Corellium

Video Webinar

Episode 6: Mobile Malware & Threat Research Without Limits

Full Transcript

(00:00:09)
Brian Robison: Good morning, good afternoon, everybody. Thank you very, very much for taking the time out of your day to join us today, or I should say me. I'm flying solo on today's webinar. For those of you who've been with us for the past few months, I've had one of our researchers on with me doing a lot of the cool demos and things around pen testing, but today you're just stuck with me. So I do appreciate all of you coming in. There's quite a few of you in the attendee area and I really, really appreciate taking the time out of your day to come in and talk about mobile malware and threat research. So that's really what we're going to do today. I actually had quite a bit of fun developing this content and playing with malware. It's always fun to play with dangerous types of stuff and see just how crazy some of these things are or how good some of the social engineering is.

(00:01:11)
And if any of you have followed me over the past few years with my work back at Silence using the Hacking Exposed and building malware demos and things like that, those were a lot of fun times. So doing this on the mobile side is interesting as well, and some of it might be a little spooky, but we'll see how things go. Please realize that today's demos are live. I'm actually using real malware on our virtual phones, and so the chances sometimes with real malware is you might see something that might be objectionable or offensive. And I promise you if something like that does happen, I will do what I can to get it off the screen as quickly as possible. But please realize that we are dealing with live types of things and some things may work, some things may not be as good, but we're going to do what we can.

(00:02:11)
And as I said, if we see something horrible, then I'm going to do what I can to get it off the screen as quickly as possible. So bear with me and thank you very much for joining and I really appreciate taking the time. So hopefully you've got some coffee or a cold drink or whatever and we can go ahead and get started. Just a little bit of housekeeping before we do get started into the main content. All attendees are in muted mode. This is a webinar format versus a meeting format. I sure wish that I could do more personal meetings with all of you, but with so many different people on the line, it's difficult and we want to keep the background noise to a

minimum. So please bear with us on that. We do want you to engage though, I want you to use the Q&A tab if you can, to ask me questions.

(00:03:04)
I will try to get to them as I see them on the screen while I'm doing demos and screen sharing and things. I might not be able to see some things, but we will definitely try to get your questions answered. If not, don't worry about it. If you ask a question and I don't get to it live, I will follow up with you individually. They're all recorded as part of the recording. And speaking of that, this video or this webinar is being recorded, so we will make it available on demand very shortly afterwards for you to share with your teams or review some other things in more detail. And as I said before, the presentation does kind of consist of live demos and some slides with live demos. So basically we're going to talk about certain things, talk about what's important about this malware or something for example, and then we're going to look at it.

(00:03:59)
Questions came in. Great, thank you very much. Are we going to be talking about both iOS and Android today? It's going to kind of be mainly Android. I do have some iOS stuff I want to show, but most of the really meaty stuff currently is on Android. But I plan on doing a follow-up, a Part Two webinar to this where I want to focus more in depth on iOS malware. It's just going to take me some more time to do some research I had kind of as a stretch goal. I have one kind of malware for iOS and maybe we'll launch it if we have some spare time, but I haven't been able to have enough time essentially to kind of research it and see what's really cool about it beyond it just being some information stealer and that kind of thing. So do look forward to a follow-up webinar on iOS and maybe even involving a third party threat researcher team and things like that that want to come in and help present.

(00:05:08)
So, OK, so I will plug one more time. I'm going to take this out of the webinar next month, I promise you, but we do have a contributor program. So if you are interested in writing content for Corellium, making a little bit of money on the side, we have this program available. A few weeks ago, we actually did publish our very first community-contributed blog and we have a pretty good stack of them coming up right behind that one. So we are paying these contributors to write blogs, and it doesn't necessarily have to be about using Corellium or how Corellium works for you, things like that. It could be more mobile security related, vulnerability research related, malware threat research related, all those kinds of things. I'm looking for content in all of that. So if you just go to our website and fill out the form, it comes to me, I'll reach back out to you and start talking with you about what kind of content you'd like to contribute.

(00:06:06)
So it's a good way to get your name out there as a thought leader, a researcher, what have you. We link back to your site or your business or your posts as well in that same content. So it's kind of a nice dual kind of thing. So just very quickly for the folks that may not be too familiar with what Corellium is and how we're different from other platforms, I just want to go through a few

slides before we go ahead and get started. And one of the things that I always talk about is why is mobile security research so difficult? It's difficult to do because of the form factors and how the operating systems are designed and things like that, but it really comes down to getting your hands on the proper devices, getting access to them, physical or emulation or simulation or whatever that you're trying to do.

