State and Local Government
A Behavior-based Approach for Ransomware

Ransomware Attacks Targeting State Local Governments are on the Rise

With over 100 incidents reported in 2019 alone, ransomware attacks targeting state and local governments are growing increasingly frequent. Tight budgets and staffing shortages at government agencies can often translate to legacy security systems and fewer backups, positioning them in hackers’ minds as easy targets. Hackers also seek notoriety from outsized media coverage of government attacks for free “publicity” for their software and services.

By the time an attacker has taken systems hostage to demand payment, the situation is out of control; city officials must either pay out, or bear the costs of downtime and lost revenue as well as the direct costs to restore their systems, often at taxpayer’s expense. Meanwhile, government employees and citizens are left with crippled systems like emergency services or police departments for critical operations.

When it comes to ransomware, anyone can be a target, including home users, small to large businesses, public or government agencies, and even politicians or celebrities. With taxpayer dollars and citizens’ private information at risk, it’s imperative for public sector agencies to find security solutions that can detect and respond to these attacks before they deal real damage.

Pramod Borkar
Technical Product Marketing Manager
Protect citizens from attackers with modern security tools

With public safety, money and trust on the line, state and local governments require a solution that allows security teams to quickly and accurately detect, investigate and respond to ransomware threats. With Exabeam, agencies can keep critical systems up and running and protect citizens’ valuable personal data. Exabeam enables security teams to improve threat detection and achieve faster investigation and response times with user and entity behavior analytics (UEBA) and security orchestration and automation (SOAR).

With Exabeam, security teams can

- Detect new and evolving ransomware attacks, even for those never yet seen before
- Enable rapid response to ransomware attacks using SOAR powered playbooks to quickly coordinate response actions across multiple security tools and disrupt the killchain
- Automate triage and forensic investigations with machine built incident timelines that automatically gather context and activity for the before and after of an alert

Detect ransomware activity

New ransomware permutations crop up frequently, meaning traditional detection approaches — such as relying on signatures or correlation rules — may be obsolete within a 24 hour period. Furthermore, agencies and offices may not have the staff, time or budget to manually monitor and tune their security tools to keep pace. As a result, state and local governments find themselves vulnerable to attacks.

With modern tools, security teams can leverage user and behavior entity analytics (UEBA) to detect these rapidly changing threats. Behavioral modeling picks up on defined ransomware activity known as a “kill chain” (See Figure 1). By analyzing log artifacts associated with each stage of the ransomware kill chain with UEBA, Exabeam enables analysts to be able to detect the latest strains of ransomware, regardless of whether they’ve been seen before and without relying on static rules.

Figure 1 – The ransomware killchain establishes a pattern of behavior that UEBA tools can detect, regardless of whether that particular strain has been seen before.
Enable rapid response

Once a system is compromised, analysts must be able to quickly identify and remove an attacker infiltrating the network, before files are encrypted and disrupting the ransomware. Security teams facing talent shortages often lack sufficient resources to move quickly enough to disrupt the attack.

Exabeam’s SOAR-powered playbooks enable rapid response that can disrupt the ransomware killchain. Playbooks string together complex workflows like detonating a file in a sandbox, then based on the results, quarantining affected endpoints or block access to command and control servers. Security analysts can define triggers to automatically kick off a playbook as soon as ransomware is detected, disrupting the killchain and containing infections in minutes.

Figure 2 – Analysts can leverage playbook templates with a simple drag and drop interface designed to automatically respond to ransomware attacks and disrupt the killchain in minutes.
Automate triage and investigations

While traditional security tools help public sector agency teams meet compliance requirements, they were not designed to support SOC workflows for incident investigation. In the case of ransomware, analysts using legacy tools often spend many cycles with tedious, manual queries that cost precious time during an attack, meaning systems containing sensitive constituent data can become encrypted before it is too late.

Exabeam automates the more tedious, time-consuming portions of the investigation workflows, enhancing analyst productivity and saving valuable time while an attack is in progress. Exabeam automatically reconstructs an attack kill chain using machine-built Smart Timelines to gain visibility into the full scope of an incident to understand which systems and assets were infected. With automated, rapid investigations, teams can use the timeline to quickly review the full attack chain and spend less time performing manual searches and focus on complete and timely responses.

Figure 3 – Machine-built Smart Timelines provide security analysts event context during forensic investigations to understand how an infection may spread across their environment.

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 Management 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.

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