By: Justin Healey
April 30, 2022

International Concerns and Solutions to Internet and Network Security

Long before Russian President Vladimir Putin launched malicious cyber-attacks to begin his invasion of Ukraine this year, cyber warfare was already rapidly converting from a mere science fiction fantasia to a real word nightmare. Historically, the Russians have been blamed and tied to countless devastating hacking incidents, and their unprovoked invasion of Ukraine was no exception. In fact, Russian hackers, both military sponsored and rouge bad actors, have been blamed for some of the most destructive cyber incidents in history; moreover, the Russian intelligence agencies and Russian associated hacking groups are internationally notorious as the most active cyber-criminals of the world. Malicious Russian cyber-attacks include BlackEnergy, NotPetya (or "WannaCry") and last year's attack on Colonial Pipeline.[1] The vast increase in international cyber-attacks, by the Russians but also by other unruly nations, has raised world-wide concerns for national security and the security of citizens around the world. In 2015, the Russian military demonstrated their powerful cyber abilities with the BlackEnergy attack against critical Ukrainian infrastructure. In 2017, a hacking group allegedly based in Russia carried out the infamous NotPetya attack that threatened entire economies; then, last year in 2021, a different hacking group (also allegedly based in Russia) executed the largest cyber-attack in United States history on Colonial Pipeline.[1] The alarming increase in frequency and severity of cyber threats has raised questions and concerns about how the billions of every-day internet users can protect their own information online, as well as how governments can protect their economies and national security.

In 2015, the United States and European Union were quick to publicly blame the Russian military for the inimical cyber-attack dubbed "BlackEnergy," an attack in which Russian military hackers succeeded in disrupting Ukraine's electricity grid, thus causing a temporary blackout for roughly 80,000 Ukrainians. This strike was thought to be a show of force – a statement – rather than an act of war; regardless, the incident raised great concern about the Russians' or any threat actor's abilities to carry out such detrimental attacks on critical infrastructure. A year later, the Russians raised the bar even higher when they carried out another nearly identical cyber-attack on Ukraine. The attack, nicknamed "Industroyer," shut down power for about one fifth of the Ukrainian Capital, Kyiv. This internationally public display by the Russians caused concern as far as the United States in the West, as Ukrainian cyber security expert Marina Krotofil described, "Russia could absolutely try to execute an attack like this against the West as an illustration of capabilities and to make a statement."[1] BlackEnergy and Industroyer showed the world how useful, or devastating, cyber warfare could be in the future. However, even though BlackEnergy and Industroyer were impressive demonstrations of power, they are far from the most damaging cyber-attacks the international stage has seen.

The historic 2017 cyber-attack "NotPetya" is known to even non-security professionals as "the WannaCry incident" and has been accurately described as the most devastating international cyber-attack in history. The attack, carried out by a black-hat hacking group who call themselves “Sandworm” and who are suspected to have strong influence from the Kremlin, uploaded ransomware to about 300,000 machines in 150 different countries, starting with Ukraine. The WannaCry worm spread like a plague – once it was downloaded onto a single machine, all machines connected to the compromised network were at risk. This approach backfired slightly on the Russians, as attacks of this nature are very hard to contain, and some machines in Russia were caught in the crossfire. Nonetheless, the incident exemplified the terrifying capabilities of ransomware and malware in the hands of bad actors. Such capabilities became particularly evident when the UK’s National Health Service was forced to cancel hundreds of medical appointments due to an inability to access their systems because of the WannaCry worm. NotPetya caused approximately ten-billion dollars in global damage, and in it’s wake it became evident that most civilians fail to recognize the immense role that internet connections, networks, and inevitably vulnerable machines play in critical infrastructure functions. After four years of hundreds of other cyber-attacks, the 2021 Colonial Pipeline attack extended this list of responsibility to humans just as much as machines.