(00:07:01)
So gaining access to these devices. We spend a lot of time in the past dumpster diving for older devices that haven't been updated and things like that. And really it's because we need very specific operating systems. And what do I mean by that? Well, I mean that we need operating systems that we can successfully jailbreak as an example on iOS or root on Android, but we need these operating systems because the public tools that are out there today rely on a vulnerability to exploit to actually do the jailbreak. And so that's why we're looking for some of these older devices and older operating systems. And then there's the time that we spend managing all of these types of things. So just like 20-plus years ago when we used to have large quantities of little cheap desktops in a lab when we were doing Wintel malware research and running around to each of those machines and restoring them with Symantec Ghost every time you ran some malware and corrupted the system with a crash cart and get a plug a screen and a keyboard in and then boot up off a CD and restore 'em.

(00:08:11)
Those things take a lot of time and we're faced with the same kind of thing on the mobile security side. So yeah, even if you got all the devices you need and all the operating systems you need, you're still going to be rebooting these things. You're still going to be potentially even re-flashing them. You're going to be re-jailbreaking them, you're going to be redoing a lot of work that just basically just takes a lot of time away from what you're supposed to be doing, which is the security research element. So what we have done with Corellium is essentially we have brought the power and the efficiency of true virtualization to the mobile space. And what I mean by that is very to what we did back in the Wintel and x86 platform when VMware came out, we were now able to stack 20 or 30 virtual machines on a physical server and have the time savings ability of restoring from snapshots and things like that to get back to those clean systems rather than having to re-image or go through an entire Ghost re-imaging process, all those kinds of things.

(00:09:23)
And we could do it remotely, we could do it through a web browser and a virtual console and things like that. So what Corellium has done is essentially kind of done that, but for the Arm-based devices that are out there, not x86. So we are true virtualization. We are basically the same as a VMware ESXI where we're a bare metal hypervisor that runs directly on an Arm server or in the cloud in the AWS Graviton Arm servers. And basically we run virtual machines. And today those virtual machines can be iOS and Android. They can also be other types of virtual machines based on Arm platforms like Raspberry Pi, Cortex processor, Cortex platforms,

things like that that are built based upon the Arm technology. So that's just a very, very quick overview of what we do and what we're all about. We are true virtualization.

(00:10:22)
We are not emulation, we are not simulation. We are actually running iOS directly on Arm-based hardware. Great question just came in. Does Corellium require an OS vulnerability to perform? Absolutely not. What's interesting about what we do, because we are virtualization, we actually can control the boot process. And so if you choose an iOS version to be jailbroken, we can do that all the way up to the latest and greatest iPhone 14 Pro Max on 16.3 or 16.4. It's already done for you. It's basically a perfect jailbreak. You don't have to hold down any sort of buttons and hope that your car's got the right color and the moon alignment is correct. There's basically none of that and that is one of the huge time savings is being able to access the devices that you need. Maybe it's a 14 Pro Max or maybe it's an iPhone 7 or something like that, but you'll be able to access any version of iOS all the way up to the latest and greatest and have it jailbroken at the same time.

(00:11:32)
It's just not something that you're going to see out there, not in the physical world and not in the virtual and not in the simulated world either. So it's basically a unique situation that occurs. Okay, so let's go ahead and get into today's content. We've got about 45 minutes or so left, and I want to make sure we get through this. I've got about five or six different demonstrations that I'd like to go through today. And so we're going to talk a little bit about malware upfront. And this is where again, we're going to kind of focus on Android. We're going to look at some malware statistics or some notes, and then we're going to look at the actual malware. So we're going to kind of bounce back and forth between slides and demo so we're not just spending all day in slides on the malware side.

(00:12:25)
We're going to look at, we're going to go from the simplest, most common to some of the more complex, where we're looking at just some kind of generic adware and looking at things like that. We're going to look at some ransomware, we're going to look at some Trojans and remote access, Trojan things, info stealers. Some of these are pretty darn complex and what they can actually do is quite scary. So let's just go ahead and get started. We are going to start today by just kind of understanding that these threats are actually real. So this was written very, very recently and in fact this is one of the samples that we're going to look at today, but it's just a pretty prevalent type of thing that just happens kind of all the time and it's not something that slows down, but it actually kind of is accelerating.

(00:13:30)
And the capabilities that are in some of these new malware like the Xenomorph there with the ATS system, this is a sample of malware that is able to basically log into your bank with your credentials or your banking app, initiate a fund transfer, automatically deal with the multifactor authentication of that transfer request and complete the funds transfer without any human

interaction. And that's kind of freaking scary when you look at this. So we're going to take a look at some of these things, but I just wanted to kind of point out here that if you hit, and these are all just screenshots off of BleepingComputer.com. If you go to BleepingComputer every day, you're going to see pretty much there's going to be something about mobile threats nearly every single day. And again, just because I have all these shots here of Android, it's not necessarily all Android, but it is definitely a significant portion of the malware market.

