- Noble 8 Nation -

A Noble 8 Independence Day Perspective 2018

Celebrating Independence Day in 2018 is one that may very well be Independence from the global e-commerce hackers, crackers and ethically challenged organized crime crawlers thriving in virtual reality and untouched by law enforcement within the now "Global E-Commerce Space."

Statements made by global e-Commerce company talking heads over the last 6 months of Noble 8 Revolution's "Digital Business Platform", made us think about true "Independence" for people and entrepreneurs operating virtually and totally dependent on the Internet. So how about operating securely and safely with "Independence" on the Internet? How about global governments trying to control the Internet? One that is challenged everyday by U.S. and International lawmakers trying to gain control of cyber-crimes, cyber-criminals as well as large and small global hacker organizations that dare to penetrate some of the largest corporation's databases and then boast about it. We are all caught in the middle and it is not only frustrating to all of us, but costing American and International business concerns as well as Governments, billions of U.S. dollars and International currencies respectively every year. In 2002, the losses were estimated at around $2 billion U.S. dollars and in 2011, $150 billion U.S. dollars. But today in 2018, the losses are estimated to be in the $400 billion dollar range…annually! (Source: Inc. Magazine)

These incredible numbers are from an estimated "top 20" worst breaches to have occurred since 2011. What? Since 2011! One would think that there should be a software or hardware solution available to help out the entire e-Commerce industry. Monetary damage hurts yes, however, more than 5 billion user accounts from some of the e-Commerce industry's biggest names have been compromised. The U.S. Feds are attempting to create suffocating laws by regulating the Internet and then groups like "Anonymous and Lul-sec" hack these government's electronic infrastructure and databases to make sure that legislation does not happen. When is this lunacy going to stop?

Please read this very important excerpt from a report available to e-Commerce industry insiders and members of "Proton Mail", an online e-Commerce communication provider:

[Dear ProtonMail Community,

We want to give everyone an update regarding the connectivity issues some of you may have experienced recently. Over the past couple of days ProtonMail has been under extremely heavy DDoS (Distributed-Denial-of-Service) attack.

During these incidents, some users may have experienced intermittent connectivity problems or delays sending/receiving emails. We are working closely with engineers at Radware, our DDoS protection provider, to resolve these issues. At this time, the attacks are still continuing.

Despite the intermittent connection problems, no emails were lost, no data was lost, and no data was breached. In any case, we utilize zero-access encryption which keeps your emails secure even in the event of a breach.

While ProtonMail defends against DDoS and other cyber-attacks on a daily basis, the attacks we faced this week posed a particularly difficult challenge because it is a new type of DDoS from a previous unknown network of compromised devices. To assist in the attack mitigation effort, we have partnered with F5 Networks to help deal with this new threat.

Our infrastructure team and the Radware and F5 Network engineering teams have put in a huge effort while working around the clock to manage this new threat. As a result of their hard work, most of the attacks in the past 24 hours have been well mitigated with minimal user impact.

We understand how important it is for ProtonMail to be not only secure and encrypted, but also always available. It is essential for the millions around the world who depend on us, and essential for our mission of making privacy and security accessible to all.

This mission is challenging. There will be setbacks from time to time, and there are also those who wish us harm. However, we have your support, and a team of experts, which will allow us to overcome these challenges.

We would like to thank you for your continued support and understanding. We will not stop fighting for you, and for your right to privacy and security.

Best Regards,
The ProtonMail Team]

This just happened within the last week. Who was the perpetrator? **Anonymous!**

In an ironic twist to this story, Noble 8 Revolution, LLC, a developer and operator of the most secure and safe "Digital Business Platform" with custom designed, collaboratively created, custom developed and system-wide stress tested software, is publicly thanking all of the aforementioned malicious hacking groups like "Anonymous" by making attempting to make e-Commerce life insecure and dependent upon mega-large corporations like Apple, Microsoft, Google, McAfee, First Data and Symantec. The founders and managers of Noble 8 Revolution has stated many times that they foresee consumers, e-Commerce businesses and yes, global governments, spending millions if not billions of precious global currency on supposed security solution software that gets compromised every day. "No Thank You" is what the leaders of Noble 8 Revolution are saying about operating in the e-Commerce industry space! "Blaine Williams, CEO and co- founder of Noble 8 Revolution, stated in the beginning of Noble 8 Revolution, before development began, that this "Digital Business Platform would revolutionize the marketing industry and that Commercial off the Shelf software was out of the question." Coach Blaine and co-founder Mark Campese, recognized early on that Noble 8 Revolution would not be held hostage by hackers or criminals, intent upon causing havoc within the Noble 8 Revolution e-Commerce business model.

If you are not aware by now, cyber-criminal individuals and groups like Anonymous, otherwise known as "bad actors" have created and successfully launched malicious programs including viruses, worms, malware, spyware, ransomware and even adware specifically to penetrate online companies and their virtual hosted businesses. These "Scum of the Internet" entities are responsible for taking advantage of people who want to securely communicate, operate an online business, socialize, pay bills, bank online, buy or sell goods and services; in addition to researching and learning about their favorite topics or hobbies, all in the safety and security of their own homes or businesses. But what's needed in the e-Commerce industry is a revolution. People learning new things and educating themselves in an effort to create a better life…right now! Well now the Noble 8 Nation Independent Business Leaders, using this fantastic resource called the Noble 8 Revolution "Digital Business Platform" can operate their e-Commerce business, safely, freely and independently and grow as fast as they know how without the worry of "bad actors" getting in their way.

