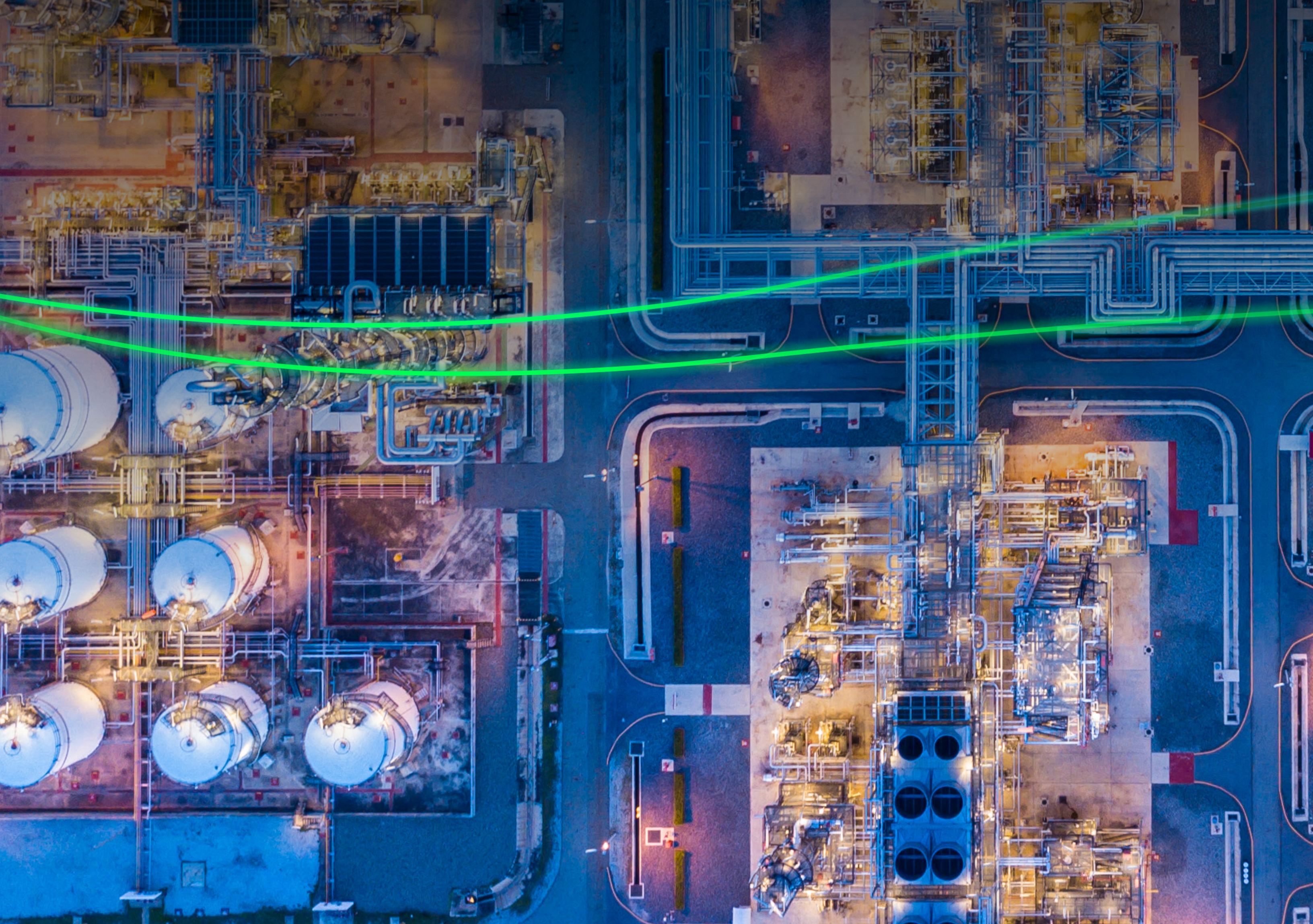
Lookout®

THREAT REPORT

At the Epicenter:

2021 Lookout Energy Industry Threat Report

LOOKOUT DATA SHOWS THE ENERGY INDUSTRY AS THE MOST VULNERABLE WITH SURGING PHISHING ATTACKS AND A HIGH RATE OF APP THREATS



