Security Operations Center (SOC) Highlights – August 2023

Welcome to the Barracuda SOC highlights. This monthly highlight provides insights into some of the success stories our Barracuda XDR's SOC teams have experienced while monitoring our customers' environments. Below are the number of events, alarms, and alerts the SOC teams went through in the month of August.

Event analyzed	Alarms generated	Alerts issued
169B	209k	30k

Event analyzed *- Refers to security-related data or events that Barracuda XDR received and processed.*
Alarms generated *- Refers to the notifications generated based on predefined criteria set by the SOC teams.*
Alerts issued *- Refers to the alarms sent after a confirmed investigation by a SOC analyst.*

Below are some examples of events Barracuda XDR detected, analyzed, and mitigated.
If you have any questions, please contact Barracuda sales at sales@barracudamsp.com.

Highlight 1:
Client: Retail Services
Product: XDR Endpoint Protection
Threat caught: Barracuda XDR detected the execution of malicious command lines, the presence of **smbexec.py** file, and other malicious activity in the environment. Smbexec allows remote code execution through a semi-interactive shell by creating services that execute commands sent by the threat actor.
Mitigation: The client confirmed it was a true positive. SOC initiated a code orange and determined an SSL VPN compromise had occurred.

Highlight 2:
Client: Manufacturing Services
Product: XDR Network Security
Threat caught: Barracuda XDR detected network events that indicated the use of Windows file sharing (also called SMB or CIFS) traffic to the Internet. SMB is commonly used within networks to share files, printers, and other system resources amongst trusted systems.
Mitigation: The client confirmed it was a true positive and blocked the IP.

Highlight 3:
Client: Commercial Services
Product: XDR Cloud Security
Threat caught: Barracuda XDR detected successful Microsoft 365 sign-in events from distinct locations that would constitute an impossible travel scenario.
Mitigation: The client confirmed there was a breach on the account and followed recommendations.

Highlight 4:
Client: Investment Services
Product: XDR Email Security
Threat caught: Barracuda XDR detected a new suspicious inbox rule was created. Inbox rules are created to automatically perform specific actions on emails that arrive in inboxes. After gaining access to a victim's account, attackers will often create a mail rule inside their mailbox to maintain stealthy access.
Mitigation: The client confirmed it was a true positive and followed the remediation recommendations.

Highlight 5:
Client: Law Firm Services
Product: XDR Endpoint Protection
Threat caught: Barracuda XDR detected a compromised device, and a threat action is attempting to run malicious code via the Pictures or Videos folder on the impacted endpoint. This is a common technique used by threat actors to hide malicious activity on a device.
Mitigation: The client confirmed true positive and followed recommendations.

Highlight 6:
Client: Public Sector
Product: XDR Server Security
Threat caught: Barracuda XDR identified a password spray attack. A password spray attack is a trial-and-error method used to obtain information, such as a user password or personal identification number targeting one or more users from multiple IP addresses or devices.
Mitigation: The client confirmed it was a true positive and followed the remediation recommendations.