FatDuke, Software S0512 | MITRE ATT&CK®

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

FatDuke can be controlled via a custom C2 protocol over HTTP.[1]

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

FatDuke has used `HKLM\SOFTWARE\Microsoft\CurrentVersion\Run` to establish persistence.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

FatDuke has the ability to execute PowerShell scripts.[1]

Enterprise T1005 Data from Local System

FatDuke can copy files and directories from a compromised host.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

FatDuke can decrypt AES encrypted C2 communications.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

FatDuke can AES encrypt C2 communications.[1]

Enterprise T1008 Fallback Channels

FatDuke has used several C2 servers per targeted organization.[1]

Enterprise T1083 File and Directory Discovery

FatDuke can enumerate directories on target machines.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

FatDuke can secure delete its DLL.[1]

Enterprise T1036 .012 Masquerading: Browser Fingerprint

FatDuke has attempted to mimic a compromised user's traffic by using the same user agent as the installed browser.[1]

Enterprise T1106 Native API

FatDuke can call `ShellExecuteW` to open the default browser on the URL localhost.[1]

Enterprise T1027 Obfuscated Files or Information

FatDuke can use base64 encoding, string stacking, and opaque predicates for obfuscation.[1]

.002 Software Packing

FatDuke has been regularly repacked by its operators to create large binaries and evade detection.[1]

.016 Junk Code Insertion

FatDuke has been packed with junk code and strings.[1]

Enterprise T1057 Process Discovery

FatDuke can list running processes on the localhost.[1]

Enterprise T1090 .001 Proxy: Internal Proxy

FatDuke can used pipes to connect machines with restricted internet access to remote machines via other infected hosts.[1]

Enterprise T1012 Query Registry

FatDuke can get user agent strings for the default browser from `HKCU\Software\Classes\http\shell\open\command`.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

FatDuke can execute via rundll32.[1]

Enterprise T1082 System Information Discovery

FatDuke can collect the user name, Windows version, computer name, and available space on discs from a compromised host.[1]

Enterprise T1016 System Network Configuration Discovery

FatDuke can identify the MAC address on the target computer.[1]

Enterprise T1497 .003 Virtualization/Sandbox Evasion: Time Based Checks

FatDuke can turn itself on or off at random intervals.[1]
