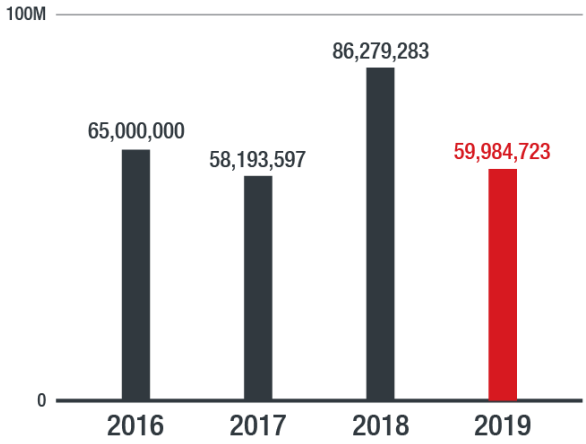
TREND MICRO | research

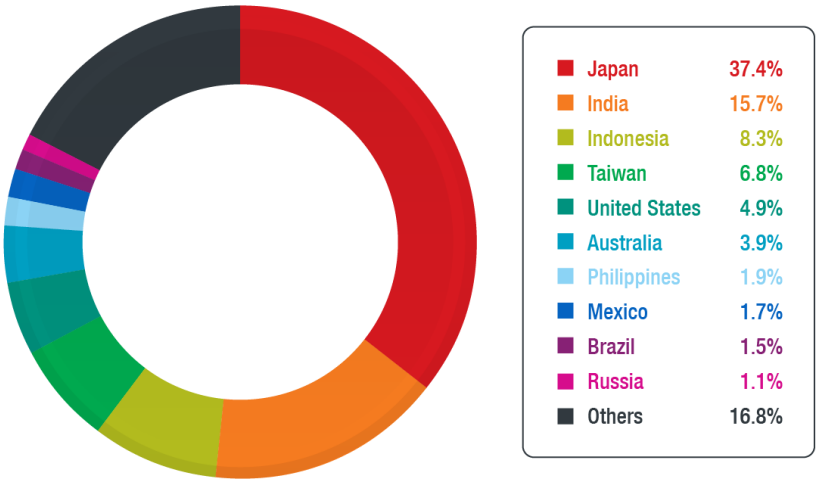
2019 Mobile Threat Landscape

Trend Micro Research

Mobile Threat Landscape

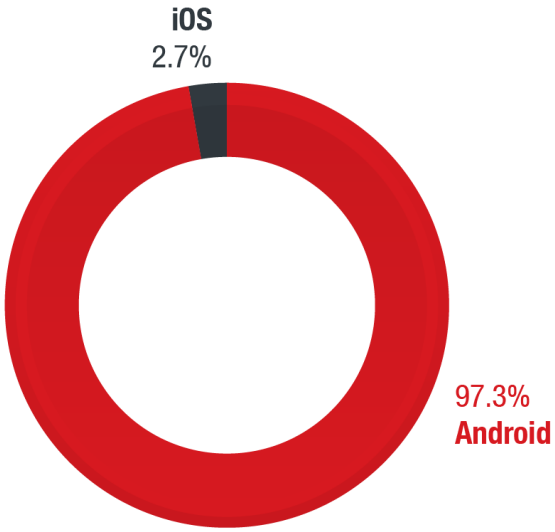


Total number of mobile threats blocked by Trend Micro from 2016 to 2019

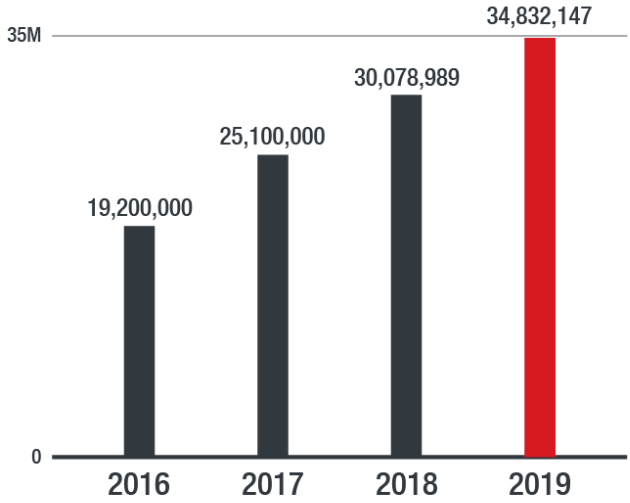


