Higaisa, Group G0126 | MITRE ATT&CK®

Archived: 2026-04-05 12:52:28 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Higaisa used HTTP and HTTPS to send data back to its C2 server.[1][2]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Higaisa added a spoofed binary to the start-up folder for persistence.[1][2]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Higaisa used `cmd.exe` for execution.[1][2][3]

.005 Command and Scripting Interpreter: Visual Basic

Higaisa has used VBScript code on the victim's machine.[3]

.007 Command and Scripting Interpreter: JavaScript

Higaisa used JavaScript to execute additional files.[1][2][3]

Enterprise T1001 .003 Data Obfuscation: Protocol or Service Impersonation

Higaisa used a FakeTLS session for C2 communications.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Higaisa used certutil to decode Base64 binaries at runtime and a 16-byte XOR key to decrypt data.[1][2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Higaisa used AES-128 to encrypt C2 traffic.[2]

Enterprise T1041 Exfiltration Over C2 Channel

Higaisa exfiltrated data over its C2 channel.[2]

Enterprise T1203 Exploitation for Client Execution

Higaisa has exploited CVE-2018-0798 for execution.[3]

Enterprise T1564 .003 Hide Artifacts: Hidden Window

Higaisa used a payload that creates a hidden window.[3]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Higaisa's JavaScript file used a legitimate Microsoft Office 2007 package to side-load the `OINFO12.OCX` dynamic link library.[3]

Enterprise T1680 Local Storage Discovery

Higaisa collected the system volume serial number.[3][1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Higaisa named a shellcode loader binary `svchast.exe` to spoof the legitimate `svchost.exe`.[1][2]

Enterprise T1106 Native API

Higaisa has called various native OS APIs.[2]

Enterprise T1027 .001 Obfuscated Files or Information: Binary Padding

Higaisa performed padding with null bytes before calculating its hash.[2]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Higaisa used Base64 encoded compressed payloads.[1][2]

.015 Obfuscated Files or Information: Compression

Higaisa used Base64 encoded compressed payloads.[1][2]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Higaisa has sent spearphishing emails containing malicious attachments.[1][2]

Enterprise T1057 Process Discovery

Higaisa's shellcode attempted to find the process ID of the current process.[2]

Enterprise T1090 .001 Proxy: Internal Proxy

Higaisa discovered system proxy settings and used them if available.[2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Higaisa dropped and added `officeupdate.exe` to scheduled tasks.[1][2]

Enterprise T1029 Scheduled Transfer

Higaisa sent the victim computer identifier in a User-Agent string back to the C2 server every 10 minutes.[3]

Enterprise T1082 System Information Discovery

Higaisa collected the system GUID and computer name.[3][1]

Enterprise T1016 System Network Configuration Discovery

Higaisa used `ipconfig` to gather network configuration information.[1][2]

Enterprise T1124 System Time Discovery

Higaisa used a function to gather the current time.[2]

Enterprise T1204 .002 User Execution: Malicious File

Higaisa used malicious e-mail attachments to lure victims into executing LNK files.[1][2]

Enterprise T1220 XSL Script Processing

Higaisa used an XSL file to run VBScript code.[3]
