ACME FINANCIAL SERVICES

Powered by GLESEC

CYBERSECURITY NEWS CUSTOM REPORT

Generated on 02/20/2020 by Sergio Heker

How Trafigura Put Its Cybersecurity To The Test

02/14/2020 13:51 Jennifer L. SchenkerFollowFeb 14 · 7 min read

The global commodities trading firm replicated the NotPetya worm, strengthened it and then unleashed it on its production environment to assess its ability to fight back

Mark Swift was sitting in his third floor office at global commodities trading firm Trafigura in the Mayfair district of London's West End when he first starting hearing reports about NotPetya, a computer worm attack. The worm rapidly spread around the world in June, 2017, crippling multinational companies including global shipping company Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser, among others, causing an estimated $10 billion + in damages.

“It was clear there was a major problem; we got a very early understanding that something was going on that was much more significant than the usual ransomware but no one had a clear picture of what was happening,” says Swift, Trafigura’s Chief Information Security Officer. “There was a huge amount of confusion and quite a bit of angst. It was incredible that so many companies were being hit at the same time and extremely worrying because you can’t defend against what you don’t understand.”

Swift’s job it is to ensure the company can effectively play defense against cyberattacks. Trafigura manages more than $54 billion in assets and moves over $170 billion per annum of commodities around the world by ship, barge, truck, rail and pipeline.

While Swift believed the company was reasonably safe he could not quantify the risk. “The questions I kept asking myself is how does the worm get in, how does it move and would our defenses hold out?” he says. “The difficult thing is you don’t have a way to test. Working on assumptions is not a good way to be measuring your defenses.”

There was only one way to be sure: do the unthinkable.

With the help of NCC Group, a global firm specializing in cybersecurity and risk mitigation, Swift hatched a plan to replicate the Notpetya worm, strengthen it, and then unleash it on the company’s production environment, with the full support of the CEO and the board. The audacious move was deemed to be an acceptable risk because Trafigura had standardized the way it exercises cyber hygiene, something the World Economic Forum’s Centre For Cybersecurity has been encouraging companies to do.

Swift, a member of a World Economic Forum committee to improve resilience for the oil and gas industry, agreed to an interview with The Innovator in the hopes that Trafigura’s experience will help other large enterprises better prepare their cyber defense.

Deconstrucing NotPetya

It was one of Trafigura’s lead engineers that first suggested testing how well the company’s defenses would stand up to the NotPetya worm under controlled circumstances. Swift liked the idea and approached NCC Group. They struck an agreement: If the cybersecurity firm could help develop a replica of the worm Trafigura would test it and- if all went well — NCC could use the case as a reference to sell the service to other big corporate clients.

Oliver Whitehouse, NCC Group’s Global Chief Technology Officer, remembers the first discussion about replicating Notpetya with Swift, whom he has known for 20 years. “We were coming off a busy summer in the U.K. We had two major worms, the last of which was NotPetya. Mark [Swift] was getting questions from his chief executive about whether it would have an impact on Trafigura. Mark could just say ‘we think our controls would limit the impact’ but it was very much a theory and he could offer no definitive assurance. When he outlined that he would like to run this test to quantify the risk I told him ‘we can do that.’ I had the confidence that we could replicate NotPetya by deconstructing it and then reconstructing it,” says Whitehouse.

Swift’s team and NCC Group started the work in November of 2017. “We decided to rewrite the worm so we knew exactly what every line of code did,” says Swift. “We discovered a coding mistake in the way it moved and stole tokens and the way it scanned. It wasn’t as efficient in moving as it might have been so we corrected those mistakes to make it even stronger.” The team also installed kill switches to ensure the worm didn’t proliferate outside of Trafigura’s network and accidentally infect suppliers and partners.

The process was supposed to take three months but took a year.

“The complex bit was having the confidence that the controls would work and that it would not go awry and be disruptive,” says Whitehouse. “ We worked on the principle that if there was any doubt the first instruction was to shut itself down, ensuring that it would only spread to computer networks directly under Trafigura’s control. There were key systems in the industrial operations technology in areas such as mining and fuel terminals that had to be excluded but all the corporate assets could be included. Then we built in various other safeguards, such as the rate at which it could propagate so it would not overload the system. We did three full environment tests before we even got near the production and were confident that the controls could do what they said they are going to do.”

