Zebrocy, Software S0251 | MITRE ATT&CK®

Archived: 2026-04-05 16:49:46 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Zebrocy uses HTTP for C2.[1][2][7][3][8][6]

.003 Application Layer Protocol: Mail Protocols

Zebrocy uses SMTP and POP3 for C2.[1][2][7][3][8]

Enterprise T1560 Archive Collected Data

Zebrocy has used a method similar to RC4 as well as AES for encryption and hexadecimal for encoding data before exfiltration. [9][7][4]

Enterprise T1119 Automated Collection

Zebrocy scans the system and automatically collects files with the following extensions: .doc, .docx, ,.xls, .xlsx, .pdf, .pptx, .rar, .zip, .jpg, .jpeg, .bmp, .tiff, .kum, .tlg, .sbx, .cr, .hse, .hsf, and .lhz.[7][8]

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

Zebrocy creates an entry in a Registry Run key for the malware to execute on startup.[7][8][6]

Enterprise T1037 .001 Boot or Logon Initialization Scripts: Logon Script (Windows)

Zebrocy performs persistence with a logon script via adding to the Registry key `HKCU\Environment\UserInitMprLogonScript`.[7]

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

Zebrocy uses cmd.exe to execute commands on the system.[8][4]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

Zebrocy has the capability to upload dumper tools that extract credentials from web browsers and store them in database files.[8]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Zebrocy has used URL/Percent Encoding on data exfiltrated via HTTP POST requests.[6]

Enterprise T1074 .001 Data Staged: Local Data Staging

Zebrocy stores all collected information in a single file before exfiltration.[7]

Enterprise T1140 Deobfuscate/Decode Files or Information

Zebrocy decodes its secondary payload and writes it to the victim’s machine. Zebrocy also uses AES and XOR to decrypt strings and payloads.[2][7]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

Zebrocy uses SSL and AES ECB for encrypting C2 communications.[7][8][4]

Enterprise T1041 Exfiltration Over C2 Channel

Zebrocy has exfiltrated data to the designated C2 server using HTTP POST requests.[6][4]

Enterprise T1083 File and Directory Discovery

Zebrocy searches for files that are 60mb and less and contain the following extensions: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .exe, .zip, and .rar. Zebrocy also runs the `echo %APPDATA%` command to list the contents of the directory.[9][7][8] Zebrocy can obtain the current execution path as well as perform drive enumeration.[6][4]

Enterprise T1070 .004 Indicator Removal: File Deletion

Zebrocy has a command to delete files and directories.[7][8][4]

Enterprise T1105 Ingress Tool Transfer

Zebrocy obtains additional code to execute on the victim's machine, including the downloading of a secondary payload.[1][2][8][6]

Enterprise T1056 .004 Input Capture: Credential API Hooking

Zebrocy installs an application-defined Windows hook to get notified when a network drive has been attached, so it can then use the hook to call its RecordToFile file stealing method.[9]

Enterprise T1680 Local Storage Discovery

Zebrocy collects the serial number for the storage volume C:.[1][2][7][3][8][6][4]

Enterprise T1135 Network Share Discovery

Zebrocy identifies network drives when they are added to victim systems.[9]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

Zebrocy's Delphi variant was packed with UPX.[3][6]

Enterprise T1120 Peripheral Device Discovery

Zebrocy enumerates information about connected storage devices.[2]

Enterprise T1057 Process Discovery

Zebrocy uses the `tasklist` and `wmic process get Capture, ExecutablePath` commands to gather the processes running on the system.[2][7][3][8][6]

Enterprise T1012 Query Registry

Zebrocy executes the `reg query` command to obtain information in the Registry.[8]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Zebrocy has a command to create a scheduled task for persistence.[4]

Enterprise T1113 Screen Capture

A variant of Zebrocy captures screenshots of the victim's machine in JPEG and BMP format.[2][7][3][8][6][4]

Enterprise T1082 System Information Discovery

Zebrocy collects the OS version and computer name. Zebrocy also runs the `systeminfo` command to gather system information. [1][2][7][3][8][6][4]

Enterprise T1016 System Network Configuration Discovery

Zebrocy runs the `ipconfig /all` command.[8]

Enterprise T1049 System Network Connections Discovery

Zebrocy uses `netstat -aon` to gather network connection information.[8]

Enterprise T1033 System Owner/User Discovery

Zebrocy gets the username from the system.[7][4]

Enterprise T1124 System Time Discovery

Zebrocy gathers the current time zone and date information from the system.[7][4]

Enterprise T1047 Windows Management Instrumentation

One variant of Zebrocy uses WMI queries to gather information.[3]
