Mobile Malware

Part of Malware Intelligence

Now is the time for Mobile Malware

With the continued advancement of smartphone capabilities and our own dependency on them for both work and pleasure, it's more important than ever to protect your device. Organizations around the world have recently been pushed further towards flexible working and servicing for both their employees and their customers, and this carries a certain risk. With more and more data, credentials and other sensitive information being stored and transmitted from smartphones, how can you ensure your customers and employees are as protected as possible?

Struggling to keep up

At the moment, organizations are struggling to properly protect their customers' and employees' mobile devices due to limited knowledge about malicious apps, active malware families, new variations and versions. There is simply so much information to go through, organizations can't be expected to accurately identify the most relevant and credible threats to mobile users without a little help.

Quality over quantity

Intel 471 has the solution to this growing problem. We provide a constant, up to date source of information about apps that can potentially target devices. With a constantly evolving threat, identifying the most relevant and critical Android malware threats is paramount to an organization taking proactive steps to mitigate any damage. With our global network we access APK information from so many sources beyond the forums, we help you understand, identify and even eliminate threats based on our expert knowledge of the most likely tools, techniques and procedures a malicious actor might use. We also provide targeted alerts and reports based on customer requests, giving focus to response teams, rather than just bombarding you with everything we can access.

Key values

- Build up a comprehensive picture of the Android malware landscape by combining in-depth analysis and tracking of mobile malware families and instances with tracking of the actors behind the development, sale and use of mobile malware across the underground.
- Use our rich feeds of timely and high-fidelity indicators to detect Android malware instances and prevent mobile malware from establishing communications with command and control centers.
- Obtain detailed analysis of new variants and families as they appear, including indicators, command and control (C2) locations, C2 commands, raw binaries, overlays.
- Mobile Malware tracks the top tier families focused on systems access, information stealing and financial fraud to allow you to detect and prevent account takeover, 2FA bypass, fraud and data leakage from employees or customers.
- Mobile Malware is a key feature of our Malware Intelligence product, which makes this package even more valuable to our customers.

About Intel 471

Intel 471 empowers enterprises, government agencies, and other organizations to win the cybersecurity war using near-real-time insights into the latest malicious actors, relationships, threat patterns, and imminent attacks relevant to their businesses.

The company's TITAN platform collects, interprets, structures, and validates human-led, automation-enhanced results. Clients across the globe leverage this threat intelligence with our proprietary framework to map the criminal underground, zero in on key activity, and align their resources and reporting to business requirements. Intel 471 serves as a trusted advisor to security teams, offering ongoing trend analysis and supporting your use of the platform.

Talk to an expert:

https://www.intel471.com