CUSTOMER Q&A

RSA CUSTOMER COMBATS WEB SHELL ATTACK WITH RSA NETWITNESS® LOGS AND PACKETS AND RSA NETWITNESS ENDPOINT

AT A GLANCE

Challenges

- A large US organization received an alert from the FBI that its data had been accessed and compromised.
- Behind the scenes, two long-term advanced persistent threats (APTs) were at work.
- The company lacked visibility of network and end points and so struggled to identify threats in a timely manner.

Results

- RSA NetWitness Logs and Packets and RSA NetWitness Endpoint provided detailed insight and visibility into the two APTs, plus other potential threats and issues.
- RSA Security assisted with a remediation plan that stopped the attackers in their tracks.
- The client is now much more security conscious and has taken steps to enhance its security strategy and culture moving forward.

"The reason for installing RSA NetWitness Logs and Packets and RSA NetWitness Endpoint was to provide the visibility that we needed to adequately investigate the incident. Without having that full visibility, being able to see the network internally and externally, as well as what was happening on the end points, we wouldn't have been able to give the client the full picture."

JARED MYERS, INCIDENT RESPONDER, RSA SECURITY

RSA

A large US organization was alerted by the FBI that some of its sensitive data had been accessed and exfiltrated. It called in RSA Security to help address and remediate the incident. RSA NetWitness Logs and Packets and RSA NetWitness Endpoint provided visibility of activity across network and end points, enabling the team to identify two ongoing threats, remediate them and create a stronger security foundation for the future.

What was the client's situation?

This client operates primarily inside the US although it does have some international presence. It employs around 1,000 people and had about 2,000 end points. It develops software for use by the government and the military.

The FBI had contacted the organization to advise that it had identified some data that had been exfiltrated from the organization's network. It needed to find out what had happened and put a stop to any potential threats.

How did RSA help respond to the FBI alert?

By installing RSA NetWitness Logs and Packets and RSA NetWitness Endpoint on the network, we saw that the client had lots of smaller problems as well as the main event that the FBI had identified. It was very eye opening for us and the client. We were able to see malware beaconing as well as the web shells that the adversary was using to come into the environment. We could also see what the adversary was doing inside the environment, the systems that they were targeting, the accounts that they were using, and the type of data that they were going after.

What approaches was the adversary using?

What most organizations fail to realise a lot of times is that these attacks are often very well choreographed. A lot of reconnaissance went in this particular engagement. They engaged a sales representative for the company and even knew that he had recently presented at a trade show. When they engaged the sales representative in a dialogue they said that they had seen him speak and that they wanted to know more. Three or four email conversations actually went back and forth before they provided the sales person with what ended up being a malicious document.

They were also brute forcing some of the perimeter devices as well. Although the client wasn't using default passwords, it only took the adversary about 9,000 tries to guess the password, which seems like a lot but it only takes a couple of minutes to try that many passwords. Once they'd found the credentials they were able to upload malware and web shells on to the server. This was one of the adversary's main ways into and out of the network.

Would you say this was an advanced persistent threat (APT)?

Yes I would. It was a very targeted attack: it wasn't opportunistic. The adversary obviously knew that this organization was developing software of interest, they did due diligence to know who would be a likely target that would help them get a foot in the door, and then once they did that the malware that they used specifically had the client's name in it as a configuration. They used C2s that we had not seen used elsewhere. All this makes it clear that they wanted to make sure that this was successful, that their base of operations was not going to show up elsewhere on some black list that's used for commodity malware.

Why did you use RSA NetWitness Logs and Packets and RSA NetWitness Endpoint to respond to this incident?

The reason for installing RSA NetWitness Logs and Packets and RSA NetWitness Endpoint was to provide the visibility that we needed to adequately investigate the incident. Without having that full visibility, being able to see the network internally and externally, as well as what was happening on the end points, we wouldn't have been able to give the client the full picture. What the client was notified of by law enforcement was just a small piece of the pie, so we wanted to provide the entire picture and scope everything out to let the security team know exactly what had occurred on the network.

When we looked at the logs and some of the other artefacts that we were able to recover from the end points, we saw that there had actually been two distinct intrusions. One was from approximately two years ago and the other one had been ongoing for almost three years.

Once we had visibility across the network and the end points, it took us about a week to really scope out the incident.

How did RSA Security help set the appropriate level of response?

Once we were actually able to show the client what data had been taken and how long this incident had been going on, we worked very closely with the security team on reacting versus overreacting.

A lot of organizations immediately want to start reimaging servers and completely shut things off, but we were able to help the client understand that we needed to completely remove this adversary from its environment. Although the client had already sustained quite a bit of exposure, we suggested monitoring for a week to give us time to scope out the incident and develop a plan to make sure that remediation was successful.

How was remediation handled and what was the adversary's response?

During the investigation up to the remediation process we were using RSA NetWitness Logs and Packets and RSA NetWitness Endpoint to track the adversary's actions. Even though the majority of data had already been taken in the years prior, they were still coming back fairly regularly to get deltas of intellectual property and communications between higher-ups in the

company. So we were able to use NetWitness Logs and Packets to track the actions and observe the characteristics that they typically used inside the network, the accounts that they were using, even the times when they were coming and going so that we had a good idea of when to expect them, to try to renter the network.

The remediation aspect as far as the actual takeback only took about a day. Once we remediated this client, we saw the adversary try to come back in a couple of times. Initially they went back and tried to engage in a dialog again with the sales representative but because the attack had gone on for so long he was no longer there. Then they went back to the perimeter, looking at some of the different web applications that they had been running. We've seen over the last couple of months that they continue with some of these spear fishing attempts.

What difference have RSA NetWitness Logs and Packets and RSA NetWitness Endpoint made?

Had RSA NetWitness Logs and Packets and RSA NetWitness Endpoint been installed at the client's site before this incident, it would have helped the efficiency of our investigation quite a bit. They could have had a lot of logs already pulled in, and we would have had network traffic as well as some of the netflow. This would have boosted the efficiency with which we were able to scope it, therefore decreasing the client's exposure time.

Once we deployed RSA NetWitness Logs and Packets and RSA NetWitness Endpoint the company was surprised to see some of the problems that they had. RSA NetWitness Logs and Packets enabled us to see different commodity malware that had been beaconing. We looked into it and some of it had been there months, but AV had still not picked up on it.

With RSA NetWitness Endpoint we were able to see some banking malware that had also been installed. Some of these learnings were opportunistic, but once separated the wheat from the chaff we were able to actually flag to the client things that need to be taken care of even if they were not relevant to the ongoing investigation.

What impact did the attack have on internal attitudes to security?

The organization never considered itself a target up until this incident, and it actually helped to engage a dialog with the corporate board that focused on the need to put more resources towards security. As a result, the company completely overhauled its security, putting additional technology in place and hiring additional people to almost double the security team.

What actions has the client taken in the wake of this incident?

After the incident was completely remediated, the client air gapped some of its sensitive data, so that only people in a central location could access it. This greatly reduced any attacker's opportunities to get at some of the more sensitive intellectual property. The client also implemented things like two-factor authentication. It completely overhauled some of its technology and took a look at some of its existing technology and decided that it was not getting out of it what it needed. So it replaced some of its firewalls, as well as its SIEM component with RSA NetWitness Logs and Packets for logging.

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.rsa.com