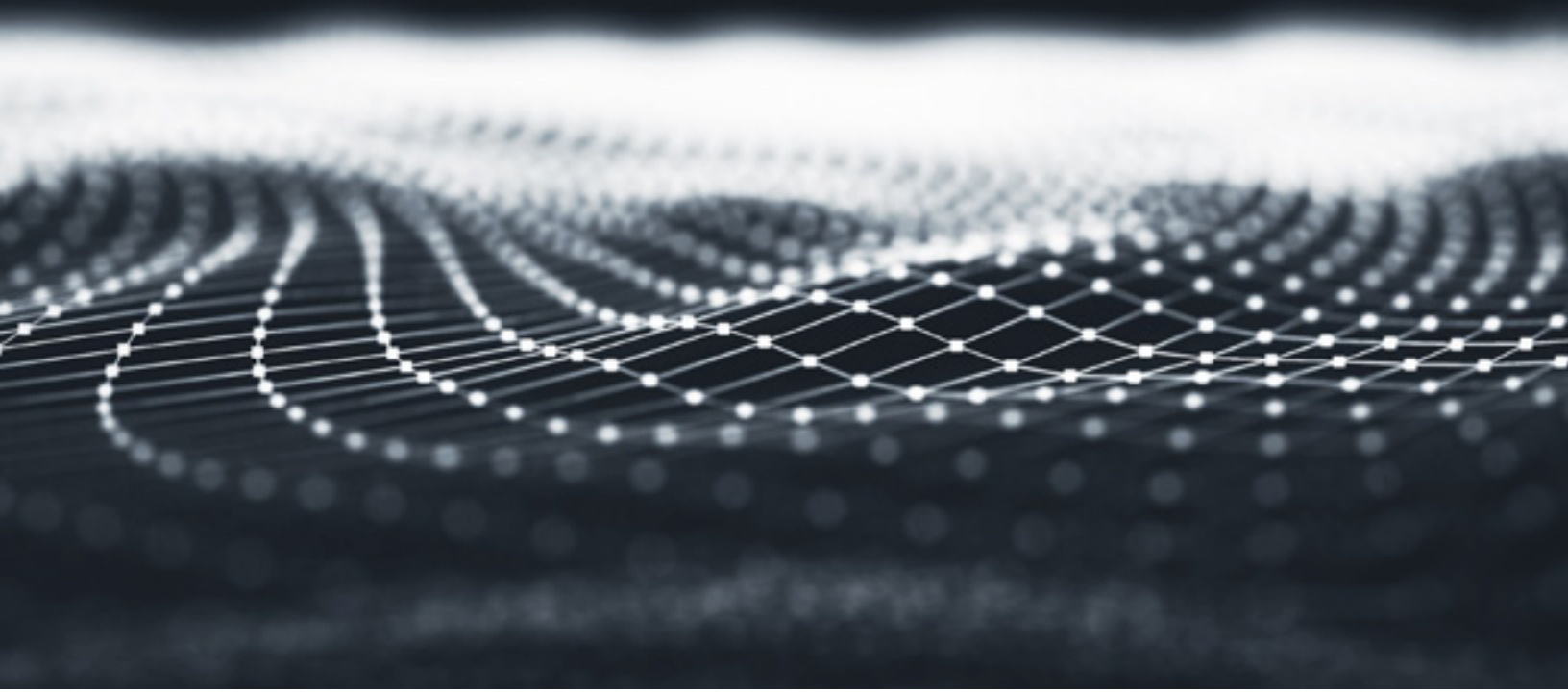
ThreatINSIGHT

A Deep Dive into Mobile Threats

Research Report



Gigamon®

Overview

It's time to look at mobile threats in a whole new light: while the numbers may look small, the threat is huge. Mobile devices greatly expand the attack surface and provide easy ways for hackers to break into your network and steal sensitive information. Learn how to protect your network through the top six mobile security best practices.

Finding the Truly Risky, Dangerous Threats Posed by Mobile Threats

More than ever, workers use their personal phones for work. A recent study found that 80%[1] of workers use their personal phones for work-related purposes. In fact, as a policy, a whopping 70% of businesses allow employees to bring their devices to work[2]. We have all come to rely on our smart phones as a critical tool for everyday life –they're almost a part of our anatomy. They are being used constantly, and more than ever those devices are used for work.

