exabeam

Solution Brief

Ransomware

Ransomware is a form of malware designed to encrypt a target organization's files, holding the data hostage until the organization pays the ransom demanded by the attackers.

Ransomware should be on your radar

According to Verizon's 2021 DBIR1 report incidents of successful ransomware attacks doubled from 2020, making up 10% of all attacks publicly reported. While there are many potential reasons for the increase in ransomware, attackers continue to deploy ransomware because ransomed organizations pay the ransom to retrieve their data and it returns a profit. With ransomware-as-service available on the dark web, attackers no longer need to be proficient in writing malicious code to deploy a ransomware attack. In a matter of minutes, virtually anyone can initiate a ransomware attack that will likely pay for itself in a matter of days or hours.

Ransomware, like most other modern malware, attempts to evade modern detection products by continually modifying its code, making traditional detection methods based on hash/signature ineffective. That said, next-generation products that make use of machine learning methods to identify never seen before strains of ransomware are available. Rather than using hash/signatures, these tools analyze the composition of any files moving onto a protected machine and, if deemed malicious, block the file from either being copied to the machine or executing.

> The major change this year with regard to action types was ransomware coming out like a champ and grabbing third place in breaches (appearing in 10% of them, more than doubling its frequency from last year).
>
> **2021, Verizon DBIR**

Even the best detection and prevention tools on the market will fail to identify a file as malicious ransomware occasionally, opening the door for a successful attack. To mitigate these cases organizations must have a solid secondary behavior-based detection method coupled with an automated recovery and response mechanism that enables them to limit damage and return to a trusted state fast, without paying any ransom.

Ransomware should be on your radar

Exabeam helps security teams outsmart adversaries committing ransomware attacks with the support of behavior analytics, automation, and purpose-built content across the full analyst workflow, from detection to response. Exabeam detects ransomware attacks by identifying abnormal behavior that is indicative of an active ransomware attack. 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 ransomware 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 ransomware on multiple fronts. Exabeam analyzes file, web, DNS, and endpoint activities, to rapidly detect ransomware arriving on an endpoint or operating from an endpoint. Behavior analytics flags users attempting to access a domain or IP addresses associated with ransomware as well as suspicious processes or commands that aim to encrypt critical files or disable recovery mode.

Benefit

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

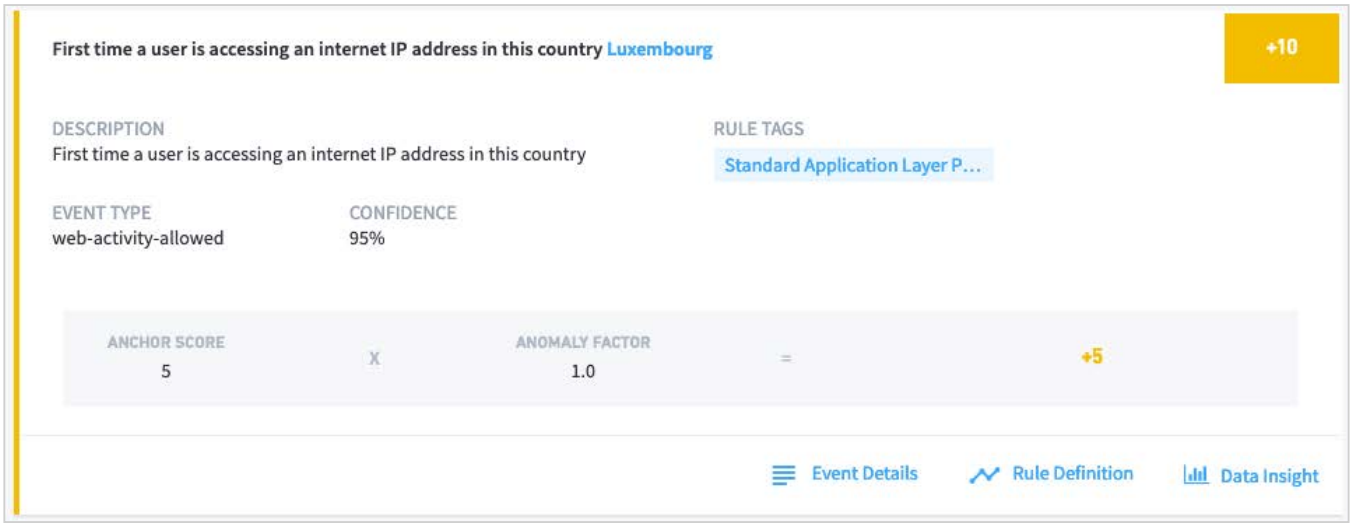

Figure 1: This Smart Timeline event shows a user is accessing an internet IP in a country they never have accessed before.

