Cyber Threats and the Role of the FBI

Eric Brelsford
Special Agent
FBI CHICAGO

Thursday, March 31, 2022

- 56 Field Offices
  - –Cyber Task Forces
- 63 Legal Attaché Offices
  - –Cyber Agents within Attaché Offices
- FBI HQ
  - –Cyber Division
    - National Cyber Investigative Joint Task Force
    - Internet Crimes Complaint Center / CYWATCH

Who are the cyber adversaries?

- State-sponsored cyber attackers
- Financially motivated criminal hackers
- Hacktivists
- Insider Threats

What are the most prevalent attacks?

- Data Breaches
- Ransomware
- Business Email Compromise
- Financial Account Takeovers
- Denial of Service / Destructive Attacks

Data Breaches & Ransomware

- Ransomware is a simple concept – attacker encrypts all of your data and demands a payment to get it decrypted again.

- Evolution in ransomware – attacker now often first steals your data and then encrypts it.

- Attacker then threatens to post stolen data on the internet or sell it to other criminals unless you pay the ransom.

Typical method of compromise

- Phishing emails
- Unpatched internet-facing applications / servers
- Compromised remote access credentials (e.g. VPN / RDP)

Data Breaches & Ransomware

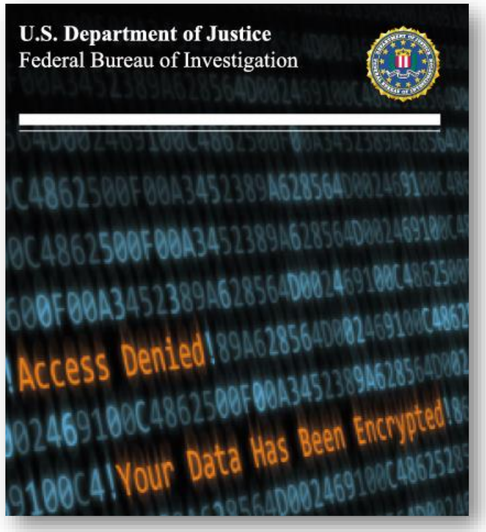
- After initial compromise:
  - Attackers attempt to obtain administrative account credentials and spread throughout the network.
  - Attackers typically “live off the land” and use built-in Windows tools (e.g. Powershell).
  - Attacker’s Primary objective: Get Domain Administrator credentials which can be used to deploy ransomware across network.
  - Hacked Domain Admin Account = Game Over

Data Breaches & Ransomware

- Amount of ransom demanded varies from a few thousand to millions. Ransom payment will be demanded in cryptocurrency (usually Bitcoin).

- Often ransomware gets deployed at off hours (nights, weekends, holidays) to minimize change the victim may discover it before its too late.

Paying the Ransom?



The Ransom

The FBI does not support paying a ransom to the adversary. Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after having paid a ransom. Paying a ransom emboldens the adversary to target other organizations for profit, and provides for a lucrative environment for other criminals to become involved. While the FBI does not support paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

How to Prevent Initial Compromise

- Keep your software updated (especially for internet facing systems/devices).
- Utilize multi-factor authentication for any remote access into your network.
- User awareness training (e.g. phishing exercises).
- Endpoint Detection & Response (EDR) software.
- Application whitelisting controls to prevent execution of unauthorized programs.

How to Prevent a Widespread Incident

- Require administrators to have regular accounts and separate privileged accounts that are used only when necessary.
- Strictly limit number of domain admin accounts and only use those accounts when and where necessary.
- Don’t use the same local administrator password across all systems. (e.g. use solutions like LAPS)
- Limit systems / network shares that users can access.
- Make regular backups that are secured.

How to Detect the Attack

- Endpoint Detection & Response (EDR) software.

- Robust monitoring of your logs and internal network traffic for anomalous activity:
  - Data exfiltration
  - Remote connections from unexpected locations / at unexpected times.

- Push alerts out for all domain admin logins / new admin account creations.

Business Email Compromise

- The business email compromise (BEC) is an online scam in which the attacker interacts with a victim via email while pretending to be someone they trust.

- Objective is to trick victim into wiring money to a bank account controlled by the criminal.

Business Email Compromise – How does it work?

- Attacker compromises an email account.
- Attacker will identify an upcoming payment to target OR will make up a nonexistent payment to try and submit.
- Attacker will either use the compromised email account to send the fraudulent emails OR will create a new email address that mimics the compromised account in appearance.
- Attacker will send victim an email with the attacker's bank account information included in it.

Business Email Compromise – How to protect against it?

- Multi-factor authentication for email access.
- Monitor for anomalous account login activity.
- Double-check the email address you are responding to.
- Don’t rely on just email for significant transactions (i.e. actually pick up the phone and call someone to confirm).

