CyberTalk.org

CISO's Guide to Mobile Security

Protecting mobile devices from zero day attacks

TABLE OF CONTENTS

INTRODUCTION

In the last year, cyber security researchers have observed an explosion in terms of the number of mobile-specific zero day vulnerabilities in use by cyber criminals, who find these vulnerabilities convenient for purposes of data theft and monetary gain.

In 2021, **30%** of all zero day vulnerability exploits targeted mobile devices. This represents a **466%** increase, year-over-year. In spite of a reputation as the most secure ecosystem, vulnerabilities in iOS accounted for **64%** of mobile-specific zero day attacks.[1]

466% increase in zero day vulnerabilities actively exploited via mobile devices.

Many mobile zero day attacks begin with a phishing lure. Although security capabilities with anti-phishing functions can help prevent zero day exploits on mobile devices, organizations need to do more to limit the probability of successful zero day attacks on employee devices.

If reading this as someone who is not a security pro, know that zero day attacks can take multiple forms and lead to unexpected network traffic, cyber espionage, intellectual property theft, extortion or other cyber perils.

The growing number of devices (mobile phones, Tablets, and other 'smart devices') in use for work purposes means that mobile device-based zero day attacks are a growing risk.

While it's not possible to mitigate all zero day threats, it is possible to take the right precautions, which can limit your employees' level of vulnerability and that of your organization as a whole.

---

[1] Nearly a third of known, zero-days discovered in 2021 targeted mobile devices, Steve Zurier, SC Media, March 15, 2022

In the same way that you wear a seatbelt, regularly replace brake fluid, get the brake pads replaced and stop at the red lights to prevent a traffic accident…you can take a layered approach to preventing zero day threats on mobile devices.

RECENT ZERO DAY ATTACKS ON FLEETS OF MOBILE DEVICES

In June of 2022, Google spotted the enterprise-grade "Hermit" spyware, which targets both Android and iOS users. The spyware relies on a series of different exploits in order to operate, two of which are zero day vulnerabilities.

Hermit spyware is so vicious and insidious that Google has publicly expressed concern over it. Once installed on a device, Hermit can record calls, harvest photos and videos, read text messages and install location trackers. Google has sent notification to affected Galaxy device customers.

Hermit can record calls, harvest photos and videos, read text messages and install location trackers.

In the future, cyber criminals could potentially leverage other zero day threats to launch tough-to-stop spyware attacks or to inflict other forms of digital sabotage.

"…since 2014, there has been proof of targeted attacks on mobile devices using zero day vulnerabilities. They are used by attackers who aim to evade traditional anti-malware solutions."

— Peter Elmer, Principle Security Expert, Check Point Software

DYNAMIC TRENDS

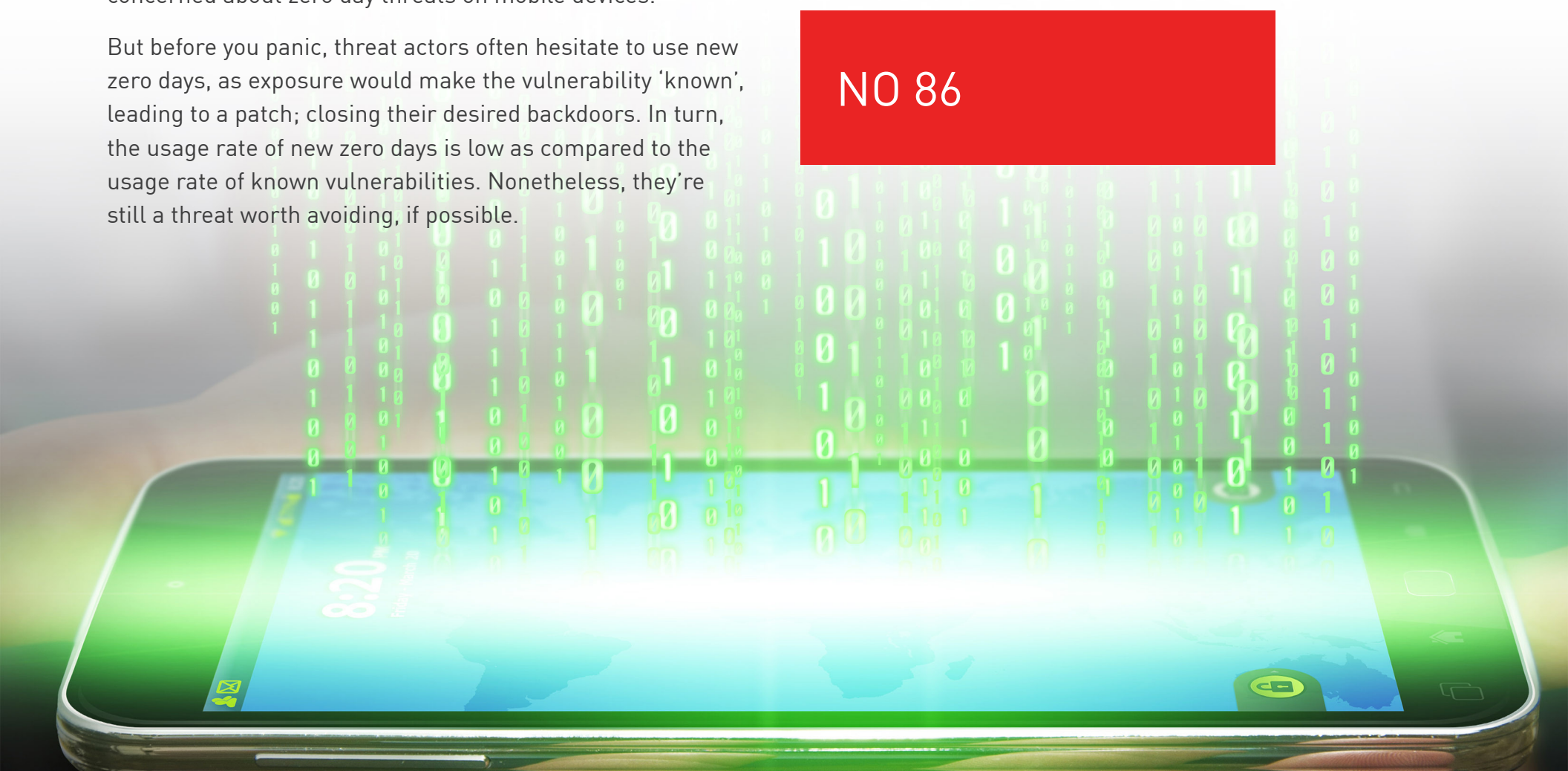
According to a survey conducted by CyberTalk.org, nearly 60% of cyber security professionals are concerned about zero day threats on mobile devices.

