Amitai Ben Shushan Ehrlich, Threat Intelligence Researcher at SentinelLabs, talks to Dvir Sayag on the Hands-On Security podcast.

Amitai discusses his research into a series of extortion attacks against organizations carried out by Iranian APT group BlackShadow. He shares details of the group's modus operandi and attack vectors, offering valuable insight into how BlackShadow operates as well as practical mitigations.

Click 'play' and enjoy the show!

PODCAST
Behind the Scenes of BlackShadow APT with Amitai Ben Shushan Ehrlich
SentinelOne

Commentary: Yes. You're listening to Hands on Security Hunter's hands on security podcast Cybersecurity, of course, and practical.

Dvir Sayag: Hello, everyone. I'm Dvir Sayag and welcome to the 10th episode of Hands-On Security Podcast. This is very exciting because it's the last episode of the season. It's the like, literally the end of the season. And for this special episode, the most dynamic dive from SentinelOne. Amitai is a great researcher in the SentinelOne Threat Intelligence Group. So in this episode, we are going to talk about the black shadow extortion group discussed the way they operate and give examples of their attacks. How you Amitai?

Amitai Ben Shushan Ehrlich: I'm great. I'm great. Great to be here.

Dvir Sayag: It's like very cozy and rainy outside. So yeah, it's fun to be in the studio and let's jump just like into the subject. First of all, just tell me what is your role when you are researching the the first extortion group? And then just like, give a quick overview of them, OK?

Amitai Ben Shushan Ehrlich: Uh, first of all, introduce like myself a little bit. At the moment. I work at SentinelOne Threat Intelligence Group as a threat researcher where I usually deal with regional threats. Iranians, mostly in the past, have been part of Sygnia, which is an incident response services company. It was part of their incident response and threat hunting team and prior to that I was in the IDF, like many other Israelis. Yeah. So yeah, one of the most interesting topics that I researched lately was egregious, which is how we call the group behind the black shadow operations. It's a group that we agree with. That's a great question, because it's cool. Oh, there's no reason. No, actually,

Dvir Sayag: There's no idea behind that.

Amitai Ben Shushan Ehrlich: Just no, no. And actually, like, it's the only group that I named after a mythical creature. So it's just a standalone name right now. Ok.

Dvir Sayag: So tell us about them.

Amitai Ben Shushan Ehrlich: Ok, so everything started around December 2020 with a series of extortion attacks carried out against Israeli organizations by a secret group that referred to itself as Black Shadow. Black Shadow presented themselves as a financially motivated group, although it does did seem weird at the time because of two things two main things.

Dvir Sayag: Right? So they when they presented themselves, it was like on a website or by email.

Amitai Ben Shushan Ehrlich: Most of their, uh, their communication channels with their victims is Telegram, which they opened. Like public channels, they also open the Twitter account. They contacted journalists. This is one of the weird things about them that they're very craving for media attention. That's one of the things that characterizes them.

Dvir Sayag: I guess that we will get to it after, but maybe the main goal is not only money.

Amitai Ben Shushan Ehrlich: Yeah, it's not not only money, it's not money at all. It's like they're mostly interested in the effect that their attacks are causing. That's why they're probably interested in the media attention. And other than that, they're also very much focused on Israel, which doesn't make any sense for any financially motivated actor. And when we take those two things together, we realize that there is something fishy about this operation that it's not really financially motivated. Hmm. And we have to give them credit, by the way, because they're quite good at it. There were a lot of, uh, ransomware as a disruption tool groups operating in Israel like Turkey and others. But Black Shadow really made a lot of noise. A lot of us drew a lot of attention from both the media, the Israeli public and threat researchers alike, and that got us to start and take a deeper look into what's going on there. Who is behind it and what are their motivations?

Dvir Sayag: How did this story get into the public to the media?

Amitai Ben Shushan Ehrlich: Not quite sure. Like the first major incident was the Sherbert incident, which is a very large Israeli insurance company. If will go around and ask people in Israel about the security incidents, I guess a lot of people will know it even if they're not really into cybersecurity because it made a lot of noise. And ever since then, they're trying to recreate the success in the Shubert incident, even though they're not really making as much noise as they used to do back then. But when we looked at those incidents, we realized that black shadow is just extortion lies used by a threat group that has been operating around the Middle East for a much longer period of time that went mostly unnoticed that we call agrees, and we believe that is operating both in Israel and in other countries in the region.

Dvir Sayag: Like, what do you see any examples of the attacks? Not in Israel?