How to Report Cyber Incidents to the FBI

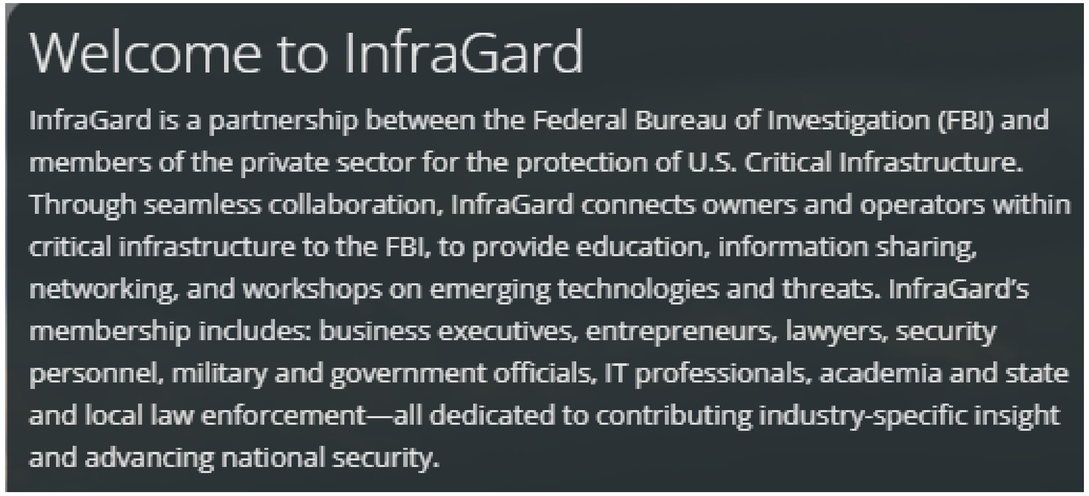
- Internet Crime Complaint Center (www.ic3.gov)
- Contact your local FBI Field Office (FBI Chicago: 312-421-6700)
- Valuable to establish liaison relationship with FBI prior to having an incident.

Reporting via IC3.GOV

- IC3.GOV
- IC3.GOV/Home/Ransomware

Infragard

- Infragard.org

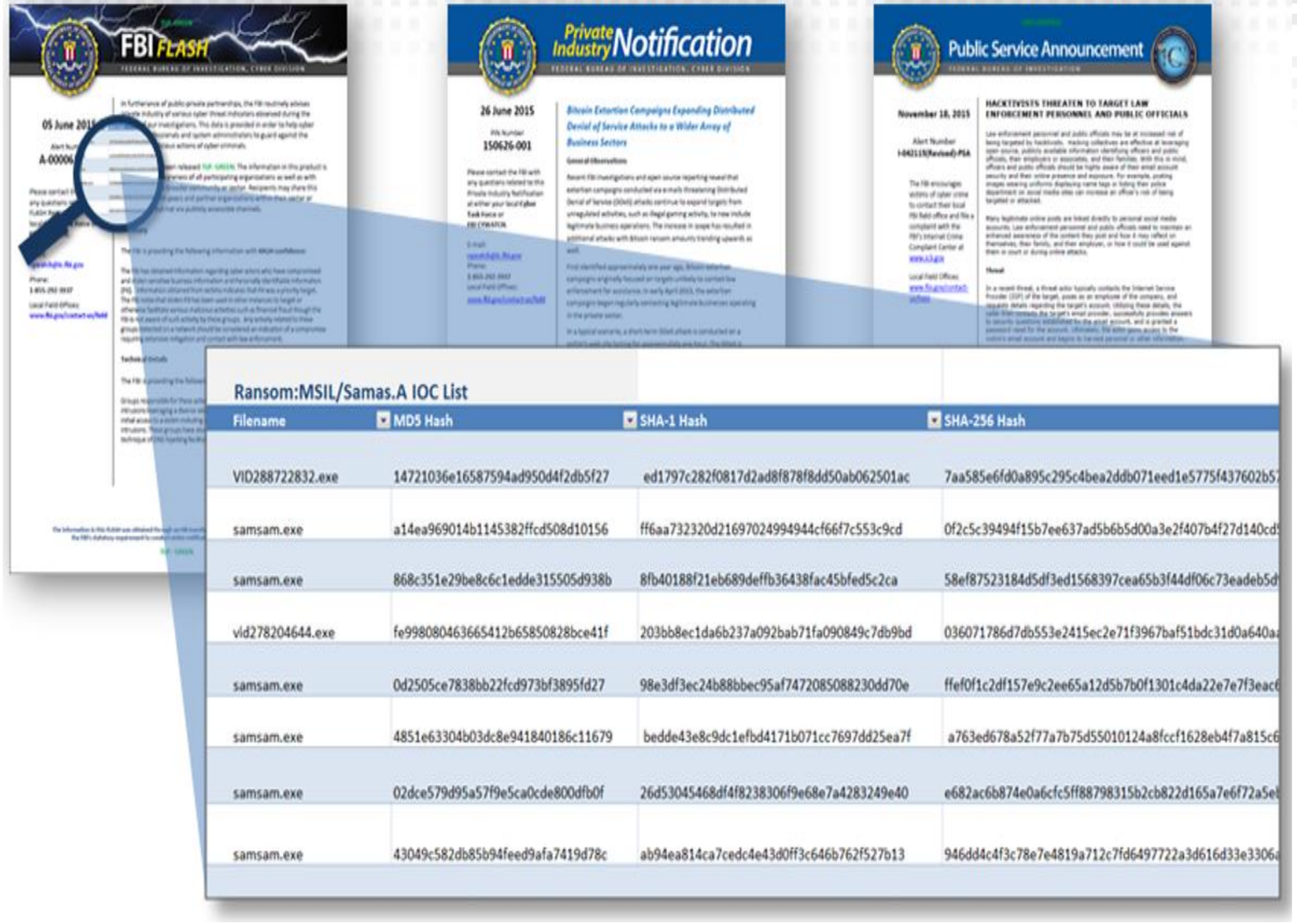


PINs - FLASHs

FLASH Messages

Private Industry Notifications

Public Service Announcements



“The most effective weapon against crime is cooperation… The efforts of all law enforcement agencies with the support and understanding of the American people”

- J. Edgar Hoover

CyberDIVISION
FEDERAL BUREAU OF INVESTIGATION

FBI SA Eric Brelsford
etbrelsford@fbi.gov

FBI CHICAGO CYBER