On May 7th, 2021, the largest oil pipeline in the United States, Colonial Pipeline, was forced to shut down for the first time after remaining fully operational for 57 years.[2] The shutdown was a manual response to a ransomware attack by a black-hat ransomware group, DarkSide, which is thought to be based in Russia. The group gained access to the pipeline’s networks through a compromised password to a virtual private network (VPN) of a former employee. It is unclear how they obtained the username to the account, or why the employee’s account was even still active in the system, but it was later found that this employee used the same password for many different less-secure accounts and that those credentials had been leaked in numerous places on the Dark Web. Once DarkSide had access to Colonial’s networks, they carried out a textbook ransomware attack. According to IBM X-Force, DarkSide uploaded their own version of ransomware that steals and encrypts data using Salsa20 and RSA-1024 protocols and then erases any backups on the network.[3] Colonial ended up paying the 4.4-million-dollar ransom in bitcoin, about half of which was later recovered by the U.S. Department of Justice.[4] It took Colonial, the FBI and the CISA 5 days to re-secure the networks and reopen the pipeline,[3] causing a major crash in the U.S. markets and a never-before-seen increase in fuel and gas prices, the remnants of which are still visible today over a year later. DarkSide allegedly also stole 100 gigabytes of sensitive data and threatened to leak it if Colonial refused to pay the ransom. This incredibly devastating attack raised many concerns about the future of cyber security and how many other critical infrastructure utilities were at risk; however, along with all the negatives, the Pipeline attack also sparked a great deal of realization in the cyber security field and with everyday citizens regarding the necessity of their security online.

Among the countless other attacks carried out by black-hat hackers every day all over the world, the attacks mentioned (BlackEnergy, Industroyer, NotPetya and Colonial Pipeline) all brought with their havoc some new breakthroughs and realizations in the cyber security field. BlackEnergy and Industroyer, for example, revealed the true amount of damage that cyber-weapons could inflict on critical infrastructure. In addition, NotPetya caused tremendous distress and desolation to nearly 300,000 people and businesses; nonetheless, the havoc caused more people to see that cyber security is a real concern for individual citizens of any nation and to all businesses and corporations, especially those that provide critical infrastructure and utilities. This newly found diligence and concern for internet and network security ironically stemmed from one of the worst cyber-attacks in history to date. Moreover, the Colonial Pipeline hopefully opened the eyes of anyone still shelled under the assumption that they will not be targeted. Simply put, average citizens are the easiest targets. With a single password from a seemingly random person, malicious actors were able to shut down the largest oil pipeline in the United States and simultaneously crash one of the largest stock markets in the world. These incidents, along with the hundreds and thousands of cyber-attacks that occur around the world annually, bring a special spotlight to the increasingly popular question: what can be done to prevent this from happening again?

In the wake of all the agony caused by some of the most devastating cyber-attacks in history, people are finally starting to notice the root cause of cyber-attacks: under-redundant security. Hopefully it is becoming obvious to more people that reusing passwords is a horrible idea and often leads to compromised accounts; such accounts, as proven with the Colonial Pipeline hack, can cause devastating damage to even some of the largest economies in the world. The reality is that humans are imperfect, but luckily there are other measures that can be put in place to protect accounts and networks. For example, it is likely that every student, corporate employee, bank user, Spotify listener, and any person who owns a password-protected account has seen a drastic increase in 2-factor authentication (2FA) over the last few years. 2FA can be an inconvenience at times, but it could also be the difference in allowing another Colonial Pipeline incident, or potentially worse. 2FA has proven itself to be the single most effective tool in preventing accounts and networks from being compromised and it is often very easy to implement. Ideally, the most secure 2FA uses an encrypted physical key (typically a USB-drive or card) that must be plugged into the computer or swiped to access the account in question. However, this is not always possible, thus a more common implementation of 2FA is to use a code that is texted to the account holder’s cellphone, sent to their email, or randomly generated by a third-party application to verify their identity. With such measures, even if a threat actor has a username and password, he is unable to access the account. Of course, 2FA has its flaws – if a hacker can gain access to your email, he can gain access to any account tied to that email that uses 2FA, and the same goes for third-party applications and their generated codes – however, especially when combined with other security-enhancing measures, 2 FA can make an immeasurable difference in the level of security of all user accounts and networks.

