

FINANCIAL SERVICES THREAT REPORT

# Cloud and mobile reliance pushes financial services beyond device management



### **Executive summary**

The financial services industry is in the midst of accelerating its digital transformation. Even before the pandemic forced organizations to embrace cloud services and mobile devices, the finance industry experienced a 71 percent increase in the adoption of mobile apps in 2019.<sup>1</sup>

Employees and customers of financial services organizations use tablets and smartphones more frequently for day-to-day operations and transactions. Since most cloud-based services and infrastructure are accessible from any device, mobile devices have unlocked previously untapped potential. With digital collaboration skyrocketing, corporate data now goes wherever it's required. This means your organization needs to embrace modern security technologies and strategies to stay secure, competitive, and relevant on the devices that employees and customers use the most.

Threat actors are constantly finding ways to exploit mobile devices that access cloud services and infrastructure. Lookout found a 125 percent increase in the average quarterly exposure to mobile phishing between 2019 and 2020. During the same period, average quarterly exposure to malicious and risky apps increased more than five times regardless of whether the devices were running mobile device management (MDM) solutions. While many organizations have turned to MDM as a first step to mitigate mobile risk, managing a device is not the same as securing it against increasingly complex mobile threats.

To prevent account fraud and takeover, it is important to consider how to secure the mobile app experience for your customers. When building consumer applications, security must be integrated from the ground up. By integrating security into the mobile app development process, mobile security capabilities are natively delivered to your customers without asking them to install any additional software.

Security is a business requirement that can create technology challenges. A cyberattacker can exploit countless channels

## Key findings in the financial services industry <sup>°</sup>

- There was a 50 percent increase in MDM adoption from 2019 to 2020.
- In 2020, average quarterly exposure to mobile phishing attacks grew 125 percent. This was the largest increase for any industry.
- The motive of almost 50 percent of phishing attacks was to steal corporate login credentials.
- Nearly 20 percent of mobile banking customers had a trojanized app on their device when trying to sign into their personal mobile banking account.
- Seven months after the release of iOS 14 and Android 11, 21 percent of iOS devices were still on iOS 13 or earlier, and 32 percent of Android devices were still on Android 9 or earlier.

and put your organization's infrastructure, its reputation, and customer data at risk. Permitting employees to work from more devices and remote locations puts stress on the balance of complying with regulations and respecting user privacy. Across the financial services industry, 76 percent of CIOs and IT professionals are modernizing their infrastructure to mitigate risk associated with out-of-date technology that can't keep up with modern needs.<sup>2</sup> The key to modernizing security is ensuring that smartphones and tablets don't give threat actors a backstage pass to corporate data.

### Methodology

To understand the mobile challenges facing the financial services industry, data was analyzed in the Lookout Security Graph specific to financial services and insurance organizations. The Lookout Security Graph includes telemetry data from the threat analysis of nearly 200 million devices and over 140 million apps, and it enables customers to rapidly detect and respond to cyberattacks to prevent data breaches.

<sup>&</sup>lt;sup>1</sup> Source: https://www.forbes.com/sites/johnkoetsier/2020/04/15/report-35-85-fintech-growth-on-mobile-thanks-to-coronavirus-after-1-trillion-app-opens-in-2019 <sup>2</sup> Source: https://www.protiviti.com/US-en/insights/modernizing-legacy-systems-financial-institutions

sourcer impose were protected on the original modernizing regacy systems middle

<sup>&</sup>lt;sup>3</sup> Source: Lookout Data January 2019-April 2021

### Financial services are in the crosshairs

As more users access cloud services and infrastructure from mobile devices, cyberattackers deliberately target phones, tablets and Chromebooks to increase their odds of finding a vulnerable entry point. A single successful phishing or mobile ransomware attack can give attackers access to data across your entire backend infrastructure.

This includes proprietary market research, client financials, investment strategies and cash or other liquid assets. These attacks can take the form of mobile phishing, apps containing malware, device vulnerability exploits and risky network connections outside the traditional office perimeter.

Security teams need visibility for individual devices and the entire fleet while balancing end-user privacy and compliance with security requirements. For example, you may want to know what malware was downloaded to a device, but not the app that carried it. You also want to know the threat posed by a risky website, but not the specific URL. Doing so creates a healthy balance between security and end-user privacy, which is important for organizations that enable bring-yourown-device (BYOD) in a highly regulated industry like financial services.

In addition to securing employee mobile devices, consumer banks have an opportunity to protect their customer base. Nearly 80 percent of banking customers say mobile devices are the primary way they access their account.<sup>4</sup> Ensuring that customer mobile devices used for transactions are safe and secure protects them from phishing attacks, screen overlays and trojanized apps that steal login credentials.

