Mobile Device, Network & App (DNA) Threats

Preventing mobile DNA attacks with Zimperium zIPS

Mobile devices are now standard computing platforms in businesses of all sizes. While this new paradigm improves user satisfaction and productivity, it also exposes personal and company data on the devices (e.g., emails, documents, photos), and in the networks and applications the devices are allowed to access, to theft and other misuse.

IT and security teams must implement mobile threat defense (MTD) solutions that detect device, network and app ("DNA") threats. Failing to stop attacks in any of these vectors will still leave the device, data and access exposed. This document highlights some of these attacks and explains how Zimperium detects all three threat vectors in real-time on the device, without requiring network connectivity or frequent updates

Device Attacks

Attackers are constantly finding new and unique ways to exploit mobile operating systems. Many attacks do not even require end user interaction. An attacker can gain remote, root access to the device, and all of the information on that device, by the user simply visiting a webpage or receiving a text message. An example of this type of user transparent attack is Stagefright, in which a device receives a text message, and without the user even opening the text message, the attacker is able to elevate their privileges, tamper with the system, gain root access and fully compromise the device and all of its data. Another example is the local elevation of privileges exploit targeting iOS 10.1.1 that was released by Ian Beer, from the Google Project Zero research team. New mobile device attacks are released every day so it is imperative to detect not only known attacks, but zero-day, unknown exploits as well.

For illustrative purposes, here is a partial list of device attack categories detected by Zimperium:

- **Device Jailbreaking / Rooting:** Jailbreaking and rooting are the processes of gaining unauthorized access or elevated privileges on a system. Jailbreaking and rooting can potentially open security holes that may have not been readily apparent, or undermine the device's built-in security measures. This type of persistence is usually the result of a system tampering event, that was then leveraged by the end user to add a third party app store on iOS, or make some file system modifications on both iOS and Android, which fundamentally breaks the underlying operating system security architecture.
- **Vulnerability Detection:**
  - **Out-of-date Operating System:** The device is running an out of date version of the iOS or Android OS and is vulnerable to compromise.
  - **Stagefright Vulnerability:** Stagefright vulnerability indicates the device is on an OS patch version susceptible to compromise.
- **Elevation of Privileges:** A malicious process that results in the elevation of privileges on the mobile device, which allows the attacker to take full control of the device.
- **Device Encryption:** The device is not setup to use encryption to protect device content.
- **System Tampering:** A process of removing security limitations originating from the device manufacturer and indicates that the device is fully compromised and can no longer be trusted. Once an attacker has gained root access by compromising the device with system tampering, they can then add surveillance tools, decrypt containers, and access all data on the device without triggering any Jailbreak or Rooting detection.
- **Abnormal Processes:** Abnormal activity that necessitates the need for the device to be monitored for any attacks.
- **File System Changes:** Persistent file system modification that necessitates the need for the device to be monitored for any attacks.
- **Untrusted Profiles:** An untrusted profile could be used to control devices remotely, monitor and manipulate user activities and/or hijack a user's traffic.
- **DNS Change:** DNS configuration change on the mobile device. If the DNS change happened in your own network to an unknown DNS server, it enables a MitM attack.

Network Attacks

If an attacker can intercept a mobile device's network traffic through techniques such as a Man-in-the-Middle (MitM) attack or a Rogue Access Point, the device and its data can be exposed to many different threats. An attacker could read and steal credentials, emails, and other sensitive data by redirecting traffic to a cloned website where a user innocently divulges credentials, by decrypting traffic though techniques like SSL Stripping or by presenting their own SSL Certificate. Attackers can even inject code into websites, that then leverage OS vulnerabilities to compromise the device itself. Even seemingly benign network activities like scans are often early indications of a network reconnaissance probe that can lead to other threats.