(00:14:37)
Now, that doesn't mean, and we're going to talk about in that other webinar, we're going to talk about smishing and phishing attacks and things like that that are cross platform, but at least on the malware side, the actual runnable code is really what the attackers are really targeting the Android side. So let's begin with CamScanner. Now this is an oldie but a goodie. I like this one because of its scale. So this basically was a legitimate app on the Google Play Store. It's an app that if you're kind of familiar with this, it's a business type app where you can scan a receipt and it turns it into a black and white picture, PDF, or it also has optical character recognition capabilities to convert photos into text and things like that. It's a good app and it was installed hundreds of millions of times. And what happened is a version of this was released with a malicious ad library.

(00:15:48)
So the vendor of this offered the app for free. They used ads in the application to monetize some of the stuff if you didn't sign up for their account. And there was a version released that basically had this malicious ad library installed. There were also other apps that had the same kind of malicious advertisement library installed that were even pre-installed on Chinese smartphones. And really what this is, it is a Dropper. So it basically will run just fine and it downloads malicious code or executes other malicious code out of an encrypted payload that it contains and things like that. And really what the users noticed with this is that the ads were extremely intrusive. They were constantly there and they basically were getting signed up for subscriptions for other things in these ads that they didn't know about. So phones get hot because these things get, basically these apps are clicking on ads in the background generating revenue for the ads framework. So CamScanner is fun, but like I said, it's an old one. But what I like doing with CamScanner is actually taking a look at and using the Corellium platform to take a look and see what is going on in the background. And I'm not sure why these devices got turned off, but let me get these things turned back on.

(00:17:19)
So while this phone boots up here fairly quickly, I'll just kind of go through the platform a little bit. So this is basically the Corellium platform and you've got access to your VMs here and I've got my Android phone running here and I can do fun things with it both interactively with my mouse. The cool thing is I can use my physical keyboard, so that's kind of a nice thing. And then I've got things like that, but I can also interact with these devices via API and CLI. A question came in: are Play services present in Corellium for Android? No, they are not built in, but you can install them in the app side loader here. You can actually install the open GApps if you need access to

Play services, then you can actually sign in some of the devices. I actually have done that we're going to take a look at today.

(00:18:15)
So good question. Thank you very much. I appreciate that. Okay, so devices booted up and what we're going to do is we're going to use our Network Monitor, which is essentially our network sniffer, and I've got a copy of CamScanner here. And the interesting thing that we're going to do is we're going to basically show how I can use Network Monitor to sniff out some kind of C2 traffic, if you will, that the app uses. So this is the actual malicious version of CamScanner and it has in it the vulnerable library and the vendor knows about this. So when this app launches, it's going to check with its command and control and it's going to basically tell us that we need to update because there's a bad thing in this application. So we're going to use Network Monitor actually to sniff that out. So as we launch this app, you're going to see all this kind of network traffic go bouncing down through and begin to get logged over here.

(00:19:23)
Now, even before we get all the way into the application, we can use this Network Monitor to see this traffic to this server right here. And this is kind of the backend C2 if you will, but if this were something malicious, this could be the server that's actually doing something bad, but we can basically see that we sent a request or the app sent a request and it got a response back. And again here you can see everything in clear text because we are already stripping out all of the SSL and TLS in the network communication. But you can see here that there's going to be, hopefully at some point, there's going to be a dialogue box that's going to pop up and say that there's a new version available and we fixed an issue that may cause advertising fraud in the current version that you're using and that they strongly recommend that we update.

(00:20:15)
So we see this traffic coming in, but we don't see that dialogue box over here in the app itself. So we actually have to kind of go through the app, we go through its setup wizard and we click use now, and then we actually get the dialogue box that pops up where we actually saw the code come in through the network scanner. So this is a good example of using the built-in Network Monitor tools if you're trying to gather information about the communication that the app is doing as it's running and actually executing code. The other things you can do here, I mean the data URLs, is actually downloading imagery and things like that into the application when it first launches. And again, we can show that to you in clear text here and make it easily understood. All right, so we've got a lot of questions coming in here.

(00:21:11)
So is there a way to simulate an internet connection to prevent malware from connecting? So yes, in Corellium you can actually turn off internet access, but the devices still have IPs and things like that. So you can do that where basically the app isn't being allowed to communicate to its C2, but you're going to see all the posts and the requests and things like that that's going to happen. So that's a good thing. Does it work with certificate pinning? Yes, we do have ways

of disabling and bypassing certificate pinning both on Android and iOS. And the last one, is it possible to send the traffic to Burp Suite? Absolutely it is, and we're actually going to take a look at that here in a few minutes. So Burp Suite is going to be one of the demonstrations that you're going to see today.

