■侵入の痕跡（Indicators of Compromise、IoC）

侵入の痕跡（Indicators of Compromise、IoCs）はこちらを参照してください。

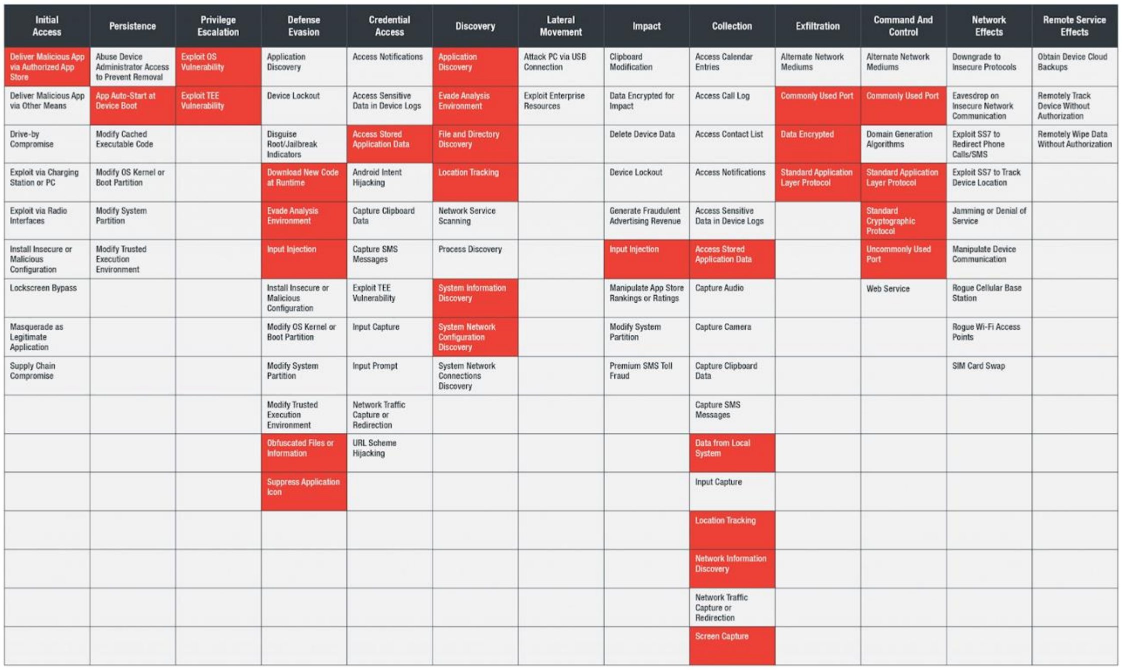
SHA256	パッケージ名／ファイルタイプ	アプリ名／検知名
ec4d6bf06dd3f94f4555d75c6daaf540dee15b18d62cc004e774e996c703cb34	DEX	AndroidOS_SWinderSpy.HRXA
a60fc4e5328dc75dad238d46a2867ef7207b8c6fb73e8bd001b323b16f02ba00	DEX	AndroidOS_SWinderSpy.HRXA
0daefb3d05e4455b590da122255121079e83d48763509b0688e0079ab5d48886	ELF	AndroidOS_MtkSu.A
441d98dff3919ed24af7699be658d06ae8dfd6a12e4129a385754e6218bc24fa	ELF	AndroidOS_BinderExp.A
ac82f7e4831907972465477eebafc5a488c6bb4d460575cd3889226c390ef8d5	ELF	AndroidOS_BinderExp.A
ee679afb897213a3fd09be43806a7e5263563e86ad255fd500562918205226b8	ELF	AndroidOS_BinderExp.A
135cb239966835fefbb346165b140f584848c00c4b6a724ce122de7d999a3251	ELF	AndroidOS_MtkSu.A
a265c32ed1ad47370d56cbd287066896d6a0c46c80a0d9573d2bb915d198ae42	com.callCam.android.callCam2base	callCamm

パッケージ名／ ファイルタイプ	アプリ名／検知名
com.abdulrauf.filemanager	FileCrypt Manager
com.callCam.android.callCam2base	callCamm
com.camero.android.camera2basic	Camero

C&C サーバ

- ms-ethics.net
- deb-cn.net
- ap1-acl.net
- ms-db.net
- aws-check.net
- reawk.net

MITRE ATT&CK Matrix™



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				

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, 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 targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thoughtprovoking research that can shape strategic industry direction. www.trendmicro.com