Stage set for cyber war

Recent ransomware attacks suggest that the target has now been changed from individuals to the nation states. It also seems to be an attack on pirated operating systems, writes **SANJIB SINHA**

Forget the past. The future of war suddenly presents itself with great razzmatazz. Two consecutive ransomware attacks — 'WannaCry' and 'GoldenEye' — shook the world with such ferocious force that it was evident — they were intended to attract only attention. The noisy and noticeable activity was not meant for stealing money only but to shout out a certain kind of presence in the cyber sphere. After that with every new computer installation the hardware people are now coming up with a warning — please don't use pirated or back dated Windows operating system. Forget and forgive their naivety. The hacker's target is no longer the singular person.

A new war front has opened up. Nation states have become the target now. Not persons. In the recent past generally the hardware people happily install old Windows operating system without any caveat — of course. What happened to them? Why are they so scared? The recent consecutive ransomware attacks that affected thousands of individuals and organizations worldwide suddenly changed the whole postulated sequences of possible events and our mindset.

First 'WannaCry'and then 'GoldenEye' has changed it permanently. In May, it had been deliberately done by the hackers to extort money by locking personal or organizational computer and networks. With 'WannaCry' virus hackers were successful in their mission. No one had been arrested. As ransom more than one hundred thousand dollar had been deposited by the affected. The money was put into the designated account through Bitcoin — the mysterious digital currency used in dark web. And it's unbelievable — they didn't touch the money. Actually it was not money. It was something else they had wanted to prove!

In June we saw the 'GoldenEye' attack after which Russia's largest oil production company, Rosneft and Denmark-based Maersk, the largest shipping company in the world, had to shut down several of its systems. New Jersey-based Merck, one of the

largest pharmaceutical companies in the world, was also hit by a massive hack. The list had been endless since then!

GoldenEye did just like what the WannaCry ransomware had done. It hit in May and locked up more than 200,000 computers across the globe. And, only forty four days after WannaCry had hit GoldenEye surfaced to stare us down. In May, the origin of the attack had been one Ukrainian company from which it spread through Russia, Western Europe and the US. But if you wanted to dig deep, you'd have found more gruesome reality. All the hell broke loose after the Shadow Brokers hacker group leaked US National Security Agency exploits in April. After that cyber criminals launched a much more dangerous and sophisticated weapon. Until then they had not been given a giant net to head out to sea! Now they have. And the cyber war has unofficially been declared against American cyber-invasion with their leaked weapon.

WannaCry and GoldenEye serve just as prelude. By this time you have heard the term — Ransomware; so you are not going to ask your hardware people why you're not supposed to install backdated or pirated Windows operating system. You've also probably heard the breaking news — how the hackers gained the backdoor to each affected system that were running backdated or pirated Windows. The maker of Windows — Microsoft, has categorically warned about the potential risk of running old versions. They are asking people to avoid the old versions to which they had stopped giving security patches and updates. It was amazing to learn this fact: many giant corporations and government institutions used to run old Windows-based operating system happily without any update or security patches so far.

It sounded like science fiction when we had first come to know about Ransomware. But it was, actually, an old tactic. It changed a little bit in practical sense but in actual sense this professional wrongdoing had been tormenting people for long until it was publicized recently with humongous noise. We've probably forgotten about the Canada's Carlton University affair.

In the middle of last year, a graduate student of Canada's Carlton University emailed CBC news service and let them know a ghastly plan of cyber attack. At that time experts believed it could sweep over the web world, quite disturbingly, and might be a trend setter in the near future. The Carlton University, later, confirmed its IT network was attacked by 'RANSOMWARE' — a type of computer virus that had used encryption to hold essential files hostage. They were told that they could get back 'very important' access to their files in exchange of money.

It sounded like science fiction when we had first learnt about ransomware. But it was, actually, an old tactic

It was conditional. They were supposed to buy their freedom! They had to pay them in bitcoin — a digital currency known only in the 'dark web' and difficult to trace. The attackers wanted 39 bitcoin in total, amounting to almost US$39 thousand holding tons of important research and official papers as hostage. Their message was clear: 'get back your all important files, get back your freedom by paying us a ransom'.

