Infocyte

If they try it, we'll stop it.

CASE STUDY

HOSPITAL ATTACK MITIGATED

ABOUT THE CUSTOMER

LEVEL 1 TRAUMA CENTER / MAGNET HOSPITAL WITH 7,000+ EMPLOYEES

EXISTING DEFENSES:
Network: Forcepoint Web Gateways, Cisco Firewalls
AV/Endpoint: Cisco AMP Endpoint Security, Defender, Invanti App Control
Monitoring Service: Optiv 24/7 Monitoring

TIMELINE

SUNDAY-MONDAY

Security team was alerted to multiple unknown file execution attempts on PCs.

TUESDAY

Infocyte used to triage network and placed into Active Monitor mode.

INFOCYTE DETECTION & RESPONSE WORKFLOW

DETECTION	ANALYSIS	ROOT CAUSE ANALYSIS	RESPONSE
Infocyte alerted security team to active Cobalt Strike beachheads on three key servers	Attackers achieved full domain takeover and were actively staging ransomware	A user with overly-elevated privileges lost control of their account over the weekend	Infocyte Incident Response support team reviewed data and made initial response recommendations and took direct action

Infocyte

Infocyte proved value quickly

Satisfied Customer & Investigators:

"You guys rock! Thanks for all the help."

"Thanks for the out of this world support!"

INFOCYTE RESPONSE AT-A-GLANCE:

RECOMMENDATIONS

- IP Blocks
- Disabled user's account
- Reset admin accounts

MONITORING

- No new attacker activity seen through the rest of the week

ACTIONS

- Infocyte removed ransomware from 1,000s of systems
- Killed Cobalt Strike injections
- Deleted volume shadow copy hiding places

RESULT

- Ransomware actors were purged
- Incident was handed over to digital forensic investigators led by Infocyte partner, CyberDefenses, LLC

PHONE: 844.463.6298

EMAIL: sales@infocyte.com

ABOUT INFOCYTE

Founded by the leaders of the United States Air Force Cyber Incident Response Team (AFCIRT), Infocyte is the globally trusted leader in proactive threat detection and incident response. The world's leading security and incident response companies use Infocyte's platform to proactively detect and respond to vulnerabilities and threats within their customers' endpoints, data centers, and cloud environments. Infocyte's team and partner ecosystem help organizations maintain compliance, stop ransomware and account takeover, reduce risk, optimize security operations, and scale security teams. Infocyte is the faster, simpler, smarter way to detect and orchestrate response to sophisticated threats.

Learn more at infocyte.com | Follow us on Twitter: @InfocyteInc | Follow us on LinkedIn: linkedin.com/infocyte-inc