DETECTION AND RESPONSE GAME

IMPACT

DETECTION AND RESPONSE GAME

IMPACT

DETECTION AND RESPONSE GAME

IMPACT

DETECTION AND RESPONSE GAME

IMPACT

DETECTION AND RESPONSE GAME

IMPACT

DETECTION AND RESPONSE GAME

IMPACT

DETECTION AND RESPONSE GAME

IMPACT

DETECTION AND RESPONSE GAME

IMPACT

DATA DESTRUCTION

The hacker has overwritten large amounts of files and folders on every Windows device outside of the Windows folder with randomly generated data.

MITIGATION
Diversify backups

DETECTION
Monitor for large quantities of file modifications

RESOURCE HIJACKING

The hacker uses network resources to mine cryptocurrency with a crypto jacking script.

MITIGATION
Disable JavaScript

DETECTION
Monitor for common crypto mining software

ACCOUNT ACCESS REMOVAL

The hacker changed the passwords of all administrator accounts and logged off active users.

MITIGATION
Two- factor authentication for user privilege changes

DETECTION
Monitor for large quantities of user privilege changes

SERVICE STOP

The hacker stopped or disabled the email service to make it unavailable to all employees.

MITIGATION
Limit privileges of user accounts and groups

DETECTION
Monitor for edits or modifications to services and startup programs

DATA MANIPULATION

The hacker changes important product data to affect production.

MITIGATION
Encrypt sensitive information

DETECTION
Inspect important file hashes

DATA ENCRYPTED FOR IMPACT

The hacker encrypts large amounts of data to interrupt availability of system and network resources.

MITIGATION
Diversify backups

DETECTION
Monitor for large quantities of file modifications

DEFACEMENT

The hacker modifies the content of the company's official website in order to create a bad reputation.

MITIGATION
Diversify backups

DETECTION
Monitor websites for unplanned content changes

NETWORK DENIAL OF SERVICE

The hacker performs a Network Denial of Service attack on the DNS.

MITIGATION
Filter network traffic

DETECTION
Network monitoring tools