Amitai Ben Shushan Ehrlich: Yes, so. We are seeing them operating a lot in the United Arab Emirates, like both on the espionage level, like long maintaining persistence, exfiltration information and both, and the disruptive sides carrying out ransomware attacks. So like they're doing what they're doing in Israel under the black satellites. Also in other countries in the Middle East use different aliases. So it will take a look at Agrius as a group, then Blackshadow is just one subset of their activity. While they do have other extortion aliases used both in Israel and in the United Arab Emirates, for example.

Dvir Sayag: Yeah. So I just want to say that for the listeners from the US, probably this is a great example of how to deal with this kind of group. So even if they are not attacking in the United States, there is a lot to learn when you deal with this kind of groups.

Amitai Ben Shushan Ehrlich: So, yeah, yeah. So I agree. It's like Dryset is just one of many Iranian threat groups that deploy ransomware as some sort of destructive tool. Not all of them operate exclusively in the Middle East. Some of them also work in the United States.

Dvir Sayag: Yes, so I think that we can go back to Shirbit, maybe. Can you elaborate about the timeline of the attack? The extortion?

Amitai Ben Shushan Ehrlich: Yes. Shirbit started off as a classical extortion incident, with the attackers approaching the victim asking them for ransom in bitcoin, although there was something a bit off there. Most of the communication was carried out in public channels. They started leaking information from the network at a very slow pace, releasing information piece by piece, mostly

Dvir Sayag: Kind of information.

Amitai Ben Shushan Ehrlich: So mostly like personal information of Israelis like IDs, insurance documents, stuff like that. And when they did it, they also approach journalists and media outlets. There were actually some people that interviewed the attackers, which is very unusual in the context of a ransomware attack, and it's quite interesting to see how invested they were in sharing it like a classical ransomware group or ransomware syndicate probably operates ransomware attacks against several organizations, and at once they're not very invested in each one of their organizations. It's a way to make money, but those guys were very much invested in shielded. That's what like they did for days, and they put a lot of effort, not just in the technical breach into the network and the exfiltration, but also in the extortion and the leaking of public information forms of it.

Dvir Sayag: Yes. So from my experience with this kind of group, I know that when you try to get to the media, you need to do something that will attract attention. So when they try to get information about Israel exists because they want the public, they want the media, they want the journalists to actually have interest in them and to publish it. And then if the public doesn't know, it literally didn't happen. So you can see it as clear as they can do it.

Amitai Ben Shushan Ehrlich: Yeah, imagine like being just a random person and then suddenly someone leaks your idea or your information that you automatically panic.

Dvir Sayag: Yes. So with the story, as we said before. But if we want to like, look at them at a technical point of view, what kind of tips are they mostly using the use of specific malware? Does it have special characteristics?

Amitai Ben Shushan Ehrlich: So Agrius has quite a unique modus operandi. Also, they have the customer tools that they use. Most of the reparations start by exploiting public-facing applications, mostly web servers, which is quite interesting. We don't see them engage in phishing, they're into minimum user interaction. It is important to know, though we haven't observed them using any zero days or anything of that sort. Mostly one day's exploits, they're very fond of the Fortinet vulnerabilities and also exchange vulnerabilities lately.

Dvir Sayag: Can you explain a little bit about the Fortinet vulnerability?

Amitai Ben Shushan Ehrlich: Yeah, so they're very fond of exploiting the Fortinet VPN product. There was this specific CV that they used that allowed them to actually, like, exploit the public facing VPN interface and get access to the network. To some extent, those kind of attacks have minimum user interactions, so they're less likely to be detected, unlike phishing attacks and stuff. When they successfully exploit the public facing application, which is a web server, for example, they deploy a web show. The rebels are quite unique. Actually, there are variations of ISP Spy, which is a very known common website used by a variety of threat actors, but they do their own modifications to it, so they

Dvir Sayag: Download it somewhere or buy it somewhere, and then they modify it. Yeah.

Amitai Ben Shushan Ehrlich: Like if you look at the code of the Web share. You will see that it's pretty much the same. They mostly change variable names. They add a little bit of obfuscation. But the basic functionality is the same. One thing that they do that is interesting is that HP Ex-Spy is a very large, comprehensive web shells website with a lot of functionality. And what they do is actually take chunks of it and make smaller web shells that use each functionality according to to the necessity of the attacker at the moment. Like if it needs to run a command, for example, it will take only the snippet from the web shell that is responsible for command, line the execution and deploy that. Also, they have a version to upload the file and like when you take chunks of the website each time the the it's less likely to be detected because it's smaller, it's

Dvir Sayag: It's less detailed. This is like something that they use and we don't see it anywhere else.

