GLOBAL GUARDIAN

THREAT ASSESSMENT – BOMB THREAT EMAILS

13 DECEMBER 2018

Prepared for: GALLAGHER

INTRODUCTION

Threat Assessment Overview

Purpose: To conduct a deep dive threat assessment of the series of bomb threats made to institutions across the United States and Canada.

Global Guardian attempted to answer the following questions:

- What is the nature of the threat that has manifested and how severe is it?
- What prompted this massive cyber-attack and why now?

Situation Update & Executive Summary

On 13 December 2018, hundreds of businesses, law enforcement agencies and public services across the United States and Canada received email threats demanding a bitcoin payment of $20,000 in the early afternoon, prompting evacuations, building sweeps and overloading police call centers. What's more, the bomb threats sewed panic across the continent and undoubtedly defrauded thousands. Global Guardian concurs with many police departments assessment that the threats were not predicated on credible evidence — no explosive devices have been found or are likely to be found in the coming hours. The scale of this mass bomb threat implies that:

(a) The perpetrators commanded serious resources, indicating possible state actors

(b) The motivation was disruption (and possibly showcase capability), rather than monetary gain

Risk Probabilities

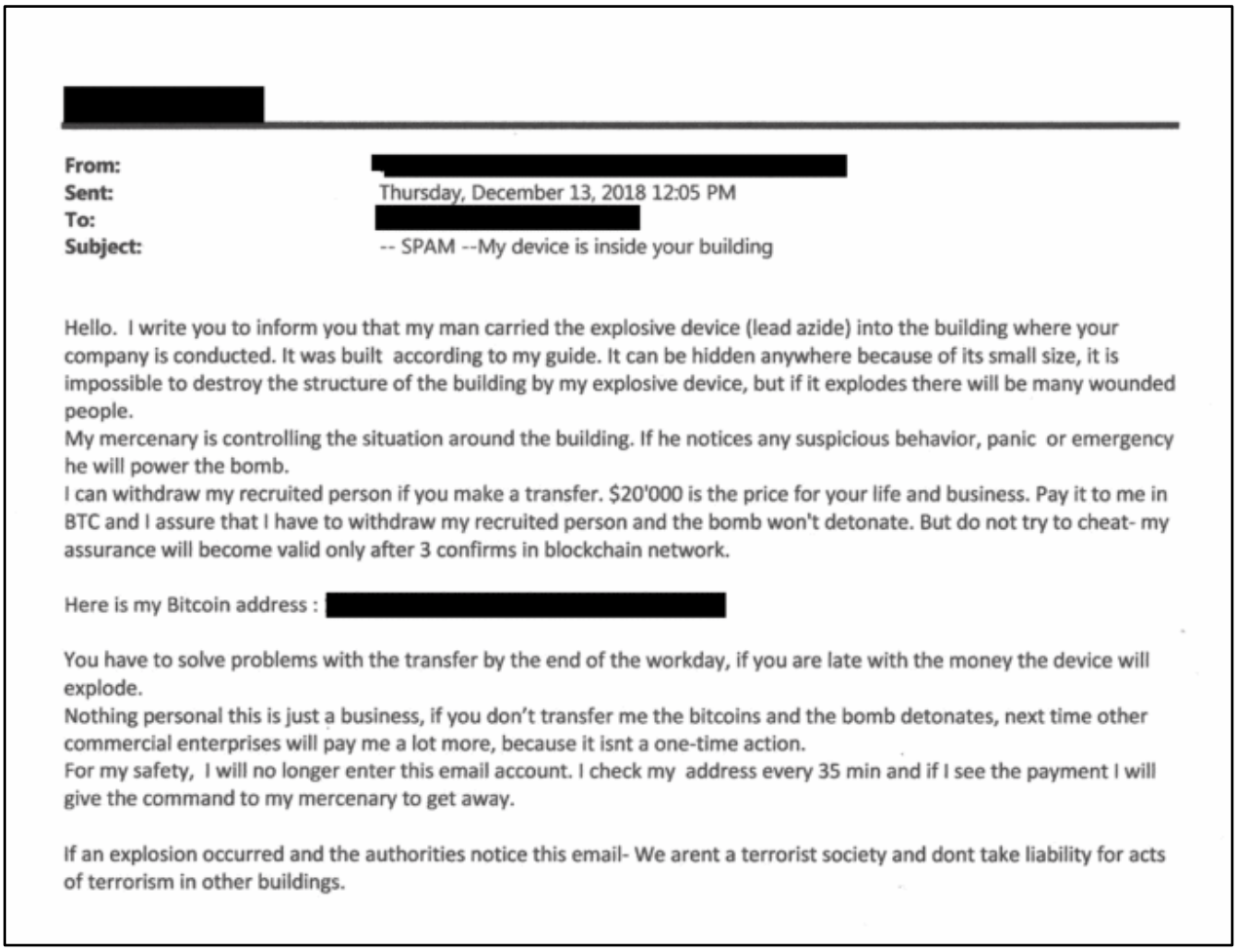
- Materialization of bomb threat – LOW
- Copycat incidents – MEDIUM

