Evolution of attacks on Cisco IOS devices

By Graham Holmes,

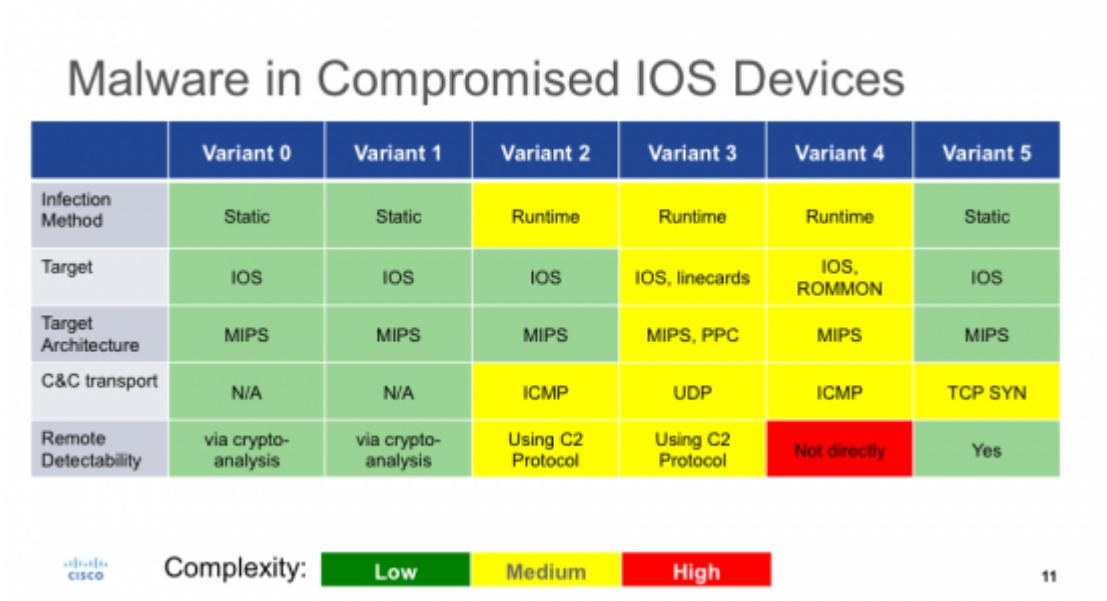
Published: 2015-10-08 · Archived: 2026-04-05 14:37:18 UTC

While “SYNful Knock” is the latest identified malware targeting Cisco devices running Cisco IOS, we have identified and investigated six other malware incidents during the last four years that target Cisco devices running Cisco IOS. The nature of threats is evolving and Cisco will continue to adapt technology delivering trustworthy solutions that our customers can rely on. This also means that customers will need to evolve, fully utilizing the security tools that are available, as well as ensuring security best practices are in place.

The malware used in these evolved Cisco IOS attacks show increasing levels of complexity in the type of modifications made to Cisco IOS, the behavior of its Command and Control (C&C) network (when present), and the platforms they target.

Before talking about specifics of each investigated malware incident, it is important to note that in all cases, no evidence has been found that attackers exploited a previously known or unknown vulnerability to install the malware. All available data points suggest either the use of compromised administrator credentials or physical access to the devices or images.

The following table and associated description provides a brief overview of the malware samples, as well as an overview of the actions that Cisco took in response to those findings. The source of this information is internal analysis performed by Cisco forensics teams.



Notes to table:

INFECTION METHOD: Static means “modifications to the IOS binary stored in the device’s flash”, Runtime means “modifications performed to the runtime memory code without changes to the IOS binary in flash”

REMOTE DETECTABILITY: refers to the means to remotely look for the presence of the malware on a compromised system through scanning systems and signatures. Other means of detecting modifications through memory analysis is possible in all cases.

Incidents 0 and 1

The first two incidents were detected in 2011 and 2012 respectively, and were most likely custom malware targeting a specific victim. Those incidents were very basic (from a technical point of view) and involve binary patches to a Cisco IOS image. They allowed the modified IOS image file to be installed on the target routers (C3825, C2800nm, and C3845). Devices affected were in the Cisco 2800 and 3800 family of routers. No other Cisco devices were identified as affected by this malware.

The modification essentially affects the Diffie-Hellman key exchange protocol in order to weaken the derived keying material. The result is that with casual inspection the encrypted traffic seems unmodified, but the effect is that an attacker could decrypt protected traffic with less effort than would normally be required.

Platforms implementing Trust Anchor technologies and signed binaries would not be affected by either one of those two malware examples.

Incidents 2 and 3

Two new malware samples were identified in 2013, both targeting the Cisco 7600 series of devices. In both cases, the attacker leveraged compromised administrator credentials to modify the in-memory copy of the Cisco IOS code, using debugging and troubleshooting Cisco IOS command line interface (CLI) commands.

The primary purpose of the added code appears to be exfiltration of IPv4 packets that match criteria set by the attacker. The targeted traffic is copied and those packets are then forwarded to a specified IP address that is under the control of the attacker. A secondary purpose is to provide NAT (Network Address Translation) capabilities, so an attacker is able to access an IPv4 address within a compromised network that would normally not be reachable from the public Internet (ie: devices using RFC-1918 addresses).

Since both of these malware samples involved the modification of the in-memory code for Cisco IOS, neither Trust Anchor technologies nor image validation features would have detected or prevented the attack. But, because the modifications were performed on the in-memory copy of Cisco IOS, neither attack would achieve persistency across device reloads.

Incident 3 has only been detected in a single customer network. It was discovered while troubleshooting crashes on line cards on installed Cisco 7600 devices. Forensic analysis of the associated core dumps found that this attack used a C&C mechanism similar to Incident 2 to provide the malware with instructions for data exfiltration. What is unique in this incident is targeting of multi-architecture line cards – something we have not seen in any other malware analyzed as of this writing.