Amitai Ben Shushan Ehrlich: So I haven't like a lot of threat actors. Use speaks by the usage of like specific functionalities and the chunking. So smaller web shells is something that I think is quite unique to them, but it's not like something novel or new. It's just like, you know, the way they decided to operate. But it is quite unique in the context of us being able to pivot off this web shells that we've seen to find additional web shells. So when we like search for additional web shells with similar characteristics which are like chunked and they have specific obfuscation and specific variable names, we came across a lot of other web shells, almost all of them uploaded from the Middle East like countries like Saudi Arabia, United Arab Emirates, Israel, Iran, which indicates a clear regional focus around the Middle East. Also, Pakistan is a country of interest to them, which aligns in general with the interest of of an Iranian threat group. And this is like one of the first indications that we get that this is not just like a financially motivated group, but a group that is focused around the region

Dvir Sayag: And we see them moving on in the network like the lateral movement.

Amitai Ben Shushan Ehrlich: Yeah. So the way they do lateral movement is quite generic, actually, like they have their own specific pathways and file names that they use. But they use like common tools such as the exec for lateral movement. They also use proctored for credential harvesting. Nothing very much special about how they operate in the network, but it it works like they know what they're doing. They're quite good at it, but they don't use like any very sophisticated methods to move laterally or anything like that. But when they do reach to a host of interest, they deploy a custom backdoor that they developed that it's called IP stack helper. Mm hmm. We see it mostly installed on domain controllers. It's pretty much a basic backdoor in the way it operates. It retrieves commands from command and control servers over an HTTP channel, but it is quite well maintained like it does seem to have been developed for a lot of time. When we see it in the current wave of like black shadow incidents in Israel, we see that there is an internal version on it, like two point fifteen point five. So that's a clear indication that they are like older versions that went unnoticed for quite a long time.

Dvir Sayag: But I guess that you did release an IOC list that, yeah, people can block.

Amitai Ben Shushan Ehrlich: Of course, when we got like the first samples of the IP cycle, but we obviously tried to find all the variants and like one of them, actually popped up on video that was uploaded in like twenty nineteen. It has like the internal version one point five. So and we believe like the compilation timestamp on that specific sample is quite authentic. Mm hmm. So we believe that IP EPP has been around for at least two years now and like the incidents in Israel and the black shadow ones were just like, I guess they were, they felt comfortable, like burning it or getting rid of it because maybe they have additional tool sets. And that's the reason it was exposed because those incidents were very loud. They drew a lot of attention. Obviously, when someone gets ransomware attack, then their network is being analyzed and research into. So that's where they found it. But it was active throughout the region for quite a long time.

Dvir Sayag: Can you offer any detection methods that people can implement what they are dealing with this kind of actor? Yes.

Amitai Ben Shushan Ehrlich: So general network hygiene methods are very recommended.

Dvir Sayag: Always, always matching.

Amitai Ben Shushan Ehrlich: Yeah, like patching is obviously always the answer to pretty much anything. Like I said, I agree use uses mostly one day vulnerabilities and exploits, so just patching your public facing applications would be very much effective in. Lists delaying them or stopping them completely when it comes to lateral movement, then monitoring for tools such as sex and the executions of ProComp is very much helpful in the context of it's not just a race. A lot of other threat actors use those tools, both financially motivated ones and nation sponsored group. And in the context of the EPP caliber as a backdoor, then suspicious services are always something to look for. This vector registers itself as a service.

Dvir Sayag: What about the ransomware itself?

Amitai Ben Shushan Ehrlich: The ransomware itself is a good point, because that's what you would expect a financially motivated group to deploy. But during the black shadow incidents, agrees did not deploy ransomware. Wow.

Dvir Sayag: They actually attack without ransomware.

Amitai Ben Shushan Ehrlich: Yeah, that sounds a bit weird. When you look into what happened, you can actually see the data flow wipers, which are like destructive tools only made to completely destroy your computer. Not a thing you want lying around your network. They use two of them. Actually, one of them is called Deadwood., which was actually deployed in the past against the target in Saudi Arabia in 2019. That's also an interesting fact in the context of the attribution because deadwood was attributed to Iran in the past during twenty eighteen, and the version that they use is an updated version of the version that was used in the attacks in 2019, indicating that they have access to the code itself. They're not like just, I don't know, download it from anywhere or something like that. And they also used another wiper, which was not very much successful in its work. It didn't work. Yeah, it was quite badly written. Like, it seems like two guys were sitting in the room and they were like, Yeah, let's write a wiper. Let's take chunks of code from the IP stack helper and just make something work. And they wrote it like really quickly. And they didn't do it quite well because the way it searches for files to wipe has some sort of logic flaws, which makes it, uh, not work.

