DARKFON

SECURE VOICE, VIDEO CALLS & MESSAGING

EYEONIX

SAMSUNG | PRIVORO®

THREATS

“Pegasus is military-grade spyware that can remotely hack into mobile phones and take total control of the device. Once Pegasus secretly infects a phone, it can copy messages, photos, emails, record calls and activate microphones and cameras for continuous surveillance without the owner's knowledge. This lets Pegasus transform personal phones into 24/7 monitoring tools for prying government eyes.”

“A zero-click attack takes advantage of vulnerabilities in software to carry out an attack without user interaction. By exploiting this vulnerability, the exploit can install malware or perform other malicious interactions on a user’s device without the target needing to click on a link, open a malicious file or take any other action.”

“Man-in-the-Middle (MitM) attacks involve an attacker intercepting network communications to either eavesdrop on or modify the data being transmitted. While this type of attack may be possible on different systems, mobile devices are especially susceptible to MitM attacks. Unlike web traffic, which commonly uses encrypted HTTPS for communication, SMS messages can be easily intercepted, and mobile applications may use unencrypted HTTP for transfer of potentially sensitive information.”

“MitM attacks typically require an employee to be connected to an untrusted or compromised network, such as public Wi-Fi or cellular networks. However, the majority of organizations lack policies prohibiting the use of these networks, making this sort of attack entirely feasible if solutions like a virtual private network (VPN) are not used.”

IN BRIEF

The system is private and invisible to the national and global communications network

Darkfon is a system installed on customer premises and operated in a suitable, secure installation, isolated from external threats and providing completely secure, un hackable communications.

Darkfon creates an isolated, closed network of users in which all information exchanged is anonymous and completely secure, combining hardware systems and software .

By implementing government-certified secure communication capabilities, the Darkfon system achieves the highest level of security on the market, protecting sensitive communications and ensuring the privacy of communications.

It has state-of-the-art technology tools maximizing all security challenges faced by offline users.

The combination of hardware and software results in strong encryption, secure communication channels and strict access controls to ensure the confidentiality and integrity of all information.

It offers physical tamper resistance, signal isolation, hardware encryption, advanced access controls and secure device management, protecting sensitive information and ensuring the highest level of mobile device security.

The system also protects against unauthorized access and tampering and fully meets the prescribed strict security standards.

IN BRIEF

No interference with other communications systems

Darkfon uses in the field a special Samsung Galaxy S22 device , not marketed outside the US , with built-in Samsung Hypervisor Device Manager (HDM) , Privoro's secure case and an external 4G VPN layer and a special Full Duplex Voice and Video module

Configured security shielding and ultra-secure architecture are applied , in collaboration with the customer’s information security skilled engineers.

DARKFON users will be able to communicate by Voice, Video and Messaging with a simple and common process

Darkfon user's device is disconnected and invisible from any mobile operator and legal or illegal interception systems preventing any type of detection and attack attempt .

Anti-tracking counter-espionage features that provide physical protection to prevent audio and video data from being scanned by third parties.

Protection against malware such as Pegasus , Chrysaor , Hermit, Predator and any other existing or future malware / trojan .

Unable to track user's location .

The wireless transmission is prevented from being detected of the smartphone.

Users are protected from IMSI catchers and other offensive systems especially when traveling to classified businesses or abroad, where they become the target of all relevant national and international agencies.

SAMSUNG - PRIVORO

INSIGHTS

Samsung - Privoro partnership brings highly secure capabilities

The latest partnership between Samsung and Privoro now provides a powerful new security capability: high-assurance control over the radios, sensors, and other hardware peripherals within Samsung's flagship mobile devices. These new hardware controls allow individuals and organizations at risk of targeted cyberattacks to prevent the devices they carry from being used against them to track their location and monitor their communications and data.

Protect against local and remote device attacks

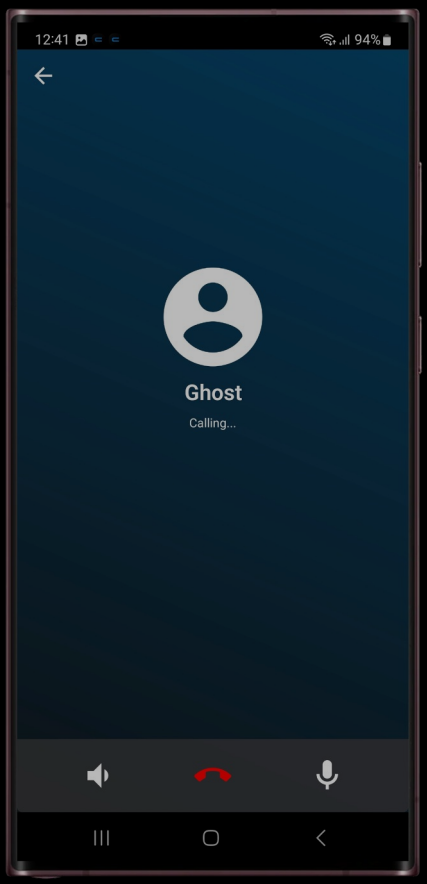
With the mobile device's cellular radio truly disabled, a user is protected from local attacks, including from mobile tracking solutions that monitor your calls, messages, and location data. The joint solution also protects against remote attacks against your device's cellular radio, like those initiated by IMSI catchers (e.g., Stingrays), which attempt to intercept your communications by pretending to be legitimate cell towers. As a second layer of defense, audio masking and physical camera shutters provided by SafeCase ensure no audio or video data can be captured from the device to eavesdrop on the user and their environment.

