XECURITYPULSE

UNMASKING SALT TYPHOON

DEFENDING 5G NETWORKS AGAINST ADVANCED PERSISTENT THREATS

XECURITYPULSE

TABLE OF CONTENTS

XECURITYPULSE

XECURITYPULSE

ABOUT THE AUTHOR

TAHA SAJID, CISSP, MSC

FOUNDER OF XECURITY PULSE

Taha Sajid is an industry leader and world-renowned authority in cybersecurity, telecom, and emerging technologies. As the Founder of Xecurity Pulse and a Principal Architect, he has led innovative initiatives in Zero Trust Security, AI-driven Threat Intelligence, and Blockchain Security, making him a leading pioneer in the emerging field of digital security.

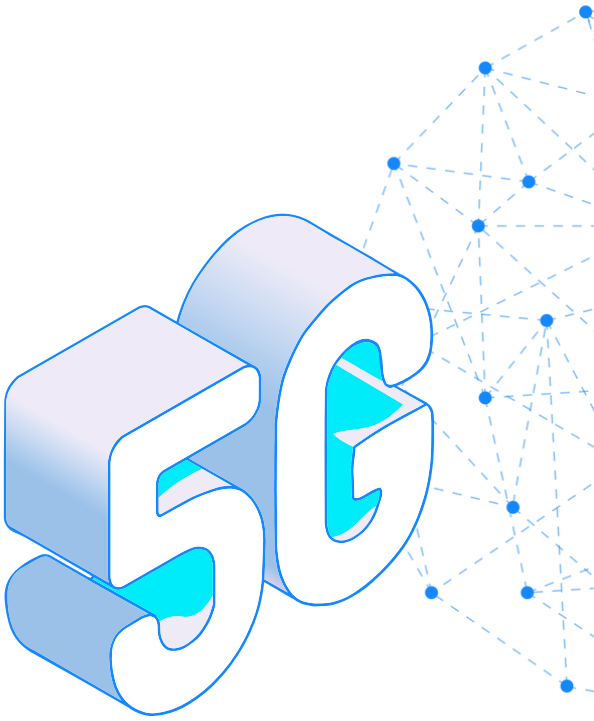
With expertise honed from years of leadership in telecom and cybersecurity, Taha has contributed to securing critical infrastructures and building powerful, scalable, and future-proof systems for organizations. He is the author of The Blockchain Security Handbook, a comprehensive guide to navigating the complexities of blockchain technology with security as a priority

Taha's contribution goes beyond technical expertise, he is a mentor, EB1A Coach, and trusted advisor, aiding individuals and organizations to achieve excellence. As a certified leader, LinkedIn Instructor, and Infosec Board Member, his commitment to sharing knowledge and innovation impacts the industry.

He is dedicated to making the digital world more secure, by bringing together visionary leaders and technical experts to inspire the next generation of cybersecurity professionals and provide unparalleled support to the global tech community.

XECURITYPULSE

FOREWORD



MILIND GUNJAN, CISSP

TELECOM INNOVATOR | ZERO TRUST ARCHITECT

Milind Gunjan is an esteemed leader with expertise in 5G/6G networks, cloud-native infrastructure, AI, and cybersecurity. As the Lead Solutions Architect of 5G Strategy at Netskope, the world's leading cloud security (SASE) platform, Milind brings over 10 years of innovative experience to the telecom and cybersecurity sectors.

Milind's technical expertise is matched by his ability to transform complex challenges into clever solutions. From pioneering new technologies and filing patents to developing hands-on MVPs for validating concepts, his contributions drive bottom-line growth and shape the future of connectivity and security. His leadership in Zero Trust Architecture, SASE, and product innovation has earned him a reputation as a trusted advisor to enterprises and operators looking to unleash the transformative power of 5G.

Through his work, Milind pushes the boundaries of technological innovation, delivering scalable and secure solutions tailored to the dynamic needs of enterprises and operators around the world. His commitment to solving significant problems, fostering strategic partnerships, and shaping the future of technology solidifies his legacy as a leader in his field.

