Eye on Security

Ransomware and Observations from Recent IR Investigations

Transcript

Luke McNamara

Welcome to another episode of the Eye on Security Podcast. As always I'm your host Luke McNamara and joining me today I'm excited to have Mandiant SVP and CTO Charles Carmakal here. Charles, welcome to the episode.

Charles Carmakal:

Thanks for having me here.

Luke McNamara:

So I wanted to have you on not just because of your perspective on the very front lines of security, the threats that we're seeing impact organizations, but also because you have a front-row seat into how these organizations are thinking about these threats from the business perspective, from the C-suite perspective, so I think that would be a very kind of interesting window into what we're seeing in the threat landscape today and how organizations are responding. And of course if we're going to talk about the front lines of cybersecurity in 2020 you can't get away from ransomware so maybe we'll start there. What are we seeing this year when it comes to ransomware and maybe some of the trends that have been developing for a while but especially what we're seeing in earnest this year.

Charles Carmakal:

Yeah, so ransomware incidents have really evolved over the past 12 months or so. So in December of last year we saw a group called MAZE and it's an affiliate network of threat actors that operate under the MAZE name that have really changed the game from an extortion perspective. And so what they do is when they break into organizations they will steal materially-sensitive data from organizations first and then they'll deploy encryptors across the environment and start encrypting a bunch of systems. And so what they want to do is they want to really coerce victims into paying very high extortion demands in typically 6-figures, 7-figures, and sometimes even 8-figure demands and they do that by asking for money in exchange for not publicizing the data that they've stolen from the organization.

They also ask for money to provide working decryptors to help organizations to get their data back and so for a lot of victims it feels like a 1-2 punch to them. They're getting extorted form 2 different angles and actually something that's pretty interesting about MAZE is they're also charging for what they call a vulnerability assessment report or a remediation report to help the organization to understand how it was the threat actors actually got into their environment. Their reports aren't very good, sometimes they're pretty generic, every so often you get some information that might be useful to the victim organization, but yeah, the MAZE group has kind of from their perspective done a pretty effective job of coercing victims, which unfortunately is a pretty bad situation for the industry.

A lot of other groups have taken notice because the MAZE folks have made a lot of money and so you see a lot of other threat actors at this point launching their own naming and shaming site like MAZE did the last year so the NetWalker crew, the Conti crew, the DoppelPaymer crew, lots of other crews have their own sites and it's a way to amplify breaches, it's a way to coerce victims into paying, and unfortunately that created an environment where a lot of folks that may not have paid in the past that were just exclusively dealing with ransomware encrypting data and systems are feeling compelled to pay now because they don't want their data to get publicly disclosed.

Luke McNamara:

So it seems like at least some of this activity is compounding on top of each other say groups that maybe were involved in other aspects of cybercrime that are not entering the space because they've seen in some cases the very public successes of the other groups. What do you think is driving the increase in this and is it really an increase in this or are we just more aware of some of these operations?

Charles Carmakal:

Yeah, absolutely. So I definitely think there's an increase and I say this because look, there are a few reasons. One, I think a lot of threat actors recognized that 1 of the most effective ways to monetize your intrusions now is to both steal materially sensitive data from organizations and deploy ransomware encryptors and if you think about how long an operation could take, I mean an operation could take actually just a few days from the point in which they actually get access to an environment up to the point where they gain enough privileges and access to systems in which they could steal data and then also deploy encryptors.

And a lot of times we see that these victims end up paying $250,000 at a minimum for some of these intrusions. Sometimes again they're paying $1 million or $5 million or so and if you think about the level of effort associated with the operation again it could only be a few days in which the intrusion starts to the point in which they actually get paid. And sometimes it takes a little bit longer, maybe a few weeks or so, but if you compare that to some of the legacy intrusions and the way that other threat actors have monetized their acts a lot of times in the past we used to see threat actors going after creditor information and if you think about how to monetize that you've got to steal a lot of credit card data in order to be able to sell it in the markets to be able to amass the same amount of money that you would with ransomware or with extortion.

