

Cyber Threats and the Role of the FBI



Eric Brelsford

Special Agent

FBI CHICAGO



Thursday, March 31, 2022



OUR MISSION PRIORITIES:

1. Protect the U.S. from terrorist attack
2. Protect the U.S. against foreign intelligence, espionage, and cyber operations
3. Combat significant cyber criminal activity
4. Combat public corruption at all levels
5. Protect civil rights
6. Combat transnational criminal enterprises
7. Combat significant white-collar crime
8. Combat significant violent crime

OUR CORE VALUES:

Respect • Integrity • Accountability
Leadership • Diversity • Compassion
Fairness • Rigorous Obedience
to the Constitution



OUR MISSION:

Protect the American People and Uphold the Constitution of the United States

UNCLASSIFIED

- 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



UNCLASSIFIED

Who are the cyber adversaries?



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

UNCLASSIFIED



UNCLASSIFIED

What are the most prevalent attacks?



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

UNCLASSIFIED



UNCLASSIFIED

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.

UNCLASSIFIED



UNCLASSIFIED



Typical method of compromise

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

UNCLASSIFIED



UNCLASSIFIED

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

UNCLASSIFIED



UNCLASSIFIED

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 chance the victim may discover it before it's too late.

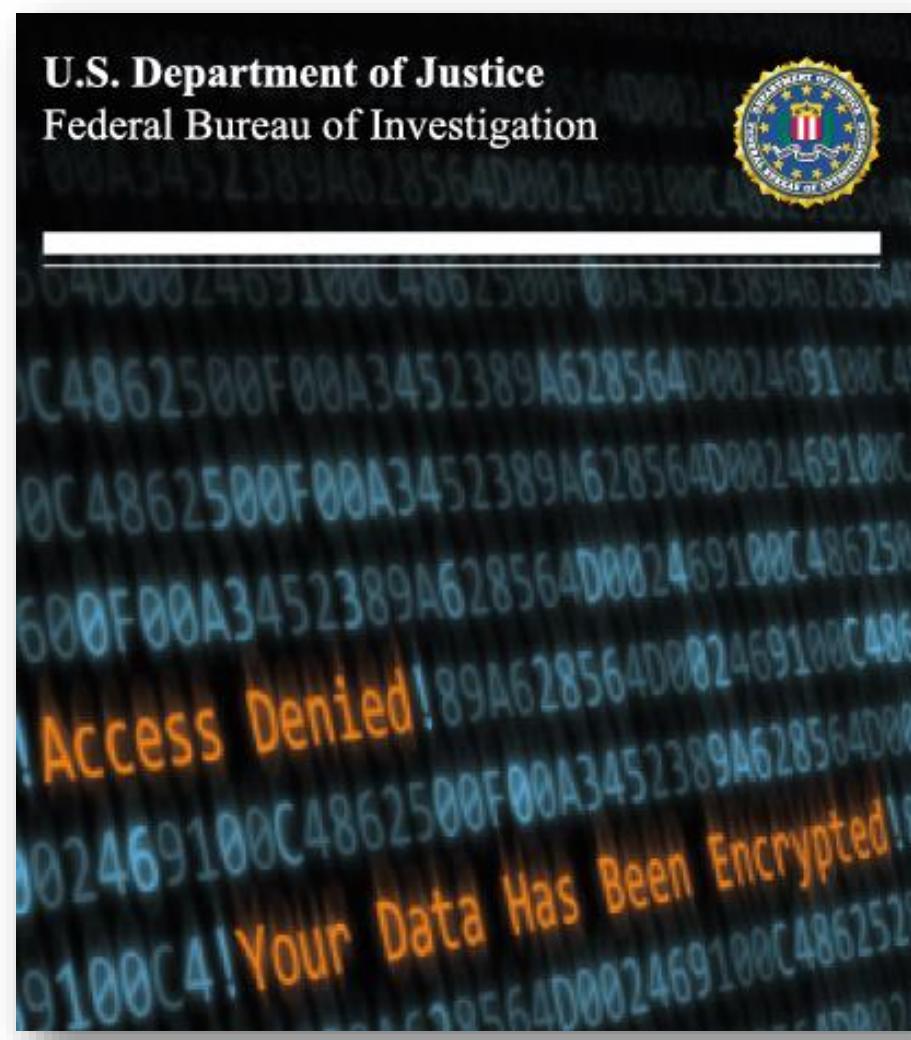
UNCLASSIFIED



UNCLASSIFIED



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.

UNCLASSIFIED



UNCLASSIFIED

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.

UNCLASSIFIED



UNCLASSIFIED

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.

UNCLASSIFIED



UNCLASSIFIED

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.

UNCLASSIFIED



UNCLASSIFIED

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.

UNCLASSIFIED



UNCLASSIFIED

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.

UNCLASSIFIED



UNCLASSIFIED

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).

UNCLASSIFIED



UNCLASSIFIED

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.



