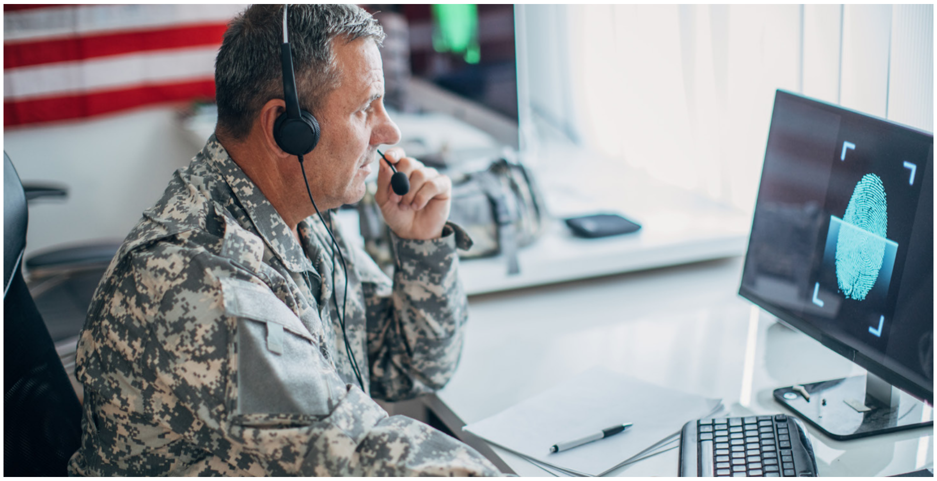
How this federal systems integrator protects against mobile phishing with Lookout



The Challenge

Mobile phishing is a global threat, and a leading government systems integrator, that focuses on secure communication and information systems technology, is a prime target.

This SI has a long history of building systems and integrating technology for combat vehicles, submarines, aircraft, and satellites for military defense and civil government. Its mission-critical systems are used by the military and first responders.

"Being a target of phishing attacks is a nature of our business," says the security architect for the company.

With safeguarding systems used for national defense a top priority, the company has strong protection for its information technology (IT) systems, but mobile is used for business and viewed as a target by malicious actors. Incorporating more rigorous safeguards to protect mobile users was necessary given the threat landscape. Company-owned and managed mobile devices give employees the flexibility they need. But even with mobile device management (MDM), there are risks.

The call to arms was the Trident vulnerability which is composed of three previously unknown zero-day iOS vulnerabilities that installed the Pegasus spyware on mobile devices. An innocuous text or WhatsApp message with a link, or a WhatsApp call that a person ignored, was enough to enable a bad actor to spy on all email, audio, video and text messages on the phone.

Customer Profile

This government systems integrator serves the global defense community with secure communications solutions for land, airborne, maritime, and public safety applications.

Industry: Aerospace and Defense

The Solution

Lookout Mobile Endpoint Security
Lookout Mobile Phishing Protection
Lookout Web Access Controls

The Results

- Protected key employees and mobile devices from phishing attacks via SMS, email, or in-app messages
- Smooth operations and seamless integration with UEM platform
- Laid the foundation for greater use of cloud apps

> "Being a target of phishing attacks is a nature of our business."
>
> Security Architect

Selection Criteria

With detailed engineering plans of defense systems at stake, the secure communications integrator needed an effective way to stop mobile malware and phishing without compromising an employees' personal privacy.

"At that time, only Lookout could detect Pegasus and Trident on smartphones," says the security architect.

The Lookout Security Platform is a highly scalable, cloud-based mobile-first platform that provides advanced mobile phishing and malware protections with a privacy-centric approach. Lookout continuously protects people, their devices, and enterprise data from the latest phishing, application, device, and network threats.

The architect and their team conducted a proof-of-concept test of the Lookout Mobile Endpoint Security (MES) solution, deploying Lookout on the mobile devices of 50 executives, business development, and finance managers who were likely targets of cybercriminals. Employees were assured that Lookout only collected security telemetry data, protecting their personal privacy.

The Solution

After a successful pilot, the SI deployed Lookout to a wider range of employees, including engineers and field service personnel, to protect their company-owned mobile devices from threats.

Lookout protects against phishing attacks across text message, email, browser, and in-app messages—the vectors attackers use to socially engineer and trick users into exposing account credentials or downloading malware.

