Research Proposal: Analyzing the Breadth of the Supply-Chain Attack on Android Consumer Devices

Budington, William
Public Interest Technologists
Electronic Frontier Foundation
San Francisco, USA
bill@eff.org

***Abstract*—A marked uptick in the presence of malware at the point of sale in consumer Android devices has been noted by researchers. This proposal seeks to explore new methods of accounting for the breadth of the supply-chain attack, and explore policy venues for addressing this ongoing danger to consumers**

I. Motivation

In January 2023, security researcher Daniel Milisic discovered malware which came bundled with Android TV set-top boxes produced by manufacturers AllWinner and RockChip.[1] The malware reached out to domains publically known to be Command and Control (C2) servers, downloading and extracting a Stage-1 payload which facilitated carrying out a sophisticated click-fraud attack.

The researcher reached out to the author of this proposal noting similarities with characteristics the author had previously found on a separate malware sample.[2] As a result, the author separately ordered and independently verified the findings of the researcher, publishing a blog post to raise awareness of the dangers to consumers.[3]

Separately, researchers at HUMAN Security investigated the click-fraud operation and other functions the malware in question was performing, uncovering further functionality such as usage of the infected devices as residential proxies for remote operators.[4] Peeling back the layers on the entire operation, researchers at HUMAN's Satori Threat Intelligence group discovered further details about the hardware supply chain creating and distributing malware controlled by the same C2 operators.[5]

On the tail of the HUMAN Security report, we at the EFF found it our duty as a public interest nonprofit to raise these issues to the FTC in an open letter which was sent in Novemnber, which was also sent to CISA director.[6]

While some aspects of the operation became clearer, many questions still remain. Android devices manufactured by large brands wishing to protect their reputation are not affected by this type of attack, but the affected devices came from no-name manufacturers largely based in China, supplying cheaper hardware than their well-known competitors. What devices other than the ones we've observed are involved in such supply-chain attacks? How widespread is this operation and ones like it? What is the likelihood that a given Android device from a little-known manufacturer comes preloaded with malware, exposing consumer to significant risks? Are there other motivations, other than profit, at play in such attacks? What risk do consumer-end devices in close network proximity to critical infrastructure pose? An industry-wide survey which focuses on uncovering both the risk of exposure for a consumer to such an attack and the prevalence of such devices is the first step in answering these questions.

II. Description of Idea

Without having insight into which specific models are infected with malware, we are unable to perform an "outside-in" analysis of how widespread supply-chain attacks of various sorts are—no vendor can supply sales figures for an unknown set of infected devices. It is therefore necessary to take a different approach which takes this unknown set as a given.

Random sampling may be one effective approach. Selecting a number of devices from different little-known manufacturers and performing an in-depth analysis of these devices to uncover any malware included at the point of sale. Generalizing findings over a random sample to the larger industry may provide some powerful insights.

Backbone internet infrastructure providers may also be able to provide statistics to quantify the scope of an attack. Metrics of residential IP addresses reaching out to known C2 servers would give important insights. Researchers at our own Threat Lab would be interested in collaborating with others who find this important research worthwhile to follow up on.

Acknowledgment & Funding

This proposal is wholly funded by the Electronic Frontier Foundation (EFF), and is a project of the Public Interest Technologists team internal to EFF. EFF is a 501(c)3 nonprofit with over thirty thousand members, and our own funding sources have also been publicly disclosed.[7] This research project does not have a discreet budget of its own, but is incorporated in ongoing research EFF regularly conducts to guide internet development in a direction beneficial to the public interest. We would like to thank all the generous individual and organizational donors that have made this research possible.

References

[1] https://github.com/DesktopECHO/T95-H616-Malware

[2] https://www.eff.org/deeplinks/2022/04/anatomy-android-malware-dropper

[3] https://www.eff.org/deeplinks/2023/05/android-tv-boxes-sold-amazon-come-pre-loaded-malware

[4] https://www.humansecurity.com/hubfs/HUMAN_Report_BADBOX-and-PEACHPIT.pdf

[5] https://www.humansecurity.com/learn/blog/badbox-peachpit-and-the-fraudulent-device-in-your-delivery-box

[6] https://www.eff.org/press/releases/eff-urges-ftc-address-american-resellers-malware-android-tv-set-top-boxes

[7] https://annualreport.eff.org/#financials