Executive Summary

An Already-Strained Energy Industry is at the Epicenter of Cyberattacks

The energy industry is closely linked to the safety and wellbeing of society. Being responsible for an important part of our global infrastructure, these organizations sit at the center of everything from food supplies, education to healthcare and economic growth.[1]

For this very reason, the industry is also at the epicenter of cyberattacks. 17.2% of all mobile cyberattacks globally target energy organizations, making the industry the biggest target by hacktivists, cybercriminals and nation-state sponsored attackers.[2]

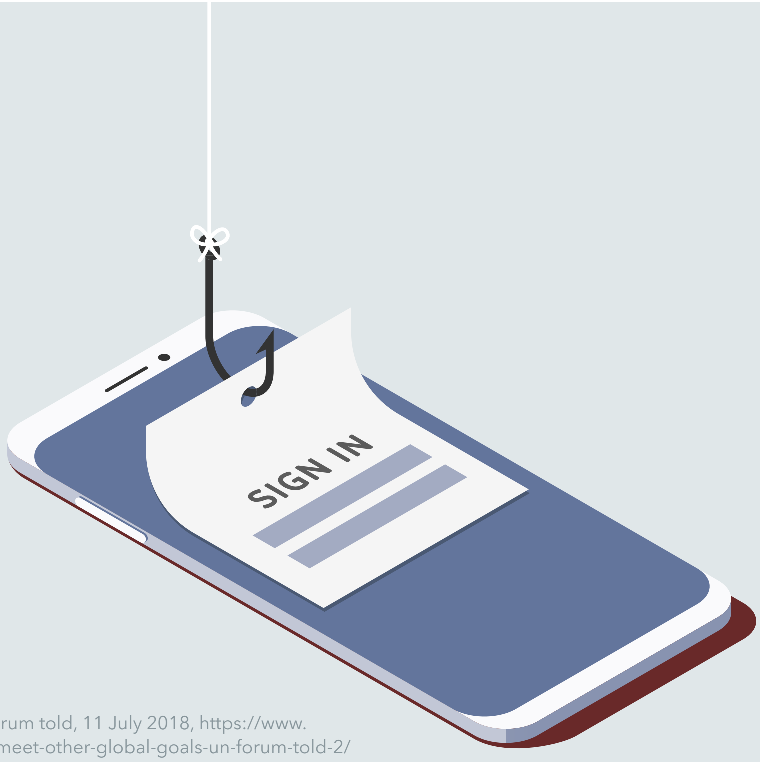
The attack surface of energy organizations is ever-increasing due to complex supply chain relationships and digital transformation initiatives, where organizations are shifting workloads to mobile devices and cloud applications.

Such initiatives enable employees, partners and third-party vendors to remain connected from anywhere. However, this ecosystem exposes energy organizations to significant cyber risks, where a single vulnerability could expose an entire supply chain – as we saw with the SolarWinds and Microsoft Exchange attacks of 2020 and 2021.

To better understand the cybersecurity challenges facing the energy industry, research data was analyzed from the Lookout Security Graph between July 1, 2020 and June 30, 2021. The Graph encompasses telemetry from more than 200 million devices, 150 million apps and detections from Lookout Secure Web Gateway (SWG). Lookout SWG is used by customers to protect against phishing attacks on their mobile devices. Lookout researchers analyzed this information specific to organizations involved in the production and sale of energy, including fuel extraction, manufacturing, refining and distribution.

Key Findings

Reflecting an expanded threat surface, **Lookout found a significant surge in phishing attacks targeting mobile devices.** We also found **a much higher mobile app threat exposure rate compared to other industries**. The report demonstrates that despite high-profile ransomware and surveillanceware cases, **risky apps and other vulnerabilities are more common threats than sophisticated malware.** Our research also found that **many organizations still do not properly secure mobile devices** allowing them to run outdated operating systems with known vulnerabilities.



[1] United Nations, Achieving targets on energy helps meet other Global Goals, UN forum told, 11 July 2018, https://www.un.org/sustainabledevelopment/blog/2018/07/achieving-targets-on-energy-helps-meet-other-global-goals-un-forum-told-2/

[2] Lookout data, Q3 2020 to Q2 2021

Phishing Attacks Surge

20% of energy employees were exposed to a mobile phishing attack in the first half of 2021, a 161% increase from the second half of 2020.

