Safeguarding China Operation (Part 4)

——*Mobile Security Threat Analysis, Response, and Disposal*

Antiy CERT

First draft completed: October 6, 2024

First published: October 6, 2024

The original report is in Chinese, and this version is an AI-translated edition.

On the occasion of the 75th anniversary of the National Day, Antiy CERT has gathered and sorted out the historical work in security event handling, major event analysis, advanced threat analysis, etc. In order to summarize experience, refine rules, and improve deficiencies, our subsequent analysis and response work can more effectively support the national security struggle.

Threat analysis and response is an important capability spectrum of Antiy. Antiy conducts a series of work such as threat perception, capture, analysis, disposal, tracing, reporting, and exposure for attack activities, attack equipment, and threat actors, continuously promotes iterative improvements in core engines and product and service capabilities, and effectively supports public security governance and national security struggles.

Antiy Mobile Security Company (Wuhan) plays an important role in Antiy's analysis and response capabilities. Antiy Mobile Security has developed the Antiy AVL SDK anti-virus engine intelligent terminal version, which is known as the "national-level" engine. It continuously tracks APT attacks, malicious code infections, black and gray production activities, etc. on mobile phones and smart terminals.

Today we bring you **the fourth part of Antiy's emergency response and threat analysis work track - Mobile Security Threat Response and Disposal.**

Antiy Mobile Security Team has been tracking and responding to the rapid growth of Android malicious code and the generalization of security threats to intelligent system platforms. Based on the embedding of a wide range of engines, the spread of malicious code on mobile phones has been effectively curbed. Actively track and analyze the comprehensive migration of mobile security threats to corporate organizations, business fraud, and technical confrontation, continuously analyze the chain of network black and gray production activities, and provide governance support for relevant departments. Antiy Mobile Security Team works in collaboration with Antiy CERT

to improve the cross-platform intelligence clues and sample analysis capabilities in APT attack analysis. In this review, we will sort out the key points around malicious code under mobile smart terminals, as well as the mobile Internet risk application behavior and ecological governance that we have proposed in recent years.

1. Malicious Code

2014.10.13

Text message interception and illegal activities exposed

For the first time, a highly active and highly harmful SMS interception type Trojan was disclosed.

2014.12.10

Chronicle of typical mobile malware

For the first time, it summarizes and publishes the major events of malicious code development on Android and iOS platforms since 2009, as well as typical malicious code screened from massive malicious code libraries.

2014.12.26

PoisonCake In the ROM

Discovered and disclosed a sophisticated malicious code module embedded in ROM.

2014.12.31

2014 Mobile Malicious Pornographic Applications Research Report

Disclose sample behaviors of malicious applications that use pornographic content to induce users to download and install them. These applications are not only suspected of spreading obscene and pornographic content, but may also perform malicious deductions, malicious promotions, steal user privacy, and cause user privacy leaks or economic losses.

2015.02.13

2014 Android Malicious Code Development Report

Released the first full-year mobile malicious code threat landscape report.

2015.04.07

PermAd Analysis Report

privilege escalation vulnerabilities to implement rogue advertising promotions was disclosed.

2015.08.19

Sadstrot Trojan Analysis Report

A complex malicious Trojan was disclosed. After running, the Trojan will steal the user's QQ and WeChat accounts, friend lists, message records, etc., and will use the subtrate hook framework to monitor any information input by the keyboard. In addition, the application will also receive cloud commands to perform remote control operations such as module updates and deletion of specified files, which seriously affects system security.

2015.10.30

Rogue plugin that modifies the install-recovery.sh script

A rogue plug-in that tampers with the phone's startup script is disclosed. Once loaded and run, the plug-in first attempts to request superuser permissions, then maliciously tampers with the phone's startup script and releases a specific repackaged app (app store type) to the system app directory. In addition, the released repackaged app will silently upload the device 's system app information to a remote server, infringing on user privacy.

2016. 02.05

Read all the mobile security news in 2015 in one minute

2015 Mobile Threat Situation Report: 2015 was a year of widespread mobile security threats. A large number of phenomenal cases reflected that the black technology behind them is developing rapidly and gradually completing the transformation from small workshop operations to big data applications.

2016.04.28

Dark • Mobile • Bank Tracking Analysis Report

For the first time, it disclosed the persistent underground black industry attacks and threats against mobile finance and mobile payment systems since 2013.

