Collaboration between network access brokers and ransomware actors deepens

May 20, 2021 in Uncategorized 6 min read

In this Help Net Security podcast, Brandon Hoffman, CISO at Intel 471, discusses about the increased collaboration between network access brokers (NAB) and ransomware operators, and how they funcion it today's threat landscape.

Here's a transcript of the podcast for your convenience.

Hi everybody. My name is Brandon Hoffman. I'm the CISO at Intel 471, a threat intelligence firm. I'm excited to join the podcast today, and I was planning to talk a little bit about the increased cooperation between what's commonly referred to as access brokers or network access brokers and ransomware operators. And then, recent activity has caused a little bit of a shift in maybe some of what I was going to talk about, but I think the topic is still relevant.

And just to establish some background, for those who may not be as familiar, when we look at the cybercrime underground, what we're talking about is two different groups of people. So the cybercrime underground really is comprised of people providing tools, services to each other, to perpetrate different types of attacks. And there's a wide variety of different products, goods, and services that are available out on the market, so to speak, today. One of those is network access brokers.

If you look across at the landscape of attacks, one of the initial ways that threat actors get into a network is of course they have to establish access. And there are people in the underground who specialize in establishing this initial access vector. And what they do is, that's their skill set, they gather up a bunch of different access to different organizations around the world, and then they broker them. They sell them off to the highest bidder or for a specified price. And in the past this was, you know, commonly done and widely available to anybody who was on the different marketplaces or forums where this activity takes place.

People in the past would buy network access from one of these brokers, and then they might exfiltrate data or load some different type of malware, and in certain cases, as is the case more recently, load ransomware. And of course it's all based on their ability to perpetrate a further attack. So it also depends on their goals. So whether they were trying to steal other credentials, whether they were trying to steal data, you know, most of it of course is all financially driven.

What we noticed, what was taking place is that there was this kind of increased cooperation between network access brokers and ransomware actors or ransomware-as-a-service operators. So what we found is that, as ransomware-as-a-service continued this kind of boom, it overshadowed to a degree some of the network access brokers' success. So, it's not that network access and these brokers are no longer prevalent and not still taking place, but what happened is all of the reporting and all of the kinds of sensational news that's going on is about these ransomware groups.

And so what we found is that these network access brokers started working more closely with the ransomware actors. Of course, this makes sense from a business perspective, it almost becomes a supply chain mechanism. If you have a commodity that you're trying to sell to a market, but you find one person who is willing to buy all of your product or provide a guaranteed return on a certain portion of your product, you're going to have some more cooperation between them. And that's exactly what we saw taking place here with network access brokers and ransomware-as-a-service groups.

So, essentially what was taking place is, these network access brokers would have a volume of network accesses instead of offering them to kind of the general marketplace. And by general marketplace I still mean the cybercrime underground, not just on Google. Instead of offering it that way, they were working in collaboration with ransomware groups to provide all the network access they have, and essentially have ready-made set of victims where they could go in. And if they had to do further escalation of privileges or move laterally, and then of course deploy ransomware for extortion mechanisms.

But, it's interesting because they really started getting very close and it almost seemed to us, to a degree that, instead of actually taking direct compensation for the network access, it almost appeared that some of them were just doing a profit sharing model with ransomware groups. So instead of saying "hey, this network access is $10,000", they're just saying, "we'll take 1% of the ransom take", which, you know, once you get to a profit-sharing model, it becomes really interesting. It really proves how mature this business has become.

So, originally this really started out kind of as a bias. It's just something that we thought, but we're seeing a lot of the operations really lean towards this way. So, all of the, not all but many of the high profile network access brokers that you've probably heard reported on the news, are working very closely with these ransomware groups. And this is more confirmed through recent reporting and recent observation, really starting, I would say, probably in the middle of 2020.

Obviously, this collaboration started much longer ago, but the confirmation of this bias really started taking place earlier this year. And I don't think we're planning to get into any specifics of the actors, but if there was more technical interest in how this takes place, you know, one threat actor would compromise a company, exfiltrate some data credentials or something else that could be used later. Potentially that those credentials were used in something like account takeover, they might take payment card information. They might even sell that data off as something separate than the access they have.

It's almost like sweating all the assets you have. Once somebody gets in, they're going to take what they can use or what they could then sell to other actors. They're trying to monetize all the different components. A less politically correct way to put it, it's almost like butchering an animal once the animal has been butchered. You're gonna take different cuts of it. You're going to sell it to different people who are going to prepare it a different way. So they might take payment card information, they might take credentials.

Once all of those pieces are taken out, then that leftover access would then be leveraged by a ransomware actor to kind of do what we would consider the final, the end of the attack chain, the final malware that would get loaded for to extort all that money.

It's really interesting that these actors, again, it proves the maturity of this market that they're starting to collaborate. They're starting to kind of monopolize network access brokers to create a more stable and smooth transition from initial access through the attack chain, all the way to ransomware and payment. So that's been interesting to observe in the underground.

Now, what's happened recently and by very recently, I mean, essentially today and even over the past couple of days, is there has been some very high-profile ransomware attacks on victims that probably were not the right victims for these ransomware groups to let affiliates target. And so, you know, we're talking about folks like DarkSide and the Colonial Pipeline Attack.

And we've seen ransomware groups start to back away. And even we saw some of this before where ransomware groups would extract this data and they would leak data to put pressure on victims to pay. But what we're starting to see a little bit is more around ransomware operators kind of talking about parting ways with the actual encryption. So the whole ransomware, what we know it to be, encrypting the data and then decrypting it for a certain amount of money. But what they're planning to kind of maintain, or what they're alluding to is that the leaked data, the stolen data, is essentially enough of a blackmail tactic to pressure victims into paying. And what that does is it allows them to attack more high profile victims or even more sensitive victims.

Ransomware groups allow them to have talked about, "we don't want to attack or critical infrastructure because we don't want to, we're not political, we don't want to disrupt", things like that. But if they don't do the actual encryption and they leave the operational network intact and they just use the data really as an extortion tactic to get them to pay, it allows them to kind of essentially reap all the benefits and the encryption-based exploitation no longer is a necessity.

I think this was interesting to bring up here today. Again, this doesn't reduce or remove the need for the network access brokers. I think we'll still continue to see that collaboration deepen and continue to take place. But what is interesting about it is that potentially what we'll see is more emergence of data marketplaces and still name and shame blogs for leaked data, but less actual encrypting of operational networks to bring them down.

Some of the interesting things that I thought would be good to talk about here today, and I'd be happy to follow up with anybody if they had questions. Again, my name is Brandon Hoffman, it's been great being here today, and I hope you found the content useful. Have a great day, everybody. Thanks.

Credit: Source link

Previous Post
Why passwordless is not always passwordless

Next Post
Sweeping Reforms To Overhaul Britain's 'Complicated' Rail System