ASSOCIATION OF AMERICAN RAILROADS

RAIL AWARENESS DAILY ANALYTIC REPORT (RADAR)

December 11 - 14, 2018

Worldwide: Weekly Incident Map

RADAR Map December ...

December 10 - 14, 2018

- Minnesota: Activists Claim Shut Down of...
- United Kingdom: Man Sentenced for Pos...
- United Kingdom: Three Suspected Neo-...
- Symantec Announces New Product Inte...
- Ireland: Increased Security for Sallins an...
- North America: US District Judge Blocks...
- Canada: Antifa Activists Protest Global ...
- Ukraine: Ukraine's Infrastructure Suscept...
- Oregon: Activists to Argue Dangers of Oi...
- Ohio: FBI Announces the Arrests of Two ...
- Connecticut: Police Documents Shed Lig...
- Canada: Experts Says Organized Crime i...
- France: Shooting in Stasbourg's Christm...
- United Kingdom: Environmental Activists...
- Researchers Identify New Trojan Being D...
- Pennsylvania: Anarchist Publication War...
- United Kingdom: Police Raid Newcastle ...
- Researchers Identify Phishing Campaign...
- New Malware Campaign Targets Global ...

Summary of Content

➢ Weekly Incident Map

➢ Rail Security Awareness

- North America: US District Judge Blocks Keystone XL Pipeline 'Preconstruction'
  - ❖ On Friday, December 7, a United States District Court judge in Montana ruled that TransCanada can proceed with planning Keystone XL pipeline construction. However, the judge further ruled that any sort of "preconstruction" work on the pipeline project is prohibited. Under this ruling, "preconstruction" includes transporting pipeline pieces and erecting work camp sites along the proposed route.
- Oregon: Activists Argue Dangers of Oil Trains at Port of St. Helens Commission Meeting
  - ❖ On Wednesday, December 12, activists with Stand Up To Oil and Columbia Riverkeeper attended the Port of St. Helens Commission meeting to demand denial of a request from energy company, Global Partners, for refinement of heavier materials at its Port Westward facility. None of the posted communications on the action indicated an intent to disrupt rail operations. Nor did any such activity occur.

➢ Active Shooter

- Connecticut: Police Documents Shed Light on Mind of Sandy Hook School Shooter
  - ❖ According to published reports, a court recently ordered Connecticut State Police to release documents from the investigation into the massacre at Sandy Hook Elementary School. These documents reportedly include several writings by attacker Adam Lanza that shed light on his anger, scorn for other people, and deep isolation in the years leading up to the shooting.

➢ Terrorism

- Worldwide: Effectiveness of "See Something, Say Something" Programs in Attack Prevention in Public Surface Transportation
  - ❖ As of December 2018, the renowned Mineta Transportation Institute (MTI) has published an analysis of the effectiveness of "See Something, Say Something" programs in detection and prevention of terrorist plots directed at public surface transportation. Addressing the fundamental question, "Do 'See Something, Say Something' programs work?," the MTI report concludes that evidence strongly suggests that in the specific case of public surface transportation, the answer is "yes." Transport staff and passengers play an important role in the prevention of terrorist attacks. In economically, advanced countries, which includes the United States and Canada, more than 14 percent of the attempts are detected – and this rate has been improving.

Summary of Content

➢ **Terrorism (cont'd)**

- **France: Suspect in Shooting Attack near Strasbourg Christmas Market Killed by Police**
  - ❖ **On Thursday, December 13, French police killed the lone attacker who opened fire in a mass shooting at the Christmas market area in Strasbourg, France, on Thursday evening, December 11. The deceased suspect, Cherif Chekatt, killed three people and caused serious injuries to several others. The Amaq news agency, affiliated with ISIS, claimed Chekatt is a soldier of the Islamic State.**
- **Ohio: FBI Announces the Arrests of Two Domestic Terror-Plotters in Toledo**
  - ❖ **On Monday, December 10, the FBI announced the arrests of two people in Ohio on separate and unrelated domestic terrorism plots. One is an alleged ISIS-supporter who planned to attack a synagogue; the other is an anarchist who allegedly planned to bomb a pipeline.**

➢ **Cyber**

- **Worldwide: Threat Actors Use of SSL Certificates for Encrypted, Validated Websites**
  - ❖ **An article published on Thursday, December 13, states researchers "discovered over 1,150 new HTTPS phishing sites over the course of one day, not including the plethora of the malicious HTTP phishing URLs" already known – meaning "a new secure phishing site goes up every two minutes." The lack of an entry barrier for obtaining SSL/TLS certificates allows hackers to obtain certificates inexpensively.**
- **Worldwide: Save the Children - Loss of $1 Million to Business Email Compromise**
  - ❖ **A published article on Friday, December 14, indicates that a Business Email Compromise, which occurred in May 2017 but announced only recently, resulted in misdirection of almost $1 million in funds from Save the Children to an unidentified recipient in Japan.**
- **Worldwide: McAfee Report – Rising Sun Variant in 'Operation Sharpshooter'**
  - ❖ **A report published on Wednesday, December 12, indicated organizations in the transportation sector, as well as nuclear, defense, energy and financial companies, were targeted by the Rising Sun implant variant with 14 backdoor capabilities in 'Operation Sharpshooter' – a "campaign…masquerading as legitimate industry job recruitment activity [to] gather information to monitor for potential exploitation."**
- **Canada / United States: Numerous Emailed False Bomb Threats in Hoaxes Attempting to Perpetrate Cyber Fraud**
  - ❖ **On Thursday, December 13, numerous law enforcement jurisdictions in the United States and Canada reported hoax bomb threats sent by email in an apparent large-scale attempt to perpetrate cyber fraud targeting private business organizations, schools, government departments and agencies, and individual residences. All messages contained a demand for payment of funds to avoid detonation of the purported explosive. All proved to be hoaxes. Security advisories shared technical details for awareness and preventive measures.**

North America: US District Judge Blocks Keystone XL Pipeline 'Preconstruction'

On **Friday, December 7**, 2018, a **United States District Court judge in Montana ruled** that **TransCanada can proceed with planning Keystone XL pipeline construction**. However, the judge **further ruled that any sort of "preconstruction" work on the pipeline project is prohibited**.

- According to the judge, **"preconstruction" includes transporting pipeline pieces and erecting work camp sites along the proposed pipeline route**.

This ruling effectively **prevents TransCanada from proceeding with the project** – because the order banning "preconstruction" precludes action to transport the 80-foot long segments of pipe to storage areas for work in Montana. Nor can TransCanada establish work camps to support construction work. The judge's order directly affects at least two sites in northern Montana – which constitute the starting points for construction work on the Keystone XL project in the United States.

In response to this federal court decision, **Native American and environmentalist groups have declared victory** in their fight against the pipeline. A leader among the identified groups involved with pushing for a court injunction against the pipeline in Montana has been the **Indigenous Environmental Network**.

The judge who made the ruling, Brian Morris, justified his stance by stating **that additional reviews on safety procedures need to be conducted by TransCanada before beginning with construction**. Judge Morris stated that **TransCanada failed to prove that it had properly tested for such issues as oil spills and greenhouse gas emissions**. [1]

North America: US District Judge Blocks Keystone XL Pipeline 'Preconstruction'

The federal District Judge in this case used a term that has gained favor in recent actions by activists professing opposition to fossil fuels development, production, and transport – "preconstruction" activities. As noted, these include transportation of materials used for building a planned pipeline.

Two actions conducted by tribal and environmental activist groups in Minnesota late last month specifically focused on disruption of "preconstruction" activities. During the morning of Tuesday, November 27, Native American groups posted videos and images from these actions to oppose transport of materials for the Enbridge Line 3 pipeline. Canadian energy company Enbridge is replacing the Line 3 pipeline that transports tar sands crude oil from Hardisty in Alberta to Superior in Wisconsin. The cited triggers for the November 27 actions were the rail delivery of pipes and their storage in volume by Enbridge for work on the project. One of the sites targeted in a demonstration by a small group numbering just several tribal activists set up a teepee, or tripod, bearing a banner opposing construction on a roadway leading to an area to which BNSF Railway had delivered pipe for further transport by truck to Enbridge storage areas near anticipated work sites for the project.