(00:22:02)
So I'll show you guys how to do that. And I'm not sure why this device is powering off, but at least we're done with this one. And I'm just going to go ahead and restore it from a snapshot. So this is probably the most valuable feature in my opinion because we've actually run that software on the device. The device is essentially corrupted. So if I were a physical device, I would have to potentially delete and restore and let it do all of its kind of thing and then do whatever I need to do to get it back up and running. However, in this world, I can just click 'Restore' and it's going to restore a snapshot that I took and restore the device basically back to its clean and working state.

(00:22:48)
Is there a snapshot-diff feature in the making? Not really. We don't really show the differences between the snapshots, but one of the things that I do is obviously I name my snapshots certain things so that I know what state that device was in when I took that snapshot. So that is the very first one. We looked at CamScanner, we gathered some traffic, and that's kind of a cool thing, but it's very basic and I just wanted to show and highlight some of the things that we can do when you're doing dynamic malware analysis. You obviously want to sniff the traffic, and then we're going to show you more advanced traffic redirection and sniffing here in a little bit. Okay, let's move to Black Rose Lucy. Now this is an interesting one because this is categorized as ransomware. And the interesting thing on Android is most of the ransomware up to, oh, let's say mid 2020 or so was really just extortion, meaning it really just threw up a fake overlay image or webpage or whatever, but it didn't really do anything behind the scenes.

(00:24:07)
And the reason that Black Rose Lucy is interesting to me when it came back in mid-2020 and 2021 is because now it actually encrypts files, which is an interesting twist. So it mimicked a lot of the fake FBI…this one has an interesting sextortion twist. We'll show it to you here in a minute, but it actually encrypts files and we're going to use some of the tooling that is available within the Corellium platform to actually show that happening and what is actually happening to the file system itself. So yeah, Check Point originally tracked this group, the Lucy Gang, which is a MaaS, and I'm not sure if you're familiar with that or not, but this is a malware-as-a-service. So again, if you're kind of familiar with me and you followed me, we used to do a lot of malware as a service demonstrations back in the Silence days because these organizations exist to enable their customers, essentially these attackers to go do bad things on behalf of them.

(00:25:09)
And usually it's kind of like an App Store concept. They'll take 20 percent of the ransomware payments and send 80 percent to you, or some of them make you pay upfront and then you get

all the ransom payments, things like that. It's an interesting concept and storyline, but this one became active in 2020 and 2021. And you're going to see in all of these malware, really it is exploiting the Android accessibility service beyond exploiting the user, social engineering the user, to actually install payloads and do things without any user interaction. This one has a fake ransom note, which is kind of cool if we do ransomware research on Wintel platforms. We all love to see the popups and see all of that kind of thing happen on the screen. Okay, so let's take a look at Lucy. Alright, so here I have basically a clean Android 9 device and I have this built-in file browser, which is really, really cool because I can browse in and see all of my operating system and anything I want in it.

(00:26:25)
I can go into my downloads on my SD card and I can see that I have a TextFile here. Now, this TextFile, I can actually view the contents or I can download it, but I'll just go ahead and view the contents. And you can see it's just a dummy TextFile. There's nothing meaty in here, but it basically just represents some local storage, some local data that I have stored in my Android device. So now what we're going to do is we're actually going to install Lucy and Lucy is, let's see, you see here, I have all kinds of fun things to play with, but Lucy basically purports itself as a video play library. And when you install Lucy, you'll see here that this is actually Black Rose Lucy. And so I'll go ahead and execute it, but I want to come back here and we can watch this TextFile here.

(00:27:25)
So when I execute Black Rose Lucy, it's going to tell me that I need to enable the service. So it's going to say, OK, you need to enable this service, but if I just kind of click OK, the app actually goes away and I need to actually enable this service, and you'll notice it's in the accessibility portion of the Android device. Now, some people don't spend a lot of time reading, they're really convinced that they just need to turn these things on and use them, but if you just look at this one, “Android optimization must be enable for play video on your phone.” It just doesn't sound right either, but they needed to have something here. And if they put so much here, the most common button that users click on is next, next, next, next, next. If they're convinced that they really need this streaming optimization service so they can play videos on their phone, they're not even going to look at this, they're just going to check use service.