Country distribution of mobile threats detected by Trend Micro MARS in 2019

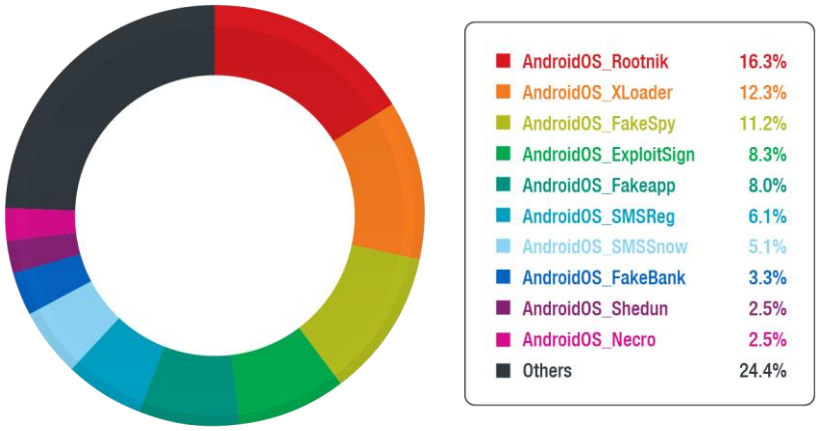
Android and iOS Malware



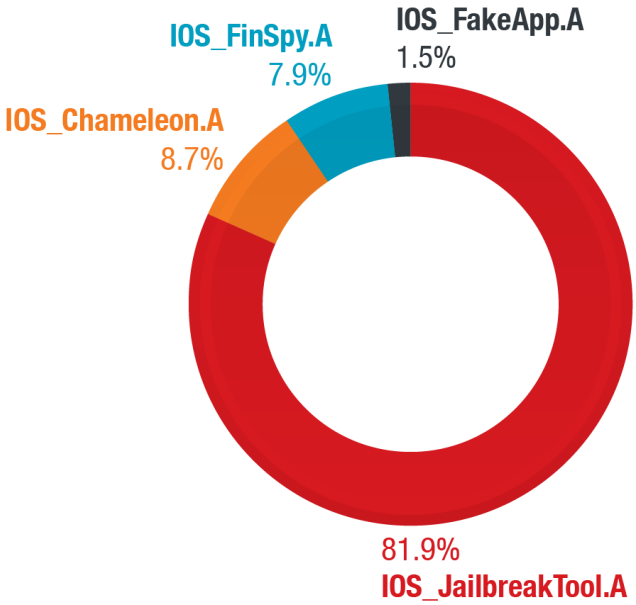
Percentage of malicious Android and iOS applications sourced and analyzed by Trend Micro MARS for 2019



Total number of malicious Android applications sourced and analyzed by Trend Micro MARS from 2016 to 2019

