe
self.events.data.microsoft.com	-	53	-	No risk	-	SWIFT_pdf.exe
clients2.google.com	-	53	-	No risk	-	SWIFT_pdf.exe

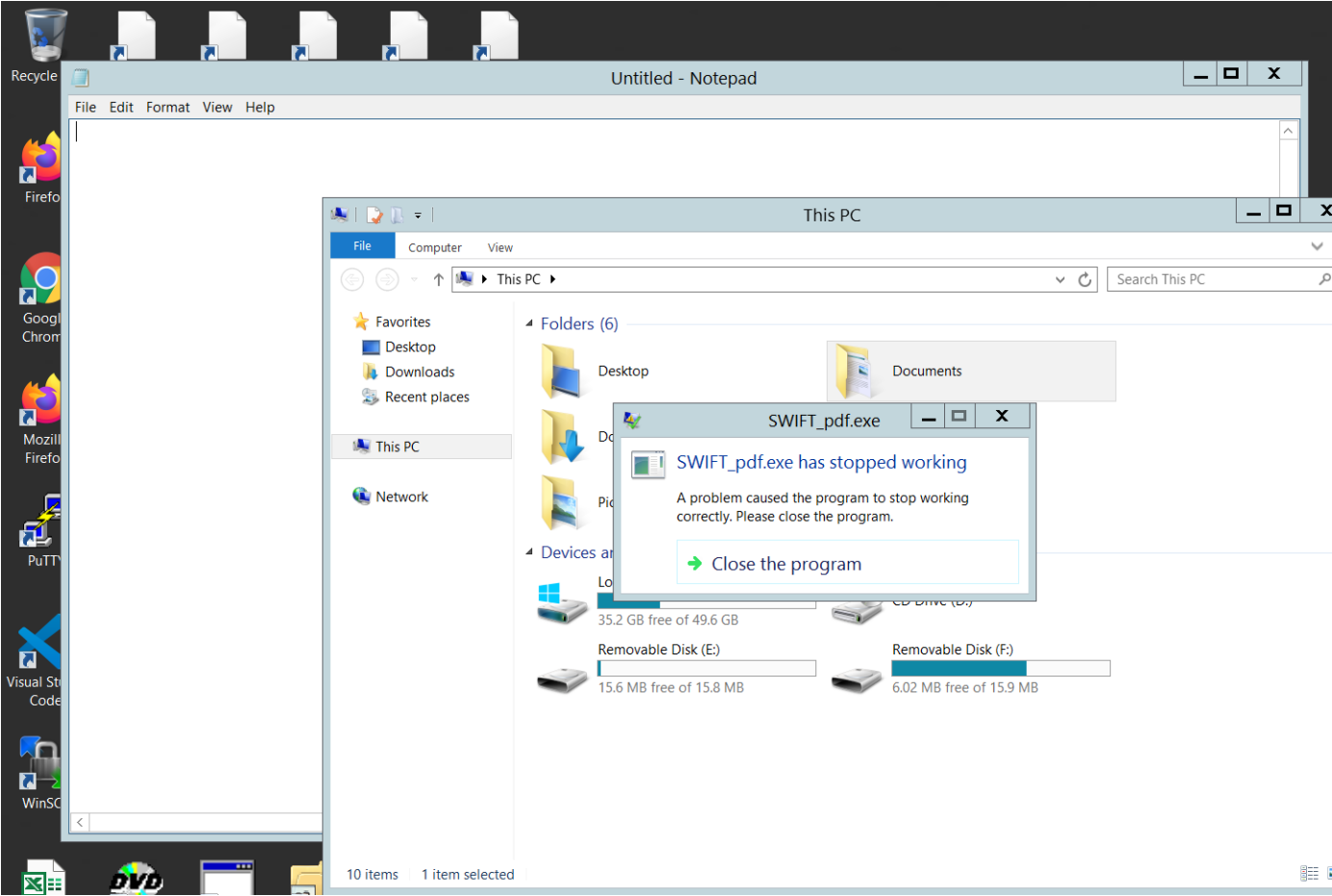
Suspicious Objects

Type	Object	Risk Level
File (SHA1)	0B84F126BF178A63E8602808D383344875D276D	High

Analysis


Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as malware by Predictive Machine Learning Detection Name: Troj.Win32.TRX.XXPE50FFF039		
Detection	Threat Characteristic: Uses suspicious packer File Name: %WorkingDir%\SWIFT_pdf.exe Packer: UNKNOWN		
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\SWIFT_pdf.exe, , , , CREATE_SUSPENDED, , , Process:1488:%WorkingDir%\SWIFT_pdf.exe) Return: 1		2512
Detection	Threat Characteristic: Creates process Process ID: 2512 Image Path: %WorkingDir%\SWIFT_pdf.exe Shell Command:		
Call Thread API	API Name: SetThreadContext Args: (Process Name:1488:%WorkingDir%\SWIFT_pdf.exe) Return: 1		2512
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2512 Injected API: SetThreadContext Target Process ID: 1488 Target Image Path: %WorkingDir%\SWIFT_pdf.exe		
Detection	Threat Characteristic: Creates process Process ID: 1488 Image Path: %WorkingDir%\SWIFT_pdf.exe		
Detection	Threat Characteristic: Causes process to crash Process ID: 1488 Image Path: SWIFT_pdf.exe		


▼ Screenshot





Process Graph Legend


Node

Submitted sample

Root process

Child process


Direct event

Indirect event


Created

Event actions


Notable Threat Characteristics


Anti-security, self-preservation


Autostart or other system reconfiguration


Deception, social engineering


File drop, download, sharing, or replication

Hijack, redirection, or data theft

Malformed, defective, or with known malware traits

Process, service, or memory object change

Rootkit, cloaking

Suspicious network or messaging activity