Most Exposed Industry

The average mobile app threat exposure rate was 7.6% – nearly double the average of all other industries combined.

Outdated Operating Systems Rampant

56% of Android users were exposed to nearly three hundred exploitable vulnerabilities by continuing to run out-of-date versions of Android OS.

Education Works

62.5% of employees who were notified they had clicked on a mobile phishing link did not click on another.

Credentials Harvesting Focus

67% of phishing attacks harvested user credentials rather than focusing solely on malware delivery.

Risky Apps Most Damaging

95% of the mobile app threats facing the energy industry were either riskware or vulnerabilities.

Unmanaged Mobile Devices Increasing

Use of unmanaged and BYOD mobile devices increased by 41% over the past 12 months.

Best Practices Decrease Risks

Three basic mobile security safeguards can be implemented to better protect your organization while increasing the use of mobile devices and cloud solutions.

An Increased Need for Mobile Security as the Energy Industry Transforms

The energy industry is not a stranger to cyberattacks. In fact, mobile cyberattacks targeting energy organizations accounted for 17.2% of all mobile attacks globally.

Percent of Mobile Threats by Industry

Energy	Finance	Government	Pharma	Manufacturing
17.2%	14.0%	11.7%	13.1%	10.6%

However, due to significant digital transformation initiatives, historically air-gapped systems are now connected to IT networks, cloud apps and mobile devices. This allows organizations and their partners to create new processes that increase efficiency – including maintenance, management, monitoring, and control of networks, assets and facilities.

Mobility is at the forefront of this transformation: there was a 44% increase in mobile devices connecting to energy organizations over the past 12 months. Both employees and partners use mobile devices to connect to operational technologies, industrial controls systems and sensitive information. These devices increase productivity and are an integral extension of the energy supply chain but many are loaded with a plethora of personal and work apps.

With remote work now a mainstay for most, employees are increasingly using personal smartphones and tablets for work. Lookout found that unmanaged mobile devices in the industry increased 41% over the past year – which means organizations are losing control and visibility over how these devices are used. This places greater emphasis on the need for mobile security to protect against mobile-related risks such as device, app, phishing and network threats.

Mobile Phishing Attacks Surge With No Signs of Slowing

Global Energy Industry Phishing Exposure Rates by Region, 3Q2020 to 2Q2021

	3Q2020	4Q2020	1Q2021	2Q2021	Average
EMEA	10.8%	9.7%	21.1%	21.7%	15.8%
North America	6.8%	7.0%	15.0%	15.9%	11.2%
APAC	2.9%	3.8%	21.8%	24.2%	13.2%
All Regions	7.7%	7.7%	19.1%	20.0%	13.6%
All Other Industries	6.6%	6.2%	14.1%	14.1%	10.2%

Bad actors leverage social engineering tactics such as phishing to manipulate users into performing certain actions – often to either click a malicious link with the intent to steal credentials or deliver malware on a device. Once credentials are obtained, these individuals can access systems, networks, applications or other sensitive data. They employ this covert access to navigate laterally through corporate infrastructure, attempting to identify additional vulnerabilities and valuable information.

Mobile phishing is one of the easiest ways for an attacker to compromise an organization's infrastructure and the energy industry has seen a surge in these attacks. Over the past 12 months, one out of every seven employees (13.6%) was exposed to a mobile phishing attack, which was three percentage points higher than all other industries combined.

Even more surprising, the exposure rate surged significantly during the first half of 2021 when one out of every five employees (nearly 20%) encountered a mobile phishing attack. This was a dramatic increase of 161% over the previous six months.

Europe, the Middle East and Africa (EMEA)

Employees in EMEA are more frequently exposed to mobile phishing attacks than their North American and APAC peers. The average exposure rate in EMEA was 15.8% – or one out of every seven employees, over the past 12 months. This spiked at more than 21% in the first six months of 2021. Part of the reason for this peak is attributed to the large-scale phishing campaign that delivered the Flubot banking trojan across Europe.