Dvir Sayag: Yeah. So this is funny because it's actually a ransomware group that doesn't deploy a ransomware. And if they are financially motivated as the other consumer groups, you would realize that they would. Extortion made extortion with ransomware payload. But we can see now that, as we said before, they're probably not financial motivated with this example.

Amitai Ben Shushan Ehrlich: The thing is, they did try to look financially motivated that as we monitor their activity, we actually came across a version of this wiper that was turned into an actual ransomware. So like in current egregious events where they deploy Apostle, it is really a ransomware, so they're intrusions would look more credible.

Dvir Sayag: So how would you how would you steal this use case, this stupid use case with a sentence? Just give me a sentence that you seal it with

Amitai Ben Shushan Ehrlich: Sentence is quite hard. I wasn't prepared. I think this is a clear indication that state sponsored threat actors use ransomware as a disruptive tool because that's not one sentence. But yeah. But that's because we can see the evolution from the wiper that was deployed in Israeli organizations to the ransomware that was deployed in the United Arab Emirates and later on in Israel as well. So that's like, for me, a clear proof that the ransomware is used as a disruptive tool.

Dvir Sayag: I agree, and I think that it's a good sentence to finish with because now our listeners can understand that maybe when they are dealing with this kind of threat, they don't need to pay or maybe the threat actor that actually attacks them as other interests. So maybe it's time to talk to someone, to a specialist about this kind of subject. But I actually want to take a step back you and your company, you have a lot of research history and your threat. Intelligence methods and tools are amazing. So I want you to give us a little bit of that. And what are the research steps that you take when you start investigating a group, any specific tools that you use?

Amitai Ben Shushan Ehrlich: Yes. So like there is this intelligence cycle which is used in in intelligence in general and is also applicable to threat intelligence that starts by planning. Why are you doing your research to begin with? That's a very important point. Whether it is to find intrusion in your network, whether it is to improve detection, it has could be a lot of things, but you need to know why you're looking into what you're looking for in order to start following that. I would say collection trying to find as much information possible about what you're looking at from public information and so on. There are a lot of. Good tools to do that. Nowadays there's MRTP, which is like the model information sharing platform and open source platform that is used to share our. There is open thread exchange by all involved. Pretty much the same concept also open CTI. A lot of tools out there that helps us gather information already available to the public about the threats that we're looking at. Following that, I would start by like processing the information that you just gathered, trying to leverage the data you just collected to gain additional insights or information about what you just got.

Dvir Sayag: So for files, this is where VT comes to the picture.

Amitai Ben Shushan Ehrlich: Yeah. Like VirusTotal is obviously a very useful tool for threat researchers. The instant response? Everything, pretty much. It’s like a dictionary for files. I don’t know. Uh, so a lot of times it is very helpful, very a lot of fun as well. I also personally like Intezer, a lot of time categorized like binaries and help you understand attribution in the context of who, what group is behind it or what other files it’s similar to which it doesn’t always offer.

Dvir Sayag: And what about infrastructure analysis?

Amitai Ben Shushan Ehrlich: So for infrastructure, there are a lot of sources nowadays as well when it comes to passive DNS, who is records and scanning data? There are a lot of possibilities since this Shodan binary edge are very good sources for scanning information, referring to into passive DNS and who is information that’s also on VETY, by the way. But other tools include Risk IQ and domain tools, which are very, very much good to look at. My opinion and I also like each organization, has its own sources, and that’s pretty much what makes the research unique. Whether it is telemetry or information from your network, that’s that’s always something to put into your research and look at, because that gives your own perspective which others can get.

Dvir Sayag: Amazing. Thank you so much for sharing this kind of knowledge that you have and sharing about Tibet and about specifically the black shadow extortion group. It was really fun having you here. So, guys, please follow Amitai on Twitter. What’s your Twitter

Amitai Ben Shushan Ehrlich: Tag? So my Twitter handle is Amitai, BC 3.

Dvir Sayag: Amazing. So thank you very much, everyone. And until next time.

Commentary: This was hands on security. Everything you need to know about cyber security. Up close and practical. Well, luckily, the Peka CEO Michel It podcast is a late.

Behind the Scenes of BlackShadow.mp3

Transcript

00:00:00Commentary

Yes. You're listening to Hands on Security Hunter's hands on security podcast Cybersecurity, of course, and practical.