University authority took some drastic steps immediately after they had got the ransom call from the 'cyber kidnappers.' Students and employees were warned that any Windows-based system accessible from the main network might have been compromised. Students were told to refrain from using Windows system and shut down their computers expecting more damages. It took one more day to get back to normalcy — but that was partial. Only email service had been restored after one day.

In June of 2016, when University of Calgary was first attacked by a same type of assault, people didn't take notice. The University paid 20 thousand dollar to regain access to their computers. Within a few months same incident of Ransomware attack happened and it indicated that the trend might soon turn into a more sinister bend.

At that time security people guessed after testing the first blood in Education sector cyber kidnappers might now target government and banking system, social media giants, and corporate sectors which needed to handle important data on-line. It might hack from daily transport system to individual locking systems. Even it could make you hostage inside your room, car or even in the public toilet where WI-FI was available.

Now it happened exactly before our eyes. It has been proved by this time that cyber attackers can swoop on any computer network and lock the essential files encrypting them and demand for a ransom that you have to pay in bitcoin — a digital currency that runs in the dark web. Denial of service — an old and classical tactic hackers deployed before to jam one network — has been morphed into a new avatar presently. Your service has been denied this time but in a new, complex and encrypted way. And you are being asked to pay a ransom this time — around three hundred dollar - to get back your access to your essential files.

The real life kidnapping model has just morphed into a new ava-

tar in the virtual world encrypting your essential files, demanding money, holding you as a hostage. Cyber criminals have now adopted the same 'real-life' kidnapping technique to snatch your valuable documents holding you for a hostage to make a deal. In such situations you need to buy your freedom for exchange of a ransom.

Will they strike back again with more ransom demand? This question is pertinent but this time security people don't bother about it. More sinister plot waits in a condition of biological rest as they guess. These attacks are just dormant buds. And that is the real danger. Why?

The payment infrastructure hackers used in this attack was rudimentary. And it was in contrast with their advanced hacking technical knowledge. This fact is worrying. Why it's so? It's because the computer virus was camouflaged to look like the infamous Petya ransomware but it had an extremely poor payment pipeline. There was a single hard-coded BTC wallet and the instructions required only sending an email with a huge amount of complex strings. Expert computer criminals would not have done that definitely. Because they knew from the very beginning that within hours the email address would be disabled by the service provider. And exactly that happened.

Cyber criminals have adopted the 'real-life' kidnapping technique to snatch your valuable info

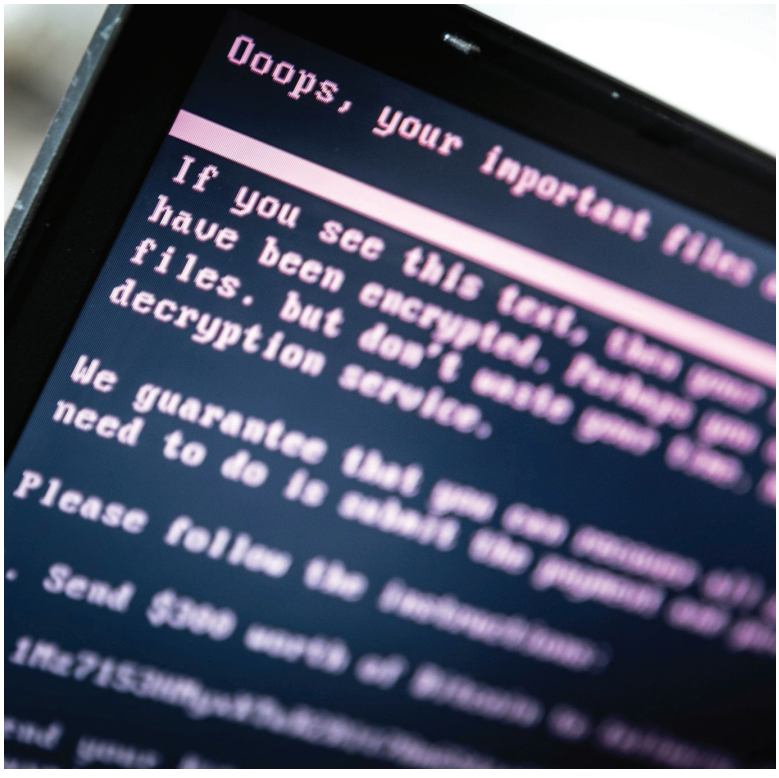
The superficial resemblance to Petya virus was made intentionally. Now it's clear from the design. It was designed to spread panic and cause damage. It appeared to be a ransomware which it was actually not! Under its false appearance something else has been hidden.