Employees and customers can be as productive using smartphones or tablets as they are using desktop or laptop computers. However, if these mobile endpoints are not properly secured, they can create security gaps that are equally significant as users who don't have endpoint security on a laptop or desktop computer. This puts your security architecture and compliance posture at risk.

### Lookout discovery: BancamarStealer

#### What is it?

- In 2018, Lookout researchers published their discovery of the banking trojan BancamarStealer.
- BancamarStealer is a mobile-specific banking trojan and is an example of malware-as-a-service. Out of the box, it can be configured to target specific banks and will support a wide range of remote commands.
- Between 2018 and March 2021, the number of BancamarStealer versions have increased almost 10 times from 7,700 to over 74,000.

#### How does it work?

- BancamarStealer is delivered by SMS message and prompts the user to download a trojanized app that looks legitimate.
- It can be used in social engineering campaigns across messaging, social media or dating apps.
- The malware can harvest credentials, implement screen overlays, send the user to malicious sites, retrieve all SMS messages, and remotely take control of the entire device.



Source: Lookout Blog, February 2018

## Managed or unmanaged, mobile devices are at risk

During the last two years, there has been an increase in the percentage of managed devices in the financial services industry's mobile fleets. While deploying an MDM solution to try to implement basic controls over apps and devices outside the perimeter is a good start, it doesn't provide security against mobile cyberthreats. This is especially true when it comes to protecting against phishing attacks. MDMs only enable your administrators to set app and access policies. They do not provide the visibility necessary to monitor the risks that occur when employees are using apps and networks you don't control, which makes it even more difficult to visualize the risks your organization faces.

| Use of managed vs unmanaged mobile devices <sup>a</sup> |       |       |       |       |       |      |       |       |
|---|-------|-------|-------|-------|-------|------|-------|-------|
|   | 1Q19  | 2Q19  | 3Q19  | 4Q19  | 1Q20  | 2Q20 | 3Q20  | 4Q20  |
| Managed   | 50.1% | 57.3% | 63.5% | 71.6% | 70.9% | 76%  | 76.1% | 74.9% |
| Unmanaged   | 49.9% | 42.7% | 36.5% | 28.4% | 29.1% | 24%  | 23.9% | 25.1% |

## Phishing attacks increased more than 120 percent year over year

Mobile phishing is a modern security issue. Attackers build phishing campaigns that catch people when they are most vulnerable and least expect it. Sending phishing links in SMS messages, third-party messaging apps and social media apps is the primary channel for delivery because it is easy to socially engineer targets on these platforms. Employees targeted by phishing campaigns run the risk of having their credentials stolen, which could lead to serious financial and data loss. The financial services industry is under siege from mobile phishing. Between 2019 and 2020, there was a 126.1 percent year-over-year increase in average quarterly exposure to mobile phishing attacks, which is the largest across all major industries.<sup>6</sup> The next largest jump was in transportation, which experienced a 76.5 percent increase.<sup>7</sup> Across Lookout enterprise customers in all industries, there was a 28.5 percent increase in average quarterly phishing exposure rate for the same period.

| Year-over-year growth in average quarterly mobile phishing exposure® |      |       |         |  |  |
|--|------|-------|---------|--|--|
|  | 2019 | 2020  | Growth  |  |  |
| All enterprise   | 7.2% | 9.2%  | +28.5%  |  |  |
| Transportation   | 6.8% | 12%   | +76.5%  |  |  |
| Financial services   | 6.9% | 15.6% | +126.1% |  |  |

#### Managed or not, mobile phishing persists

Whether a device is managed or unmanaged, attackers have had equal success deploying phishing campaigns. Spotting phishing attacks on mobile devices is much more difficult than on laptop or desktop computers. In addition, mobile devices are treated as extensions of ourselves. We trust them to be inherently safe. Identifying a phishing attack on a mobile device is harder than on a personal computer because the features, functionality, and even the screen size make it harder to determine what is real versus what is fake. The first line of defense against mobile phishing is educating users so they don't tap the link in the first place. Employees might understand how to identify a phishing attack on a PC, but as malicious actors get better at leveraging social engineering on mobile devices, even the best-trained employees can fail to identify an attack. It is critical to ensure that employee training includes mobile devices and why mobile phishing attacks are more successful than desktopbased campaigns.

| Quarterly phishing exposure rate for managed v unmanaged devices° |      |       |       |       |       |       |       |       |
|---|------|-------|-------|-------|-------|-------|-------|-------|
|   | 1Q19 | 2Q19  | 3Q19  | 4Q19  | 1Q20  | 2Q20  | 3Q20  | 4Q20  |
| Managed   | 2%   | 3.2%  | 4.2%  | 9.2%  | 23.3% | 14.2% | 13.7% | 5.7%  |
| Unmanaged   | 7.4% | 11.8% | 19.7% | 27.7% | 36%   | 26.6% | 14.9% | 11.1% |

### Mobile app threats trending upward

Visualizing the serious risk that mobile apps can introduce into your organization is not easy. Even if a mobile device is company-owned, employees still treat it as a personal device and will download apps unrelated to work. In effect, mobile apps have become the new frontier of shadow IT.

