2d2fa291...85b4 | VMRay Analyzer Report

▶ Try VMRay Analyzer

VTI SCORE: 100/100

emotet_e2_2d2fa29185ad0f48f665f9c93cc8282d3eeca9c848543453cd223333ea2485b4_2019-03-15__142003.doc
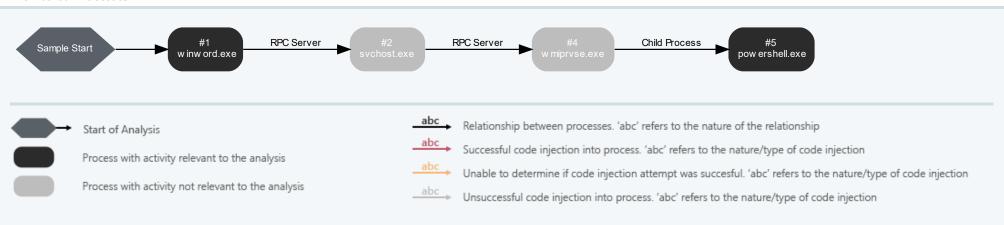
Word Document

Dynamic Analysis Report

Created 6 years ago

•••

Classification: Downloader

Overview	Network	Behavior	Files	AV & YARA	IOCs	Environment

VMRay Threat Indicators (13 rules, 26 matches)

	Severity	Category	Operation	Classification
▷	5/5	Local AV	Malicious content was detected by heuristic scan	-
▷	5/5	File System	Known malicious file	Downloader
▷	4/5	Process	Tries to create process	-
▷	4/5	Network	Reads network adapter information	-
▷	4/5	Network	Associated with known malicious/suspicious URLs	-
▷	3/5	Network	Performs DNS request	-
▷	3/5	Network	Connects to remote host	-
▷	2/5	Network	Connects to HTTP server	-
▷	2/5	VBA Macro	Executes macro on specific worksheet event	-
▷	1/5	Process	Creates system object	-

⌄

Screenshots

Monitored Processes

Sample Start → #1 winword.exe —RPC Server→ #2 svchost.exe —RPC Server→ #4 wmiprvse.exe —Child Process→ #5 powershell.exe

▢→ Start of Analysis

▬ Process with activity relevant to the analysis

▬ Process with activity not relevant to the analysis

abc→ Relationship between processes. 'abc' refers to the nature of the relationship

abc→ Successful code injection into process. 'abc' refers to the nature/type of code injection

abc→ Unable to determine if code injection attempt was succesful. 'abc' refers to the nature/type of code injection

abc→ Unsuccessful code injection into process. 'abc' refers to the nature/type of code injection

Sample Information

ID	#594823
MD5	e9ef35217d83597d41a528a7bfd07847
SHA1	8f14fa07250aa12b4876ef055df604b40fdbf992
SHA256	2d2fa29185ad0f48f665f9c93cc8282d3eeca9c848543453cd223333ea2485b4
SSDeep	6144:X77HUUUUUUUUUUUUUUUUUT52VYl2ZGP+ZQttKcA:X77HUUUUUUUUUUUUUUUUUTCYl2yA4S
Filename	emotet_e2_2d2fa29185ad0f48f665f9c93cc8282d3eeca9c848543453cd223333ea2485b4_2019-03-15__142003.doc

2d2fa291...85b4 | VMRay Analyzer Report

▶ Try VMRay Analyzer

Has VBA Macros	✓

Analysis Information

Creation Time	2019-04-14 16:36 (UTC+2)
Analysis Duration	00:05:09
Number of Monitored Processes	4
Execution Successful	✓
Reputation Enabled	✓
WHOIS Enabled	✓
Local AV Enabled	✓
YARA Enabled	✓
Number of AV Matches	1
Number of YARA Matches	0
Termination Reason	Timeout
Tags	