What was their actual motive? Was there any unifying idea behind this attack that'd take place in coming future? Cyber security researchers are frantically trying to get the answers quickly. Time is running out fast! They might strike again. Any time! The real trouble begins with the speculation that Russian hackers have developed a new kind of cyber weapon that can disrupt power grids. The tools are not new — it's been around in many forms — but this time its implications are more frightening.

Unfortunately the first test of such a weapon was planned and tested by the United States government. It was tested 10 years ago. On March 4, 2007, the Department of Energy conducted an experiment—called the Aurora Generator Test. They wanted to see whether a hacker could destroy a physical object through strictly cyber means. It was a brainchild of Michael Assante. He had been, at the time, the chief security officer for American Electric Power, which delivered electricity to millions of customers throughout the South, Midwest, and mid-Atlantic.

They wrote a code and that was able to stop the generator's protected system — the code was only twenty one lines. It was an effective malware. It entered through the digital relay system and threw the whole grid out of sync in a minute!

The real question is: are the Russian hackers targeting US power grid? Is this attack just a prelude — serving as a preceding event? The question is easy to be asked rather than to be answered. Cyber attackers always find a new way to play with your digital soul but you cannot just sit back and watch help-



lessly and surrender to their dirty tactics. You can maintain an austere approach and show controlled emotions of not clicking any link or downloading any application. In fact, this is considered as a good gesture to keep your soul out of harm's way. Problem is: it's really very difficult to adhere to this austere practice, always. You can suspect an unknown link but some links, especially those coming from friends, are not always falling under suspicion. Moreover, you have to download new applications to run your system. You have to get the update patches, upgrade your system. Then What?

Well, let's first understand the scenario — the difference between present and past needs of computer technology. When computer technology wave first began to cause ripples people were unsure about how far that flutter could reach. How far it would go was beyond imagination at that time and, above all, the number of enthusiasts was very undersized. It was a closed community who could have been trusted and data were being shared fearlessly. You can't compare that time with today's widespread needs and pervasive hunger for data. The aspect of security has been added as an afterthought.

Today, as we know, the Internet actually consists of millions of networks and they are interconnected without any frontier. Can you imagine building an Internet-border between countries and issue web passports and visas to enter into other nation's network? No. That is unthinkable and also against the idea of Internet itself. The idea of sharing has made any organized or non-organized network accessible from any computer in the world and it's also made it vulnerable to threats from any individual without any physical access to it. Computer Security Institute (CSI) in a recent survey says, seventy percent of the organizations have been polled and they confirm that their network security defenses had been breached in recent past. In most cases, the insiders had made the system vulnerable by clicking outer links or downloading applications. And the percentage was whooping sixty!

Speculation is rife that Russian hackers have developed a new cyber weapon that can disrupt power grids

It appears that every organization should teach their staff about the computer security first because it's really difficult to assess exactly how many computers are connected now and how they become cause for other's security breach.

But common people are not supposed to know about the different infection vectors that hackers had used this time — ETERNALBLUE, Harvested password hashes and psexec. They are not supposed to get wind of Fake Microsoft signature or XOR encrypted shellcode payload that bypass signature checks.

But using this ignorance Petya, the new ransomware attack not only encrypted crucial files of the victim company of Ukraine but it also encrypted the entire hard drive and then forced their computers to restart. At the same time it also deleted the computer's event logs to cover its tracks and hide from analysts to understand its true nature.

The actual fear comes from here. Russian hackers had been trying to penetrate the US power grid since Obama's time. It surfaced recently. At that time Russian hacking operation was dubbed as Grizzly Steppe by the Obama administration. Now Ukraine's Prime Minister officially accuses Russian backed hackers for causing disruption to their power grid. They successfully stopped the power supply for a long time. The engineers had to start and restore the power manually. Quite naturally it raises fears in the U.S. government that Russian government backed hackers are actively trying to penetrate the power grid to carry out potential attacks after their successful Ukraine mission. Cyber war had been there deep inside. Now it came out in the open with the booming launch of two consecutive ransomware attacks!

LETTERS@TEHELKA.COM