RANSOMWARE IS NOT GOING AWAY

Evaluating trends in the cyber threat landscape: A conversation with Mandiant

| JULY 2021

CYBERSECURITY GLOBAL CONVERSATION SERIES

As cybersecurity threats continue to evolve, organizations face challenges from both a technical and reputational perspective. Monitoring emerging and growing trends, like ransomware, can help companies avoid trouble spots that can lead to harmful compromise.

In the latest installment of Finsbury Glover Hering's global cybersecurity conversation series, Global Managing Partner Paul Holmes and Managing Director Mike Dolan spoke with Manny Jean-Georges, Manager, and Brice Daniels, Director, at Mandiant Consulting, a leading provider of incident response, strategic readiness, technical assurance and security training services. The following is part one of a two-part series in this conversation and has been edited for length.

Mike: Looking back on 2020, what are some of the common characteristics among companies that handled cyber incidents successfully from your perspective? And less successfully?

Manny: In 2020, it certainly seemed like there was a dramatic increase in the number of intrusions. Organizations that handled it best were able to react quickly — especially when we're considering things like ransomware. So, recognizing the signs that they were the victim of an intrusion. Most importantly, organizations that were prepared to engage and respond were in a better position. For instance, having incident response retainers in place with a security or IR firm may have allowed organizations to more quickly and effectively respond to these incidents.

Conversely, I'd say organizations that weren't able to respond as well fall into two categories: First, some larger organizations may be less agile due to factors like network complexity, making it difficult for them to respond appropriately, and second, some smaller organizations lack the security staff and capabilities to respond effectively to today's modern threats.

Brice: And I think that, for some incidents, some organizations respond intuitively, but their natural response may hinder what we would do from an investigative standpoint—which can sometimes set an organization back. For example, is it always the best idea to unplug or completely disconnect systems during a ransomware incident, versus other alternatives like restricting network traffic?

Those are not necessarily decisions that can be easily made in the heat of the moment. Having a relationship with an incident response organization, or at least having some tabletop exercise experience, gives the type of support an organization would benefit from in terms of being ready to respond. It's really important to give thought, at the executive and practitioner levels, to how you're going to respond not only technically, but with regard to strategic business and operational decisions as well.

Paul: Manny, you mentioned that ransomware had been a significant theme in 2020. If you had one piece of advice that you would give a company or an organization to prevent or prepare for a ransomware incident, what would it be?

Manny: A primary piece of advice I'd provide is regarding network visibility and overall visibility into the assets within a client's environment. Organizations that can quickly understand what systems are impacted are going to fare better than organizations that don't have a good understanding of what certain systems are, where those systems are located on the network—and the data that is stored and where that data resides.

As reported in M-Trends 2021, with one of every four Mandiant incident response engagements in 2020 involving ransomware, a growing trend that we've seen is threat actors stealing data to use for extortion prior to ransoming or encrypting devices. This is now often referred to as double extortion ransomware or multifaceted extortion attacks. Therefore, being able to understand what data was impacted, where the threat actor could have accessed that data, and how it could have gone out—is equally as important.

We also reported that organizations are detecting these types of attacks inside their networks quickly, with a median global dwell time of only five days, likely due to the immediately noticeable impact.

Investing in services like proactive ransomware assessments can significantly help an organization prepare for the onset of one of today's most common and destructive attacks.

> A growing trend that we've seen is threat actors stealing data to use for extortion prior to ransoming or encrypting devices.

Mike: It seems like the sophistication of cyber threats and their impact is increasing exponentially every year. Do you think we're on that kind of trajectory for good? What do you anticipate the rest of 2021 will look like from a cyber-risk perspective?

Manny: There's been a resurgence of espionage-based threat activity, including the SolarWinds compromise in 2020, as well as the Microsoft Exchange vulnerabilities and exploitation disclosed in early 2021. Attacker behaviors will likely be motivated by geopolitical events and classic espionage-related types of incidents.

But I also don't see ransomware or ransomware-related extortion slowing down at all either. We continue to see different evolutions of ransomware and how ransomware operators are acting. For instance, we know of one threat actor who has started to go after not only devices themselves but, for example, also targeting virtual machines, the VM host and hypervisor for encryption as well. That's something we haven't seen before.

Brice: Manny mentioned that ransomware is not going away, and he's right. There have been financially-motivated attackers for decades, and in my opinion, there will continue to be increasing sophistication because of the fact that there is so much money to make from ransomware and extortion. And as we raise the bar to protect our clients, these attackers are going to continue to look for the next lowest-hanging fruit.

> Ransomware is not going away. And as we raise the bar to protect our clients, these attackers are going to continue to look for the next lowest-hanging fruit.

Paul: Are particular types of organizations being targeted right now by threat actors? Is it particular industries like health care, or is it organizations with specific political affiliations? Or is it companies from which the threat actors can spread out and get in elsewhere?

Brice: First and foremost, no one is exempt from cyber attacks. We were just talking about the prevalence of ransomware actors using whatever they can find to make money. As such, attackers often don't care who they attack if they think they will get paid. There might be a situation where a large organization lacks cohesion because it grew through acquisition or something similar, which increased its attack surface and made it more vulnerable because of the patchwork of IT practices and security. That patchwork denies it visibility and may introduce low-hanging fruit vulnerabilities as well.

> No one is exempt from cyber attacks. Attackers often don't care who they attack if they think they will get paid.

Manny: The classic espionage-type of activity and nation-state actors will continue to target organizations within critical industries such as defense and high-technology. From a ransomware and extortion perspective, one trend that we saw over the last year was the targeting of hospitals as well as cities and municipalities. These victims were susceptible because they often run legacy systems and may not have the budget of a Fortune 500 company to allocate proper safeguard investments in cybersecurity. Regardless of budget, there are proactive measures that can be taken to reduce the attack surface and make it more costly for an attacker to successfully complete an attack. For example, performing an audit of privileged accounts within Active Directory only costs time.

Mike: As criminal organizations have increasingly used ransomware as kind of a business model, has that impacted how you see companies or organizations responding?

Brice: We do get the feeling that there is commoditization of various types of the attacker lifecycle, if you will. We may be seeing this show up significantly in our data as M-Trends 2021 reported that in just under 30% of all intrusions, multiple threat groups were active in one single environment, which is nearly double in comparison to our previous report. So, one attack group may focus simply on gaining access to a company. They work simply on phishing, getting the initial payload into the environment, etc. Then, a subsequent attacker simply buys access into the target environment so they can then use that access to deploy the ransomware. From there, the latter attacker would monetize it. At this point, attackers often focus on what they're good at — specialization works well for maximizing their profit, and that can complicate things for defenders since every organization can be targeted when the substantial motivation is profit.

BRICE DANIELS

Director, Mandiant

brice.daniels@mandiant.com

MANNY JEAN-GEORGES

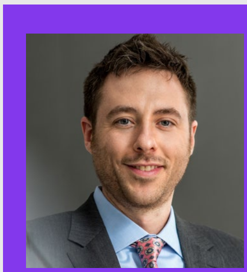
Manager, Mandiant

Emmanuel.Jean-Georges
@mandiant.com

PAUL HOLMES

Global Managing Partner,
Finsbury Glover Hering

Paul.Holmes@fgh.com



MIKE DOLAN

Managing Director,
Finsbury Glover Hering

Mike.Dolan@fgh.com

NEW YORK

+1 646 805 2000 | enquiries-us@fgh.com