UNCLASSIFIED



UNCLASSIFIED

Reporting via IC3.GOV



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

The screenshot shows the homepage of the Internet Crime Complaint Center (IC3). The top navigation bar includes links for "FILE A COMPLAINT", "CONSUMER ALERTS", "INDUSTRY ALERTS", "BEC", "RANSOMWARE", "ELDER FRAUD", and "SCAMS". Below the navigation is the "FEDERAL BUREAU OF INVESTIGATION Internet Crime Complaint Center" logo. The main content area features a large blue padlock icon and the text "Filing a Complaint with the IC3". A subtext below states: "The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant." A red "File a Complaint" button is at the bottom.

The screenshot shows the "Ransomware" category page on the IC3 website. The top navigation bar is identical to the homepage. The main content area features the "FEDERAL BUREAU OF INVESTIGATION Internet Crime Complaint Center IC3" logo. The text "What is Ransomware?" is displayed, followed by a description: "Ransomware is a form of malware targeting both human and technical weaknesses in an effort to make critical data and/or systems inaccessible. Ransomware is delivered through various vectors, including Remote Desktop Protocol, which allows computers to connect to each other across a network, and phishing." A red "File a Ransomware Complaint" button is at the bottom.

UNCLASSIFIED



UNCLASSIFIED

Infragard



- Infragard.org

Welcome to InfraGard

InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure. Through seamless collaboration, InfraGard connects owners and operators within critical infrastructure to the FBI, to provide education, information sharing, networking, and workshops on emerging technologies and threats. InfraGard's membership includes: business executives, entrepreneurs, lawyers, security personnel, military and government officials, IT professionals, academia and state and local law enforcement—all dedicated to contributing industry-specific insight and advancing national security.