Challenge 2: Visibility and investigation

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

Solution

Exabeam provides a comprehensive solution for tracking, investigating, and responding to ransomware 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.

Challenge 3: Response

Implementing automated ransomware 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 is 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 phishing triage and investigation.

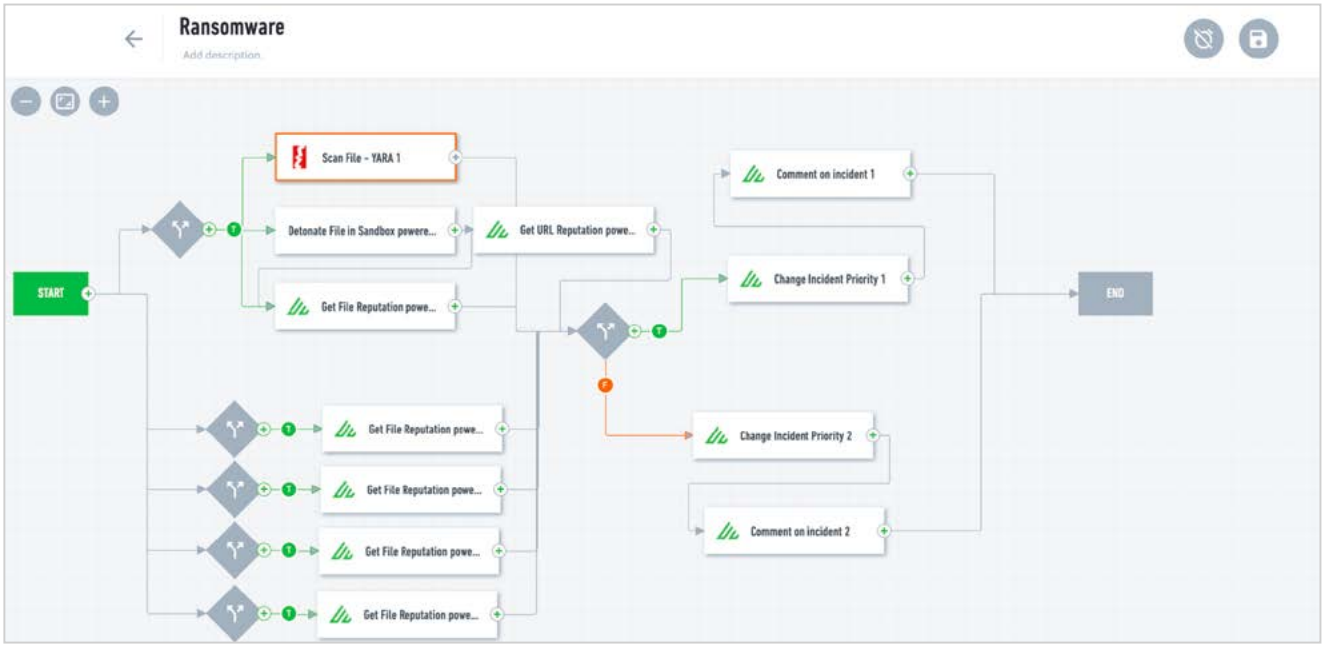

Figure 2: This ransomware playbook analyzes a suspicious file against available threat intelligence as well as detonation capabilities to gain additional context.

Use case content

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

Key data sources

- Endpoint activity
- Network activity
- Web activity

Key detection rule types

- Ransomware

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

Incident checklist

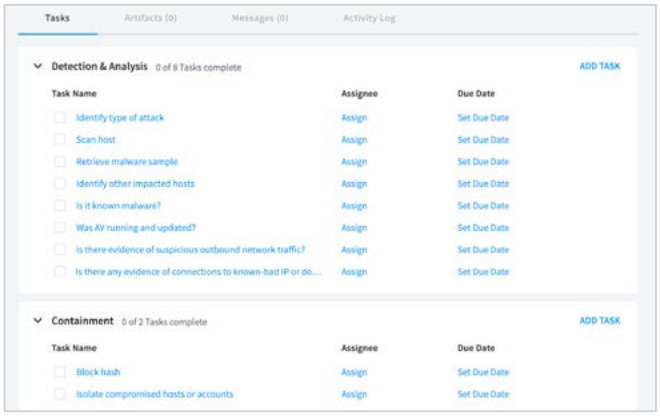

Figure 3: The ransomware checklist prompts analysts to answer specific investigation questions and take containment actions.

Response actions

- Suspend user
- Reset password/expire password
- Quarantine/isolate host
- Get domain, URL, IP reputation
- Block malicious domains, URLs, and/or IP address
- Kill process
- Scan host
- Search email by sender
- Delete emails by sender/ message ID
- Block sender - block the sender's email address
- Add hash to backlist
- Add asset to watchlist

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.

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

exabeam