BLUELIGHT, Software S0657 | MITRE ATT&CK®

Archived: 2026-04-05 18:41:05 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

BLUELIGHT can use HTTP/S for C2 using the Microsoft Graph API.[1]

Enterprise T1560 Archive Collected Data

BLUELIGHT can zip files before exfiltration.[1]

.003 Archive via Custom Method

BLUELIGHT has encoded data into a binary blob using XOR.[1]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

BLUELIGHT can collect passwords stored in web browers, including Internet Explorer, Edge, Chrome, and Naver Whale.[1]

Enterprise T1041 Exfiltration Over C2 Channel

BLUELIGHT has exfiltrated data over its C2 channel.[1]

Enterprise T1083 File and Directory Discovery

BLUELIGHT can enumerate files and collect associated metadata.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

BLUELIGHT can uninstall itself.[1]

Enterprise T1105 Ingress Tool Transfer

BLUELIGHT can download additional files onto the host.[1]

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

BLUELIGHT has a XOR-encoded payload.[1]

Enterprise T1057 Process Discovery

BLUELIGHT can collect process filenames and SID authority level.[1]

Enterprise T1113 Screen Capture

BLUELIGHT has captured a screenshot of the display every 30 seconds for the first 5 minutes after initiating a C2 loop, and then once every five minutes thereafter.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

BLUELIGHT can collect a list of anti-virus products installed on a machine.[1]

Enterprise T1539 Steal Web Session Cookie

BLUELIGHT can harvest cookies from Internet Explorer, Edge, Chrome, and Naver Whale browsers.[1]

Enterprise T1082 System Information Discovery

BLUELIGHT has collected the computer name and OS version from victim machines.[1]

Enterprise T1016 System Network Configuration Discovery

BLUELIGHT can collect IP information from the victim's machine.[1]

Enterprise T1033 System Owner/User Discovery

BLUELIGHT can collect the username on a compromised host.[1]

Enterprise T1124 System Time Discovery

BLUELIGHT can collect the local time on a compromised host.[1]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

BLUELIGHT can check to see if the infected machine has VM tools running.[1]

Enterprise T1102 .002 Web Service: Bidirectional Communication

BLUELIGHT can use different cloud providers for its C2.[1]
