Enhanced Attack Report

Jaguar Tooth

Generated on 2025-04-09

Disclaimer

This report has been generated automatically and should be used for informational purposes only. To generate this report, Large Language Models (LLMs) were used to analyze the provided data. This technology is not perfect and may generate incorrect or misleading results. The results should be reviewed by a human expert before taking any action based on the information provided.

Definitions

Pre-Conditions: Conditions that must be true to execute the attack steps in the milestone.

Post-Conditions: Traces that an attacker leaves behind after executing the attack steps in the milestone.

Attack Steps: Steps that an attacker would take to achieve the goal of the milestone.

MITRE Technique: Techniques from the MITRE ATT&CK; framework that are relevant to the milestone.

STIX

Malware Name: Jaguar Tooth
Malware Description: Jaguar Tooth is non-persistent malware that targets Cisco IOS routers. Collects device information and exfiltrates over Trivial File Transfer Protocol (TFTP). Enables unauthenticated backdoor access. It is deployed and executed via exploitation of the patched Simple Network Management Protocol (SNMP) vulnerability CVE-2017-6742.

Quick Overview

Milestone 1
1. Exploit Public-Facing Application as used by the malware (T1190)

Milestone 2
1. Modify Authentication Process as used by the malware (T1556.002)
2. Modify System Image: Patch System Image as used by the malware (T1601.001)

Milestone 3
1. Remote System Discovery as used by the malware (T1018)
2. File and Directory Discovery as used by the malware (T1083)
3. System Network Configuration Discovery as used by the malware (T1016)
4. System Information Discovery as used by the malware (T1082)

Milestone 4
1. Automated Collection as used by the malware (T1005)
2. Data from Configuration Repository: Network Device Configuration Dump as used by the malware (T1602.002)

Milestone 5
1. Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol as used by the malware (T1048.003)
2. Automated Exfiltration as used by the malware (T1020)

Milestone 1

Attack Step 1.1

==========
Name: Exploit Public-Facing Application as used by the malware
Description: The vulnerability designated as CVE-2017-6742 within the Simple Network Management Protocol (SNMP) subsystem of affected devices is exploited by the Jaguar Tooth malware. Exploitation is initiated through the transmission of a specially crafted SNMP packet to an exposed SNMP service on the target device, leveraging the buffer overflow vulnerability inherent in the SNMP software. Successful exploitation results in the granting of remote code execution privileges to the attacker on the target system. This enables the execution of arbitrary commands and malicious code. Furthermore, write access is provided to the target operating system, facilitating file modification, the installation of additional malware, or the creation of persistent backdoors. Following the establishment of remote code execution and write access, the Jaguar Tooth payload is deployed onto the vulnerable device. The vulnerability is exploited through an exposed SNMP service functioning as a public-facing application. The exploit affects various operating systems contingent upon the software implementing the vulnerable SNMP functionality. All versions of SNMP (1, 2c, and 3) are susceptible to this specific exploit.

Pre-Conditions:

- The application has a vulnerability exploitable by the malware.
- A public-facing application is accessible.

Post-Conditions:

- Network disruption
- New files created by the attacker
- System event logs recording unauthorized access attempts
- Altered process lists with unknown processes running
- Data exfiltration
- Network traffic analysis showing communication with malicious servers
- Denial of service
- Modified system configuration files
- Firewall logs indicating blocked or suspicious connections
- System compromise
- Remote code execution
- SNMP log entries with unusual activity

MITRE Technique

ID: T1190
Name: Exploit public-facing application
Description: Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.
More info: https://attack.mitre.org/techniques/T1190/

Indicators

- A malicious actor attempts to exploit a public-facing application.

Milestone 2

Attack Step 2.1

==========
Name: Modify Authentication Process as used by the malware
Description: Cisco IOS device authentication processes are subject to modification by the Jaguar Tooth malware. Two specific authentication functions are targeted for patching by the malware. These modifications enable unauthenticated access to local accounts via both Telnet and physical console sessions. The malware identifies target authentication functions responsible for credential verification during Telnet and physical login attempts. Malicious code is injected into these functions, resulting in alterations to their normal behavior. The patched functions are configured to bypass password checks, allowing an attacker to gain access to the device by entering any username. This compromises the authentication process, granting unfettered access to sensitive system information and potentially facilitating further malicious activities.

