CROWDSTRIKE

PREVENT AND RESPOND TO RANSOMWARE

With expertise and award-winning technology from CrowdStrike Services

RANSOMWARE PREVENTION SERVICES THAT WORK: IN-DEPTH EXPERIENCE + AWARD-WINNING FALCON TECHNOLOGY

Ransomware incidents can impose significant operational and financial costs on organizations. Recently, organizations across 150 countries fell victim to the WannaCry outbreak, which cost victims an estimated $4 billion*. It's essential that organizations get ahead of these evolving threats before incurring the costs of both investigating the attack and restoring lost data.

With CrowdStrike ® Services and the Falcon platform, you can immediately and confidently protect your organization from advanced ransomware and other targeted attacks.

RANSOMWARE ADVISORY SUPPORT

CrowdStrike Services provides both remote and on-site advisory support to help you respond to ransomware attacks, including:

- **Recommendations to help you resume business operations**
- **Guidance on recovering data and protecting against future attacks**
- **Guidance concerning ransom payments**
- **Ransomware attack intelligence**

RANSOMWARE INCIDENT RESPONSE SERVICES

CrowdStrike Services can conduct both deep-dive forensic analysis of individual systems as well as a broad compromise assessment of your entire environment, to determine the full scope of the attack. As part of this service, CrowdStrike Services provides ongoing monitoring and prevention of ransomware using the award-winning, cloud-delivered CrowdStrike Falcon® platform. This service will:

- **Determine the initial point of entry and root cause of the attack**
- **Identify the full scope of system(s) targeted with ransomware**
- **Explain the type of data affected by the ransomware attack**
- **Prevent future ransomware attacks**
- **Conduct ongoing monitoring and hunting**

What if you could immediately detect harmful activity and confidently protect your organization from advanced ransomware?

CrowdStrike Services offers a full portfolio of proactive and reactive services that enable organizations to detect, prevent and respond to harmful ransomware such as WannaCry, Locky and CryptoLocker.

CrowdStrike provides experienced assistance and proactive defense against sophisticated attacks.

Contact us for more information:
services@crowdstrike.com

* CBS Marketwatch:
"WannaCry ransomware attack losses could reach $4 billion"
May 16, 2017

RANSOMWARE MATURITY ASSESSMENT AND ROADMAP

This focused, interview-based assessment helps you identify security control gaps, immediate-value controls, and also provides a roadmap to implement the proper defenses against ransomware. Key benefits of this service include:

• An evaluation of existing ransomware defenses and configurations

• Insights and recommendations for strengthening your backup, recovery and patching processes

• Security control recommendations to prevent ransomware attacks

• A strategy for protecting against ransomware and similar threats

ADDITIONAL RANSOMWARE SERVICE OFFERINGS

CrowdStrike Services offers a full portfolio of services to help you prepare for future ransomware attacks, document an effective response process, and test your security against ransomware and other advanced and evolving threats .

The following are some of the services CrowdStrike offers:

• **Tabletop Exercises:** CrowdStrike Services conducts a ransomware-specific tabletop exercise to test your team, focusing on isolated ransomware attacks, self-replicating ransomware and interactive ransom attack scenarios.

• **Playbook Development:** The CrowdStrike Services team works with you to develop a tailored ransomware playbook that includes both business and technical responses to these attacks.

• **Adversary Emulation:** CrowdStrike Services leverages the CrowdStrike Red Team to test your total response plan against simulated "hands-on-keyboard" ransomware attacks.

LEARN HOW CROWDSTRIKE STOPS BREACHES:

Speak to a representative to learn how Crowd-Strike Services can help your organization fight ransomware and reduce costs associated with cyber incidents.

Phone: 1.888.512.8906
Email: services@crowdstrike.com
Web: www.crowdstrike.com/services

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging the cloud-delivered CrowdStrike Falcon™ platform — next-generation endpoint protection, cyber threat intelligence gathering and reporting operations, and a 24/7 proactive threat hunting team — the CrowdStrike Services security team helps customers identify, track and block attackers in real time. This unique approach allows CrowdStrike to stop unauthorized access faster and prevent further breaches. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks, and ultimately stop breaches.

The Evolution of Modern Ransomware

2005 — First variant of modern ransomware appears in the wild

2006 — Ransomware goes from 56-bit encryption to 660-bit RSA public key encryption

2008 — Scareware dominates with fake AV and rogue utility tools

2009
- Malware evolves from pushing rogue AV to encypting files
- Scam program FileFix Pro extorts $40 to "help" decrypt files

2010
- 10,000 ransomware samples
- Birth of Bitcoin
- Screen-locking ransomware appears

2012
- Over 10,000 ransomware samples
- Ransoms set to $200
- Law enforcement imitation ransomware appears

2013
- Over 250,000 ransomware samples
- Cryptolocker appears
- Useage of 2048-bit RSA encryption keys
- Ransomware demands increase to $300
- Crytolocker revenue reaches $300 million in 100 days

2015
- Over 4 million ransomware samples
- Ransomware as a service appears
- Teslacrypt appears

2016
- JavaScript ransomware appears
- Locky rises to prominence
- Hospital pays $17K in ransom
- Ransomware revenue surpasses $1 billion

2017 — WannaCry variant appears, impacting 150 nations globally

Timeline years: 2005 | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017