



Man-in-the-Network:
Network Devices are Endpoints Too

Router> show whoami

ABOUT ME

!

10+ years in information security for government and military

Threat Hunting and Incident Response

Detection Engineering

Engineering data pipelines for eventlog collection

!

 twitter.com/c2defense

 github.com/c2defense

 medium.com/@c2defense



Austin Clark
Security Engineer

U.S. Army

```
Router> banner login
```

```
#
```

```
"The views expressed in this presentation are those of the author  
and do not reflect the official policy or position of the US Army,  
Department of Defense or the US Government."
```

```
#
```

Router> show startup-config

Network Device Targeting

Network Infrastructure

Vulnerability

Threat

!

MITRE ATT&CK

Overview

Techniques

!

Detections

Logging

Analytics

Tuning

!

Mitigations

Router> show cdp neighbors

Network Devices

Routers, Switches, VPN, Firewalls, Wireless LAN Controllers, Access Points

Any infrastructure device that provides that backbone network for connectivity

Not necessarily Linux based

Applicable to varying vendors

Yes they provide a service, but they are still endpoints that can be exploited by an adversary.

!

How can we detect an adversary in a network device?

!

We must assume that they will circumvent the protection measures we put in place and still engineer detections.

!

Router> show version

Have you patched? **Cisco IOS has 521 CVEs**

Network devices are slowly patched, and the hardware is rarely upgraded. Some devices may no longer be vendor supported.

No Anti-Virus

Multi-Factor Authentication is not common

Have you changed default credentials?

Are the configurations hardened against internal devices? The gateway of a compromised workstation is a great pivot point.

!

Have you disabled cisco smart install on all devices?

Smart install is one of the most common network device exploits out today; there are many writeups on how to exploit it, commonly referencing <https://github.com/Sab0tag3d/SIET>.

!

Router> show ip sockets

Advanced Persistent Threats are:

- Exploiting network device vulnerabilities

- Extracting device configurations

- Harvesting credentials

- Modifying configurations to redirect or block traffic

- Replacing the IOS firmware

!

SYNFul Knock, Dragonfly 2.0/Berserk Bear, Gekko Jackal

!

https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html

<https://www.darkreading.com/endpoint/privacy/russian-apt-compromised-cisco-router-in-energy-sector-attacks/d/d-id/1331306>

<https://go.crowdstrike.com/rs/281-OBQ-266/images/15GlobalThreatReport.pdf>

<http://2015.zeronights.org/assets/files/05-Nosenko.pdf>

Router> enable



<https://attack.mitre.org/>

!

"The adversary behavior model for Network Infrastructure Devices is being developed with routers, switches, and firewalls in mind...targeting an initial release of our research in the fall [2020]"

<https://medium.com/mitre-attack/2020-attack-roadmap-4820d30b38ba>

!

ATT&CK Enterprise matrix currently comprises Windows, macOS, & Linux

Working towards network infrastructure subset

!

75 current techniques can apply to networking devices

https://github.com/c2defense/network-device-logs/tree/master/mitre_attack

!

Router> show run **MITRE** | **ATT&CK**[®]

Label	Tactic	Technique	Sub-Technique	Data Sources	Example Commands	Comments
T1565.002	Impact	Data Manipulation	Transmitted Data Manipulation	Accounting	access-list * ip access-group *	An adversary might modify data in transit from other hosts, by modifying the configuration on a network device. They might change an ACL so the data doesn't get to it's intended destination, or change the QOS so the service delivery isn't what was originally intended. You'll want to whitelist the known authorized access list's in your baseline config.
T1074.001	Collection	Data Staged	Local Data Staging	Accounting	append * mkdir	Create or edit a file or directory locally
T1560.001	Collection	Archive Collected Data	Archive via Utility	Accounting	archive tar /create	Network devices support compressing and decompressing files to the file system.
T1490	Impact	Inhibit System Recovery		Accounting	archive maximum 1	As T1488 already covers deleting files off the filesystem, I take this technique as referring to deleting backup configurations. If the administrators are archiving locally and the adversary doesn't want to directly delete the files, they could change the maximum number of archive configurations that are kept. (A logic bomb could be done here).
T1551.003	Defense Evasion	Indicator Removal on Host	Clear Command History	Accounting	clear cli history clear archive *	A definite evasion technique, clearing the log is not often done by regular administrators and would be a good indicator of someone trying to hide.
T1551.002	Defense Evasion	Indicator Removal on Host	Clear Linux or Mac System Logs	Accounting	clear logging *	Adversaries may clear or alert the event logs to remove data indicating their presence on the system