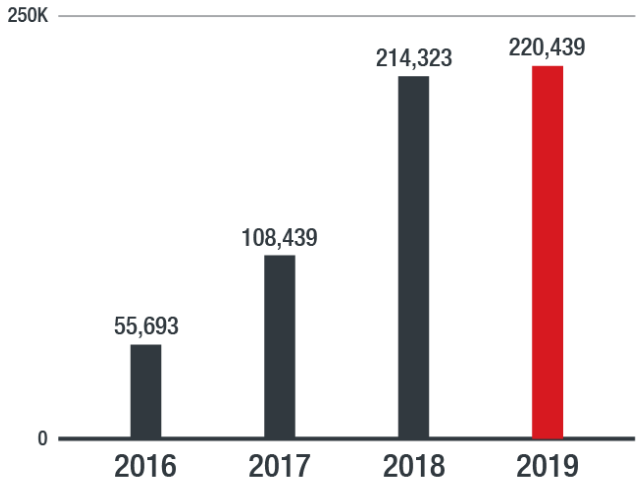


Top Android malware detected by Trend Micro MARS in 2019

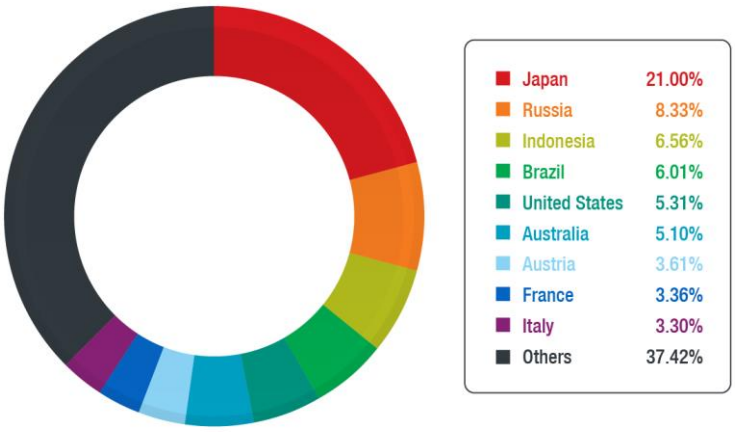


Top iOS malware detected by Trend Micro MARS in 2019

Banking Malware



Comparison of unique mobile banking trojans Trend Micro sourced from 2016 to 2019



Country distribution of mobile banking trojans' impact in 2019

MITRE ATT&CK Framework

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command And Control	Network Effects	Remote Service Effects
Deliver Malicious App via Authorized App Store	Abuse Device Administrator Access to Prevent Removal	Exploit OS Vulnerability	Application Discovery	Access Notifications	Application Discovery	Attack PC via USB Connection	Clipboard Modification	Access Calendar Entries	Alternate Network Mediums	Alternate Network Mediums	Downgrade to Insecure Protocols	Obtain Device Cloud Backups
Deliver Malicious App via Other Means	App Auto-Start at Device Boot	Exploit TEE Vulnerability	Device Lockout	Access Sensitive Data in Device Logs	Evade Analysis Environment	Exploit Enterprise Resources	Data Encrypted for Impact	Access Call Log	Commonly Used Port	Commonly Used Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Drive-by Compromise	Modify Cached Executable Code		Disguise Root/Jailbreak Indicators	Access Stored Application Data	File and Directory Discovery		Delete Device Data	Access Contact List	Data Encrypted	Domain Generation Algorithms	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Exploit via Charging Station or PC	Modify OS Kernel or Boot Partition		Download New Code at Runtime	Android Intent Hijacking	Location Tracking		Device Lockout	Access Notifications	Standard Application Layer Protocol	Standard Application Layer Protocol	Exploit SS7 to Track Device Location	
Exploit via Radio Interfaces	Modify System Partition		Evade Analysis Environment	Capture Clipboard Data	Network Service Scanning		Generate Fraudulent Advertising Revenue	Access Sensitive Data in Device Logs		Standard Cryptographic Protocol	Jamming or Denial of Service	
Install Insecure or Malicious Configuration	Modify Trusted Execution Environment		Input Injection	Capture SMS Messages	Process Discovery		Input Injection	Access Stored Application Data		Uncommonly Used Port	Manipulate Device Communication	
Lockscreen Bypass			Install Insecure or Malicious Configuration	Exploit TEE Vulnerability	System Information Discovery		Manipulate App Store Rankings or Ratings	Capture Audio		Web Service	Rogue Cellular Base Station	
Masquerade as Legitimate Application			Modify OS Kernel or Boot Partition	Input Capture	System Network Configuration Discovery		Modify System Partition	Capture Camera			Rogue Wi-Fi Access Points	
Supply Chain Compromise			Modify System Partition	Input Prompt	System Network Connections Discovery		Premium SMS Toll Fraud	Capture Clipboard Data			SIM Card Swap	
			Modify Trusted Execution Environment	Network Traffic Capture or Redirection				Capture SMS Messages				
			Obfuscated Files or Information	URL Scheme Hijacking				Data from Local System				
			Suppress Application Icon					Input Capture				
								Location Tracking				
								Network Information Discovery				
								Network Traffic Capture or Redirection				
								Screen Capture				

First Active Attack Exploiting CVE-2019-2215 Linked to SideWinder APT Group

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com