2016.05.20

Macbeth virus implanted in popular social applications, hundreds of millions of users may be affected

Disclose a globally popular virus sample that tampers with internationally renowned social applications and implants malicious modules.

2016.08.24

Mobile Banking Application Phishing Attack Threat Analysis Report

A sister version of Dark Mobile Bank, this is a targeted phishing attack targeting bank users.

2016.09.19

The first capture of the stubborn virus "Phoenix"

Disclose a very difficult to remove malicious code called Fushicho.

2016.12.02

Antiy Mobile Security responds to the "DressCode" threat and releases enterprise mobile threat inspection tool

We responded to DressCode, a popular Trojan that penetrated corporate intranets through mobile devices, and released an enterprise mobile threat inspection tool.

2017.03.10

2016 Antiy Mobile Security Annual Report: Comprehensive Migration of Threats

The 2016 Mobile Malicious Code Threat Situation Report was released, which was a year in which the amount of malicious code exploded.

2017.06.09

Analysis report on the "Dvmap" Android malware

Analysis report of an Android malware with code injection capabilities

2017.12.15

Analysis of the "Dirty Cow" vulnerability (CVE-2017-1000405)

Dirty COW vulnerability targeting the Android system.

2017.12.24

In-depth analysis of Janus high-risk vulnerabilities

This paper analyzes the principle of the "nuclear-level" vulnerability Janus (CVE-2017-13156) on the Android platform. This vulnerability allows malicious attackers to arbitrarily modify the code in Android applications without affecting their signatures.

2018.03.22

2017 Antiy Mobile Security Annual Report - The rising tide and undercurrents in the process of development

2017 Mobile Threat Landscape Report.

2018.05.22

ZipperDown vulnerability, hype or imminent?

Actual impact assessment of the ZipperDown hotspot vulnerability.

2. Risky Applications

Starting from 2020, based on the generalization trend of mobile threats, Antiy Mobile Security is no longer limited to the threat types defined by traditional malicious code in the past, but discloses application risks with the purpose of infringing on user rights and user security.

2020.09.30

The "Sacred Wine Transfer" APP was exposed for issuing coins in violation of regulations. Antiy's special action on mobile security has achieved initial results

For the first time, a risky application in the name of blockchain was disclosed, which was suspected of illegal pyramid selling.

2020.10.30

With the large-scale infiltration of black and gray industries, is Apple's iOS closed ecosystem really safer?

Research findings on the black and gray market industry chain within the iOS ecosystem

2020.11.18

"Taimugu" APP "Time Investment" is involved in a scam, Antiy Mobile Security has issued a risk warning

Disclosing an APP application that is a time investment scam.

2021. 02.20

[APP advertising chaos] Developers use Deeplink technology to maliciously push ads

Antiy Mobile disclosed the first research report on risky advertising behavior, and subsequently released a series of research reports on the technologies used to implement risky advertising behavior in different ways.

2021.04.15

APP generation platforms are exploited by black and gray industries, threatening the security of the mobile ecosystem

A research report that reveals the chaos on APP generation platforms.

2021.08.17

Infringement of user rights through advertising monetization, advertising issues and technical analysis of online earning apps

Antiy Mobile Security disclosed for the first time the risky advertising behavior of online money-making apps, which involved infringement of user rights.

2021.08.22

Social networking with strangers is gradually becoming a rigid demand, and some industry problems need to be corrected

The first research report on risky behaviors of stranger social apps was disclosed.

2022.01.26

APP Online Generation Platform Security White Paper

A security research report on the APP application ecosystem generated by online generation platforms.

2022.02.21

Mobile Internet Application Supply Chain (SDK) Behavior Security Status Research Report

A research report on in-app SDKs that infringe on user rights and conduct risky behaviors.

2022.03.12

White Paper on Risky Applications of Mobile Internet (2021)

Released the full text of the first white paper on mobile Internet risk application technology.

2022.03.18

The secret behind the female anchor

Published several research reports on the black and gray industrial chains behind the social APP ecosystem, involving guilds.

2022. 06.21

Analysis of Typical Problems in Social App Channel Distribution Monitoring

Disclosure of risk issues regarding applications distributed through social APP channels.

2022.06.23

Research on application hot update technology trends and risk issues

A research report on the risks of hot update behavior of applications.

