LightNeuron, Software S0395 | MITRE ATT&CK®

Archived: 2026-04-05 18:22:40 UTC

Enterprise T1071 .003 Application Layer Protocol: Mail Protocols

LightNeuron uses SMTP for C2.[1]

Enterprise T1560 Archive Collected Data

LightNeuron contains a function to encrypt and store emails that it collects.[1]

Enterprise T1119 Automated Collection

LightNeuron can be configured to automatically collect files under a specified directory.[1]

Enterprise T1020 Automated Exfiltration

LightNeuron can be configured to automatically exfiltrate files under a specified directory.[1]

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

LightNeuron is capable of executing commands via cmd.exe.[1]

Enterprise T1005 Data from Local System

LightNeuron can collect files from a local system.[1]

Enterprise T1565 .002 Data Manipulation: Transmitted Data Manipulation

LightNeuron is capable of modifying email content, headers, and attachments during transit.[1]

Enterprise T1001 .002 Data Obfuscation: Steganography

LightNeuron is controlled via commands that are embedded into PDFs and JPGs using steganographic methods.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

LightNeuron can store email data in files and directories specified in its configuration, such as `C:\Windows\ServiceProfiles\NetworkService\appdata\Local\Temp\` .[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

LightNeuron has used AES and XOR to decrypt configuration files and commands.[1]

Enterprise T1114 .002 Email Collection: Remote Email Collection

LightNeuron collects Exchange emails matching rules specified in its configuration.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

LightNeuron uses AES to encrypt C2 traffic.[1]

Enterprise T1041 Exfiltration Over C2 Channel

LightNeuron exfiltrates data over its email C2 channel.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

LightNeuron has a function to delete files.[1]

Enterprise T1105 Ingress Tool Transfer

LightNeuron has the ability to download and execute additional files.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

LightNeuron has used filenames associated with Exchange and Outlook for binary and configuration files, such as `winmail.dat`.[1]

Enterprise T1106 Native API

LightNeuron is capable of starting a process using CreateProcess.[1]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

LightNeuron encrypts its configuration files with AES-256.[1]

Enterprise T1029 Scheduled Transfer

LightNeuron can be configured to exfiltrate data during nighttime or working hours.[1]

Enterprise T1505 .002 Server Software Component: Transport Agent

LightNeuron has used a malicious Microsoft Exchange transport agent for persistence.[1]

Enterprise T1082 System Information Discovery

LightNeuron gathers the victim computer name using the Win32 API call `GetComputerName`.[1]

Enterprise T1016 System Network Configuration Discovery

LightNeuron gathers information about network adapters using the Win32 API call `GetAdaptersInfo`.[1]