Recommendations

- Based on information uncovered during its initial investigation, Global Guardian recommends against opening any subsoquent emails with similar subject lines
- Global Guardian recommends against issuing any cryptopayment to any anonymous body
- Global Guardian recommends the consideration of a **Global Guardian Defender program**, wherein cyber assessments, asset hardening are conducted.
- Additionally, we recommend **continued online monitoring** of threats and sentiment toward Gallagher or any of its clients, stakeholders or shareholders

Findings

The following section contains a summary of the information that Global Guardian was able to gather through open sourced intellegence and simple text analysis.



[redacted]

From: [redacted]
Sent: Thursday, December 13, 2018 12:05 PM
To: [redacted]
Subject: -- SPAM --My device is inside your building

Hello. I write you to inform you that my man carried the explosive device (lead azide) into the building where your company is conducted. It was built according to my guide. It can be hidden anywhere because of its small size, it is impossible to destroy the structure of the building by my explosive device, but if it explodes there will be many wounded people.
My mercenary is controlling the situation around the building. If he notices any suspicious behavior, panic or emergency he will power the bomb.
I can withdraw my recruited person if you make a transfer. $20'000 is the price for your life and business. Pay it to me in BTC and I assure that I have to withdraw my recruited person and the bomb won't detonate. But do not try to cheat- my assurance will become valid only after 3 confirms in blockchain network.

Here is my Bitcoin address : [redacted]

You have to solve problems with the transfer by the end of the workday, if you are late with the money the device will explode.
Nothing personal this is just a business, if you don't transfer me the bitcoins and the bomb detonates, next time other commercial enterprises will pay me a lot more, because it isnt a one-time action.
For my safety, I will no longer enter this email account. I check my address every 35 min and if I see the payment I will give the command to my mercenary to get away.

If an explosion occurred and the authorities notice this email- We arent a terrorist society and dont take liability for acts of terrorism in other buildings.

Figure 1: Copy of Bomb Threat Email *Source: CNN*

- It is clear the author is not a native English speaker or that he/she sought to lead authorities to place attribution on a foreign entity
- If the author's intent was to accrue revenue, he/she would have given more detailed payment instructions. The use of cryptocurrency is more prevalent amongst individuals under 45, the targets of the attacks do not match the demographics of crypto users
- The statement: "We aren't a terrorist society" implies the need to rebuke terrorism. Therefore, it is likely that the origination of the email comes from a society under threat of terrorism

Recent Incidents

- **09/08/2018 - Chinese Ministry of State Security (MSS) — the country's civilian spy agency — breach Marriott's Starwood chain hotel reservation system**. The hack resulted in the stealing of private information and travel details of as many as 500 million people. Specifically, names, addresses, phone numbers, passport numbers and credit card numbers, as well as information on where people traveled and with whom were obtained in the cyber-attack.
    - On 12 December, Secretary of State Mike Pompeo insinuated that China was behind the attack on network news.
- **12/13/2018 – EU declared an extension of economic sanctions on Russia over Ukraine conflict.**

