

Forum:[Hack Forums](#)

Thread: [Man-In-The-Cloud \(MITC\) smartphone attack](#)

SulY_Pipin76 - March 11, 2020, 9:12 am

Hello!

This thread is about a possible MITC attack and exfiltration of information by stealing the synchronization authentication Token used by some cloud services (e.g. GDRIVE, Dropbox, etc).

See more:

https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

Do you guys have any knowledge about this happening to you/someone else via exfiltration of info such as pictures, audio etc from a smartphone?

Like, my company uses MEGA.nz for co-working different projects shared (SHARED folder) by the team (me, colleagues, boss) and I myself use MEGA to upload some pictures to my personal cloud. I also use/used GDRIVE, mostly for work but now very sparingly. Those files somehow ended up in attacker's hands (don't know how). Imperva showed that the attacker would need to somehow pass the SWITCHER code (malware/spyware) to the victim so they could copy the synch/auth token (without needing the auth credentials, user and pass).

I'm requesting a demo from <https://www.skyhighnetworks.com> to test somehow if there's a cloud breach on my company that could've affected all the devices connected to the MEGA service and ISP, including my smartphone. In the meantime, I'm trying to figure out and researching how this could've happened...how hard it would be to "catch" the perpetrators since the monitoring is still ongoing!? Any ideas?

Any help is greatly appreciated!

compalabee - March 11, 2020, 12:10 pm

(Mar 11, 2020 09:12 AM)SulY_Pipin76 Wrote: [\[CITE\]](#) This thread is about a possible MITC attack and exfiltration of information by stealing the synchronization authentication Token used by some cloud services (e.g. GDRIVE, Dropbox, etc).

Android phones can be flashed with an OS called a Nethunter ([link here](#)) that can do wireless attacks. The intruder may have physically entered your premises (or just outside the door!) with nothing but an inconspicuous phone, did a MITM attack to steal your API tokens, then pivoted to MITC when he got them.

Another possibility is that they may have actually used a computer, albeit a very small one. Raspberry Pis do this job pretty well. (Personally I use a TinkerBoard but I'll be switching to this rig soon).

Another (waaay more plausible explanation) is that you have a corporate spy in your ranks, some internal threat actor. An underpaid employee? Someone with a corporate vendetta?

SIM-4294714 - March 11, 2020, 12:23 pm

(Mar 11, 2020 12:10 PM)compalabee Wrote: [\[CITE\]](#) Android phones can be flashed with an OS

called a Nethunter ([link here](#)) that can do wireless attacks. The intruder may have physically entered your premises (or just outside the door!) with nothing but an inconspicuous phone, did a MITM attack to steal your API tokens, then pivoted to MITC when he got them.

Another possibility is that they may have actually used a computer, albeit a very small one. Raspberry Pis do this job pretty well. (Personally I use a TinkerBoard but I'll be switching to this rig soon).

Another (waaay more plausible explanation) is that you have a corporate spy in your ranks, some internal threat actor. An underpaid employee? Someone with a corporate vendetta? Disgruntled employees? In my organization? It's more likely than you think.

SuLY_Pipin76 - March 12, 2020, 3:57 am

(Mar 11, 2020 12:10 PM)compalabee Wrote: [\[CITE\]](#) Android phones can be flashed with an OS called a Nethunter ([link here](#)) that can do wireless attacks. The intruder may have physically entered your premises (or just outside the door!) with nothing but an inconspicuous phone, did a MITM attack to steal your API tokens, then pivoted to MITC when he got them.

Another possibility is that they may have actually used a computer, albeit a very small one. Raspberry Pis do this job pretty well. (Personally I use a TinkerBoard but I'll be switching to this rig soon).

Another (waaay more plausible explanation) is that you have a corporate spy in your ranks, some internal threat actor. An underpaid employee? Someone with a corporate vendetta? Interesting...

How can I install Nethunter on my phone? (Samsung Galaxy A10)?

Thanks!

About corporate vendettas and underpaid employees, it's unlikely. Currently we are a team of 3 and a small company.

compalabee - March 13, 2020, 12:27 am

(Mar 12, 2020 03:57 AM)SuLY_Pipin76 Wrote: [\[CITE\]](#) Interesting...

How can I install Nethunter on my phone? (Samsung Galaxy A10)?

Thanks!

About corporate vendettas and underpaid employees, it's unlikely. Currently we are a team of 3 and a small company.

I don't think it works on the A10. Last I checked there's a pretty limited list of compatible devices. IIRC you don't even need to jailbreak your phone.

The Offensive Security website should help you out more.

SuLY_Pipin76 - March 13, 2020, 3:28 am

(Mar 13, 2020 12:27 AM)compalabee Wrote: [\[CITE\]](#) I don't think it works on the A10. Last I checked there's a pretty limited list of compatible devices. IIRC you don't even need to jailbreak your phone.

The Offensive Security website should help you out more.

Actually I could download it but Symantec anti-virus blocked it as 'Trojan - Malware' as I was installing it.

I assume this is normal because it's a pentesting tool.

So, safe to whitelist (downloaded directly from Offensive Security as F-Droid app)!?

compalabee - March 13, 2020, 3:36 am

(Mar 13, 2020 03:28 AM)SulY_Pipin76 Wrote: [\[CITE\]](#) Actually I could download it but Symantec anti-virus blocked it as 'Trojan - Malware' as I was installing it.

I assume this is normal because it's a pentesting tool.

So, safe to whitelist (downloaded directly from Offensive Security as F-Droid app)!?

Ya, it's safe. In fact mastering Kali Linux (or Kali Nethunter too?) is a requirement of getting PWK and OSCP certificates. Those certs are some of the most sought-after in infosec.

It should be malware otherwise it'll be useless as an attack simulation tool ? You have tools in there that allow you to craft viruses and RATs on the fly.

SulY_Pipin76 - March 16, 2020, 3:59 am

(Mar 13, 2020 03:36 AM)compalabee Wrote: [\[CITE\]](#) Ya, it's safe. In fact mastering Kali Linux (or Kali Nethunter too?) is a requirement of getting PWK and OSCP certificates. Those certs are some of the most sought-after in infosec.

It should be malware otherwise it'll be useless as an attack simulation tool ? You have tools in there that allow you to craft viruses and RATs on the fly.

Ok, cool!

Dangerous stuff, I see!