ExtraHop

Stop Ransomware in Its Midgame Before it Springs its Extortion Trap

Ransomware crews have expanded their playbooks to use your IT infrastructure to amplify damage and improve their payment calculus. As a result, ransomware moves through the territory of IT before springing its trap, putting the attention and responsibility directly on IT security.

CHALLENGES

The conventional approach for ransomware focuses on preventing initial access and relying on backup recovery—but it hasn't slowed the extortion menace. Unfortunately, prevention is an uphill battle for defenders: attackers only need to succeed once. And, restoring data doesn't negate downtime or the consequences of a data breach. Defenders need a much broader window to catch and stop ransomware before the damage is done.

SOLUTION

Preventing initial access may not be possible, but with Reveal(x) 360, defenders can stop extortionists in their midgame before they do real damage. Reveal(x) 360 stops ransom-driven attackers as they attempt to pivot through your infrastructure, enumerating targets, escalating domain privileges, and sending C2 over noisy DNS channels. It spots data staging before encryption starts, as seen by one ExtraHop customer alerted to an attack by a data staging detection—allowing them to avert damage.

Using guided investigative workflows with ninety days of traffic record lookback and scalable PCAP repository, incident responders can pinpoint the root cause and scope all assets and data compromised. With these ground-truth packet insights, defenders can eradicate intruder residue, close security gaps to prevent a recurrence, and move to recovery confidently.

KEY BENEFITS

DETECT EARLY INDICATIONS OTHER TOOLS MISS

Uncover evidence of an active ransomware attack 84% faster with cloud-scale ML applied over one million predictive models.

STOP RANSOM-DRIVEN INTRUDERS

Leave ransomware operators no place to hide with continuous visibility across all devices and workloads—even encrypted authentication and Active Directory ticket escalation attempts.

STOP DATA EXFILTRATION AND ENCRYPTION STAGING

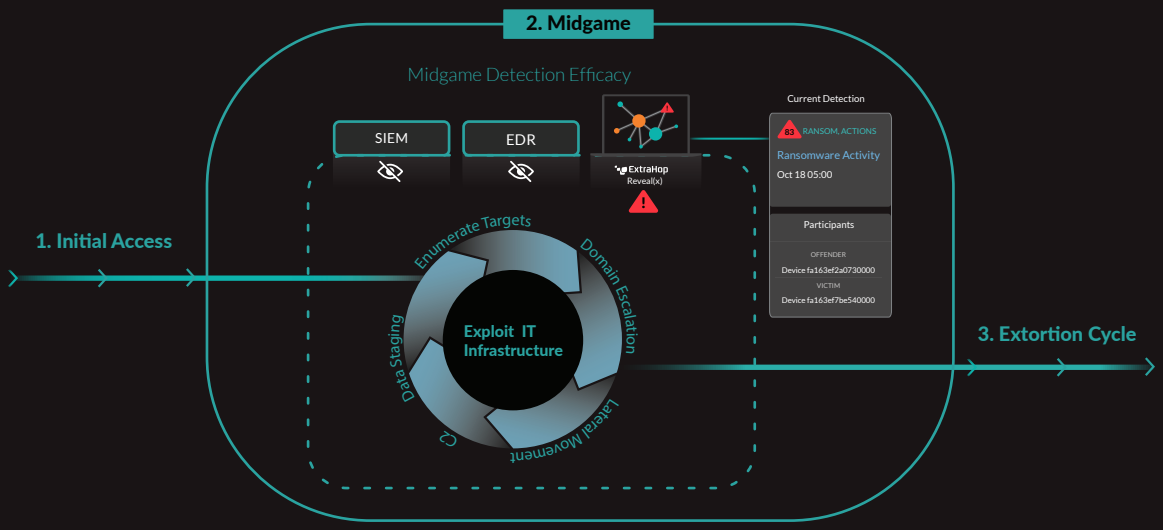
Block rogue database and SMB accesses before they steal your data and leave an encrypted copy behind for their double extortion scheme.

AUTOMATE RAPID ASSET ISOLATION

Automatically orchestrate the quarantine and recovery of impacted endpoints with integrated solutions from CrowdStrike, Phantom, Palo Alto, and more.

HOW IT WORKS

Stop the Ransomware Playbook



Use Cases

DETECT COMPROMISED ASSETS

Network data gives a superior understanding of normal behavior and quickly detects deviations. Reveal(x) 360 spots ransomware intruders other methods miss, dynamically adjusting cloud-scale ML to your changing environment.

APPLY COMPENSATING CONTROLS FOR SLOW EDR ROLLOUT

Ransomware attackers evade EDR-enabled endpoints by applying living-off-the-land techniques—plus exploiting the prevalence of unmanaged servers, Linux hosts, and IoT devices.

PROTECT SENSITIVE DATA

With Reveal(x) 360, you can prevent data theft and encryption of high-value databases and file systems before they're held hostage. Enable faster, more confident actions with immediate context.

HUNT RANSOMWARE THREATS

Reveal(x) 360 makes meaningful ransomware hunting accessible to analysts of all skill levels. Analysts form and test hypotheses faster with automated and efficient investigation workflows.

RECOVER FASTER WITH NETWORK FORENSICS READINESS

Incident responders jump into action with 90 days of continuous traffic record lookback and long-term PCAP repository scalable to 24 PB. Eradicate intruder residue and prevent ransomware recurrence.

ABOUT EXTRAHOP NETWORKS

ExtraHop provides cloud-native network detection and response for the hybrid enterprise. Whether you're investigating threats, ensuring the availability of critical applications, or securing your cloud investment, ExtraHop's breakthrough approach helps you rise above the noise so you can protect and accelerate your business. Learn more at www.extrahop.com.

ExtraHop

info@extrahop.com
www.extrahop.com