Pre-Conditions:

- The target device runs Cisco IOS software.
- The malware has access to the target device's memory.
- Network connectivity exists between the compromised device and a command-and-control server (implied).
- A running instance of the Jaguar Tooth malware is present on the target device.

Post-Conditions:

- Network traffic containing Jaguar Tooth payload
- Modified system image
- Compromised system authentication
- Logs of unauthorized access attempts and successful logins
- Data exfiltration
- Files containing extracted code and data from network traffic
- Modified Cisco IOS authentication functions
- Patches in the system image memory
- Unauthenticated access to local accounts

MITRE Technique

ID: T1556.002
Name: Modify authentication process: password filter dll
Description: Adversaries may register malicious password filter dynamic link libraries (DLLs) into the authentication process to acquire user credentials as they are validated.
More info: https://attack.mitre.org/techniques/T1556/002

Indicators

- The content contains "| 2 b 0 6 0 1 0 4 0 1 0 9 0 9 5 f 0 1 0 2 0 4 0 1 0 3 |".
- The content contains "| 0 3 8 1 6 0 0 0 0 8 |".
- The content contains "| 2 4 0 2 0 0 0 1 |".

Attack Step 2.2

==========
Name: Modify System Image: Patch System Image as used by the malware
Description: The "Modify System Image: Patch System Image" action executed by the Jaguar Tooth malware involves the exploitation of a stack-based buffer overflow vulnerability within Cisco IOS software. This vulnerability is triggered during the processing of extended Object Identifiers (OIDs) associated with Simple Network Management Protocol (SNMP) operations. Return Oriented Programming (ROP) techniques are utilized by the malware to exploit the identified vulnerability. ROP involves the identification and chaining of existing code snippets ("gadgets") within vulnerable memory regions to execute malicious instructions. Through a series of ROP-driven manipulations, critical portions of the running system image are overwritten. This patching process enables the bypassing of authentication checks implemented for Telnet and physical console connections. The successful execution of this action grants near-complete control over the infected Cisco device to the attacker.

Pre-Conditions:

- The ability to execute code on the target system.
- Knowledge of the CVE-2017-6742 vulnerability and its exploitation method.
- The target system is running Cisco IOS or Cisco IOS XE software.
- A working connection to the target system.
- Access to the target system.
- A vulnerability exists in the SNMP subsystem of the target system (CVE-2017-6742).

Post-Conditions:

- Log entries indicating Telnet and physical session logins without password verification
- Modified system image
- Compromised system authentication
- Exfiltration of device configuration data
- Potential for remote code execution
- Altered authentication functions
- Unauthorized access to local accounts
- Snort alert logs matching the signature for Jaguar Tooth payload deployment
- Network traffic containing the dumped device configuration
- Files containing extracted malware code from network traffic.
- Presence of malicious code in memory

MITRE Technique

ID: T1601.001
Name: Modify system image: patch system image
Description: Adversaries may modify the operating system of a network device to introduce new capabilities or weaken existing defenses. Some network devices are built with a monolithic architecture, where the entire operating system and most of the functionality of the device is contained within a single file. Adversaries may change this file in storage, to be loaded in a future boot, or in memory during runtime.
More info: https://attack.mitre.org/techniques/T1601/001

Indicators

- The content contains "| 03 81 60 00 0 8 |".

- The content contains "| 24 02 00 0 1 |".

Milestone 3

Attack Step 3.1

==========
Name: Remote System Discovery as used by the malware
Description: Remote system discovery within Jaguar Tooth is effectuated through the utilization of Cisco IOS CLI commands. These commands are employed to acquire data pertaining to ARP entries, facilitating the establishment of IP-to-MAC address mappings and identification of interconnected devices on the network infrastructure.

