Podcast Transcript

2022 DSIR Report Deeper Dive: Forensics

Date: July 6, 2022

Guest: Joseph Bruemmer **Host:** Amy Kattman

Run Time: 14:29

For questions and comments contact:

Joseph L. Bruemmer

Partner
Cincinnati
T:
1.513.929.3410 | jbruemmer@bakerlaw.com

Kattman: Ransomware, MFA, extortion, fraudulent fund transfer schemes, these topics and many others make up the key finding section of the Eighth Annual Data Security Incident Response Report, informally known as the DSIR Report. Each year, the incident response attorneys within the Digital Assets and Data Management Group, or DATM, provide statistics and analytics around the incidents they encountered the previous year in a report that is eagerly received by clients, vendors, media outlets, and frankly anyone interested in or tasked with their company's digital assets and risks. I'm Amy Kattman and you're listening to BakerHosts.

This, our third episode in the series exploring the 2022 DSIR Report, discusses forensics in depth, the importance of proper configuration and monitoring when building your defense against security incidents. Our guest today is Joe Bruemmer, partner and member of our Digital Risk Advisory and Cyber Security team. Welcome to the show, Joe.

Bruemmer: Thanks Amy, glad to be here.

Kattman: Joe, can you tell us what types of trends you are noticing in network intrusions and ransomware?

Bruemmer: Definitely. So, many of the trends that we observed in 2020 continued into 2021 and partly into 2022. Network intrusions and ransomware were in full force over the past couple of years, representing more than half of the incidents that we handled in 2021. Threat actors have continued to encrypt data and to steal data, but they're also trying other tactics to try to apply pressure on companies to pay their ransoms. They have resorted to distributed denial of service attacks, they've contacted company employees by e-mail and phone call to threaten them if ransoms aren't paid, and they've been looking for new targets in company networks like Linux-based systems.

The threat actors are also leveraging the data stolen during ransomware incidents for other purposes like business e-mail compromise and wire transfer fraud, and one thing with the war in Ukraine, we have seen the pace of ransomware slow in the first two quarters of 2022, but I don't think organizations would be well served by mistaking this lull for the demise of ransomware. I think instead they should view this as a temporary factor and use it as an opportunity to strengthen their defenses so that if ransomware experiences a resurgence, which I think is going to happen, they're in a better position to respond to and prevent it.

Kattman: Now that we've talked about the trends, let us talk about how companies have been combating these trends.

Bruemmer: Yes, ransomware has been all over the news for the past couple of years as we've seen, and organizations have become increasingly aware of the threat that it poses. More and more clients are implementing a variety of tools to help combat ransomware, among them multi factor authentication or MFA, endpoint detection and response tools, or EDR, and immutable backups, but it is not enough to just have the tools. You have to make sure that they're appropriately configured and monitored, so consider endpoint detection and response tools, or EDR tools. What those tools are, are tools that can provide companies with the ability to monitor the devices on which they're deployed in real time, and then remotely contain and remediate unauthorized activity.

So, if you see a legitimate user account behaving in a strange way, EDR tools will pick up that activity and they will either block it or alert on it, and one thing that I just said is block or alert. That is because EDR tools can be configured either to just detect the activity or to block it. If you don't configure the tools to block the activity, then what you may find is that they fired an alert at some time in the wee hours of the morning when the threat actors typically launch their attacks, no one was monitoring it, you wake up the next morning to find that your devices are encrypted even with the EDR tool because no one was there to actually stop the activity. Whereas if you've configured the tool to block unauthorized activity, you will have a better chance of preventing that kind of stuff from occurring.

Another feature with these tools is that they have an anti-tampering mechanism that companies can enable so that even if a bad guy gets access to administrator level credentials or the keys to the kingdom, they can't just log into the management console for the tool and disable it. We have certainly seen instances where companies have not enabled that feature, and bad guys have gotten in, gotten administrative level credentials, logged into the management console that the companies use to manage the EDR tools, and have simply disabled or uninstalled them from devices. So, even though companies thought they were protected, they find all of these devices encrypted with ransomware because the tool was just removed.

Kattman: These are really good points. One way to limit the risk of ransomware attacks is to employ a Zero Trust framework. Could you tell us a little bit about Zero Trust and how it works?

Bruemmer: Sure. I'm going to give you a technical definition of what Zero Trust is, and then I'm going to try to explain it in simpler terms. So, Forrester defines Zero Trust is an information security model that denies access to applications and data by default. Threat prevention is achieved by only granting access to networks and workloads utilizing policy informed by continuous, contextual risk-based verification across users and their associated devices.

So, what does that actually mean? I think the easiest way to figure out what that means is to compare it with the traditional cyber security model. So, in a traditional model, once users sign into a network using their username and password or authenticate to the network as it is called, they will have the ability to access applications and data that they are authorized to access. So, if you want to access your e-mail after you signed in, you can access your e-mail. If you want to access your network share drive where you've stored a bunch of documents, you can access it, and if you want to access a company intranet page, you would have the rights to access that page.

With Zero Trust though, there are going to be additional security challenges as you try to access those different applications or as you try to access particular data, and in the case of IT personnel, there may be additional security challenges as they try to access additional devices. Those security challenges could take a number of forms. It could be that you need to re-enter your username and password, it could be that you need to approve another MFA prompt, or it could be something else. Zero Trust also leverages a number of enhanced security tools to monitor the activity that is going on in the environment to look for things that are out of the ordinary, so that the information security team can take steps to investigate and, if necessary, contain it.

