Enhanced Attack Report

Jaguar Tooth

Generated on 2025-03-27

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

Pre-Conditions:

- The target system has a public-facing application vulnerable to exploitation.
- A network connection to the target system.
- The malware executable.
- Knowledge of the target system's IP address or domain name.
- The malware is capable of exploiting the vulnerability in the target application.

Post-Conditions:

- Modified configuration files
- Unusual network traffic patterns
- Altered routing tables
- Malware deployment
- Network disruption
- New files created by malware
- Loss of system functionality
- Data exfiltration
- Presence of malicious code in memory
- System compromise
- SNMP log entries

Attack Step 1.1

==========
Name: Exploit Public-Facing Application as used by the malware
Description: Vulnerable systems are identified through scans targeting open SNMP ports (typically UDP port 161) on public IP addresses. Exploitation of affected systems is achieved by transmitting a crafted SNMP packet designed to leverage the CVE-2017-6742 vulnerability, which involves a buffer overflow condition within the SNMP subsystem. Successful exploitation results in remote code execution, enabling the execution of arbitrary code within the context of the target system's operating system. Remote code execution often grants write access, facilitating file modification, tool installation, and establishment of persistence on compromised systems.

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

Pre-Conditions:

- The target device is accessible via Telnet or physical session.
- A running instance of the Jaguar Tooth malware is present on the target device.
- The target device runs Cisco IOS software.
- The malware has access to the target device's memory.
- Network connectivity between the attacker and the target device.
- The malware has the capability to modify memory.
- The system image is accessible in memory.
- The malware must be able to execute code on the target device.
- A vulnerable Cisco IOS or IOS XE device running SNMP.

Post-Conditions:

- Network traffic logs showing communication with malicious IP addresses.
- Presence of backdoor tools or modified system binaries.
- Potential for data exfiltration and manipulation.
- Traces of buffer overflow exploits in system memory or log files.
- Unusual file activity, such as creation of new files or modification of existing ones.
- Modified device configuration files.
- Compromised system authentication processes.
- Altered system logs indicating unauthorized access attempts and successful logins.
- Unauthorized access to device configuration and sensitive information.
- Increased risk of further attacks and malware infections.
- New user accounts created
- SNMP log entries with unusual activity
- Modified system registry settings
- Unusual file access patterns
- Network traffic analysis showing communication with malicious IPs
- Modified system configuration
- Data exfiltration
- Remote code execution
- Authentication bypass
- Modified device configuration files
- Altered authentication logs
- Presence of malware in system memory or storage
- System compromise

Attack Step 2.1

==========

Name: Modify Authentication Process as used by the malware
Description: The malware, Jaguar Tooth, modifies system authentication processes to facilitate unauthenticated access to local accounts for both Telnet and physical sessions. This modification involves direct alteration of two authentication functions responsible for credential validation during Telnet and physical connections. The core functionality of these patched functions is modified to disable standard password verification procedures. Consequently, any provided password, irrespective

of its validity, is accepted as correct. This results in unrestricted access to local accounts and system resources via Telnet or physical connections, utilizing any username without encountering authentication barriers.

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

Attack Step 2.2

==========
Name: Modify System Image: Patch System Image as used by the malware
Description: The malware "Jaguar Tooth" modifies system image memory to circumvent user authentication processes. A vulnerability within the system image, triggered by manipulation of specific OID data transmitted via the SNMP protocol, results in a stack-based buffer overflow. Return Oriented Programming (ROP) is employed by "Jaguar Tooth" to overwrite operating system memory. This technique utilizes existing code snippets ("gadgets") within the target's memory to execute malicious instructions incrementally. The overwritten memory effectively disables standard user authentication procedures, granting "Jaguar Tooth" unauthorized access to system functions.

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

Pre-Conditions:

- The malware has access to Cisco IOS CLI commands.
- The target network is accessible.
- A Cisco IOS device exists on the target network.
- The malware has access to a command line interface (CLI) on the target device.
- The target device runs Cisco IOS software.
- The target device is a Cisco router.
- A compromised Cisco router.
- Connectivity to the TFTP server for exfiltrating data.
- The malware has access to the target device's command line interface (CLI).
- The Jaguar Tooth malware.
- A network connection exists between the malware and the target device.
- The malware has access to a Cisco IOS CLI interface.
- The target device is running Cisco IOS software.

Post-Conditions:

- Log entries indicating unusual activity (e.g., unauthorized access attempts, file modifications)
- Modified ARP table entries
- Presence of malicious files or code on the system
- Exfiltrated sensitive data
- SNMP log entries indicating suspicious OID requests and responses
- Modified system software
- Altered device configuration files
- Increased vulnerability to further attacks
- Network traffic logs showing communication with external servers
- Compromised system configuration
- Presence of malicious scripts or backdoors on the device
- Network traffic logs showing communication with attacker's TFTP server
- Altered system event logs
- Modified device configuration files
- Increased vulnerability to further attacks
- Potential for remote code execution
- Access logs indicating unauthorized login attempts
- Exfiltration of sensitive data
- Compromised system configuration
- TFTP server logs with exfiltrated data
- Exfiltration of sensitive device information
- System event logs recording suspicious activity
- TFTP server logs with evidence of data transfer
- Altered ARP table entries
- Modified device configuration files
- New files created on the device containing exfiltrated data
- Increased risk of further attacks
- Potential for malware deployment and execution
- Compromised system configuration
- Network traffic logs showing communication with external IP addresses

- Increased vulnerability to future attacks
- Altered SNMP settings
- Presence of malicious payloads or patches
- Access logs showing unauthorized login attempts
- Modified device configuration files
- Potential for remote code execution
- Logs containing unusual activity and commands
- Changes to routing tables and firewall rules
- Exfiltration of sensitive data
- Compromised system configuration
- Network traffic indicative of data exfiltration
- Files created or modified by the attacker

Attack Step 3.1

==========

Name: Remote System Discovery as used by the malware
Description: Remote system discovery is conducted by the malware through the execution of Cisco IOS CLI commands. Information regarding connected devices is retrieved via these commands, encompassing: - ARP tables, which delineate the association between IP addresses and MAC addresses on the network. - Routing tables, which disclose the routes utilized by the device to access distinct networks. - Interface information, providing details such as names, IP addresses, and operational status of active network interfaces. Analysis of data obtained through CLI commands enables the malware to construct a local network map and identify potential targets for subsequent attacks.

