exabeam

Solution Brief

Evasion

Detect and respond to attackers who are performing actions to evade detection

After initial compromise, an adversary seeks to avoid detection to establish persistence within the network. As a result, hackers will leverage a variety of evasion methods in order to circumvent detection, such as clearing audit logs, encrypting data and scripts, or using a TOR proxy to hide web activity.

By hiding their activity and evading the organization's detection mechanisms, they are awarded enough time to carry out their true objective such as deploying malware for exfiltrating data, encrypting files for ransomware, or exploiting resources for crypto-mining. The longer the cybercriminals evade detection, the greater the costs to the organization. Today, it takes on average 280 days to identify and contain a data breach. However, an organization will save on average $1.12 million if they contain a breach in less than 200 days.[1]

> Bankshot is a remote access tool (RAT) that was first reported by the Department of Homeland Security in December of 2017. In 2018, Lazarus Group used the Bankshot implant in attacks against the Turkish financial sector. Bankshot deletes all artifacts associated with the malware from the infected machine and marks files to be deleted upon the next system reboot and uninstalls and removes itself from the system and is associated with Defense Evasion techniques in the MITRE ATT&CK framework.[2]

[1] Cost of a Data Breach Report 2020

[2] https://attack.mitre.org/software/S0239/

Exabeam and Evasive Activity

Exabeam helps security teams outsmart adversaries taking evasive actions with the support of automation and use case content across the full analyst workflow, from collection to response.

Exabeam automatically detects the anomalous behaviors that are indicative of evasive actions by leveraging machine learning and user behavior analysis to baseline normal behavior for every user, device and peer group, regardless of the attacker's techniques. Detection models work out of the box and do not require security engineers to create complex correlation rules.

Analysts can leverage user and asset contextual data in conjunction with the flagged abnormal evasion activity to determine if the user is acting with malicious intent or has been compromised. Finally, they are provided with lists of notable accounts, user activity timelines, and customized response plans to support their incident investigations.

Key Capabilties

Challenge 1: Collection and Detection

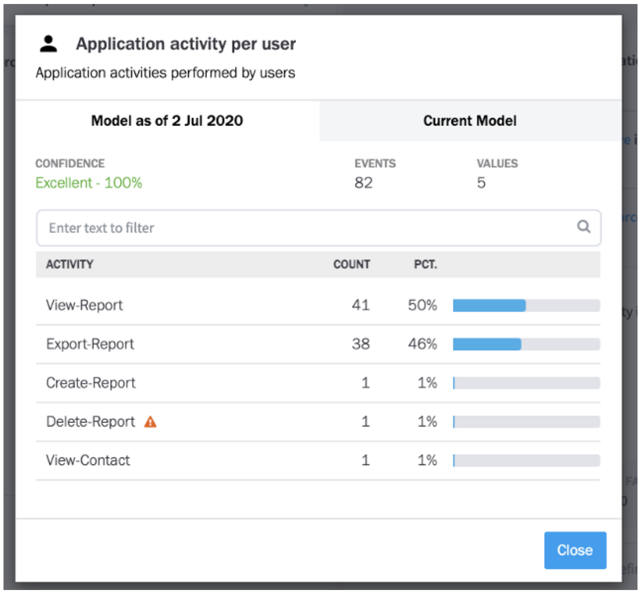
Correlation rules alone are ineffective in detecting the evasive behaviors of attackers such as abnormal file deletions and first time clearing audit logs.

Solution

Exabeam behavioral models enable analysts to quickly spot what is normal versus abnormal user behavior, delivering a solution that doesn't just detect audit tampering, file deletions, and other defense evasion techniques but crucially detects anomalous behaviors such as the first time clearing audit logs for a user, deleting an abnormally large volume of files, and other evasion tactics that are indicative of a hacker attempting to evade detection and establish a presence.

Benefit

Improve security posture by detecting the leading indicators of audit tampering and preventing users from their eventual goal of exfiltrating data, sabotage, or otherwise malicious behavior.