In both cases, the modifications were made to the in-memory copy of the executable code for the Cisco IOS image (with no changes to the actual binary Cisco IOS image in flash). The use of signed Cisco IOS images would not be a defense. It does, however, highlight the need for strong protection of administrative credentials and authorization mechanisms for privileged access to any network device.

Incident 4

Incident 4 was discovered in late 2014 and affected Cisco 1800, Cisco 3800 and Cisco 7200 devices. Like the malware seen in Incidents 2 and 3, the attack leveraged compromised administrative credentials to gain access to target devices for the purpose of installing the malware.

This malware, however, showed an increase in complexity compared to previous malware analyzed. It is the only analyzed malware so far that is capable of persistence through both device reload as well as through Cisco IOS software upgrades.

The malware has two separate components:

- An initial infection, where the ROMMON on the targeted Cisco device is modified to ensure persistence of the C&C channel;
- A secondary infection occurs when the ROMMON is used to inject binary code into the in-memory Cisco IOS image to support data exfiltration.
    - Note: This malware does not modify the binary Cisco IOS image in flash.

The ROMMON component of the malware handles the C&C messages, which are embedded within the payload of ICMP packets delivered through the IPv4 protocol.

The secondary infection component is highly modular, and supports the loading and unloading of optional “modules,” which are delivered to the device through the C&C channel. One of the observed modules purpose is to exfiltrate device-specific data via ICMP packets. This module creates an ICMP Echo Request packet with the data to be exfiltrated as its payload. Other modules provide NAT capabilities, so C&C messages can reach devices that would otherwise not be accessible from the public Internet, and additional exfiltration capabilities for other traffic defined by the attacker.

Like Incident 3, the use of signed IOS images would not prevent this attack, as the binary Cisco IOS image stored in flash is never modified. However, the ROMMON compromise (used to achieve persistence between reloads and Cisco IOS software upgrades) would not be successful with current devices that incorporate secure boot, trust anchor modules, and image signing capabilities.

Incident 5 (SYNful Knock)

The last example (known as SYNful Knock and jointly disclosed by Cisco and Mandiant’s FireEye), uses the same static modifications to the Cisco IOS binary seen in Incidents 0 and 1. It also uses a C&C approach similar to the one observed in Incident 2, but uses TCP instead of ICMP for C&C traffic (hence the name SYNful Knock).

SYNful Knock (like malware #0, #1, #2 and #3) CANNOT survive the installation of a known good Cisco IOS binary image, obtained from a known, trusted source and verified to have the correct hash values.

Cisco actions to prevent and detect attacks against Cisco devices

Since 2008, the Cisco Secure Development Lifecycle framework has provided development teams with standards and requirements to build products designed with protection features and capabilities. Boot time and run time security features, such as Trust Anchor modules, secure boot, and memory protection are standard requirements. The goal of these features is to protect customers from remote code injection attacks or static modifications to Cisco IOS binary images.

As soon as the first malware was detected “in the wild,” forensics and analysis teams at Cisco began accelerating the development of detection capabilities. We’ve developed forensics tools that can quickly validate the authenticity of IOS images from core dumps or in-memory images. These are key tools used in incident response to help our customers confirm whether there is a compromise and the extent of such a compromise.

Concurrently with the development of such forensics tools, we implemented measures to further ensure our supply chain integrity: verifying Cisco IOS image integrity through development, compilation, testing and release, and all the way to distribution points. As part of those efforts, we recently introduced and began posting SHA-512 hash values for any Cisco image to further increase customer confidence on their image authenticity. These are available for customer download on www.cisco.com.

We have also posted instructions and guidance for customers to harden their router authentication, authorization and accounting process and for validating Cisco IOS binary images already installed or to be installed on their Cisco devices.

We’ve deployed tools that automatically analyze core dumps provided by customers to the Cisco Technical Assistance Center (TAC) as part of a Service Request. These tools automatically detect modifications to Cisco IOS images. They also detect malicious and/or counterfeit images by analyzing binary images installed on any Cisco device that come through our RMA process.

We have reviewed all Cisco IOS command line interface (CLI) commands, and have removed commands that provide limited value to customers during normal device operation, but could be misused by attackers with access to the device CLI.

We are in the pilot phase of an image validation service that offers customers the ability to quickly and automatically analyze and detect modified Cisco IOS images running on their Cisco devices.

We have released SNORT and Yara signatures that detect SYNful Knock malware.

We have worked with all customers to quickly address their concerns or help them validate the running images in their network have not been compromised.

What Can You Do?

We have published several documents that can be used by Cisco customers wanting to better understand how to protect their Cisco IOS devices, harden their device configurations (including credential management procedures), and verify binary or in-memory running Cisco IOS images. The following are some of the resources you can find on www.cisco.com:

- Cisco IOS Software Integrity Assurance
- Cisco Guide to Harden IOS Devices
- Telemetry-Based Infrastructure Device Integrity Monitoring
- Trust Anchor Technologies on Cisco products

While some of the previously listed measures have been reactive, we are also taking active steps in developing new capabilities to meet the challenges of an ever changing threat landscape. In terms of the attack continuum – protect, detect, recover – Cisco has focused for many years on addressing the challenges of protecting our products through hardening, resiliency, and security capabilities. We will continue and even accelerate those efforts, while also rapidly developing and adding detection and recovery capabilities to our products in the medium and long term.

The challenge is clear: the nature of the threat to our customers is ever evolving. Cisco will continue to focus on providing trustworthy solutions that our customers can rely on in this changing landscape.
