4.0

# Attacks on virtualised infrastructure

**With the rollout of 5G, the industry is migrating to cloud-based network elements and infrastructure. This virtualised infrastructure can be implemented through 'virtual machines' and 'containers'. Containers can provide a process-level separation between workloads that make them quick and cheap to deploy.**

As product and function-related software can now run on a range of non-proprietary platforms, operators ensure that whatever combination of hardware and software they use, it stays secure. This includes ensuring that the software is up to date, is running on original and authentic hardware and that it hasn't been altered by an unauthorised party.

Here are some recent examples of attacks on virtualised infrastructure.

- Mandiant reported[19] an incident in Microsoft Azure whereby the attacker employed malicious use of the Serial Console on Azure Virtual Machines (VM) to install third-party remote management software within client environments.
- SentinelLabs reported[20] a threat activity, labelled 'WIP26', targeting telecommunication providers in the Middle East. WIP26 was characterised by the abuse of public cloud infrastructure – Microsoft 365 Mail, Microsoft Azure, Google Firebase, and Dropbox – for malware delivery, data exfiltration and command & control (C2) purposes.
- The Ermetic research team reported three vulnerabilities in the Azure API Management service[21]: two Server-Side Request Forgery (SSRF) vulnerabilities and a file upload path traversal on an internal Azure workload. As the vulnerabilities were shared via coordinated disclosure, they have been fully patched. The GSMA encourages disclosure of vulnerabilities to CVD schemes to enable them to be assessed and patched (where required) before the vulnerabilities are more widely disclosed. The GSMA's CVD scheme[22] provides a mechanism for reporting and addressing industry-wide vulnerabilities that do not affect a single vendor or company.

## Analysis

5G is designed to be cloud-native and 6G is likely to further rely on cloud and virtualised network infrastructure. As such, virtualised infrastructure is an important and growing component of mobile networks, as demonstrated by:

- The specification for emerging 5G standalone core networks relying on cloud and virtualised infrastructure
- The O-RAN Alliance specifications[23] include the concept of supporting 'O-Cloud' infrastructure.
- Mobile Edge Compute (MEC) solutions, which move core functions closer to the network edge, usually entailing the use of virtualised infrastructure.

[19] https://www.darkreading.com/cloud/microsoft-azure-vms-highjacked-in-cloud-cyberattack
[20] https://www.sentinelone.com/labs/wip26-espionage-threat-actors-abuse-cloud-infrastructure-in-targeted-telco-attacks/
[21] The Azure API Management service is a fully managed platform that enables organizations to create, manage, secure and analyse their APIs across all environments
[22] GSMA | CVD Programme
[23] O-RAN Specifications

Correspondingly, some national telecom security regulations have prioritised increased security controls for virtualised and cloud implementations. The cloud providers are responding to these regulations by releasing public documents[24] that demonstrate how their services meet some of the new government mandates.

For containerised deployments, the underlying kernel and resource scheduling is shared between every container running on the host within the same trust domain. However, a single kernel-level vulnerability might allow an attacker to impact the underlying host and, therefore, all concurrent containers. This force-multiplier means that identified vulnerabilities must be remediated as quickly as possible to minimise the attack window and the attack impact. 2023 saw reports[25] from hosting providers and the French Computer Emergency Response Team (CERT-FR) warn that attackers were continuing to target VMware ESXi servers that were unpatched against a two-year-old remote code execution vulnerability to deploy ransomware.

A virtualised, multi-vendor solution-stack may result in security considerations moving from being the responsibility of the network vendor to being the responsibility of the MNO. For example, in the case of an integrated product from a single vendor, the internal design and integration of the hardware platform, virtualisation and software modules are the sole responsibility of the vendor. With a disaggregated approach, the underlying virtualised platform, virtualisation code and application code may be sourced from different vendors. The responsibility for these components working together in a secure manner will rest with the operator (or its systems integrator/lead vendor).

The security of virtualised and cloud infrastructure is, and will continue to be, vital. A successful attack on such infrastructure can have widespread effects at significant scale. However, there is substantial guidance available to help secure virtualised solutions, including how to manage distributed trust relationships. The GSMA has recently updated its Baseline Controls[26] adding further guidance specifically on network function virtualisation and there is ongoing activity within the GSMA's Open Infrastructure Group (closely linked to Linux Networking Foundation's Anuket[27] project). GSMA document FS.33[28] Network Function Virtualisation (NFV) Threats Analysis provides a detailed view of identified threats and guidance on appropriate countermeasures.

[24] E.g. https://d1.awsstatic.com/whitepapers/compliance/Considerations_on_the_UK_Telecommunications_Security_Act.pdf and https://docs.aws.amazon.com/pdfs/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.pdf
[25] https://www.databreaches.net/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide-more-than-500-systems-affected-already/
[26] https://www.gsma.com/security/resources/fs-31-gsma-baseline-security-controls/
[27] https://lfnetworking.org/anuket-orinoco-released/
[28] A GSMA member-only document