SECURITYWEEK NETWORK:

- Cybersecurity News
- Infosec Island
- Virtual Events

Security Experts:

WRITE FOR US

SECURITY WEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe
- 2021 CISO Forum
- ICS Cyber Security Conference
- Contact

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - IoT Security
  - Threat Intelligence
  - Endpoint Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance

GriftHorse Android Trojan Infects Over 10 Million Devices Worldwide

By Ionut Arghire on September 30, 2021

A recently discovered cybercrime campaign leveraging mobile premium services has made over 10 million victims worldwide, potentially causing hundreds of millions in losses, according to mobile security firm Zimperium.

To maximize spread, the campaign operators used trojanized applications that posed as harmless software, but which subscribed the victims to paid services that charged them roughly €36 (roughly $42) per month.

The campaign operators started distributing the Android Trojan – which Zimperium calls GriftHorse – in November 2020 through Google Play and third-party stores. The malware has since been removed from Google Play but continues to be distributed via third-party application stores.

To date, users in more than 70 countries fell victim to the attackers, which served them tailored malicious pages, based on geo-location, using the local language. On infected devices, users are bombarded with notifications that they have won a prize, until the offer is accepted.

Once that happens, the victim is redirected to a webpage where they are prompted to provide their phone number for verification. Instead, however, the victim is submitting the phone number to a premium SMS service.

The attack has proven highly successful because it takes advantage of misinformation, curiosity, small phone screens, and the trust users put in local web pages. Furthermore, the attackers attempted to stay under the radar by avoiding hardcoded URLs or the reuse of domains, in addition to serving malicious payloads based on the user's IP address.

According to Zimperium, the attackers likely generated millions in revenue each month, potentially causing hundreds of millions in total losses. Some of the victims are believed to have lost more than €200 (approximately $232) over the course of the campaign.

"The timeline of the threat group dates back to November 2020, suggesting that their patience and persistence will probably not come to an end with the closing down of this campaign. […] The numerical stats reveal that more than 10 million Android users fell victim to this campaign globally, suffering financial losses while the threat group grew wealthier and motivated with time," Zimperium notes.

Related: **Android Banking Trojan 'Vultur' Abusing Accessibility Services**

Related: **Research Shows Many Security Products Fail to Detect Android Malware Variants**

Related: **Fake Netflix App Luring Android Users to Malware**

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

Neiman Marcus Confirms Payment Cards Compromised in Data Breach
Google Patches Two More Exploited Zero-Day Vulnerabilities in Chrome
Threat Actor Promises Pegasus Spyware Protection, Serves Trojan Instead
GriftHorse Android Trojan Infects Over 10 Million Devices Worldwide
New CISA Tool Helps Organizations Assess Insider Threat Risks

Tags:

Mobile Security NEWS & INDUSTRY Virus & Threats Virus & Malware Malware