

Forum:[Hack Forums](#)

Thread: [Securing compromised device](#)

Goingby - September 11, 2019, 10:30 am

Hi everyone! This is my first post, but I have used the search tool already without success. I am just a user, not developer and frankly a newby regarding mobiles and IT security, but I need some guidance and I'd appreciate any help.

Situation

1. I've got hacked, total control (photos, emails, camera, contacts, whatsapp, screen etc) of my unrooted android phone (xiaomi redmi note 7).

It was a targetted attack, no manual app installed, no unsafe 3rd party apps allowed. Attackers only had my gmail account (linked to android) and telephone number. I know them personally, and they leaked personal information to people at work (who enjoy it but won't help me with this issue).

No high consumption of battery/data. Just leeching information, launching some apps eventually, and few interactions with the screen minimizing etc. I bet I should learn to analyze network traffic (?).

2. I Installed antimalware (e.g malwarebytes), antivirus (avg, eset etc). No positive results. I also installed "No-root firewall" to control programs accessing internet, nothing strange.

3. I've changed emails(new), SIM + Telephone. Got hacked again. I suspect my own wifi was compromised (changed router password, wifi password, internal ip, deactivated ping, port forwarding, remote control).

Additionally, I added 2 step verification to emails (app), changed passwords, encrypted the device etc. I have found no IP from them in the emails log, nor alert from gmail. Only once a session from Linux device (not mine) in my gmail account, and some fake profiles in social networks requesting friendship and sending a message. I believe they have accessed through the device.

4. I want to restore the device somehow and avoid getting hacked again.

One of the problems I face is that now I'm not in the same circle of people from which I gathered most of the info on the leaked information, so I can't get to know if the actions I am taking got rid of the hack, besides some punctual actions they may do (launch app etc). So I have to act quite paranoid and do the most secure action.

Question

Any idea on how they managed to do that? how can I prevent it or prove it?

I thought about a hard reset, but I'd be in the same situation. If there was an exploit, restoring stock ROM would place me in the same position as before, i.e vulnerable.

Also, a reset would get rid of any proof, but I kinda prefer it if that would solve it.

As far as I know, a hard reset in android only formats one partition (user data), so if there is a trojan located in /system it would be pointless. With an unrooted device I can only get rid of /cache and /data.

Should I install another ROM? (my phone has always been unrooted) which one? (restoring the stock ROM would probably be pointless if the vulnerability is due to android...

Is there any other measure I could take? documents I could read regarding this issue?

Thank you in advance, I'd appreciate any help.

P.S Let me know if the forum is not the right one, I thought forensics would be suitable.

CyberStrike - September 12, 2019, 10:24 am

You just added 2fa? Did you initially have a crummy password? Perhaps you had a "remember me" checked? Did you check your other devices/computers? Your phone runs what Android Pie? There are a few exploits but just 3 which appear to be remote for Android OS if it's Pie, applications might be another vector which some applications have remote exploits. Are you downloading any cracked or garbage apps? (Be honest here I have heard many people tell me they didn't install whatever and after looking they admit to having crapware)

Have you considered contact law enforcement? If you did factory reset then they would have to deploy the exploit again, perhaps this time you may not click on random links? Then again evidence probably is gone at this point if you hard reset.

SIM-4294714 - September 12, 2019, 10:33 am

If you've got someone who's willing to root your phone, take down your router, and move laterally inside your wifi, I hate to say it but there's not a lot you can do. Maybe talk to your ISP. Once they start pivoting, eventually they get so deep that they can override or replace any action you cause. Swapping out antiviruses, disabling firewalls, all that. A targeted APT threat is for all intents and purposes impossible to stop.

Goingby - September 13, 2019, 10:04 am

(Sep 12, 2019 10:24 AM)CyberStrike Wrote: [\[CITE\]](#) You just added 2fa? Did you initially have a crummy password? Perhaps you had a "remember me" checked? Did you check your other devices/computers? Your phone runs what Android Pie? There are a few exploits but just 3 which appear to be remote for Android OS if it's Pie, applications might be another vector which some applications have remote exploits. Are you downloading any cracked or garbage apps? (Be honest here I have heard many people tell me they didn't install whatever and after looking they admit to having crapware)

Have you considered contact law enforcement? If you did factory reset then they would have to deploy the exploit again, perhaps this time you may not click on random links? Then again evidence probably is gone at this point if you hard reset.

