Duqu, Software S0038 | MITRE ATT&CK®

Archived: 2026-04-05 17:03:53 UTC

Enterprise T1134 Access Token Manipulation

Duqu examines running system processes for tokens that have specific system privileges. If it finds one, it will copy the token and store it for later use. Eventually it will start new processes with the stored token attached. It can also steal tokens to acquire administrative privileges.[2]

Enterprise T1087 .001 Account Discovery: Local Account

The discovery modules used with Duqu can collect information on accounts and permissions.[1]

Enterprise T1071 Application Layer Protocol

Duqu uses a custom command and control protocol that communicates over commonly used ports, and is frequently encapsulated by application layer protocols.[1]

Enterprise T1010 Application Window Discovery

The discovery modules used with Duqu can collect information on open windows.[1]

Enterprise T1560 .003 Archive Collected Data: Archive via Custom Method

Modules can be pushed to and executed by Duqu that copy data to a staging area, compress it, and XOR encrypt it.[1]

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

Duqu creates a new service that loads a malicious driver when the system starts. When Duqu is active, the operating system believes that the driver is legitimate, as it has been signed with a valid private key.[1]

Enterprise T1001 .002 Data Obfuscation: Steganography

When the Duqu command and control is operating over HTTP or HTTPS, Duqu uploads data to its controller by appending it to a blank JPG file.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Modules can be pushed to and executed by Duqu that copy data to a staging area, compress it, and XOR encrypt it.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

The Duqu command and control protocol's data stream can be encrypted with AES-CBC.[1]

Enterprise T1056 .001 Input Capture: Keylogging

Duqu can track key presses with a keylogger module.[1]

Enterprise T1057 Process Discovery

The discovery modules used with Duqu can collect information on process details.[1]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

Duqu will inject itself into different processes to evade detection. The selection of the target process is influenced by the security software that is installed on the system (Duqu will inject into different processes depending on which security suite is installed on the infected host).[1]

.012 Process Injection: Process Hollowing

Duqu is capable of loading executable code via process hollowing.[1]

Enterprise T1572 Protocol Tunneling

Duqu uses a custom command and control protocol that communicates over commonly used ports, and is frequently encapsulated by application layer protocols.[1]

Enterprise T1090 .001 Proxy: Internal Proxy

Duqu can be configured to have commands relayed over a peer-to-peer network of infected hosts if some of the hosts do not have Internet access.[1]

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

Adversaries can instruct Duqu to spread laterally by copying itself to shares it has enumerated and for which it has obtained legitimate credentials (via keylogging or other means). The remote host is then infected by using the compromised credentials to schedule a task on remote machines that executes the malware.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Adversaries can instruct Duqu to spread laterally by copying itself to shares it has enumerated and for which it has obtained legitimate credentials (via keylogging or other means). The remote host is then infected by using the compromised credentials to schedule a task on remote machines that executes the malware.[1]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

Duqu has used `msiexec` to execute malicious Windows Installer packages. Additionally, a PROPERTY=VALUE pair containing a 56-bit encryption key has been used to decrypt the main payload from the installer packages.[2]

Enterprise T1016 System Network Configuration Discovery

The reconnaissance modules used with Duqu can collect information on network configuration.[1]

Enterprise T1049 System Network Connections Discovery

The discovery modules used with Duqu can collect information on network connections.[1]

Enterprise T1078 Valid Accounts

Adversaries can instruct Duqu to spread laterally by copying itself to shares it has enumerated and for which it has obtained legitimate credentials (via keylogging or other means). The remote host is then infected by using the compromised credentials to schedule a task on remote machines that executes the malware.[1]

ICS T0811 Data from Information Repositories

Duqu downloads additional modules for the collection of data in information repositories, including the Infostealer 2 module that can access data from Windows Shares.[3]

ICS T0893 Data from Local System

Duqu downloads additional modules for the collection of data from local systems. The modules are named: infostealer 1, infostealer 2 and reconnaissance. [3]

ICS T0882 Theft of Operational Information

Duqu's purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, in order to more easily conduct a future attack against another third party.[3]