00:00:15Dvir Sayag

Hello, everyone. I'm Dvir Sayag and welcome to the 10th episode of Hands-On Security Podcast. This is very exciting because it's the last episode of the season. It's the like, literally the end of the season. And for this special episode, the most dynamic dive from SentinelOne. Amitai is a great researcher in the SentinelOne Threat Intelligence Group. So in this episode, we are going to talk about the black shadow extortion group discussed the way they operate and give examples of their attacks. How you Amitai?

00:00:49Amitai Ben Shushan Ehrlich

I'm great. I'm great. Great to be here.

00:00:51Dvir Sayag

It's like very cozy and rainy outside. So yeah, it's fun to be in the studio and let's jump just like into the subject. First of all, just tell me what is your role when you are researching the the first extortion group? And then just like, give a quick overview of them, OK?

00:01:12Amitai Ben Shushan Ehrlich

Uh, first of all, introduce like myself a little bit. At the moment. I work at SentinelOne Threat Intelligence Group as a threat researcher where I usually deal with regional threats. Iranians, mostly in the past, have been part of Sygnia, which is an incident response services company. It was part of their incident response and threat hunting team and prior to that I was in the IDF, like many other Israelis. Yeah. So yeah, one of the most interesting topics that I researched lately was egregious, which is how we call the group behind the black shadow operations. It's a group that we agree with. That's a great question, because it's cool. Oh, there's no reason. No, actually,

00:02:00Dvir Sayag

There's no idea behind that.

00:02:02Amitai Ben Shushan Ehrlich

Just no, no. And actually, like, it's the only group that I named after a mythical creature. So it's just a standalone name right now. Ok.

00:02:12Dvir Sayag

So tell us about them.

00:02:13Amitai Ben Shushan Ehrlich

Ok, so everything started around December 2020 with a series of extortion attacks carried out against Israeli organizations by a secret group that referred to itself as Black Shadow. Black Shadow presented themselves as a financially motivated group, although it does did seem weird at the time because of two things two main things.

00:02:38Dvir Sayag

Right? So they when they presented themselves, it was like on a website or by email.

00:02:44Amitai Ben Shushan Ehrlich

Most of their, uh, their communication channels with their victims is Telegram, which they opened. Like public channels, they also open the Twitter account. They contacted journalists. This is one of the weird things about them that they're very craving for media attention. That's one of the things that characterizes them.

00:03:03Dvir Sayag

I guess that we will get to it after, but maybe the main goal is not only money.

00:03:08Amitai Ben Shushan Ehrlich

Yeah, it's not not only money, it's not money at all. It's like they're mostly interested in the effect that their attacks are causing. That's why they're probably interested in the media attention. And other than that, they're also very much focused on Israel, which doesn't make any sense for any financially motivated actor. And when we take those two things together, we realize that there is something fishy about this operation that it's not really financially motivated. Hmm. And we have to give them credit, by the way, because they're quite good at it. There were a lot of, uh, ransomware as a disruption tool groups operating in Israel like Turkey and others. But Black Shadow really made a lot of noise. A lot of us drew a lot of attention from both the media, the Israeli public and threat researchers alike, and that got us to start and take a deeper look into what's going on there. Who is behind it and what are their motivations?

00:04:01Dvir Sayag

How did this story get into the public to the media?

00:04:05Amitai Ben Shushan Ehrlich

Not quite sure. Like the first major incident was the Sherbert incident, which is a very large Israeli insurance company. If will go around and ask people in Israel about the security incidents, I guess a lot of people will know it even if they're not really into cybersecurity because it made a lot of noise. And ever since then, they're trying to recreate the success in the Shubert incident, even though they're not really making as much noise as they used to do back then. But when we looked at those incidents, we realized that black shadow is just extortion lies used by a threat group that has been operating around the Middle East for a much longer period of time that went mostly unnoticed that we call agrees, and we believe that is operating both in Israel and in other countries in the region.

00:04:54Dvir Sayag

Like, what do you see any examples of the attacks? Not in Israel?

00:04:58Amitai Ben Shushan Ehrlich

Yes, so. We are seeing them operating a lot in the United Arab Emirates, like both on the espionage level, like long maintaining persistence, exfiltration information and both, and the disruptive sides carrying out ransomware attacks. So like they're doing what they're doing in Israel under the black satellites. Also in other countries in the Middle East use different aliases. So it will take a look at Agrius as a group, then Blackshadow is just one subset of their activity. While they do have other extortion aliases used both in Israel and in the United Arab Emirates, for example.

