Report: Concerted Global Cyber Attack Could Disrupt Global Economy

- Feb 21, 2019
- Security Awareness

According to a hypothetical cyber risk scenario prepared by the Cyber Risk Management (CyRiM) project for risk management purposes, a ransomware strain that can disrupt more than 600,000 businesses worldwide within 24 hours would potentially lead to damages in the amount of billions of dollars.

Cyber Risk Management (CyRiM) project is a collaborative partnership including Lloyd’s of London, the Cambridge Centre for Risk studies, the Nanyang Technological University in Singapore and others. The report ‘Bashe Attack: Global infection by contagious malware’ uses a theoretical catastrophic ransomware attack to model the broader impact of such an incident and “explores how a ransomware attack might take place and what the impacts would be on governments, businesses, and the insurance sector.” The “hypothetical scenario [is] developed as a stress test for risk management purposes.”

While fictional, the ‘Bashe’ ransomware campaign uses data and tactics from past global cyber attacks, including WannaCry and NotPetya, as a basis for how hackers could spread malware around the world. The main finding of the report is that a worldwide cyber attack could cost global economic losses of almost $200 billion as organizations across sectors are still unprepared to face the consequences of a malicious global cyber campaign.

The Scenario

In the scenario, ‘Bashe’ is delivered to targets via phishing emails that appear to come from the target’s payroll departments. These emails attempt to trick recipients into opening a PDF attachment that triggers the ransomware.

In this scenario, the malware is so potent that once one employee runs the ransomware on their computer, it’s enough to spread the file-locking malware around the network, with a demand of $700 in cryptocurrency for each machine. Around 30 million devices at organizations around the globe are locked in just 24 hours. The report sets out how the cybercriminal group behind Bashe has learned from the mistakes of previous ransomware campaigns, including the use of a kill switch, in order make the campaign “the most infectious malware of all time” when it comes to the number of targets infected.

Major Findings

Consequences of the attack are catastrophic, with organizations of all sizes in all sectors unable to perform day-to-day operations. The report shows a ransomware attack on this scale would cause substantial economic damage to a wide range of business sectors through reduced productivity and consumption, IT clean-up costs, ransom payments and supply chain disruption.

As a result, some organizations opt to pay ransoms. Among them are healthcare companies, which need to keep life-saving equipment online.

No matter how companies choose to deal with the attack, the Lloyd’s report predicts that such an event would cost a total of $193 billion around the world as a result of cyber incident response, damage control and mitigation, business interruption, lost revenue and reduced productivity. To put that figure into perspective, it’s estimated that WannaCry caused a total of $4 billion in damages.

The scenario estimates that:

- Retail and healthcare would be the most affected ($25 billion each), followed by manufacturing ($24 billion).
- Regionally, the US would be the hardest hit with $89 billion at risk. Europe could lose $76 billion, with Asia losing $19 billion. The rest of the world could lose $9 billion.
- Despite the high costs to business, the report shows the global economy is under-prepared for such an attack, with 86% of the total economic costs uninsured, leaving an insurance gap of $166 billion.

Commenting on the report, Dr Trevor Maynard, Head of Innovation at Lloyd’s, said the following:

This report shows the increasing risk to businesses from cyber attacks as the global economy becomes more interconnected and reliant on technology. Companies must ensure they are better prepared for ransomware attacks, and that includes working with insurers to reduce the risks before they are attacked and ensure they have the right insurance cover in place to respond after the event. The reality for business is it’s not if you get attacked but when.

**Discussion and Critique**

Although some argue that such a catastrophic attack might seem unlikely and practically impossible, the aim of the report is to show that the global economy is still under-prepared for a massive cyber event and that companies need to act to make sure their systems can withstand such a scenario.

Despite the fact that the report “identifies opportunities for insurers to expand their business in insurance classes associated with ransomware attacks,” recent events show that, in some circumstances, insurers have refused to cover the losses generated by ransomware attacks. In the case of Mondelez, for example, according to Bloomberg, the company “claimed $100 million on its insurance policy because it believed the permanent damage to 1,700 of its servers and 24,000 laptops, inflicted by NotPetya. […] In June 2018, Zurich countered that NotPetya fell under an exclusion in the policy covering ‘hostile or warlike action in time of peace or war,’ which meant the insurer didn’t have to make good on the claim.”

Furthermore, seeing that this study was co-produced by insurance and reinsurance organizations and sellers, it is important to note that there is a benefit to be gained from a theoretical report like this that would make businesses want to buy specialized cyber insurance.

Data Breaches and Cyber Attacks as Global Risks

The CyRIM report comes shortly after the World Economic Forum Global Risks Report listed large-scale cyber attacks and data breaches as some of the biggest risks facing the world today. Cyber attacks and data breaches featured heavily in the 2018 report, ranking as the third and fourth most likely types of global risks, only finishing behind extreme weather events and natural disasters. This year, massive data breaches and large-scale cyber attacks are ranked as the fourth and fifth most likely global risks, with failure of climate-change mitigation and adaptation ranked second behind extreme weather. Natural disasters again ranked above cyber attacks and data breaches.

That doesn’t mean the risk of cyber attacks is decreasing. Quite the contrary. The vast majority of respondents expect cyber attacks to be a major problem during 2019. Eighty-two percent of those surveyed believe there’s an increased risk of cyber attacks leading to the theft of money and data, and 80 percent believe there’s an increased risk of cyber attacks leading to the disruption of operations.

Whether this scale of attacks is hypothetical or fictional, the lesson to be learned by all organizations is simple: when it comes to cyber attacks, be prepared for the worst case scenario. With what has happened over the last 10 years, has this changed your behavior? Do you have plans to enhance your visibility, deploy protective controls and continuously monitor your environment? It’s only a matter of time until the next unintentional piece of malware seeks to disrupt your day-to-day business, damage your reputation and cost you millions of dollars.

Fortunately, Tripwire’s solutions can help with visibility, protective controls and continuous monitoring all through data collection techniques that are non-intrusive to organizational processes.