exabeam TUCANA CYBER SECURITY SOLUTIONS

Checklists

External Threats: Ransomware, Phishing, and Malware

Looking for help with ransomware, phishing, and malware? Here are checklists to help.

External threats such as ransomware, phishing, and malware attacks are a daily occurrence for every organization. While defense against these attacks is improving, their quickly evolving nature means prevention is never guaranteed. SOC teams must be prepared to respond to an active attack at any time.

Defending against external threats is more than just choosing the right security solutions. It's also creating a security program that puts people, processes, and technology together. The following checklist is meant to be a guide when defending and responding to external attacks.

Ransomware

According to Verizon's 2021 DBIR 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 it returns a profit. With ransomware-as-service available on the dark web, attackers no longer need to be proficient in writing malicious code. In a matter of minutes, virtually anyone can initiate a ransomware attack that could pay for itself in days or hours.

Even the best detection and prevention tools on the market can fail to identify a file as malicious ransomware. 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.

Detection

- Analyze file, web, DNS, and endpoint activity for behavioral anomalies to detect ransomware arriving on or operating from an endpoint
- 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
- Extract key evidence and link to attach as evidence to a case
- Look for known ransomware techniques, tactics, and procedures (TTP) for visibility into assets with vulnerabilities or misconfigurations that attackers might exploit

Response actions

- Suspend user: Lock the affected account(s)
- Reset password/expire password: Change password(s) for an affected account(s)
- Quarantine/isolate Host: Quarantine the affected asset(s)
- Get domain, URL, IP reputation: Determine the reputation of the URL, IP, and/or domain
- Block malicious domains, URLs, and/or IP addresses
- Kill processes: Terminate the malicious processes on the compromised endpoint(s) identified
- Scan Host: Initiate antivirus scan on a machine
- Search email by sender: Search for other users who received the phishing email from the same sender
- Delete emails by sender/message-ID: Proactively delete malicious emails based on the sender or message ID from other users' inbox
- Block sender: Block the sender's email address
- Add hash to blacklist
- Add asset to watchlist

Phishing

Phishing attacks typically involve social engineering, which is the use of deception to manipulate users into divulging their credentials by clicking a weaponized link or opening a malicious attachment.

Phishing is an entry point for many attacks and can lead to malware infection, lateral movement across the network, account takeover, data exfiltration, and more. With the high volume of threats and new phishing campaigns appearing daily, security teams require a means to stay ahead of attacks.

Detection

- Find phishing attacks through emails forwarded by employees or natively via behavioral analytics to automatically create an incident
- Check user website activity against whitelists and blacklists of known domains and senders, as well as analyze using machine learning with lexical analysis and substring searches for resemblance to popular domains
- Use behavioral analytics to identify unknown threats, establishing a baseline for typical domains or countries that a user normally receives emails from, and alerting on abnormal activity
- Check URLs against the list of top-ranked domains from the Alexa 1M and Majestic Million, as well as domains flagged as malicious by proxy logs

Response actions

- Get domain, URL, IP reputation: Determine the reputation of the URL, IP, and/or domain
- Get IP WHOIS: Collect contextual information about the IP address such as who it's registered to or the ASN
- WHOIS: Collect contextual information about the domain such as the age, when it was registered
- Detonate file in a sandbox: If the phishing email has email attachments, detonate them in a sandbox and get the reputation results
- Search email by sender: Search for other users who received the phishing email from the same sender
- Delete emails by sender/message ID: Proactively delete phishing emails based on the sender or message ID
- Extract key evidence from phishing emails such as file attachments and links to attach as evidence to an incident case
- Investigate other potential related events or embedded email functionality to communicate with users and assemble additional evidence
- Reduce potential attacker dwell time with integrated incident management and investigation

Malware

A favorite tool in attackers' toolbox continues to be malware — from trojans to more destructive malware families. 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.

Using advanced techniques, such as machine learning and AI, detection models can identify never-before-seen malware before it has an opportunity to carry out its objective. 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.

Detection

- Utilize behavioral analytics and user context to find applications and/or code acting abnormally, indicative of the suspected app or file being malware
- Analyze web, DNS, and endpoint activities to rapidly detect malware arriving on an endpoint or operating from an endpoint
- Analyze the behavior of accounts associated with the device and the unique characteristics of those alerts
- Pay attention to frequent alerts with no other signal which are often deprioritized, where unique alerts with signs of compromise in surrounding activities rank at the top of the triage list
- Streamline investigations and reduce potential attacker dwell time with integrated incident management and investigation

Response actions

- Leverage machine-built incident timelines to investigate other potential related events, or embedded email functionality to communicate with users and assemble additional evidence
- Extract key evidence and link to attach as evidence to a case
- Suspend user: Lock the affected account(s)
- Reset password/expire password: Change password(s) for the affected account(s)
- Quarantine/isolate host: Quarantine the affected asset(s)
- Get domain, URL, IP reputation: Determine the reputation of the URL, IP, and/or domain
- Block malicious domains, URLs, and/or IP addresses
- Kill process: Terminate the malicious processes on the compromised endpoint(s) identified
- Scan host: Initiate antivirus scan on a machine
- Search email by sender: Search for other users who received the malware from the same sender
- Delete emails by sender/message-ID: Proactively delete malicious emails based on the sender or message ID from other users' inbox
- Block sender: Block the sender's email address
- Add hash to blacklist
- Add asset to watchlist

About Exabeam

Exabeam is a global cybersecurity leader with the mission to add actionable intelligence to every IT and security stack. The leader in Next-gen SIEM and XDR, Exabeam is reinventing the way security teams use analytics and automation to solve threat detection and incident response (TDIR). Exabeam offers a comprehensive cloud-delivered solution that uses machine learning and automation focused on a prescriptive, outcomes-based approach. We design and build products to help security teams detect external threats, compromised users, and malicious adversaries while minimizing false positives to protect their organizations.

For more information, visit

exabeam

TUCANA
CYBER SECURITY SOLUTIONS
www.tucana.com info@tucana.com