UNCLASSIFIED



UNCLASSIFIED

PINs - FLASHs



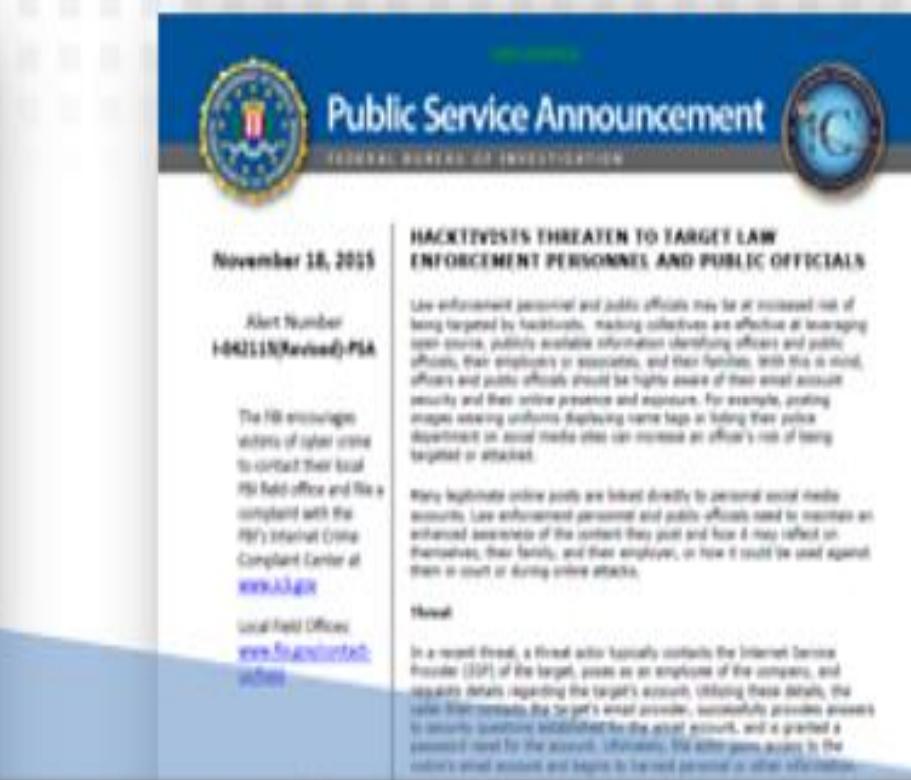
FLASH Messages



Private Industry Notifications



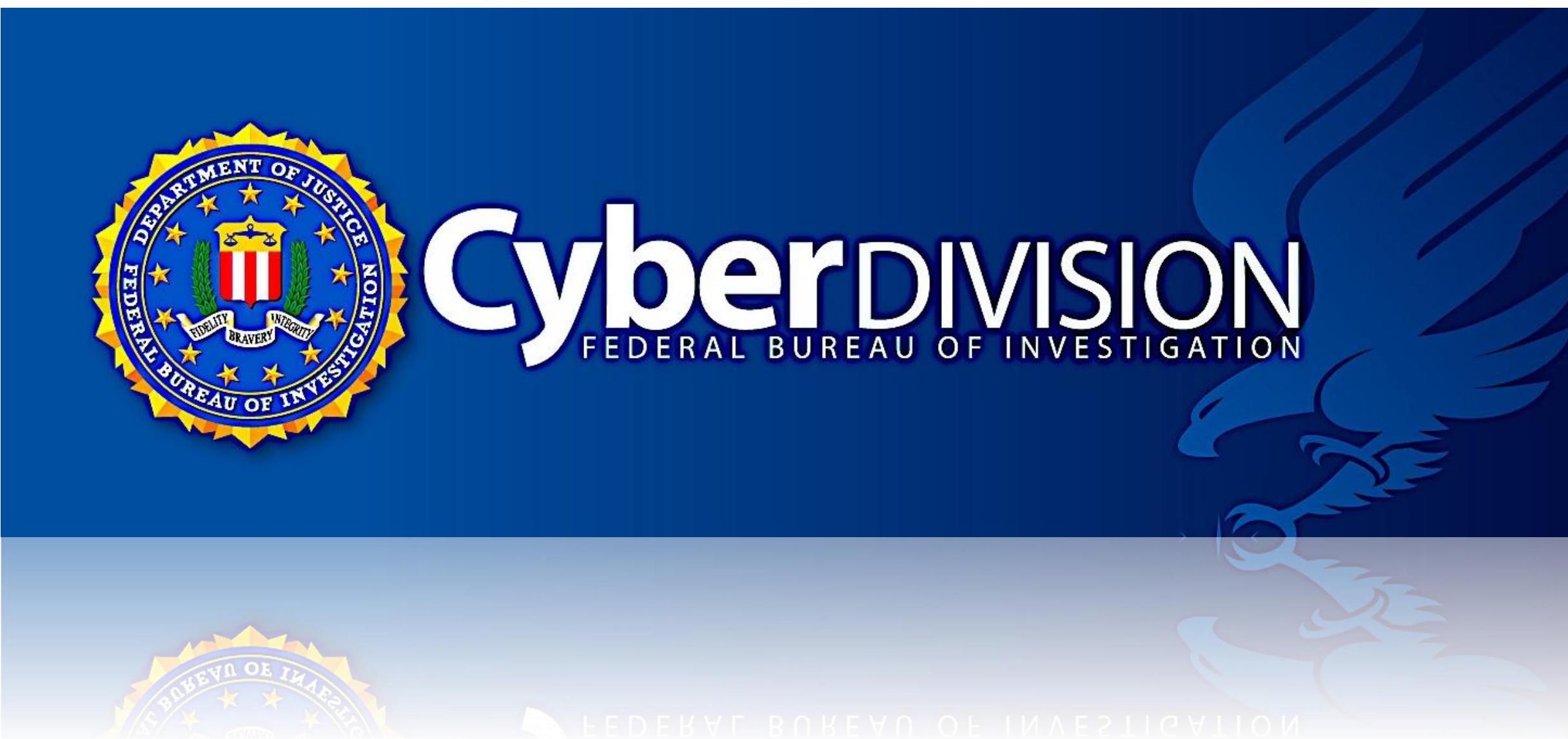
Public Service Announcements



Ransom:MSIL/Samas.A IOC List			
Filename	<input checked="" type="checkbox"/> MD5 Hash	<input checked="" type="checkbox"/> SHA-1 Hash	<input checked="" type="checkbox"/> SHA-256 Hash
VID288722832.exe	14721036e16587594ad950d4f2db5f27	ed1797c282f0817d2ad8f878f8dd50ab062501ac	7aa585e6fd0a895c295c4bea2ddb071eed1e5775f437602b57
samsam.exe	a14ea969014b1145382ffcd508d10156	ff6aa732320d21697024994944cf66f7c553c9cd	0f2c5c39494f15b7ee637ad5b6b5d00a3e2f407b4f27d140cd5
samsam.exe	868c351e29be8c6c1edde315505d938b	8fb40188f21eb689deff36438fac45bfed5c2ca	58ef87523184d5df3ed1568397cea65b3f44df06c73eadeb5d
vid278204644.exe	fe998080463665412b65850828bc41f	203bb8ec1da6b237a092bab71fa090849c7db9bd	036071786d7db553e2415ec2e71f3967ba51bcd31d0a640aa
samsam.exe	0d2505ce7838bb22fc973bf3895fd27	98e3df3ec24b88bbec95af7472085088230dd70e	ffef0f1c2df157e9c2ee65a12d5b7b0f1301c4da22e7e7f3eac6
samsam.exe	4851e63304b03dc8e941840186c11679	bedde43e8c9dc1efbd4171b071cc7697dd25ea7f	a763ed678a52f77a7b75d55010124a8fccf1628eb4f7a815c6
samsam.exe	02dce579d95a57f9e5ca0cde800dfb0f	26d53045468df4f8238306f9e68e7a4283249e40	e682ac6b874e0a6fc5ff88798315b2cb822d165a7e6f72a5e1
samsam.exe	43049c582db85b94feed9afa7419d78c	ab94ea814ca7cedc4e43d0ff3c646b762f527b13	946dd4c4f3c78e7e4819a712c7fd6497722a3d616d33e3306a

UNCLASSIFIED

“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



FBI SA Eric Brelsford
etbrelsford@fbi.gov



FBI CHICAGO CYBER