Egregor, Software S0554 | MITRE ATT&CK®

Archived: 2026-04-05 14:00:33 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Egregor has communicated with its C2 servers via HTTPS protocol.[4]

Enterprise T1197 BITS Jobs

Egregor has used BITSadmin to download and execute malicious DLLs.[4]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Egregor has used an encoded PowerShell command by a service created by Cobalt Strike for lateral movement.[4]

.003 Command and Scripting Interpreter: Windows Command Shell

Egregor has used batch files for execution and can launch Internet Explorer from cmd.exe.[5][6]

Enterprise T1486 Data Encrypted for Impact

Egregor can encrypt all non-system files using a hybrid AES-RSA algorithm prior to displaying a ransom note.[1] [6]

Enterprise T1039 Data from Network Shared Drive

Egregor can collect any files found in the enumerated drivers before sending it to its C2 channel.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Egregor has been decrypted before execution.[1][6]

Enterprise T1484 .001 Domain or Tenant Policy Modification: Group Policy Modification

Egregor can modify the GPO to evade detection.[6] [4]

Enterprise T1574 .001 Hijack Execution Flow: DLL

Egregor has used DLL side-loading to execute its payload.[2]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Egregor has disabled Windows Defender to evade protections.[4]

Enterprise T1105 Ingress Tool Transfer

Egregor has the ability to download files from its C2 server.[6][4]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Egregor has masqueraded the svchost.exe process to exfiltrate data.[4]

Enterprise T1106 Native API

Egregor has used the Windows API to make detection more difficult.[2]

Enterprise T1027 .002 Obfuscated Files or Information: Software Packing

Egregor's payloads are custom-packed, archived and encrypted to prevent analysis.[1][2]

Enterprise T1069 .002 Permission Groups Discovery: Domain Groups

Egregor can conduct Active Directory reconnaissance using tools such as Sharphound or AdFind.[4]

Enterprise T1055 Process Injection

Egregor can inject its payload into iexplore.exe process.[2]

Enterprise T1219 Remote Access Tools

Egregor has checked for the LogMein event log in an attempt to encrypt files in remote machines.[2]

Enterprise T1218 .010 System Binary Proxy Execution: Regsvr32

Egregor has used regsvr32.exe to execute malicious DLLs.[5]

.011 System Binary Proxy Execution: Rundll32

Egregor has used rundll32 during execution.[6]

Enterprise T1082 System Information Discovery

Egregor can perform a language check of the infected system and can query the CPU information (cupid).[5][1]

Enterprise T1049 System Network Connections Discovery

Egregor can enumerate all connected drives.[1]

Enterprise T1033 System Owner/User Discovery

Egregor has used tools to gather information about users.[4]

Enterprise T1124 System Time Discovery

Egregor contains functionality to query the local/system time.[5]

Enterprise T1497 Virtualization/Sandbox Evasion

Egregor has used multiple anti-analysis and anti-sandbox techniques to prevent automated analysis by sandboxes. [2][1]

.003 Time Based Checks

Egregor can perform a long sleep (greater than or equal to 3 minutes) to evade detection.[5]

Source: https://attack.mitre.org/software/S0554