BlackFog® Mobile Device Security

Next Generation Cyber Security Protection

Dr. D. Williams, BlackFog, Inc.

Introduction

Mobile devices now total 5.1 billion users, penetrate 68% of the world population and represent 52% of global web traffic (1). More than half of these are ‘smart’ devices with Internet access (1). iOS now represents 1.3 billion active devices (10). It is no wonder that cyber criminals specifically target mobile devices.

As a result, mobile cyber attacks have grown dramatically over the last few years with 40% growth in 2017 alone (2). These attacks increasingly focus on individuals’ personal data and privacy. New forms of attack such as ransomware, crypto-mining and malvertising are now common.

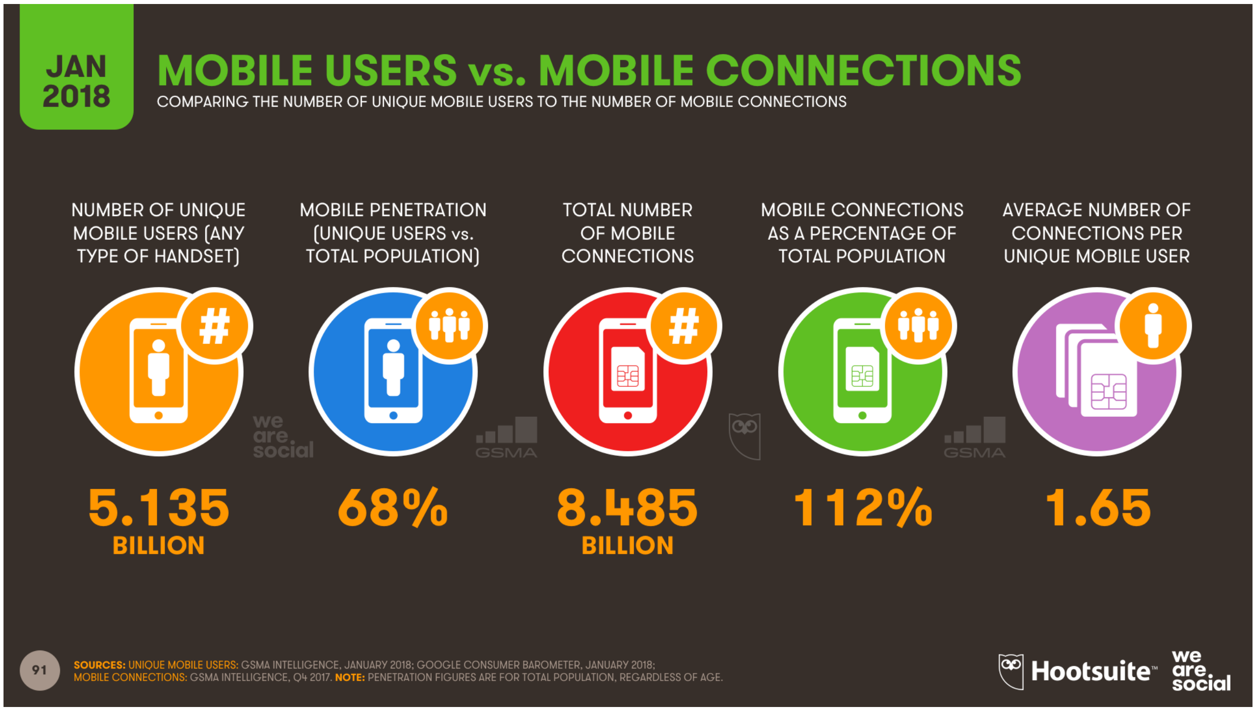
Existing solutions are no longer enough.

The Firewall Age

In the early days of cyber security it was considered best practice to install a firewall on the perimeter of the network. Blocking open ports with known vulnerabilities ensured existing exploits could not be used to infiltrate a device. This was often enough when attacks leveraged protocol weaknesses or focused on Denial of Service (DoS) (3). Unfortunately, cyber attacks have grown increasingly sophisticated and target multiple points of weakness. Today, most cyber criminals can easily bypass firewalls and often employ tunneling and encryption to evade detection.

The Anti-Virus Age

The second generation of cyber security recognized that threats were increasingly targeting the mobile device itself, often referred to as the endpoint.



JAN 2018

MOBILE USERS vs. MOBILE CONNECTIONS

COMPARING THE NUMBER OF UNIQUE MOBILE USERS TO THE NUMBER OF MOBILE CONNECTIONS

NUMBER OF UNIQUE MOBILE USERS (ANY TYPE OF HANDSET)	MOBILE PENETRATION (UNIQUE USERS vs. TOTAL POPULATION)	TOTAL NUMBER OF MOBILE CONNECTIONS	MOBILE CONNECTIONS AS A PERCENTAGE OF TOTAL POPULATION	AVERAGE NUMBER OF CONNECTIONS PER UNIQUE MOBILE USER
5.135 BILLION	68%	8.485 BILLION	112%	1.65

91

SOURCES: UNIQUE MOBILE USERS: GSMA INTELLIGENCE, JANUARY 2018; GOOGLE CONSUMER BAROMETER, JANUARY 2018; MOBILE CONNECTIONS: GSMA INTELLIGENCE, Q4 2017. NOTE: PENETRATION FIGURES ARE FOR TOTAL POPULATION, REGARDLESS OF AGE.

This was the era of Anti-Virus solutions. While these applications are now quite common, few end-users truly understand how they operate and why they are of limited use against modern cyber attacks.

Once attackers evade the firewall they can install a payload on the device and proceed to steal data. This malware often remains latent on the device and may install a Remote Administration Tool (RAT) to remotely control your device (4).

Anti-Virus solutions use a technique known as fingerprinting to identify malicious software. Fingerprinting technology looks at every file on a device and generates a unique identification number, or signature. This signature is then compared to a database of known "bad actors". When a match is found the offending file is removed.

It is important to understand the limitations of this technique in terms of device and data protection. First, fingerprinting takes time. The bad actor needs to be identified. Just like in the real world, after a break-in, the police have to arrive at the scene, investigate and take fingerprints, then compare the prints to a list of known criminals. This is no different in the digital world. It takes teams of people to identify, analyze and classify the problem. Of course, this takes time. Typically, a best case scenario hovers around 4 hours, but the reality is usually significantly longer, often 24 hours or more.

Since the majority of cyber attacks do critical damage within the first few hours, time is truly of the essence and global dissemination is the result. Recent examples include WannaCry (5) and Petya (6). Second generation Anti-Virus protection is therefore based upon prior knowledge of the attacker. Naturally, cyber criminals are aware of this and have specifically designed malware to avoid the entire fingerprinting process.

Modern Cyber Attacks

Modern cyber attacks employ a host of new techniques to evade detection. To stay ahead of Anti-Virus solutions attackers now randomly change signatures. Known as polymorphic malware, this type of attack mutates every time it copies itself to a new location (7). Other techniques include fast fluxing (dynamically changing network domains) and fileless based attacks (8).

The BlackFog Age

Using an analogy we can relate cyber security products to medical conditions. Whereas a firewall focuses on known vulnerabilities (pre-existing conditions we can manage), anti-virus solutions focus on treatment once you become ill. If we extend this further we can think of BlackFog as preventive medicine whereby we can prevent infection by being immunized.

Rather than detecting malware after it is installed, BlackFog prevents activation and therefore propagation on the device. Since all cyber attacks require an active network connection to function BlackFog analyzes all outbound network activity (data exfiltration).

Using behavioral profiling techniques BlackFog is able to prevent most cyber attacks by looking at specific traits. By analyzing the type and destination of connections it is able to prevent malvertising, crypto-mining, ransomware, phishing and other malware in real-time.

Typically, attackers use fileless techniques to avoid detection and download or execute remote payloads with the purpose of stealing data. To do this it is necessary to connect to a remote server. Since this needs to remain anonymous to avoid detection, it is usually performed over the Dark Web. By blocking:

- Fileless execution
- The Dark Web
- Remote targets

BlackFog stops the attacker at each stage of the cycle.

Data Privacy

Mobile technology has evolved over the last several years as have the business models of major technology companies.

These companies have become reliant on advertising to monetize and hence grow their business for shareholders.

The increased sophistication of the algorithms used to track and monetize users means that Advertisers are now focused on changing behavior to influence your purchasing decisions and change social discourse. This also means that it tends to amplify negative and minority views quicker than positive views, because this creates results much faster (9).

BlackFog specifically protects user privacy by preventing the collection and dissemination of data to third parties. This includes blocking of Facebook, advertising and data profiling.

With 77% of successful attacks now incorporating techniques not covered by firewalls and anti-virus solutions it is more important than ever to include BlackFog as part of your overall security solution.

BlackFog is currently available for Windows, Mac, iPhone and iPad. Android support will be available in the latter half of 2018.

References:

1. Digital in 2018: World’s Internet Users pass the 4 Billion mark. We Are Social. Nathan McDonald. January 2018.

2. Mobile cyber attacks on a dramatic increase. Information Age. Nick Ismail. September 2017.

3. Denial-of-service attack. Wikipedia.

4. Top Remote Administration Tools (RATS) of 2018. Ethical Hacking Tutorials. April 2017.

5. WannaCry Ransomware and the NHS attack. BlackFog. Dr. Darren Williams. May 2017.

6. Petya cyberattack hits Europe and is quickly spreading. BlackFog. Dr. Darren Williams. June 2017.

7. How Hackers Hide Their Malware: The Basics. DARKReading. Corey Nachreiner. August 2017.

8. Fileless Network Protection. BlackFog. Dr. Darren Williams. March 2018.

9. How we need to remake the Internet. TED. Jaron Lanier. April 2018.

10. Notes of interest from Apple's Q1 2018 conference call. AppleInsider. AppleInsider Staff. February 2018.