

Credential leak leading to BGP attack

Original report published on: Jan 03, 2024^[1]

Executive Summary

Leaked credentials of a network administrator account belonging to Spain's second largest mobile operator, Orange, was used by a malicious actor to perform a Border Gateway Protocol (BGP) attack and caused around 3 hours of Internet outage^[2].

Background

On 3 January 2024, the Regional Internet Registry (RIR) for Europe, the Middle East, and Central Asia, known as RIPE, stated that a compromise of an administrator account had "resulted in some services of the account holder being temporarily impacted"^[3].

The RIPE administrator account of Orange, Spain's second largest mobile operator, was compromised. The threat actor sabotaged their BGP routing by modifying the autonomous system (AS) number associated with the company's IP addresses and enabled an invalid Resource Public Key Infrastructure (RPKI) configuration^[1], leading to around 3 hours of Internet outage^[2]. An X (previously Twitter) user 'Ms_Snow_OwO' claimed responsibility for the attack, stating that there was no financial motivation behind it and that it was done for entertainment^[4].

Researchers discovered that the credential leak happened on 4 September 2023, months before the attack^[5]. Orange's RIPE account used a weak password that had not been changed since the leak and did not have two-factor authentication (2FA) set up^[1].

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validating of existing security controls to ensure detection and prevention against the MITRE ATT&CK techniques identified in this advisory:

- Refer to the MITRE ATT&CK techniques in this advisory and create detection rules and deny processes related to these techniques if there is no business need.
- Create and enforce a password policy with adequate complexity requirements or use an access management system.
- Maintain good password hygiene by not reusing or sharing passwords, implementing a password expiry policy and using a VPN for logins whenever possible.
- Enable multi-factor authentication (MFA) on your Asia-Pacific Network Information Centre (APNIC) or RIPE accounts and/or accounts that has access to your BGP routing and RPKI configuration.
- Implement alerts for APNIC/RIPE account usage for monitoring.






IMDA encourages organisations to conduct thorough analysis to identify potential risks and assess their potential impact prior to deploying defensive measures.

MITRE ATT&CK Tactics and Techniques^[1]

Tactic	Technique ID	Technique Name
--------	--------------	----------------

Persistence	T1547.001	Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder
Privilege Escalation	T1055	Process Injection
Defense Evasion	T1497	Virtualisation/Sandboxing Evasion
	T1112	Modify Registry
	T1564.004	Hide Artefacts: NTFS File Attributes
Credential Access	T1056	Input Capture
Discovery	T1012	Query Registry
	T1082	System Information Discovery
	T1120	Peripheral Device Discovery
Collection	T1056	Input Capture
Exfiltration	T1041	Exfiltration Over Command-and-Control Channel

References

1. ^ [“Hacker hijacks Orange Spain RIPE account to cause BGP havoc”](#) .
2. ^ [“Digging into the Orange España Hack”](#) .
3. ^ [RIPE NCC Access: Security Breach Investigation](#) .
4. ^ [X \(Previously Twitter\) thread by @Ms_Snow_OwO](#) .
5. ^ [“Infostealer infection of an Orange employee results in BGP disruptions”](#) .