
RANSOMWARE
IT'S NOT IF, BUT WHEN

THIS IS A RANSOMWARE ALERT
ALL SYSTEMS ARE LOCKED

WHAT IS RANSOMWARE?

A TYPE OF MALICIOUS SOFTWARE DESIGNED TO BLOCK ACCESS TO A COMPUTER SYSTEM UNTIL A SUM OF MONEY IS PAID

HOW IS RANSOMWARE DIFFERENT THAN A VIRUS?

- RANSOMWARE IS MALICIOUS SOFTWARE WHICH ENCRYPTS FILES ON YOUR COMPUTER OR COMPLETELY LOCKS YOU OUT.
- RANSOMWARE SCRAMBLES YOUR FILES TO RENDER THEM UNUSABLE, THEN DEMANDS YOU PAY UP.
- VIRUSES INFECT YOUR FILES OR SOFTWARE, AND HAVE THE ABILITY TO REPLICATE.

WHO IS A TARGET?

EVERYONE

WHAT TYPE OF INFORMATION IS TARGETED?

ANY INFORMATION DEEMED ATTRACTIVE BY ANY RANSOMWARE ENGINEER

GOVERNMENTAL INCIDENTS

BALTIMORE

- $18 M IN REVENUE LOSS AND RECOVERY COSTS
- DID NOT PAY THE RANSOME
- 2 ATTACKS IN LESS THAN A YEAR
- NO BUSINESS CONTINUITY PLAN

LAKE CITY, FLORIDA

- PAID $600,000 RANSOME
- DISABLED THE CITY'S COMPUTER SYSTEMS FOR 2 WEEKS
  - PHONE LINES, EMAIL NETWORKS AND SERVERS, LOCKED CITY SYSTEMS
  - INFECTED DUE TO AN EMPLOYEE DOWNLOADING A DOCUMENT RECEIVED VIA EMAIL

22 TOWNS IN TEXAS

- $2.5 M RANSOME
- IMPACTED CITY SERVICES SUCH AS PAYMENT PROCESSING AND PRINTING OF IDENTITY DOCUMENTS
- TARGETS: TOWNS THAT WERE TOO SMALL TO HAVE THEIR OWN IT DEPARTMENTS
- DISABLED PAYMENT PROCESING
- 3 POLICE DEPARTMENTS
- ROOT CAUSE: VENDOR COMPROMISE

STATISTICS

- RANSOMWARE ATTACKS ARE ON THE RISE IN 2019 – UP 118 PERCENT
- THROUGH SEPTEMBER 621 REPORTED ATTACKS
- TOP 4 TARGETS ARE: HOSPITALS, HEALTH CARE CENTERS, SCHOOL DISTRICTS, AND CITIES
- TOTAL COST THROUGH SEPTEMBER 30 - $186 MILLION

SOLUTIONS

- PAY THE RANSOM
  - MAY GET DECRYPTION KEY
  - MAY GET ATTACKED AGAIN IN THE FUTURE
- RESTORE FROM LAST GOOD BACKUP
  - MAY REQUIRE MANUAL DATA INPUT
  - MAY HAVE VIRUS BACKED UP IN THE DATA
- RECOVER FROM STRONG DISASTER RECOVERY PLAN
  - MAY REQUIRE REPLACEMENT OF INFECTED HARDWARE (E.G., HARD DRIVES)
  - REQUIRES STRONG SECURITY PROGRAM
  - REQUIRES REGULAR SECURITY AUDITS

PREVENTION

- DATA MUST BE BACKED UP WITH REGULARITY
- DEVELOP STRONG DATA RETENTION POLICY – HOW LONG TO KEEP DATA
- CHECK INTEGRITY OF BACKED UP DATA REGULARLY TO AVOID INFECTION OF BACK UP
- BACKED UP DATA MUST BE STORED IN LOCATION THAT IS INACCESSIBLE TO HACKERS OR VIRUS
- SECURITY POLICIES MUST PREVENT ESCALATION OF PERMISSIONS
- EDUCATE USERS!

RECOMMENDATIONS

- ANNUAL SECURITY SUMMIT – FEDERAL, STATE, AND LOCAL
  - OPPORTUNITY TO COME TOGETHER TO LEARN BEST PRACTICES
- STATE/LOCALITY PARTNERSHIP
  - REVIEW AND UPDATE COOP PLANS
    - ADD RANSOMWARE PROTOCOL TO DISASTER PLANS
  - ALLOWS SHARING OF RESOURCES
- PROVIDE TECHNOLOGY GRANTS TO LOCAL JURISDICTIONS
  - GRANTS WOULD REQUIRE CONSISTENT METHODOLOGIES
  - ALLOWS LOCALITIES BETTER USE OF RESOURCES

SOURCES

- GARTNER SECURITY AND RISK MANAGEMENT SUMMIT 2018 PRESENTATION, FIX WHAT MATTERS; PROVIDE DEVOPS TEAMS WITH RISK- PRIORITIZED VULNERABILITY GUIDANCE JUNE 4-7, 2018
- CPOMAGAZINE.COM/CYBER-SECURITY/MASSIVE.RANSOMWARE ATTACK
- CBS NEWS WEBSITE, OCT 3 2019, HTTPS://WWW.CBSNEWS.COM/NEWS/RANSOMWARE-ATTACKS-ON-THE-RISE-AND-GOVERNMENTS-ARE-IN-THE-CROSSHAIRS/
- MSSP ALERT WEBSITE, OCT 3 2019, HTTPS://WWW.MSSPALERT.COM/CYBERSECURITY-NEWS/RANSOMWARE-ATTACK-HITS-BALTIMORE-CITY-SERVERS/
- MSSP ALERT WEBSITE, OCT 3 2019, HTTPS://WWW.MSSPALERT.COM/CYBERSECURITY-BREACHES-AND-ATTACKS/RANSOMWARE/LAKE-CITY-FLORIDA-PAYS-HACKERS/
- TREND MICRO WEBSITE, OCT 3 2019, HTTPS://WWW.TRENDMICRO.COM/VINFO/US/SECURITY/NEWS/CYBER-ATTACKS/TEXAS-MUNICIPALITIES-HIT-BY-REVIL-SODINOKIBI-PAID-NO-RANSOM-OVER-HALF-RESUME-OPERATIONS
- NPR WEBSITE, OCT 3 2019, HTTPS://WWW.NPR.ORG/2019/08/20/752695554/23-TEXAS-TOWNS-HIT-WITH-RANSOMWARE-ATTACK-IN-NEW-FRONT-OF-CYBERASSAULT
- KNOWBE4 INC., RANSOMWARE GUIDE, 2016, ACCESSED OCT 3 2019,HTTPS://WWW.KNOWBE4.COM/HUBFS/ENDPOINT%20PROTECTION%20RANSOMWARE%20EFFECTIVENESS%20REPORT.PDF