00:05:33Dvir Sayag

Yeah. So I just want to say that for the listeners from the US, probably this is a great example of how to deal with this kind of group. So even if they are not attacking in the United States, there is a lot to learn when you deal with this kind of groups.

00:05:47Amitai Ben Shushan Ehrlich

So, yeah, yeah. So I agree. It's like Dryset is just one of many Iranian threat groups that deploy ransomware as some sort of destructive tool. Not all of them operate exclusively in the Middle East. Some of them also work in the United States.

00:06:05Dvir Sayag

Yes, so I think that we can go back to Shirbit, maybe. Can you elaborate about the timeline of the attack? The extortion?

00:06:15Amitai Ben Shushan Ehrlich

Yes. Shirbit started off as a classical extortion incident, with the attackers approaching the victim asking them for ransom in bitcoin, although there was something a bit off there. Most of the communication was carried out in public channels. They started leaking information from the network at a very slow pace, releasing information piece by piece, mostly

00:06:38Dvir Sayag

Kind of information.

00:06:40Amitai Ben Shushan Ehrlich

So mostly like personal information of Israelis like IDs, insurance documents, stuff like that. And when they did it, they also approach journalists and media outlets. There were actually some people that interviewed the attackers, which is very unusual in the context of a ransomware attack, and it's quite interesting to see how invested they were in sharing it like a classical ransomware group or ransomware syndicate probably operates ransomware attacks against several organizations, and at once they're not very invested in each one of their organizations. It's a way to make money, but those guys were very much invested in shielded. That's what like they did for days, and they put a lot of effort, not just in the technical breach into the network and the exfiltration, but also in the extortion and the leaking of public information forms of it.

00:07:35Dvir Sayag

Yes. So from my experience with this kind of group, I know that when you try to get to the media, you need to do something that will attract attention. So when they try to get information about Israel exists because they want the public, they want the media, they want the journalists to actually have interest in them and to publish it. And then if the public doesn't know, it literally didn't happen. So you can see it as clear as they can do it.

00:08:03Amitai Ben Shushan Ehrlich

Yeah, imagine like being just a random person and then suddenly someone leaks your idea or your information that you automatically panic.

00:08:11Dvir Sayag

Yes. So with the story, as we said before. But if we want to like, look at them at a technical point of view, what kind of tips are they mostly using the use of specific malware? Does it have special characteristics?

00:08:27Amitai Ben Shushan Ehrlich

So Agrius has quite a unique modus operandi. Also, they have the customer tools that they use. Most of the reparations start by exploiting public-facing applications, mostly web servers, which is quite interesting. We don't see them engage in phishing, they're into minimum user interaction. It is important to know, though we haven't observed them using any zero days or anything of that sort. Mostly one day's exploits, they're very fond of the Fortinet vulnerabilities and also exchange vulnerabilities lately.

00:09:01Dvir Sayag

Can you explain a little bit about the Fortinet vulnerability?

00:09:05Amitai Ben Shushan Ehrlich

Yeah, so they're very fond of exploiting the Fortinet VPN product. There was this specific CV that they used that allowed them to actually, like, exploit the public facing VPN interface and get access to the network. To some extent, those kind of attacks have minimum user interactions, so they're less likely to be detected, unlike phishing attacks and stuff. When they successfully exploit the public facing application, which is a web server, for example, they deploy a web show. The rebels are quite unique. Actually, there are variations of ISP Spy, which is a very known common website used by a variety of threat actors, but they do their own modifications to it, so they

00:09:52Dvir Sayag

Download it somewhere or buy it somewhere, and then they modify it. Yeah.

00:09:56Amitai Ben Shushan Ehrlich

Like if you look at the code of the Web share. You will see that it's pretty much the same. They mostly change variable names. They add a little bit of obfuscation. But the basic functionality is the same. One thing that they do that is interesting is that HP Ex-Spy is a very large, comprehensive web shells website with a lot of functionality. And what they do is actually take chunks of it and make smaller web shells that use each functionality according to to the necessity of the attacker at the moment. Like if it needs to run a command, for example, it will take only the snippet from the web shell that is responsible for command, line the execution and deploy that. Also, they have a version to upload the file and like when you take chunks of the website each time the the it's less likely to be detected because it's smaller, it's

00:10:48Dvir Sayag

It's less detailed. This is like something that they use and we don't see it anywhere else.

