H-ISAC TIC Threat Bulletin

Date: December 13, 2018

TLP – GREEN

Event: Email Bomb Threats Demanding Bitcoin Payments Observed

Summary: Multiple organizations across the country are reporting having received email threats indicating that threat actors had placed explosive devices within their facilities and are demanding Bitcoin payment in order to avoid their detonation.

Assessment: These email messages appear to match patterns associated with common extortion scams, with the exception of the verbiage specific to a bomb threat. At this time, the TIC assesses the credibility of these threats as low.

Relevance: These email threats are being reported across multiple industries, including healthcare. State law enforcement agencies are reportedly investigating these threats, with some having resulted in facilities being evacuated. We have heard reports of multiple schools and hospitals being evacuated in response to these threats. At this time, we do not have any indication that explosive devices have been located within any of the facilities that have received these email threats. We have also not observed any traffic to the Bitcoin wallets reported as having been associated with these email threats.

IOCs:

Sender IP addresses observed:

- 194.58.61[.]134
- 134.0.115[.]208
- 178.21.11[.]42
- 194.58.58[.]70
- 194.58.61[.]73

Observed Bitcoin wallet addresses:

- 12bzhtdr2kx5Tum4MJqmsfiePnKFvQLw7L
- 1DKej2QVvLWf2B8kJpqvnUGycmoS3Rm7C9
- 1LVZqNEUHnhGxZ2qgJApd3qbHWZtpMhkAo
- 1BHasGex1jhRZeY7KyUGGKUNRtVgKedRY8
- 19nShJMkTbP6VCVaoAjzzTQuXLPzXH1Qb7
- 1Dnw2qJxGFCZdE3PzCaVioBB9zERc7SzRB
- 1GHKDgQX7hqTM7mMmiiUvgihGMHtvNJqTv

- 1LeReNiUgHNXvvR8TpgQG1b5nzqoKeUxDY
- 1CdD3nthrWR76RkL1WwLH7BSqCFASLjbhu

Observed email subject lines:

- Your building is under my control
- Think twice
- You don’t have much time
- You are responsible for people
- I give you a chance
- Bomb is in your building

Observed email senders:

- Hannah[@]viscositycups[.]com
- Niko[@]viscositycups[.]com
- Frank[@]broadwayboxing[.]com
- Sofia[@]amiracles[.]com
- Danny[@]odalog[.]com

Example email text:

Subject: Your building is under my control

Hello. There is an explosive device (tronitrotoluene) in the building where your company is located. It is assembled according to my guide. It has small dimensions and it is covered up very carefully, it is impossible to damage the structure of the building by my explosive device, but in case of its explosion there will be many victims. My man is watching the situation around the building. If any unnatural behavior, panic or emergency is noticed he will blow up the device. I can withdraw my mercenary if you make a transfer. You transfer me $20'000 in BTC and the bomb will not detonate, but do not try to cheat -I ensure you that I will withdraw my mercenary solely after 3 confirmations in blockchain network.

Here is my BTC address - 12bzhtdr2kx5Tum4MJqmsfiePnKFvQLw7L

You must pay me by the end of the working day. If you are late with the transaction the bomb will explode. Nothing personal, if you don’t transfer me the bitcoins and an explosive device detonates, next time other commercial enterprises will send me more money, because this is not a one-time action. For security and anonymity reasons, I will no longer enter this email account. I check my Bitcoin address every forty min and after receiving the bitcoins I will give the command to my person to leave your district.

If the explosive device blows up and the authorities notice this message! We are not terrorists and dont take responsibility for acts of terrorism in other buildings.

Potential Actions:

1. Check your email gateways for indications that users within your facilities may have received similar email messages.

2. Alert your HelpDesk staff to be on alert for any reports of incoming emails matching the reported pattern.
3. Report any observed indicators.

References:

1. https://www.reddit.com/r/sysadmin/comments/a5wb42/latest_bitcoin_extortion_spam_is_now_bomb_threats/
2. https://whdh.com/news/authorities-investigating-after-multiple-bomb-threats-emailed-to-bay-state-businesses/
3. https://www.wkbw.com/news/local-news/buffalo-police-investigating-multiple-bomb-threats
4. https://www.geekwire.com/2018/spam-bomb-threats-schools-businesses-nationwide-demand-bitcoin-ransom-payments/
5. https://www.nbcchicago.com/news/national-international/Bomb-Threats-Across-United-States-502713491.html