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 on target systems is conducted by the "Jaguar Tooth" malware through the exploitation of a Cisco IOS CLI command. The specific command employed remains undisclosed, but its utilization suggests the malware leverages Cisco IOS functionalities to enumerate files and directories within the flash filesystem.

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 CLI commands are employed by the malware to ascertain information pertaining to the target system's network configuration. Commands such as "show running-config," "show ip interface brief," and "show ip route" are utilized to retrieve details regarding the router's configuration, interface status and IP addresses, and routing table information, respectively. The execution of these and other CLI commands enables the malware to construct a comprehensive understanding of the target network's topology, configuration parameters, and potential security weaknesses.

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 utilization of various Cisco IOS CLI commands. These commands enable the retrieval of details pertaining to the target device's interfaces and software versioning. Information regarding network interfaces, including names, MAC addresses, IP addresses, and status, can be obtained. Additionally, the running software version of Cisco IOS on the target device is ascertainable through these commands.

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

Milestone 4

Pre-Conditions:

- A Cisco IOS router is present in the environment.
- A running instance of the Jaguar Tooth malware exists on the target Cisco IOS router.
- The target Cisco IOS router is connected to a network with TFTP server access.
- The target Cisco IOS router has enabled SNMP.
- A compromised Cisco network device running Cisco IOS software.
- The "Jaguar Tooth" malware.
- The target network device is running Cisco IOS software.
- The malware has access to the target network device.

Post-Conditions:

- Presence of malicious code in router memory
- Data breach
- Logs of executed Cisco IOS CLI commands
- Network traffic logs showing TFTP transfers
- Compromised device configuration
- Backdoor access established on the compromised device
- Unauthorized access to network resources
- Potential for further malware infection
- System instability
- Exfiltrated TFTP data containing device information
- Altered ARP table entries
- Modified Cisco IOS configuration files
- Presence of malicious files or scripts on the affected system
- SNMP log entries indicating unauthorized access attempts
- Network traffic logs showing data exfiltration
- Altered system timestamps and event logs
- Modified device configuration files
- Increased vulnerability to further attacks
- Potential for remote code execution
- Unusual network connections to external IP addresses
- Exfiltration of sensitive data
- Compromised system configuration

Attack Step 4.1

==========

Name: Automated Collection as used by the malware
Description: The "Jaguar Tooth" malware employs an automated data collection process characterized by the execution of predefined Cisco IOS CLI and Tcl commands against target devices. The results of these command executions are subsequently transferred to a remote server via TFTP protocol. This mechanism facilitates the exfiltration of sensitive information from targeted network devices.

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: A Cisco IOS CLI command is utilized by the malware to extract and retrieve a copy of the active running configuration from the target device. This "configuration dump" provides the malware with insights into the device's settings, potentially revealing sensitive information such as firewall rules, authorized users, and network 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

Pre-Conditions:

- An active TFTP server is accessible from the compromised device.
- A compromised Cisco router with the vulnerability CVE-2017-6742 exploited.
- An SNMP exploit has been successfully executed on the target device.
- The malware "Jaguar Tooth" has gained remote code execution and write access on the target operating system.
- The target device is running a vulnerable version of Cisco IOS or IOS XE software.
- A Cisco IOS device is present in the network.
- A hard-coded list of Cisco IOS CLI and Tcl commands exists within the malware.
- Network connectivity between the infected Cisco IOS device and a remote server.
- The malware has successfully gained access to the target Cisco IOS device.

Post-Conditions:

- TFTP server logs showing data transfers
- Data exfiltration from targeted devices
- SNMP log entries indicating unauthorized access attempts
- Network traffic analysis revealing communication with C2 servers
- Potential for further malicious activity
- Modified device configurations on affected routers
- Altered ARP tables reflecting connected devices
- Presence of malicious code within router firmware
- Backdoor access established on compromised devices
- New files or directories created on affected devices containing stolen data
- Compromised Cisco IOS routers
- System logs capturing execution of malicious commands
- Increased vulnerability to future attacks
- Presence of malicious software on affected devices
- Altered SNMP community strings
- Exfiltrated sensitive device information
- Network traffic logs showing communication with attacker's infrastructure
- Buffer overflow errors in system logs
- Access logs indicating unauthorized access attempts
- Modified device configuration files
- Potential for remote code execution
- TFTP server logs with exfiltrated data
- Data breaches
- Compromised device configurations

Attack Step 5.1

==========

Name: Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol as used by the malware
Description: Device information collected by the malware is exfiltrated via TFTP, an unencrypted protocol.

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 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 5.2

==========
Name: Automated Exfiltration as used by the malware
Description: Automated data exfiltration is facilitated by the malware's utilization of a predetermined set of Cisco IOS CLI and Tcl commands, executed autonomously on compromised devices. The resultant output generated from these command executions is transmitted externally via the TFTP protocol.

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 |".