00:10:55Amitai Ben Shushan Ehrlich

So I haven't like a lot of threat actors. Use speaks by the usage of like specific functionalities and the chunking. So smaller web shells is something that I think is quite unique to them, but it's not like something novel or new. It's just like, you know, the way they decided to operate. But it is quite unique in the context of us being able to pivot off this web shells that we've seen to find additional web shells. So when we like search for additional web shells with similar characteristics which are like chunked and they have specific obfuscation and specific variable names, we came across a lot of other web shells, almost all of them uploaded from the Middle East like countries like Saudi Arabia, United Arab Emirates, Israel, Iran, which indicates a clear regional focus around the Middle East. Also, Pakistan is a country of interest to them, which aligns in general with the interest of of an Iranian threat group. And this is like one of the first indications that we get that this is not just like a financially motivated group, but a group that is focused around the region

00:12:07Dvir Sayag

And we see them moving on in the network like the lateral movement.

00:12:11Amitai Ben Shushan Ehrlich

Yeah. So the way they do lateral movement is quite generic, actually, like they have their own specific pathways and file names that they use. But they use like common tools such as the exec for lateral movement. They also use proctored for credential harvesting. Nothing very much special about how they operate in the network, but it it works like they know what they're doing. They're quite good at it, but they don't use like any very sophisticated methods to move laterally or anything like that. But when they do reach to a host of interest, they deploy a custom backdoor that they developed that it's called IP stack helper. Mm hmm. We see it mostly installed on domain controllers. It's pretty much a basic backdoor in the way it operates. It retrieves commands from command and control servers over an HTTP channel, but it is quite well maintained like it does seem to have been developed for a lot of time. When we see it in the current wave of like black shadow incidents in Israel, we see that there is an internal version on it, like two point fifteen point five. So that's a clear indication that they are like older versions that went unnoticed for quite a long time.

00:13:30Dvir Sayag

But I guess that you did release an IOC list that, yeah, people can block.

00:13:36Amitai Ben Shushan Ehrlich

Of course, when we got like the first samples of the IP cycle, but we obviously tried to find all the variants and like one of them, actually popped up on video that was uploaded in like twenty nineteen. It has like the internal version one point five. So and we believe like the compilation timestamp on that specific sample is quite authentic. Mm hmm. So we believe that IP EPP has been around for at least two years now and like the incidents in Israel and the black shadow ones were just like, I guess they were, they felt comfortable, like burning it or getting rid of it because maybe they have additional tool sets. And that's the reason it was exposed because those incidents were very loud. They drew a lot of attention. Obviously, when someone gets ransomware attack, then their network is being analyzed and research into. So that's where they found it. But it was active throughout the region for quite a long time.

00:14:31Dvir Sayag

Can you offer any detection methods that people can implement what they are dealing with this kind of actor? Yes.

00:14:38Amitai Ben Shushan Ehrlich

So general network hygiene methods are very recommended.

00:14:42Dvir Sayag

Always, always matching.

00:14:45Amitai Ben Shushan Ehrlich

Yeah, like patching is obviously always the answer to pretty much anything. Like I said, I agree use uses mostly one day vulnerabilities and exploits, so just patching your public facing applications would be very much effective in. Lists delaying them or stopping them completely when it comes to lateral movement, then monitoring for tools such as sex and the executions of ProComp is very much helpful in the context of it's not just a race. A lot of other threat actors use those tools, both financially motivated ones and nation sponsored group. And in the context of the EPP caliber as a backdoor, then suspicious services are always something to look for. This vector registers itself as a service.

00:15:29Dvir Sayag

What about the ransomware itself?

00:15:33Amitai Ben Shushan Ehrlich

The ransomware itself is a good point, because that's what you would expect a financially motivated group to deploy. But during the black shadow incidents, agrees did not deploy ransomware. Wow.

00:15:47Dvir Sayag

They actually attack without ransomware.

00:15:49Amitai Ben Shushan Ehrlich

Yeah, that sounds a bit weird. When you look into what happened, you can actually see the data flow wipers, which are like destructive tools only made to completely destroy your computer. Not a thing you want lying around your network. They use two of them. Actually, one of them is called Deadwood., which was actually deployed in the past against the target in Saudi Arabia in 2019. That's also an interesting fact in the context of the attribution because deadwood was attributed to Iran in the past during twenty eighteen, and the version that they use is an updated version of the version that was used in the attacks in 2019, indicating that they have access to the code itself. They're not like just, I don't know, download it from anywhere or something like that. And they also used another wiper, which was not very much successful in its work. It didn't work. Yeah, it was quite badly written. Like, it seems like two guys were sitting in the room and they were like, Yeah, let's write a wiper. Let's take chunks of code from the IP stack helper and just make something work. And they wrote it like really quickly. And they didn't do it quite well because the way it searches for files to wipe has some sort of logic flaws, which makes it, uh, not work.