Pre-Conditions:

- The Jaguar Tooth malware.
- The malware has successfully gained access to a Cisco IOS device.
- Access to the Cisco IOS CLI.
- The Cisco IOS device is connected to a network.

Post-Conditions:

- System logs containing unusual activity related to executed commands
- Snort alert logs indicating payload deployment
- Altered Cisco IOS configuration files
- Modified device running configuration
- Compromised system configuration
- TFTP server logs with evidence of data transfer
- Presence of malicious code within Cisco IOS memory
- Network traffic analysis revealing communication with command and control servers
- Modified ARP table entries reflecting discovered devices
- Potential for further malware deployment
- Exfiltrated sensitive data

MITRE Technique

ID: T1018
Name: Remote system discovery
Description: Adversaries may attempt to get a listing of other systems by IP address, hostname, or other logical identifier on a network that may be used for Lateral Movement from the current system. Functionality could exist within remote access tools to enable this, but utilities available on the operating system could also be used such as Ping or net view using Net.
More info: https://attack.mitre.org/techniques/T1018/

Indicators

- The content contains " | 03 81 60 00 08 | ".
- The content contains " | 24 02 00 01 | ".

Attack Step 3.2

==========
Name: File and Directory Discovery as used by the malware
Description: File and directory discovery within the target system is executed by the malware, Jaguar Tooth, leveraging a Cisco IOS CLI command. The enumeration of local flash filesystem contents is performed through this specific command.

Pre-Conditions:

- The target device runs Cisco IOS software.
- Network connectivity exists between the malware and the target device.
- The malware has access to a command line interface on the target device.

Post-Conditions:

- Altered SNMP configuration settings
- Remote access to compromised devices
- Modified ARP table entries
- Data exfiltration
- Modified device configuration files (e.g., running-config)
- Exfiltrated data files (e.g., TFTP transfers)
- Network traffic logs showing unusual activity (e.g., connections to command and control servers, data exfiltration)
- Compromised system configuration
- Potential for further malware deployment
- Presence of Snort alert logs indicating Jaguar Tooth payload deployment
- Presence of malicious code in memory or on disk

MITRE Technique

ID: T1083
Name: File and directory discovery
Description: Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from File and Directory Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
More info: https://attack.mitre.org/techniques/T1083/

Indicators

- The content " | 03 81 60 00 08 |" is present.
- The content "| 24 02 00 01 |" is present.

Attack Step 3.3

==========
Name: System Network Configuration Discovery as used by the malware
Description: Cisco IOS malware designated as "Jaguar Tooth" obtains system network configuration details through the execution of various Cisco IOS CLI commands. The specific commands employed remain undisclosed; however, their functionality suggests the acquisition of information pertaining to: - IP addresses assigned to the infected device, encompassing both internal and external identifiers. - Network masks delineating subnet boundaries and defining the range of utilizable IP addresses within a network. - Default gateway configurations identifying the router responsible for directing traffic external

to the local network. - DNS server addresses utilized for domain name resolution into corresponding IP addresses. Analysis of the command output generated by Jaguar Tooth enables the construction of a comprehensive network topology map centered on the infected device. This mapping may facilitate the identification of potential targets for subsequent exploitation endeavors.

Pre-Conditions:

- The malware has access to a command line interface on the target system.
- A Cisco IOS device with network configuration information.
- The target system is running Cisco IOS software.

Post-Conditions:

- Altered SNMP OID values
- Compromised system network configuration
- Exfiltration of sensitive system information
- Potential for further exploitation of vulnerabilities
- Log entries indicating suspicious CLI commands execution
- Network traffic containing Jaguar Tooth payload data
- Evidence of exploitation attempts in system logs
- Unusual network connections to external IP addresses
- Presence of malicious code within Cisco IOS memory
- Buffer overflow artifacts in system memory
- Deployment of malicious payloads and patches
- New files or modified existing files containing malware components
- Modified Cisco IOS configurations

MITRE Technique

ID: T1016
Name: System network configuration discovery
Description: Adversaries may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems. Several operating system administration utilities exist that can be used to gather this information. Examples include Arp, ipconfig/ifconfig, nbtstat, and route.
More info: https://attack.mitre.org/techniques/T1016/

Indicators

- The content contains " | 03 81 60 00 08 | ".
- The content contains " | 24 02 00 01 | ".