The participants contended that even preparation for construction is unlawful because Enbridge has not obtained all of the required permits for completion of the project. The federal District Judge who ruled to block "preconstruction" activities for the Keystone XL pipeline ruled that TransCanada had failed to complete necessary preparatory actions, delineating specific safety tests.

Oil Trains Stopped Near Lake Superior

submitted anonymously to the Earth First! Journal

On Nov. 19th, action was taken on the invisible border of Wisconsin and Minnesota to halt and block the movement of oil trains to and from one of the refineries on Lake Superior, near the Namadji River. This was done by "tricking" the sensor system on the rails to "believing" there was a train already present on the tracks, thus impeding the way for oil to be transported via railroad for many hours. Our actions today are in solidarity with all those fighting to oppose the racist & colonial Enbridge Line 3, but especially, today of all days, we are in solidarity with the Youth Climate Interveners!

The United States District Court's emphasis on "preconstruction" activities may have two substantial effects – more legal actions brought by activist groups to obtain orders precluding preparations for construction and more direct actions seeking to disrupt such preparations.

In this context, the visible delivery of materials by rail, notably pipe, may trigger more actions intended to disrupt train operations or block or impede access to rail yards and other supporting facilities. A recent anonymously posted false claim of disruption of oil train traffic at the eastern border area between Minnesota and Wisconsin "for many hours" further indicates a potential shift in attention to rail operations.

Oregon: Activists Argue Dangers of Oil Trains at Commission Meeting

On **Wednesday, December 12**, at **8:30 am local time (LT), activists associated with Stand Up To Oil and Columbia Riverkeeper** attended the **Port of St. Helens Commission meeting to demand that officials deny a request from energy company, Global Partners, for refinement of heavier materials at its Port Westward facility**.

The event occurred at the **St. Helens Library,** located at 375 South 18th Street in **St. Helens, Oregon** (45.855044, -122.814852) – a venue located **less than ½ mile from Portland and Western Railroad track.**

On their social media sites, both generally and on pages for this event, organizers specifically highlight the "risks posed by oil trains and oil spills" as one of their primary concerns in opposing the Global Partners' request. The activists directly assert that "oil trains are dangerous" and cite the derailment that occurred in Mosier, Oregon, in early June 2016 as evidence of this allegation. Their overall stance is that if Global Partners' request is granted, the company's oil trains will travel through "Columbia River Gorge, Spokane, Vancouver and/or Portland, and through Columbia County communities." As a result, they are demanding that the Port Commissioners "decline Global's request and protect public health, safety, and drinking water" from the risks posed by oil trains.

It should be noted that Stand Up To Oil and the Washington Environmental Council have additionally created petitions on their websites encouraging supporters to join their cause and support ongoing efforts to convince the Port Commissioners to deny Global Partners' request. Similar to the event page created by Stand Up To Oil, the Washington Environmental Council places particular emphasis on the message, "Oil Trains are dangerous," at the start of its petition.

Significantly, none of the posted communications on participation in the Port Commission meeting indicated an intent to stage actions targeting railroad assets. Nor did any such activity occur. 2, 3, 4

DEC 12

Port of St. Helens Commission Meeting

Public · Hosted by Stand Up To Oil and Columbia Riverkeeper

★ Interested ✓ Going Share ···

Wednesday, December 12, 2018 at 8:30 AM – 4 PM PST
2 days from now · 41–50°F Rain Showers

375 S 18th St, St Helens, OR 97051-2215, United States Show Map

Hosted by Stand Up To Oil
Typically replies within a few hours Message Host

STAND UP TO OIL communities fueling change

Oil Trains are dangerous.

Urge the Port of St. Helens Port Commissioners to decline Global Partner's request to handle crude oil trains.

Connecticut: Police Documents Shed Light on Mind of Sandy Hook School Shooter

According to published reports, a **court recently ordered Connecticut State Police to release documents from the investigation into the massacre at Sandy Hook Elementary School**. These documents reportedly include **several writings by attacker Adam Lanza that shed light on his anger, scorn for other people, and deep isolation in the years leading up to the shooting**.

- In the attack executed in December 2012, **Lanza first shot his mother before driving to the school and killing 20 children and six educators before ultimately shooting himself**.
- Even with several years of effort, **investigators have not been able to establish a clear motive for the attack**.

In one **online communication with a fellow gamer,** Lanza wrote: **"I incessantly have nothing other than scorn for humanity. I have been desperate to feel anything positive for someone for my entire life."**

A report by the Connecticut child advocate said Lanza's severe and deteriorating mental health problems, his preoccupation with violence, and his ease of access to his mother's weapons "provided a recipe for mass murder." From 10th grade, Lanza's mother kept him at home, where he spent long hours playing violent video games. His medical and school records included references to diagnoses of autism spectrum disorder as well as anxiety and compulsive disorder.

The newly released documents were seized by authorities during a search of Lanza's home. They include some of his own writings, such as the "Big Book of Granny," which describes violence against children, and a spreadsheet listing the mass killings dating back to Lanza also wrote a list, captioned "Problems," detailing a range of grievances including lights that are too bright and his hair touching his brother's towel.

Other writings from Lanza express hatred for "fat people" and for doctors who touched him during physical examinations as a child. There are reportedly references to pedophilia as a form of love. In another message written to an online gamer, he said: "Most of my social contact was through those players. All of them are typical detestable human beings, and it bred an aura of innumerable negative emotions for me. You were a respite from that." 5, 6

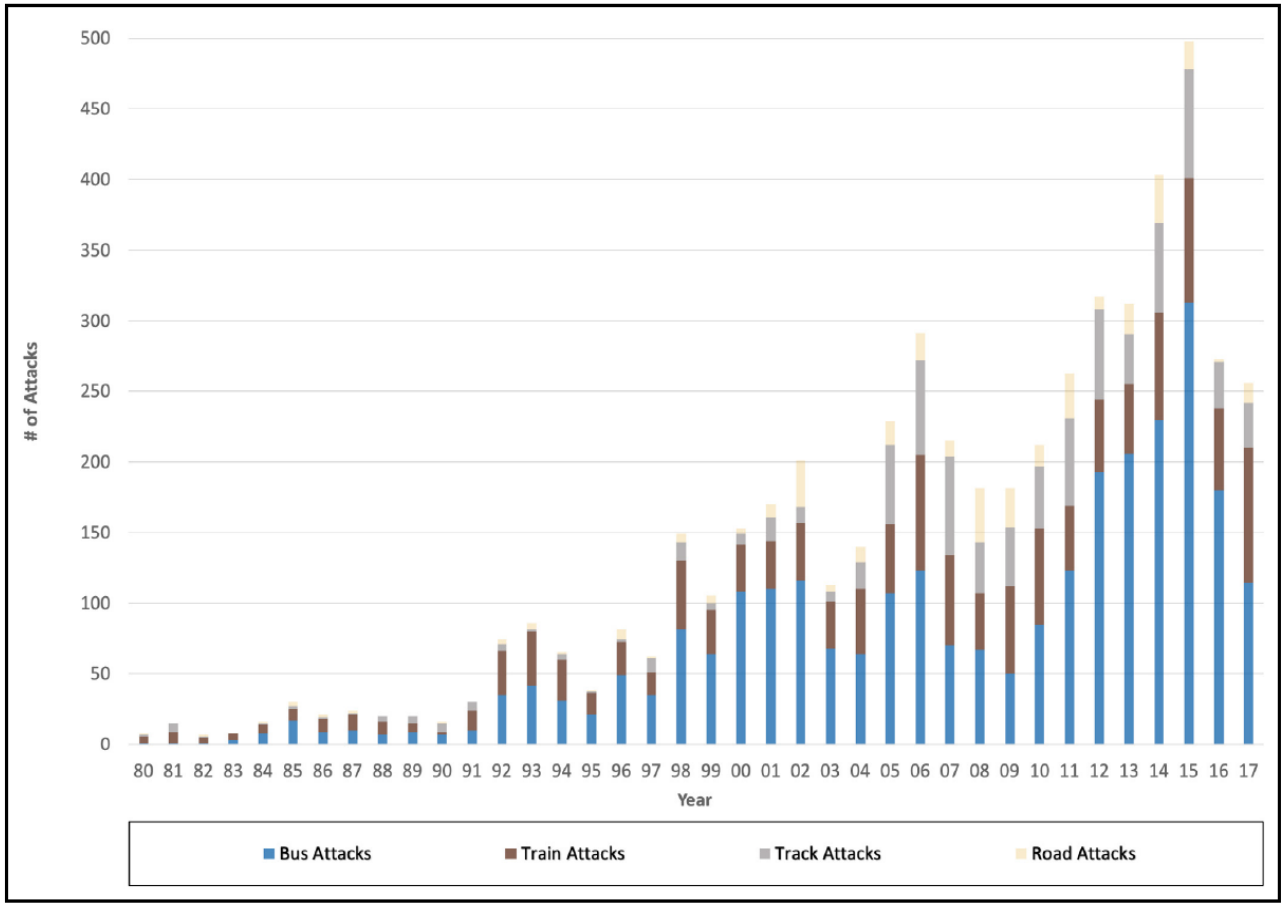
Worldwide: MTI Analysis - Effectiveness of "See Something, Say Something"