00:17:09Dvir Sayag

Yeah. So this is funny because it's actually a ransomware group that doesn't deploy a ransomware. And if they are financially motivated as the other consumer groups, you would realize that they would. Extortion made extortion with ransomware payload. But we can see now that, as we said before, they're probably not financial motivated with this example.

00:17:33Amitai Ben Shushan Ehrlich

The thing is, they did try to look financially motivated that as we monitor their activity, we actually came across a version of this wiper that was turned into an actual ransomware. So like in current egregious events where they deploy Apostle, it is really a ransomware, so they're intrusions would look more credible.

00:17:53Dvir Sayag

So how would you how would you steal this use case, this stupid use case with a sentence? Just give me a sentence that you seal it with

00:18:02Amitai Ben Shushan Ehrlich

Sentence is quite hard. I wasn't prepared. I think this is a clear indication that state sponsored threat actors use ransomware as a disruptive tool because that's not one sentence. But yeah. But that's because we can see the evolution from the wiper that was deployed in Israeli organizations to the ransomware that was deployed in the United Arab Emirates and later on in Israel as well. So that's like, for me, a clear proof that the ransomware is used as a disruptive tool.

00:18:34Dvir Sayag

I agree, and I think that it's a good sentence to finish with because now our listeners can understand that maybe when they are dealing with this kind of threat, they don't need to pay or maybe the threat actor that actually attacks them as other interests. So maybe it's time to talk to someone, to a specialist about this kind of subject. But I actually want to take a step back you and your company, you have a lot of research history and your threat. Intelligence methods and tools are amazing. So I want you to give us a little bit of that. And what are the research steps that you take when you start investigating a group, any specific tools that you use?

00:19:21Amitai Ben Shushan Ehrlich

Yes. So like there is this intelligence cycle which is used in in intelligence in general and is also applicable to threat intelligence that starts by planning. Why are you doing your research to begin with? That's a very important point. Whether it is to find intrusion in your network, whether it is to improve detection, it has could be a lot of things, but you need to know why you're looking into what you're looking for in order to start following that. I would say collection trying to find as much information possible about what you're looking at from public information and so on. There are a lot of. Good tools to do that. Nowadays there's MRTP, which is like the model information sharing platform and open source platform that is used to share our. There is open thread exchange by all involved. Pretty much the same concept also open CTI. A lot of tools out there that helps us gather information already available to the public about the threats that we're looking at. Following that, I would start by like processing the information that you just gathered, trying to leverage the data you just collected to gain additional insights or information about what you just got.

00:20:38Dvir Sayag

So for files, this is where VT comes to the picture.

00:20:42Amitai Ben Shushan Ehrlich

Yeah. Like VirusTotal is obviously a very useful tool for threat researchers. The instant response? Everything, pretty much. It's like a dictionary for files. I don't know. Uh, so a lot of times it is very helpful, very a lot of fun as well. I also personally like Intezer, a lot of time categorized like binaries and help you understand attribution in the context of who, what group is behind it or what other files it's similar to which it doesn't always offer.

00:21:14Dvir Sayag

And what about infrastructure analysis?

00:21:16Amitai Ben Shushan Ehrlich

So for infrastructure, there are a lot of sources nowadays as well when it comes to passive DNS, who is records and scanning data? There are a lot of possibilities since this Shodan binary edge are very good sources for scanning information, referring to into passive DNS and who is information that's also on VETY, by the way. But other tools include Risk IQ and domain tools, which are very, very much good to look at. My opinion and I also like each organization, has its own sources, and that's pretty much what makes the research unique. Whether it is telemetry or information from your network, that's that's always something to put into your research and look at, because that gives your own perspective which others can get.

00:22:02Dvir Sayag

Amazing. Thank you so much for sharing this kind of knowledge that you have and sharing about Tibet and about specifically the black shadow extortion group. It was really fun having you here. So, guys, please follow Amitai on Twitter. What's your Twitter

00:22:23Amitai Ben Shushan Ehrlich

Tag? So my Twitter handle is Amitai, BC 3.

00:22:30Dvir Sayag

Amazing. So thank you very much, everyone. And until next time.

00:22:38Commentary

This was hands on security. Everything you need to know about cyber security. Up close and practical. Well, luckily, the Peka CEO Michel It podcast is a late.

SentinelOne

-
-
-
-
-

- 1.00x

00:00:0000:22:5400:00:0000:00:00 / 00:22:54