When users download personal mobile apps, granting permissions like access to contacts or location may seem innocuous and they may not allow extensive access to their device's data. If these devices have access to the corporate network, apps and data – especially in a highly-regulated industry like financial services – seemingly harmless data access and transfer practices could violate data governance, risk and compliance mandates.

## iOS and Android app risks grew exponentially in 2020

In addition to the risk of violating corporate policy and compliance, mobile apps can introduce malware and riskware, which is software that might not be outright malicious but could pose privacy or compliance risks to an organization. Much like with mobile phishing, there was significant growth in mobile app exposure rates. In 2019, the average quarterly exposure rate was just 0.27%, but that number increased over five times to 1.45% in 2020.

| Quarterly app threat exposure rates <sup>10</sup> |        |        |        |        |        |        |        |
|---|--------|--------|--------|--------|--------|--------|--------|
| 1Q2019  | 2Q2019 | 3Q2019 | 4Q2019 | 1Q2020 | 2Q2020 | 3Q2020 | 4Q2020 |
| 0.31%   | 0.28%  | 0.30%  | 0.17%  | 0.15%  | 0.24%  | 3.08%  | 2.26%  |

In the second half of 2020, there was significant growth in app risk exposure for financial services. The spike in the third quarter of 2020 is due to the updated classification of SourMint, a widely used advertising software development kit (SDK) for iOS apps, to riskware. The classification update was made due to SourMint's insight into user browsing habits and other private user data that could be sold to third parties for data analytics. Many components of mobile apps aren't evident to the end user. The SourMint SDK exemplifies how risky software can unknowingly be introduced into your mobile ecosystem when users download and allow all permissions for a new app.

In addition to risky SDKs, vulnerabilities exist in new versions of mobile apps every week. In late 2020, a version of the Chrome browser for Android was discovered to have a dangerous vulnerability. To exploit this vulnerability, an attacker only needed to send a malcrafted HTML page to the device. In the event of a successful exploit, a threat actor could access any Chrome capabilities, including the camera and microphone, location data and browsing history. With over 5 billion devices running the app, this vulnerability posed serious risk across every industry.

Additional risks caused by malicious apps include:

- Compliance violations due to data handling practices (e.g., encryption in transit or at rest)
- Excessive permissions that enable cross-app data sharing on a device
- Access to the camera and microphone to spy on a user
- Access to a device's file system
- Connections to servers in foreign countries

| Quarterly app threat exposure rates for managed iOS and Android devices <sup>11</sup> |        |        |        |        |  |
|---|--------|--------|--------|--------|--|
|   | 1Q2020 | 2Q2020 | 3Q2020 | 4Q2020 |  |
| Android   | 0.47%  | 0.27%  | 0.24%  | 2.43%  |  |
| iOS   | 0.01%  | 0.05%  | 4.33%  | 2.36%  |  |

#### You can't assess what you can't see

Maintaining risk and compliance policies means your organization needs to know which apps have access to corporate data, how it's being transferred and where it's stored. Most organizations have visibility into how their desktop and laptop applications are handling data, but not mobile endpoints. Because of how iOS, Android and Chrome OS run their apps, it's challenging to inspect them. Without any insight, the security team has no visibility into how these apps handle your data.

As was observed with mobile phishing, app threats also cannot be mitigated solely by relying on MDM solutions. As shown above, devices with an MDM solution still encountered malicious apps. With managed devices, organizations have visibility and controls over which apps employees use through MDM or mobile app management (MAM). But they don't provide insight into real-time app permissions and data access controls.

Having visibility into the permissions and capabilities of all apps on a mobile device is key to ensuring a strong security posture for your organization. But you must also respect enduser privacy. Since many employees want the flexibility to use personal devices for work, mobile apps have become the new frontier of shadow IT. By understanding the capabilities of all apps across your mobile fleet and being able to build access policies around them, you can ensure you alignment with data privacy laws and keep your organization's confidential information secure from malicious actors.

