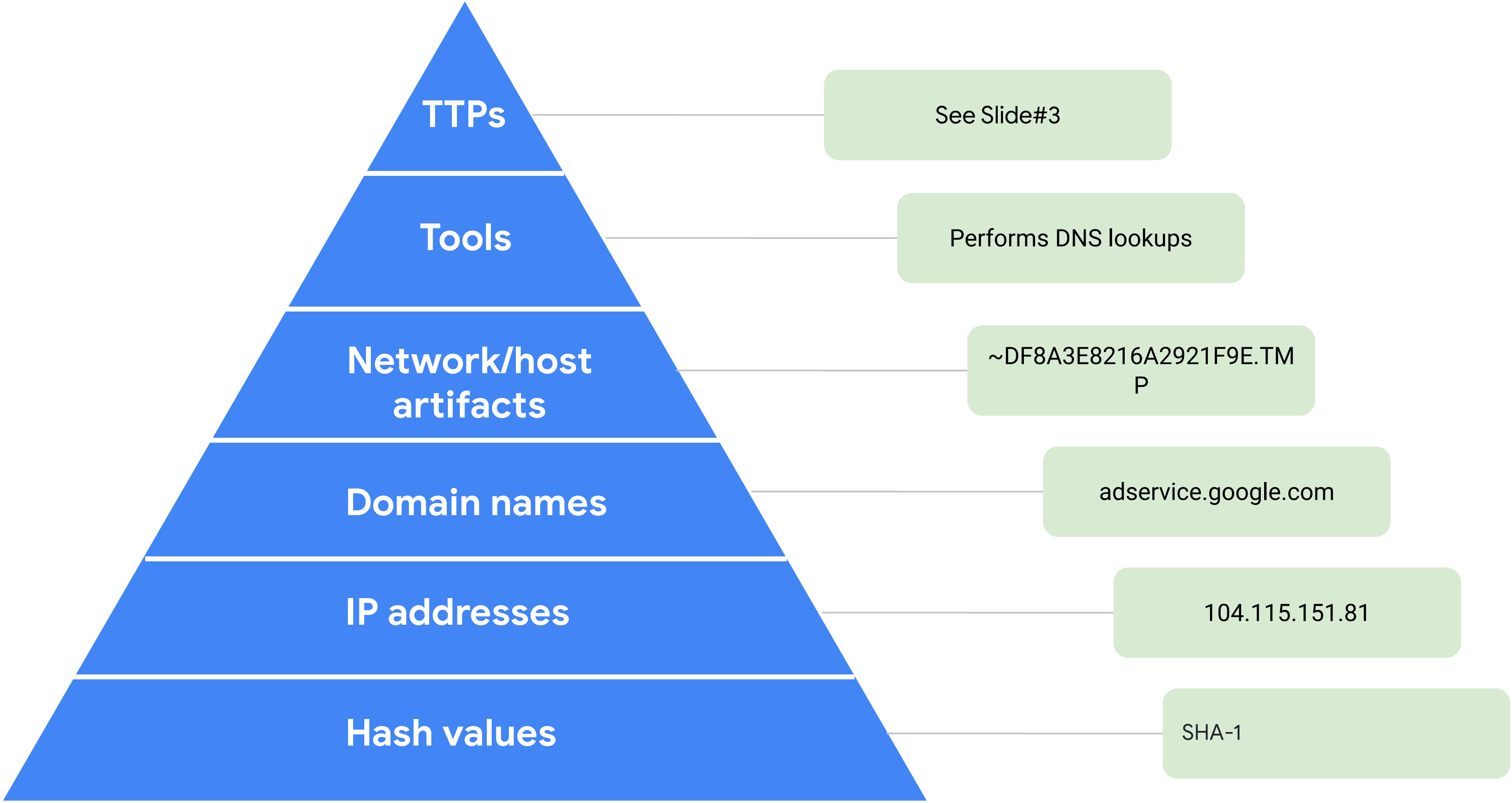
Has this file been identified as malicious? Explain why or why not.

The file is considered malicious because it executed a harmful payload on the employee's computer, went beyond the expected functionality of a legitimate file, involved social engineering tactics, and triggered suspicious alerts in the organization's security systems.

Additionally, the VirusTotal analysis of the SHA-256 hash for this file indicates that it is likely malicious.



TTPs	See Slide#3
Tools	Performs DNS lookups
Network/host artifacts	~DF8A3E8216A2921F9E.TMP
Domain names	adservice.google.com
IP addresses	104.115.151.81
Hash values	SHA-1

TTPs

Execution TA0002
Shared Modules T1129
Link function at runtime on Windows
Link many functions at runtime
Component Object Model T1559.001
Privilege Escalation TA0004
Process Injection T1055
Spawns processes
Defense Evasion TA0005
Obfuscated Files or Information T1027
Encode data using Base64
Encrypt data using DPAPI
Encrypt data using RC4 PRGA
Reference Base64 string
Masquerading T1036
Creates files inside the user directory
Process Injection T1055
Spawns processes
Virtualization/Sandbox Evasion T1497
May sleep (evasive loops) to hinder dynamic analysis
Contains long sleeps (>= 3 min)
Contains medium sleeps (>= 30s)
Time Based Evasion T1497.003
Credential Access TA0006
Input Capture T1056
Creates a DirectInput object (often for capturing keystrokes)
Windows Credential Manager T1555.004
Acquire credentials from Windows Credential Manager
Discovery TA0007
Application Window Discovery T1010
Find graphical window
System Information Discovery T1082
Reads software policies
File and Directory Discovery T1083
Get common file path
Reads ini files
System Time Discovery T1124
Virtualization/Sandbox Evasion T1497
May sleep (evasive loops) to hinder dynamic analysis
Contains long sleeps (>= 3 min)
Contains medium sleeps (>= 30s)
Time Based Evasion T1497.003
Collection TA0009
Input Capture T1056
Creates a DirectInput object (often for capturing keystrokes)
Command and Control TA0011
Application Layer Protocol T1071
Performs DNS lookups
Uses HTTPS
Non-Application Layer Protocol T1095
Performs DNS lookups
Encrypted Channel T1573
Uses HTTPS for network communication, use the SSL MITM Proxy cookbook for further analysis
Uses HTTPS