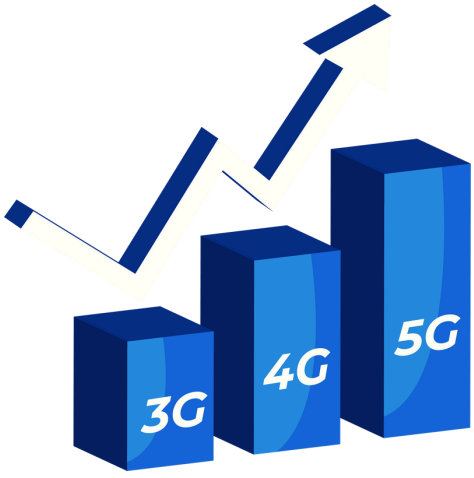
XECURITYPULSE

EXECUTIVE SUMMARY

STORMS HAVE SWEPT THROUGH THE DIGITAL LANDSCAPE, TARGETING THE EPICENTER OF TODAY'S MODERN INNOVATION: 5G NETWORKS.

This report sheds light on Salt Typhoon (GhostEmperor), a state-sponsored Advanced Persistent Threat (APT) group, as it exploits vulnerabilities in 5G architectures, particularly in Service-Based Architecture (SBA), Network Function Virtualization (NFV), and out-of-band interfaces.

This report provides GhostEmperor's strategies, tactics, and plans (TTPs) to combat these threats effectively. It explores Zero Trust frameworks, API Security, advanced monitoring tools, and the critical role that Xecurity Pulse plays in securing 5G.



XECURITYPULSE

INTRODUCTION

2.1 OVERVIEW OF SALT TYPHOON

In the race to adopt 5G technology, organizations are unlocking the potential for transformation, but they are also exposing themselves to unprecedented threats. One such adversary, Salt Typhoon (GhostEmperor), stands out for its precision and resilience.

Since its emergence in 2020, Salt Storm has targeted critical sectors such as telecommunications, government agencies, and commercial companies. Its arsenal includes zero-day exploits and Demodex, a custom kernel-based exploit that allows the group to infiltrate networks, evade detection, and exfiltrate sensitive information.

2.2 THREAT LANDSCAPE

The shift to 5G Standalone (SA) and Non-Standalone (NSA) architectures welcomes unique challenges. These networks introduce a larger attack surface by relying on virtual network functions (VNFs) and cloud-native designs. Salt Typhoon exploits this complexity to stay one step ahead of traditional defenses.

This report unveils the inner workings of Salt Typhoon, providing a roadmap to counter its threats and strengthen next-generation connectivity.

XECURITYPULSE

TECHNICAL ANALYSIS OF SALT TYPHOON

3.1 TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)

The Salt Typhoon playbook is a masterclass in advanced cyberespionage. Its operations can be divided as follows:

- **Initial Access**
  - Exploitation of public-facing applications (e.g., vulnerabilities in Microsoft Exchange Servers)
  - Use of phishing attacks to compromise credentials
- **Execution**
  - Runs PowerShell scripts and WMI commands to deploy payloads and execute commands remotely
- **Persistence**
  - Deploys Demodex (a kernel-mode rootkit) to establish persistent backdoor access
  - Uses DLL hijacking and obfuscated code for persistence
- **Privilege Escalation**
  - Exploits known vulnerabilities to elevate permissions
  - It uses tools like Mimikatz to steal credentials
- **Defense Evasion**
  - Utilizes living-off-the-land techniques to avoid detection
  - Obfuscates payloads and encrypts C2 communications
- **Credential Access**
  - Extracts credentials from LSASS memory and deploys keyloggers
- **Lateral Movement**
  - Moves laterally using SMB, WMI, and RDP protocols
  - Installs backdoors on other devices within the network
- **Exfiltration**
  - It focuses on collecting sensitive data such as Call Detail Records (CDRs) and metadata
  - Encrypts and transmits data to Command-and-Control (C2) servers

XECURITYPULSE

3.2 ROOTKIT ANALYSIS - DEMODEX

Demodex, a custom-built kernel-mode rootkit, is Salt Typhoon's secret weapon to ensure secrecy and persistence.

KEY FEATURES

- Operates at the **kernel level** for privileged access
- Ensures **persistence** by embedding itself in the OS
- Deploys **anti-forensics** techniques to evade detection
- Establishes **encrypted C2 communication channels** for data exfiltration

STEALTH CAPABILITIES

- **Obfuscates code** and uses **polymorphic techniques** to avoid detection
- Manipulates **Windows APIs** to hide processes, files, and registry entries
- Uses **fragmented payload delivery** to bypass Intrusion Detection Systems (IDS)

XECURITYPULSE

3.3 EXPLOITATION PATHWAYS

ATTACKERS EXPLOIT VULNERABILITIES IN ROUTERS, PUBLIC-FACING SERVERS, AND HYBRID ENVIRONMENTS. IT GAINS A FOOTHOLD IN NETWORK MANAGEMENT BY SELECTING THE MOST CRITICAL PARTS.

