Counting the Cost of Cyber Attacks

Introduction

- The Rescator team specialized in scamming the credentials from credit cards and selling the details for around a 10th of a bitcoin each (approximately $1 in 2012) on sites in the dark web and other black market outlets, such as the Russian ‘octavian’ marketplace.

- A major theft of US credit card information during next year’s holiday spending spree.

The Malware

- Rescator began by buying a malware kit from one of the underground forums to create a RAM scraper, similar to other point-of-sale (PoS) hacking malware known as BlackPOS, but significantly more sophisticated.2 The Rescator software later became known as Kaptoxa, Russian slang for potato.
- in 2013, when a shopper swiped a credit card through the card reader, the information was read from the card’s magnetic stripe, and under Payment Card Industry-Data Security Standard (PCI-DSS) rules, the data was encrypted immediately. This protected it at rest while stored on the local device’s hard drive, and in transit when it was transmitted to the back-end servers for processing. The 2013 point-of-sale systems had a vulnerability: the card details were read into the computer’s temporary memory (RAM) and encrypted while in memory. The malware RAM scraper could detect and copy the credit card details at the microsecond just before the data was encrypted, and send it to a server that Rescator would configure to receive the stolen data.

Using Suppliers with Authorized Access

- During 2012 and throughout 2013, most of the big-name US retailers announced or implemented new installations of malware and data exfiltration detection services – various vendor security systems to prevent unauthorized access to IT systems, to sweep networks for malware, and to monitor traffic on the network to detect suspicious packets that could be data being stolen.

- Instead of directly targeting the retail companies themselves, they started researching their suppliers and counterparties, particularly anyone who might be granted access into the retailers' information technology (IT) systems. In September 2013 they hit the bull's-eye. An employee at Fazio Mechanical Services fell for one of their phishing attacks by opening an attachment on an unsolicited email enabling another piece of spyware, Citadel, a password-stealing Trojan, to infect Fazio's IT network.

Installing the Malware

- November 2013 when most of the company was closed, they used these access codes to log in to the Target IT network and install their RAMscraping malware on a few point-of-sale systems in Target stores.

- Kaptoxa malware was sophisticated enough to be invisible to some of the best anti-malware systems in use at that time. Target was running 40 different commercial anti-malware tools, sweeping its networks and point-of-sale systems, and ooking for any software that matched suspicious signatures. None of the systems identified the Kaptoxa installations as malicious.

Harvesting the Data

- In a period from November 27, to December 15, 2013, the Kaptoxa malware on the point-of-sale systems in Target stores across the United States captured the details of transactions from 40 million debit and credit cards. An additional overlapping customer database that contained names and addresses of 70 million people was also stolen. It was the largest cache of credit card data that had ever been stolen.

Buy Back and Discovery

- The sites where credit card information is offered for sale are routinely monitored by fraud detection officers from the card companies and major banks. It is a poorly-kept secret that the banks themselves buy back some of the card details on offer to take them off the black market and protect their cardholders. Banks may in fact be some of the best customers of credit card hackers.

- December 18. Target's forensic teams and their security consultants identified and removed the malware from the infected point-of-sale systems in a few hours, and began a full internal systems security audit and investigation. The investigation took many weeks to complete.

Target's Cost

- Target’s direct costs from the breach reached over $200 million, and took several years to accrue. In 2015, Target paid out $40 million to banks and credit unions that lost money, paid out to buy back card data, or incurred further loss resulting from the data breach.9 A consumer class action was settled at $10 million to establish a fund for victims of the data breach, with individual customers able to claim up to $10,000 if they could provide satisfactory evidence of their losses and costs incurred. Victims were also allowed to apply for up to two hours of their ‘lost time’, billable at $10 per hour.
- Target came to a $18.5 million collective settlement for the regulatory fines with the state attorney generals in the 47 states where it had stores in 2017, the largest payout being $1.4 million for California, with 7.7 million affected Target customers. An additional component of the regulatory settlement ensured that Target implemented a comprehensive information security rogram, overseen by an independent, qualified third party, and employed a chief information security officer, reporting to the chief executive and board.

Strategic Impacts on Target Corporation

- The damage to the company’s reputation caused a reduction in visits to its stores. Target attempted to offset this with a 10% discount offer immediately after the breach, but customer confidence was not easily restored, and Target continued to struggle for some months.

- $1 billion and $2 billion, more than five times the direct costs and between 1.4% and 2.8% of Target’s annual revenue. Share prices dropped several times in response to various stages of disclosure about the breach, initially alling 11% in the weeks after the breach, recovering around 7% with a comforting financial outlook reporting in the following quarter of 2014.

