FGT5018.004 Theft of assets

Description: An adversary accesses a shared site, or remote location, with intent to steal valuable materials (such as copper, batteries, and fuel) for resale.

As towers are often located in remote locations, base stations are prime marks for thieves and vandals in search of an easy target. These sites contain a wealth of valuable copper wire, high-performance batteries, and fuel. Thieves and vandals take advantage of remote locations of cell sites by trespassing freely, without the fear of being identified. Copper wires and battery theft exploit the second-hand market fueled by the worldwide demand for these goods.

Labelling:

* Sub-techniques: N/A.
* Applicable Tactics: Impact

Metadata:

* Architecture Segment: PHYS & Env
* Platforms: remote/shared location physical assets
* Access type required: Physical
* Data Sources: Incident and event monitoring
* Theoretical/Proof of concept/Observed: Observed

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Cable/Copper Theft | Copper’s value transforms remote cellular base stations into prime targets for thieves. The costs for telecom and tower operators to replace the cost of the cable and damage to the site can be thousands of dollars per incident. This is not taking into consideration the additional costs of loss of network service. Even the theft of a small amount of copper can cause extensive damage to site equipment, costing cell towers owners thousands of dollars in repairs, replacement, and network downtime. There are several expensive copper items at cell sites that are very attractive to thieves, such as the **ground wires, copper grounding busbars, and waveguides** |
| Battery Theft | Battery theft can easily become the root cause of cell services outage. Similarly, to the case of cable theft, telecom towers are increasingly affected by the rise of battery theft and vandalism incidents. |
| Fuel Theft | Fuel is a major asset at telecom sites that can easily and directly be sold by thieves. The threat of diesel theft is widespread in many emerging markets and even in the rural areas of the developed markets. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM5005 | Implement physical and environmental controls  Shared/Remote sites should be provided with a full set of physical and environmental controls aimed to assure access control, monitoring, continuity of operations and protection against environmental disasters. Failure to do so may lead to unauthorized access, destruction of assets and impairment of operations. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Improper security monitoring of remote/shared facilities | Remote/shared sites have to be integrated in the network-wide Security Incident and Monitoring System, but with additional considerations: development of use-case specific alert rules, integration and correlation of data at all levels (network, application), integration and correlation with service provider -level monitoring mechanisms. Failure to do so may leave advanced or sustained threats undetected, as well as technical failures or malfunctions of local resources. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Physical assets and commodities | Physical assets and commodities used by the mobile network operators in their infrastructure. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5012 | Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed. Additional considerations: development of use-case specific alert rules, integration and correlation of data at all levels (network, application), integration and correlation with service provider-level monitoring mechanisms. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Service unavailability | Theft of these assets may cause an unavailability of resources. |
| Increased maintenance costs | Theft of these assets may cause an increase in maintenance costs for the operator. |

References

|  |  |
| --- | --- |
| Name | URL |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, page 202, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| Baars, J. “Telecom Sites Physical Security White Paper”, December 2019, Asentria | https://www.asentria.com/blog/telecom-sites-physical-security-white-paper/. |