Lookout®

THREAT REPORT

Pharmaceutical Industry Threat Report

Introduction

Pharmaceutical organizations are leaders in innovating and adopting modern technology. To be the first to bring ground-breaking treatments to the market, these companies need employees to be productive regardless of whether they are in the office or remote. By empowering employees to stay productive with mobility, this enables the pharmaceutical industry to serve patients and the healthcare community more effectively.

Mobile devices and cloud services have unlocked previously untapped potential for your employees to work however and from wherever they're the most productive. These endpoints have the same access to sensitive data and intellectual property (IP) as traditional computer endpoints regardless of where they are being used. Attackers know this and build strategies to target both mobile devices and desktops to increase their odds of finding a vulnerable entry point. A single successful ransomware or phishing attack will enable intruders to gain access to research data, formulas, intellectual property, and other valuable data. While mobility and cloud applications enable your workers to remain productive while remote, they also significantly increase the risk of successful attacks.

To stay competitive, data must be accessible on mobile endpoints across your business including research and development, manufacturing, and distribution channels. This data must be transferred and handled securely to align with data privacy and security compliance standards like HIPAA, CGMP and GDPR. For example, HIPAA requires that if mobile devices are used to access, store or transmit electronic protected health information (ePHI), they must have access and multi-layered security controls in place to reduce the risk of unauthorized data access.[1] In the new frontier of mobile computing, your security team needs to extend your existing data access and acceptable use policies to all smartphones, tablets and Chromebooks.

Traditional endpoint security cannot protect mobile devices. iOS, Android and Chrome OS devices operate differently and present a unique attack surface for threat actors that increases risk to pharmaceutical companies. Taking a modern approach to securing mobile devices mitigates the risk of mobile phishing attacks, malicious applications, and device compromise along the supply chain for your entire organization.

[1] https://www.hipaajournal.com/mobile-data-security-and-hipaa-compliance/

Challenges

One of the biggest security challenges for pharmaceutical organizations is protecting IP. Independent of whether your organization has a bring-your-own-device (BYOD) policy or issues employees company-owned mobile devices, mobile endpoints broaden the attack surface for threat actors. Most prominently, attackers have turned to spear phishing campaigns to steal your employees' login data or deliver malicious payloads to their mobile devices to compromise your infrastructure. These attacks use social engineering to convince an individual to visit a phishing page or tap a link that silently delivers malware. While you can't block social engineering, you can block access to phishing sites.

Malicious actors are focused on mobile phishing because they can use any of the hundreds of apps the average person has on their mobile device. Attackers can socially engineer targets on a personal level through social media apps, messaging platforms, games, and even dating apps. An attacker will target particular individuals, including heads of research, manufacturing plant managers, sales leaders, or company executives, to gain privileged access to the data they want.

On a global scale, there have been multiple reports of foreign adversaries targeting pharmaceutical industry executives with mobile spear phishing attacks. Both the National Cyber Security Centre in the U.K. and the Cybersecurity & Infrastructure Security Agency in the U.S. issued advisories to organizations involved in the COVID-19 response to shore up their security practices. State-sponsored campaigns prove that nation-state virtual espionage is not just an issue for government entities.

When it comes to drug or vaccine development, the race is led by private sector organizations. You and your team need to be sure you're taking a modern approach to protecting your organization's IT structure and the patients you serve.

The Pharmaceutical Risk Surface

R&D	Clinical Trials	Manufacturing	Distribution
Researchers	Patients and subjects	Plant workers	Field sales reps
Scientists	Study sites	On-site scientists	Physicians
	Investigators		Pharmacies
	Operations		Patient support services
			Distribution channel

Since most employees use either a smartphone or tablet, or both, to access data within your infrastructure, there is a widespread risk surface. If these endpoints are not properly secured, they can represent a significant gap in your security architecture and compliance posture.

Traditional security protocols tethered to your labs or office space are no longer adequate on their own. To modernize your team's approach to securing mobile devices, you need security solutions that can easily integrate with your existing security and business productivity tools. For guidance on how to secure iOS, Android, and ChromeOS devices, many IT and security teams have turned to NIST Special Publication 800-124 as a framework to develop their strategy to secure mobile devices in a complex environment.

Encounter Rates Across the Industry

The rate at which devices encounter mobile phishing, app threats, device threats and risky networks is increasing. These encounter rates are specific to pharmaceutical companies protected by Lookout, which help contribute to our industry-leading dataset of security telemetry from almost 200 million devices and over 125 million mobile apps.

Out-of-date Operating Systems

Android – 1 month after Android 11 release***

Version	# of CVEs	% of devices in pharma
10	>170	47.9%
9	>155	38.9%
8	>170	9.9%
7	>210	2.8%

iOS – 1 month after iOS 14 release

Version	# of CVEs	% of devices in pharma
13*	>195	64.4%
12*	>65	12%
11*	>130	3.7%
10**	>355	0.2%

Software updates are intended to address bugs and vulnerabilities for apps and devices. However, since many pharmaceutical organizations have proprietary mobile apps, they often delay OS updates on employee devices until they're certain the new version works with their internal apps. If your organization operates on this policy, then it represents a certain risk tolerance you have. Even if you don't, there may be other places where you tolerate a certain amount of risk to ensure smooth internal operations. Regardless of which approach you take, having visibility into the OS status of mobile devices across your fleet is a necessity for security operations.