And nowadays with organizations really shifting to end-to-end encryption or data tokenization it becomes harder to amass a high volume of credit card information. Sure, you could still amass it through ecommerce sites and you could skim credit card data that way but it's not as lucrative as it is to deploy ransomware and also to steal data to other organizations. And so I think a lot of threat actors have realized that this is just a very effective way for them to make money and now we see more and more threat actors doing it.

Luke McNamara:

Is there on 1 level a sense where it should be expected that we see this expansion of extorted behavior given what we've seen over the last several years with the shift and even ransomware operations moving to moving to more post-compromise activity where there's more kind of – they're moving laterally through the network, they're escalating privileges, but I would imagine in those sorts of operations they're also coming across data that they realize this could have value for extortion. Do you see that as having shaped maybe some of this activity or the shift into the sort of naming and shaming that we're seeing?

Charles Carmakal:

Yeah, so as I think about the evolution of ransomware in the early days you know around the 2013, 2014 timeframe when you were dealing with CryptoLocker and CryptoWall and locking and variants like that, back in those days when people talked about ransomware they were really talking about the encryptors that a lot of times either self-propagated or were distributed in a purely automated means. And so for example people got CryptoLocker infections because they receive malicious emails that had malicious attachments and they'd open it up and when they opened up that attachment a code would run on their computer that would essentially encrypt everything on their systems and maybe even encrypt everything on the network shares they were connected to.

So for the most part it was pretty automated and when you think about the ransom demands the authors behind CryptoLocker and CryptoWall, et cetera, they were looking to make money in bulk so they wanted to shock on as much ransomware out there as they possibly could and ideally they'd have a lot of different people that would end up paying and so they were asking for about $500 and they didn't know who their victims were so they didn't know if they were hitting a multi-billion dollar corporation or a grandmother that was trying to get the photos back of her grandchildren and so that's why they'd ask for such a small amount of money.

Fast forward by a few years you started to see a group called SamSam emerge and what was different about them was that instead of shot-gunning ransomware across the world they would break into organizations, usually they'd find some known vulnerable of breaking in, so a vulnerability or exposed RDP with easily guessable credentials, but they'd log into the network, escalate privileges, move around laterally, find systems and data that were of interest to them or that were critical to the organization, and then deploy their encryptors on those systems. And they started to ask for larger extortion demands and so they were asking for about $15,000, $20,000 or so and they were 1 of the first groups that kind of provided – it sounds weird to say this but they provided pretty good customer support in that if their ransomware decryptors didn't work, and they didn't work all the time, customers would complain or victims would complain to threat actors and they'd say, "Hey, we're really sorry. We'll get our developers on it right away and fix it," and low and behold they'd fix and provide updated working versions of the decryptors.

And a lot of other groups, they took note of that and they realized you could ask for more money when you know who the victims are. And again that's the difference between the Locky folks and the CryptoLocker's because they didn't know who they were hitting versus the SamSam crew and later on the LockerGoga Folks, the Megacortex folks, the RYUK folks, et cetera., they know which network they're in and they definitely do a little bit of research to try to figure out what is the revenue of the organization, what is their willingness to pay, and there's certainly a perception by a lot of these actors that if the company has hundreds of millions in revenue or billions in revenue they're probably more susceptible to pay large ransom demands. I guess maybe they have cybersecurity insurance that helps them with the payments or there could be any number of reasons.

In terms of the data theft quite frankly I don't actually think many of these threat actors actually have enough business acumen to understand the real value of the data that they find and that they steal and I still think that a lot of these actors they look for data that they perceive to be high value that may not necessarily be high value. So they'll look for directories that say finance or HR or contracts or maybe the word 'confidential' in it and they may grab lots of directories or lots of files that have these keywords in it and they pray that they're stealing something that's valuable to the victim organization. And I've seen many times where the victim organization looks at the data that was stolen and they say, "Hey, this is actually not that material to us. It's not sensitive." Yes, it has the word 'confidential' sometimes but just because it has the word 'confidential' on it a lot of documents have the word 'confidential' on it because that's sometimes just the standard template that they use.