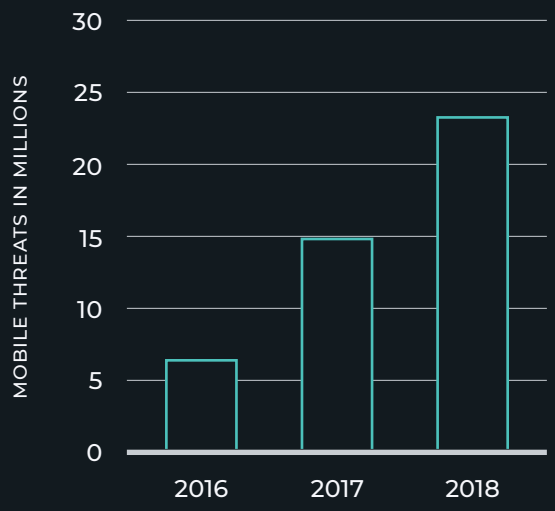
Studies show that 53% of all device usage worldwide is mobile devices; desktops and laptops only account for 43.99% of device usage, with tablets representing 2.72%.[3] We've seen a huge rate of increase in overall internet usage[4] and especially in the use of mobile devices for web browsing: 58% of site visits in 2018 were from mobile devices[5]. With the advent of 5G, providing faster cellular wireless download speeds and more bandwidth, it's safe to say that internet use is exploding exponentially, with mobility leading the charge.

Along with the huge increase in the number of mobile devices and the frequency with which they are being used to access the internet, we see a similarly impressive increase in the amount of malware: an astonishing 750 million pieces of malware, responsible for more than 10 billion attacks in 2018 alone.[6]

Mobile malware represents a relatively small percentage of the total number of malware instances seen today, but numbers don't tell the whole story. When it comes to mobility, it's not about the sheer numbers but the type of threat and the potential to access sensitive data. Security teams that weight their budgets heavily in favor of network or endpoint security and allocate minimal funds to mobile security would do well to fully understand mobile threats.

Mobile Threats

Year over year, the number of mobile threats is rising rapidly, from 10 million in 2016, to 20 million in 2017, increasing to 30 million in 2018[12].



This may seem obvious, but the reality is that many organizations' IT and security teams are not overly concerned about the use of BYOD in their networks. They either believe that the percentage of use is relatively small, or that the risk posed by using personal mobile and computing devices on the corporate network isn't really all that great.

Gigamon Applied Threat Research (ATR) recently looked at mobility data more closely to discern patterns within what is being observed, and to try to determine the level of mobile device communication on corporate networks. ATR took a sampling of organizational network metadata over a month in December 2019 (a time of end-of-year activities for many organizations), and saw that 82.5% of the organizations surveyed[7] had some form of Android and/or iOS traffic within their organizational networks.

It is important to note that these findings are not just limited to guest networks. In fact, ATR analyzed a sampling of environments that experienced mobile device usage on some 1500 subnets. A full 96% of the environments showed such usage on corporate networks; only 4% was seen on guest networks. This shows that Android and iOS network-related activity is not just a theoretical occurrence, it's a reality.

A Closer Look at Mobile Usage on Corporate Networks

Mobile Devices are a Gateway to Sensitive Information

It's easy to underestimate the threat posed by mobile devices, but organizations would do well to remember two key facts. First, although many organizations don't store their prized possessions on mobile entities, valuable information is easily accessible through mobile devices. Highly sensitive data such as consumer credit card information, personally identifiable information and intellectual property, even when stored securely, can be and often is accessed through SaaS-based applications that are increasingly being used on mobile devices. With the proper permissions, even the most critical data can be accessed and often downloaded or manipulated.

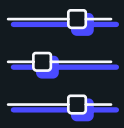
It's important to keep in mind that the prime motivation of most threat actors is financial gain. They are focused on the location of the biggest payoff: the company. Because they are targeting a company, and going after as many targets as possible, mobile is one important threat and could potentially provide access to sensitive information tied to literally millions of individuals. The attacker, ultimately, is running a business, where high risk/high reward still reigns supreme.

Second, the threat is that when mobile or BYOD devices access sensitive corporate data, very often there is little or no monitoring in place to even alert security teams of the compromise. It's difficult to determine just what percentage of threats is targeted toward organizations, especially based on the trends of BYOD, because it is a challenge to keep track of which devices are accessing data, moving it out of the organization, or perhaps being targeted by a specific threat.

