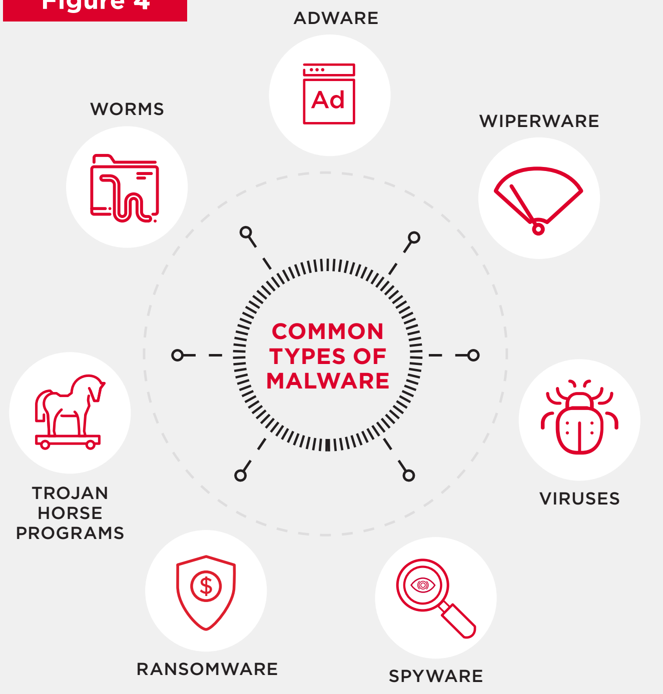
7.0 Malware & Ransomware

The wide reporting and severe nature of many malware[45] and ransomware[46] attacks mean this threat continues to be a major security consideration for MNOs and other enterprises. Common types of malware are shown in the diagram below.

A joint report[47] provided a technical analysis of the Infamous Chisel malware that targeted Android devices used by the Ukrainian military[48]. Infamous Chisel comprises a collection of components designed to enable remote access and to exfiltrate information from Android devices (see the joint report[49] by national agencies that provides a technical analysis of the malware). When successfully deployed, it undertakes periodic scanning of files and network information for subsequent exfiltration.

Malware can be engineered to undertake remote code execution and propagate wider fraud attacks by sending smishing messages, as well as other fraud schemes, such as SMS AIT (where large volumes of SMS are sent to high cost destinations) and abuse of direct carrier billing (where the customer's account is used to pay for digital goods and services).

Figure 4



[45] Malware' is short for 'malicious software' and is the generic term for any computer programme that is written with the intent of performing acts on a computing device without the knowledge or permission of the owner or user of that device

[46] Ransomware is a type of remote malware-enabled cybercrime whereby the attacker initiates a successful compromise of a target system, then seeks to extort a ransom payment in return for restoring data, or not exposing or deleting data.

[47] https://www.cisa.gov/news-events/analysis-reports/ar23-243a

[48] https://ssu.gov.ua/en/novyny/sbu-exposes-russian-intelligence-attempts-to-penetrate-armed-forces-planning-operations-system

[49] https://www.cisa.gov/news-events/analysis-reports/ar23-243a

Below are some examples of malware and ransomware attacks in 2023:

- Dish reported[50] a ransomware attack that caused a network outage that affected internal servers and IT telephony and extracted certain data from the corporation's IT systems.
- Lumen reported[51] that a malicious intruder had inserted ransomware into some of the company's servers that support a segmented hosting service.
- Attributed[52] to a campaign named 'Operation Triangulation', one form of malware utilises an undisclosed zero-day exploit in Apple's iMessage platform, enabling it to execute code without user interaction or elevated privileges. Once the device is infiltrated, the malware proceeds to download additional malicious payloads to the compromised device, allowing for further C2 and data collection.
- Roaming Mantis group campaigns have targeted every continent[53], with Africa, Asia, and Europe the most impacted. Additionally, 14 MoqHao[54] malware family C2 servers have been identified, according to some reports. Whilst MoqHao's delivery infrastructure has a short shelf life, its C2 infrastructure has been used for extended periods of time and, in some cases, reused after periods of inactivity.
- Reportedly[55] a new version of a Mirai (IoT botnet) variant called RapperBot has been identified that focuses on installing malware. RapperBot appears to contain large chunks of Mirai source code, but modified to include a new protocol for C2 communications and a built-in feature for brute-forcing SSH servers.

Analysis

Malware and ransomware represent a significant, enduring and ongoing threat to the mobile industry, its customers and wider service provider supply chains. The mobile industry (along with all others) has to accelerate its ability to patch and mitigate vulnerabilities. The time it takes to exploit a vulnerability has moved from weeks to days and there are skilled and motivated groups who are including newly published exploits in their toolkits. Although an accelerated patching process is not a panacea, making this a company priority will mitigate a large number of commonly-exploited attacks.

Related defences include:

- 'sinkholing' known malware download sites,
- ensuring fallback and off-site data recovery arrangements are fully tested and operational,
- implementing network segmentation to make lateral movement harder to achieve,
- deploying technical solutions to detect and block malicious inbound SMS spam to the network
- and providing a well-established route for reporting malware issues to operators where the information should flow through to the cyber-security and fraud teams.

Government action has stepped up too, for example:

- the advent of the StopRansomware[56] initiative and joint advisories[57] for network defenders that detail various ransomware variants and ransomware threat actors.
- UK NCSC Guidance: Mitigating malware and ransomware attacks[58].
- CISA Advisory aimed at stopping ransomware[59] [60].

[50] https://www.sec.gov/ix?doc=/Archives/edgar/data/1001082/000155837023002254/dish-20230223x8k.htm
[51] https://d18rn0p25nwr6d.cloudfront.net/CIK-0000018926/32a7d44f-2b57-4acc-8307-665dedf21348.pdf
[52] https://www.blackhatethicalhacking.com/news/operation-triangulation-malware-strikes-ios-devices-worldwide/
[53] https://www.team-cymru.com/post/moqhao-part-3-recent-global-targeting-trends
[54] This Chinese threat actor is known for its DNS hijacking campaigns, where they "redirect" visitors from websites
[55] https://www.darkreading.com/remote-workforce/new-mirai-variant-employs-uncommon-tactics-to-distribute-malware
[56] https://www.gov.uk/government/news/efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware-joint-statement
[57] For example, this advisory providing known Royal ransomware IOCs and TTPs https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
[58] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
[59] https://www.cisa.gov/stopransomware
[60] https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware