Top

Back to Contents

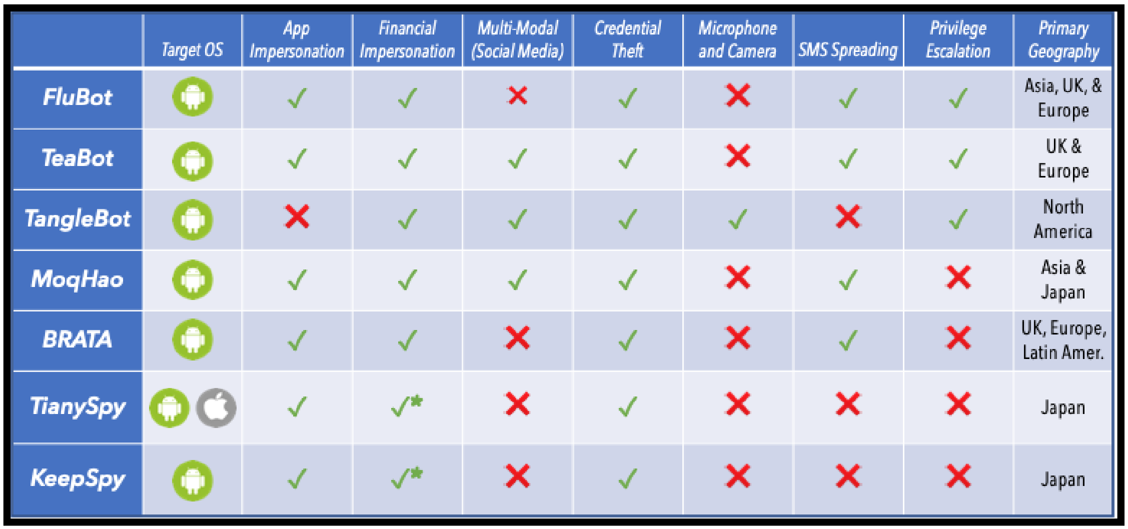
Newsletter 6/28/2022

A Printable PDF of this post is available here.

The Smartphone is now the attack surface
We always knew it would become

You never call me when you're sober
You only want it 'cause it's over, it's over .

— Call Me When You're Sober, Amy Lee / Terry Balsamo



	Target OS	App Impersonation	Financial Impersonation	Multi-Modal (Social Media)	Credential Theft	Microphone and Camera	SMS Spreading	Privilege Escalation	Primary Geography
FluBot	🤖	✓	✓	✗	✓	✗	✓	✓	Asia, UK, & Europe
TeaBot	🤖	✓	✓	✓	✓	✗	✓	✓	UK & Europe
TangleBot	🤖	✗	✓	✓	✓	✓	✗	✓	North America
MoqHao	🤖	✓	✓	✓	✓	✗	✓	✗	Asia & Japan
BRATA	🤖	✓	✓	✗	✓	✗	✓	✗	UK, Europe, Latin Amer.
TianySpy	🤖 🍎	✓	✓*	✗	✓	✗	✗	✗	Japan
KeepSpy	🤖	✓	✓*	✗	✓	✗	✗	✗	Japan

Source: Proofpoint 3/09/2022
https://www.proofpoint.com/us/blog/email-and-cloud-threats/mobile-malware-surging-europe-look-biggest-threats

The chart above details both the common and unique characteristics of certain types of malware attacking smartphones this calendar year. Clearly from the chart above, we see that there are more samples of malware attacking Android users than Apple's iOS. Nevertheless, this is not a complete list of current malware attacking smartphones. **On June 23, 2022, Google published its findings on a particular piece of spyware that attacked both iOS (Apple) and Android smartphones**. The hackers carefully circumvented the Apple Store controls against malware distribution from the Apple Store. Dubbed the "Hermit" spyware, the Verge reported that "**the spyware can infect both Android and iPhones by disguising itself as a legitimate source, typically taking on the form of a mobile carrier or messaging app.**" On May 1, 2022, the **Dispatches reported on the growing "Smishing" trend**.