Fallout

It is no longer acceptable practice to have point-of-sale systems accessible through the same IT network as HVAC controls and other general activities accessed by a broader, less secure community. Hacks like these have accelerated the take-up of chip-and-PIN (EMV) credit card technology in many countries of the world, which cuts card-related theft by up to 70%.

The Direct Payout Costs of a Cyber Attack

1. The response and forensics costs of the IT security team, both internal personnel and typically involving external consultants, that has to diagnose what happened as quickly as possible and render the system safe from further exploitation. New technology, equipment, software, and systems may need to be purchased to remedy vulnerabilities.

2. Compensation for people whose personal data is compromised, including costs of notification, managing their enquiries and providing customer support, providing credit watch services, and payouts for any losses these individuals may suffer.

3. Fines that may be imposed by regulators.

4. Legal costs to defend any litigation that might be brought against the company, including the costs of settling the action or losing the case and paying damages or even punitive awards.

5. Losses from the theft of financial assets – currency, transfers, trading value – which is the motivation behind many attacks.

Operational Disruption causing Loss in Revenue

- Costs are also incurred to the affected company from the disruption to business operations resulting from the attack, particularly lost revenues from commercial activities that are unable to be performed. Operational disruption can last for several hours or days and affect many parts of an organization. Surveys of corporate security executives show that breaches impact more than a third of a company's systems in around 40% of cases and more than half of systems in 15% of cases.
- Companies are part of a network of commerce, and the failure or reduction in performance by one ompany has consequential effects on others. Economists term this the multiplier effect, or 'financial spillover'. Cyber attacks have a clear multiplier effect on the economy as a whole.

- The reduction in annual revenues of any of these large corporations has a consequential effect in reducing their requirement from their suppliers and curtailing their ability to purchase from trading partners.

- For a medium-to-large company losing around 20% of its annual revenue (something that occurs in around 12% of data breach cases), we estimate the economic multiplier to be around 1.6 – i.e. the suppliers and customers collectively lose an additional total of 1.6 times the losses that the company itself loses in a cyber attack.

Cyber Catastrophes

The NotPetya virus release in June 2017 penetrated at least 8,000 computer networks, infecting many hundreds of thousands of individual devices, in organizations across 65 countries. More than 300 public companies declared losses to their quarterly results as a result of their infections from NotPetya, several reporting losses of hundreds of millions of dollars. The direct and consequential business losses to the infected organizations is estimated to have exceeded $10 billion.

The WannaCry ransomware attack in May 2017 was more widespread, but less severe overall. It caused more than 300,000 infections, mainly smaller businesses, but the impact did disrupt the operations of some major organizations, including healthcare providers whose patients were put at risk.

The concept of cyber threat having the ability to scale up to cause systemic losses to thousands of organizations, with potential to cause catastrophic consequences for our society and our economy, is better accepted now, but the recognition of this potential is relatively recent. This led people to assume that cyber threat is predominantly characterized by separate loss events at individual organizations, and is limited in its ability to propagate more broadly.

There are Different Ways in which Cyber Catastrophes can occur following are the points signifying that:-

1. We have developed plausible scenarios that are used as stress tests by organizations in their cyber protection planning.
2. Another potential cyber catastrophe scenario is a contagious ransomware virus that achieves infection rates much higher than anything previously seen, and is both destructive and disruptive to business activities across large numbers of organizations, of all sizes and nationalities.

3. The analysis considers the practical constraints of attack vectors, the capabilities of attackers, how many organizations could potentially be impacted, and what limits there might be to the severity of the consequences. ‘zero day’ exploit operates on a particular software system, so only the companies operating that software system would potentially be affected by that exploit.

Cyber Catastrophe could impact our Infrastructure

- In 2014 and 2015 when we published these analyses, the idea that foreign agents could potentially attack the power supplies in another country appeared far-fetched, until cyber attacks on the Ukraine power grid in December 2015 left 80,000 people without electricity.

- A cyber attack that used known vulnerabilities to damage 50 generators in the most populous Northeastern region of the United States could result in loss of power to 90 million people, with reconnection for most of them taking a day or two, but full restoration taking between two and four weeks.We estimate the total economic impact of such an event at between $243 billion and, under extreme pessimistic assumptions, over a trillion dollars of lost output from the US economy.

- Cyber attacks and technology errors could potentially trigger a future financial crisis. Flash crashes have been seen on trading exchanges as a result of trading algorithm malfunctions, cryptocurrencies have been hacked and destabilized, and major financial trading systems have been cyber attacked and plundered.

- They fear cyber attacks that will cause them losses and so are reluctant to rely on digital bank accounts, transact online, or embrace further innovations that could be to their benefit. Various names have been used for this phenomenon, including ‘tech aversion’, ‘e-luctance’, ‘cyber malaise’, and ‘technophobia.

