Okrum, Software S0439 | MITRE ATT&CK®

Archived: 2026-04-05 15:02:53 UTC

Enterprise T1134 .001 Access Token Manipulation: Token Impersonation/Theft

Okrum can impersonate a logged-on user's security context using a call to the ImpersonateLoggedOnUser API.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Okrum uses HTTP for communication with its C2.[1]

Enterprise T1560 .001 Archive Collected Data: Archive via Utility

Okrum was seen using a RAR archiver tool to compress/decompress data.[1]

.003 Archive Collected Data: Archive via Custom Method

Okrum has used a custom implementation of AES encryption to encrypt collected data.[1]

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

Okrum establishes persistence by creating a .lnk shortcut to itself in the Startup folder.[1]

.009 Boot or Logon Autostart Execution: Shortcut Modification

Okrum can establish persistence by creating a .lnk shortcut to itself in the Startup folder.[1]

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

Okrum's backdoor has used cmd.exe to execute arbitrary commands as well as batch scripts to update itself to a newer version.[1]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

To establish persistence, Okrum can install itself as a new service named NtmSsvc.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Okrum has used base64 to encode C2 communication.[1]

Enterprise T1001 Data Obfuscation

Okrum leverages the HTTP protocol for C2 communication, while hiding the actual messages in the Cookie and Set-Cookie headers of the HTTP requests.[1]

.003 Protocol or Service Impersonation

Okrum leverages the HTTP protocol for C2 communication, while hiding the actual messages in the Cookie and Set-Cookie headers of the HTTP requests.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Okrum's loader can decrypt the backdoor code, embedded within the loader or within a legitimate PNG file. A custom XOR cipher or RC4 is used for decryption.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Okrum uses AES to encrypt network traffic. The key can be hardcoded or negotiated with the C2 server in the registration phase. [1]

Enterprise T1041 Exfiltration Over C2 Channel

Data exfiltration is done by Okrum using the already opened channel with the C2 server.[1]

Enterprise T1083 File and Directory Discovery

Okrum has used DriveLetterView to enumerate drive information.[1]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

Before exfiltration, Okrum's backdoor has used hidden files to store logs and outputs from backdoor commands.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Okrum's backdoor deletes files after they have been successfully uploaded to C2 servers.[1]

Enterprise T1105 Ingress Tool Transfer

Okrum has built-in commands for uploading, downloading, and executing files to the system.[1]

Enterprise T1056 .001 Input Capture: Keylogging

Okrum was seen using a keylogger tool to capture keystrokes. [1]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Okrum can establish persistence by adding a new service NtmsSvc with the display name Removable Storage to masquerade as a legitimate Removable Storage Manager.[1]

Enterprise T1027 .003 Obfuscated Files or Information: Steganography

Okrum's payload is encrypted and embedded within its loader, or within a legitimate PNG file.[1]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Okrum was seen using MimikatzLite to perform credential dumping.[1]

.005 OS Credential Dumping: Cached Domain Credentials

Okrum was seen using modified Quarks PwDump to perform credential dumping.[1]

Enterprise T1090 .002 Proxy: External Proxy

Okrum can identify proxy servers configured and used by the victim, and use it to make HTTP requests to C2 its server.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Okrum's installer can attempt to achieve persistence by creating a scheduled task.[1]

Enterprise T1082 System Information Discovery

Okrum can collect computer name, locale information, and information about the OS and architecture.[1]

Enterprise T1016 System Network Configuration Discovery

Okrum can collect network information, including the host IP address, DNS, and proxy information.[1]

Enterprise T1049 System Network Connections Discovery

Okrum was seen using NetSess to discover NetBIOS sessions.[1]

Enterprise T1033 System Owner/User Discovery

Okrum can collect the victim username.[1]

Enterprise T1569 .002 System Services: Service Execution

Okrum's loader can create a new service named NtmsSvc to execute the payload.[1]

Enterprise T1124 System Time Discovery

Okrum can obtain the date and time of the compromised system.[1]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

Okrum's loader can check the amount of physical memory and terminates itself if the host has less than 1.5 Gigabytes of physical memory in total.[1]

.002 Virtualization/Sandbox Evasion: User Activity Based Checks

Okrum loader only executes the payload after the left mouse button has been pressed at least three times, in order to avoid being executed within virtualized or emulated environments.[1]

.003 Virtualization/Sandbox Evasion: Time Based Checks

Okrum's loader can detect presence of an emulator by using two calls to GetTickCount API, and checking whether the time has been accelerated.[1]
