Mphasis
The Next Applied

The TeaBot Android Banking Trojan

Date: 01st June 2024 | Severity: High

Summary

The TeaBot Android banking Trojan targets banking apps mostly in Europe, in countries such as the United Kingdom, Belgium, Italy, Spain, Germany, and the Netherlands.

Attack Vectors

- The TeaBot Android banking Trojan targets banking apps mostly in Europe, in countries such as the United Kingdom, Belgium, Italy, Spain, Germany, and the Netherlands. It supports six languages: Spanish, English, Italian, German, French, and Dutch. Sometimes, the TeaBot banking Trojan was distributed alongside other banking malware, such as FluBot (AKA Cabassous).
- TeaBot usually spreads via smishing campaigns, in which SMS messages are sent to the victims, enticing them to download a seemingly legitimate application, or directing them to compromised websites from which the app could be downloaded. TeaBot uses various types of malicious apps, such as media players (e.g. VLC MediaPlayer), delivery services (e.g. UPS), streaming apps (e.g. TeaTV), and antivirus software (e.g. Kaspersky). Once the app is installed on a victim's device, communication with a command and control (C2) server is established and the TeaBot payload is executed targeting predetermined banking apps.
- Like other banking malware, TeaBot is capable of collecting system data, accessing the device's contact list, intercepting and managing SMS messages, logging keystrokes, taking screenshots, triggering overlay attacks via Accessibility Services to steal credentials and credit card information, and gaining full control of the device. The malware can also steal Google Authentication 2FA codes and disable security software. The obtained data is exfiltrated to a remote C2 server every 10 seconds.
- In May 2024, Zsclaer reported an increase in TeaBot instances being distributed through malicious apps in Google Play, such as PDF and QR code readers. Malware infections were observed in the United States, the United Kingdom, Germany, Spain, Finland, South Korea, and Singapore.

Indicator of compromise

INDICATOR TYPE	INDICATORS
File Hash	• c0c8be7a8cdef01a9e10b7899fc734704abd60fc50073b4e6416b17654a15dab • 784ade29f486e0446e7a5e4d07591e7bd3e2ccf3fcf3470ef042db44e0aae191 • 70d51d4d8673adf1bc53b742cc10b388bf1d6b1fd60bb73e66acc6e202693709 • ad3886b8517d41dfd73068b40e1d56bf5a6cc55dd187063a468dda21252a47b1 • 770b95a7894b32b139a9bf93bfaf7d26 • 6089aed8ad4e6c9ef2324050ac1c1f2d68c614e922916c2dcf52ed2812b9939b • ad8ee869e34892d79f8a93976b56ca723a4f7931f0719821e86f4bc21c68c905 • 638f5a51aca3308e00418dc119a481feb0f72b04041a9a7fafce8587b74f62da • df3a29f9b6fa7a7da495a4bc2cf55ea1922b64cf57fc0d491ec8648069d35e7f • f76696a3eb8f42bfa0bed2788a5a22586308698fe603ec2764ae4d48e599164a • 66308f9b10ec24b5666fb541e14a70ef46340541d5b6b680ba21d883da0eb740 • 7b6f3be55480e07e5364fc49c629ca192dcdf22feb99f4542f9ae98069c076d0 • 779004c05f535a070c7e7baa04b6332e3bf84e7962c1656714cebd9c5d96b49a • 112fc4be91ef529db595c9cdc40fdc82 • e82b7c1de78e08afca72e5fb059afa3e47852ee80217c96ff907cbe8abe4c2b8
Domains	• ohk4ose4on4npserho[.]top • kopozkapalo[.]xyz • kolaosmaoiamal[.]top • sepoloskotop[.]xyz • zoposoekaoejn[.]top • awehsjslpjanoad[.]top • be[.]keytradebank[.]phone • vivid[.]money • ssedonthep[.]biz • sityinition[.]top
Urls	• 1http://185[.]215[.]113[.]31:84/api/botupdate • http://gaweawgeaweg232[.]top/api/ • http://batroslunk[.]top/api/ • http://185[.]215[.]113[.]31:84/api/getkeyloggers • https://becorist[.]com/trani • http://91[.]215[.]85[.]55:85/api/ • https://menusand[.]com/86[.]apk • http://178[.]63[.]27[.]182:84/api/botupdate • http://178[.]63[.]27[.]182:84/api/ • https://becorist[.]com/juranfile
IP Address	• 37[.]1[.]218[.]149 • 178[.]32[.]130[.]170 • 185[.]215[.]113[.]31 • 178[.]32[.]130[.]175 • 91[.]215[.]85[.]55 • 185[.]215[.]113[.]39

Recommendation

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- Prioritize remediating known exploited vulnerabilities.
- Enable multifactor authentication (MFA) for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- Regularly patch and update software and applications to their latest version and conduct regular vulnerability assessments.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.infosecurity-magazine.com/news/teabot-banking-trojan-activity/
- https://www.zscaler.com/blogs/security-research/technical-analysis-anatsa-campaigns-android-banking-malware-active-google
- https://thehackernews.com/2022/03/teabot-android-banking-malware-spreads.html