For illustrative purposes, here is a partial list of network attacks detected by Zimperium:

- **Man-in-the-Middle Attacks:** A malicious attacker hijacks traffic and potentially steals credentials or delivers malware to the device.
  - **ARP MitM:** MitM attack using ARP (Address Resolution Protocol) table poisoning.
  - **Fake SSL Certificate MitM:** MitM attack using a fake SSL certificate.
  - **ICMP Redirect MitM:** MitM attack using ICMP (Internet Control Message Protocol).
  - **Traffic Tampering:** MitM attack that allows a malicious attacker to change the content of the network traffic and deliver malware to the device.
  - **SSL Stripping:** MitM attack using SSL stripping that allows a malicious attacker to change HTTPS traffic to HTTP so they can hijack traffic and steal credentials or deliver malware to the device.
- **Rogue Access Point:** Exploits a device vulnerability to seemingly connect to a previously known Wi-Fi network by masking preferred/known networks.
- **Scans:** A reconnaissance scan that is often an indicator of a malicious attacker searching for a device that is vulnerable for a network attack such as MitM.
  - ARP Scan: A reconnaissance scan using the ARP protocol.
  - IP Scan: A reconnaissance scan using the IP protocol.
  - TCP Scan: A reconnaissance scan using the TCP protocol.
  - UDP Scan: A reconnaissance scan using the UDP protocol.

App Attacks

Apps can be used to execute malicious code that can fully compromise a device, or an app itself can be leveraged by an attacker to exploit privacy or security risks to gain information about the user, device, and its surroundings. App based attacks are becoming well publicized. Examples of app-based attacks are XcodeGhost on iOS and Gooligan, a family of Android-based malware that has compromised millions of Google accounts. Gooligan fully compromised the Android devices, providing the attacker with complete control over the accounts and data.

While there are thousands of variations of malicious app attacks, here is a partial list of app attack categories detected by Zimperium:

- Malicious Apps: Malicious iOS or Android apps that may have the ability to capture and exfiltrate data (e.g., emails, contacts, photos), initiate recordings or take photos/videos and/or otherwise jeopardize the device and user.
- Sideloaded Apps: A malicious app that attempts to take control of the device in some manner (e.g. elevate privileges, spyware, etc).

Zimperium's Real-time, On-device DNA Detection

The most security conscious companies select Zimperium because of our multifaceted approach to detection--an approach that has detected 100% of zero-day exploits to date without requiring an update. Powered by our patented machine-learning detection engine, "z9", Zimperium is the only Mobile Threat Defense (MTD) solution to provide real-time, on-device DNA threat detection even when the device is not connected to the network.

Zimperium's advanced cloud-based threat analysis capabilities are among the best in the world, providing a secondary layer of defense and research rather than needing to be the primary or only layer. Alternative solutions require cloud connectivity to operate. If the network is compromised, these solutions see diminished protections because the device is no longer able to securely connect back to "home base", leaving disconnected devices, data and access exposed to DNA threats.

Here are just a few examples of techniques used in Zimperium's detection stack:

Devices: Using its patented z9 detection engine, Zimperium is able to behaviorally detect device attacks in real time by examining system level data that is fundamental to the operating system. By analyzing generic, system level attributes such as memory and battery utilization, processes data, kernel statistics, and other data points, Zimperium has been able to detect 100% of zero-day exploits to-date without requiring an update.

The z9 detection engine is enhanced and improved by analyzing devices, and the data points (attributes) available to applications on those devices, while they are under attack and in normal operation mode. Zimperium then applies machine learning techniques to the aggregate raw data. This machine learning process refines the z9 detection engine's ability to determine which system level data points indicate a device threat--without requiring any prior knowledge of it. By applying machine learning techniques to analyze these fundamental system data points on the device, Zimperium offers its customers real-time detection of both known, but more importantly unknown, device threats without requiring constant updates and upgrades.

Networks: "Alert fatigue", the excessive number of false alerts that crush administrators and increases the mean time to detection of real threats, is one of the biggest challenges facing understaffed security teams. Many MTD solutions have major issues with network detection false positives. By analyzing attributes such as traffic encryption, network reputation, certificates and other data points, Zimperium's on-device protection (supplemented by cloud intelligence) improves security and avoids alert fatigue with proven network detection, almost no false positives and detailed forensics.

Apps: When an application is downloaded or installed, Zimperium's on-device engine analyzes the code to determine if it contains anything malicious. Zimperium can also query our cloud intelligence infrastructure (e.g., the Zimperium Global Malware Database) for additional activities such as code analysis. On-device and cloud-assisted code analysis includes, but is not limited to, activities like:

- Disassembly and feature extraction
- Methods, Classes, API's (internal / external), Bytecode analysis
- Feature metadata analysis, layered with intelligent cross-application correlation
- Unknown malware, variants, repackaging
- Developer Reputation
- Retrospective analysis

See For Yourself:

To see how Zimperium detects even zero-day, previously never seen before DNA attacks in real-time, request a demo or trial at info@zimperium.com or www.zimperium.com.