As of **December 2018**, **Brian Michael Jenkins** and **Bruce R. Butterworth** of the renowned **Mineta Transportation Institute (MTI)** have published an **analysis of the effectiveness of "See Something, Say Something" programs in detection and prevention of terrorist plots directed at public surface transportation**.

Based on its empirical analysis, **MTI has determined that more than 10 percent "of the documented attempted attacks on public surface transportation systems worldwide were foiled because some individual at the scene saw and reported something suspicious."** MTI clarifies that while the practical effects of "See Something, Say Something" campaigns were not necessarily evaluated, the analysis supports the conclusion that "heightened awareness contributes to the detection and prevention of attacks."

Prevention Rates by Geographical Group and Target Category

	All Attacks	% Detected All	# Attacks Group One	% Detected Group One	# Attacks Group Two	% Detected Group Two	# Attacks Group Three	% Detected Group Three
Bus	2793	6.6%	141	5.0%	2328	6.4%	324	9.3%
Train	1381	13.3%	311	14.8%	1045	12.7%	25	16.0%
Track	835	17.6%	168	18.5%	666	17.3%	1	N/A
Road	363	12.9%	14	42.9%	349	11.7%	0	N/A
All	5372	10.5%	634	14.2%	4388	10.0%	375	10.0%



Number of Attacks by Target Category

Data results culled from **5,372 incidents** – comprised of **2,793 against buses, 1,381 against trains, 835 against rail tracks, and 363 on roadways occurring from January 1970 to the end of 2017 – were examined** to delineate the **range of public surface transportation target categories**; **evaluate successes in rates of detection and prevented attacks**; determine factors that **differentiated between prevention of suicide bombings and responses to reported suspicious packages**; establish whether general economic conditions geographically contributed to variations in detection rates; and further **detail factors contributing to detection, deterrence, and prevention**. 7

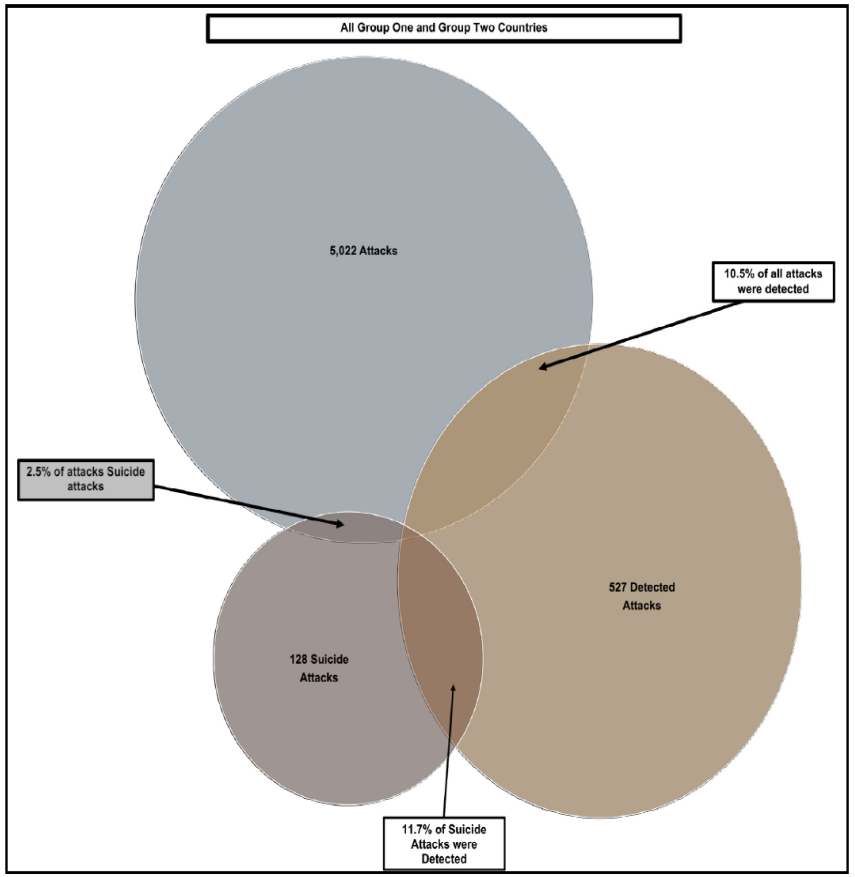
Worldwide: MTI Analysis - Effectiveness of "See Something, Say Something"

Addressing the fundamental question, "**Do 'See Something, Say Something' programs work?**," the MTI report concludes that **evidence strongly suggests** that in the specific case of **public surface transportation**, the **answer is "yes."**

Transport staff and passengers play an important role in the prevention of terrorist attacks. By **discovering and reporting suspicious objects**, they have **prevented more than 10 percent** of **all terrorist attacks on public surface transportation**. Detection rates are even better in **economically advanced countries** where **more than 14 percent of the attempts are detected** – and this rate has been improving. This statistical analysis suggests that "See Something, Say Something" campaigns are worthwhile. Key findings in the report from analysis of detections since 1970 follow:

Prevention Rates by Geographical Group and Target Category

	All Attacks	% Detected All	# Attacks Group One	% Detected Group One	# Attacks Group Two	% Detected Group Two	# Attacks Group Three	% Detected Group Three
Bus	2793	6.6%	141	5.0%	2328	6.4%	324	9.3%
Train	1381	13.3%	311	14.8%	1045	12.7%	25	16.0%
Track	835	17.6%	168	18.5%	666	17.3%	1	N/A
Road	363	12.9%	14	42.9%	349	11.7%	0	N/A
All	5372	10.5%	634	14.2%	4388	10.0%	375	10.0%



Overall Detection Rates: **On-site police, security personnel, transportation employees, train and bus passengers, and ordinary citizens have prevented 10.6 percen**t of the 5,372 terrorist attacks on train, bus, track and road targets in public surface transportation systems since 1970. Of the prevented attacks, **99% involved the discovery of suspicious packages that almost always turned out to be functioning bombs**.