- **Telecom Networks:** Many home routers, switches, and firewalls exploit flaws in firmware or outdated network device management protocol vulnerabilities. By infiltrating these critical components, attackers establish a path, increase mobility, and continue to gain access to sensitive data.

- **Public-Facing Servers:** This category targets web servers, email gateways, and VPN appliances exposed to the Internet. Zero-day exploits and credential-based attacks allow organizations to breach these ports and compromise infrastructure.

- **Supply Chains:** The main focus areas are trusted contractors, third-party service providers, and software updates. Attackers can spread malicious code by infiltrating supply chains for various reasons, often undetected, until the damage is already done

- **Cloud and Hybrid Environment**: This attack targets containerized applications and virtual machines in hybrid cloud setups. Unmanaged Kubernetes clusters, vulnerabilities in container runtimes, and poor IAM (Identity and Access Management) configuration allow attackers to gain access and control over cloud computing.

3 IN 5 COMPANIES FALL VICTIM TO ATTACKS TARGETING ROUTERS, SERVERS, OR CLOUD SYSTEMS

XECURITYPULSE

5G NETWORKS: VULNERABILITIES AND THREAT VECTORS

4.1 OVERVIEW OF 5G SA AND NSA ARCHITECTURES

5G deployment has resulted in two primary deployment models:

1. Standalone (SA): SA is independent of traditional networks, leveraging cloud-native core to provide ultra-low latency, high device connectivity, and high bandwidth.
Vulnerabilities: Reliance on cloud-native architecture introduces new attack vectors, including container security flaws, API misconfigurations, and vulnerabilities in Service-Based Architecture (SBA).

2. Non-Standalone (NSA): Combining 5G access with the existing 4G LTE core speeds up deployment but creates reliance on legacy systems.
Vulnerabilities: Incorporating outdated 4G infrastructure makes 5G networks vulnerable to LTE network vulnerabilities, such as insufficient encryption and weak protocol signaling.

Salt Typhoon exploits the complexity of both models and modifies its approach to increase its impact.

XECURITYPULSE

4.2 EXPLOITING SERVICE-BASED ARCHITECTURE (SBA)

The heart of 5G SA lies in the Service-Based Architecture (SBA), where network functions communicate via HTTP/2 APIs. This architectural shift improves scalability and flexibility but also introduces new risks:

- **API Exploitation:** Attackers can manipulate less secure APIs to gain unauthorized access to key functions.
- **Service Discovery Abuse:** Salt Typhoon uses a service registry to identify and target critical components, bypassing traditional firewalls.

4.3 OUT-OF-BAND INTERFACE EXPLOITS

Out-of-band interfaces support network management and analysis, often with access controls:

- **Key Vulnerability:** This interface is often configured poorly or lacks strong security, providing a direct path to the network
- **Salt Typhoon's Strategy:** By targeting these interfaces, the group avoids detection by operating outside the usual data pathways

4.4 NFV AND MANO LAYER ATTACKS

5G relies heavily on the Network Function Deployment (NFV) and the Management and Orchestration (MANO) layers to facilitate operations. However, this dependency poses its own risks:

- **NFVI Vulnerability:** Salt Typhoon targets the virtualization layers, exploiting hypervisor vulnerabilities to compromise virtual network functions (VNF).

MANO Manipulation: By infiltrating the orchestration layer, an attacker can control how network services are deployed, injecting malicious VNFs or intercepting data.

