Ransomware and BEC attack briefing

Andy Green, Ph.D.

Assistant Professor of Information Security and Assurance

Kennesaw State University

Principal – Strategic Security Consulting Services

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Overview

- Introduction
- Ransomware
  - Definition
  - Scope
  - Cost to firms
  - Common attack vectors
  - Pre-attack measures
  - Post-attack response
- BEC
  - Definition
  - Scope
  - Cost to firms
  - Common attack vectors
  - Pre-attack measures
  - Post-attack response
- Q&A

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Introduction

- 20+ years in Information Security field as a practitioner
- Ph.D. in Information Systems / Information Security concentration
- Provide InfoSec consulting services focusing on SMB clients

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

My own sympathy has always been with the little fellow, the man without advantages.

Harry S. Truman

Ransomware

- Definition
  - Malware that prevents users from system access
  - Encrypts data and prevents user access
  - Adversary require payment to release systems and data
  - Data may be taken and sold to other adversaries

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Ransomware

- Scope
  - Global estimates
    - 2020 - $20 billion
    - 2019 - $11.5 billion
    - 2018 - $8 billion
  - Global cost per incident
    - 2020 - $8100
    - 2019 - $5900
    - 2018 - $4300
  - Global average cost of downtime per incident
    - 2020 - $283,000
    - 2019 - $141,000
    - 2018 - $46,800
  - $8500/hour lost due to downtime

Source: https://purplesec.us/resources/cyber-security-statistics/ransomware/

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Ransomware

- Cost to firms
  - Data loss
  - Employee downtime and production loss
  - Ransom
  - IT consultant time and labor
  - Forensic investigation cost
  - Data leak and compliance issues
  - Reputation harm and loss of business
  - IT infra upgrade or rebuild

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Ransomware

- Common attack vectors
  - Social engineering
  - Web browsing
  - Phishing
  - Compromised employee accounts and credentials
  - Software vulnerabilities
  - Systems exposed to Internet

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Ransomware

- Pre-attack measures
  - Ransomware policy
  - Incident response policy
  - Cyber insurance
  - Employee and client education
  - Robust backup and restore process
  - Endpoint protection
  - Vulnerability management process
  - Multi-factor authentication

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Ransomware

- Post-attack response
  - Activate incident response playbook
  - Isolate infected systems
  - Isolate or power off infected systems not fully corrupted
  - Contact law enforcement
  - Reset all account credentials
  - Do not pay ransom

Business email compromise (BEC)

- Definition
  - Email message sent by adversary designed to trigger funds transfer from the firm to the adversary
  - Attack comes in different variations
    - Spoofed email account or website
    - Spearphishing email sent to accounts payable
    - Firm executive's email account compromised and used to send directions to accounts payable
    - Diversion of payroll funds or W-2 data

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Business email compromise (BEC)

- Scope (2019 only)
  - Incidents – 23,775
  - Losses - $1,776,549,688
  - Average cost - ~$75,000

Source: https://pdf.ic3.gov/2019_IC3Report.pdf

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Business email compromise (BEC)

- Cost to firms
  - Data loss
  - Forensic investigation cost
  - Reputation harm and loss of business
  - Employee harm

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Business email compromise (BEC)

- Common attack vectors
  - Fraudulent emails
  - Fraudulent text messages
  - Fraudulent telephone calls

Business email compromise (BEC)

- Pre-attack measures
  - BEC policy
  - Incident response policy
  - Cyber insurance
  - Employee and client education
  - Multi-factor authentication
  - Out-of-band verification of changes or requests

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Business email compromise (BEC)

- Post-attack response
  - Contact law enforcement
  - Preserve data
  - Contact bank

Q and A

What did I not cover that you want to talk about?

What did I cover that you want more information about?

KENNESAW STATE UNIVERSITY
COLES COLLEGE OF BUSINESS
Department of Information Systems and Security

Thank you for your attention!

Andy Green, Ph.D.

andy.green@kennesaw.edu

agreen@stratsec.info