Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Static Tundra Fuels Espionage Campaigns Through an Old Cisco Bug

Date of Publication

August 22, 2025

Admiralty Code

A1

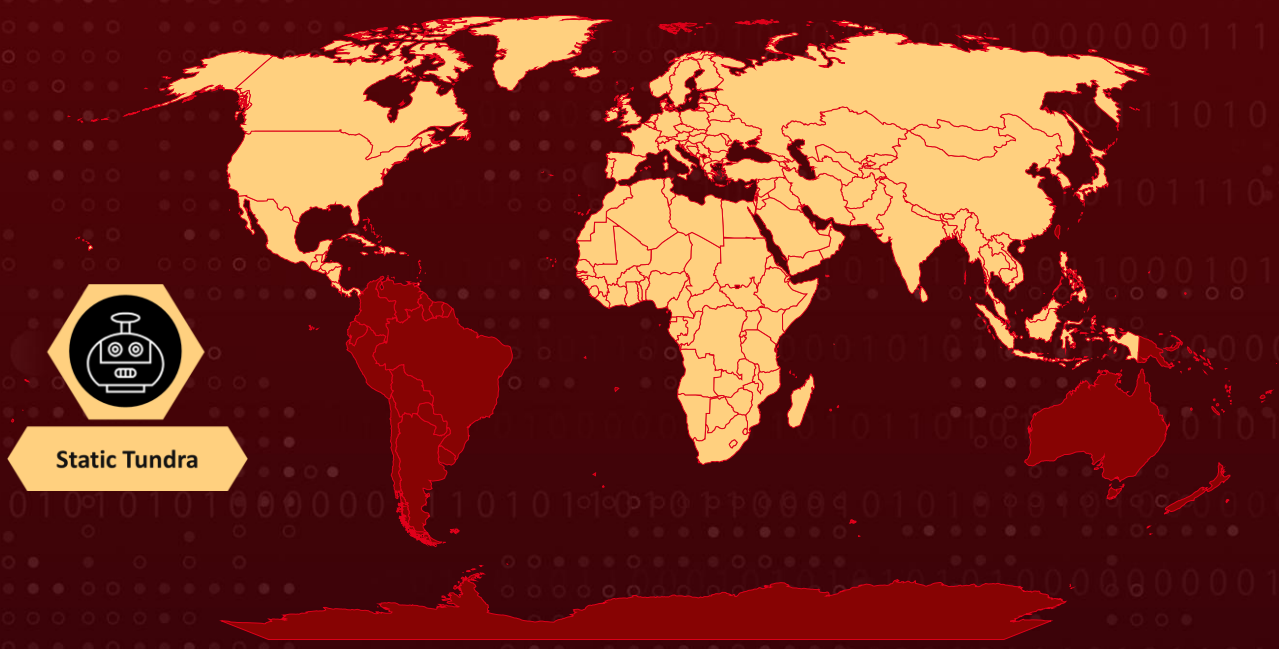
TA Number

TA2025256

Summary

Attack Commenced: 2021
Threat Actor: Static Tundra
Malware: SYNful Knock
Targeted Regions: North America, Asia, Africa, Europe
Targeted Industries: Telecommunications, Higher Education, Manufacturing
Attack: Static Tundra is a Russian state-sponsored cyber espionage group tied to the FSB, notorious for compromising unpatched Cisco network devices with advanced implants and custom tooling. Believed to be a sub-cluster of the Energetic Bear threat actor. The group has expanded its targeting in recent years, focusing heavily on Ukrainian organizations and critical industries, while maintaining long-term, stealthy access to support Russia's strategic intelligence goals.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2018-0171	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	Cisco IOS and IOS XE Software	✗	✓	✓

Attack Details

#1 Static Tundra is a Russian state-sponsored cyber espionage group linked to the Federal Security Service's Center 16 unit. Active for more than a decade and first observed in 2015, the group is considered a sub-cluster of the well-known Energetic Bear threat actor, also referred to as Crouching Yeti, Dragonfly, or Havex.

#2 Static Tundra's operations have consistently focused on compromising network devices, enabling long-term intelligence collection in support of Russian strategic objectives. At the core of Static Tundra's activity is the targeting of outdated or unpatched Cisco network devices. The group takes advantage of a long-standing vulnerability, CVE-2018-0171, found in Cisco IOS software's Smart Install feature.

#3 By exploiting this flaw, the attackers can harvest device configurations and credentials, then use that information to embed durable backdoors. This approach allows them to quietly expand their access within victim environments and maintain persistence over extended periods. To strengthen their foothold, Static Tundra uses both advanced implants and configuration changes that make removal difficult.

#4 A notable example is the SYNful Knock malware, a malicious firmware modification that provides a stealthy, modular backdoor into compromised routers. Because it relies on specially crafted packets for activation, SYNful Knock is challenging to detect and can be updated over time, ensuring continued access.

#5 In addition, the group creates privileged user accounts, adds new SNMP community strings, and alters authentication settings such as TACACS+ to further entrench themselves within victim networks. The group's operations are characterized by tailor-made tooling that automates exploitation and data theft.

#6 These tools enable the rapid targeting of specific IP ranges, which are likely identified through public scanning data. Once inside, the attackers pivot deeper into the network, compromise additional devices, and establish long-lasting channels for espionage. Their ability to remain undetected for years underscores their technical sophistication and methodical approach.

