Cloudy Days

More and more organizations are moving to the cloud to cut costs and simplify operations. But as this move takes place, it’s important to ensure security policies remain in place as well as review what third party providers are doing to protect assets.

In a recent instance, a FireEye Managed Defense Consultant (MDC) was called in to verify a client’s Cloud Provider’s findings after they started experiencing performance issues.

The client thought that their Cloud Provider would be monitoring their environment and alert on any compromises. Unfortunately, this proved to not be the case, especially when the provider tabled the issues until the following week and invoiced the client for additional bandwidth/utilization needed.

Upon engagement, the MDC discovered that the degradation was falsely attributed to a Windows based Trojan on a Linux server. The MDC was able to quickly determine the activity to be a Mirai malware variant and began efforts to ensure the client was fully protected.

Bottom line: Moving to the cloud also transfers risk to the cloud. Ensure that your cloud provider is fully protecting your assets and whatever on-prem security capabilities, expertise, policies, etc. are in place are also being leveraged in Cloud environments.

PROBLEM:
Reliance on cloud service provider to provide security.

HOW WE DID IT:
Correctly diagnosed third party findings and conducted a Rapid Response engagement to ensure the threat was contained and no other systems had been effected.

HOW WE DID IT BETTER:
Front line experience enabled Managed Defense to quickly review Cloud Providers findings and correctly attribute activity, launching into immediate remediation efforts after client waited 72+ hours for Cloud Provider to ‘fix’.

RESULT:
In under 8 hours, the FireEye team was able to determine the threat had been misdiagnosed, attribute it correctly and quickly eradicate to help ensure the client’s assets were secure.
Cloudy Days

Moving to the cloud also transfers risk to the cloud. It’s important to ensure that whatever security capabilities, expertise, policies, etc. are in place on-prem are also applied to a cloud environment to help ensure full protection.

Managed Defense can help to identify and disrupt malicious attackers quickly and effectively.

In this instance, the Managed Defense team was able to review third party findings, correctly diagnose and contain the threat within eight hours, saving the client from any financial damages occurring.
Cloudy Days
FULL STORY

Today, more and more organizations are moving to the cloud to cut costs and boost efficiencies. But sometimes, the “cheaper” solution in the short term might cost you more long term if not properly configured.

Organizations need to ensure that whatever on-prem security processes are in place are applied to cloud environments. They also need to vet and understand what third party providers, including Cloud Services, are doing to protect their valuable data.

In a recent instance, a FireEye Managed Defense Consultant was called in to verify a client’s third party Cloud Provider’s findings after they started experiencing performance issues.

The Managed Defense client began experiencing issues with slow processing and a non-responsive web interface which they reported to their cloud service provider on a Friday afternoon. Deemed unimportant, their provider tabled the issue until Monday.

When Monday morning arrived, the client walked in to find an invoice for “Weekend Surge in Bandwidth Utilization” and asked their provider to look into it further. Upon re-engaging, they were informed that a trojan was found on one of their appliances and was determined to be the cause of the issue.

The client reached out to their Managed Defense Consultant to provide a second opinion to verify these third party findings, as MDC’s serve as an extension of a client’s security team. Upon review, it was determined the threat had been falsely attributed to a Windows-based trojan running on their Ubuntu box. Managed Defense analysts were able to correctly determine the activity, in this case, as a Mirai malware variant.

The client was able to quickly launch into a Rapid Response engagement with Managed Defense to ensure the threat was contained and no other systems had been effected.

The moral of the story: don’t assume your data is protected by someone else; ensure your security procedures are in place, whether on-prem or in the cloud.

About Mirai Malware

Mirai is a distributed denial-of-service (DDoS) botnet malware that primarily exploits vulnerable Linux-based Internet of Things (IoT) devices. It has been modified and deployed by several actors since its source code was publicly released on Sept. 30, 2016.

The malware exploits vulnerable Linux-based Internet of Things (IoT) devices, resides purely in volatile memory, and is capable of self-propagation. The botnet has been more successful than other DDoS botnets due to its high customizability and a larger set of default credentials in the dictionary attacks it performs.