Deep Discovery Analyzer

Virtual Analyzer Report

Submission Context

Logged	2021-10-25 10:17:42
Submitter	Manual Submission
Type	Windows 32-bit EXE file

Analysis Overview

Overall risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.		
Detections	VAN_DROPPER.UMXX, TROJ.Win32.TRX.XXPE50FFF049		
Exploited vulnerabilities	-		
Analyzed objects	Windows 32-bit EXE file	1 - vbc.exe	EDC27955B5D2388C7A2B792721941D2C270EAC5A

Analysis Environments

	w2008	CentOS	W10
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			

w2008

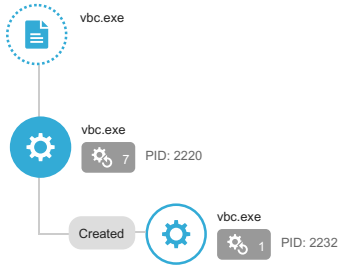
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	VAN_DROPPER.UMXX
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - vbc.exe (Windows 32-bit EXE file)

File name	vbc.exe
File type	Windows 32-bit EXE file
SHA-1	EDC27955B5D2388C7A2B792721941D2C270EAC5A
SHA-256	DE43DF6BD459B56AEC0CD86E0873CC0C5B556E08547E2B9EA79082C44D9B72 20
MD5	538AF9B3EB449AAF53EEAF6ECF3C4037
Size	963914 byte(s)

Risk Level	High risk
Detection	VAN_DROPPER.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1) Process, service, or memory object change (8)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1
Privilege Escalation	Process Injection	Characteristics: 1, 2 Characteristics: 1
Defense Evasion	Process Injection	Characteristics: 1, 2 Characteristics: 1
	Process Hollowing	Characteristics: 1

Notable Threat Characteristics

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Rare executable file	■□□	Global Detections: 3

Process, service, or memory object change (8)

Characteristic	Significance	Details
Resides in memory to evade detection	■■■	Injecting Process ID: 2220 Injected API: SetThreadContext Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 2220 Injected API: WriteProcessMemory Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 2220 Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe Injected Address: 0x0
Resides in memory to evade detection	■■□	Injecting Process ID: 2220 Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe Injected Content: U...E...t.V.u.P.E.PV.'..
Resides in memory to evade detection	■■□	Injecting Process ID: 2220 Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe Injected Content: MZER.
Creates process	■□□	Process ID: 2232 Image Path: %WorkingDir%\vbc.exe
Creates process	■□□	Process ID: 2220 Image Path: %WorkingDir%\vbc.exe Shell Command:
Injects memory with dropped files	■□□	Injecting Process ID: 2220 Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe File: MZER.

