Android bank app users targeted in sophisticated malware attack - blueAPACHE

Canonical: https://www.blueapache.com/blog/android-bank-app-users-targeted-in-sophisticated-malware-attack

Details:

Android bank app users targeted in sophisticated malware attack - blueAPACHE Services Services Integrated services to keep your technology secure, reliable and ready to scale. View All Services Managed Services Proactive IT support and monitoring Managed Service Bundles Advanced Infrastructure Managed Services Field Services & Staff Augmentation Managed Services Security Integrated security and response emPOWER Security Exposure Management Governance, Risk & Compliance Human Risk Management Managed Detection & Response Security Cloud Cloud, backup and recovery emPOWER Cloud Public Cloud - Microsoft Azure Azure Local Disaster Recovery as a Service Offsite Backup as a Service Private and Public SaaS Backup Storage as a Service (Private S3) Cloud Connectivity Secure business connectivity emPOWER SASE emPOWER Core Network & Data Centre Interconnect Connectivity Collaboration Voice, meetings and collaboration Microsoft Teams Zoom RingCentral Collaboration Procurement Simplified technology procurement blueapache.store Procurement Microsoft Practice Microsoft cloud, security and AI Microsoft Practice Consulting & Advisory Tech strategy and specialist advice Consulting & Advisory Industries Industries Technology services shaped around the needs of your industry. View All Industries Healthcare & Aged Care Secure IT for healthcare providers Not for Profit Practical IT for not-for-profits Financial Services Secure IT for financial services Professional Services Reliable IT for professional teams Transport & Logistics Always-on IT for transport operations Retail & Consumer Services Connected IT for retail businesses Utilities Resilient IT for essential services Government & Public Sector Secure IT for public services Resources Resources Explore insights, stories and events shaping the future of technology. Research Insights and research for IT leaders Case Studies Real outcomes from partnerships Blog News, ideas and practical advice Events Upcoming and past events About About Learn more about blueAPACHE, our people, story and partnerships. About Us Who we are and how we work Our Story Our journey since 1998 Careers Build your career with blueAPACHE Leadership Team Meet the people leading blueAPACHE Our Partners The partners behind our solutions Awards Most awarded mid-market IT provider Contact us Contact Us Blog Android bank app users targeted in sophisticated malware attack Share on social Facebook Link Linkedin Link Linkedin Link Play Video Written By blueAPACHE Date Published March 11, 2016 Read Time 4 minute/s Hot on the tail of our recent article on new Android malware discovered by Palo Alto Networks (and the scary numbers released by Bitdefender), ESET has identified that a new trojan named Android/Spy.Agent.SI is mimicking banking and other financial applications on Android devices. According to media releases, millions of customers of Australia and New Zealand’s largest banks may be targeted. Discovered January 29 2016, the trojan is also known as HEUR:Trojan-Banker.AndroidOS.Agent.au (Kaspersky) and Android.SmsBot.539.origin (Dr.Web). The malware presents victims with a fake version of the login screen of their banking application and locks the screen until they enter their username and password. Using the stolen credentials, the thieves can then log in to the victim’s account remotely and transfer money out. They can even get the malware to send them all of the SMS text messages received by the infected device, and remove these. “This allows SMS-based two-factor authentication of fraudulent transactions to be bypassed, without raising the suspicions of the device’s owner,” explains Lukáš Štefanko, ESET Malware Researcher who specialises in Android malware. In its current state, the Trojan spreads as an imitation of Flash Player application. After being downloaded and installed, the app requests administrator rights to protect itself from being easily uninstalled from the device. It then checks if any target banking applications are