We know that there are huge numbers of mobile devices in use and have evidence that many of them are being used inside the corporate network. As mentioned earlier, we are not just seeing mobile devices on guest networks, so we need to get a better understanding of exactly what kinds of threats these devices pose.

Mobile Device Threats Expand the Attack Surface.

What Threats do These Devices Pose?



NUMBER OF APPLICATIONS

Most mobile devices run an average of 60-90 applications[8], facilitating access to email, SaaS-based solutions, cloud storage, social networks, games, news feeds and much more. Contrast this with laptops which run an average of 10 programs[9]. Add to this the fact that most people spend an average of 2.2 hours per day on their laptop, while they spend 3.1 hours on their mobile devices[10]. It's easy to see that the potential for risk increases with the more applications, more protocols, and more time spent on the device.

FORM FACTOR

A classic espionage threat posed by mobile devices is the fact that the phone has both a camera and a microphone. Whereas it may be difficult or impossible to bring a laptop into a sensitive corporate meeting, no one even notices if someone comes in with a mobile phone in their pocket or bag. It's not too difficult to live-stream the meeting to an outsider or take photos of sensitive documents or presentation materials using such a small device.

INCREASED ATTACK SURFACE

A second threat comes from the increased attack surface provided by mobile devices. While much of the device activity on a corporate network is likely tied to WiFi connectivity for traffic moving out of the network, large numbers of cloud services (MSOffice 365, DropBox, file sharing, social media, etc.) bring additional ways to exfiltrate data or access sensitive information. We are seeing a large and growing amount of mobile activity associated with cloud services. What this means to the hacker is that it is relatively easy to construct highly targeted phishing emails, using information freely offered up by users, and gain access to the mobile device. There are other ways to gain access to a mobile device and use it as a springboard into the corporate network: drive-by downloads, waterhole attacks, website compromises.... the list goes on.

BLURRING THE LINE BETWEEN WORK AND PERSONAL USE

Users often commingle contact information, with the result that it's easy to email or text sensitive information to the wrong person. It's likewise trivial to post company-sensitive information to social networks. If the device has been hacked (e.g. while using public WiFi), it's possible that the user's social media, email or VoIP conversations could be compromised[11]. This creates ample opportunities for sensitive information to get into the wrong hands.

Real-world Mobile Threats

These examples of applications can be troublesome given that so many companies allow employees to bring their own devices (BYOD) to work. The presence of such threats on sensitive networks creates a major exposure, with the ability to record room and call audio, spy on other communications or data on devices, and socially engineer users into taking further action. ATR recommends that devices should be audited for installed applications such as this, and if no BYOD policy is in place, Android devices should be locked down and kept updated to avoid rooting or installation of unauthorized software.

One of the biggest mobile threats has come from Shanghai-based ADUPS, an Android "firmware provisioning" company whose firmware turned out to be not so benign. In fact, it contained built-in malware that directly transmitted call logs, SMS, contact and location information and more from mobile devices within the US, directly to Chinese servers. In 2016, Barnes & Noble found that their newest tablet included ADUPS. A year later, the company ADUPS was found to have pre-installed an auto installer with system-level rights on mobile devices from manufacturers such as BLU and other mobile devices found on online stores. As preinstalled software, it cannot be removed or even disabled, and still has the ability to install dangerous apps.

Gigamon ATR recently investigated a pattern of unexpected network behavior and pinpointed the source as an Android application called Taslal[13]. This is an app that helps parents keep tabs on their children. However, the application's activity went far beyond what would be expected. After installation it regularly communicates with a Command and Control server, sending back details such as network location and WiFi information. It can record and exfiltrate calls and room audio, send text messages and read from SMS, WhatsApp, Google Hangouts, Facebook and more. Its permissions include the ability to erase all data, change the screen-unlock password, set password rules and more.

Recently, several hundred Israeli soldiers found that their mobile phones had been infected by malware sent by Hamas cyber militants. Using fake profiles of women, the app lured soldiers into chatting over messaging platforms. In the process, the soldiers downloaded malicious malware that returned critical device information, contact information and message; it was also able to access the camera and microphone.[7]

What's an Organization to Do?

Locking down the mobile environment is calls for a defense-in-depth strategy employing several steps:

LIMIT USE

One of the most effective ways to secure your environment is to limit the use of mobile devices in sensitive business locations.

MONITOR YOUR NETWORK

Make sure you employ Network Detection and Response (NDR) solutions to analyze mobile device traffic for inbound, outbound and interoffice communication activity associated with threats.