While operating system CVEs (Common Vulnerabilities and Exposures) are patchable, there are still some obstacles to overcome such as:

- CVEs are known exploitable vulnerabilities attackers can actively target to take over a device or surpass its built-in security measures.
- Patching usually requires action by the mobile user to update the device.
- If an employee is running an old OS version, they're walking around with a doorway to your organization's data in their pocket.

In order to protect against exploitation of known CVEs, your team needs to have mobile vulnerability and patch management capabilities. Only with visibility into endpoint and app vulnerabilities will you know exactly where vulnerabilities exist and when they need to be updated to prevent those vulnerabilities from being exploited by threat actors.

* Source: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=ios

** Source: https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

*** Source: https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224

Phishing

Mobile phishing threats can be broken into two categories: credential harvesting and malware delivery. With credential harvesting, a threat actor can log in as an employee and move laterally around the infrastructure until they find the data they're looking for and exfiltrate it. Malware delivery attempts to trick users into installing malicious apps or payload to the device, such as the well-known Wroba trojan, which silently delivers itself to the device in the background when the link is tapped. Both of these types of phishing threats can also be delivered through social engineering within apps, such as social media platforms or third-party messaging apps.

	4Q2019	1Q2020	2Q2020	3Q2020
Pharmaceutical mobile phishing encounter rate	7.06%	15.26%	7.59%	6.18%
	Breakdown of phishing attack by intent **Note: Some devices encountered both**			
Credential harvesting	83.33%	40.42%	36.4%	27.71%
Malware delivery	50%	78.72%	69.1%	81.92%

The spike in the first quarter of 2020 indicates threat actors targeted pharmaceutical companies during the COVID-19 pandemic by delivering more phishing attacks to mobile devices. They did this because the global shift to remote work meant employees were relying much more heavily on mobile devices to be productive from home.

The 106% increase in malware delivery signals the following:

- Attackers are investing in more complex malware delivery methods and using phishing links to deliver malware to the device.
- Social engineering can convince an employee to download a sideloaded app just as well as it can convince them to enter their login credentials in a fake site.
- Successful delivery of spyware or surveillanceware to a device could result in longer-term success for the attacker.
- Attackers want to be able to observe everything the user is doing and look into the files their device accesses and stores.

We find there are also some devices that encountered both credential harvesting and malware delivery phishing links, which exemplifies the persistence of attackers and contributes to the percentages adding up to over 100% in some cases.

Application Threats

	4Q2019	1Q2020	2Q2020	3Q2020
Overall	0.82%	0.53%	0.32%	8.26%

Lookout users encountered fewer application threats in the first half of 2020 than they did in the first half of 2019. Groups like the Google App Defense Alliance work to prevent malicious apps from making it onto official app stores in the first place. However, the primary concern is in sideloaded applications, which are downloaded from third-party app stores with minimal security requirements, if any at all.

The spike in the third quarter of 2020 is due to the updated classification of a widely-used advertising SDK (software development kit) as riskware because of its insight into user browsing habits. Across all industries, there was a 4% encounter rate in that same quarter, which shows that pharma was particularly susceptible to the malicious SDK.

Some of the risks malicious apps pose to a pharmaceutical organization include:

- Compliance violations because of data handling practices
- Excessive permissions that allow them to see data in other apps on the device
- Access to the camera and microphone to spy on the user
- Access to the device's file system
- Connections to servers in foreign countries

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 end-user privacy. Since many users 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 are aligned with data privacy laws and keep your organization's IP secure from malicious actors.

Network Threats

	4Q2019 – 1Q2020	2Q2020 – 3Q2020
Average Rate	0.13%	0.025%

Since network attacks usually require the attacker and victim to be in close proximity to each other, large trade shows and busy travel hubs were a feeding ground for threat actors to carry out a mobile attack through malicious Wi-Fi hotspots or man-in-the-middle attacks. With trade shows canceled and travel on the decline, network-based threats are important to keep an eye on and protect against but have been on a steady decline over the last couple of years.

Recommendations

Employees in pharmaceutical organizations use iOS, Android and ChromeOS devices every day to stay productive and increase efficiency no matter their role. This makes them targets for cyberattackers because their devices are a treasure trove of data and a gateway to enterprise cloud infrastructure.

Protecting these modern endpoints requires a different approach, one that is built from the ground up for mobile. Only a modern endpoint protection solution can detect mobile threats in apps, device operating systems and network connections while also protecting against credential harvesting and malware delivery attacks through phishing. Due to the personal nature of smartphones and tablets, endpoint security must protect the user, the device and the organization while respecting user privacy. At the same time it has to provide the same protection for employee-owned and company-owned devices.

About 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. We enable consumers and employees to protect their data, and to securely stay connected without violating their privacy and trust.

To learn more about how Lookout protects pharmaceutical organizations, visit lookout.com/solutions/pharmaceutical.