Recommendations

Smart Install and Software Version Validation: Administrators should determine whether Cisco Smart Install is enabled by using the show vstack config command. Devices returning "Role: Client and Oper Mode: Enabled" or "Role: Client (SmartInstall enabled)" must be prioritized for patching or feature disablement. The running Cisco IOS or IOS XE version should be validated using the show version command. To assess exposure, Cisco's IOS **Software Checker tool** can be used to identify impacted releases and the earliest fixed versions.

Cisco-Specific Hardening Measures: Organizations should establish end-of-life management plans for outdated technology. Telnet must be disabled on all devices by configuring VTY lines with "transport input ssh" and "transport output none." Administrative interfaces such as SNMP, SSH, HTTP, and HTTPS should be secured and continuously monitored for unusual exposure. Type 8 passwords should be implemented for local accounts, and Type 6 encryption should be used for TACACS+ key configurations.

Logging and Monitoring: System logs, including syslog and AAA logs, must be continuously monitored for unusual activity, such as unexpected gaps or reductions in logging events. Environments should be profiled through NetFlow and port scanning to detect shifts in device behavior, such as unexpected port activity or volumetric changes in network traffic. Administrators should also monitor for non-standard artifacts, such as large or non-empty .bash_history files, which may indicate unauthorized activity.

Configuration and Access Management: Organizations should implement comprehensive configuration management practices, including regular audits, to ensure devices remain aligned with security best practices. Strong authentication and authorization controls must be enforced, with careful monitoring of command execution. Access control lists should be reviewed and verified for all management protocols, ensuring that only approved methods are permitted. All configurations should be centrally stored and pushed to devices, preventing devices themselves from becoming the trusted source of truth.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
TA0003 Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0008** Lateral Movement	**TA0011** Command and Control	**TA0010** Exfiltration
T1190 Exploit Public-Facing Application	**T1601** Modify System Image	**T1596** Search Open Technical Databases	**T1596.005** Scan Databases
T1543 Create or Modify System Process	**T1210** Exploitation of Remote Services	**T1587** Develop Capabilities	**T1587.004** Exploits
T1018 Remote System Discovery	**T1046** Network Service Discovery	**T1040** Network Sniffing	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities	**T1542.005** TFTP Boot	**T1068** Exploitation for Privilege Escalation	**T1543.003** Windows Service
T1036 Masquerading	**T1105** Ingress Tool Transfer	**T1601.002** Downgrade System Image	**T1552.001** Credentials In Files
T1016 System Network Configuration Discovery	**T1602.002** Network Device Configuration Dump	**T1059** Command and Scripting Interpreter	**T1571** Non-Standard Port
T1048 Exfiltration Over Alternative Protocol			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	185[.]141[.]24[.]222, 185[.]82[.]202[.]34, 185[.]141[.]24[.]28, 185[.]82[.]200[.]181

Patch Link

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

References

https://blog.talosintelligence.com/static-tundra/

https://www.ic3.gov/PSA/2025/PSA250820

https://sec.cloudapps.cisco.com/security/center/softwarechecker.x

https://www.talosintelligence.com/scanner

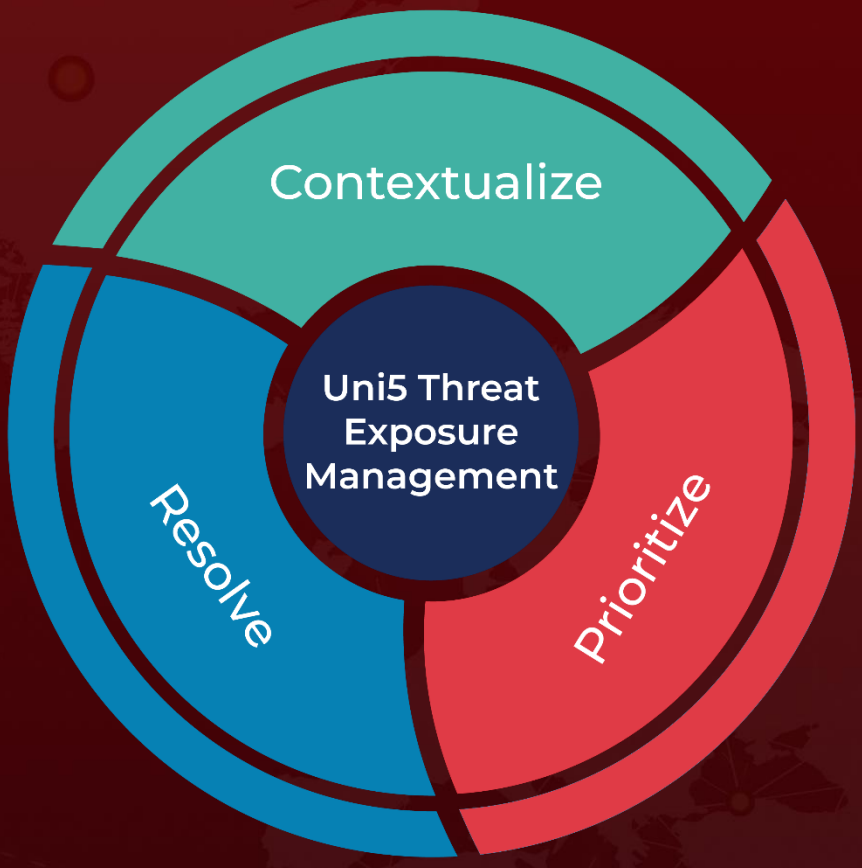
https://cloud.google.com/blog/topics/threat-intelligence/synful-knock-acis

https://hivepro.com/threat-advisory/salt-typhoons-covert-campaign-targeting-u-s-telecom-networks/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 22, 2025 • 4:00 AM

More at www.hivepro.com