Boston CYBER TASK FORCE

FEDERAL BUREAU OF INVESTIGATION

FBI Boston Private Sector Cyber Task Force Newsletter March 2021 Edition

Important Note:

To receive FBI cyber alerts, including FBI Private Industry Notifications (PINs) and FBI Liaison Alert System (FLASH) Reports, send a request to be added to the distribution list for these products at Cyber_Outreach@fbi.gov.

Calendar Year 2020 Review: FBI Boston AOR Records 90 Ransomware Infections, a 23.6% Increase in Internet Fraud Complaints, and an Estimated $107 Million in Cyber Crime Losses

The FBI Boston AOR (Maine, Massachusetts, New Hampshire, and Rhode Island) recorded a 23.6 % increase in internet fraud complaints between calendar year 2019 (CY19) and calendar year 2020 (CY20) according to the FBI's Internet Crime Complaint Center (IC3.gov). A significant amount of complaints in CY20 were regarding malicious emails, websites and other cyber threats related to COVID-19 pandemic fraud.[i]

Statistics for each state in the FBI Boston AOR are listed in Table 1 below:

State	Number of Complaints	Total Adjusted Loss (million)
Maine	1,672	$3.3
Massachusetts	11,468	$85
New Hampshire	2,015	$9.1
Rhode Island	1,677	$9.6
Total	**16,832**	**$107.2**

Table 1: Total Complaints and Adjusted Financial Loss during CY20[1]

Year	Number of Complaints
2019	14,506
2020	16,832
Percentage Increase	**23.6%**

Table 2: Year-by-year Comparison of IC3 Complaints

[1] (U//FOUO) **Adjusted Loss**: The true nature of the impact from IC3 reports may be somewhat overstated as victims may inflate losses. The adjusted loss reflects IC3 assessment on the victim's actual financial loss. The level of activity is considered reliable. According to IC3's director, cyber crime incidents reported to IC3 typically only represent 10% to 12% of cyber crimes actually committed in the U.S. each year.

The most prevalent type of Cyber Crime Complaints in the Boston AOR during CY20:

IC3 Crime Type	Number of Reports	Financial Loss
Non-payment/Non-Delivery	3,248	$6,364,870
Extortion	2,884	$951,779
Identity Theft	1,759	$5,421,475
Personal Data Breach	1,287	$3,236,932
No Lead Value	914	$0
Spoofing	833	$8,212,522
Phishing/Vishing/Smishing/Pharming	805	$708,782
Misrepresentation	774	$649,146
BEC/EAC	753	$62,309,734
Confidence Fraud/Romance	569	$11,722,558

Table 3: Top 10 Cyber Crime Report Types in the Boston AOR during CY20

Ransomware Infections Impact in the Manufacturing Sectors

In CY20, there were 90 ransomware infections reported to the FBI Boston office. However, based on open source reporting, the actual number of ransomware infections in our region is sustainably higher. The top 5 industries targeted by these ransomware operators were as follows:

Industry	Infections	Percentage
Healthcare	15	16%
Manufacturing	13	14%
Web Commerce / IT Provider	12	13%
Construction	10	11%
Law Firms	9	10%

Table 4: Top 5 Industries Infected with Ransomware within FBI Boston AOR, January 1 through December 31, 2020.

Notably, 31% of reported ransomware infections in the Boston AOR in CY20 affected construction, manufacturing, and transportation entities.

Historically, the largest cyber threat to these organizations entities was espionage. Cyber actors would steal proprietary business data, executive communications, and business plans to benefit competitors. However, the top cyber threats now include ransomware infections, which have disrupted or halted production/operations, crippled supply chains, and led to the theft of employee and customer PII. On the surface, industries like banking and finance appear to be more lucrative ransomware targets; however, the manufacturing, transportation, and construction sectors are also at high risk to ransomware attacks.

Integration of Technology into Today's Manufacturing Facilities

Manufacturing facilities use physical machines but the advancement of technology and Internet-connected systems have introduced computer equipment into most manufacturing environments. Engineering workstations which contain blueprints, design documents, programs, and configuration settings are often necessary to manufacture products. Although a ransomware attack that affects these file repositories and databases would not necessarily disrupt the production line, it would hamper business operations, supply chain management, and product engineering and design. Additionally, data obtained from ransomware infections could include technology data concerning the operation of pumps, compressors, and motors. According to a July 2020 report published by security firm Kivu Consulting, the manufacturing sector paid 62% of total ransomware payments in 2019. (Source: Trend Micro; "The Impact of Modern Ransomware on Manufacturing Networks"; Source: https://www.trendmicro.com)

In May 2020, security firm FireEye reported that the manufacturing sector was the second most targeted sector by all ransomware variants, after the government sector.[ii]

The FBI continues to investigation and pursue ransomware groups and their individual actors. In January 2021, FBI Tampa participated in a coordinated international law enforcement action to disrupt a sophisticated form of ransomware known as NetWalker. The NetWalker action includes charges against a Canadian national in relation to NetWalker ransomware attacks in which tens of millions of dollars were allegedly obtained, the seizure of approximately $454,530.19 in cryptocurrency from ransom payments, and the disablement of a dark web hidden resource used to communicate with NetWalker ransomware victims. For information on the Netwalker actions please visit the Department of Justice press release at: https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware

Individual Pleads Guilty to Participating in Internet-of-Things Cyber Attack Affecting New Hampshire-based Dyn, Inc., in 2016

In December 2020, an individual, formerly a juvenile, pleaded guilty to committing acts of federal juvenile delinquency in relation to a cyberattack that caused massive disruption to the Internet in October 2016.

According to court documents and information gathered by FBI Boston's office, in September and October of 2016, the individual and others created a botnet, which was a variant of the Mirai botnet, for use in launching DDoS attacks. Mirai infected "Internet-of-Things" devices, such as Internet-connected video cameras and recorders, and turned them into bots to be used to launch DDoS attacks.

On Oct. 21, 2016, the individual and others used the botnet they created to launch several DDoS attacks in an effort to take the Sony PlayStation Network's gaming platform offline for a sustained period. The DDoS attacks impacted a domain name resolver, New Hampshire-based Dyn, Inc., which caused websites, including those pertaining to Sony, Twitter, Amazon, PayPal, Tumblr, Netflix, and Southern New Hampshire University (SNHU), to become either completely inaccessible, or accessible only intermittently for several hours that day. As a result of the individual's DDoS attacks, Dyn, Sony, SNHU, and other entities and individuals suffered losses including lost advertising revenues and remediation costs. Sony estimated that its resultant losses included approximately $2.7 million in net revenue. For information on this guilty plea, please visit the Department of Justice press release at: https://www.justice.gov/opa/pr/individual-pleads-guilty-participating-internet-things-cyberattack-2016

[i] IC3.gov | https://www.ic3.gov/media/2020/200401.aspx

[ii] Open Source Report | *TrendMicro* | "The Impact of Modern Ransomware on Manufacturing Networks" | 8 July 2020 | https://www.trendmicro.com/en_us/research/20/l/the-impact-of-modern-ransomware-on-manufacturing-networks.html | accessed 27 December 2020