侵入の痕跡（Indicators of Compromise, IoC）

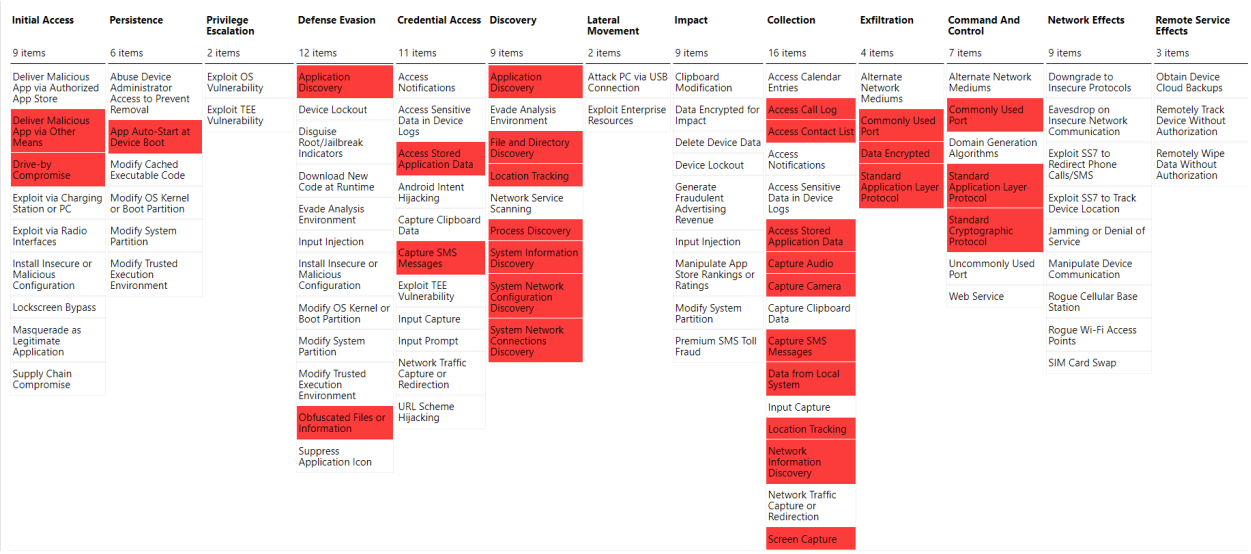
以下の不正アプリはすべて AndroidOS_ActionSpy.HRX として検出されます。

SHA256	Package Name	Label
56a2562426e504f42ad9aa2bd53445d8e299935c817805b0d9b9431521769271	com.omn.vvi	Ekran
b6e2fdbf022cd009585f62a3de71464014edd58125eb7bc15c2c670d6d5d3590	com.isyjv.klxblnwc.r	系统优化
de6065c63f05f8cddaec2f43a3789cca7d8e16221bd04bf3ce8092809b146ebe	com.isyjv.klxblnwc.r	系统优化
2117e2252fe268136a2833202d746d67bf592de819cc1600ac8d9f2738d8d4d6	com.isyjv.klxblnwc	Service Runtime Library
588b62a2e0bffa8935cd08ae46255a972b0af4966483967a3046a5df59d38406	com.isyjv.klxblnwc	Service Runtime Library
d6478b4b7f0ea38947d894b1a87baf4bed7a1ece934fff9dfc233610de232814	com.isyjv.klxblnwc	Service Runtime Library
8d0a123e0fe91637fb41d9d9650a4b9c75b6ce77a2b51ac36f05a337da7afd80	com.ecs.esap	Service Runtime Library
9bc16f635fde4ff0b6b02b445a706d885779611b7813c5607ab88fdff43fcc2f	com.cd.weixin	VWechat
334dbd15289aaeaf3763f1702003de52ff709515246902f51ee87a41467a8e55	com.android.dmp.rec	Recording

50c10ab93910a6e617c85a03f8c38a10a7c363e2d37b745964e696da8f98a93d	com.android.dmp.rec	Recording
6575eeda2a8f76170fb6034944eeda5c88dac8009edccc880124fa729dd3c1fd	com.android.dmp.l	Location
eff30f6cc2d5d04ce4aef0c50f1fb375fb817a803bf3e8e08c847f04658185ba	com.android.dmp.l	Location
a0a48d7e0762ab24b2ec3ec488b011db866992db5392926fe43dd3d1c398e30d	com.android.dmp.cm	Camera
088769a80b39d0da26c676a5a52eaccdb805dc67cba85e562785c375c642b501	com.android.dmp.c	Core
87306b59aaaba0ea92ea6a05feb9366eeb625e8da08ed3ef6c86a5cf394fada5	com.android.dmp.c	Core

Indicator	**Type**
gotossl.ml	Domain used by Earth Empusa
goforssl.top	Domain used by Earth Empusa
geo2ipapi.org	Domain used by Earth Empusa
appbuliki.com	Domain used by Earth Empusa
umutyole.com	Domain used by Earth Empusa
t.freenunn.com	Domain used by Earth Empusa
start.apiforssl.com	Domain used by Earth Empusa
bloomberg.com.cm	Domain used by Earth Empusa
static.apiforssl.com	Domain used by Earth Empusa
cdn.doublesclick.me	Domain used by Earth Empusa
static.doublesclick.info	Domain used by Earth Empusa
status.search-sslkey-flush.com	Domain used by Earth Empusa
http://114.215.41.93/	ActionSpy C&C URL
http://static.doubles.click:8082/	ActionSpy C&C URL

MITRE ATT&CK



Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Impact	Collection	Exfiltration	Command And Control	Network Effects	Remote Service Effects
9 items	6 items	2 items	12 items	11 items	9 items	2 items	9 items	16 items	4 items	7 items	9 items	3 items
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 thought-provoking research that can shape strategic industry direction.

www.trendmicro.com