(00:28:29)
And then here at the end it just says “some additional benefits include” and then just trails off to nothing. How did this actually get installed on anybody's phone if you even just barely look at this? But the social engineering aspect of it overcomes a lot of the common sense that people have. So we click use service. Now, once I do this, I'm going to take my hands off of the keyboard and mouse because this is where it takes over and does things all by itself. So we're going to use the service. And then here is where Andrea will normally tell you what services it's going to be using and what permissions to your device that it needs. As you can see here, there's nothing on this screen. However, if you scroll down, you swipe up, basically, you're then going to see, oh, it's going to do all of these kinds of things.

(00:29:19)
You're going to give it permission to observe your actions. You're going to give it the ability to take screenshots and things like that and actually perform gestures on your behalf, which is interesting. But again, the social engineering aspect of it, oh, there's nothing here. So the user simply clicks, OK—now this is when I'll click, OK. I'll take my hands off. And you'll basically see the application start giving itself all the permissions and turning on all the settings that it needs to actually begin what it's going to be doing and begin working. And there is our traditional ransomware popup that says, “Hey, we've scanned your device and found pornographic imagery” and things like that, and you need to go to one of these stores over here. We're going to go to Dollar General and we're going to buy a gift card, a Visa gift card, because that's how the FBI wants to get paid.

(00:30:18)
Obviously not something that's legit. Now, however, if you look over here at this file, this file now has a new extension on it, and if I try to view the contents, I get an error because the file is no longer a TextFile, so I'm going to have to download it and I'll pop it up in TextEdit, and you'll be able to basically see here, this is the actual file. Now it has actually been encrypted and this is what Black Rose Lucy is doing. That's different from some of the other ransomware that is out there and causing havoc with just these kind of fake pop ups. And hopefully somebody will pay it. It's actually getting in and tweaking with files. Once again, restore our snapshot so we can go back and play with it at a later date. So that's Black Rose Lucy. Let's standby one second. Got my windows out of order. Let's see, we've got lots of questions.

(00:31:27)
Sometimes we have to use VPN due to customer whitelisting. How do you combine this VPN? We're going to talk about that in a minute. So hang on about the double VPNing, I'll show that in a second. Will Network Monitor feature work for non-proxy-aware applications. So Network Monitor is under some interesting development right now to turn it more into a true Wireshark type sniffer because we have access to the device at the network stack, we're actually able to see that versus what you can do with Burp Suite and proxying. So we're working on that now. So look for Network Monitor to get pretty boosted here in the very near future. Where do I get the samples? There's a couple of these things. Really when you read the reports that are out there, usually there'll be IOCs, there'll be hashes of the files. I download them from my VirusTotal Intelligence account that I have.

(00:32:28)
But yeah, that's basically where you can source malware. I mean so far I have been able to download every single example I have directly from VirusTotal. So you need to know the hash of the file to get the exact one, and sometimes there'll be lots and lots of variants. So it does take a lot of research and time to figure out variants that work properly and all those kinds of things, but definitely fun stuff to play with. So good questions about gaining access to these fun APKs and things like that. We'll get onto the VPN in just a minute. Can we attach peripherals such as

external fingerprints, scanners to Corellium? Possibly yes and no. In the iOS world, we actually create, with our USBFlux application, we actually create a USB connection to the device so that it looks, even if it's running in the Cloud or somewhere else, as if it were physically connected to our local machine, but that doesn't necessarily make peripherals available to the devices at this time.

(00:33:37)
Most people interested in doing that can actually add to the VM itself and build virtual modeling and add additional peripherals. But if you're interested in that, we can definitely have a conversation about that. Okay, let's get a little more interesting. SOVA is another malware group that is out there, and these are kind of the more common thing that we're beginning to see a lot more of now, which are the banking Trojans. Can I gain access to your financial information? And can I steal that information from you, can I steal money from you? Why would I want you to voluntarily pay a ransom when I can steal all your Bitcoin wallet or something like that? So this is relatively new.

(00:34:27)
It was interesting because when this one was published first in September of 2021, the threat actor actually published a roadmap of all the features they were going to be adding. So they actually did multiple releases throughout 2022 and added these features that were on their website that listed out these things like two-factor interception, cookie stealing, injecting of new banking targets, things like that. A big update happened in July last year with v4 that targeted greater than 200 mobile banking and crypto apps. This is kind of interesting. And then in November, v5 came out that changed a bunch of how the thing worked, a bunch of code refactoring. So this is still a very active developing malware for Android, which is designed to basically steal money from you. This one is kind of interesting because it's designed to hide in plain sight.

(00:35:27)
So they use icons and names. It looks like the Amazon app or it looks like the Chrome app or NFT, things like that. And beyond doing VNC connections to your mobile device, which is interesting, it's kind of a remote access Trojan as well, but it can obtain screenshots, record sensitive information using these accessibility services. So I really advise you be very, very, very, very careful about what has access to your devices' accessibility services because there is a full capability of essentially like you saw before, the app is actually making swipes and gestures and asking for permissions and doing things on behalf of you without any interaction. And that can be really, really dangerous.