There are a variety of other security features that can be combined with 2FA to provide optimal network/account security. For example, some universities and companies have begun only allowing their users to access portals and sensitive information on the establishment’s servers from the establishment’s WIFI or through a VPN with the proper credentials. This approach is not as effective as 2FA, since if an attacker is able to obtain the client’s VPN credentials, this method of verification becomes effectively useless; nonetheless, it does provide an extra layer of security and if combined with 2FA would cause a much greater headache to any bad actors trying to compromise the account or network. In addition to software that restricts server access to certain networks, some modern hardware can also aid in preventing cyber-incidents. Such hardware includes biometric scanning devices; for example, retina scanners, face-ID, fingerprint scanners and other like-devices. Methods of security enhancement that rely on hardware rather than credentials (like 2FA via a code sent to email, or a VPN connection that uses login credentials) are in general harder to crack, but it is still possible in some cases. For example, when the new iPhone came out with Face-ID, a team of researchers discovered a way to fool the biometric sensor using a 3-D model that replicated the owner's face. Although it is possible, this solution requires specialized skills and much more work on the attacker's side. Thus, even though it isn't flawless, face-ID provides an exceptionally effective layer of security to the network and/or account in question. Despite its flaws, face-ID is still much more secure than fingerprint scanners, which can in many cases be fooled by a simple strip of tape that mimics the fingerprint of the client. Retina scanners are the most secure, and high-grade scanners can even detect the difference between two identical twins. Retinal scanners are nearly impossible to fool,[5] but no form of biometric security will always be 100% reliable. Therefore, it is always ideal to combine security measures, such as using 2FA, ideally via an encrypted physical key, in conjunction with a biometric sensor such as a retinal scanner, wherever necessary and plausible.

In short, the growing use of cyber weapons and international cyber-attacks has caused great concern for civilians and nations all over the world. Although Russia has seized the international cyber-stage by demonstrating their powerful capabilities, The United States, China, Turkey, and other nations have proven themselves to be right alongside in this ever-expanding field. Regardless, every day new black-hat hackers and military sponsored groups manage to raise the bar and illustrate the alarming amounts of damage they can inflict. As evident in the NotPetya and Colonial Pipeline attacks, both of which shut down major companies and caused immense distress worldwide, all it takes to strike and compromise some of the largest organizations in the world is file of ransomware and a single compromised password. Hopefully more people have learned from such attacks and recognize that their company and nation's futures lie in their hands and are taking the proper measures to secure their accounts and credentials. New technology is constantly emerging to combat the constant flow of new cyber-related threats, but it is as important as ever that civilians, corporations, and governments remain vigilant to prevent another NotPetya or potentially irreversible devastation to their economy.

Sources

1. *BBC News*, "The three Russian cyber-attacks the West most fears." https://www.bbc.com/news/technology-60841924

2. *Bloomberg*, "Hackers Breached Colonial Pipeline Using Compromised Password." https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

3. *ZDNet*, "Colonial Pipeline ransomware attack: Everything you need to know." https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

4. *Thomson Reuters*, “The Justice Department's seizure of ransom paid by Colonial Pipeline to hackers shows that cryptocurrency may not be that untraceable after all.” https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/colonial-pipeline-ransom-funds/

5. Smart Eye Technology, “How accurate are retinal security scans.” https://getsmarteye.com/how-accurate-are-retinal-security-scans/

6. Brookings Institution, “How the NotPetya attack is reshaping cyber insurance.” https://www.brookings.edu/techstream/how-the-notpetya-attack-is-reshaping-cyber-insurance/