MANAGED SECURITY CASE STUDY: LAYERED PROTECTION

Ascend TECHNOLOGIES

ENVIRONMENT

- Managed Service Provider's Client

THE INCIDENT

- Malicious PowerShell identified on 2 hosts.
- Malicious payloads blocked in memory protection on both machines
- Attacker attempted to establish persistence with guest account.

THE SOLUTION

- Analysis & investigation completed in real time with Malware Prevention, EDR, and SIEM.
- Attacker access revoked
- Security holes identified
- Advice for patching and additional security measures provided to MSP and end client.

EXECUTIVE SUMMARY

A Managed Service Provider's (MSP) client experienced a small-scale security event within their network. Aided by layered security protection provided by Ascend, which included Malware Prevention, Endpoint Detection & Response (EDR), and a Log Analysis (SIEM) solution, the security event was identified and investigated as the activities took place.

The external attacker's activities alerted EDR, were tracked by SIEM, and the malicious payloads were blocked by the Malware Prevention. With the added benefit of security experts from Ascend's Security Operations Center (SOC) monitoring the solutions and the client's network, the incident was actively investigated and quickly shut down before further damage could be done. With the attacker's access revoked, the MSP was provided with further recommendations for network configurations and next steps to ensure the same attack vector could not be used again.

THE INCIDENT

In March 2020, Ascend security analysts discovered a possible security event in action. Alerts from both the Malware Prevention and the EDR solutions installed in the MSP's client network indicated a potential threat: malicious payloads had been blocked by Malware Prevention on two machines, and EDR identified PowerShell commands being executed. The team discovered it was a true hit and began investigating.

Looking at the command line, the team was able to determine that the Powershell code being run was malicious in nature. Then, when investigating the Malware Prevention console, two memory protection events were present: blocking malicious payload on both machines. While the malicious payloads were unable to be delivered and executed, the SIEM logs told the rest of the story: not all attacker activities had been blocked. Logs

showed that at 10:53:17 AM, the user XYZ\Guest* logged on to the first machine (entry-point) through an RDP session. From here, the attacker manually started PowerShell and began to run malicious commands on the host. Logs also showed that at 10:56:14 AM the attacker was able to pivot to the second host over SMB. From there they attempted to run malicious PowerShell commands similar to what was done on the first machine. The MSP was immediately notified of the events after the attack path was assembled through analysis.

It was determined that the 'XYZ\Guest' account was a domain level account. The Infogressive team gained permission to isolate both hosts for protection. Then, per Infogressive advice, the MSP logged into the domain controller and deleted the Guest account, revoking the attacker's access. Additional analysis was done and no additional malicious behavior was observed on the affected machines or the client network.

THE SOLUTION

The Ascend SOC Team provided the following recommendations to the MSP:

- Disable the 'XYZ\Guest' domain level account [Completed during investigation]
- Block or Restrict RDP (3389) traffic to only the external addresses that are necessary

  Several external entities were found to be attempting to log into this host on a regular basis.
- Block a determined list of IP addresses from the incident [IPs Redacted]
- Check for any scheduled tasks on the hosts that may include powershell commands that are unauthorized.

Thanks to the SOC and the multi-layered protection provided by the three services (Malware Prevention, EDR, Log Analysis), this small-scale security event was handled by security professionals in real time — preventing the event from turning into a larger scale security incident.

We're proud to share this story and the details of how our security services work together as an example of how a damaging cyberattack can be prevented with the right cybersecurity in place. Reach out to us for more information.