The Cyber Threat of Triggering War

1. we list some of the 91 national cyber operations teams that are active today. At least 20 of these are potentially antagonistic to Western democracies.
2. these ops teams are spying on industrial secrets, stealing funds for impoverished regimes, exploring weaknesses in military systems, and probing and learning about vulnerabilities in the infrastructures and economies of their potential future enemies.
3. It is still of course against international law for cyber ops teams to carry out attacks that damage assets in another country, but several western democracies, including the United States, UK, Germany, and Australia, have now passed laws giving their own cyber ops teams the authority to carry out cyber offensive activities in foreign jurisdictions.
4. In 2016, NATO decided that a cyber attack on any member country would constitute an attack under the provision of Article 5, the mutual defense uarantee, that would trigger collective response, including options for retaliation with conventional military weapons

5. Nations like North Korea that cannot match the military firepower of the superpowers, now have extensive cyber ops capability. The existence of national cyber ops teams, both as an extension of military capability and as national security protection, makes the possibility of international cyber retaliatory strikes a lot more likely, and these have the potential to rapidly escalate into a conventional military conflict.

6. Wars in the last century alone have caused millions of deaths, the loss of trillions of dollars of economic output, and the biggest disruption to society. In our analysis of possible costs to the global economy from even a contained conflict between two advanced economies, our estimates ranged from $17 trillion to $32 trillion.

Risk Terminology

1. Risk means the likelihood of loss. We quantify risk by assessing the probability of a specified severity of loss within a given time period. For example, the odds of a large US healthcare company experiencing a cyber attack that causes it direct costs of $10 million or more in the next 12 months would 1/100.

2. Its chances of having a more severe event that causes a higher level of cost, say $100 million, are much less likely: around 1 in 700. The more severe the event, the less likely it is. There is a continuous scale from low levels of cost to the most severe, and at each level of loss there is a corresponding range of likelihood, with the low levels being most common and the most severe being least likely.

3. The relationship between loss severity and likelihood, known as the ‘risk profile’, the ‘frequency-severity distribution’, or the ‘loss exceedance probability curve’, is the measurement of risk, and is how risk managers assess and think about risk. This is how the term risk is used within this book. We use the term threat to mean the likelihood of an attempted cyber attack on your organization.

A framework for Risk Management

1. Risk varies over time, and for different environments in which organizations operate. Most organizations experience many attempted cyber attacks, and with good security systems in place, their vulnerability rates are low, so the chances of experiencing a cyber loss in any given period are relatively small.

2. You could experience a future cyber loss as a result of unknown vulnerabilities in your trusted systems, attacker ingenuity using techniques you have not foreseen, failures in your security processes, human error, malicious insiders, alignment of multiple unexpected events, or other unpredictable circumstances.

Risk Tolerance of the organization

1. But most companies want to avoid having a severe loss above a certain threshold, particularly one that will cause reputation damage, lead to missing earnings targets, materially damage the balance sheet, trigger a rating downgrade, or threaten the viability of the organization itself.
2. The point of estimating a cyber risk profile for an organization is to assess the value and effectiveness of measures taken to reduce the risk of an unacceptable loss.
3. Cyber risk profiles vary significantly from one organization to another. The main attributes of an organization, its size and the types of activities it engages in, provide a benchmark for the base level of risk of enterprises of that type. There are many individual characteristics, however, that make a difference to an organization and determine how far above or below it is relative to the average risk rate of its peer group.

Risk of Cyber Catastrophes

- The potential for a severe loss to an individual organization, there is the potential for multiple organizations to be impacted in a single event, which we have termed a cyber catastrophe.

- The events Wanna Cry and Not Petya that cost billions of dollars through to potential scenarios where cyber attacks could cost the economy trillions of dollars and destabilize our way of life.

Cost of Cyber Attack in the Advance Countries

1. This analysis suggests that in the most advanced economies at least 1% of large companies. Very large losses occur much less often than smaller losses, but when they do, they result in destabilization of a business, which can lose revenues over the following months as a result of the event, and with consequences for the company’s suppliers and counterparties.

2. in United States the direct costs of payouts and operational disruption to organizations from cyber attacks is averaging around $20 billion a year. A further $225 billion of lost revenues is suffered by businesses that are impacted so severely that they suffer consequential business loss.In total we estimate that cyber losses cost over $500 billion a year to the US economy, which is around 2.5% of US gross domestic product (GDP).

3. estimate that for organizations across the world, the total direct costs of payouts and operational disruption from cyber attacks each year exceeds $65 billion. In total we estimate that cyber losses cost over $1.5 trillion a year to the global economy, just under 2% of the global world product.