Router# configure terminal

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Exploit Public-Facing Application	Command and Scripting Interpreter	Create Account	Event Triggered Execution	Exploitation for Defense Evasion	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
External Remote Services	Python	Local Account	Exploitation for Privilege Escalation	Impair Defenses	Password Guessing	Local Account	Lateral Tool Transfer	Archive via Utility	Web Protocols	Data Transfer Size Limits	Data Destruction
Replication Through Removable Media	Native API	Event Triggered Execution	Scheduled Task/Job	Indicator Removal on Host	Password Cracking	File and Directory Discovery	Remote Service Session Hijacking	Automated Collection	File Transfer Protocols	Exfiltration Over C2 Channel	Data Manipulation
Supply Chain Compromise	Scheduled Task/Job	External Remote Services	Cron	Clear Linux or Mac System Logs	Password Spraying	Network Service Scanning	SSH Hijacking	Data Staged	Traffic Signaling	Exfiltration Over Physical Medium	Stored Data Manipulation
Compromise Software Dependencies and Development Tools	Cron	Pre-OS Boot	Valid Accounts	Clear Command History	Credential Stuffing	Network Sniffing	Remote Services	Local Data Staging	Port Knocking	Exfiltration over USB	Transmitted Data Manipulation
Compromise Software Supply Chain		System Firmware	Default Accounts	File Deletion	Exploitation for Credential Access	Password Policy Discovery	SSH	Remote Data Staging	Web Service	Scheduled Transfer	Disk Wipe
Compromise Hardware Supply Chain		Scheduled Task/Job	Local Accounts	Pre-OS Boot	Network Sniffing	Process Discovery	Replication Through Removable Media	Data from Local System	Dead Drop Resolver		Disk Content Wipe
Valid Accounts		Cron		System Firmware	Unsecured Credentials	Remote System Discovery		Data from Removable Media	One-Way Communication		Disk Structure Wipe
Default Accounts		Server Software Component		Subvert Trust Controls	Credentials In Files	System Information Discovery					Endpoint Denial of Service
Local Accounts		Web Shell		Install Root Certificate	Bash History	System Network Configuration Discovery					Service Exhaustion Flood
		Traffic Signaling		Traffic Signaling	Private Keys	System Network Connections Discovery					Firmware Corruption
		Port Knocking		Port Knocking		System Owner/User Discovery					Inhibit System Recovery
		Valid Accounts		Valid Accounts		System Time Discovery					Network Denial of Service
		Default Accounts		Default Accounts							Direct Network Flood
		Local Accounts		Local Accounts							System Shutdown/Reboot

legend

- High - Accounting
- Medium - Accounting
- Low - Accounting
- Device Syslog (1-7)
- Authentication Logs
- Netflow, IDS

Router(config)# logging traps 6

Ensure logs are centralized

Syslog can have errors from
failed/successful exploitation

Log local authentications

Use archive to log commands locally
without AAA

!

Authentication Authorization
Accounting (AAA)

Accounting logs contain command-line
input

Authentications are good for
correlation

!

Example configuration:

```
archive
  log config
    logging enable
    logging size 500
    hidekeys
    notify syslog
logging enable
logging timestamp
logging host interface1 192.168.0.1 tcp/10514 format emblem
logging traps 6
```

<http://itknowledgeexchange.techtarget.com/cisco/tracking-configuration-changes-with-the-cisco-ios-built-in-using-the-archive-command/>

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/Baseline_Security/securebasebook/appendxA.html

<https://tacacs.net/>

Router(config) # monitor event-trace

Sigma by Florian Roth

<https://github.com/Neo23x0/sigma/tree/master/rules/network/cisco/aaa>

Data Collection/Discovery

show *

monitor capture point

set rspan

!

95 suspicious commands can be mapped to a technique

!

11 Sigma Rules

!

```
title: Cisco Sniffing
id: b9e1f193-d236-4451-aaae-2f3d2102120d
status: experimental
description: Show when a monitor or a span/rspan is setup or modified
references:
  - https://attack.mitre.org/techniques/T1040
author: Austin Clark
date: 2019/08/11
tags:
  - attack.credential_access
  - attack.discovery
  - attack.t1040
logsource:
  product: cisco
  service: aaa
  category: accounting
fields:
  - CmdSet
detection:
  keywords:
    - 'monitor capture point'
    - 'set span'
    - 'set rspan'
  condition: keywords
falsepositives:
  - Admins may setup new or modify old spans, or use a monitor for troubleshooting.
level: medium
```

The Sigma logo is a stylized, circular emblem. It features a thick, light blue outer ring. Inside this ring, there is a white, abstract shape that resembles a lowercase 's' or a stylized 'sigma' symbol. The overall design is clean and modern, with a focus on geometric forms.

```
Router(config)# monitor event-trace |  
include
```

Network Administrators can and do perform similar activities

Frequency Analysis of commands

!

Tune analytics for less false-positives

Which admins have access to network devices?

!

Where are they remotely logging in from?

!

What times are the changes being made?

!

Is there an associated Change Control Board reference?

!

Is that change commonly implemented?

Router(config)# do show running config

Mitigations. Raise the bar - make the adversary work harder.

Authorization to limit administrators' capabilities, not everyone needs Level 15, nor the ability to execute every command.

Turn off unused and outdated services:

no ip http server

no ip http secure-server

Disable Cisco Smart Install.

!

Cisco Hardening Guide:

<https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

Center for Internet Security Benchmarks:

<https://www.cisecurity.org/cis-benchmarks/>

<https://www.us-cert.gov/ncas/alerts/TA16-250A>

https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_ND_17-004.pdf

Router(config) # exit

Network are endpoints too

!

Collect Syslog and AAA logs

!

Harden your devices, and write detections

!

Give back to the Open Source Community

```
Router# end
```

```
Questions
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```

```
!
```