Asia Pacific (APAC)

One out of every four employees in APAC (24.2%) was exposed to a mobile phishing attack in the second quarter of 2021, experiencing an astonishing 734% percent increase over the past year.

This spike caused the region to hit an all-time high annual average exposure rate of 13.2% – or one of every eight employees – and is likely due to the region's economic struggles, causing some individuals to turn to cyber and other types of crime.[3]

North America

Phishing exposure rates in North America more than doubled over the past year, with a 134% increase. Organizations experienced an average of attack rate of 13.2% – or one of every nine employees – below the average of their regional peers. The data does not point to a primary cause or event for this dramatic increase.

[3] United Nations Office on Drugs and Crime, UNODC report: Darknet cybercrime is on the rise in Southeast Asia, 25 February 2021: https://www.unodc.org/southeastasiaandpacific/en/2021/02/darknet-cybercrime-southeast-asia/story.html

Credential Harvesting Primary Goal of Phishing Attacks

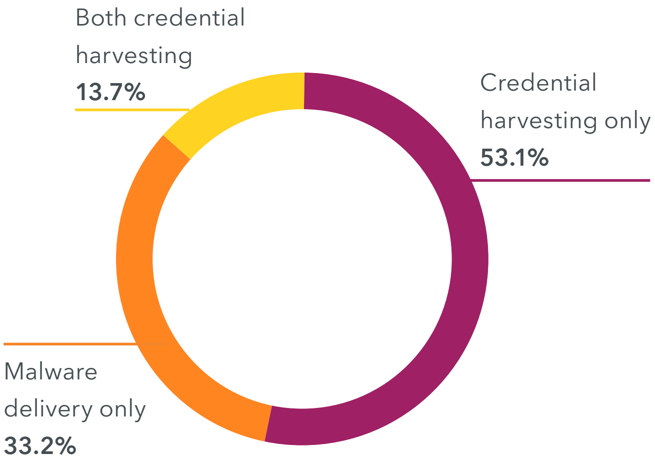
The goals of phishing attacks can be broken into two categories: credential harvesting and malware delivery.

Mobile devices make it easy for attackers to phish for credentials and deliver malware since smartphones and tablets are used for both personal and work. Because devices have a smaller screen and simplified user interfaces, classic telltale signs of phishing are difficult to identify.

Bad actors target employees through the use of infected emails, SMS, messaging apps, social media platforms and mobile websites. Mobile phishing can also exploit any app that communicates to an external site such as gaming, dating apps and even supply chain tools. Information gathered may be used to track the whereabouts of personnel and to capture additional login and password information.

Credential harvesting – or stealing user credentials – is the goal of two thirds (67%) of phishing attacks in the energy industry. Attacks specifically designed for malware delivery was the goal of bad actors one third (33%) of the time.

Phishing Attacks: Credential Harvesting vs. Malware Delivery



Stolen credentials provide everything a threat actor needs to quietly log in to an organization's infrastructure as if they are an employee. Once access is obtained, they can remain undetected for extended periods of time, identifying vulnerabilities and exploiting sensitive data.

In fact, researchers found that on average, vulnerabilities in industrial control systems exist in the wild for more than five years before they are identified and remediated.[4]

VPN access is often a target of credential harvesters who employ phishing schemes. This is because a VPN gives unlimited access to those who use them, giving threat actors free and open access to any app in the organization's infrastructure. In addition, it is difficult to detect anomalous activities indicative of a compromised account or device in a VPN.

Malware delivery – or tricking employees into installing malicious apps to their device – is a lucrative cybercrime. While ransomware is only one example of the many types of malware, companies reported 2,474 incidents to the FBI costing $29.1 million in losses during 2020.[5]

Similar to credential harvesting, malware can be delivered through multiple mobile channels. By leveraging social engineering techniques, attackers trick employees into downloading, installing or clicking on links with malware.

Consequently, the quick detection of intruders and other mobile security vulnerabilities is essential to reducing and mitigating the impact of a breach. Lookout Phishing and Content Protection module, which provides secure web gateway capabilities to iOS Android and Chrome OS devices, helps to speed the identification of corporate breaches and the threat actors who cause them.

