CASE STUDY

ENDGAME PROTECTS ENTERPRISES FROM RANSOMWARE

DoD Funded Research Facility. Over 1,000,000 Devices.

THE CUSTOMER

One of the largest federally funded research facilities in an educational institution with over 20 IT departments, serving 11 universities, 7 stand-alone 'operating units', including healthcare providers, research institutions with US DoD projects, and multiple state government agencies. Their decentralized security and operations teams manage cybersecurity and risk for over 80,000 employees, and nearly 1,000,000 connected devices. They are also responsible for ensuring compliance with PCI, HIPPA/PHI, and FERPA.

The SOC team's objectives are to reduce the time to detection and rapidly remediate threats within their network. The SOC team faces three major challenges to meeting these objectives:

- Skills: Analysts must understand advanced attacker methods and the technologies.
- Tools: Analysts must have the right tools to gather relevant host data and analyze it in time to stop damage and loss.
- Process: Current processes are dominated by data collection and known indicator search, which is not designed to identify unique, polymorphic attacks.

THE CHALLENGE

The help desk received an alert for a malicious file on an endpoint. The alert highlighted a suspicious activity on the machine, triggering a ticket to the tier 1 SOC analyst. The SOC analyst scanned the infected host system with an anti-malware software, identified a variant of the Locky ransomware and deleted the malicious ransomware file. Once the file was deleted, the IT administrator re-imaged the machine and restored encrypted data from a backup. The tier 1 SOC analyst changed the alert status to 'resolved' and the help desk closed the ticket thinking that ransomware was removed.

Although the file was deleted, the malicious process was still running on the infected systems. Because the attack included a persistence mechanism, a comon technique used by attackers to maintain access after system reboot, the ransomware executed on reboot and a tier 2 SOC investigated the alert. Despite the time SOC team spent detecting, analyzing and responding to the alert, they failed to eliminate the threat from the infected system.

ENDGAME PROTECTS AGAINST RANSOMWARE

With Endgame deployed on endpoints, the tier 1 SOC analyst receives an alert before the JavaScript downloads and the file executes. Our signature-less malware engine generates an alert with a MalwareScore™, a high confidence score depicting the maliciousness of a file. The security analyst deletes the file with a single click on the alert. To ensure that the file has no remnants on the system, the tier 1 SOC analyst runs network, process and persistence hunt to eliminate any suspicious activity. In less than a minute, the tier 1 analyst gathers the data and explores various automated hunt capabilities, including how:

- The automated network hunt finds suspicious communications to C2.
- The process hunt identifies suspicious processes that were not backed by a file.
- Endgame's automated hunt for persistence identifies an uncommon path where a file is running from the temp directory.

Once the hunt artifacts are detected, the tier 1 SOC analyst deletes the file, kills the process, and stops persistence without any business disruption. The automated hunts enable the SOC to look for similar occurrences across the environment and stop further damage and loss.

THE ENDGAME VALUE

Endgame reduces the time, cost and complexity of traditional incident response by instantly detecting techniques and patterns used by ransomware and memory resident malware at the earliest and all phases of the kill chain, without indicators of compromise. Our unique prevention technology halts attacker techniques such as encryption, lateral movement within the network, stopping any damage and loss.

	TRADITIONAL SOLUTION*	ENDGAME.
TIME TO IDENTIFY AN ALERT *(Time to triage false positives)*	157 minutes	5 mins
TIME TO INVESTIGATE & RESPOND *(Time to triage/root cause the extent of incident)*	350 minutes	10 minutes
COST TO CLEAN UP A SINGLE INCIDENT ACROSS 10,000 MACHINES *(Time to remediate)*	$68,715	$3,750
COST OF INCIDENTS PER MONTH	$190,875	$11,719
SAVINGS OF A FULL TIME EMPLOYEE (FTE)	-	1.5 per month

* Numbers are provided by Endgame customers