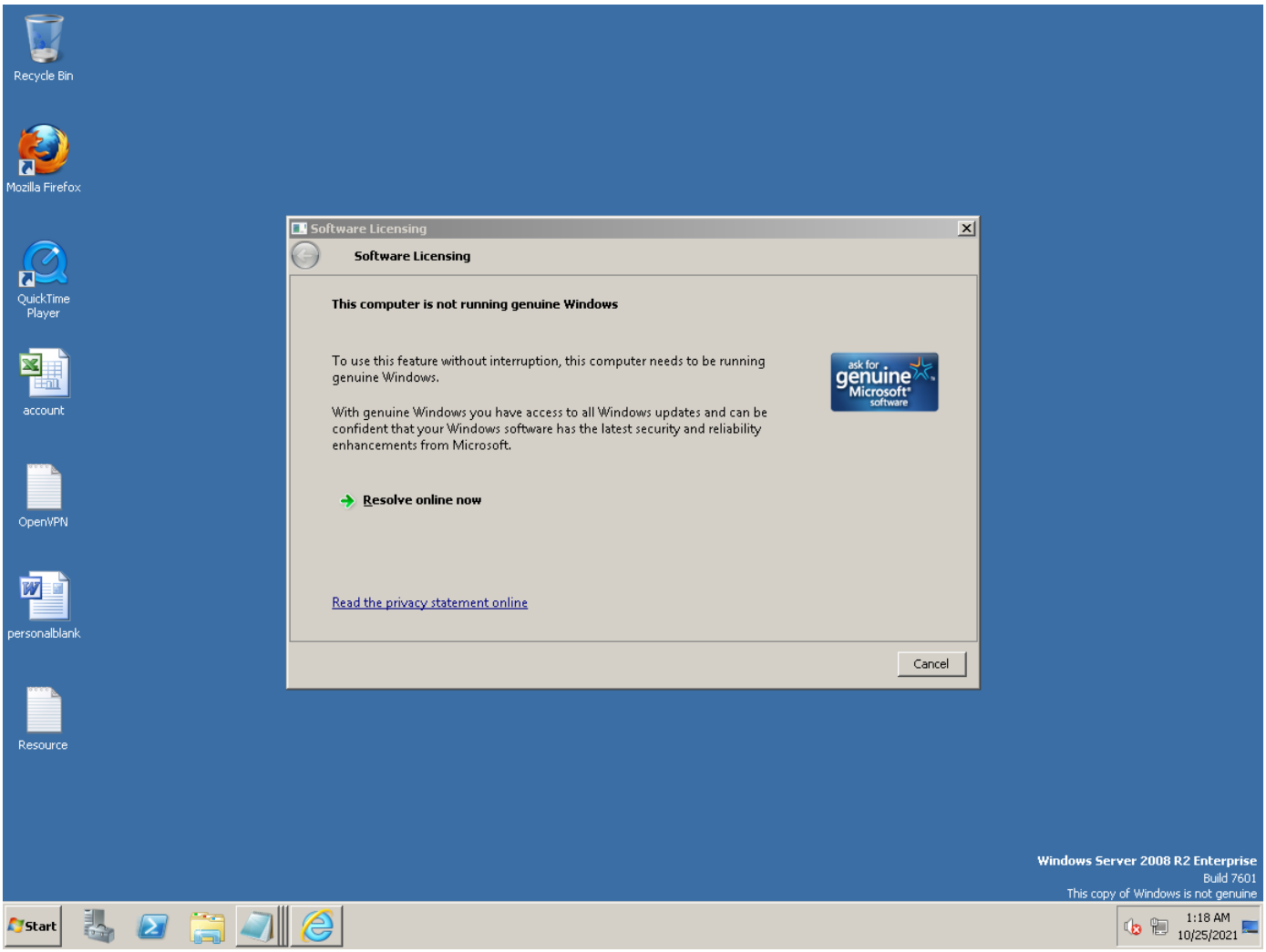
Suspicious Objects

Type	Object	Risk Level
File (SHA1)	EDC27955B5D2388C7A2B792721941D2C270EAC5A	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Rare executable file Global Detections: 3		
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:2232:%WorkingDir%\vbc.exe) Return: 1		2220
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2220 Injected API: SetThreadContext Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2220 Injected API: WriteProcessMemory Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 2220 Image Path: %WorkingDir%\vbc.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2232:%WorkingDir%\vbc.exe, 400000, MZER., 512, 64927c) Return: 1		2220
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2220 Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe Injected Content: MZER.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2220 Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe File: MZER.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:2232:%WorkingDir%\vbc.exe, 401000, U...E...t.V.u.P.E.PV.'.., 162816, 64928c) Return: 1		2220
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2220 Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe Injected Content: U...E...t.V.u.P.E.PV.'..		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7efde000 Process:2232:%WorkingDir%\vbc.exe, 7efde008, , 4, 64928c) Return: 1		2220
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2220 Target Process ID: 2232 Target Image Path: %WorkingDir%\vbc.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:2232:%WorkingDir%\vbc.exe) Return: 1		2220
Call Thread API	API Name: NtResumeThread Args: (Process:2232,) Return: ?		2220
Call System API	API Name: evtchann.SendEvent Args: (e), pid[2232], ppid[2220) Return: 1		2220
Detection	Threat Characteristic: Creates process Process ID: 2232 Image Path: %WorkingDir%\vbc.exe		

▼ **Screenshot**



CentOS

Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	TROJ.Win32.TRX.XXPE50FFF049
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - vbc.exe (Windows 32-bit EXE file)

File name	vbc.exe
File type	Windows 32-bit EXE file
SHA-1	EDC27955B5D2388C7A2B792721941D2C270EAC5A
SHA-256	DE43DF6BD459B56AEC0CD86E0873CC0C5B556E08547E2B9EA79082C44D9B72 20
MD5	538AF9B3EB449AAF53EEAF6ECF3C4037
Size	963914 byte(s)

Risk Level	High risk
Detection	TROJ.Win32.TRX.XXPE50FFF049
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1)

Notable Threat Characteristics

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Detected as malware by Predictive Machine Learning	■■■	Detection Name: TROJ.Win32.TRX.XXPE50FFF049

Suspicious Objects

Type	Object	Risk Level
File (SHA1)	EDC27955B5D2388C7A2B792721941D2C270EAC5A	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Detected as malware by Predictive Machine Learning Detection Name: TROJ.Win32.TRX.XXPE50FFF049		

W10

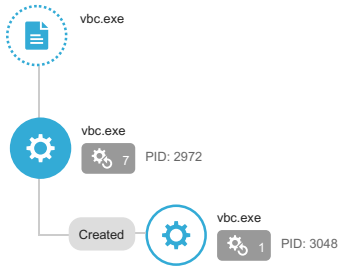
Environment-specific risk level	High risk The object exhibited highly suspicious characteristics that are commonly associated with malware.
Detections	VAN_DROPPER.UMXX
Exploited vulnerabilities	-
Network connection	Custom