And I've actually had some clients say, "What the threat actor has stolen or what they've shown us is not valuable, but what they don't realize is they actually do have some valuable data. They didn't show it to us but we know they have it but they don't realize that it's valuable or they could've looked at this other server that they had access to and they could've taken this directory and that would have been much valuable to us and we probably would've paid." And so again I don't know that the threat actors truly have an understanding of what they're stealing. I think they just again look for certain keywords and they pull it out of an environment as best as they can and to them they feel like if they've stolen a gig of data or a few hundred gigs of data or a terabyte of data to them the volume of data that they still is more valuable than the content of the data that they're stealing.

Luke McNamara:

So with that and moving over to the organizational response side of this and as I alluded to at the beginning you're someone who is working with not just the security teams involved kind of at a tactical and operational level with dealing with these events, but you're interacting with the board, with the C-suite. How are you seeing how they're thinking about this particular challenge that often represents to them continuity of operations, problems, increasingly with the leakage of data brand reputation problems? How are you seeing them respond to this and maybe in some ways where it differs with other types of criminally-motivated data breaches or IP theft from a nation state actor?

Charles Carmakal:

Yeah, so look I think over the years business leadership and executive leadership has become much more aware of cybersecurity and just general risk management principles and so they are thinking about cybersecurity as 1 of the risk management areas that they need to focus on and they hear about the headlines all the time, they know people at other organizations that have been impacted, and so there's definitely much more awareness in the industry today from a business perspective. But it's never really real to an organization until it's actually real to them.

And so what I find is a lot of times when organizations deal with a security incident to a security person we may sometimes look at maybe a non-sophisticated type of an event as maybe not as big of a deal but if it becomes a situation where maybe mainstream media or customers hear about it the problem becomes amplified to a level where it's perceived to be a pretty big deal to business leadership. On the flipside sometimes as security professionals we see something that might be a very sophisticated attack, maybe a very damaging incident to the organization, maybe it's a state-sponsored incident or something like that, but the victim organization doesn't necessarily perceive it to be a very high risk to them. Again there's a lot of different variables that come into play here and I actually distinctly remember having a conversation with an organization about a nation state that we believed was actively stealing intellectual property from that organization. And while that organization, they cared about it and they tried to respond to it, there was a much different level of response by that organization a few years later when they actually got hit with the ransomware incident.

And so the reason why it felt different is because in that ransomware incident the organization didn't have the ability to send emails to their employees or to business partners. They didn't have the ability to protect their business partners. The executives at the organization just couldn't do their work. And when you're in a situation where you work at a company but you can't write emails to people and you can't conduct business operations and you can't produce revenue you find religion and you find it quickly and you do a lot of things that you may not have otherwise done. And so whereas in the first situation I would've thought it would've been a pretty significant incident with the organization losing information to another government that was less relevant to that organization than the ransomware incident was a few years later. So I tell you security is definitely becoming much more visible at the board level, at the executive level, but it's not really real to a company until it's real.

Luke McNamara:

Yeah, I think that's a great story that showcases sometimes the things that we think organizations should care about differ not just in the organization itself but at the level and part of the business that they're in. I would be remiss if I didn't ask you this about ransomware and I think it's probably the most difficult in this discussion around ransomware, but what turns the tide of this? As I was preparing for this episode I was reminded of the activity we saw back in I think it was 2015 and 2016 from groups like DD4BC and Armada Collective that were carrying out DDoS acts on financial services, ecommerce platforms for extortive purposes. And so I think we've seen waves where DDoS as an extortion tool or just as a threat tool period has kind of come through waves and as security controls for that to mitigate that particular type of threat have gotten better it doesn't seem to be as much the threat that it used to be for a lot of organizations, although as we've recently seen in New Zealand it certainly can still be a threat.

Given the fact that there's evidence at least some of or most of these groups are operating in regions where law enforcement cooperation may be a bit difficult and comparing to other types of threat activity law enforcement operations where we've had arrests have seem to only have a minimal impact, what turns the tide of this? What changes with this threat being – stopping this threat from increasing in terms of impact?