Security vendor Proofpoint published a report March 9, 2022, that contended from the beginning of February 2022 to the end of February 2022, malware attacks on Smartphones rose by 500%. And there is no mystery as to why attacks on smartphones are increasing so dramatically. The smartphone holds the keys to our private and not so private lives, same as our desktops. **As the TechTimes put it**:

> **Usually, the cybercriminals behind these attacks have a common goal to achieve: stealing confidential information from the users. These include bank account details, email addresses, passwords, and usernames.**
>
> **Furthermore, they could also access the device through remote code execution. It's quite disturbing to think that our smartphones could be an outlet of privacy invasion from unknown hackers.**

Indeed, most of the malware attacking smartphones are directed toward systems based on Android. Nonetheless, the newer and more sophisticated malware attacking smartphones is independent of any vendors' "store." Smishing and sending malware via SMS texting is becoming a very real problem, as well as one big nuisance. A current example was discovered that employs Chinese language based malware. This so-called "**SMS Bomber Tool with Malware Hidden Inside**," is presently very active.

> **SMS Bomber, as the name indicates, allows a user to input a phone number (not their own) so as to flood the victim's device with messages and potentially render it unusable in what's a denial-of-service (DoS) attack.**

A long running malware campaign that infected machines using the Apple Safari web browser went undetected for 5 years. **The Hacker News, June 20, 2022**, reported on a Google effort that found "**A security flaw in Apple Safari that was exploited in the wild earlier this year was originally fixed in 2013 and reintroduced in December 2016, according to a new report from Google Project Zero.**" The same article noted that "**In early February 2022, Apple shipped patches for the bug across Safari, iOS, iPadOS, and macOS, while acknowledging that it "may have been actively exploited**."

Attacks seem to increase at an exponentially greater rate on a daily basis. Also, considering that creating the necessary patching means the rewriting of the 1000s of lines of code, the article cited above rightly concludes: "**It seems untenable for any developers or reviewers to understand the security implications of each change in those commits in detail, especially since they're related to lifetime semantics**."

In other words, if the programmers doing the patching aren't really sure if any one patch will work or hold, we mere users are at a great disadvantage when it comes to protecting our devices and ourselves while online. And, with the wide adoption of smartphones by even old holdouts like me, we are online 24/7. And that statement holds especially true for IPhone users.

An iPhone is never really turned off. So, of course, "**Cybersecurity researchers have discovered a way to run malware on Apple's iPhones, even when the device is switched off**." When an iPhone is powered down, the device is actually put into a deep low power mode (LPM), but the device is for all intents and purposes still powered on. And there exists the possibility of communication with the powered down, but not really "OFF", device . "**LPM allows device certain smartphone facilities - such as Bluetooth, near-field communication (NFC) and or ultra-wideband.**" The purpose for this is so "**people will still be able to use their on-device wallets and keys, even when they are out of battery.**" Since LPM is a function of hardware and not software, this vulnerability cannot be patched.

Under the current state of the art, an attacker would need to first **jailbreak the device**, which would be very difficult to do remotely. Yet, with each passing day, hackers find ways to get into any system that is vulnerable. **Factor in all the devices logged into old unsupported and hopelessly out of date routers, and it becomes easy to imagine that in time the LPM vulnerability will be exploited**.

These are just some of the reasons it is time that we protect our smartphones with security software. I have had my best results in terms of having the least impact on system performance from **Malwarebytes** and Microsoft/Windows Defender. Both products come from trusted sources: the manufacturers themselves. While no antimalware product is 100% effective all the time and against all threats, both products will provide you with reasonable protection against most threats. **MSDefender** is free, however, if you or someone in your household has a Office 365 subscription. And unlike Malwarebytes, MSDefender is one app for any popular system: Windows, macOS, iOS, and Android. A review, with pros and cons of the Microsoft Defender for Individuals, as is its full name, can be read at **Ars Technica**. My walk through the setup of MSDefender appeared in the **Dispatches, June 22, 2022**.

Some people have had difficulty installing MSDefender. You must access the installer from your phone. Open this link below :

https://www.microsoft.com/en-us/microsoft-365/microsoft-defender-for-individuals#office-CustomMosaicCta-atxj7x0

ON YOUR PHONE using the phone's web browser, like Safari on an iPhone. Click the appropriate button for your device's operating system. Follow the prompts to install. **Or follow the steps in the first posting about MSDefender**.

There is a malware process known as msdefender.exe. It is not the antimalware application from Microsoft and predates the application discussed herein. Just setting the record straight. It's kinda my job.

Lock it down for the quarantine
Love quarantine
Lock it down down down

— Lock It Down (Quarantine Love), Blair Edwards

Back to Top

Gerald Reiff

Back to Top

next post ⟶