SAMSUNG - PRIVORO

A defense-in-depth security approach

This two-system, defense-in-depth approach creates a foundation for trusted mobility for security-conscious organizations like federal defense and research agencies as well as corporate entities vulnerable to industrial espionage. By selectively allowing protected and secured mobile devices into controlled workplaces, personnel will have timely access to key resources and can increase productivity through improved situational awareness and faster decision making.

INSIGHTS



PRIVORO Safe Case

INSIGHTS

What is the SafeCase?

The Privoro SafeCaseTM is a first-of-its-kind electronic wraparound companion for smartphones that provides a high-security platform on which features and services can be built.

What is the Anti-Surveillance feature?

SafeCase has built-in anti-surveillance features which provide physical protections
to prevent audio and visual data in the vicinity of the phone from being swept up by third parties who have hijacked the mobile device's cameras and microphones

Prevent mobile surveillance

Smartphone users can keep sensitive information from slipping out in the form of in-person conversations and visuals via device sensors.

Stop location tracking

Individuals can stop broadcasting their movements when needing to protect sensitive locations or block insights into their activities and behaviors.

Prevent wireless attacks

Users can shield their smartphones from IMSI catchers and rogue access points when traveling through chokepoints and other high-risk areas.

Hide from RF detection

Disconnect and "go dark" from the cellular network without potentially drawing unwanted attention from spies or alerting adversaries.

SAMSUNG SDD EMM HS

High Security Version
On Premises Installation

Proven Security
for Classified Mobile Communication

All Data in Transit (DIT) between the EMM server and device is protected via a secure TLS 1.2 channel

Tactical law enforcement and military agencies rely on mobile devices to exchange classified data and mission-critical voice calls. In order to manage these devices, they need to control access and keep sensitive data secure using an independently verified solution

Samsung SDS Enterprise Mobility Management (EMM) for on-premise is the first and only government-grade EMM solution validated for the highest level of security to manage mobile devices and prevent critical data leaks.

Supporting RSA 2048 or ECDSA p256/p384 up to SHA384

All encryption and decryption is done using FIPS 140-2 validated cryptographic kernels

Samsung SDS EMM can use “triggers” in an offline capacity to apply different IT policies based on different network or application conditions

INSIGHTS

Secured by Knox

SAMSUNG KNOX

On Premises Installation

RUNTIME PROTECTION & ENCRYPTION

Periodic Kernel Measurement & Real-time Kernel Protection work to constantly inspect the core software of the OS: the kernel.

These checks ensure that requests to bypass device security are blocked and sensitive data is protected.

SECURE / TRUSTED BOOT AND HARDWARE ROOT OF TRUST

To prevent security measures from being bypassed or compromised, Knox uses Boot- time Protections backed by Hardware Root of Trust to verify integrity of the device during the boot process

Offering multi-layered security, it defends your most sensitive information from malware and malicious threats

INSIGHTS

VAULT

Privoro Vault™

Vault is a two-in-one portable Faraday enclosure and audio masking chamber for smartphones

Vault provides unsurpassed protection against wireless attacks, location tracking, eavesdropping and spying.

Engineered and Manufactured to a Nation-State Threat Model Standard.

Vault mitigates smartphone signals more effectively than any other portable Faraday product, delivering a minimum of 100 dB of radio frequency (RF) attenuation/10 billion times signal reduction. When placed in Vault, a smartphone can no longer be reached via cellular, Wi-Fi, Bluetooth, near-field communication (NFC) and radio-frequency identification (RFID). Integrated audio masking prevents the illicit capture of intelligible audio via the smartphone's microphones in the event that the device has been compromised.

SYSTEM

- 5 x DELL R740 Servers with all necessary software
- SAMSUNG GALAXY S22 Mobiles Special US edition
- DARKFON On Premises Server License
- SAMSUNG SDS EMM High Security On Premises Server License
- SAMSUNG KNOX On Premises Server License
- DARKFON Terminal Users' Licenses
- SAMSUNG SDS EMM High Security Terminal Users' Licenses
- SAMSUNG KNOX Terminal User's Licenses
- Safe Cases H/W
- Safe Cases S/W Tenant
- Safe Case Terminal Licenses
- SAMSUNG HDM Licenses
- Check Point for Terminals
- Secure Mobile Wi-Fi Routers

darkfon@eyeonix.com
www.eyeonix.com