Charles Carmakal:

Yeah, I wish I had a great answer here. I think there could be a few things that may curb these types of destructive and disruptive attacks and let me give you a few examples. So we talked a bit about the SamSam crew from a few years ago. Well in 2018 the Department of Justice had indicted 2 individuals out of Iran that were purportedly behind the SamSam ransomware operation and there possibly were other people that were involved in that operation, but since the indictment we have not seen a single SamSam ransomware incident beyond that point. And so there's a lot of speculation what actually caused the halting of intrusion operations by the SamSam crew and I won't go into those details but I think arrests will certainly help if you are able to identify some of the criminals that are behind these operations.

Now the problem becomes a lot of these folks operate in countries in which we have no extradition laws with the United States or other countries that may seek legal recourse. What we can rely on is when people come into a lot of money, and so a lot of ransomware operators they tend to have a lot of money or a fair amount of money, they want to do something with it and there's only so many good things you can buy in the home country that they operate in. So a lot of these folks have the inclination or the desire to travel and they hope that law enforcement and other intelligence agencies don't know who they are. And so every so often you'll see them, they'll travel to certain countries, and they'll get picked up when they travel to those countries.

The problem is I think there's just so many of those operators right now that operate in eastern European countries that don't have any real recourse that they could continue to operate with a sense of impunity and we do expect that they'll continue. I wish I had a great answer. I wish we could solve this. I do worry that we'll probably see more of this activity until things get a little bit better but I do hope that the future indictments, future arrests help curb this activity.

Luke McNamara*:*

So shifting gears a little bit looking at the rest of the threat landscape on the victims' side or what we're seeing on the front lines, any notable changes in TTPs or tooling that we've seen this year or we're seeing continue? I think 1 of the more interesting ones that we've seen for some years and I think it's still continuing is the usage of publicly available malware, the 12 Tools, Red Teamer Tools, particularly in kind of early stages of operations, even being used by some of the more advanced and well-resourced groups that we track. We're continuing to see that sort of activity, correct?

Charles Carmakal:

Yeah, absolutely. So I think the public offensive security tools, it enables new threat actors to enter the game that can leverage a lot of the tools that are available. Obviously legitimate security professionals could also leverage the tools and so it definitely does make it a little bit easier for criminals and for security testers to be able to leverage what's out there. But then I also think that there's an element of some of the more advanced groups tend to want to use and stick to only using publicly available tools or commercially available tools because what that does is it helps them mask who the identity of the threat actors actually are. And so there's times when we investigate APT 28 intrusions. So APT 28 is a group based out of Russia that conducts a number of high-profile intrusions and there are cases and situations where we've seen APT 28 only use publicly available tooling.

I distinctly remember conducting this in a response engagement at an organization that we believed was infected by APT 28 but when we looked at the tooling that was used we only saw the use of publicly available tools like sqlmap and a few other things. But the infrastructure that was used was only toward exit nodes and so if you just look at the technical tooling and the infrastructure you really couldn't tell who was actually behind the intrusion. And then to actually even further complicate things 1 of the Russian personas that was used for several years was Anonymous Poland and I distinctly remember seeing a video on YouTube of somebody from Anonymous Poland running sqlmap against a website and you know some of the folks on the instant response team that I was helping this organization saw this and said, "Hey, there's no way this is APT 28. We see Anonymous Poland running this scan and what we're seeing in this YouTube video matches exactly what we're actually seeing in the logs." And to me it actually felt like classic Russian disinformation. They wanted to muddy the water for us, they wanted to confuse us, they wanted to make it look like it was somebody else, a group of unsophisticated criminals that – or unsophisticated kids that were conducting the intrusion and they threw a number of false flags out there.

So we were able to connect the dots and determine with a high level of confidence that we were dealing with APT 28 because of some of the other connections that we were able to make from this intrusion and other intrusion sets but it's just interesting to see the usage of publicly available tools as far as some of the intrusions that we respond to. I think we're going to continue to see more though.