Suicide bombings: Although it would seem that suicide bombings, where the device is concealed on the bomber would be more difficult to detect than explosive devices left in public places where people may discover them, the **data show that the rate of detecting suicide bombers at 13.8 percent is better than the rate for detecting devices left by non-suicide attacks, which is 10.6 percent**. In **Israel, the West Bank and Gaza Strip**, which have experienced a disproportionate share of suicide bombings - 63 (or 18 percent) of the world's total of 195 - the **record of detection at 19 percent is considerably higher** than the world average for detection of non-suicide devices. The rate of detection of the 128 suicide bombings in all **other countries excluding Israel is 11.7 percent**, which is comparable to, if slightly higher than, the **detection rate for non-suicide attacks which is 10.2 percent**. 8

Worldwide: MTI Analysis - Effectiveness of "See Something, Say Something"

Although suicide bombers, when confronted, often still detonate their devices, the resulting casualties are far less than if they had detonated their bombs at the intended target. The MTI report assesses that the recorded data on detection rates for suicide attackers "suggests that training programs designed to detect particular behaviors of suicide bombers (including clothing that can hide a device) can be effective." Specifically acknowledged is the impact of suicide attackers - "In nearly half of the detected suicide attacks, there were fatalities or injuries." Also, addressed, however, is the mitigating effect of detection and confrontation in significantly diminishing the suicide attacker's ability to inflict high numbers of fatalities. "The average number of deaths per attack for undetected suicide attacks worldwide is high—11.4— whereas the same figure for detected suicide attacks worldwide is only 1.1."

The data does suggest, interestingly, that detection of suicide bombers isn't less robust than the detection of objects left by non-suicide attackers. In fact, it is the reverse. The detection rate for suicide bombers in Israel and the West Bank & Gaza Strip is 19 percent (as opposed to 8 percent for non-suicide attacks), and the detection rate for all other countries is 11.7 percent (slightly higher than for the 10.2 percent for non-suicide attacks). Looking at all countries together, the overall detection rate for suicide attacks is 13.8 percent, and 10.6 percent for non-suicide attacks.

Geographical Differences: What are categorized in the report as Group One countries (those like the United States with high income economies) have the highest detection rates - 14.2 percent. Group Two countries (rest of the world, including Russia and China, but excluding Israel and the West Bank and Gaza Strip) account for far more attacks - 4,388 versus 634 - and detect only 10.0 percent. Group Three (Israel and the West Bank and Gaza Strip), with only 350 attacks, detect the same - 10.0 percent.

Figure 13: % of Detected Attacks by Target Category

Target Category	All % Passengers etc.	All % Security Officials	All % Unknown
Bus	29.7%	26.5%	43.8%
Train	23.5%	27.3%	49.2%
Track	10.9%	25.9%	63.3%
Road	2.1%	42.6%	55.3%
All	20.5%	27.9%	51.6%

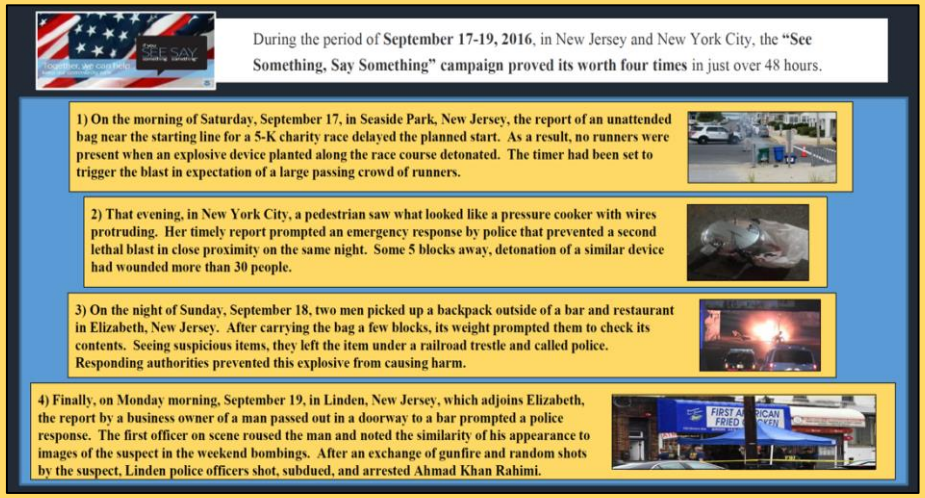
<u>Changes in Detection Rate by Target Category and Geography</u>: With the exception of 14 road attacks - a number too small to reveal trends - Group One countries have shown the greatest improvement. The detection rates for track targets is approaching 30 percent; it is at 20 percent for train targets. Meanwhile, detection rates in Group Two countries are improving for all target categories. Finally, for Group Three countries (Israel/West Bank/Gaza), the detection rate has declined for bus targets and increased for train targets. There were no road attacks and only one track attack so no trends are reported. However, if the time frame begins at 1990 instead of 1980, there is some improvement for detection of attacks against buses and a slight decline for train targets. There are a few cases - only eight - in which the device found had failed to detonate; there were also eight hoax devices, left to disrupt operations at the targeted entity. 9

Worldwide: MTI Analysis - Effectiveness of "See Something, Say Something"

Who is Detecting the Devices: In roughly half of the preventions, researchers were not able to determine who was responsible for the detection. Worldwide, police and security personnel account for approximately 28 percent of the detections. Transport employees (other than security personnel) and passengers account for approximately 21 percent. Some of the unknown detections could be additional finds by employees and passengers.

Categories of Detectors and Target Categories: Worldwide, transport employees and passengers play the greatest role in detecting attacks on bus targets (29.7 percent of the detections) and train targets (23.5 percent).

> Detecting suspicious behavior is necessarily a judgment with subjective elements, which can lead to reports and confrontations that reflect personal prejudices. While controversial in the United States even when used by police, behavioral detection is widely used by law enforcement organizations abroad. Israeli authorities seem to have become good at detecting suicide bombers, unfortunately because the frequency of the threat demanded it, and under the threat conditions faced by Israel's civilian population, they tolerated the false alarms and damage to dignity.
>
> This is not a call for increased efforts by the public to track down potential terrorists. Rather, the research presented here concludes that alert security personnel, transportation staff, and passengers have played a role in thwarting terrorist attacks by reporting suspicious objects. It will always be a low-yield activity, but detecting and reporting suspicious objects has demonstrably enabled police to prevent over 500 attacks.



Categories of Detectors and Geography: Passengers, other citizens and transport employees account for the highest share of detections for attacks on bus targets in Israel, the West Bank, and Gaza Strip. Meanwhile, in the Group One countries, transport employees, citizens, and passengers on train and bus systems account for 30.4 percent and 28.6 percent respectively of detections against those targets. [10]