To better protect information accessible in the mobile domain and support the increased appetite to conduct business on the go, the SI leverages Lookout's flexible modules for mobile protection, detection, visibility, analysis, response and remediation.

"Lookout's secret sauce is the ability to identify zero day threats in applications," says the security architect. "The bread-and butter of Lookout is application analysis."

Lookout inspects roughly 100,000 apps every day, analyzing every version of every app across the world's largest app stores, third-party stores, and more. Lookout's machine learning security engines identify and auto-convict approximately 10,000 new malicious apps each day. Continuous threat analysis is supplemented by Lookout's cutting-edge mobile threat research, which then informs the SI's security operations team priorities.

The risk of compromise on public Wi-Fi was of particular concern. "Equipping our mobile workforce with a tool that can perform a sanity check on a public network before connecting other devices arms our users with more insight into the security of the network they are about to conduct business on," says the security architect. "If Lookout flags the network as suspicious, users will not connect other devices to it. Instead, users could tether their phones to their laptops and use the cellular network if necessary."

If Lookout identifies malicious or non-compliant behavior on a personal app, the company's security operations team can quickly identify how many employees use the app, so the team can take action to protect their mobile users.

Lookout Web Access controls enable the SI to block access to risky or offensive content on mobile devices. And personal data privacy is maintained, as Lookout automatically prevents connections to inappropriate content without inspecting the user's app, web, or email traffic.

According to the security architect, the initial deployment and ongoing operations have been smooth. The Lookout MES solution is integrated with BlackBerry Enterprise Server Unified Endpoint Manager on company-owned devices.

"The expectation was that there would be some push back from the user population as deploying such a tool could be perceived as "Big Brother watching"," added the architect. "Upon deployment, the team released a detailed description of what information is collected and there was not a single concerned response. The anonymity offered to users has been well received and security practices have not been impeded in our 3+ years of experience."

The Results

"With Lookout protecting the personal side of their phones, our employees have more freedom and appetite to accept more mobile apps," says the security architect

As a result of strong protection, the company now permits access to non-internal web sites from email in an EMM container to the device's native browser. This enables productivity 'on-the-go' with seamless access to cloud services leveraged by the company. While phishing is still a threat vector here, the safeguards around phishing protection Lookout provided a level of confidence that malicious content would be detected and blocked. Whereas before, employees were frustrated that they couldn't click on links that led outside the MDM container.

"With Lookout on our phones, we've added the protection and assurance we need to forward that link outside the container and let people open that link from within Safari," he says. "Our director was thrilled with that capability."

"Lookout enables people to work the way they want on their phones," says the security architect.

With national security and public safety at stake, rules around remote access to core business, engineering applications, and data are necessarily stringent. But Lookout provides increased confidence to roll out cloud apps for collaboration and project management.

In addition to this, the company has found new ways to improve efficiency in their manufacturing plants by leveraging Lookout on wifi connected tablets. Innovation opportunities like this continue to present themselves and Lookout has provided a level of assurance that the mobile domain demonstrates sufficient security posture to explore these opportunities.

"We've laid the foundation for mobile threat protection with Lookout," says the security architect. "We have the assurance that our mobile devices are protected, which affords us the ability to consider provisioning access to information from mobile devices as we adopt Cloud Services."

Why Lookout

Lookout is the leader in mobile security, protecting the device at the intersection of the personal you and the professional you. Our mission is to secure and empower our digital future in a privacy-focused world where mobile devices are essential to all we do for work and play.

The broad adoption of smartphones and tablets have created new and endless ways for cybercriminals to convince you to willingly use your mobile device for their unlawful gain. The most common start of a cyberattack is a phishing link and mobile devices have created new ways to send them to you. Phishing risks no longer simply hide in email, but in messaging, social media, and even dating apps. Because we use these devices for both, protecting against phishing is critical for our personal and professional lives.

Lookout enables consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust. Our platform uses artificial intelligence to analyze data from nearly 200 million devices and over 100 million apps to protect users from the full spectrum of mobile risks. This enables us to deliver modern endpoint security with the most comprehensive protection from device, network, app and phishing threats without prying.

Learn more about how to protect your organization from mobile phishing

https://www.lookout.com/products/phishing-content-protection