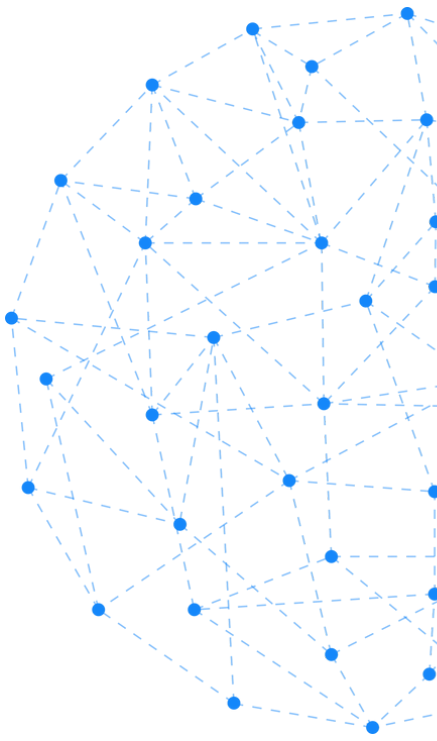
XECURITYPULSE

CASE STUDY:

SALT TYPHOON EXPLOITATION IN A 5G SA ENVIRONMENT

Salt Typhoon's attack on a 5G SA network demonstrates its capability:

- **Initial Access:** Exploit an API vulnerability in the AMF exposed through an unpatched out-of-band router interface
- **Lateral Movement:** Deploy the Demodex rootkit on a Kubernetes node hosting SMF and UPF containers
- **Persistence:** Hide malicious processes and manipulate logs using kernel-mode rootkit techniques
- **Exfiltration:** Extract Call Detail Records (CDRs) from Unified Data Management (UDM) and transfer the data through a compromised router interface to an external Command-and-Control (C2) server



XECURITYPULSE

DETECTION AND EVASION TECHNIQUES

Salt Typhoon's operations stand out due to its advanced techniques for avoiding detection and ensuring consistency in compromised systems. Below are the five main methods employed by the group:

6.1 LIVING-OFF-THE-LAND TECHNIQUES

It uses legitimate system tools like WMI and PowerShell, making it hard to distinguish from normal operations.

6.2 POLYMORPHIC PAYLOADS AND ENCRYPTED COMMAND-AND-CONTROL (C2)

The communication between the affected system and the C2 server is fully encrypted using TLS, ensuring data encryption privacy. These polymorphic techniques allow payloads to bypass even the most advanced intrusion detection systems (IDS).

6.3 ROOTKIT PERSISTENCE AND EVASION

Salt Typhoon's Demodex rootkit works at the kernel level and manipulates Windows APIs to hide processes, files, and registry entries. The rootkit can evade detection by anti-malware solutions even when the system is scanned, extending its presence on the target computer.

6.4 OBFUSCATION AND ANTI-FORENSIC TECHNIQUES

The group uses advanced techniques to eliminate traces of its presence. Payloads are heavily obfuscated to hinder reverse engineers from analyzing them. Log tampering and selective deletion are used to cover tracks, complicating post-incident investigations.

6.5 FRAGMENTED PAYLOAD DELIVERY

Salt Typhoon splits its payload into smaller fragments to bypass network security measures. The fragments are distributed separately and collected only after reaching the destination. This method avoids detection by network monitoring tools tuned to identify complete payloads.

XECURITYPULSE

PREVENTIVE MEASURES AND MITIGATION STRATEGIES

7.1 PATCH MANAGEMENT

Regularly update patch vulnerabilities, especially those in Microsoft Exchange Servers, VPNs, and firewalls.

7.2 NETWORK SEGMENTATION

Enforce strict network segmentation to prevent lateral movement.

7.3 ZERO TRUST ARCHITECTURE

Implement a Zero Trust Security model for strict access controls and continuous validation to eliminate unauthorized access.

7.4 ADVANCED THREAT DETECTION TOOLS

Deploy behavior-based anomaly detection tools and Endpoint Detection and Response (EDR) solutions to identify and mitigate advanced threats.

7.5 KERNEL-LEVEL MONITORING

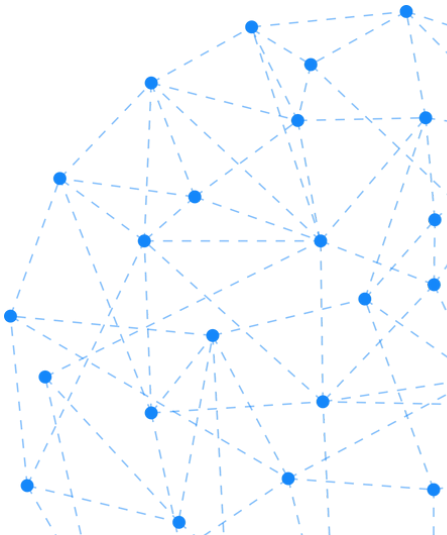
Use tools like Sysmon and Falco to monitor kernel-level changes and detect suspicious rootkit behavior.