(00:36:17)
And they also added the ability to steal information from Google Services. So your username passwords, your Gmail, getting into GPay, Password Manager. This is really interesting, and v5 did add a ransomware module and I don't think the sample of v5 that I have. Actually, I haven't been able to get it to actually do the ransom portion of it, but the interesting self-protection

mechanisms and things are there, which are interesting as well. Okay, so let's take a look at SOVA. We have a question pop in here. Yeah, so somebody else looked at SOVA as well and accessibility services is an interesting surface. Yep, good comment. It absolutely is because once you give it access into accessibility—wow, the stuff that these apps can actually do. Alright, so SOVA again here. So I've got this one again, it's the same 9.0, but as I said before, we can add Play Store and things like that when you open the GApp. So I can do things like install NOVA and get a better launcher. I can install Google Play apps where I get Google Earth and things like that. We're going to use some of these things here in a few minutes. So let's go ahead and install. I think the version of SOVA that I have mimics Chrome.

(00:38:01):
Yeah, so this is Sova v5 and you launch it and it's going to say, Hey, you need to update some access for Chrome. So you can click activate and it takes you in once again into accessibility. And here it's basically asking over and over again until I do it. So we turn on the service, this one does say, oh, it needs these things, but hey, it's Chrome, right? So I trust it. And then again, you can take your hands off the keyboard and the app is going to start plugging away and doing interesting things, giving itself deeper access. And this is where some of the ransomware modules and things like that would kick in if this sample was actually able to communicate with a live Command and Control. I think on this one, the command and control is essentially down, but it's still going. It's still giving itself all the permissions and things that it needs.

(00:39:17):
So I think this one has a very similar self-protection mechanism. So if I try to uninstall it, I do a long press on the app itself and it automatically sees that and swipes it away before I can actually click the uninstall. And that's a newer-ish mechanism that a lot of the malware is using now to basically keep itself running. And we'll take a look at that with another sample of malware as well. But it is a very interesting mechanism of self-protection, and that's what I wanted to show with SOVA v5 is this newer protection mechanism that it's using to essentially keep itself running no matter what you as a user do. Now the interesting thing is because of our app side loader here, and obviously com.bean.cousin is not the name of Chrome, the app name, but I can, because our app manager here that we have built into Corellium, I can actually kill the app and I can actually uninstall it from outside of the device. And actually on this one I did get a failure because of the Device Policy Manager. So it's making changes to even where even through ADB, I mean not able to really uninstall this application. And so again, those self-protection mechanisms are very, very, very interesting in how they are actually functioning. Once again, snapshot restore, my device will come back in a nice clean state so I don't have to worry about it anymore. So that is SOVA. SOVA is fun.

(00:41:16)
Okay, now this one is like SOVA on steroids. This one is one that is, again, it's being actively developed. Its first couple of test distributions came late last year, but this one was written about just a week or two ago. And again, this one is an interesting one because of how its threat actors are using these short and very, very contained distribution mechanisms. Essentially it's

indicative of a testing program. So they're going to release this into really tiny places with very, very focused actions to see how it does. The really bad thing about this one is the automated transfer system. So this has a version in it. Again, this is using the accessibility services where they're able to actually do gestures, capture information even from authentication apps, third party authentication apps like Google Authenticator or Microsoft Authenticator. They're actually able to obtain the MFA tokens from those applications in clear text and actually use that so they're able to complete fraudulent transactions automatically extracting.

(00:42:38)
So this is if you have this installed along with one of these more than 400 different banking apps on your device, basically it can extract the credentials from those apps. It can get your account balances, initiate a transaction, obtain the MFA token from a third party authenticator app if you have that on there. Again, it's something I've always talked about. Why do we have our authenticator apps on the same device that we have our app that we're trying to authenticate, but that's a personal issue and it's basically able to do that MFA token push, finalize the fund transfer, and it can do all of this without any human interaction. And yeah, that's dangerous in my opinion. The latest version of this that came out in March upped the ante with the a TS system as well as now it has over 400 different banking and financial institution and crypto wallet capabilities.

(00:43:43)
So if you have a crypto app on your device, this app is actually able to see that. The interesting thing is that they bound it to a legitimate currency converter called CoinCalc. And then what CoinCalc does is basically acts as the dropper and it downloads and installs this fake Google Protect app. So it's Google Protect, why shouldn't I install that and have that running on my phone? That sounds like a good thing to do. So let's take a look at Xenomorph and Zombinder. So Zombinder was the name of the test deploy, and again, we're just going to install Zombinder. Okay, here's CoinCalc.

