Lookout

Pegasus and Trident

Executive four-minute read

What are Pegasus and Trident?

Lookout and Citizen Lab uncovered an active, targeted mobile spyware threat called Pegasus that uses three critical and previously-unknown ("zero-day") iOS vulnerabilities. The vulnerabilities, when exploited, form an attack that subverts even Apple's strong security environment. We call these vulnerabilities "Trident."

Once Pegasus uses the Trident vulnerabilities to infect the device, the spyware causes catastrophic data loss, and can access all messages, calls, emails, logs, and data from apps including end-to-end encrypted applications.

Lookout worked directly with Apple's security team to immediately patch all three Trident iOS vulnerabilities in Apple's 9.3.5 update. The Pegasus spyware appears to persist even if you update the device's software, however, and can self destruct if it believes its stealthy position is at risk, preventing victims from ever finding the compromise and addressing the breach that has occurred.

Who do attackers target?

Threat actors will use this kind of targeted and expensive spyware to attack "high-value" individuals who have access to important, sensitive, and confidential information. The Pegasus attack reported in the media targeted a political activist, but it is also likely being used to attack specific targets for multiple purposes, including high-level corporate espionage. CEOs, CFOs, executive administrators, and financial teams, are often in the crosshairs of a targeted attack as they usually access confidential data, especially via their mobile devices.

As TechCrunch writes, "Apple zero-days mark a new era of mobile hacking."

Pegasus is the most sophisticated attack we've seen on any endpoint because it takes advantage of:

1. How integrated mobile devices are in our lives
2. The combination of features only available on mobile – always connected, voice communications, camera, email, messaging, GPS, passwords, and contact lists. It also includes information that could be answers to your security questions like birthdays, addresses, and children's information.

What are others saying about it?

THE WALL STREET JOURNAL.

"Their report sheds new light on the capabilities of private security companies to produce sophisticated software for state-sponsored spying. It also suggests that the iOS operating system behind Apple's iPhones isn't as impregnable as it appeared earlier this year…" *Read more here*

The New York Times

"Together, they discovered that the spyware relied on three previously unknown iOS vulnerabilities – called 'zero days' because Apple didn't know about them and had zero days to patch them." *Read more here*

MOTHERBOARD

"Until this month, no one had seen an attempted spyware infection leveraging three unknown bugs, or zero-days, in the iPhone." *Read more here*

WIRED

"Meanwhile, even though this vulnerability has been patched, the next one likely won't be far behind..." *Read more here*

Congressman Ted Lieu (D-CA) also released a statement saying:

"I am pleased that Apple was able to quickly address this security breach, but it is clear that Congress must do more to address the issues of mobile security. I believe a congressional hearing is in order and plan to work with my colleagues to examine these critical security concerns." Congressman Ted W. Lieu, (*D-CA)*

Read his full statement here.

YOUR TOP 3 QUESTIONS ANSWERED:

1) Can't my Mobile Device Management (MDM) solution solve this problem?

No. MDMs find jailbreaks by detecting known techniques, or by detecting evidence left behind by these known techniques. Pegasus jailbreak techniques were unknown to the entire world, including MDM vendors, until discovered by Lookout. When an attack like Pegasus comes out, an MDM will not be able to detect it immediately, meaning your mobile fleet will be open to attack during the crucial first days when threat actors are mobilizing to attack still-unpatched devices.

2) Why can't I just tell my employees to upgrade to the latest operating system?

The iOS 9.3.5 update does not uninstall Pegasus from previously infected iPhones, nor does it detect infected iPhones. We believe that this spyware has been in the wild for a significant amount of time based on some of the indicators within the code, meaning it has had a lot of time in the market to infect victims.

Your organization needs to know if an employee's device is infected with Pegasus, otherwise it will not be possible to conduct a forensic investigation to understand the scope, timing, and implications of the breach that has already occurred. This kind of data is crucial for the enterprise to know what steps to take next.

iPhones in your organization that were already infected before Apple issued the security update need to be:

1. **Identified immediately**
2. **Turned off**
3. **Reported to your IT Security team**

The IT Security team then needs to address the data compromise that has occurred.

3) How do I determine if there is a compromised device in my organization?

There may already be compromised devices in your organization. Given the high price of this commercially available software, this is a case of a low probability, yet extremely high impact threat.

Lookout Mobile Endpoint Security can detect the presence of Pegasus and alert your IT Security team of existing infections as well as any new infections. Lookout is also best positioned to track and protect against targeted threats like Pegasus because we are a mobile-focused security company with the right partnerships, technology, and people to focus on this problem.

"A lot of people think mobile is a solved problem. If I had said five years ago that committed attackers are attacking phones, you would have looked at me like I was crazy. The era of the highly resourced attacker going after phones instead of network or desktop infrastructure has arrived."

-Mike Murray, *VP of Security Research, Lookout*

Interested in learning more or want to determine if an infection exists in your organization? Contact Lookout today.