7.6 INCIDENT RESPONSE PLAN

Develop and regularly test incident response plans to handle breaches effectively.

7.7 MULTI-FACTOR AUTHENTICATION (MFA)

Enforce MFA to prevent credential-based attacks.



7.8 LOGGING AND MONITORING

Enable SIEM systems to log and monitor for suspicious activity.

7.9 THREAT HUNTING

Conduct proactive threat-hunting exercises to identify and eliminate dormant threats.

7.10 RED TEAM ASSESSMENTS

Perform regular penetration testing and red team exercises to simulate attacks.

XECURITYPULSE

RECOMMENDATIONS FOR 5G SECURITY TEAMS

To protect against dangerous threats like the Salt Typhoon, 5G security teams must adopt a Zero-Trust security model to authenticate all devices and users. Strengthening API security, maintaining external group controls, and implementing small steps will help reduce attackers' ability to move across the network. Proactively patching vulnerabilities in network functions, virtualized environments, and management layers will further minimize the attack surface.

Additionally, a combination of real-time threat intelligence and advanced analytics tools ensures teams stay ahead of ever-changing attack tactics, enabling early detection and rapid response to suspected threats.

Integrating comprehensive incident response plans, regular threat-hunting exercises, and kernel-level monitoring will help identify persistent threats like rootkits and encrypted command-and-control channels. Security teams must focus on ongoing training and international operations to improve skills and readiness. By carefully applying these technologies, 5G networks will be hardened against state-sponsored APTs and future-proofed against key threats and critical infrastructure.

XECURITYPULSE

HOW XECURITY PULSE CAN HELP

9.1 SECURITY ASSESSMENTS AND THREAT MODELING

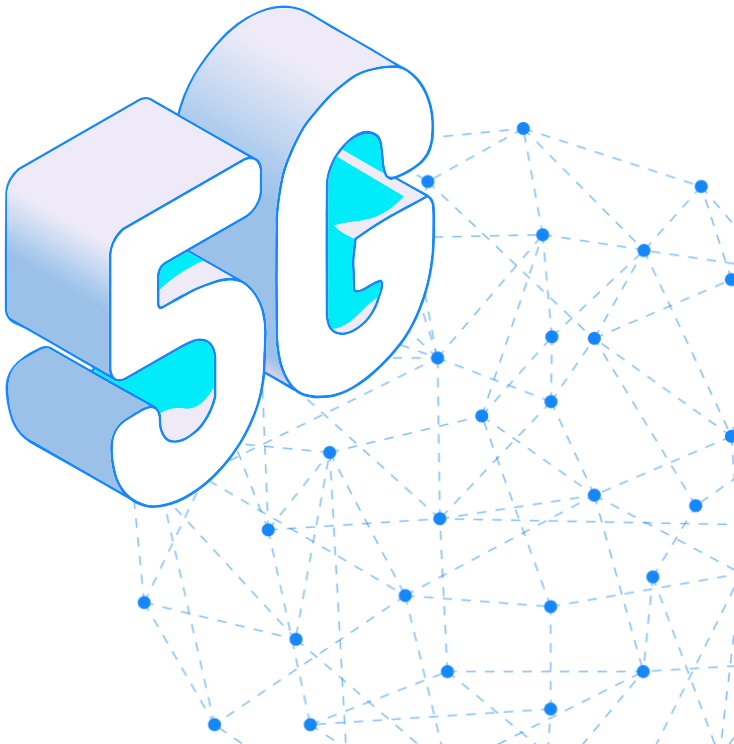
We perform detailed security assessments to detect vulnerabilities in your SBA architecture and out-of-band interfaces, providing threat modeling to identify risks before deployment.