Analysis

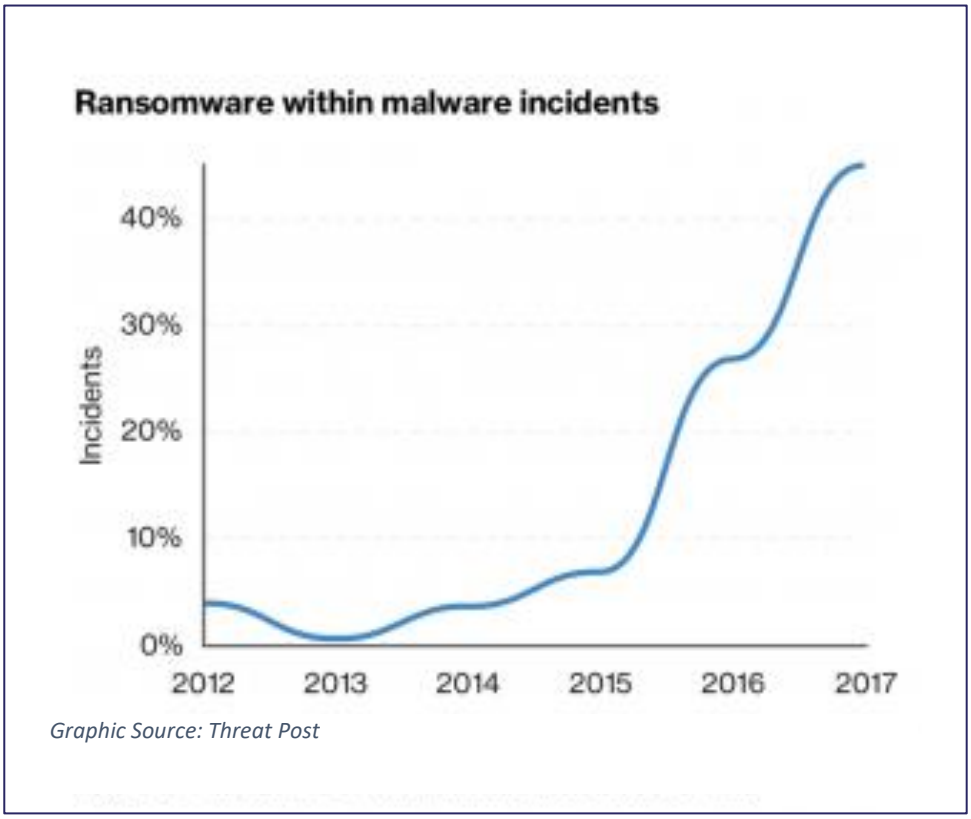
The timing, motivation and the actual text of the bomb threat likely point to Russian involvement. Whether or not there was actual state involvement, is yet to be determined. Numerous cyber-attacks originating from Russia have occurred following international condemnation or implementation of sanctions. As stated above, the goal of the attack was to sow chaos and cause disruption. Since the event comes on the heels of possibly the largest cyber-attack by a state actor — especially, given how it compliments the data obtained from China's other hacks of US government databases — it is conceivable that a group of Russian hackers, either saw vulnerability or wanted to prove that they too possess the capability to disrupt Western institutions on a mass scale. Finally, the reproach of "terrorism" and poor English are compatible with Russian hackers.

Bomb Threat Emails in Context

Today's event did occur within a vacuum, but rather, it should be considered within the wider theater of cyber-crime in general. While the mass cyber-attack did not employ code as sophisticated as that of malicious software, those responsible have been encouraged by the success and rapid proliferation of ransomware.

- **Ransomware is now the most prevalent type of malicious software used in cyber-attacks. Ransomware is a crypto virus — a type of malware that extorts its victims by threatening to block access to specific files or an entire system or drive, potentially crippling the day-to-day operations of an organization. Unlike older and less advanced malware, ransomware is able to target critical business systems, which can do more damage to an organization, making it possible to extort higher ransoms and devastate operations.**

- Ransomware attacks have been increasing in frequency over the last five years, and the last six months have witnessed a 229 percent year-to-date increase. This type attack is appealing to attackers because they are low cost and high reward: they are difficult and costly to attribute; and the use of cryptocurrencies allows the attackers to receive untraceable payment. Ransomware takes one of two forms: lockers and cryptos



Graphic Source: Threat Post

Conclusion

It is critical that bomb threats are viewed as a well-coordinated cyber-attack, rather than an ordinary criminal act or extortion. The Bomb Threat attacks illustrate our vulnerability and susceptibility as a society to more sinister cyber-attacks, specifically, malware or ransomware. Had the email included an attachment for a credit card authorization or a hyperlink, then millions of computers across the continent could have become infected. Further, the disruption caused by the incident will likely spawn future copycat attacks and may be used as future benchmark for amateur cyber-criminals or hacktivists. Finally, today's events do not even constitute the tip of the iceberg as far as the cyber capabilities of states including China, Iran, Russia and North Korea. In 2019, we are likely to see at least one of these actors demonstrate their cyber-might by attacking multinationals and governments of their rivals.

CONTACT US

Please contact the 24/7 Global Guardian Operations Center at any time with questions or comments on this special report, or for any travel security need.

Email: operationscenter@globalguardian.com

Phone Numbers
Emergency Line: +1 (703) 566-9475
Non-Emergency: +1 (703) 566-9463