Analysis Report 8YQym0faQ4.cmd

Sample Name: 8YQym0faQ4.cmd
Filesize: 101617
MD5: d93a5554b0cb981e9a8eb7f297c1f5c6
SHA1: cd084bc4d30fd9065707831f0af405d28645c3b6
SHA256: 9fca19c2b9971c7010ed0cc99d8f9ca5fd37775927c0721ae51e13c892a58266
AIML: 0 **(UNKNOWN)**
Static: **(CLEAN)**
MultiAV: **(MALICIOUS)**
Dynamic Analysis Using Sandboxing: 24 **(SUS)**

MITRE ATT&CK MATRIX

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Command and Scripting Interpreter 1 1	Process Injection 1 1	Masquerading 1	Disable or Modify Tools 1	Virtualization/Sandbox Evasion 2 1	Process Injection 1 1	Process Discovery 1	Virtualization/Sandbox Evasion 2 1	Application Window Discovery 1	System Information Discovery 1 2				
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder	Process Injection 1	Masquerading 1	OS Credential Dumping	System Information Discovery 2	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder	Software Packing	LSASS Memory	Application Window Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Carrier Billing	Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Risk Summary

- Analysis Advice
- Compliance
- System Summary
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Static Summary

- Yara
- oletools

AV Engines Scan Summary

- clamav
- comodo
- mcafee
- node32
- sophos
- microsoft (Trojan:Script/Malgent!MSR)
- cyren
- kaspersky
- avast

BEHAVIOUR ANALYSIS

SYSTEM STARTUP PROCESS

-> **cmd.exe** (PID: 3308, CMD: C:\Windows\system32\cmd.exe /c ""C:\Users\user\Desktop\8YQym0faQ4.cmd" ", MD5: 9D59442313565C2E0860B88BF32B2277)
-> **conhost.exe** (PID: 5060, CMD: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1, MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
-> **cmd.exe** (PID: 1400, CMD: C:\Windows\system32\cmd.exe /K "C:\Users\user\Desktop\8YQym0faQ4.cmd" , MD5: 9D59442313565C2E0860B88BF32B2277)

URL ANALYSIS

FOUND URLS IN SOURCE

Not Found

IP ANALYSIS

IP FOUND IN SOURCE

Not Found

DOMAINS ANALYSIS

DOMAIN FOUND IN SOURCE

Not Found

BEHAVIOUR

FOUND INLINED NOP INSTRUCTIONS (LIKELY SHELL OR OBFUSCATED CODE)

Filetype : DOS batch file, ASCII text, with very long lines (65234), with CRLF line terminators

Entropy : 6.019913823840677

Trid :
@arraytag : def

Filename : 8YQym0faQ4.cmd

Submissionpath : C:\Users\user\desktop\

Filesize : 101617

Md5 : d93a5554b0cb981e9a8eb7f297c1f5c6

Sha1 : cd084bc4d30fd9065707831f0af405d28645c3b6

Sha256 : 9fca19c2b9971c7010ed0cc99d8f9ca5fd37775927c0721ae51e13c892a58266

Sha512 : 8c68162ab5811ed42c3f6c23baac81efad77cc8763f854324e2142cb6e2ec0b2be6cf7735f8bc013c9cddefde2 ccaf2309e15c758a1bcdc3a532d8df996af95e

Ssdeep : 1536:8Es9iOqjx4OhT1RvqUnwsNqG79FSTvUGcLjMM748pkHilGvpw3EmFWeBHyq:cFCZ3qUnpp9FS4jjTlkHvGvpG 5FvEq

Tlsh : 92A3F1B9F4D039E8C52C6C0A17961F6903706665C086FDEB4C98D88E2299B935DF3CF9

Preview : @echo off..set "sSxFXf=sscPaNet scPaNFscPaNGscPaNVm=scPaN1scPaN scPaN&&scPaN stscPaNascPaN rtscPaN scPaN"scPaN" scPaN/miscPaNn scPaN"..set "RXDoGX=&&scPaN exscPaNitscPaN"..set "DBJf yx=nscPaNoscPaNt dscPaNefscPaNiscPaNnescPaNd scPaNFscPaNGVmscPaN..if %DBJfy