The founders, management and leaders of Noble 8 Revolution are saying "No" to those who use the aforementioned nefarious malware tools to disrupt all e-Commerce businesses. Noble 8 Revolution has meticulously labored for the past 7 months designing, creating and building this "Revolutionary" Digital Business Platform that was developed from 28 years of experience with virtual hardware and software tools in an effort to protect businesses and people operating in the e-Commerce industry.

Noble 8 Revolution, in collaboration with several "global" third party support companies, began in earnest, educating their management groups about a custom developed "Digital Business Platform" complete with virtual tools specifically created for stopping the destruction of data as well as privacy invasion and also corporate intellectual property loss. Through daily calls and updates about the progress of the development of this e-Commerce juggernaut, the majority of the current and future IBL's along with prospective customers slowly began to realize and understand that it takes time to build, develop and test a system like this "Revolutionary" e-Commerce vehicle. All while adhering to legal implications, industry standard policies and procedures as well as changes in the e-Commerce industry due to data loss concerns by companies that Noble 8 Revolution depends upon for its daily operations. The founders of Noble 8 Revolution recognized the problems with securing an e-Commerce platform and clearly stated that "the revolution in the online marketing industry is going to be Noble 8!" Noble 8 Revolution's CTO Robert Morales states that "criminals have taught us to protect and encrypt networking systems of all types. Including their operating languages, desktop hardware, laptops, tablets and yes even mobile phones belonging to users that have probably dealt with online security issues and data loss and also grown tired of dealing with the constant bombardment of malicious software."

Our job as the "Noble 8 Nation of Entrepreneurs" is to work hard at building a successful global online business; safely and securely! With this enthusiasm, motivation and goodwill towards helping people all over the world, the founders of Noble 8 Revolution required a scalable, sustainable, secure and safe "Digital Business Platform" for these intelligent and inspired "Independent Business Leaders" so that they can achieve all of their life's goals, objectives and maybe more importantly their dreams of a better life. The IBL's of Noble 8 Revolution deserve a world class global computing operational networking system that matches the efforts of their entrepreneurial passion. These wonderfully patient, always believing in the best and fundamentally passionate people will be able to grow and become "Independent" in their lives. More importantly those IBL's, by working this revolutionary business consistently, will also affect their family's lives positively as well.

Here is the message and intent of this "Independence Day" communication. As an IBL, you also must remain diligent and vigilant when protecting your computer's vital data information, your mobile device's information and also protect your usernames and passwords like they are your lifeline. Because literally they are! Would you leave the front and back door open to your house at night while you are comfortably resting? Would you leave your house for work, errands or family functions without locking all doors and windows, setting alarms or making sure your video cameras were on and operating correctly? Of course not. Your access to and working with, the Noble 8 Revolution "Digital Business Platform" is your new house. It is ours together along with every other current and future IBL that are operating in a collaborative environment. We must help grow but also to protect one another. One small chink in the armor of the "Digital Business Platform" could cause a glitch in your computing devices as well as slow down the efforts of the Noble 8 Revolution projected growth patterns. For all of the founders, managers, leaders and IBL participants wanting to make this e-Commerce "Revolution" a success; please guard your vital personal and corporate information with your best efforts and capabilities so that all of us together can move forward at lightning fast speeds without any interruptions from careless actions as we all matriculate through the Life Mastery Academy offered by Noble 8 Revolution.

Here is an Independence Day gift from Noble 8 Revolution founders and management. Education is the most powerful gift to give as ultimate knowledge is ultimate power!

Below is a list of the top "8" computer viruses on the Internet since hacking became a global "dark web" business.

1. CryptoLocker: When it comes to malware, ransomware is the new kid on the block. While most people can rattle off names like 'Trojan', 'viruses', and 'spyware', they're often not too familiar with ransomware. Ransomware is a kind of malware that takes your files hostage. Something similar to heist movies when the bad guy grabs someone and threatens them in return for money? Ransomware works much like that, except your computer is taken hostage by a faceless bad guy. Released in September 2013, CryptoLocker spread through email attachments and encrypted the user's files so that they couldn't access them. The hackers then sent a decryption key in return for a sum of money, usually somewhere from a few hundred pounds up to a couple of grand. With some of the hacking attempts, System Restore or recovery software worked. Although with many of the infected computers, if the victims didn't pay up they'd lose all their files. Now is a good time to remind you to always back your files up!

In June 2014, Operation Tovar took down Evgeniy Bogachev, the leader of the gang of hackers behind CryptoLocker. In February, the FBI offered a cool $3 million reward for Bogachev.

Cost of the malware: With 500,000 victims, CryptoLocker made upwards of $30 million in 100 days.