- Password wasn't that strong and I didn't have 2fa on previously, despite that, it is not through brute force they've got inside, otherwise I would have notifications or a different password. I changed password from another device immediately and activated 2fa.

- I haven't clicked any phishing url/email - or so I think.

- Apps downloaded only through playstore, 3rd party apps have always been deactivated. No porn/hack/stupid apps, just common ones and language learning ones. Nothing suspicious. I am neither giving permissions blindly when installing apps.

On the other hand, PC does have some cracked soft, but all this started through the phone, by people I know with a concrete purpose of harming me. Now I run a clean system with a different OS, same hardware and router though...

- Non rooted phone, no virus/malware found. It's an Android 9, currently PKQ1.180904.001 but there was a security update no long ago. It all started in mid may.
- Law enforcement requieres solid proof to take any action. I don't have enough (IPs that may be behind a VPN, fake social network profiles that get banned...). I contacted lawyers and computer science judicial experts to no avail, former can't do anything and later are dubious even about their success...

- Regarding the reset, it would only get rid of one partition, and there is malware capable of installing itself in /system, so I'm digging on how to get rid of it all, it just in case.

So far I can't (or I don't know how) remove the partition tables and redo everything, which I guess would be the wisest option. Is it even possible? the most similar approach is to install another ROM.

(Sep 12, 2019 10:33 AM)deadshort Wrote: [\[CITE\]](#) If you've got someone who's willing to root your phone, take down your router, and move laterally inside your wifi, I hate to say it but there's not a lot you can do. Maybe talk to your ISP. Once they start pivoting, eventually they get so deep that they can override or replace any action you cause. Swapping out antiviruses, disabling firewalls, all that. A targeted APT threat is for all intents and purposes impossible to stop.

Thank you for putting it like that. My ISP installs routers with 1234 username & password and remote access on, so I am not sure they will be of great help, but I may try.

I am afraid that my chances to sniff traffic and getting some results are quite low, specially knowing nothing at all, but any idea on how to reduce risks or make it more boring for them (e.g delete whatsapp messages) would be appreciated.

Thank you guys for your understanding

SIM-4294714 - September 13, 2019, 10:51 am

(Sep 13, 2019 10:04 AM)Goingby Wrote: [\[CITE\]](#) - Password wasn't that strong and I didn't have 2fa on previously, despite that, it is not through brute force they've got inside, otherwise I would have notifications or a different password. I changed password from another device immediately and activated 2fa.

- I haven't clicked any phishing url/email - or so I think.
- Apps downloaded only through playstore, 3rd party apps have always been deactivated. No porn/hack/stupid apps, just common ones and language learning ones. Nothing suspicious. I am neither giving permissions blindly when installing apps.

On the other hand, PC does have some cracked soft, but all this started through the phone, by people I know with a concrete purpose of harming me. Now I run a clean system with a different OS, same hardware and router though...

- Non rooted phone, no virus/malware found. It's an Android 9, currently PKQ1.180904.001 but there was a security update no long ago. It all started in mid may.
- Law enforcement requieres solid proof to take any action. I don't have enough (IPs that may be behind a VPN, fake social network profiles that get banned...). I contacted lawyers and computer science judicial experts to no avail, former can't do anything and later are dubious even about their success...

- Regarding the reset, it would only get rid of one partition, and there is malware capable of installing itself in /system, so I'm digging on how to get rid of it all, it just in case.

So far I can't (or I don't know how) remove the partition tables and redo everything, which I guess would be the wisest option. Is it even possible? the most similar approach is to install another ROM.

Thank you for putting it like that. My ISP installs routers with 1234 username & password and remote access on, so I am not sure they will be of great help, but I may try.

I am afraid that my chances to sniff traffic and getting some results are quite low, specially knowing nothing at all, but any idea on how to reduce risks or make it more boring for them (e.g delete whatsapp messages) would be appreciated.

Thank you guys for your understanding
Forget to pay your electrical, phone, and internet bill for a month or two and see what happens ;) They can't stop that one.
Don't actually do that, but seriously consider unplugging everything that can talk to the outside world. Format anything unimportant.

CyberStrike - September 13, 2019, 3:24 pm

(Sep 13, 2019 10:04 AM)Goingby Wrote: [\[CITE\]](#) - Password wasn't that strong and I didn't have 2fa on previously, despite that, it is not through brute force they've got inside, otherwise I would have notifications or a different password. I changed password from another device immediately and activated 2fa.