Object 1 - vbc.exe (Windows 32-bit EXE file)

File name	vbc.exe
File type	Windows 32-bit EXE file
SHA-1	EDC27955B5D2388C7A2B792721941D2C270EAC5A
SHA-256	DE43DF6BD459B56AEC0CD86E0873CC0C5B556E08547E2B9EA79082C44D9B72 20
MD5	538AF9B3EB449AAF53EEAF6ECF3C4037
Size	963914 byte(s)

Risk Level	High risk
Detection	VAN_DROPPER.UMXX
Exploited vulnerabilities	-
Threat Characteristics	Malformed, defective, or with known malware traits (1) Process, service, or memory object change (8)

Process Graph



Process Graph Legend

MITRE ATT&CK™ Framework Tactics and Techniques

Tactics	Techniques	Notable Threat Characteristics
Execution	Execution through API	Characteristics: 1
Privilege Escalation	Process Injection	Characteristics: 1, 2 Characteristics: 1
Defense Evasion	Process Injection	Characteristics: 1, 2 Characteristics: 1
	Process Hollowing	Characteristics: 1

Notable Threat Characteristics

Malformed, defective, or with known malware traits (1)

Characteristic	Significance	Details
Rare executable file		Global Detections: 3

Process, service, or memory object change (8)

Characteristic	Significance	Details
Resides in memory to evade detection	■■■	Injecting Process ID: 2972 Injected API: SetThreadContext Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 2972 Injected API: WriteProcessMemory Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe
Resides in memory to evade detection	■■□	Injecting Process ID: 2972 Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe Injected Address: 0x0
Resides in memory to evade detection	■■□	Injecting Process ID: 2972 Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe Injected Content: U...E...t.V.u.P.E.PV.'..
Resides in memory to evade detection	■■□	Injecting Process ID: 2972 Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe Injected Content: MZER.
Creates process	■□□	Process ID: 3048 Image Path: %WorkingDir%\vbc.exe
Creates process	■□□	Process ID: 2972 Image Path: %WorkingDir%\vbc.exe Shell Command:
Injects memory with dropped files	■□□	Injecting Process ID: 2972 Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe File: MZER.

Network Destinations

Domain	IP Address	Port	Location	Risk Level	Threat	Accessed By
ocsp.digicert.com	93.184.220.29	53	-	No risk	-	vbc.exe
ctldl.windowsupdate.com	93.184.221.240	53	-	No risk	-	vbc.exe
iecvlist.microsoft.com	152.199.19.161	53	-	No risk	-	vbc.exe
sqm.telemetry.microsoft.com	65.55.252.93	53	-	No risk	-	vbc.exe
ocsp.digicert.com	93.184.220.29	80	-	-	-	vbc.exe
sqm.telemetry.microsoft.com	65.55.252.93	443	-	-	-	vbc.exe
iecvlist.microsoft.com	152.199.19.161	443	-	-	-	vbc.exe
ctldl.windowsupdate.com	93.184.221.240	80	-	-	-	vbc.exe

URL	Site Category	Risk Level	Threat	Accessed By
http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDl7I90VUCEAJ0LqoXyo4hxxe7H%2Fz9DKA%3D	Computers / Internet Cloud Applications	No risk	-	vbc.exe
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1d154a93017e3f6e	Computers / Internet	No risk	-	vbc.exe
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?a82a0d5825e83372	Computers / Internet	No risk	-	vbc.exe

