exabeam

Solution Brief

Malware

Malware is any malicious program or code developed by adversaries with the intent to cause damage to data or a system or gain unauthorized access to a network

Malware continues to be an effective means to an end

It is a well-accepted fact that today's attackers use any and all means available to them to attempt to infiltrate a target's environment. Whether using stolen credentials, exploiting known vulnerabilities, or the tried and true phishing attack, attackers are pragmatic in their approach to compromising an environment. A favorite tool in attackers' toolbox continues to be malware. Given its ability to carry out any number of tasks and the virtual unlimited variants available, attackers will use malware across the entire attack chain, from infiltration to data exfil. To that end, organizations make every effort to identify malware as soon as it appears in their network. Using advanced techniques, such as machine learning and AI detection models, organizations have a better chance today than ever before at identifying never-seen-before malware before it has an opportunity to carry out its objective. Unfortunately, detecting and preventing 100% of malware is not feasible, so it is critical organizations employ secondary behavior-based detection capabilities to catch malware that slips past their primary prevention layer.

> With regard to Malware, well, given the Swiss Army Knife behavior of modern variants, it looks like you can eat your cake and have it too.
>
> **Verizon 2021 DBIR - "Actions have Consequences"**

Exabeam and Malware

Exabeam helps security teams outsmart adversaries employing malware with the support of behavior analytics, automation, and purpose-built content across the full analyst workflow, from detection to response. Exabeam detects malware attacks by identifying abnormal behavior that is indicative of malicious applications. Our Turnkey Playbooks automatically triage and investigate each incident, while guided investigation checklists provide analysts recommended next steps for containment, recovery, and remediation. Exabeam further automatically enriches cases with contextual information to reduce false positives and increase alert fidelity, allowing analysts to focus on the most dangerous threats. Smart Timelines and complete lists of compromised users and assets are automatically available for additional analysis.

Key capabilities

Challenge 1: collection and detection

Organizations can receive hundreds of malware attacks a day, increasing the risk that a single variant will bypass all primary detection capabilities, roaming free within the network, causing significant damage.

Solution

Exabeam arms analysts with tools against malware on multiple fronts. Exabeam analyzes web, DNS, and endpoint activities, to rapidly detect malware arriving on an endpoint or operating from an endpoint. The endpoint-focused early detection capabilities of this use case supplement those of the credentials-focused lateral movement use case. In addition to detecting endpoint compromise, Exabeam ranks AV or EDR security alerts by analyzing the behavior of accounts associated with the device and the unique characteristics of those alerts. Frequent alerts with no other signal are deprioritized while unique alerts with signs of compromise in surrounding activities rank at the top of the triage list. Finally, analysts are provided with lists of compromised systems and accounts as well as user and device activity timelines to support their investigations.

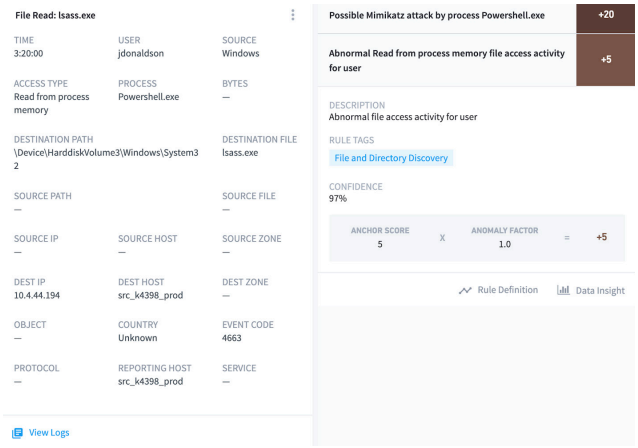

Figure 1 - This Smart Timeline shows a suspected Mimikatz attack with abnormal file access activity for the user.

Benefit

Strengthen security posture against malware attacks through a robust combination of threat indicator and behavior-based detection.

Challenge 2: visibility and investigation

Investigating malware incidents in disparate tools is time-consuming and manual.

Solution

Exabeam provides a comprehensive solution for tracking, investigating, and responding to malware incidents. Our integrated incident management automatically extracts key evidence and links to attach as evidence to a case. Analysts easily pivot to machine-built incident timelines to investigate other potential related events, or embedded email functionality to communicate with users and assemble additional evidence. Guided checklists are provided directly within the case to ensure analyst investigations are comprehensive and complete.

Benefit

Streamline investigations and reduce potential attacker dwell time with integrated incident management and investigation.

Figure 2 - This malware playbook analyzes a suspicious file against available threat intelligence as well as detonation capabilities to gain additional context.

Challenge 3: response

Implementing automated malware playbooks requires significant time, resources, and expertise, slowing time to value.

Solution

Exabeam offers the only security operations, orchestration, and response (SOAR) solution with Turnkey Playbooks that work out of the box, no additional licenses to third-party tools or API token configuration required. Our strategic partners provide native response actions such as obtaining the reputation of files, URLs, domains, email senders, and IP addresses against commercial threat intelligence services or analyzing evidence with detonation services.

Benefit

Accelerate time to value from your SOAR tool with Turnkey Playbooks designed for malware triage and investigation.

Use case content

To provide coverage for malware, Exabeam identified key data sources and has built content for collection, detection, investigation, and response.

Key data sources

- Endpoint activity
- Web activity

Key detection rule types

- Malware

MITRE technique coverage

- T1070 Indicator Removal on Host
- T1218 Signed Binary Proxy Execution
- T1003 OS Credential Dumping
- T1071 Application Layer Protocol
- T1486 Data Encrypted for Impact
- T1490 Inhibit System Recovery

Response actions

- Malware turnkey playbook
- Suspend user - lock the affected account(s)
- Reset password/expire password
- Quarantine/isolate host
- Get domain, URL, IP reputation
- Block malicious domains, URLs, and/or IP addresses
- Kill process
- Scan host
- Search email by sender
- Delete emails by sender/message ID
- Block sender
- Add hash to blacklist
- Add asset to watchlist

Incident checklist

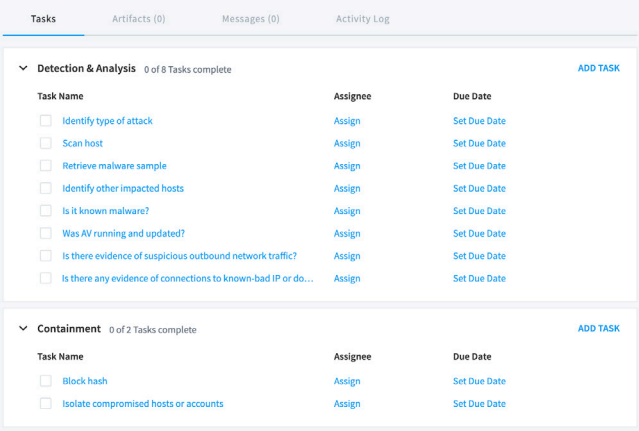

Figure 3 - The malware checklist prompts analysts to answer specific investigation questions and take containment actions.

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Operations Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users and malicious adversaries, minimize false positives, and make security success the norm. For more information, visit www.exabeam.com.

exabeam

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