State-sponsored campaigns target global network infrastructure

blog.talosintelligence.com/state-sponsored-campaigns-target-global-network-infrastructure/

Matt Olney April 18, 2023

By Matt Olney

Tuesday, April 18, 2023 11:04

Threats SecureX Threat Advisory

Cisco is deeply concerned by an increase in the rate of high-sophistication attacks on network infrastructure — that we have observed and have seen corroborated by numerous reports issued by various intelligence organizations — indicating state-sponsored actors are targeting routers and firewalls globally. We have spoken about infrastructure security for a long time. However, while working with network infrastructure in various parts of the world, we have observed both espionage and obvious targeting to support future destructive attacks. While working with our partners, we have experienced the operational barriers that slow and sometimes stop security teams from properly securing network infrastructure. In

this report, we are sharing both our observations of top-tier attackers and their activities on network devices, and recommendations and resources to help you improve your network infrastructure resilience.

Background

Recently, the UK's National Cyber Security Centre (NCSC) released a report on a sustained campaign by a Russian intelligence agency targeting a vulnerability in routers that Cisco had published a patch for in 2017. This campaign, dubbed "Jaguar Tooth," is an example of a much broader trend of sophisticated adversaries targeting networking infrastructure to advance espionage objectives or pre-position for future destructive activity. While infrastructure of all types has been observed under attack, attackers have been particularly successful in compromising infrastructure with out-of-date software.

Because of the large presence of Cisco network infrastructure around the world, any sustained attack against network infrastructure would likely target Cisco equipment, but attacks are by no means limited to Cisco hardware. In reporting on Russian intelligence contracting documents, samples of which were recently shared with Cisco Talos, it was shown that any infrastructure brand would be targeted, with one scanning component targeting almost 20 different router and switch manufacturers (see the image below). Looking at past research, in 2018 Talos looked into the VPNFilter threat, also believed to be of Russian origin, which showed a well-developed capability targeting Asus, Huawei, Linksys, MikroTik, Netgear, QNAP, TP-LINK, Ubiquiti, and Upvel devices.

оборудования, представляют следующие классы производителей: Cisco, Huawei, Juniper, а также 3Com, Alcatel, Allied Telesis, Avaya, D-Link, Extreme Networks, HP, Linksys, MikroTik, Motorola, MOXA, Netgear, Nortel, Ubiquiti, Wind River, ZyXEL. Эти классы должны фильтроваться СПО АРМ тестирования телекоммуникационного оборудования в выводе nmap и отображаться в интерфейсе оператора.

Russia is not alone in its actions. CISA has reported on Chinese adversaries targeting network equipment from a similarly broad set of manufacturers. These are certainly not the only campaigns targeting network equipment, nor the only actors. It is reasonable to conclude that any sufficiently capable national intelligence operation would develop and use the capability to compromise the communications infrastructure of their preferred targets.

Talos investigations are consistent with these findings. We have observed traffic manipulation, traffic copying, hidden configurations, router malware, infrastructure reconnaissance and active weakening of defenses by adversaries operating on networking equipment. Given the variety of activities we have seen adversaries engage in, they have shown a very high level of comfort and expertise working within the confines of compromised networking equipment.

Our assessment is clear, that national intelligence agencies and state-sponsored actors across the globe have attacked network infrastructure as a target of primary preference. Route/switch devices are stable, infrequently examined from a security perspective, are often poorly patched and provide deep network visibility. They are the perfect target for an adversary looking to be both quiet and have access to important intelligence capability as well as a foothold in a preferred network.

Campaign observations

We'd like to share a non-exhaustive list of the sorts of activities we have observed actors take on various infrastructure devices. Our analysis for this set of actors is that they were (depending on the incident) either engaging in espionage or establishing a foothold for follow-on actions in support of any number of strategic goals, which may include destructive attacks. While these activities span several different incidents and campaigns, they demonstrate the technical capability of the actor. So, in brief, we have seen the following actor behaviors across different infrastructure platforms at critical infrastructure facilities:

- The creation of Generic Router Encapsulation (GRE) tunnels and the hijacking of DNS traffic, giving the actor the ability to observe and control DNS resolution
- Modifying memory to reintroduce vulnerabilities that had been patched so the actor has a secondary path to access
- Modification of configurations to move the compromised device into a compromised state to allow the actor to execute additional exploits to further access
- Installation of malicious software into an infrastructure device that provides additional capabilities to the actor, including:
    - Masking of certain configurations so that they can't be shown by normal commands
    - Bypassing of ACLs so that traffic can't be blocked properly by the router
    - Allowing for authenticated access to devices outside of the normal SSH/Telnet methods
    - Modular design allowing for easy updating as new capabilities are needed or developed
    - Capability to corrupt and disable the infrastructure device
    - Redirection of actor-defined traffic to actor-controlled infrastructure
- Creation of hub-and-spoke VPNs designed to allow the siphoning of targeted traffic from network segments of interest through the VPN
- The capture of network traffic for future retrieval, frequently limited to specific IPs or protocols
- A variety of logic to allow network packets to enable and disable certain capabilities
- The use of infrastructure devices to deliver attacks or maintain C2 in various campaigns

Additionally, we have seen traditional enterprise attacks explicitly targeting the environments that support infrastructure devices such as TACACS+ servers, enterprise management servers and jump hosts. Further, we have seen espionage activity on enterprise networks specifically searching for network data such as credentials, network diagrams, contracts with network customers and configuration information.