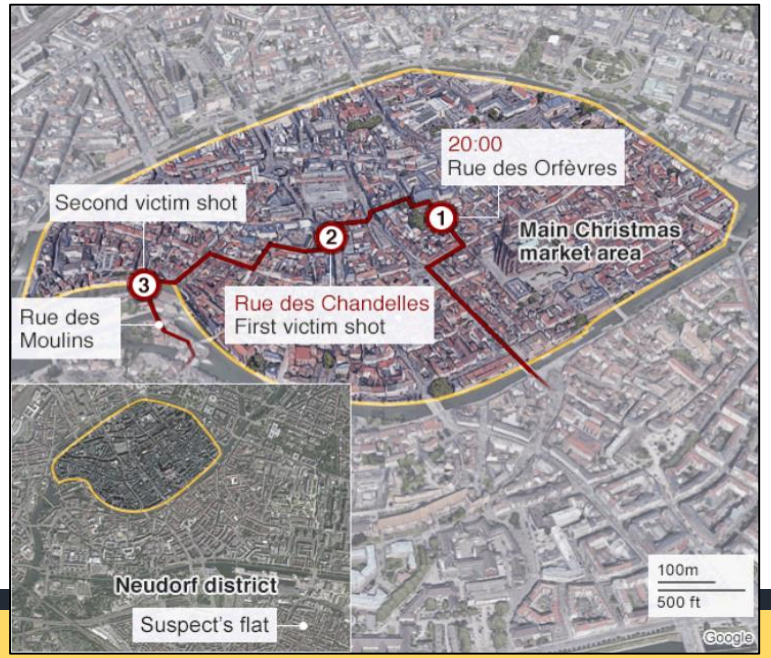
Practical Application: Continuous improvement is the constant goal of security plans and programs generally and for employee and public security awareness in particular. The MTI report cites the content of the slide at left, embedded with this report, developed by the Association of American Railroads and disseminated via the Railway Alert Network. The slide depicts the four instances over the course of about a 48-hour period during September 17 - 19, 2016, in which members of the public in New York City and in Seaside Park and Elizabeth, New Jersey, "saw something and said something," prevented harm, and supported progress in the investigation in identifying and arresting the attacker. The most effective way to show the value of "See Something, Say Something" is to highlight its successes. This slide does so; the MTI report does so; as do summaries of disrupted plots posted by the FBI on its public website as part of news releases on arrests and charging of terrorist suspect. Ironically, a tool purportedly developed to ensure the public understands the terrorism threat and the role they can play in detection and prevention – the National Terrorism Advisory System Bulletins – do not. This despite specific input, including the AAR slide, provided on multiple occasions by the Critical Infrastructure Cross Sector Council, comprised of representatives of each of the sectors and sub-sectors. After joint meetings with DHS earlier this week, the Council will offer its input anew – to enhance the effectiveness of the Bulletins in meeting their intended purpose.

France: Suspect in Shooting Attack near Strasbourg Christmas Market Killed

On **Thursday, December 13**, 2018, French police killed the lone attacker who opened fire in a mass shooting at the Christmas market area in Strasbourg, France, on Tuesday, December 11. The French Interior Minister confirmed the action by police and the death of the identified suspect, Cherif Chekatt.

Interior Minister Christophe Castaner reported that **three police officers had spotted a man matching Chekatt's description** on rue du Lazaret, in the Neudorf area of Strasbourg, at **9:00 pm local time** on **Thursday evening**. As the officers moved to stop him, the **suspect turned around and opened fire**. The **officers fired back and "neutralized" the attacker**. Interior Minister Castaner later visited the scene.

Chekatt killed three people in the shooting at the Christmas market, opening fire at pedestrians at about **8:00 pm local time on Tuesday night, December 11**. Several more people suffered serious injuries. The attacker, aged 29, had multiple criminal convictions in France and Germany. He had allegedly become a radicalized Islamist while serving time in prison for conviction of these offenses. [11]



The attack occurred close to the famed Christmas market near place Kléber, which attracts thousands of visitors. France's anti-terror prosecutor, Rémy Heitz, said the man had shouted "Allahu Akbar" ("God is greatest") as he opened fire. Chekatt was reportedly armed with a gun and a knife and escaped the area after jumping into a taxi. As he fled he came into contact with four soldiers and fired at them, as well. The soldiers fired back, apparently hitting him in the arm. The taxi driver reported that Chekatt that he had killed 10 people and had been injured during a firefight with soldiers. He ordered the taxi driver to drop him near the police station in Neudorf. When he got out of the vehicle, Chekatt fired at police officers before escaping. A search of his apartment in Neudorf revealed a grenade, a rifle, four knives, and ammunition.

The self-styled news agency for the Islamic State of Iraq and Syria (ISIS), Amaq, posted a claim on Thursday, December 13, that Chekatt was "an Islamic State soldier" who had "carried out the operation in response to calls for targeting citizens of coalition countries "fighting its militants in Syria and Iraq." This type of claim, using the same terminology each time, has now become commonplace for any incident involving a Muslim attacker. No further evidence of a connection to ISIS was offered. [12]

Ohio: FBI Announces the Arrests of Two Domestic Terror-Plotters in Toledo

On **Monday, December 10**, 2018, the **Federal Bureau of Investigation (FBI) announced the arrests of two people in unrelated domestic terrorism plots**.

The first case involved **21-year-old Damon Joseph**, who **allegedly planned attacks against synagogues in Toledo, Ohio, on behalf of the Islamic State of Iraq and Syria (ISIS)**.

- Joseph had been the **target of an undercover FBI investigation for several months after agents determined he was a radicalized supporter of ISIS.**

As his radicalization progressed, the FBI reported, **Joseph's online jihad turned into a physical jihad, in which he plotted to harm Jews**.

- He allegedly stated, **"Jewish people were evil and deserved what was coming to them," in the wake of the recent synagogue shooting in Pittsburgh**.
- Further, he allegedly **expressed his admiration for the attack to an undercover FBI agent.**

Joseph is **additionally accused of making videos with the hope they would be used to recruit for ISIS**.

On Sunday, December 2, Joseph allegedly forwarded a document laying out his plans for an attack, using the name "Abdullah Ali Yusuf" for himself.

- **In what is described as a kind of memo, he allegedly described plans to attack where the most people are gathered, inflict mass casualties, and make sure no one escaped.**
- **He then allegedly expressed that he did not necessarily see this attack as "a martyrdom operation" as his plan accounted for an escape and potential combat with law enforcement.**

At a meeting with an undercover agent on Thursday, December 6, in the Toledo area, Joseph provided the exact details of his attack plan, which included the address of the synagogue and the purchase of AR-15 AK-47 semi-automatic rifles, Glock pistols, and ammunition for each of these firearms.

- **Joseph allegedly stated that he wanted to time the attack to coincide with the Jewish Sabbath in order to ensure maximum carnage.**
- **He also specifically stated that he wanted to kill a rabbi.**

Authorities arrested Joseph on Friday, December 7. He will remain in custody until his case is heard before a grand jury for determination of indictment. [13], [14]

Ohio: FBI Announces the Arrests of Two Domestic Terror-Plotters in Toledo

The **second case, unrelated to the first, involves 23-year-old Elizabeth Lecron, accused of purchasing and transporting materials that could be used in a bomb for a domestic terror plot in Toledo**.

- According to the FBI, she **purchased black powder and hundreds of screws that she expected would be used to make a bomb.**
- Lecron allegedly had been **active on social media and glorified and expressed admiration for mass murderers**, such as the **Columbine High School shooters** in 1999 and **Dylann Roof, who committed a mass shooting at a Charleston church in 2015**.

After her **Tumblr account was shut down because of offensive content,** Lecron started a **new profile under the name "CharlestonChurchMiracle**," where she **continued to post photos and comments about mass casualty attacks**, the FBI alleged in a public statement on her arrest and charging.

In August 2018, undercover FBI agents began communicating with Lecron. At one point, she allegedly divulged that she and an associate had devised a plan to commit an "upscale mass murder" at a Toledo bar. Lecron stated the bar only had two ways in or out, which could be a tactical advantage when police arrived.

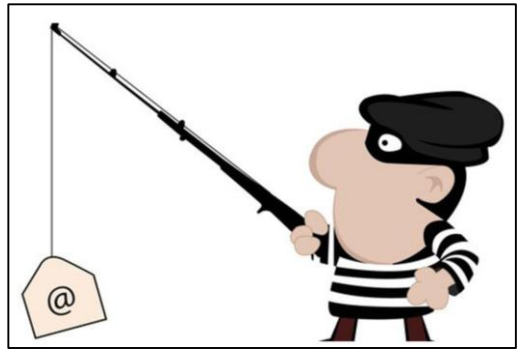
Later that month, Lecron indicated that she wanted to meet other anarchists to form a team, claiming she was willing to sabotage anything that harms the environment. In September, she met with an undercover FBI agents and stated that she and an associated started to make a pipe bomb.