Getting Sign-Off

Getting the company’s leadership to sign-off was an important part of the process. Trafigura, stores and delivers the commodities it trades, which includes approximately six million barrels of oil a day. In order to buy the assets that it later trades it has established access to credit from 155 banks. It has to manage credit risks, legal risks, IT risks and liquidity risks and all of these risks are integrally linked. “We are a high volume, low margin business,” explains Christophe Salmon, Trafigura’s Chief Financial Officer. “Our business is based on arbitrage, we fight for the last cent per barrel. Any basis point matters in terms of protection of our margins. If the integrity of our system was compromised it would have consequences in being able to conduct our business and in the daily reporting to our financial partners,”, a factor that could impact Trafigura’s access to both credit and its liquidity. “This was why, in discussing with Mark, testing the strength and integrity of our system — and identifying any potential vulnerabilities — was so important,” says Salmon.

Unleashing The Worm

On November 8**,** 2018 the worm was unleashed. Swift, together with Trafigura's lead engineer, Whitehouse and an NCC Group developer huddled around a group of computer screens. "We looked at each other and said 'should we run it?', remembers Swift. "I paused for a moment and wondered 'What on earth am I doing?' before giving the green light. And then we waited for the havoc to begin."

Thirty minutes went by. Nothing happened. Then the worm found its way in through an unpatched computer in Switzerland and exploited that entry to gain privileges. At that point the team thought it would spread like wildfire. But to their surprise it didn't, due to a security configuration Trafigura had made that they had not fully appreciated. So the team launched different scenarios, purposely infecting different 'patient zeros' increasingly notching up the level of exposure. Eventually a misconfiguration in a software development network lit the fuse and the worm started to spread aggressively throughout the development environment, moving from from machine to machine and location to location. "We tracked the various ways the worm jumped between systems and were able to create a good map and a good understanding of its speed and its ferociousness," Whitehouse says.

The value of the test data can't be overstated, he says. Trafigura used it to make adjustments to its network. "This one configuration change by Trafigura significantly disrupts the speed at which worms can propagate even if they can access highly privileged systems," says Whitehouse.

To Swift's great relief unleashing the worm in this controlled manner had no operational impact on the business. None of the company's computer users noticed a thing.

Key Takeaways

NCC Group is eager to run similar tests for other big corporates but so far there have been no other takers. Although a number of big companies have expressed interest in doing so they have had trouble getting internal sign-off. Whitehouse says that often organizations think they have a picture of what their computer networks look like. However, 99% of the time this does not reflect reality. Knowing who is connected is one of the first things a company has to do to ensure its cyber security. The map needs to be accurate "at any point in any week," he says. "When I ask what is on their network, who is responsible for it, what each device does and what business operation it underpins they look at me quizzically and say they don't know. If you don't know then you don't know what your risk is. You have to understand the material risks before you can unleash tests like Trafigura's."

Swift agrees. "One of the reasons why we were more capable of running this was we know where the edge of our network boundary is," he says. "You have to fundamentally understand how many machines you have and where they are to be able to sign off on something like this. We spend a lot of time standardizing our environment because we believe you need to do things to standard and enforce things to standard."

One of thetakeaways from the test was that having hard data and being able to really measure risk is key, says Swift. Trafigura thought that being 99.9% compliant in some areas was good enough. It was not. “So now we understand that and if anybody says we are being overly cautious we can demonstrate why we need to do what we do. We believe it is worthwhile to get better at testing and measuring the effectiveness of security in our internal network, but is only worth doing if you also have an appetite to introduce major controls.”

Swift says he has no illusions. Controls or no controls the attacks will keep coming. The next worm, the next virus, is likely to be more virulent. And no matter how good its cyber defense is Trafigura — like any other company on the planet — will have to continue to be vigilant in the never-ending battle to keep its systems safe.