CHECK POLICIES

Make sure your BYOD policies are tight enough to give you peace of mind. They should reflect a clear understanding of what types of apps cannot be used organizationally and what usages are permitted or disallowed (e.g. transferring company files from approved cloud storage to unapproved cloud storage).

MOBILE DEVICE MANAGEMENT

Solutions that allow policy implementation on mobile devices are always a good idea. Make sure that you have policies in place that lock down devices, whitelist applications, and ensure VPN access.

MULTI FACTOR AUTHENTICATION (MFA)

This type of authentication has become widespread and should be one of the many implementations to be included.

USER EDUCATION

Never forget that users are the first line of defense. It's not enough to do compliance training once a year: threat actors continuously update and enhance their attacks, so continuous education (including phishing simulation) can go a long way toward keeping security top-of-mind for employees.

Seeing Mobile Threats in a New Light

It's clear that mobility threats are nothing to ignore or treat lightly. While there may not be an overwhelming number of attacks aimed directly at mobile devices, we see them as the next likely entry point into the organization mobile devices have multiple capabilities such as identity-corroboration (MFA, biological, facial recognition), voice recording[16], video capture and more, making them favored tools and targets for threat actors whose malware can hijack these capabilities[17].

With ever-greater use of mobile devices and their upcoming expansion into the world of 5G, it's important to protect your network now, before this dangerous trend escalates.

Go to gigamon.com/threatinsight to learn more about how Gigamon ThreatINSIGHT, a cloud-native, high-velocity network detection and response solution, can protect your network against mobile threats.

The Gigamon Applied Threat Research (ATR) team's mission is to dismantle the ability of an adversary to impact our customers. Our team of expert security researchers, engineers and analysts focuses on continuous research of threat actors and emerging attack techniques while building detection and investigation capabilities leveraging the Gigamon ThreatINSIGHT solution's network telemetry and intelligence datasets.

Learn more about ATR at gigamon.com/atr

References

[1] https://www.trackvia.com/blog/infographics/mobile-devices-are-a-necessity-in-todays-business-world/

[2] https://www.trackvia.com/blog/infographics/mobile-devices-are-a-necessity-in-todays-business-world/

[3] https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet

[4] https://ourworldindata.org/internet

[5] https://www.perficientdigital.com/insights/our-research/mobile-vs-desktop-usage-study

[6] https://www.techradar.com/news/over-10-billion-malware-attacks-detected-in-2018

[7] https://www.forbes.com/sites/zakdoffman/2020/02/16/terrorist-android-malware-exposed-here-are-the-hamas-apps-that-targeted-israeli-soldiers/#3c8eb4f523ae

[8] https://buildfire.com/app-statistics/

[9] https://www.microsoft.com/en-us/windows/windows-10-apps

[10] https://mindsea.com/app-stats/

[11] https://securityaffairs.co/wordpress/38510/cyber-crime/3-uk-politicians-hacked-wifi.html

[12] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/2018-mobile-threat-landscape

[13] https://atr-blog.gigamon.com/2020/07/16/mobile-threats-taslal

[13] https://www.linuxjournal.com/content/adups-android-malware-infects-barnes-noble

[14] https://blog.malwarebytes.com/cybercrime/2017/12/mobile-menace-monday-upping-the-ante-on-adups-fwupgradeprovider/

[15] https://www.forbes.com/sites/zakdoffman/2020/02/16/terrorist-android-malware-exposed-here-are-the-hamas-apps-that-targeted-israeli-soldiers/#26f83b5723ae

[16] https://www.forbes.com/sites/leemathews/2018/02/28/creepy-new-android-malware-can-secretly-record-your-conversations/#4afddd94335f

[17] https://www.zdnet.com/article/the-ultimate-guide-to-finding-and-killing-spyware-and-stalkerware/

About Gigamon

Gigamon is the first company to deliver unified network visibility and analytics on all data-in-transit, from raw packets to apps, across physical, virtual and cloud infrastructure. We aggregate, transform and analyze network traffic to solve for critical performance and security needs, including rapid threat detection and response, freeing your organization to drive digital innovation. In short, we enable you to run fast, stay secure and innovate.

Gigamon has been awarded over 75 technology patents and enjoys industryleading customer satisfaction with more than 3,000 organizations, including 80 percent of the Fortune 100. Headquartered in Silicon Valley, Gigamon operates globally.

For the full story on how Gigamon can help you, please visit www.gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com