Cyclops Blink, Software S0687 | MITRE ATT&CK®

Archived: 2026-04-05 15:27:03 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Cyclops Blink can download files via HTTP and HTTPS.[1][3]

Enterprise T1037 .004 Boot or Logon Initialization Scripts: RC Scripts

Cyclops Blink has the ability to execute on device startup, using a modified RC script named S51armled.[1]

Enterprise T1132 .002 Data Encoding: Non-Standard Encoding

Cyclops Blink can use a custom binary scheme to encode messages with specific commands and parameters to be executed.[1]

Enterprise T1005 Data from Local System

Cyclops Blink can upload files from a compromised host.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Cyclops Blink can decrypt and parse instructions sent from C2.[1]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

Cyclops Blink can encrypt C2 messages with AES-256-CBC sent underneath TLS. OpenSSL library functions are also used to encrypt each message using a randomly generated key and IV, which are then encrypted using a hard-coded RSA public key.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Cyclops Blink has the ability to upload exfiltrated files to a C2 server.[1]

Enterprise T1083 File and Directory Discovery

Cyclops Blink can use the Linux API `statvfs` to enumerate the current working directory.[1][3]

Enterprise T1562 .004 Impair Defenses: Disable or Modify System Firewall

Cyclops Blink can modify the Linux iptables firewall to enable C2 communication on network devices via a stored list of port numbers.[1][3]

Enterprise T1070 .006 Indicator Removal: Timestomp

Cyclops Blink has the ability to use the Linux API function `utime` to change the timestamps of modified firmware update images.[1]

Enterprise T1105 Ingress Tool Transfer

Cyclops Blink has the ability to download files to target systems.[1][3]

Enterprise T1559 Inter-Process Communication

Cyclops Blink has the ability to create a pipe to enable inter-process communication.[3]

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

Cyclops Blink can rename its running process to `[kworker:0/1]` to masquerade as a Linux kernel thread. Cyclops Blink has also named RC scripts used for persistence after WatchGuard artifacts.[1]

Enterprise T1106 Native API

Cyclops Blink can use various Linux API functions including those for execution and discovery.[1]

Enterprise T1571 Non-Standard Port

Cyclops Blink can use non-standard ports for C2 not typically associated with HTTP or HTTPS traffic.[1]

Enterprise T1542 .002 Pre-OS Boot: Component Firmware

Cyclops Blink has maintained persistence by patching legitimate device firmware when it is downloaded, including that of WatchGuard devices.[1]

Enterprise T1057 Process Discovery

Cyclops Blink can enumerate the process it is currently running under.[1]

Enterprise T1572 Protocol Tunneling

Cyclops Blink can use DNS over HTTPS (DoH) to resolve C2 nodes.[3]

Enterprise T1090 .003 Proxy: Multi-hop Proxy

Cyclops Blink has used Tor nodes for C2 traffic.[2]

Enterprise T1082 System Information Discovery

Cyclops Blink has the ability to query device information.[1]

Enterprise T1016 System Network Configuration Discovery

Cyclops Blink can use the Linux API `if_nameindex` to gather network interface names.[1][3]

Source: https://attack.mitre.org/software/S0687