- **On Tuesday, December 4, Lecron had discussions with an undercover agent regarding a pipeline bombing.**
- **Shortly thereafter, she met with a source at a retail sporting goods store, where she purchased two pounds of Hodgson Triple Seven Muzzleloading Propellant.**
- **She then went to a larger retailer, where she purchased 665 screws of various sizes, some as large as three inches.**

Lecron was arrested on Monday, December 10. The search of her residence revealed multiple weapons, including an AK-47 semi-automatic rifle, a shotgun, handguns, and end caps that could be used to construct pipe bombs. 15, 16

Worldwide: Threat Actors Use of SSL Certificates for Encrypted, Validated Websites

An article published by **SC Magazine** on **Thursday, December 13**, 2018, states that **researchers "discovered over 1,150 new HTTPS phishing sites over the course of one day, not including the plethora of the malicious HTTP phishing URLs that we already know exist meaning a new secure phishing site goes up every two minutes."**



The transition/migration of legitimate businesses to recent iterations of SSL/TLS for HTTPS is well-established, as **securing internet facing enterprise web applications and implementing effective cryptographic protocols and primitives mitigate well-known vulnerabilities inclusive of man-in-middle and replay attacks**.

Less-funded enterprises often elect to **implement SSL and enforce the HTTPS port 443**, which **necessitates trusted layer security (TLS) protocol use**, then **set web servers to HTTPS protocol** as well as pieces of the cipher suite – essentially **"forcing it" to use certain ciphers**. While completely legitimate means to effect HTTPS, **among other security guarantees**, unsurprisingly these are **actively leveraged by threat actors in order to enable continued illegal activity with reduced likelihood of detection**.

The lack of an entry barrier for obtaining SSL/TLS certificates continues to result in almost all threat actors obtaining certificates through inexpensive services. Experts early on assessed that these legitimate purchases by threat actors are to be expected – aside from previous norms where threat actors were known to install a malicious root certificate into the system or browser trust store or manipulate or compromise a certificate authority.

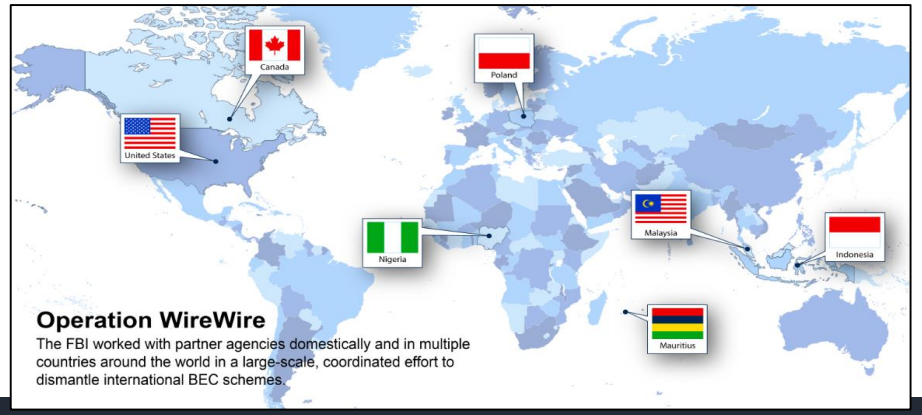
The SC Magazine article indicates **threat actors are** avoiding Extended Validation certificates and are instead **electing for domain control validation, "in which only the control of the subject is verified, to hide their identity."** 17, 18, 19

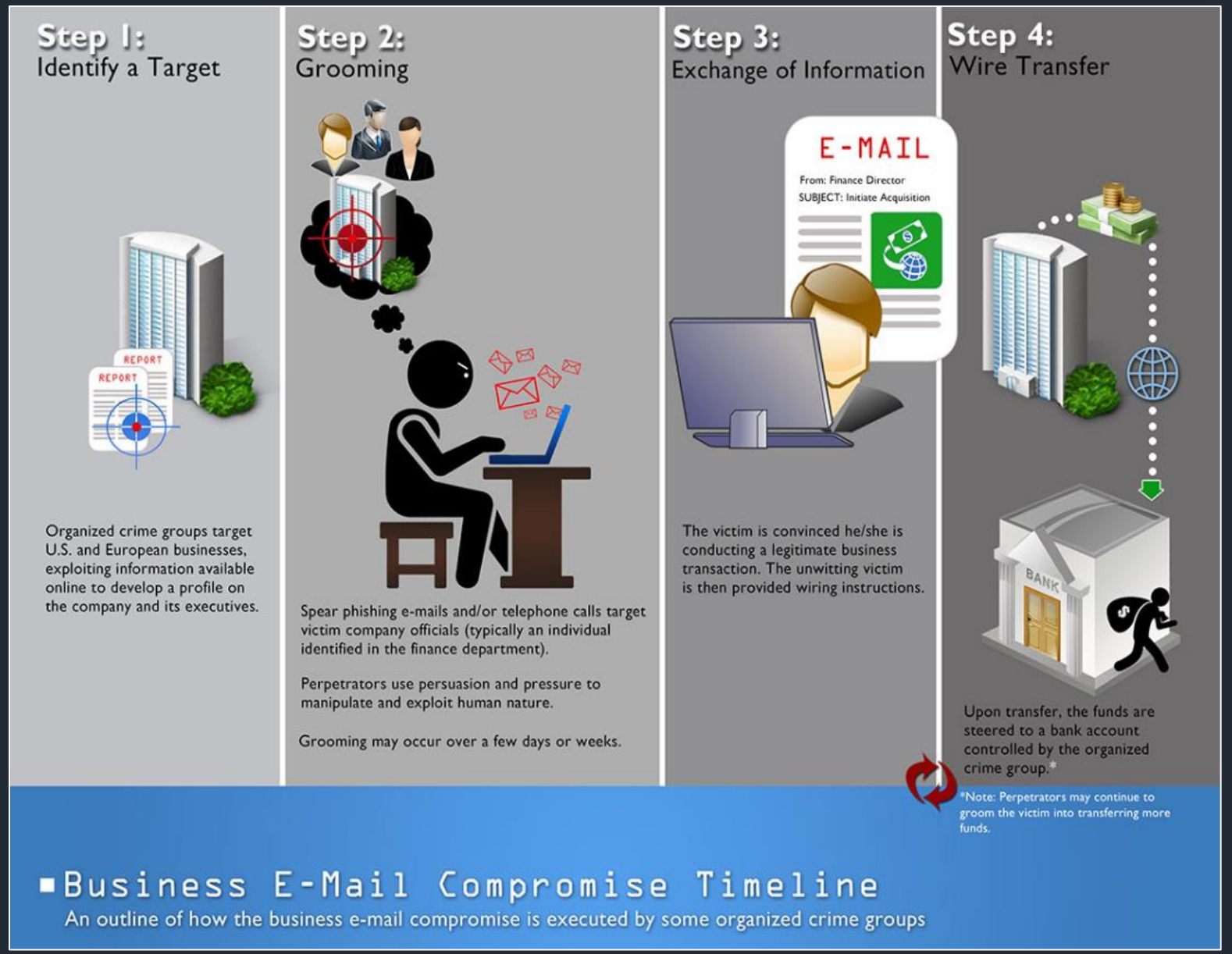
Organizations remain cognizant of the measures required to mitigate the website vulnerabilities, which include enforcing/entrusting IP restrictions, establishing rules to block activities from certain malicious internet protocol (IP) addresses, and establishing trusted relationships between select domains. Information technology professionals have indicated they are often more concerned with users unknowingly migrating to phishing sites and, as such, are even more dedicated to preventing lateral movement once an endpoint or system is infected. More disconcerting is the reality that threat actors are well-versed in cryptographic methods and measures established to protect both the information technology and operational technology spheres, as exploits undermine security guarantees for operational resiliency. Security experts point to the emerging fields tying Artificial Intelligence with endpoint detection/protection capabilities, leveraging data points indicating malicious activities from behavioral heuristics, as one of the future means to mitigate risks.

