Lookout detects 1.33 million phishing and malicious web links worldwide in Q2 2023.

Content Protection
Advanced Phishing and Content Protection

13M+
400M+

Lookout is a leader in mobile security and threat intelligence.

Stay current on mobile app vulnerability.

Lookout attributes Android surveillanceware (WyrmSpy and Lucky).}

Lookout monitors a wide range of vulnerabilities, their global presence, and their potential impacts to inform you as early as possible. Lookout attributes Android surveillanceware (WyrmSpy and Lucky).

This is a vulnerability affecting Chrome. This may allow remote exploitation and access to sensitive data.

This is an actively exploited vulnerability affecting Chrome and Edge. Attackers can exploit this vulnerability to perform unauthorized actions on your phone.

A company like yours may be restricted based on your license type or user role.

We protect your organization.

Lookout Quarterly: Q2 2023

Contact us

1. Vulnerability 677-2022: Q3 2022
2. Vulnerability 674-2022: Q1 2023
3. Vulnerability 129-2023: Q2 2023
4. Vulnerability 135-2023: Q3 2023
5. Vulnerability 371-2023: Q1 2024
6. Vulnerability 371-2023: Q1 2024
7. Vulnerability 307-2023: Q2 2023
8. Vulnerability 588-2023: Q3 2023
9. Vulnerability 83-2023: Q1 2024
10. Vulnerability 94-2023: Q1 2024
This can lead to a loss of privacy. Unwanted apps can be installed on the device, leading to financial fraud, a loss of privacy, a disrupted user experience, and the installation of hidden ads. It can forward some device information to a third party, including Wi-Fi credentials, numbers, browser bookmarks, locations, financial information, and other device data.

This application can forward user data, including call logs, location, and text messages, to a third party. This can lead to a loss of privacy.

An application can modify other applications, including system apps, and can store sensitive user data on the device. This may involve changes to security controls in place, and can lead to unexpected network traffic and a loss of privacy.

This application may contain legitimate functionality, but can also steal text messages, locations, and other device data. This application helps the user to modify other applications, including system apps, and can install other apps. This can lead to a disrupted user experience, and the installation of hidden ads. It can forward user data, including call logs, location, and text messages, to a third party.

This application can forward sensitive user data to a third party. The types of data sent include call logs, location, text messages, contacts, financial information, and other device data. This application may contain legitimate functionality, but can also steal text messages, locations, and other device data.

This application uses a software development kit (SDK) that contains the capability to access device data, location, and installed apps. This can lead to a degraded user experience, and the installation of hidden ads. It can forward some device information to a third party, including Wi-Fi credentials.
As an extended service, we provide advanced threat intelligence to empower your security team with threat intelligence.

Classification: Trojan
- This application pretends to be legitimate but is malicious.
- It can steal incoming or stored text messages and forward them to a third party. This can lead to a loss of privacy.
- It can steal incoming or stored text messages, contacts, and media to a third party and steal banking credentials. This can lead to financial fraud and a loss of privacy.
- This application extracts sensitive user information, such as SMS messages and contacts lists from the user device, and then transmits the data to a third party. This can potentially be abused to monitor user activities.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a third party. This can potentially be abused to monitor user activities.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.

Classification: Surveillanceware
- This application extracts sensitive user information, such as SMS messages and contacts lists from the user device, and then transmits the data to a third party. This can potentially be abused to monitor user activities.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.

Classification: Riskware
- This application pretends to be benign but is malicious.
- It can also send the device phone until next quarter.
- This application pretends to be a legitimate application but is malicious.
- This application pretends to be legitimate but is malicious.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.

Classification: Benign
- This application pretends to be benign but is malicious.
- It can steal incoming or stored text messages and forward them to a third party. This can lead to a loss of privacy.
- This application pretends to be legitimate but is malicious.
- This application pretends to be legitimate but is malicious.
- This application pretends to be legitimate but is malicious.

Classification: Spyware
- This application extracts sensitive user information, such as SMS messages and contacts lists from the user device.
- This application extracts sensitive user information, such as SMS messages and contacts lists from the user device.
- This application extracts sensitive user information, such as SMS messages and contacts lists from the user device.
- This application extracts sensitive user information, such as SMS messages and contacts lists from the user device.
- This application extracts sensitive user information, such as SMS messages and contacts lists from the user device.
- This application extracts sensitive user information, such as SMS messages and contacts lists from the user device.

Classification: Malware
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.

Classification: Virus
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.
- This application runs secretly in the background and monitors user activity on the device, and then transmits this data to a remote server. This can cause sensitive information to compromise user privacy.