[4] Gartner, Market Guide for Operational Technology Security', 13 January 2021 - ID G00737759, p.9

[5] Todd Feathers, The Markup, Why Is Ransomware on the Rise?", 15 June 2021 https://themarkup.org/ask-the-markup/2021/06/15/why-is-ransomware-on-the-rise

Costly Malware and Ransomware on the Rise

Flubot Banking Trojan – The Flubot malware package, discovered in late 2020, manipulated users into thinking they needed to install an app in order to validate, track or receive updates about shipments from Deutsche Post & DHL, Saturn, UPS and others. Once installed, the app intercepted and sent SMS messages, displayed screen overlays and stole contacts. The average cost of a malware attack per organization is $2.5 million.[6]

Ransomware Targeting Energy Industry – The Colonial Pipeline ransomware attack shutdown the pipeline causing gasoline shortages in the eastern United States for five days in May 2021. It targeted the billing system used by Colonial Pipeline, taking advantage of numerous security weaknesses including a weak VPN, unpatched Microsoft Exchange servers and publicly exposed network protocols that could be exploited.

Employee Education Most Effective Prevention Tool

It only takes a single click by an employee to lead to a major breach. As a result, when it comes to phishing, education – not experience – should be the best teacher.

Employees are the first line of defense and, as such, an employee's ability to identify a phishing message is the single-most important defense an organization has against phishing attacks.

However, as phishing attempts become more sophisticated – and less associated with desktop computers – it can be difficult for an employee to identify phishing links. Luckily, threat actors reuse many techniques that employees can easily recognize, if they learn how to look for them on a mobile device. With a better understanding of mobile phishing attacks, employees will learn quickly to not interact with phishing attacks.

As an example, each time a mobile employee is exposed to a phishing site, the Lookout app notifies the user and provides security tips to help them better recognize phishing messages for the future. This method of education proved to be effective.

Number of Mobile Phishing Links Energy Employees Clicked On

Number of links	1	2	3-5	6+
Percent of employees	56.4%	21.8%	16.6%	5.2%

More than half (56.4%) of employees who received a notification from Lookout that they clicked on a phishing link did not click on subsequent mobile phishing links over the past 12 months.

While it is extremely concerning that many users were the target of attacks more than five times over the past year, the good news is that by the sixth phishing attempt, only 5.2% of employees interacted with the threat, a reduction of more than 50 percentage points.

The more in-app education occurred, the less likely employees were to interact with potential threats. Energy organizations need to ensure that they evolve their phishing training beyond desktops and emails to include challenges specifically related to mobile phishing.

[6] Accenture, The Cost of Cybercrime, https://www.accenture.com/t20190305T185301Z__w__/us-en/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

Energy is the Most Exposed Industry to Mobile App Threats

Mobile App Threat Exposure Rates (3Q2020 to 2Q2021)

	3Q2020	4Q2020	1Q2021	2Q2021	Average
EMEA	4.8%	15.1%	4.5%	4.3%	7.2%
North America	6.6%	12.7%	4.3%	2.8%	6.6%
APAC	13.3%	19.9%	7.3%	5.0%	11.4%
All Regions	6.6%	15.1%	4.8%	3.9%	7.6%
All Other Industries (globally)	3.4%	7.0%	3.2%	2.4%	4.0%

App threats within the energy industry far outpace all other industries. On average, 1 out of every 14 employees (7.6%) in the industry encountered a mobile app threat over the past year. These employees are nearly twice as likely to encounter an app threat than employees in all other industries combined.

The global app threat exposure rate in the energy industry reached an all-time high during the last quarter of 2020 with a spike of more than 15% before leveling back down to a more consistent level near 4.4% in the first half of 2021.

Devices in North America had lower exposure rates than other regions. While EMEA had slightly higher exposure rates, organizations in APAC were at greater risk, experiencing a significantly higher rate of 11%.

Within the app threats the energy industry encounters, risk apps and vulnerabilities account for 95% of all threats – with the remaining being malware.

As the energy industry increasingly leverages mobile devices and apps to manage operations, organizations must better understand which app threats are most prevalent, the nature of these threats and how to defend against them.

