HOPLIGHT, Software S0376 | MITRE ATT&CK®

Archived: 2026-04-05 16:46:37 UTC

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

HOPLIGHT can launch cmd.exe to execute commands on the system.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

HOPLIGHT has utilized Zlib compression to obfuscate the communications payload. [1]

Enterprise T1652 Device Driver Discovery

HOPLIGHT can enumerate device drivers located in the registry at `HKLM\Software\WBEM\WDM`.[1]

Enterprise T1546 .003 Event Triggered Execution: Windows Management Instrumentation Event Subscription

HOPLIGHT can use WMI event subscriptions to create persistence.[1]

Enterprise T1041 Exfiltration Over C2 Channel

HOPLIGHT has used its C2 channel to exfiltrate data.[1]

Enterprise T1008 Fallback Channels

HOPLIGHT has multiple C2 channels in place in case one fails.[1]

Enterprise T1083 File and Directory Discovery

HOPLIGHT has been observed enumerating system drives and partitions.[1]

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

HOPLIGHT has modified the firewall using netsh.[1]

Enterprise T1105 Ingress Tool Transfer

HOPLIGHT has the ability to connect to a remote host in order to upload and download files.[1]

Enterprise T1680 Local Storage Discovery

HOPLIGHT has been observed collecting victim machine volume information.[1]

Enterprise T1112 Modify Registry

HOPLIGHT has modified Managed Object Format (MOF) files within the Registry to run specific commands and create persistence on the system.[1]

Enterprise T1571 Non-Standard Port

HOPLIGHT has connected outbound over TCP port 443 with a FakeTLS method.[1]

Enterprise T1003 .002 OS Credential Dumping: Security Account Manager

HOPLIGHT has the capability to harvest credentials and passwords from the SAM database.[1]

Enterprise T1055 Process Injection

HOPLIGHT has injected into running processes.[1]

Enterprise T1090 Proxy

HOPLIGHT has multiple proxy options that mask traffic between the malware and the remote operators.[1]

Enterprise T1012 Query Registry

A variant of HOPLIGHT hooks lsass.exe, and lsass.exe then checks the Registry for the data value 'rdpproto' under the key `SYSTEM\CurrentControlSet\Control\Lsa Name`.[1]

Enterprise T1082 System Information Discovery

HOPLIGHT has been observed collecting victim machine information like OS version.[1]

Enterprise T1569 .002 System Services: Service Execution

HOPLIGHT has used svchost.exe to execute a malicious DLL .[1]

Enterprise T1124 System Time Discovery

HOPLIGHT has been observed collecting system time from victim machines.[1]

Enterprise T1550 .002 Use Alternate Authentication Material: Pass the Hash

HOPLIGHT has been observed loading several APIs associated with Pass the Hash.[1]

Enterprise T1047 Windows Management Instrumentation

HOPLIGHT has used WMI to recompile the Managed Object Format (MOF) files in the WMI repository.[1]