The reason that Zero Trust is important is because it can be an effective way to limit the scope of network intrusions. What bad guys typically do once they get a foothold in the network on a particular device, is that they will conduct network reconnaissance to see what other devices are connected to the one to which they gained access. They will try to harvest credentials with the end goal of getting access to credentials that have elevated privileges that give them more rights on systems than the ones that they initially got, may have, and then they will use that enhanced or privileged access to move to other devices in the network to then steal data and deploy ransomware.

Zero Trust puts additional roadblocks in their way so that just by gaining access to one set of credentials, they don't necessarily have the ability to move to an unlimited number of devices or applications in the environment.

Kattman: More and more organizations are moving to the cloud in order to secure their digital assets. What type of risk does a cloud based environment present?

Bruemmer: Cloud environments have their own risks, just as on-premises environments do. Without proper controls for creation, tracking, and maintenance of cloud based data and assets, organizations may find they no longer have a comprehensive picture of what assets they have and what data is stored in them. We have seen situations in which companies didn't have controls in place to prevent their employees from creating cloud assets while on the company network.

So, it is not that the employees are doing anything malicious necessarily, they're just creating these unauthorized cloud instances that the companies don't have knowledge of, and then they're putting company data up on those cloud instances. The reason that becomes a problem is because employees are not always configuring these instances properly. So, it used to be the case that some cloud storage containers were set by default to be publicly accessible. If employees don't know what they're doing when they're creating these containers, they may inadvertently set the permissions to be publicly accessible and then put company trade secrets in those buckets.

Bad guys will frequently scan the internet to find accessible cloud assets, and then they'll take data from them. And we have certainly handled a number of matters where company employees without the company's knowledge set up these assets, put company trade secrets in the online storage containers, and then the company gets a message from a threat actor that says we have your source code or we have all of this employee data, and the company had no idea that that information was even in the cloud.

Another thing that you can see is that even if companies do have controls in place for the creation of the cloud assets, if you're not keeping an inventory of them, you may find that with the passage of years you have lost track of all the ones that you're you've created because they're so easy to spin up. And so, you know, we've had matters where companies knew that these assets existed at one point in time, forgot about them, forgot to update the security controls in place in them, and then threat actors got access and stole data. A third thing to keep in mind is that you need to make sure that the cloud assets have the same level of security control over them that you have for your on-premises environments.

We've had any number of matters where after the company has discovered that there has been unauthorized access, we've engaged a forensic firm to conduct an investigation. The forensic firm goes into the cloud instance and finds that there is not sufficient logging enabled to help them identify what specific objects in the cloud bucket were accessed, even though they would have that level of logging enabled in their on-premises environment. Or they may find that they did not have the same security tools in place in the cloud environment that they had in their on-premises environment, so making sure if you move to a cloud asset that you have controls in place for the provisioning of the asset, inventorying the asset, and securing the asset are critical.

Kattman: It sounds like there is no one way to prevent these types of incidents, so how should a company plan their defense?

Bruemmer: The best defensive approach that you can take is one that is called defense in depth, where you layer multiple security tools on top of each other so that there is not an easy way to, for unauthorized activity to go undetected. So, think about it in terms of the tools that we've discussed already on this podcast. Multi factor authentication or MFA, endpoint detection and response tools, or EDR, and immutable backups.

If you have multi factor authentication it reduces the chance that the threat actor is going to be able to use a set of compromised credentials to get access to your network because they are going to be prompted, or the employee that has legitimate usage of those credentials is going to be prompted to hit an approve button or enter a code when the bad guy tries to log in, and it increases the chance that the employee is going to say, well, that is not right. I wasn't trying to log in right now. I'm not going to approve this prompt. The endpoint detection and response tool increases the chance that you'll be able to identify and stop an unauthorized actor if an employee inadvertently approves MFA.

So, as I mentioned earlier, an EDR tool gives you visibility into unauthorized or anomalous activity, so that even if an employee inadvertently hits allow on an MFA prompt, which we have seen, your security team is going to see that the account associated with that employee is behaving in unusual ways and it will give them an opportunity to look into it and block that activity if necessary. And then, immutable backups will give you a better chance of recovering if an employee inadvertently approves an MFA prompt. Your EDR tool does not detect the activity or the security team monitoring it does not see the activity, and the bad guys is able to encrypt the devices. If you have immutable backups, and even though the bad guy got through the first two controls, you still have this repository of data that you can use to restore the encrypted devices.

So, the take away is that each of those tools on their own provide valuable protection but taken together and in combination with other security tools, because it is not like those three will provide a comprehensive security framework. You will have a better chance of being able to defend against and recover from a ransomware attack.

Kattman: Joe, do you have any final thoughts that you'd like to share with our listeners today?

Bruemmer: Yes. I mentioned at the outset that we have seen a little bit of a lull in ransomware activity over the first two quarters of the year. I think organizations should use this as an opportunity to enhance their defenses, so that if and when we do see a resurgence in ransomware, they're not caught on their heels, and they are prepared for it.

Kattman: Joe, thanks for joining us today and sharing this very valuable information.

Bruemmer: My pleasure Amy. I appreciate you having me.

Kattman: If you have any questions for Joe, his contact information is in the show notes. As always, thanks for listening to BakerHosts. Comments heard on BakerHosts are for informational purposes and should not be construed as legal advice regarding any specific facts or circumstances. Listeners should not act upon the information provided on BakerHosts without first consulting with a lawyer directly. The opinions expressed on BakerHosts are those of participants appearing on the program and do not necessarily reflect those of the firm. For more information about our practices and experience, please visit bakerlaw.com.