CUSTOMER Q&A

RSA CUSTOMER OVERCOMES DRIVE-BY ATTACK AND LAYS SECURE FOUNDATIONS WITH RSA NETWITNESS® ENDPOINT AND RSA NETWITNESS LOGS AND PACKETS

AT A GLANCE

Challenges

- A large global organization, with 60,000 end points, had been targeted by an advanced persistent threat for over nine months.
- Zero-day drive-by attacks were also compromising security.
- A lack of visibility across end points and network traffic meant these threats went unnoticed.

Results

- A proof-of-concept of RSA NetWitness Logs and Packets and RSA NetWitness Endpoint identified a large-scale campaign to steal credit card information, and was able to respond within hours.
- RSA Security performed a full analysis of the threat and helped create a remediation plan that enabled takeback of the environment within one day.
- With RSA NetWitness Logs and Packets and RSA NetWitness Endpoint in place moving forward, the client has greater visibility and understanding to inform a stronger security strategy.

"By sifting through network segments and all the commands being run on the end points, RSA NetWitness Logs and Packets and RSA NetWitness Endpoint enable the security team to gain instantaneous access to and visibility of overall network activity. This then allows them to detect and respond to a compromise within hours instead of months."

BRIAN BASKIN, INCIDENT RESPONDER, RSA SECURITY

RSA

When carrying out a proof-of-concept for RSA NetWitness Logs and Packets and RSA NetWitness Endpoint with a large global company, RSA identified an advanced persistent threat that had culminated in a drive-by attack that compromised the organizations data security. The RSA Security team worked with the client to analyze and mitigate the threat, and to create a more robust security posture for the future.

What was the client's situation?

This client is a large global organization, which processes tens of thousands of transactions through credit card information on a weekly basis. It has 60,000 end points across the world, each segregated across 2,000 network segments for each of its business properties.

The client's global environment was compromised due to a drive-by attack. The adversary used the registry to store shell code and to cause additional attacks within the environment. Using WMI and Powershell, they moved around, collected and archived information.

Why was this attack so serious?

We view this attack as part of an advanced persistent threat (APT) based on the expertise of the attacker. They were able to use very customized shell code that was modified from existing crime-ware in such a way that it was not detectable by any antivirus applications or by most of the security applications being used by this environment.

Once we started looking into it, we also found that the threat had been in place for as much as nine months prior to the compromise.

The other reason for this attack's success was its use of zero-day drive-bys at the onset. The tools the client was using offered only very limited detection and investigation, which made these drive-bys difficult to spot.

What security tools was the client using before the attack?

Prior to this compromise the organization was using very standard security tools, including antivirus, weblogs and proxy logs, which gave the security team very limited insight. They saw alerts and overall connections but not actual context or security information regarding those connections. The tools simply grabbed information about just the end points and network connections.

The adversary's actions were very successful because as they weren't using malware, there was no alerting capability. There was nothing with these standard security tools to actually let the team know that something malicious was taking place.

How did RSA become involved in the response?

The organization performed regular security health checks across its environment, and it called RSA Security to perform a proof of concept, using RSA NetWitness Logs and Packets to detect any gaps in visibility and any unknown or malicious activity in the environment.

Within a week of being on site and working through this proof of concept, RSA Security and the incident response team were able to detect various crimewear actions taking place, as well as a large-scale overall campaign to steal credit card information.

After detecting the compromise, we were able to detect that these connections were being made from two internal machines. By performing immediate triage on these systems we were able to identify multiple systems and network segments in play. From there we performed an investigation and performed an analysis across thousands of systems within a week to determine the entire open scope of this compromise.

How did RSA help respond to this threat?

Typically when RSA Security is called in to assist with incident response, we verify the indicators that are detected by the customer, but we also deploy RSA NetWitness Logs and Packets and RSA NetWitness Endpoint to gain additional visibility across the network and the end points. When we used RSA NetWitness Logs and Packets to look at the internal traffic, we saw much more lateral movement inside the environment that the client's tools were not actually monitoring. The information we saw going externally was through very simple, innocuous data that they typically would not see using their security tools.

By using RSA NetWitness Endpoint in the environment we were able to see native Windows components being used maliciously in the environment. There was no malware actually being used and placed on these systems, and we found that instead the adversary was using native applications to move around and steal information. By using RSA NetWitness Logs and Packets and RSA NetWitness Endpoint in this environment we gained additional context into connections being made. We were able to view not just a bad IP address or bad domain name, but any other unusual connections being made or strange traffic patterns in the network environment.

What value did RSA NetWitness Logs and Packets and RSA NetWitness Endpoint bring to the process?

The large amount of data collection from network segments all the way to end point host activity. By looking through this large amount of data and sifting through network segments and all the commands being run on the end points, the security team gains instantaneous access to and visibility of overall network activity. This then allows them to detect and respond to a compromise within hours instead of months.

What would have been different if the client had already been using RSA NetWitness Logs and Packets and RSA NetWitness Endpoint?

Had RSA NetWitness Logs and Packets and RSA NetWitness Endpoint been installed prior

to this compromise, the security team would have had additional insight into the compromised information. They would have been able to gather the drive-by attack, and assess the lateral movement and exfiltration of the data as they were occurring, instead of nine months later.

How did the client go about implementing a remediation plan?

As a very large organization with 60,000 end points and multiple network segments there were many stakeholders involved in creating a remediation plan. Once that plan was put in place, verified and reviewed we were able to perform a takeback of the environment within one day.

The incident response team ascertained every possible way that the adversary was gaining access to the environment and removing information from it. We monitored those accounts, the connections and the DNS names. Based on this comprehensive monitoring over multiple weeks we saw no additional usage of those accounts, nor any other indicators that were related to the initial compromise.

How will this experience help the client move forward?

After remediation had been performed by the client and additional comprehensive monitoring had been carried out by the incident response team, we conducted a performance knowledge transfer to the client, where we talked through the usage of RSA NetWitness Logs and Packets and RSA NetWitness Endpoint to allow them to find attacks similar to this one, as well as any possible follow-up attacks by this adversary.

Part of the follow-up is looking through their security defensive posture, finding any gaps of visibility, looking at how they could defend

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