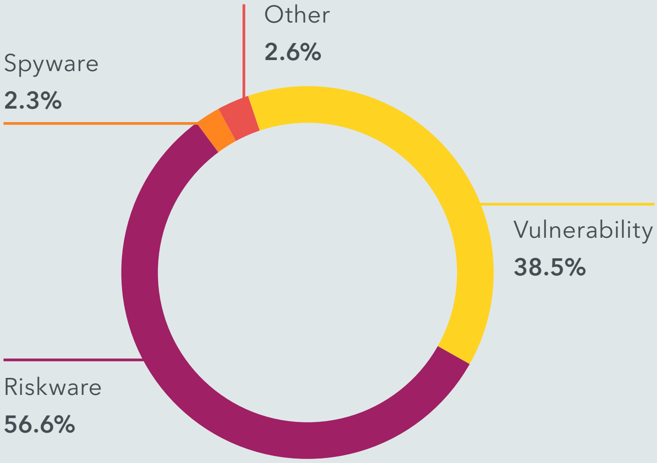
Risky Apps and Vulnerabilities Bigger Issue than Malware

Historically, the overall app threats exposure rate has hovered around 1% across all industries, including energy. This changed in the third quarter of 2020 when SourMint, a widely-used advertising software development kit (SDK) that is embedded in various mobile apps, was re-classified as riskware because of its excessive insight into user browsing habits. This boosted the global app threat exposure rate for the energy industry to nearly 7% during that quarter.

In fact, nearly 95% of mobile app threats facing the industry are either riskware or a vulnerability. Riskware are legitimate programs that pose potential risks due to a software incompatibility, security vulnerability or compliance violation. Riskware is not the same as a vulnerability, which is a defect in software code that can be exploited by an attacker.

Some of the energy industry risks caused by app threats include:

- Compliance violations due to data handling practices
- Excessive permissions that allow an app to track location, access SMS and accessibility features
- Access to the camera and microphone to spy on the user
- Access to the device's file system
- Connections to servers in foreign countries



Malware, on the other hand, is a broad category of software that is intentionally designed to cause damage to a device, server, client or network. When it comes to mobile malware there are various types – trojans, spyware, adware, keyloggers and ransomware, among others. Each type is designed to achieve a specific objective. For example, ransomware encrypts a victim's data until a ransom is paid, whereas spyware may access a camera, microphone or messages to spy on a user.

One highly-advanced mobile malware that resurfaced this year is Pegasus, which was developed by the NSO Group, an Israeli-based company and a known leader in the unregulated spyware industry. This spyware infects iOS and Android devices and enables operators to obtain GPS coordinates, messages, encrypted chats, photos and emails. Calls can also be recorded and the microphone and camera secretly turned on unbeknownst to the user.

Pegasus has evolved since it was discovered by Lookout and Citizen Lab in 2016. It now has the capability to be installed and executed on a target's mobile device without requiring any interaction by the user.

This type of malware could enable bad actors to view operations inside of energy plants or obtain confidential information. With this inside information, broader attacks could be launched, potentially crippling critical infrastructure and threatening the safety and well-being of citizens.

Outdated OSs and Vulnerabilities Continue to Plague Devices

Vulnerabilities make up nearly 40% of all app threats and unintentionally open the door for attackers. New vulnerabilities are identified nearly every day, constantly increasing the threat surface of energy organizations. On mobile devices, there are two major types of vulnerabilities: app vulnerabilities and operating system vulnerabilities.

App Vulnerabilities

For example, vulnerability CVE-2020-16010 was identified in a version of the Chrome browser for Android during the past year. To exploit this vulnerability, an attacker only needed to send a malcrafted HTML page to the device. Once successfully exploited, a threat actor can access any of the app's capabilities, including the camera and microphone, location data and browsing history. With more than five billion devices running Chrome, this vulnerability posed serious risk across every industry, including energy.

Another vulnerability, which contributed significantly to the app threat exposure rate, was found in the Google Play Core Library. The library enables a mobile app to obtain advanced functionality and updates from the Google Play Store. This vulnerability enabled threat actors to inject code into any app using the library allowing them to steal credentials, financial details and read email.

To address application threats, energy organizations need to implement mobile security with strong app threat detection capabilities. Such a solution should detect and alert users of malware and vulnerabilities from within apps.