In short, there are extremely sophisticated actors who are increasingly targeting network infrastructure devices from a variety of manufacturers. We are concerned that insufficient awareness and patching, the reliance on end-of-life equipment and the necessity for always-on connectivity makes too many infrastructure devices easy prey. The results of these issues range from being an unwitting participant in criminal activity to events of true national security impact.

Guard the creds

The Jaguar Tooth attacks are actually a sequence of attacks, the first looks for poorly selected SNMP community strings. Once a community string is found, the attacker exploits CVE-2017-6742, which was first announced on June 29, 2017, after which a software patch was made available to all customers. But even unpatched, a well-selected SNMP community string stops this attack in its tracks. It should also be noted that if you are not using SNMP v3, even well-chosen credentials are transmitted in the clear, and are subject to capture. NETCONF (Network Configuration Protocol) and RESTCONF are modern network management protocols designed to offer better security and functionality than their older counterpart, SNMP. NETCONF typically runs over SSH, while RESTCONF runs over HTTPS. Both SSH and HTTPS provide strong encryption and secure authentication mechanisms, ensuring the confidentiality, integrity, and authenticity of the data being exchanged. SNMP, particularly its older versions (v1 and v2c), lacks proper encryption and authentication, which makes it more vulnerable to cyber attacks.

In other incidents, we have observed well-positioned adversaries with preexisting access to internal environments targeting TACACS+/RADIUS servers to obtain credentials. This gives them the benefit of understanding the controls enforced by the credential server, as well as allowing their traffic to look “normal” by using jump servers and employing other techniques that a typical network administrator would use.

Many of the exploits we’ve seen used in the wild are post-compromise exploits, meaning the attacker had some form of credential to get them to the place where they could then launch the exploit and get deeper access to the device. Our recommendations are to select complex passwords and community strings, to utilize multifactor authentication where possible, to require encryption when configuring and monitoring devices and to lockdown and aggressively monitor credential systems like TACACS+ and any jump hosts.

Stay modern, stay real

Network infrastructure is built to last, and in today's always-on world, it's sometimes impossible to find a patch window. But recent reports – and our own investigations – show that it is critical to update both the hardware and the software that runs your network. This is true not just because patching eliminates known vulnerabilities, but upgrades also introduce new security capabilities and controls that weren't previously available.

Cisco has introduced a number of technologies and protocols over time that has improved the security of its products. Some of these advances can be obtained by software upgrade, while others require more modern networking equipment. For example, in order to combat certain supply chain attacks, Cisco has introduced a series of technologies. These technologies include hardware improvements such as the Trust Anchor Module and software changes like Secure Boot. Organizations that fail to update their hardware and software will both be more likely to be a victim of unpatched security vulnerabilities but also will have fewer tools to combat adversaries. Cisco customers can check their version of software to see if any known vulnerabilities exist in it here. You can learn more about Cisco Trustworthy Technologies here. Several related resources, tools, and services can be found at The Trust Center here.

Know your world and enforce it

An organization that both understands the configurations that it is running and monitors for departures from that understanding have a high probability of discovering adversaries early in the campaign. For example, an unauthorized GRE tunnel or static VPN, discovered by NetFlow analysis, would be grounds for an investigation. Additionally, monitoring for connections to edge routers from unknown external IPs would also uncover some of the activity that we've observed. Even basic configuration monitoring and alerting on modifications would help in many cases.

Authentication, authorization, and accounting (AAA) tools are another area where policy enforcement can be useful. We've seen actors take unusual action on routers that would show up in AAA logs and ideally could be denied by the correct AAA configuration. One example would be attempts to suppress logging by issuing *"no aaa accounting"* configuration commands. Attempts to disable any feature of AAA should be both logged and denied by the AAA system.

Asking organizations to monitor their environment for unusual changes in behavior or configurations is one of the hardest recommendations we are making. It will take a combination of a well-documented network infrastructure environment, network engineering and talented security operations to build a monitoring environment tuned to your implementation. While there are many technologies to support you, the excellence in your network engineering and security team, and their willingness to collaborate, will be a large factor in whether or not you are successful.

If you need us, call us

Responding to incidents involving specialized hardware can be challenging. If you suspect that a Cisco product has been compromised, please reach out to TAC for assistance. If you suspect there is a vulnerability in a Cisco product, please reach out to PSIRT. You can find out how to contact TAC for general questions here. To report or obtain support for a suspected vulnerability, you can contact Cisco's PSIRT here.

TL; DR recommendations

- Select complex passwords and community strings, avoid default credentials
- Use multi-factor authentication
- Encrypt all monitoring and configuration traffic (SNMPv3, HTTPS, SSH, NETCONF, RESTCONF)
- Lockdown and aggressively monitor credential systems like TACACS+ and any jump hosts
- Do not run end-of-life hardware and software
- Maintain current software
- Utilize AAA to deny configuration changes of key protections
- Monitor syslog and AAA logs for unusual activities
- Monitor your environment for unusual changes in behavior or configuration
- Contact Cisco TAC or PSIRT if you need assistance with a security incident involving Cisco products

Conclusion

If your network isn't secure, then nothing on that network can be properly secured. We know that there is a myriad of operational realities that make it difficult to maintain a fully defensible network infrastructure. However, given the risks and outcomes that compromised network infrastructure bring, these obstacles must be overcome for organizations to truly secure their environment. Regardless of the context, aging infrastructure is a risk. Relying on out-of-date gear or utilizing out-of-date protocols and technologies will eventually cost your organization. Work with your vendor to give yourself the best chance of defending your environment.