(00:44:44)
So we're going to install CoinCalc on the device, and here's CoinCalc, which is truly a legitimate application. It's a currency converter. We click on it and then what happens is the fake Google Play app is inside of this application and gets extracted and then becomes installed. So they are using this terms of use, this app requires a plugin app to be installed. This is how they're using their social engineering to get in here. So you have to go to settings and enable the toggle button. They don't say what toggle button, but just a toggle button. So the toggle button when we go into settings is to install an unknown app from CoinCalc. So the app CoinCalc is actually trying to install another app. And again, this is going to come up until you do it. So yes, we'll allow CoinCalc to install an app. Oh, it's Play Protect. I know what that is. So we'll choose to install it.

(00:45:59)

The app is installed and you can basically start seeing here the app's installing like, wait a minute, we need to enable Play Protect now. So again, accessibility, and we have a downloaded app, Play Protect. Yeah, we want to use Play Protect. So Play Protect is going to have full control of your device. View and control the screen, view and perform actions. Allow. And then once again here, it's going to just start taking over and doing a lot of the things that it's going to do kind of all on its own. And I think maybe this is an issue I've had recently where I lose kind of the visual. Well, it's still there. So now Play Protect is installing and it's just going to start doing stuff. Now the interesting thing is this one has self-protection mechanisms very, very similar to what SOVA did where if you try to uninstall, it's basically just going to keep you away from being able to uninstall the app.

(00:47:28)
So no matter what you do, you try to uninstall, it's just basically going to close down all the app info before you can even click on anything. This one I believe is interesting. I think it does the same thing for any app. No it doesn't. It just self protects itself essentially. Again, if you try to go to App info to uninstall it, boom, it just closes everything down. So it has that nice little self-protection mechanism that's there. And again, if you have banking apps installed, one of the more than 400 targets, it's going to start having fun with that. So that's an interesting thing. Okay, Xeno, that's a fun new one. Again, this is really recent stuff. This is stuff that's happening out there right now. The good thing is this one wasn't out on Google Play but is distributed SOVA kind of via social.

(00:48:26)
So you get tricked into going to a website or maybe it's a fake banking site that says you need to download this app to access your bank or it's a cool currency converter, et cetera, those kind of fun things. Okay, so now we're going to do something a little bit different. We're going to step away from malware. We're going to look at what do we do when we're doing mobile threat research and we need to make our device be somewhere else in the world, look like it's somewhere else in the world, actually have an IP address somewhere else in the world. And then how do we do that with the current mechanisms built into Corellium? So we have two ways to do it. We can travel the world with the GPS and I'm going to show you this. This is kind of a cool demo. I like it. So basically I've installed Google Earth on my device.

(00:49:22)
Zoom is conflicting with me. Again, I'm losing my video stream. Okay, there we have our screen back and we can go in here to our location sensor. And as you can see right now I'm sitting in Cork, Ireland. If I zoom out on my map, I can change my location into the downtown heart of London, and then I can click over here on the app and I now my location is actually changing and I'll actually fly from Cork over to downtown London. And so this is basically using the sensor. Corellium can modify the sensor on the device that apps can then use to display changes of locations and things like that. And I kind of like the Google Earth one, you can fly around and kind of see things happen no matter what you're going to do with changing your location. So this is both for iOS and Android.

(00:50:21)
This is basically the way that you're going to use Corellium to change the GPS location of your device. So now let's go back. Let's talk about changing the network location. And I just took these quick three screenshots. So basically we're going to have an iOS device. We're going to VPN into the Corellium framework and establish a connection with Burp Suite so that the iOS device is actually sending us traffic not out through AWS in Ohio, but it's actually going to come through my Mac right here in my office in San Antonio. And then from my Mac here, I can use something like a VPN to get an IP address in France. Now the reason you do this is one, because you want to capture the traffic with Burp. And two, you don't want the VPN client on the device itself because some of the services and things like that can see that it's using a VPN.

(00:51:24)
So this requires essentially no changes that are visible to software on the device. So let's go ahead and go through this quick demonstration. I think you're going to like these traveling-the-world demos. So the first thing that I'm going to do is I need to use a connection to get into the device itself. So how do I connect via VPN, right? So we have this OVPN file. You download it and you can use—sorry, I didn't have my copy of Viscosity running. So basically once I connect into this VPN, my Mac is essentially part of this iPhone's network. It's netted and firewalled off, but I have the ability to go directly to the device by its IP address and things like that once I'm connected into the Corellium VPN. Now, if you're using Corellium appliances that you've purchased from us versus the AWS, there is no VPN because your machines will be able to layer two or layer three, connect into the server. So you don't actually have to do this portion. This is only for our Cloud offering where you actually have to connect to the VPN. Once I'm on the VPN, I can then use Burp to grab and configure a proxy. And you'll see here that I get an IP address here, that is actually from the Corellium VPN. Once I'm connected into my AWS VPN into the Corellium device, I'm going to start a proxy on my Mac, a Burp Suite proxy on port 80 80.