Worldwide: Save the Children - Loss of $1 Million to Business Email Compromise

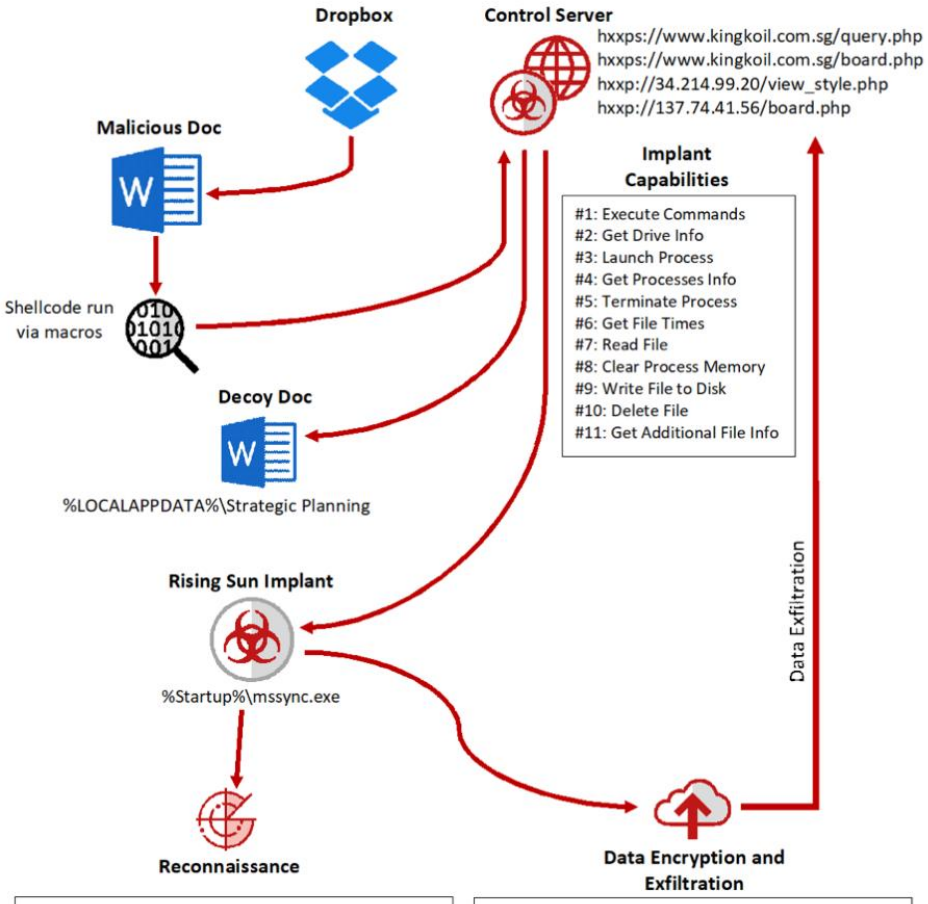
As of **Friday, December 14**, 2018, a **Bleeping Computer** article on indicates that a **Business Email Compromise (BEC), which occurred in May 2017 but was announced only recently, resulted in almost $1 million of funds being misdirected from Save the Children to an unidentified recipient in Japan**. The charity identified the theft when the money wire had been precluded by the cyber breach, **illustrating the importance of cross-checking the validity of requests and adhering to corporate security protocols prior to approving wire transfers.**

The Federal Bureau of Investigation (FBI) cites **Operation WireWire** as **an example of BEC at an international scale**, culminating in a total of 149 arrests and resulting in "the seizure of nearly $2.4 million and the disruption and recovery of approximately $14 million in fraudulent wire transfers." 20, 21, 22





Worldwide: McAfee Report – Rising Sun Variant in 'Operation Sharpshooter'



On **Wednesday, December 12**, 2018, cyber security firm McAfee published a report indicating **organizations in the transportation sector**, as well as **nuclear, defense, energy and financial companies**, were **targeted by the Rising Sun implant variant with 14 backdoor capabilities in 'Operation Sharpshooter'** – a "campaign…masquerading as legitimate industry job recruitment activity [to] gather information to monitor for potential exploitation."

The **backdoor commands reportedly "allow executing commands using Windows Command Prompt, getting details about drives, files, and running processes, or writing and deleting files, as well as change file attributes, clear process memory, read files, terminate processes, and launch processes from Windows library."**

The operation reportedly **exhibits close similarities to a former Lazarus operation** (North Korean Advance Persistent Threat or APT) **in 2017 that targeted the defense and and energy sectors in the United States**. However, these indicators **may be misleading due to the potential for false decoys**. [23], [24]

Indicators of Compromise

MITRE ATT&CK™ techniques

- Account discovery
- File and directory discovery
- Process discovery
- System network configuration discovery
- System information discovery
- System network connections discovery
- System time discovery
- Automated exfiltration
- Data encrypted
- Exfiltration over command and control channel
- Commonly used port
- Process injection

Hashes

- 8106a30bd35526bded384627d8eebce15da35d17
- 66776c50bcc79bbcecdbe99960e6ee39c8a31181
- 668b0df94c6d12ae86711ce24ce79dbe0ee2d463
- 9b0f22e129c73ce4c21be4122182f6dcbc351c95
- 31e79093d452426247a56ca0eff860b0ecc86009

Control servers

- 34.214.99.20/view_style.php
- 137.74.41.56/board.php
- kingkoil.com.sg/board.php

Document URLs

- hxxp://208.117.44.112/document/Strategic Planning Manager.doc
- hxxp://208.117.44.112/document/Business Intelligence Administrator.doc
- hxxp://www.dropbox.com/s/2shp23ogs113hnd/Customer Service Representative.doc?dl=1