Attack Step 3.4

==========
Name: System Information Discovery as used by the malware
Description: System Information Discovery is performed by the Jaguar Tooth malware through the execution of various Cisco IOS CLI commands. These commands are instrumental in retrieving details pertaining to the infected device's configuration and software environment. Information regarding network interfaces, including their names, MAC addresses, and IP configurations, is obtained. Additionally, details concerning the running software version of the Cisco IOS operating system are acquired. The compilation of this comprehensive profile facilitates the malware's subsequent malicious

activities.

Pre-Conditions:

- The target device is running Cisco IOS software.
- Access to the target device's CLI.
- The malware has access to the target device's command line interface (CLI).
- The malware must have the capability to execute Cisco IOS CLI commands.

Post-Conditions:

- Remote access to compromised devices
- Unusual network traffic patterns
- Compromised system network configuration
- Network connections to command-and-control servers
- Exfiltration of sensitive data
- Presence of malicious code in device memory
- Log entries indicating suspicious activity
- Altered file timestamps and permissions
- New files containing malware or stolen data
- System instability and performance degradation
- Modified Cisco IOS configurations

MITRE Technique

ID: T1082
Name: System information discovery
Description: An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.
More info: https://attack.mitre.org/techniques/T1082/

Indicators

- The content contains " | 03 81 60 00 08 | ".
- The content contains " | 24 02 00 01 | ".

Milestone 4

Attack Step 4.1

==========
Name: Automated Collection as used by the malware
Description: Jaguar Tooth employs an automated methodology for system information acquisition from targeted Cisco IOS devices. A predefined set of Cisco IOS CLI commands and Tcl scripts are utilized to retrieve device configurations, running processes, and other pertinent data. Automated execution of these pre-scripted commands facilitates data collection without requiring manual intervention from an attacker. The acquired results are subsequently transferred to a remote server via the TFTP protocol, enabling exfiltration of information while minimizing traces on the compromised device.

Pre-Conditions:

- The malware is active and executing its code.
- A Cisco IOS device with network connectivity.
- A hard-coded list of Cisco IOS CLI and Tcl commands exists within the malware.
- TFTP server accessible to the infected device.
- The malware is running within a Cisco IOS device's memory.

Post-Conditions:

- Altered ARP table entries reflecting compromised devices
- Presence of malicious code within router memory
- Exfiltration of sensitive device information
- TFTP server logs containing exfiltrated data
- Potential for unauthorized access and control
- Increased risk of further attacks
- Snort alert logs indicating detection of Jaguar Tooth activity
- Compromised Cisco IOS routers
- Network traffic analysis revealing communication with malicious servers
- Modified router configuration files

MITRE Technique

ID: T1005
Name: Data from local system
Description: Adversaries may search local system sources, such as file systems and configuration files or local databases, to find files of interest and sensitive data prior to Exfiltration.
More info: https://attack.mitre.org/techniques/T1005/

Indicators

- The content contains " | 0 3 8 1 6 0 0 0 0 8 | ".
- The content contains " | 2 4 0 2 0 0 0 1 | ".

Attack Step 4.2

==========
Name: Data from Configuration Repository: Network Device Configuration Dump as used by the malware
Description: The "Data from Configuration Repository: Network Device Configuration Dump" action, executed by the Jaguar Tooth malware, involves the utilization of a Cisco IOS CLI command to retrieve the device's running configuration. This process results in the acquisition of all settings and parameters currently active on the targeted device.

Pre-Conditions:

- The target device is running Cisco IOS software.
- Access to the target device's CLI.
- The malware has access to the target device's command line interface (CLI).

