

002 - Oski

Overview

- Scenario:

The accountant at the company received an email titled "Urgent New Order" from a client late in the afternoon. When he attempted to access the attached invoice, he discovered it contained false order information. Subsequently, the SIEM solution generated an alert regarding downloading a potentially malicious file. Upon initial investigation, it was found that the PPT file might be responsible for this download. Could you please conduct a detailed examination of this file?

- Skills Covered: VirusTotal, MITRE ATT&CK spotting, ANY.RUN reading

Tools Used

- VirusTotal
- ANY.RUN - Virus report website

Questions

1. Identify virus by their MD5 hash

Copied the given MD5 hash to VirusTotal search bar, it showed quite a bit details

60
/ 70
Community Score
-5

60/70 security vendors flagged this file as malicious

Reanalyze

Similar

More

a040a0af8697e30506218103074c7d6ea77a84ba3ac1ee5efae20f15530a19bb

Size311.50 KB

Last Analysis Date1 day ago

peexe

self-delete

idle

checks-cpu-name

spreader

malware

cve-2016-0101

exploit

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY22+

Join our Community

and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD512c1842c3ccafe7408c23ebf292ee3d9

SHA-14b1af84cc11a8b1e290a18a4222a49526eeadd10

SHA-256a040a0af8697e30506218103074c7d6ea77a84ba3ac1ee5efae20f15530a19bb

Vhash0350365d151015z3007cnz1fz

Authentihash64232d71f5775257fc17860be8a2c063382d6a06a7ba20b86f017e425ed37cc1

Imphash915313f9baf3d4f9e9e467fb8242a50c

Rich PE header hash04777fa4fd51f65c29f5c9cb30b066cb

SSDEEP6144sMHKlTRkt3eaAuvuOosMvhCHCEs2qwYZKmATfrdHcn5lotMperwCC5EQrZHK

TLSHT13D647E4393F17C60E5364B329E2EC2E8761EF5604E59776A2329BA2F08B05F2D673711

File typeWin32 EXE

MagiPE32 executable (GUI) Intel 80386, for MS Windows

TrIDWin32 Executable MS Visual C++ (generic) (52.5%) | Win64 Executable (generic) (17.7%) | Win16 NE executable (generic) (8.4%) | Win32 Executable (generic) (7.5%) | W...

DetectItEasyPE32 | Compiler: EP:Microsoft Visual C/C++ (2008-2010) [EXE32] | Compiler: Microsoft Visual C/C++ (16.00.30319) [LTCG/C++] | Linker: Microsoft Linker (10.00.30319) | T...

MagikaPEBIN

File size311.50 KB (318976 bytes)

You can see what it does and how it does in those Tabs

2. Self-deleting

1 / 2

Seeing this log you know it deletes itself after successfully exfiltrating user's data.

Behavior activities

(PID: 3484) VPN.exe

Source: processFirst seen: 29031 ms

?

Danger / General

Starts CMD.EXE for self-deleting

T1070.004 File Deletion

Image:

C:\Windows\System32\cmd.exe

Cmdline:

"C:\Windows\system32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\admin\AppData\Local\Temp\VPN.exe" & del "C:\ProgramData*.dll" & exit

CyberDefenders

PracticeCertifyFor BusinessMore

DashboardLabsTracksLeaderboardMITRE ATT&CKBadgesFAQ

Search for labs...

2Go Pro

Practice > SOC Analyst Tier 1 > Level 1 > Oski

Oski Lab

Category: Threat Intel

Tactics: Initial AccessExecutionDefense EvasionCredential AccessCommand and ControlExfiltration

Tools: VirusTotalANY.RUN

EasyRetired30mins4.5

BookmarkJoin the Lab SquadReport an IssueShare Achievement

Download Lab Files

Unzip the file with password cyberdefenders.org

For a safe experience, consider opening this content in a secure, isolated environment.

Scenario

The accountant at the company received an email titled "Urgent New Order" from a client late in the afternoon. When he attempted to access the attached invoice, he discovered it contained false order information. Subsequently, the SIEM solution generated an alert regarding downloading a potentially malicious file. Upon initial investigation, it was found that the PPT file might be responsible for this download. Could you please conduct a detailed examination of this file?

7 / 7 Questions

100% Completed

7 / 7 Questions