9.2 ROOTKIT DETECTION AND INCIDENT RESPONSE SOLUTIONS

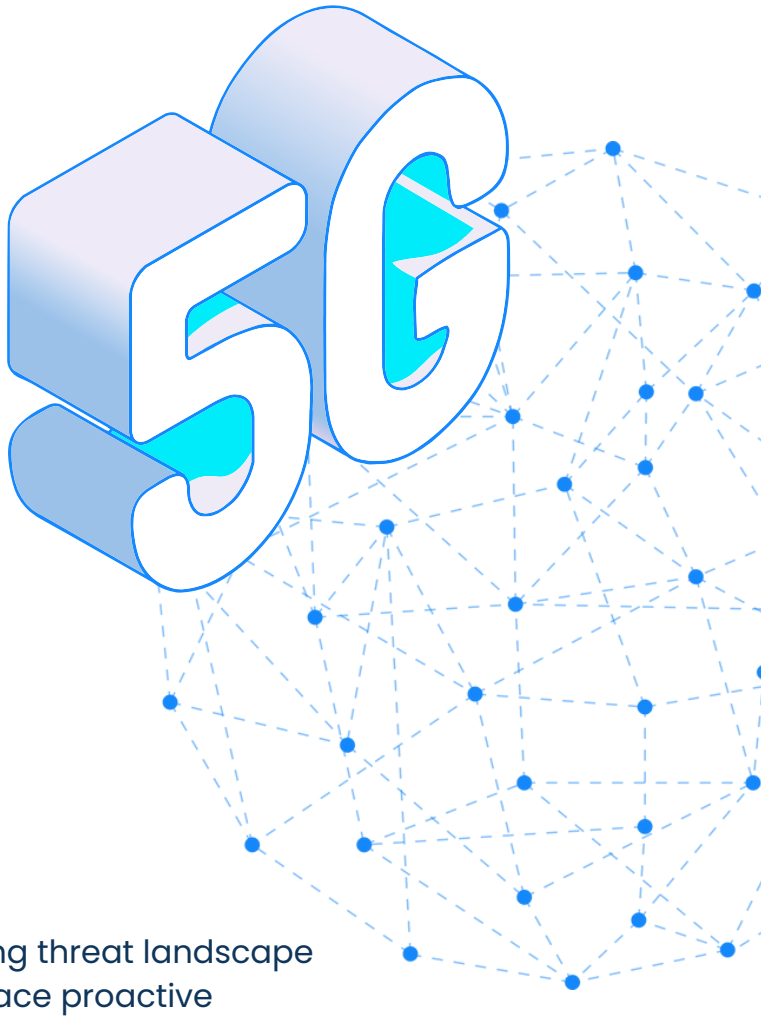
Our expert incident response solution uses AI-powered analytics and rootkit detection tools to identify hidden threats and ensures a fast and effective response to security breaches.

9.3 CUSTOM TRAINING AND SECURITY WORKSHOPS

Our custom training and security workshops focus on 5G-specific threats and Zero Trust practices to ensure your team has the tools to detect, prevent, and respond to advanced threats.



XECURITYPULSE



CONCLUSION

The Salt Typhoon attacks show the evolving threat landscape of 5G networks. Organizations must embrace proactive defenses, adopt Zero Trust frameworks, and continuously adapt their security strategies. With Xecurity Pulse as your partner, your 5G network can be protected from the most dangerous threats.

Are your 5G networks prepared to withstand sophisticated attacks like Salt Typhoon?

Don’t Wait for an Attack—Secure Your Networks Now!

Contact Xecurity Pulse today for a FREE Security Consultation and take the first step toward 5G resilience against state-sponsored threats!

XECURITYPULSE

REFERENCES

- **3GPP Technical Specifications**
  - https://www.3gpp.org/
- **Salt Typhoon and Advanced Persistent Threats**
  - https://oag.ca.gov/privacy/ccpa
- **5G Security Challenges and Threat Mitigation**
  - Bennis, M., Debbah, M., & Poor, H. V. (2020). "Ultra-reliable and low-latency wireless communication: Tail, risk, and scale." Proceedings of the IEEE, 108(10), 1834-1856. DOI: 10.1109/JPROC.2020.2995743
- **Cybersecurity Frameworks for 5G**
  - https://www.trustarc.com
- **Rootkits and Kernel-Level Threats**
  - Hoglund, G., & Butler, J. (2005). Rootkits: Subverting the Windows Kernel. Addison-Wesley Professional.
- **Zero Trust Security Architecture**
  - https://www.bigid.com
- **APT Groups Targeting Telecommunications**
  - https://www.iapp.org
- **NFV and 5G SBA Vulnerabilities**
  - https://www.nist.gov/privacy-framework
- **Detection and Evasion Technique**
  - https://edpb.europa.eu

XECURITYPULSE

THANK YOU!

XECURITY-PULSE
SUPPORT@XECURITYPULSE.COM
HTTPS://XECURITYPULSE.COM/