Application activity per user

Application activities performed by users

Model as of 2 Jul 2020 | Current Model

CONFIDENCE: Excellent - 100%

EVENTS: 82

VALUES: 5

Enter text to filter

ACTIVITY	COUNT	PCT.
View-Report	41	50%
Export-Report	38	46%
Create-Report	1	1%
Delete-Report ⚠	1	1%
View-Contact	1	1%

Figure 1 – This Data Insight Model shows the application activity for all users. Exabeam alerts on anomalous activity at the application level, in this instance it is a first time activity of deleting a report within an application.

Challenge 2: Visibility and Investigation

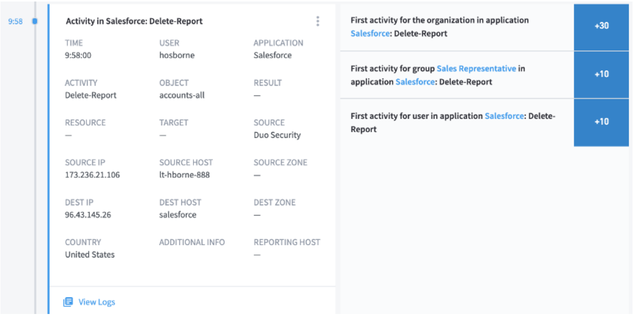
Attackers will tamper with audit logs in an effort to destroy incriminating audit trails and evade detection. This information would be missing from a users' local machine if it was deleted by an attacker, making it impossible for analysts to rely on a single source of truth.

Solution

Exabeam correlates a users session activity in a pre-assembled Smart Timeline, providing a historical view of the user activity and events prior to tampering or clearing the audit log, as well as what actions they took next; drastically reducing the time to correlate evidence, accelerating investigations and enabling analysts to determine the motive of the malicious actor.

Benefit

Complete attack visibility despite attackers efforts to avoid detection. Investigate threats in minutes not hours, without needing to write a single query.



9:58

Activity in Salesforce: Delete-Report

TIME 9:58:00	USER hosborne	APPLICATION Salesforce
ACTIVITY Delete-Report	OBJECT accounts-all	RESULT —
RESOURCE —	TARGET —	SOURCE Duo Security
SOURCE IP 173.236.21.106	SOURCE HOST lt-hborne-888	SOURCE ZONE —
DEST IP 96.43.145.26	DEST HOST salesforce	DEST ZONE —
COUNTRY United States	ADDITIONAL INFO	REPORTING HOST —

View Logs

First activity for the organization in application Salesforce: Delete-Report	+30
First activity for group Sales Representative in application Salesforce: Delete-Report	+10
First activity for user in application Salesforce: Delete-Report	+10

Figure 2 – This Smart Timeline event shows a potential attacker who is destroying files in an effort to disrupt or sabotage the corporation operations.

Challenge 3: Response

Processes and procedures related to incident response are often not tailored to the specific threat and largely entail manual processes.

Solution

Exabeam playbooks help orchestrate response with out-of-the-box checklists and recommended remediation steps (figure 3) for incident response teams. Customizable actions enable security teams to automate playbooks to respond to evasion incidents, such as the destruction of data by blocking, suspending, or imposing restrictions on the user involved in the incident.

Benefit

Leverage integrated SOAR capabilities in order to automatically terminate user sessions and/or isolate a host to disrupt a potential attack.

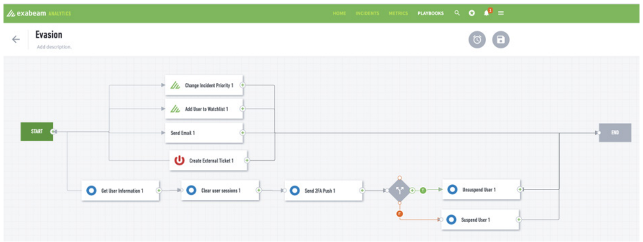


Figure 3 – This evasion playbook characterizes and escalates the incident, adds the compromised user to a watchlist while clearing their session and prompting the user for re-authentication via 2FA, before determining whether to lift the suspension on the user account.