2022.07.23

Case Study on User Security Issues in the Quick App Ecosystem

Disclose application risk issues in the quick application ecosystem for the first time.

2022.09.06

The problem of illegal inducement to pay in the payment process of App needs urgent attention

A series of disclosure reports have been released regarding risk issues such as paid apps inducing payments.

2022.12.27

False offers, suspected disguised gambling risks, blind box applications and other issues that need to be regulated urgently

First disclosure of a research report on the risks associated with blind box apps.

2023. 04.11

The current status and security risks of AIGC technology behind ChatGPT

Disclose research on risk issues of apps that utilize AIGC-type technologies.

2023.06.06

Issues such as vulgarity and pornography in voice dating apps and non-compliance with probability games need urgent attention.

The first research report on the risks of voice dating platforms was released.

2024.01.29

Conduct joint governance exploration focusing on gambling and fraud risks associated with social media applications

Disclosure of gambling and fraud risks associated with social media apps and platforms, and exploration of ecological governance measures for related behaviors.

2024. 06.14

[Euro Cup Special] "Fire the gun at online gambling!"

Exposing the black and gray industry chain in the online soccer gambling ecosystem.

2024.09.14

Resurrection! The chaos of pornography and soliciting prostitutes in small circles needs urgent attention

Disclose the risk issues of small circle dating apps.

Appendix: About Antiy

Antiy is committed to enhancing the network security defense capabilities of its customers and effectively responding to security threats. Through more than 20 years of independent research and development, Antiy has developed technological leadership in areas such as threat detection engines, advanced threat countermeasures, and large-scale threat automation analysis.

Antiy has developed IEP (Intelligent Endpoint Protection System) security product family for PC, server and other system environments, as well as UWP (Unified Workload Protect) security products for cloud hosts, container and other system environments, providing system security capabilities including endpoint antivirus, endpoint protection (EPP), endpoint detection and response (EDR), and Cloud Workload Protection Platform (CWPP) , etc. Antiy has established a closed-loop product system of threat countermeasures based on its threat intelligence and threat detection capabilities, achieving perception, retardation, blocking and presentation of the advanced threats through products such as the Persistent Threat Detection System (PTD), Persistent Threat Analysis System (PTA), Attack Capture System (ACS), and TDS. For web and business security scenarios, Antiy has launched the PTF Next-generation Web Application and API Protection System (WAAP) and SCS Code Security Detection System to help customers shift their security capabilities to the left in the DevOps process. At the same time, it has developed four major kinds of security service: network attack and defense logic deduction, in-depth threat hunting, security threat inspection, and regular security operations. Through the Threat Confrontation Operation Platform (XDR), multiple security products and services are integrated to effectively support the upgrade of comprehensive threat confrontation capabilities.

Antiy provides comprehensive security solutions for clients with high security requirements, including network and information authorities, military forces, ministries, confidential industries, and critical information infrastructure. Antiy has participated in the security work of major national political and social events since 2005 and has won honors such as the Outstanding Contribution Award and Advanced Security Group. Since 2015, Antiy's products and services have provided security support for major spaceflight missions including manned spaceflight, lunar exploration, and space station docking, as well as significant missions such as the maiden flight of large aircraft, escort of main force ships, and Antarctic scientific research. We have received several thank-you letters from relevant departments.

Antiy is a core enabler of the global fundamental security supply chain. Nearly a hundred of the world's leading security and IT enterprises have chosen Antiy as their partner of detection capability. At present, Antiy's threat detection engine provides security detection capabilities for over 1.3 million network devices and over 3 billion smart terminal devices worldwide, which has become a "national-level" engine. As of now, Antiy has filed 1,877 patents in the field of cybersecurity and obtained 936 patents. It has been awarded the title of National Intellectual Property Advantage Enterprise and the 17th (2015) China Patent Excellence Award.

Antiy is an important enterprise node in China emergency response system and has provided early warning and comprehensive emergency response in major security threats and virus outbreaks such as "Code Red", "Dvldr", "Heartbleed", "Bash Shellcode" and "WannaCry". Antiy conducts continuous monitoring and in-depth analysis against dozens of advanced cyberspce threat actors (APT groups) such as "Equation", "White Elephant", "Lotus" and "Greenspot" and their attack actions, assisting customers to form effective protection when the enemy situation is accurately predicted.