Again, nearly 60% of cyber security professionals are concerned about zero day threats on mobile devices.

But before you panic, threat actors often hesitate to use new zero days, as exposure would make the vulnerability 'known', leading to a patch; closing their desired backdoors. In turn, the usage rate of new zero days is low as compared to the usage rate of known vulnerabilities. Nonetheless, they're still a threat worth avoiding, if possible.

YES 120

NO 86



PREVENTION

How can CISOs prevent, detect and defend against mobile zero day threats before they interrupt end-user workflows or inflict widespread damage? Review the best practices outlined below and modify them to fit the unique needs of your organization.

1. **Up-to-date software and operating systems.** The importance of ensuring that everyone installs patches and maintains up-to-date operating systems cannot be overstated. Inform employees about how patches and system updates prevent cyber attackers from exploiting software. In the event that an attack occurs, Check Point Software's Principle Security Expert, EMEA, Peter Elmer, states that, from his perspective, "the dialogue should be about how to keep people safe until a patch is available."

2. **Provide guidance around essential applications.** Applications represent security liabilities for mobile devices. The more software on a device, the greater the potential for compromise. Let employees know that they can help reduce cyber risk to corporate resources by retaining only the applications that they need on their phones. It's worth mentioning that 80% of financial applications on Android devices use vulnerable encryption and 82% of retail applications on iOS lack code protection. In turn, hackers can easily exploit weaknesses, including zero day vulnerabilities, within these apps.[2]

3. **Educate about human error.** As many as ninety percent of cyber attacks occur due to human error. In offering education around social engineering and other cyber trickery, organizations can prevent employees from becoming catalysts of zero day attacks.

4. **Fight phishing.** As many as 75% of phishing sites specifically target mobile devices.[3] Offer phishing awareness training. Hold security awareness education and information sessions on a regular basis. Be sure to communicate your message in a dynamic and interesting way that remains relevant to end-users. The end-goal is employee behavior modification.

5. **Offer security tools**. Depending on your provisioning of mobile devices and the nature of your BYOD policy (if you have one), ensure that your organization has invested in threat prevention for mobile devices.

---

[2] 2021 mobile security: Android more vulnerabilities, iOS more zero-click days, Bill Toulas, BleepingComputer.com, March 14, 2022

[3] Phishing eBook Preview, CyberTalk.org

"The dialogue should be about how to keep people safe until a patch is available."

— Peter Elmer, Principle Security Expert, Check Point Software

SOLUTIONS

How can Check Point help customers in this context?

Check Point Research analyzes mobile applications using machine learning – data driven automated systems. When mobile users are adding new apps to their devices and Harmony Mobile (free trial) or ZoneAlarm Mobile is installed, our ThreatCloud Intelligence is consulted.

If Check Point's ThreatCloud has identified the app as malicious, the installation is prevented and the user is advised. If the app has not been identified, additional processes are initiated to start analyzing the app and informing the user about potential risks as soon as possible.

Here lies the value: Everyday, we are working to analyze what we see in the field, comparing it with data we collected in the past (data driven – machine learning powered) to identify new threats trying to leverage known and unknown vulnerabilities.

In Conclusion

Cyber criminals who launch zero day attacks often bet on user or organizational failure to patch and update devices. Ensure that the devices under your control have up-to-date software, and for employees who have devices beyond your reach, stress the importance of keeping software up-to-date.

Further, leverage security apps that can identify malicious content and that can flag issues for end-users. Follow additional best practices as needed.

For more insights into emerging cyber security threats, visit CyberTalk.org.