installed on the device, and if they do, it downloads fake login screens for each banking app from its command and control server. When the victim launches a banking app, a fake login screen appears over the top of the legitimate app, leaving the screen locked until the victim submits their banking credentials. It currently targets major banks in Australia, New Zealand and Turkey. In fact, the 20 financial institutions currently targeted by the app include the largest retail banks in each of the three countries. Examples of the fake overlays are: The full list of targeted banks include: ANZ Bank, Commonwealth Bank, National Australia Bank, Westpac, St. George Bank, Bendigo Bank, Bankwest, Me Bank, ASB Bank, Bank of New Zealand, Kiwibank, Wells Fargo, Finansbank, Halkbank, VakfBank, Garanti Bank, Yap Kredi Bank, Akbank, Türkiye Bankas and Ziraat Bankas. “The attack has been massive and it can be easily re-focused to any another set of target banks,” warns Lukáš Štefanko. Hackers can make millions if they get the malware model right, as we saw with cryptolocker . Successes like cryptolocker mean there will always be people and organised groups trying to develop new ways to exploit devices and systems. Fortunately, there are things you can do to protect yourself. If you see anything masquerading as Adobe Flash Player on Android, you can be sure it’s fake. Flash Player hasn’t created a client for Android since 2012, so it is highly unlikely anything legitimate is still making the rounds on the mobile platform. Only install mobile apps from the official Google Play Store rather than third-party sites. Add antivirus to your devices. This will only detect known threats, but may pick up something you miss. Last but not least, if you do become infected with Android/Spy.Agent.SI, you can remove the malware by disabling the fake Flash Player’s administrator privileges in Settings or by removing it while in Safe Mode. As always, we encourage all clients to add employee training on spotting potential security threats to their training programs. While this trojan targets banking applications, it could easily be modified to target business applications or services, presenting an entirely different array of issues for organisations. For more information on security, or educating your staff on how to identify malware before it becomes an issue, contact the blueAPACHE account team . News Related Articles View All News July 27, 2026 News You’ve Invest in Security. So Why Are Breaches Still Happening? Understanding the balance between prevention, detection and response in a modern Microsoft 365 environment. June 26, 2026 News EOFY 2026: The Reset Is Done – Now It’s About Getting Ahead By Jean Roux, CFO of blueAPACHE As we reach EOFY, the conversations I’m having with IT leaders are starting to sound very similar. … May 19, 2026 News Why Every Business Needs AI Guardrails We’re working with a growing number of clients who are adopting AI tools across their business. The technology is powerful, … February 27, 2026 News Ransomware Incident Response: Why Paying the Ransom Is a Failure of Preparation For our vCISO, the early months of 2026 have sharpened focus on the disciplines that ultimately decide whether a ransomware … January 15, 2026 News The 7 Cyber Truths Boards Must Act On In 2026 The cyber threat landscape has evolved at lightning speed. Attackers are no longer lone hackers; they’re organised, AI-powered, and industrialised. … December 22, 2025 News Reflecting on an Outstanding 2025 – Thank You for Your Partnership As we approach the end of 2025, I want to take a moment to extend my heartfelt thanks for your … December 22, 2025 News The blueAPACHE e-Store: IT purchasing made simple Have you checked out blueAPACHE e-Store yet? Designed to make sourcing IT hardware and consumables faster and easier, the portal … October 28, 2025 News Building Our Cyber Safe Culture: A Practical Guide for CSAM 2025 October marks Cyber Security Awareness Month (CSAM) in Australia, and this year’s theme ‘Building our cyber safe culture’ calls for … Ready to Outpace Change? Partner with blueAPACHE to improve performance, strengthen security and simplify complexity through IT Operations Excellence as a Service. Speak to our team Get Support Need expert support? How can we help? Support Remote Access Client Portal 1300 135 548 (Australia) +61 3 8696 9369 (International) Email Support Speak to our team Sitemap Home Services Industries About Our Story Leadership Team Careers Partners Research Case Studies Blog Events Support Contact We acknowledge the traditional owners of the lands where we work and live, and the people of those lands. We pay our respects to Elders past and present, and extend that respect to all Aboriginal and Torres Strait Islander people.