- I haven't clicked any phishing url/email - or so I think.
- Apps downloaded only through playstore, 3rd party apps have always been deactivated. No porn/hack/stupid apps, just common ones and language learning ones. Nothing suspicious. I am neither giving permissions blindly when installing apps.

On the other hand, PC does have some cracked soft, but all this started through the phone, by people I know with a concrete purpose of harming me. Now I run a clean system with a different OS, same hardware and router though...

- Non rooted phone, no virus/malware found. It's an Android 9, currently PKQ1.180904.001 but there was a security update no long ago. It all started in mid may.
- Law enforcement requieres solid proof to take any action. I don't have enough (IPs that may be behind a VPN, fake social network profiles that get banned...). I contacted lawyers and computer science judicial experts to no avail, former can't do anything and later are dubious even about their success...

- Regarding the reset, it would only get rid of one partition, and there is malware capable of installing itself in /system, so I'm digging on how to get rid of it all, it just in case.

So far I can't (or I don't know how) remove the partition tables and redo everything, which I guess would be the wisest option. Is it even possible? the most similar approach is to install another ROM.

Thank you for putting it like that. My ISP installs routers with 1234 username & password and remote access on, so I am not sure they will be of great help, but I may try.

I am afraid that my chances to sniff traffic and getting some results are quite low, specially knowing nothing at all, but any idea on how to reduce risks or make it more boring for them (e.g delete whatsapp messages) would be appreciated.

Thank you guys for your understanding
So a simple password and if anyone is a customer of your ISP and has a couple of braincells they will know that remote access is on with a simple password. God damnit... don't worry this is actually

semi normal with ISP's and taking shit seriously. (I am sure that I will get some angry PM from someone who works at an ISP.) We don't know if really it started at the phone, evidence speaks for itself, some malicious people out there can stay pretty quite for weeks, months or years.

I will post with a RAM dumping utility for the PC and I think using ADB we can snapshot the RAM on the phone. I would at the very least disconnect from the internet when you are ready to do this, if you are willing to. I'd have to analyze the RAM dump from the PC during my weekend. (Currently rushing to get ready and get to work)

(Sep 13, 2019 10:51 AM)deadshort Wrote: [\[CITE\]](#) Forget to pay your electrical, phone, and internet bill for a month or two and see what happens ;) They can't stop that one.

Don't actually do that, but seriously consider unplugging everything that can talk to the outside world. Format anything unimportant.

The computer would be something I would want to do memory forensics on.

Goingby - September 15, 2019, 6:15 am

(Sep 13, 2019 03:24 PM)CyberStrike Wrote: [\[CITE\]](#) So a simple password and if anyone is a customer of your ISP and has a couple of braincells they will know that remote access is on with a simple password. God damnit... don't worry this is actually semi normal with ISP's and taking Clay Davis seriously. (I am sure that I will get some angry PM from someone who works at an ISP.) We don't know if really it started at the phone, evidence speaks for itself, some malicious people out there can stay pretty quite for weeks, months or years.

I will post with a RAM dumping utility for the PC and I think using ADB we can snapshot the RAM on the phone. I would at the very least disconnect from the internet when you are ready to do this, if you are willing to. I'd have to analyze the RAM dump from the PC during my weekend. (Currently rushing to get ready and get to work)

The computer would be something I would want to do memory forensics on.
Thank you CyberStrike, I didn't know about that.

I am already reading some info on how to use Android Debugging Bridge and the dev tools, but I still lack info on how to do the ram dump and analyze it. I'll look further for more info.

Regards!

CyberStrike - September 15, 2019, 7:04 am

(Sep 15, 2019 06:15 AM)Goingby Wrote: [\[CITE\]](#) Thank you CyberStrike, I didn't know about that.

I am already reading some info on how to use Android Debugging Bridge and the dev tools, but I still lack info on how to do the ram dump and analyze it. I'll look further for more info.

Regards!

Sorry always busy I should have responded earlier I apologize. In Windows simple tools work personally I used the following tool it's free

<https://belkasoft.com/ram-capturer>

As for analysis I use Volatility, which is also free

<https://github.com/volatilityfoundation/volatility>

If you are comfortable I'd be happy to analyze the Windows RAM dump, if malware is found I may have to rebuild a few things on the files but if successful I can do malware analysis on any malware and I will PM you. (I used to do forensics challenges in certain sections and have not done one for a while) The only bad thing is that it might take me a week from today before I can really delve into the dump. BTW I don't charge or any of that crap, in case you are wondering.