Post-Conditions:

- Altered SNMP OID values
- Presence of malicious files or processes within device memory
- Unusual network traffic patterns (e.g., data transfers to malicious servers)
- Log entries indicating suspicious activity (e.g., failed login attempts, unauthorized access)
- Data exfiltration
- Network connections to known malicious IP addresses
- Remote code execution on vulnerable devices
- Compromised network configuration
- System instability
- Snort alert logs capturing the Jaguar Tooth payload deployment
- Modified Cisco IOS configurations

MITRE Technique

ID: T1602.002
Name: Data from configuration repository: network device configuration dump
Description: Adversaries may access network configuration files to collect sensitive data about the device and the network. The network configuration is a file containing parameters that determine the operation of the device. The device typically stores an in-memory copy of the configuration while operating, and a separate configuration on non-volatile storage to load after device reset. Adversaries can inspect the configuration files to reveal information about the target network and its layout, the network device and its software, or identifying legitimate accounts and credentials for later use.
More info: https://attack.mitre.org/techniques/T1602/002

Indicators

- The content " | 2 b 0 6 0 1 0 4 0 1 0 9 0 9 5 f 0 1 0 2 0 4 0 1 0 3 |" is transmitted.
- The content "| 0 3 8 1 6 0 0 0 0 8 |" is transmitted.
- The content "| 2 4 0 2 0 0 0 1 |" is transmitted.

Milestone 5

Attack Step 5.1

==========
Name: Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol as used by the malware
Description: The malware Jaguar Tooth transmits gathered device data to a designated server via the Trivial File Transfer Protocol (TFTP). The inherent characteristic of TFTP as an unencrypted protocol renders the data exchange susceptible to interception during transmission between the infected device and the server.

Pre-Conditions:

- A TFTP server accessible from the compromised router.
- A compromised Cisco router with Jaguar Tooth malware installed.
- The target device's network configuration allows for TFTP communication.
- An active internet connection on the compromised router.
- The malware has successfully gained access to the target device.
- The target device is running a Cisco IOS operating system.

Post-Conditions:

- Network traffic analysis showing communication with C2 servers
- Compromised system security
- Altered ARP table entries
- Data exfiltration
- Unusual system activity logs
- Modified device information files
- Snort alert logs
- System instability
- Presence of malicious code in memory
- Remote access vulnerability
- TFTP server logs with data transfers
- Modified Cisco IOS configuration files

MITRE Technique

ID: T1048.003
Name: Exfiltration over alternative protocol: exfiltration over unencrypted non-c2 protocol
Description: Adversaries may steal data by exfiltrating it over an un-encrypted network protocol other than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.
More info: https://attack.mitre.org/techniques/T1048/003

Indicators

- The malware utilizes UDP for communication.
- The malware communicates over unencrypted channels.

Attack Step 5.2

==========
Name: Automated Exfiltration as used by the malware
Description: Automated exfiltration within the Jaguar Tooth malware framework is facilitated by a predefined set of Cisco IOS CLI and Tcl commands. These commands are injected into vulnerable Cisco IOS systems for the purpose of data retrieval. The retrieved data may encompass network configuration details, system logs, or other sensitive information. Subsequently, the extracted data is transferred to a remote server via the TFTP protocol, enabling exfiltration outside the compromised network perimeter.

Pre-Conditions:

- The infected Cisco IOS router has a list of hard-coded Cisco IOS CLI and Tcl commands for data collection.
- The Cisco IOS router is vulnerable to exploitation by Jaguar Tooth malware.
- A TFTP server is accessible from the infected Cisco IOS router.

Post-Conditions:

- Presence of malicious code in router memory
- System logs recording execution of suspicious commands
- Snort alert logs indicating signature matches
- ARP table modifications reflecting device discovery attempts
- Network traffic analysis revealing unusual communication patterns
- Exfiltration of sensitive device information
- Potential for unauthorized access and control
- Increased risk of further attacks
- Compromised Cisco IOS routers
- TFTP server logs showing data transfers
- Modified Cisco IOS configuration files

MITRE Technique

ID: T1020
Name: Automated exfiltration
Description: Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.
More info: https://attack.mitre.org/techniques/T1020/

Indicators

- The content contains "| 03 81 60 00 0 8 |".
- The content contains "| 24 02 00 0 1 |".