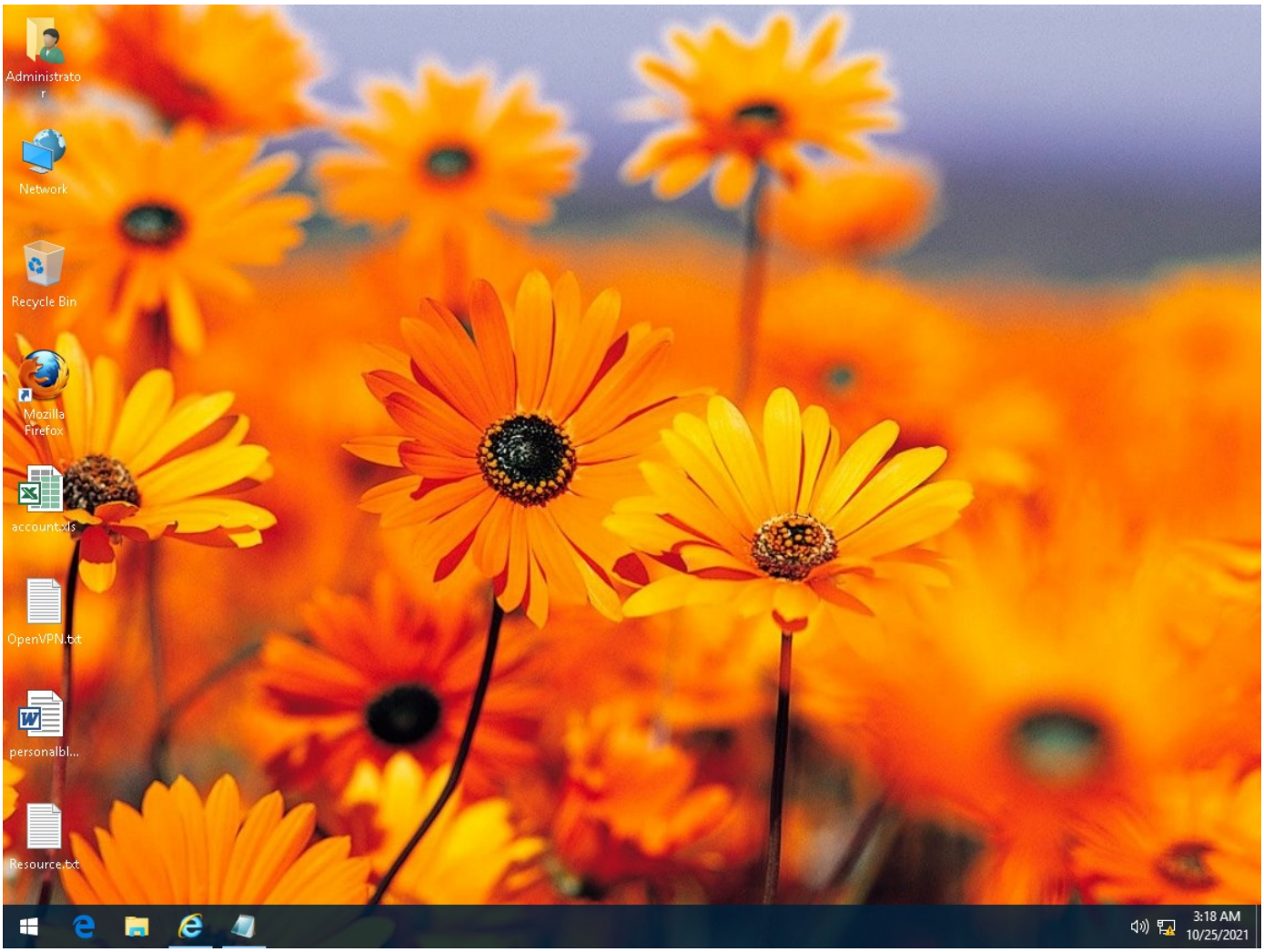
Suspicious Objects

Type	Object	Risk Level
File (SHA1)	EDC27955B5D2388C7A2B792721941D2C270EAC5A	High

Analysis

Event Type	Details	Parent PID	PID
Detection	Threat Characteristic: Rare executable file Global Detections: 3		
Call Process API	API Name: CreateProcessW Args: (%WorkingDir%\vbc.exe, , , , , CREATE_SUSPENDED, , , , Process:3048:%WorkingDir%\vbc.exe) Return: 1		2972
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2972 Injected API: SetThreadContext Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe		
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2972 Injected API: WriteProcessMemory Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe		
Detection	Threat Characteristic: Creates process Process ID: 2972 Image Path: %WorkingDir%\vbc.exe Shell Command:		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3048:%WorkingDir%\vbc.exe, 400000, MZER., 512, 683dac) Return: 1		2972
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2972 Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe Injected Content: MZER.		
Detection	Threat Characteristic: Injects memory with dropped files Injecting Process ID: 2972 Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe File: MZER.		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Process Name:3048:%WorkingDir%\vbc.exe, 401000, U...E...t.V.u.P.E.PV.'.., 162816, 683dbc) Return: 1		2972
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2972 Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe Injected Content: U...E...t.V.u.P.E.PV.'..		
Call Virtual Memory API	API Name: WriteProcessMemory Args: (Modify PEB 7ffde000 Process:3048:%WorkingDir%\vbc.exe, 7ffde008, , 4, 683dbc) Return: 1		2972
Detection	Threat Characteristic: Resides in memory to evade detection Injecting Process ID: 2972 Target Process ID: 3048 Target Image Path: %WorkingDir%\vbc.exe Injected Address: 0x0		
Call Thread API	API Name: SetThreadContext Args: (Process Name:3048:%WorkingDir%\vbc.exe) Return: 1		2972
Call Thread API	API Name: NtResumeThread Args: (Process:3048,) Return: ?		2972
Call System API	API Name: evtchann.SendEvent Args: (e), pid[3048], ppid[2972) Return: 1		2972
Detection	Threat Characteristic: Creates process Process ID: 3048 Image Path: %WorkingDir%\vbc.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