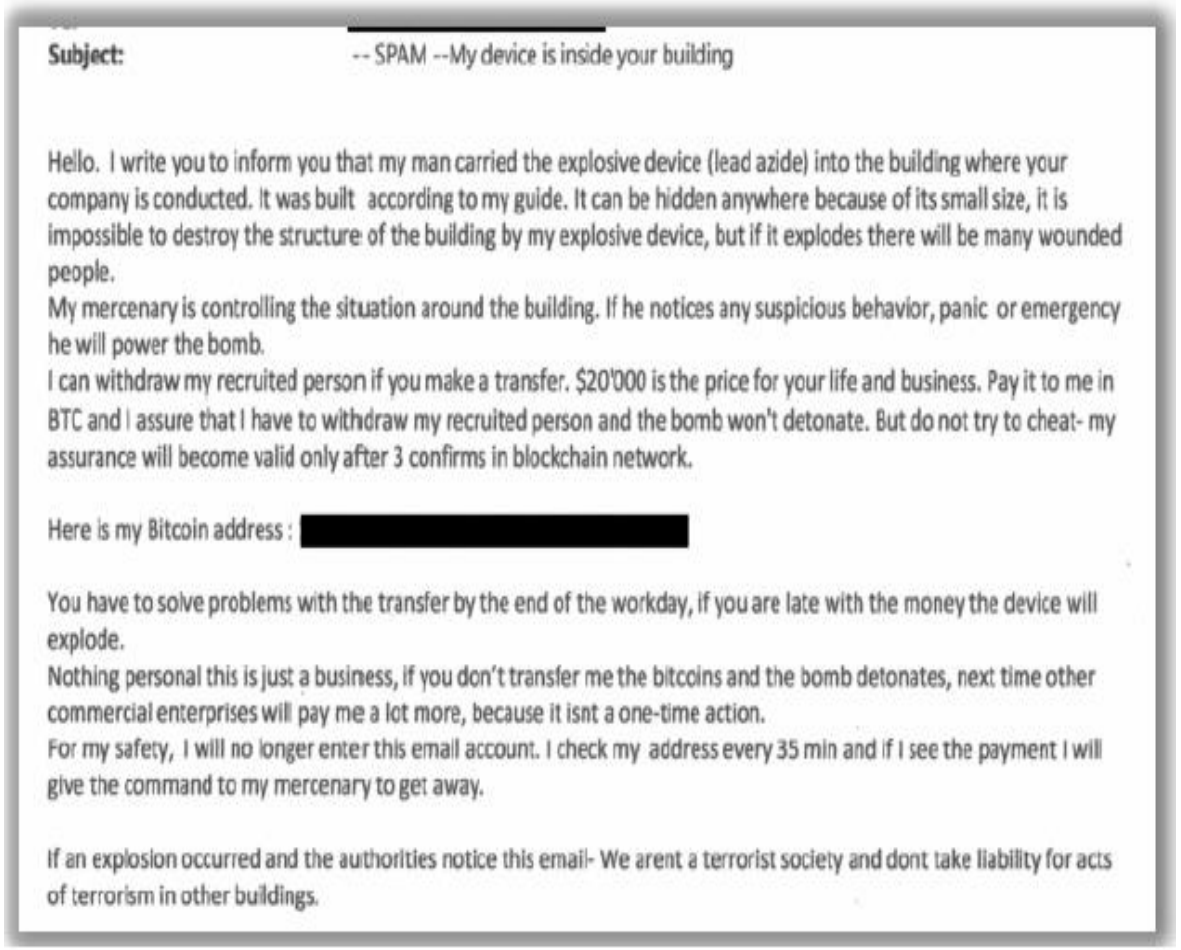
McAfee detection

- RDN/Generic Downloader.x
- Rising-Sun
- Rising-Sun-DOC

Canada / United States: Hoax Bomb Threats Attempting to Perpetrate Cyber Fraud

On **Thursday, December 13**, 2018, numerous law enforcement jurisdictions across the United States and Canada have reported **hoax bomb threats sent by email** in an **apparent large-scale attempt to perpetrate cyber fraud**.

- The emailed threats targeted **private sector business organizations, schools, government departments and agencies, and individual residences**.
- **Fusion centers and other authorities** in Alabama, Alaska, Arizona, California, Florida, Illinois, Iowa, Massachusetts, Michigan, Nebraska, New Jersey, New York, Ohio, Tennessee, Texas, and Washington, DC, confirmed receipt of emails with the hoax bomb threats and demands for payment in bitcoin.
- News media reporting in **Canada indicated five confirmed bomb threats** were made by email in the **Montreal, Quebec, area**, also demanding payment in bitcoin to prevent a purported detonation. Police reportedly investigated other **similar threats in Toronto, Ottawa, Winnipeg, and Calgary**.
- All of the threats were hoaxes intended to extort funds from the recipients.



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.

Multiple employees at Alaska Railroad were targeted by these emails on Thursday morning. **Eight versions** of the message were received. Consistent with those received in the broader hoax threat campaign, each threatened a bomb would **explode at the recipient's location unless $20,000 in bitcoin was paid**.

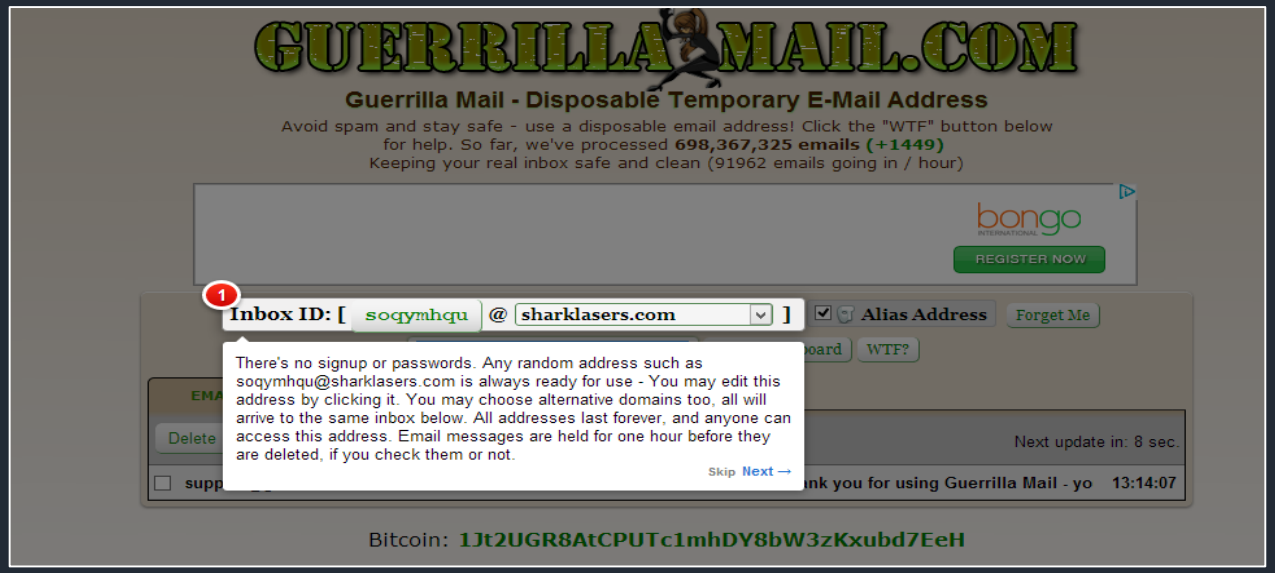
- Information technology (IT) system engineers for Alaska Railroad analyzed the email traffic and identified the **internet protocol (IP) address** from which the message had been directed **– 194.58.61.7**. Research reported by the Alaska Railroad IT engineers indicated this IP address is **based in Russia**.
- **Alaska Railroad operations did not sustain any adverse impacts from this activity**.

In a security advisory, the **Royal Canadian Mounted Police** provided **technical details on the emails messages used to make the threats**, including **user names and email addresses used by "Senders"** and the **identifiers for the bitcoin accounts**, or "wallets," to **which the demanded payment is to be sent**.

Canada / United States: Hoax Bomb Threats Attempting to Perpetrate Cyber Fraud

An assessment issued by the **Joint Regional Intelligence Center** for the **greater Los Angeles metropolitan area** highlighted the following points:

- The **emailed hoax threats falsely claim that an explosive device has been placed at a site at or near the recipient's location**.
- The **recipient is instructed to transfer funds in bitcoin to a specified address**.
- The threats use a "**Guerilla Mail**" **anonymizer** and appear to be **delivered from a variety of email addresses**.
- The **Federal Bureau of Investigation (FBI)** advised, "We are **aware of the recent bomb threats made in cities around the country**, and we **remain in touch with our law enforcement partners to provide assistance**." The statement further encouraged sustained vigilance and prompt reporting of suspicious activity that may pose a threat to public safety.



Recommended Security Measures:

- **Apprise computer network users of the hoax bomb threats being sent by email and request reporting of receipt of any such messages.**
- **Review computer network log activity for traffic from IP address 194.58.61.7; and establish a block to traffic from IP address 194.58.61.7.**
- **Reinforce with employees sound practices to follow when receiving a threat by telephone or email. An advisory issued by the Boston Regional Intelligence Center provides the following relevant guidelines:**
- **For a threat received via telephone/VOIP/Skype:**
  - ✓ **Record the call, if possible.**
  - ✓ **Identify the number calling.**
  - ✓ **Write down the date, time, and duration of the call.**
  - ✓ **Take notes on any details concerning the threat.**
  - ✓ **From the nature and tone of the voice, try to determine whether the threat is made live by a caller or conveyed using a pre-recorded message. Lack of any response, reaction, or pause to attempts by the recipient of the call to determine who the caller is or seek more details on the threat indicates a pre-recorded message.**
- **For an emailed threat:**
  - ✓ **Save the email message – do NOT delete it.**
  - ✓ **Print, photograph, or copy the email.**
  - ✓ **Obtain the full email header data from the original message.**
  - ✓ **Obtain the IP address for the email by analysis of computer network log activity for the affected organization.**
  - ✓ **Research the identified IP addresses to try to determine the source telecommunications provider and its location.**


POLICE