Additionally, energy organizations need to make informed app vetting decisions based on app permissions and capabilities. They should set app policies to send automatic alerts based on risk tolerance such as flagging apps that communicate with servers in high-risk geographies or lack proper data transport security.

OS Vulnerabilities

Outdated versions of Google and Apple operating systems are still in use across the energy industry. Old versions expose organizations to hundreds of vulnerabilities that can be exploited by bad actors seeking access to an organization's environment.

Android – 12 months after Android 11 release [7]

OS Version	Percent of Devices	Number of Vulnerabilities [8]
11 [9]	44.1%	>130
10	30.5%	>120
9	15.4%	>90
8	6.9%	>120

iOS – 12 months after iOS 14 release [10]

OS	Percent of Devices	Number of Vulnerabilities [11]
14	84.9%	>50
13	7.3%	>195
12	5.5%	>65
11	0.2%	>130

[7] https://www.cvedetails.com/version-list/1224/19997/1/Google-Android.html

[8,11] Source: Lookout, based on analysis of U.S. government users running Lookout for Work, January 1 to December 31, 2020

[9] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=android+11

[10] https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ios

More than half (55.9%) of Android devices have not upgraded to the latest available operating system that was launched in September 2020. The good news is that only 15% of iOS devices haven't yet upgraded to the latest version since it was launched the same month. Outdated operating systems expose energy organizations to hundreds of vulnerabilities that have already been fixed.

While energy organizations may choose to delay updates until their proprietary apps have been tested, mobile operating systems should be updated as soon as possible to fix bugs and resolve security issues. Any delay creates a vulnerability window during which a bad actor could use a mobile device to gain access to the organization's infrastructure and steal sensitive data.

The number of vulnerabilities associated with a particular operating system version represents the risk of remaining on that version. Although vulnerabilities can be patched, there are still obstacles to overcome:

- Vulnerability windows exist between discovery and patch availability.
- Patching typically requires user action to update the device.
- Visibility into OS versions and installed security patches is difficult to obtain.

Only with visibility into endpoint and app vulnerabilities will you know exactly where these weaknesses exist and when they need to be updated in order to prevent security gaps from being exploited by threat actors.

Recommendations: Fundamental Mobility Safeguards and Best Practices Decrease Risk

As energy organizations undergo digital transformation, securing mobile endpoints that employees use to gain access to corporate resources and operational technologies is imperative. Phishing attacks, mobile app threats and outdated operating systems present a heightened risk to the already-strained energy industry. To mitigate this risk, we recommend the following steps be taken immediately:

Ensure that mobile devices are included in overall cybersecurity programs. Too often, these devices are not included in formal programs. They must be included to ensure mobile operating systems and apps are kept up to date in order to mitigate risks and vulnerabilities. Programs should also educate users about mobile-specific threats.

Ensure mobile phishing protection is running on every mobile device. The majority of attacks start with phishing, and mobile presents a multitude of attack pathways. An anti-phishing solution must block any communication from known phishing sites on mobile devices – including SMS, apps, social platforms and email.

Ensure visibility into mobile apps on devices connecting to corporate resources. With personal and work apps on the same device, any malware in a personal app can open the door for a bad actor. Leverage a mobile security solution to gain visibility into apps in use and make responsible app vetting decisions.

To learn more about how Lookout secures organizations in the energy industry, visit

LOOKOUT.COM/SOLUTIONS/ENERGY →

Lookout®

About Lookout

Lookout is an integrated endpoint-to-cloud security company. Our mission is to secure and empower our digital future in a privacy-focused world where mobility and cloud are essential to all we do for work and play. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Lookout is trusted by millions of consumers, the largest enterprises and government agencies, and partners such as AT&T, Verizon, Vodafone, Microsoft, Google, and Apple. Headquartered in San Francisco, Lookout has offices in Amsterdam, Boston, London, Sydney, Tokyo, Toronto and Washington, D.C. To learn more, visit **www.lookout.com** and follow Lookout on its **blog**, **LinkedIn**, and **Twitter**.

For more information visit
lookout.com

Request a demo at
lookout.com/request-a-demo