Key Log Sources

- Audit logs
- Authentication and access management
- Application Activity
- Endpoint activity (EPP/EDR)
- File monitoring
- Network access, analysis and monitoring
- VPN and zero trust network access
- Web activity

Key Detection Rule Types

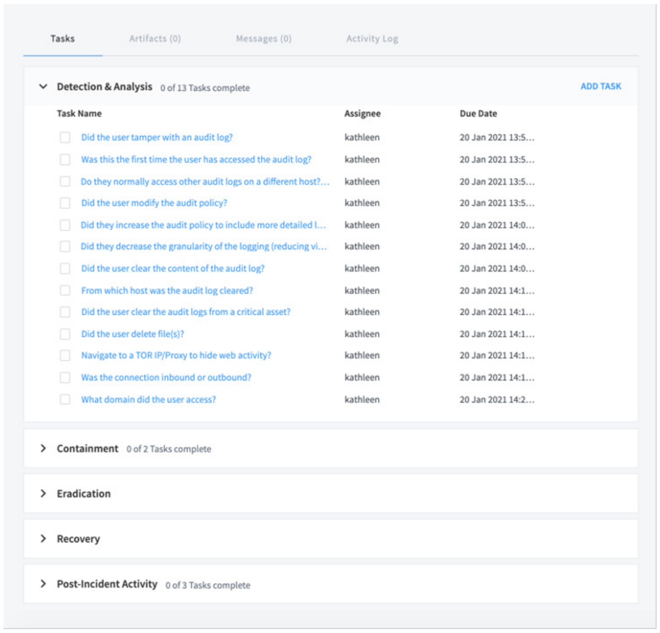
- Audit tampering
- Destruction of data
- Evasion

MITRE Techniques

- T1070: **Indicator Removal on Host**
- T1562: **Impair Defenses**
- T1485: **Data Destruction**
- TA0005: **Defense Evasion**

Response Actions

- Contact a user/manager/HR department via email
- Add a user or asset to a watchlist
- Get asset/user/process information
- Isolate hosts
- Clear user session
- Prompt for re-authentication via 2-factor/multi-factor authentication
- Block, suspend, or impose restrictions on users involved in the incident
- Rotate account credentials, expire/reset password



Detection & Analysis 0 of 13 Tasks complete

Task Name	Assignee	Due Date
□ Did the user tamper with an audit log?	kathleen	20 Jan 2021 13:5...
□ Was this the first time the user has accessed the audit log?	kathleen	20 Jan 2021 13:5...
□ Do they normally access other audit logs on a different host?...	kathleen	20 Jan 2021 13:5...
□ Did the user modify the audit policy?	kathleen	20 Jan 2021 13:5...
□ Did they increase the audit policy to include more detailed l...	kathleen	20 Jan 2021 14:0...
□ Did they decrease the granularity of the logging (reducing vi...	kathleen	20 Jan 2021 14:0...
□ Did the user clear the content of the audit log?	kathleen	20 Jan 2021 14:0...
□ From which host was the audit log cleared?	kathleen	20 Jan 2021 14:1...
□ Did the user clear the audit logs from a critical asset?	kathleen	20 Jan 2021 14:1...
□ Did the user delete file(s)?	kathleen	20 Jan 2021 14:1...
□ Navigate to a TOR IP/Proxy to hide web activity?	kathleen	20 Jan 2021 14:1...
□ Was the connection inbound or outbound?	kathleen	20 Jan 2021 14:1...
□ What domain did the user access?	kathleen	20 Jan 2021 14:2...

Containment 0 of 2 Tasks complete

Eradication

Recovery

Post-Incident Activity 0 of 3 Tasks complete

Figure 4 – The Evasion checklist prompts analysts to answer specific investigation questions and take containment actions.

About Exabeam

Exabeam helps security teams outsmart the odds by adding intelligence to their existing security tools – including SIEMs, XDRs, cloud data lakes, and hundreds of other business and security products. Out-of-the-box use case coverage repeatedly delivers successful outcomes. Behavioral analytics allows security teams to detect compromised and malicious users that were previously difficult, or impossible, to find. Automation helps overcome staff shortages by minimizing false positives and dramatically reducing the time it takes to detect, triage, investigate and respond. For more information, visit **exabeam.com.**

exabeam

To learn more about how Exabeam can help you visit exabeam.com today.