(00:53:17)
So we'll go back to the device. Now on the device, all I have to do to tell it to use my Mac's connection to the internet is I go into my wifi settings and I redirect it to that proxy that I set up for Burp. And then once I do that, you should begin to start seeing some traffic coming through Burp shortly. You can now see the device is now connecting through Burp on my Mac. So if I go to my device and I go to something like ip-api.com on the device, I should be connecting out of my Mac, which is based here in my office in San Antonio, Texas. So you can see here, it's now coming out of my office in Boerne, Texas. My phone company, all that kind of fun stuff is here. If I want to change the location, now is basically when I will come over here and do something like Nord, or actually what do I have here? I have Nord here.

(00:54:44)
So, I can now basically just click so it appears as if it's in France because it's connected through my Mac. And actually I'm going to do that. So at this point, that's when you can start doing fun

things like there was an investigation that I was doing into a threat analysis, a threat vector whereby this text message got sent to the device so we can emulate that as well. So this text message, and I actually just grabbed this directly from, so basically this is the actual threat vector that originally occurred. I can send this SMS message to my mobile device and the way this one worked, if you're interested in this one, let's see. I don't remember the name of this one. I'll check that for you here in a second. But basically what would happen is if the device was outside of France via IP address, you would get a 404 message from the when you clicked on this link in the messages. However, if you were inside France, you would get the actual targeted phishing site of the bank that they were trying to essentially get into. So this is how you essentially could use Corellium to put these virtual devices really anywhere in the world, but also still be able to sniff the traffic that's going through, for example, with Burp, so that you're able to see what is actually happening as these devices are connecting outside the world.

(00:57:24)
So you want to see if it actually is going to click on that. This site's been down, I believe for quite some time. So Burp is going to put an error into our device here and tell us that it's dead. But anyway, if you're actively researching some threats, things like that, putting the device GPS as well as network connectivity, and this can be done both for the iOS and Android. I just kind of wanted to show you one of each, they can both be done that way and that way those devices are in those other parts of the world because a lot of these threats that we're looking at today are targeted geographically. All right, let's get into some of the questions here. So there's been a lot of great questions. I really appreciate the engagement. Will I be showing debugging an app or kernel through IDA Pro, setting break points, viewing memory, things like that?

(00:58:22)
I am not today, but we have done four webinars in the previous 4 months on app pen testing using reverse engineering and tools like that. If you are interested in debugging the kernel, we do have a Corellium Quick Start training, which is free for everybody to attend. It's going to be on Tuesday. Actually, it's going to be the first Tuesday of every month. But the folks that we have teach that training are experts in kernel vulnerability research and things like that, and they can show you interesting cool things that you can do. But yes, this platform allows us to debug at several different levels, which we can't even do on physical devices for example, because we are a hypervisor. When you have the on-premises appliances, you can actually gain debugging information from the virtual device down to the hypervisor. You can actually sit in the middle there and actually debug what is trying to be executed on physical CPUs, hypervisor tracing and things like that.

(00:59:30)
In the phone itself, we have what's called CoreTrace, which is system call tracing. So basically you're able to see any call that the app is making to the kernel. We instrument all of that for you directly there. So doing dynamic debugging is a really cool thing that we offer on the platform. Static analysis, again, we did a webinar last month on static analysis. We actually have two more coming up, which you're going to go deeper into reverse engineering and static analysis

on both Android and iOS. Those will be coming up in the next couple of months. So please look for those coming up if you're interested in getting into a lot of the techniques and tactics and theory around pen testing and using those static analysis tools. So we are over the hour and there's a few more questions, but we didn't really get to 'em.

(01:00:26)
I really just wanted to thank you all for taking the time, coming and hanging out. If you have any questions, there's my contact info right there on the screen. Feel free to reach out. For those of you, I didn't get to your questions, I will answer them and send you an email directly. I really, really appreciate all of the time today. Thank you for coming to the webinar. I look forward to seeing you on our next set of webinars. So keep an eye on Corellium.com for those to come out as well as you'll probably get an invite in your email. So thank you very much and I hope everybody has a fantastic day and the rest of the week. Thank you all and we'll see you next time.