2016 PREDICTION #2: THE "WHAT" MATTERS MORE THAN THE "WHO" IN MOBILE SECURITY

POSTED BY: Brian Tokuyoshi on November 18, 2015 2:00 PM

FILED IN: Ignite, Mobility, Predictions
TAGGED: Gunpoder, iOS, mobile security, WireLurker, XcodeGhost

4 Like Tweet 5 G+1

This is the second in our series of cybersecurity predictions for 2016. Stay tuned for more through the end of the year.

As we look toward 2016, I think there's good reason to consider several shifts that we've seen in tactics used in recent attacks. Developments in several of these areas will play a significant role in mobile workforce security planning strategies for the year to come.

INVERTING THE HIERARCHY OF POLICY ENFORCEMENT

While many organizations are primarily concerned with perimeter security: controlling what people on the outside can do to the organization, there's still a lot of work to be done about the flip side of the equation: controlling what people on the inside can do to the organization. It is all too common to think of internal security as a matter of what can attach to the network, rather than asking the deeper questions of what those people and devices connected to the network should be able to do.

Twenty years ago, organizations relied on physical security to secure their network (no access unless you can get into the building). This notion started to crumble with wireless networking, in which authentication became the gating factor to control who was on the inside.

In both cases, however, these measures stop short of addressing the questions of what can a person or machine do once connected, and which applications can they access. This is particularly true when looking at the lifecycle of a cyberattack, where compromised endpoints are often employed to conduct lateral movement and exfiltrate information, all because many organizations do not have controls that inspect traffic inside the organization.

Network segmentation provides a part of the answer because compartmentalization can establish borders. However, while segmentation is a good first step, more needs to be done to control what traffic crosses the boundaries between segments.

These changes have been a long time coming, but, in 2016, I foresee significantly more emphasis on these issues, driven by the growing diversity of mobile devices in use. It has never been sufficient to simply allow or block devices from connecting. The next step is making sure we know what these devices are doing, and that's going to take better enforcement of security policy inside the network.

ATTACKING THE PERSON BEHIND THE APP

When taking a look at some of the attacks employed against mobile devices – such as recent iOS attacks like XcodeGhost and WireLurker – what's interesting is that the techniques were far more nuanced than they might appear. Instead of just developing a piece of malware, the people behind these attacks customized the delivery system that would get the malware onto the mobile device.

In the case of WireLurker, it was a matter of infecting the owner's laptop – hijacking the process for synchronizing and backing up the mobile phone's content. The attacker was able to insert the malicious content into the host and transfer the app via USB onto the mobile device.

In the case of XcodeGhost, the attackers went up the food chain and attacked the app developers themselves by distributing a modified version of the coding tools for building iOS apps. The resulting apps had dormant functionalities inside them that were not immediately visible to either the developer or the end user.

Home
Government
Partners
Unit 42 Threat Intelligence
Technical Documentation
Advanced Endpoint Protection

unit42

Get Updates
Sign up to receive the latest news, cyber threat intelligence and research from Unit 42.

Business Email

Submit

SUBSCRIBE TO THE RESEARCH CENTER BLOG

Subscribe

CATEGORIES & ARCHIVES

Select a Category

Select a Month

MORE →

RECENT POSTS

2016 Prediction #6: The Rise of Mobility in the Industrial Internet of Things
posted by Del Rodillas on December 3, 2015

Adversaries and Their Motivations (Part 3)
posted by Rob Downs on December 3, 2015

Last Chance to Register for Upcoming Spark User Summits
posted by Megan Scofield on December 2, 2015

2016 Predictions #5: Industrial IoT and NFV/SDN Growth and Public Cloud to Yield Emerging Security Opportunities for Service Providers
posted by Jonathan Lewis on December 2, 2015

Exploitation Demystified, Part 2: Overwrite and Redirect
posted by Yiftach Keshet on December 1, 2015

MORE →

Both attacks were capable of inserting malware into non-jailbroken mobile devices. This is possible because mobile devices do not exist on an island. They are always connected to an interface with a variety of systems, some of which they inherently trust. When attackers are capable of inserting themselves into, and abusing these trusts, new threat vectors emerge.

With this in mind, in 2016, security teams will need to think about what they need to protect (e.g., endpoint, network and mobile devices) in a blended effort, rather than counting on each one separately. This is because the intelligence and protection in one area serves as the compensating control for the other. If it's unknown whether a mobile device is compromised, then securing network traffic serves as a compensating control to catch malicious behavior. If malicious command and control traffic emerges from an endpoint, then any such traffic from a mobile device should also be closely scrutinized.

PUSHING THE BOUNDARIES OF GRAY

Categorically, there is a growing amount of software that isn't so easily defined as being safe or malicious. These grayware applications fall between the lines because the software typically interacts with a third party, and that third party's motivations, intent, and even identity may be unknown to the end user. At times, the end user may not know there's a third party involved at all. One person's remote desktop application is another person's remote access tool.

The prevalence of grayware in mobile app stores has weighed toward adware, especially from third-party ad networks. These packages include functions that the end user (and the developer in many cases) does not know about. In the haste to use an app, a user may not scrutinize the permissions given, thus providing advertisers with access to a treasure trove of data. These ad networks slip into the realm of grayware because, even though they may have the permission to access the data, there is no guarantee that the data will be used in an ethical manner.

It's my belief that more apps will use the cloudy edges of the grayware definition to slip in more malicious activity than advertising. Early signs of this activity can already be felt from the discovery of Gunpoder. When an app store evaluates an app for security risks, it is often done without the full view of the dynamics of how the functionality branches in the real world. In addition, without the context of threat intelligence, other clues about the activity conducted by the third party may not be clear. The only way to truly understand how an app operates is to see what it's doing on the network in real world conditions when it's being used, and that's the role of network security.

Want to explore more of our top 2016 cybersecurity predictions? Register now for Ignite 2016.

POST YOUR COMMENT

Name *

Email *

Website

Post Comment