Of course if you are not comfortable with such a thing, read up the wiki on the link above for volatility and I will post more links tomorrow on forensics and on malware analysis. Even something simple as say app.any.run (an online malware analysis platform) will give you an idea of where this crap was installed, what registry keys, any scheduled tasks or any further downloads. This can all be used to manually start removing this crap from your computer.

I have not done Android forensics so I am not too sure on how I would fair in that arena, perhaps another user might be good enough to help with that. (Hint hint if you're good with Android forensics give a hand)

Goingby - September 16, 2019, 5:09 am

Please don't apologize, it is me who is grateful! I wouldn't manage to do or get to know much of this stuff unless I had found people like you in the first place.

Regarding the RAM dump, I really appreciate your help but if you don't mind, I would like to start analyzing it myself, reading all the documentation I can and evaluating the risks at stake. My situation is not easy and I wouldn't want to expose myself further performing some actions blindly. I hope you understand it.

I don't know how far I will be able to go with this, but it is an interesting field and useful knowledge that may be handy in the future as well. I am going to check those tools, and see how to put that into practice, thank you!

CyberStrike - September 16, 2019, 6:51 am

(Sep 16, 2019 05:09 AM)Goingby Wrote: [\[CITE\]](#) Please don't apologize, it is me who is grateful! I wouldn't manage to do or get to know much of this stuff unless I had found people like you in the first place.

Regarding the RAM dump, I really appreciate your help but if you don't mind, I would like to start analyzing it myself, reading all the documentation I can and evaluating the risks at stake. My situation is not easy and I wouldn't want to expose myself further performing some actions blindly. I hope you understand it.

I don't know how far I will be able to go with this, but it is an interesting field and useful knowledge that may be handy in the future as well. I am going to check those tools, and see how to put that into practice, thank you!

No worries, I think you will learn a great deal doing it yourself. If you can check out The Art of Memory Forensics, it is really a good book. There are a few articles which I will link I will try to keep them beginner friendly.

<https://www.forensicmag.com/article/2011/06/memory-forensics-where-start>
<https://medium.com/@zemelusa/first-steps-to-volatile-memory-analysis-dcbd4d2d56a1>

I would link the following but it's a PDF and generally I am uncomfortable with linking PDFs

(Free really good 147 page tutorial kind of very good though)
Windows Memory Forensics with Volatility Andreas Schuster

Edit: Let me know if you need any help these tutorials cover a lot of the methodology and remember that you might be dealing with malware at some point, so using a Virtual Machine (VM) is a must also disable sharing when you run into crapware.

Goingby - September 16, 2019, 2:50 pm

Wow! thank you so much! those articles are easy to approach and the 147 pages is also manageable, so I am sure I will get some interesting knowledge out of it. I've also access to the book already, and it looks like it is going to be deeper.

I am glad to count with your advice, thanks! lets see if I can achieve some results)

chant - September 19, 2019, 12:48 pm

(Sep 15, 2019 07:04 AM)CyberStrike Wrote: [\[CITE\]](#) If you are comfortable I'd be happy to analyze the Windows RAM dump, if malware is found I may have to rebuild a few things on the files but if successful I can do malware analysis on any malware and I will PM you. (I used to do forensics challenges in certain sections and have not done one for a awhile) The only bad thing is that it might take me a week from today before I can really delve into the dump. BTW I don't charge or any of that crap, in case you are wondering.

Can you do this for me as well?

CyberStrike - September 19, 2019, 2:30 pm

(Sep 19, 2019 12:48 PM)chant Wrote: [\[CITE\]](#) Can you do this for me as well?

Right now I can't for the next week at least my life is truly busy busy busy. It'll be about 2 - 3 weeks before I have a day off from work. If you want pm me and I will get to it when I do.

chant - September 19, 2019, 3:39 pm

(Sep 19, 2019 02:30 PM)CyberStrike Wrote: [\[CITE\]](#) Right now I can't for the next week at least my life is truly busy busy busy. It'll be about 2 - 3 weeks before I have a day off from work. If you want pm me and I will get to it when I do.

I haven't posted enough to send PMs so PM me when you're ready. Thanks