Luke McNamara:

And do you think organizations are more aware now? I mean as you noted this is not something that's incredibly new, at least been going on for the last several years. Do you think organizations are now being more cognoscente about that so that if they're concerned with being targeted by any number of these groups that are using these tools that their consideration of tools like PowerShell Empire or Cobalt Strike, Beacon, some of these frameworks and tools that are being utilized that they're treating those as something that may be boutique and custom to 1 group?

Charles Carmakal:

I don't think so. I think maybe the more publicly available tool, the more publicly available a tool is maybe the less organizations in general think the impact of a de-identification of that is in their network. And so if the tools commonly used, and generally speaking a lot of companies may feel like that's a pentester that's conducting an attack or a simulated attack against my environment or maybe that's an unsophisticated criminal, so I think generally speaking that might be the case. Now obviously there's lots of folks that are in the now and they recognize that a lot of advanced attackers or more impactful attackers use commercially available or publicly available attack frameworks like the Cobalt Strikes of the world and Metasploit and other things like that, so I guess it just depends on the maturity of the organization but there's definitely a fair number of people that feel like the more public something is the less sophisticated it actually is.

Luke McNamara:

Yeah, that's a good point. Moving on to talk about cybersecurity in the era of the pandemic and COVID-19, how have you seen customers adapt to carrying out security and are there specific challenges that you're seeing with organizations that are now not just having remote workforces but part of that being remote security workforces? I guess I'm thinking in particular not to go back to ransomware but some of the stats that came out last year I think in M-Trends about 75 percent of ransomware being deployed in off hours either on the weekends or after peak workday and you could imagine the impact now with folks working strange hours with having kids in the family, having to adjust to that. Are we seeing any sort of impact with organizations that we're working with to help prevent some of these things?

Charles Carmakal:

Yeah, so I'll tell you probably the first major question or concern that arose during the work-from-home mandate of COVID was many organizations out there really struggled with VPN capacity. All of a sudden the entire workforce had to remotely connect into a network and you found lots of organizations that just simply didn't have the capacity and the bandwidth or the licenses to be able to support that many people concurrently accessing their VPN. And so what we found were a lot of organizations reaching out to us asking us what's the risk, the real risk of enabling split tunneling on their VPN infrastructure because a lot of people working from home you know in addition to working they want to stream music or they want to stream television shows or sports and many organizations' VPNs just couldn't handle the capacity and they wanted to be able to route the work traffic through the VPN but other traffic, social media traffic or other kinds of media traffic directly out of the employee's internet connection so that was the first challenge.

And then as you can imagine if you have split tunneling enabled then there's a really good chance that you're not actually seeing all the network traffic that's going out of the system and you're probably going to miss malicious traffic that could be exiting the system. And so when people work from home they tend to use their computers differently than when they work at the office. And so working from home people tend to install software that maybe they wouldn't otherwise install if they were at the office, they may visit websites that they wouldn't otherwise visit if they were at the office, and so it obviously increases the likelihood that individuals may get malware infections or other types of unwanted software on your computers that organizations just simply can't monitor for and control so that's become a challenge.

Another challenge that we noticed is in other parts of the world we found that a number of employees just didn't have corporate-issued laptops and so they ended up needing to use personal laptops or personal desktops to be able to access the company network and that's obviously a problem because if you're using a shared device you may have family members that might install games or other things on the computer that might introduce other security risks and deterrents on the device itself. And so there were definitely a lot of concerns that our companies had to understand and address when they moved to a COVID world. And from a response perspective 1 of the challenges that we have is sometimes the laptops people use never actually connect to the corporate network and so for us to do an investigation of somebody's asset it may be difficult for our clients to push out forensic software to computers or to be able to acquire data that they need from those machines because those computers may never connect to the VPN, they may never connect to a server in which the organization can push out patches.

So it can add some complexity and some challenges but you know from our perspective, at least from an IR perspective because we have a lot of tooling that allows us to do our incident response work remotely we haven't had much of an impact at Mandiant so we have been able to do very large-scale enterprise-wide incident response engagements 100 percent virtually by leveraging software to remotely acquire data from systems. And then we have historically wanted to go on-site to see our clients, to meet with them face-to-face, to exchange information with them, to whiteboard things with them, and in the meantime we've just had to make use of the collaboration tools that are available to us to video chat with each other, to share documents, to live edit things, and we've found that transition for us wasn't actually hard at all.

