From: Eva Ljungbert
Sent: Mon, 24 Jan 2022 15:25:44 +0100
To: N Registrator
Subject: Updated Material & Exchange of Views DMA
Attachments: 211122_MSC_DiscussionPaper_SecurityProofing.pdf, Nokia_Threat_Intelligence_Report_2021_Report_EN.pdf
Categories: PK

Från: Maija Corinti Salvén <mcorinti@apple.com>
Skickat: den 24 januari 2022 13:50
Till: Eva Ljungbert <eva.ljungbert@regeringskansliet.se>
Kopia: Linn Berggren <linn.berggren@regeringskansliet.se>; Marcus Boklund <marcus.boklund@regeringskansliet.se>
Ämne: Updated Material & Exchange of Views DMA

Dear Eva, I hope you had a good start into 2022!

The year starts by keeping us busy on the DMA, with the trilogue now on the agenda. Especially the European Parliament’s latest extension of interoperability requirements in Art 6.1.f is concerning to us; and also the security concerns around side-loading remain.

My colleague Marc and I would be very happy to exchange views with you on these points, or any others that might be relevant to you. Please feel free to propose time slots for a call over the next weeks.

Please also allow me to send you some material - incl. summaries - which you may find insightful.
As this included an MSC paper, I wanted to ask whether you might be attending the Munich Security Conference event now in February? This could be an opportunity to catch up in person, if you were interested.

With kind regards,
Maija

MAIJA CORINTI SALVÉN

HEAD OF GOVERNMENT AFFAIRS • NORDIC • BALTIC • SUISSE •
+49 (0)151 6186 9310 • maija@apple.com

Munich Security Conference Discussion Paper:

The MSC issued a paper on the need to cyber-security proofing EU digital legislation.
It explicitly mentions the DMA’s sideloading has unintended consequences on security as it may "***open the door to malware and ransomware attacks at a time when malicious (state or non-state) actors, whether their goal is infiltrating governments for intelligence or businesses for financial gain, increasingly target individuals and their mobile devices***."

Oxera Report on DMA Amendments
https://ddei5-0-ctp.trendmicro.com:443/wis/clicktime/v1/query?url=https%3a%2f%2fwww.oxera.com%2fwp%2dconte

nt%2fuploads%2f2022%2f01%2fOxera%2dReview%2dof%2dDMA%2damendments%2dFinal%2dreport%2d2022%2d01%2d10.pdf&umid=85EE0CD9-D653-6A05-9D2B-7F31BE490BE4&auth=b32f7072cb1370b7b119b85843019516260d8fac-2b0401b0e15b26ffee34593d6f1a23b28203434d
This report, commissioned by the CCIA, includes a number of concrete examples, case studies and recommendations, e.g.

On Platform Governance:

- The emphasis should be on limiting user exposure to unsafe software and content, inline with the DSA's objectives.
- A sole focus on integrity and end-user's ability to protect themselves will lessen existing protections.
- 6.1.c will reduce the gatekeeper's ability to identify and manage security threats and may increase the chances of malware infection.

On Interoperability Requirements:

- The definition of interoperability proposed by Parliament risks forcing disproportionate levels of third party integration across the board, by precluding an API approach which is more suitable to 6.1.f requirements. Full interoperability of specific services might not be necessary, and instead may have an impact on communication services and end-to-end encryption in particular.
- Free of charge access to functionalities would lead to expropriation and reduce incentives to innovate.
- Compliance timelines are too short to deliver effective third party access requirements while minimising governance issues. Longer compliance timelines should be an option within the specification process and regulatory dialogue.

Nokia's 2021 Threat Intelligence Report

Nokia's yearly Threat Intelligence Report finds that Android was responsible for over 50% of malware infections in 2021.
In contrast, iOS's percentage was so small in 2021 that it was lumped into the category of "other".
Additionally, if you look at the top 10 of the 20 most common types of Android malware listed in the report you find that 5 of the top 10 were installed directly via sideloading.