### Financial services employees are exposed to hundreds of vulnerabilities

Google and Apple release regular software updates to fix bugs and resolve security issues. A cybersecurity best practice is to keep a mobile operating system up to date. However, financial services organizations may choose to delay updates on employees' mobile devices until their proprietary apps have been tested. Users also tend to ignore updates until they're forced to install them. These delays create a vulnerability window during which a threat actor could gain access to an organization's infrastructure and steal data through mobile devices.

| Android - Seven months after Android 11 release <sup>12</sup> |                       |                              |  |  |  |
|---|-----------------------|------------------------------|--|--|--|
| OS version <sup>14</sup>                                      | Percent of<br>devices | Number of<br>vulnerabilities |  |  |  |
| 11 <sup>16</sup>  | 27.3%                 | >50                          |  |  |  |
| 10  | 30.64%                | >260                         |  |  |  |
| 9   | 20.6%                 | >170                         |  |  |  |
| 8   | 11.3%                 | >630                         |  |  |  |

| iOS - Seven months after iOS 14 release |                       |                              |  |  |  |
|---|-----------------------|------------------------------|--|--|--|
| OS version <sup>15</sup>                | Percent of<br>devices | Number of<br>vulnerabilities |  |  |  |
| 14                                      | 79.3%                 | >50                          |  |  |  |
| 13                                      | 13.1%                 | >195                         |  |  |  |
| 12                                      | 4.8%                  | >65                          |  |  |  |
| 11                                      | 2.0%                  | >130                         |  |  |  |

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:

- Attackers can exploit vulnerabilities to actively target and take over a device or surpass its built-in security measures.
- Patching usually requires employees to update their device.
- If employees run an old version, they present a risk to the organization that could be easily eliminated with an operating system update.

One way to protect against exploitation of known vulnerabilities is to use mobile vulnerability and patch management. With visibility into endpoint and app vulnerabilities, you will know if and where these weaknesses exist, and when they need to be updated to prevent threat actors from exploiting security gaps.

- <sup>14</sup> Source: https://www.cvedetails.com/version-list/1224/19997/1/Google-Android.html
- <sup>15</sup> Source: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ios

<sup>&</sup>lt;sup>12,13</sup> Source: Lookout data as of April 6th, 2021

<sup>&</sup>lt;sup>16</sup> Source: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=android+11

## Your customer experience needs protection

Customers prefer the mobile experience over having to go to a branch office. In 2019, registration for mobile finance apps jumped 71 percent, and the pandemic accelerated the use of banking apps. To prevent customer fraud and uphold your organization's reputation, it's important to develop a secure experience for mobile customers. Since consumers might not have mobile security on their device, the onus is on app developers to integrate security into an organization's customer-facing apps. Doing so helps mitigate the risk of a customer falling victim to screen overlay attacks, banking trojans and other malware that could result in fraud, account takeover and theft.



Cyberattackers use sophisticated malware, screen overlay attacks, device rooting and reverse engineering techniques to steal customer login data on mobile devices. The chart above shows the variety of threats facing financial services customers. Without this level of visibility, security and development teams have no way of creating a secure customer experience, which can be a massive differentiator in a highly competitive financial services market.

## Whether you use MDM or not, what can you do next?

The use of iOS and Android devices by employees and customers is accelerating digital transformation in the financial services industry. This makes smartphones and tablets targets for cyberattackers because they can be the gateway to a treasure trove of data, internal infrastructure and cloud assets. As organizations embrace mobile more broadly, the risk to the business increases.

Many financial services providers have turned to managing devices to mitigate the risks associated with working from smartphones and tablets. While this is a good first step, MDM still leaves employees exposed to more complex phishing, app and device threats that could compromise an entire organization.

The industry must also consider its customers, who prefer the mobile experience and inherently trust their financial services apps to be secure. While some mobile banking apps might implement security techniques into their app, such as app hardening to protect it from being reverse engineered, this isn't enough to protect customers from threats like trojans and screen overlays. With mobile as the main driver for digital transformation, security, IT and mobility teams need to work together to secure all smartphones and tablets, whether they're managed, unmanaged or a consumer device. Doing so with end-user privacy in mind will enable financial organizations to build a stronger security posture without violating corporate and international data privacy and compliance laws.

Protecting these modern endpoints requires a different approach - one that is built from the ground up for mobile devices and secures the entire data path from the endpoint to the cloud. Only a modern endpoint protection solution can detect mobile threats in apps, device operating systems and network connections while also protecting against credential theft and malware delivery attacks through phishing.

#### **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.

To learn more about how Lookout secures financial services, visit lookout.com/solutions/financial-services

#### lookout.com

© 2021 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, POWERED BY LOOKOUT®, and PROTECTED BY LOOKOUT®, are registered trademarks of Lookout, Inc. in the United States; and POST PERIMETER SECURITY ALLIANCE™ is a trademark of Lookout, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders. 20210430-Lookout-USv1.0