Luke McNamara:

I know everyone has different perspectives on remote working both at the organizational level and also the individual. Do you foresee any of the changes that we've made to maybe how we do business with incident response and going on customer sites, do you foresee any of these changes sticking after the pandemic?

Charles Carmakal:

You know it's probable that some of the changes that we've made now will continue to exist. I do expect that a number of folks will end up working from home at least more so than they have in the past. I've still got a little bit of an old school mentality. I prefer to have people in the office because I think there's so much learning and collaboration that happens when people are face-to-face with each other and sometimes you just hear things by physically being around them that you may not be able to hear through the virtualization platforms that we have available to us. So I personally plan to come back to the office when things are safe. I'd love for the team to come back to the office, but it's probably going to look and feel different than it has in the past. We probably won't have the same in-office attendance that we used to have but we would like to get back to the point where people come in.

I'd also like to hop on a plane again and start to see my clients face-to-face and go out to lunch with them, go out to dinners, and I really hope that we get back to a situation where that becomes the norm where we can see people face-to-face and share experiences with them. But I do wonder for the simply things like shaking people's hands. Will people shake hands in 2021 and 2022 and beyond or will we be doing fist bumps or elbow bumps? I don't know if that's going to change but it's definitely going to change the way we operate moving forward and some of these things that we've become accustomed to in the past several months we'll probably stick with it for quite a while.

Luke McNamara:

Yeah, I definitely do not miss the rush hour traffic in the DC area but you are right from a collaboration standpoint that you just get by being in the office and fortuitously bumping into someone who's working on something.

Charles Carmakal:

Yeah, no doubt.

Luke McNamara:

Kind of wrapping this up and as we're sitting here recording this in early September, so pre M-Trends reports although the work on collating all that data will be starting soon, any predictions you want to leave us with or things that we should be watching develop as trends, maybe a continuation of something or the emergence of something?

Charles Carmakal:

Yeah, you know the way I typically predict trends or predict what might happen in the future is I tend to look back in time and try to figure out what were the trends we observed over the past 12 to 24 months I expect we're just going to see more of that. So I expect to see more disruptive attacks, I expect to see more extortion, I expect to see more threat actors making a lot of money in the process. I do expect to see a resurgence in state-sponsored threat activity. We're probably going to continue to see the big countries continuing to engage in their offensive operations. Outside of cyber I expect to see an increase in human adversaries stealing information from organizations so the insider threat is going to – I believe will be much more noticed in 2021 and beyond and I think we've actually started seeing a fair volume of insider activity for the past few years. There are a number of situations where as an example Chinese nationals have stolen intellectual property from research organizations, healthcare organizations, oil and gas companies, other high-tech organizations, and I do believe that we're going to see more of that.

We've also seen insiders conduct criminal operations and steal data from their organizations and reach back out to their CEOs and to their boards and pretend to be external hackers that hacked into the company that are asking for $500,000 or $1 million to not publish the data that they've stolen. And so I think a lot of those malicious insider activity has actually occurred for quite some time. I just think it's hard to identify and it's hard to prove malicious intent, but I think in time we'll probably end up seeing more of it. And maybe it's not because more of it's happening but it's just because we're keeping a closer eye on it and we're expecting it more than we have in the past.

Luke McNamara:

Yeah and it'll be interesting to see if the continued work-from-home situations of a lot of organizations exacerbates some of that activity as well.

Charles Carmakal:

Yeah, it certainly could.

Luke McNamara:

Well Charles, thank you for your time and your insights here. We'll definitely have to have you back on at some point in the future and maybe you can talk about how the threats have changed since then and point to all the things you noted here and got right.

Charles Carmakal:

Awesome, good deal. Well thanks for inviting me Luke.

Luke McNamara:

Take care Charles.

Charles Carmakal:

Excellent.