2. ILOVEYOU: While ILOVEYOU sounds like a cheerful bon mot you might find printed on the inside of a Valentine's Day card, it's actually far, far more sinister than that. ILOVEYOU is one of the most well-known and destructive viruses of all time. It's been 15 years since ILOVEYOU was let loose on the internet. By today's standards it's a pretty tame virus, but in 2000 it was the most damaging malware event of all time. Likely, ILOVEYOU inspired many hackers to wield their keyboard as a weapon. But why was it so brutal?

Well, in 2000 malware was a bit of a myth. In fact, it was such a myth that malware could get away with being completely unsubtle. If you got an email today like the one that was sent around in 2000, you'd never open it. (We hope!) The virus came in an email with a subject line that said "I love you". Being curious types, people clicked into the email with aplomb—regardless of the fact the email wasn't from anyone they knew. The malware was a worm that was downloaded by clicking on an attachment called 'LOVE-LETTER-FOR-YOU.TXT.vbs'.

ILOVEYOU overwrote system files and personal files and spread itself over and over and over again. ILOVEYOU hit headlines around the world and still people clicked on the text…maybe to test if it really was as bad as it was supposed to be. Poking the bear with a stick, to use a metaphor. ILOVEYOU was so effective it actually held the Guinness World Record as the most 'virulent' virus of all time. A viral virus, by all accounts. Two young Filipino programmers, Reonel Ramones and Onel de Guzman, were named as the perps but because there were no laws against writing malware, their case was dropped and they went free.

Cost of the malware: $15 billion.

3. MyDoom: MyDoom is considered to be the most damaging virus ever released…and with a name like MyDoom would you expect anything less? MyDoom, like ILOVEYOU, is a record-holder and was the fastest-spreading email-based worm ever. MyDoom was an odd one, as it hit tech companies like SCO, Microsoft, and Google with a Distributed Denial of Service attack. 25% of infected hosts of the .A version of the virus

allegedly hit the SCO website with a boatload of traffic in an attempt to crash its servers. As well as targeting tech companies, MyDoom spammed junk mail through infected computers, with the text that said "andy; I'm just doing my job, nothing personal, sorry". Who was Andy? Who knows? In 2004, roughly somewhere between 16-25% of all emails had been infected by MyDoom.

Cost of the malware: $38 billion.

4. Storm Worm: Storm Worm was a particularly vicious virus that made the rounds in 2006 with a subject line of '230 dead as storm batters Europe'. Intrigued, people would open the email and click on a link to the news story and that's when the problems started. Storm Worm was a Trojan horse that infected computers, sometimes turning them into zombies or bots to continue the spread of the virus and to send a huge amount of spam mail.

Tip: never open a link in an email unless you know exactly what it is.

By July 2007, Storm Worm was picked up in more than 200 million emails.

Cost of the malware: An exact cost is yet to be calculated and maybe never will!

5. Sasser & Netsky: 17-year-old Sven Jaschan created Sasser & Netsky, two worms, in the early noughties. Sasser & Netsky are actually two separate worms, but they're often grouped together because the similarities in the code led experts to believe they were created by the same person. Sasser spread through infected computers by scanning random IP addresses and instructing them to download the virus. Netsky was the more familiar email-based worm. Netsky was actually the more viral virus, and caused a huge amount of problems in 2004.

A German student, Jaschan was arrested when multiple tip-offs were reported to the police. Speculation suggested Jaschan had actually written the viruses to create business for his mother and stepfather's PC business. Because he was under 18 when he wrote the virus, Jaschan spent his prison sentence on probation.

Even more interesting is Jaschan's motivation. MyDoom was spreading rapidly at the time and Jaschan, a newbie coder, wanted to see what would happen if his bug could spread faster than MyDoom. Things quickly escalated from there. Sasser was so effective it actually ground one third of the post offices in Taiwan to a halt, shut down 130 branches of a Finnish bank, and forced rail and transatlantic flights to be cancelled.

Cost of malware: Estimated to be around $31 billion.

6. Anna Kournikova: What's a tennis player got to do with a list of interesting viruses? Quite a lot, as it so happens. We're going to get this out of the way first: the Anna Kournikova virus is pretty tame compared to many on the list. So in the early to mid-nineties, Anna Kournikova was one of the most searched terms on the internet. People were just very into tennis. Jan De Wit, a 20-year-old Dutch man, wrote the virus as 'a joke'. The subject was "Here you have a Smiley Face image" written like this :); with an attached file called AnnaKournikova.jpg.vbs. Anna was pretty harmless and didn't do much actual damage, though De Wit turned himself into police anyway. The mayor of the town came forward and said the city should be proud to have produced such a talented young man and offered him a job as a techie once he was finished his education.

Cost of the malware: $166 Million.

7. Slammer: While most of the malware on this list strictly hit computers, Slammer was created with broader ambitions. Slammer is the kind of virus that makes it into films, as only a few minutes after infecting its first victim, it was doubling itself every few seconds. 15 minutes in and Slammer had infected half of the servers that

essentially ran the internet. The Bank of America's ATM service crashed, 911 services went down, and flights had to be cancelled because of online errors. Slammer, quite aptly, caused a huge panic as it had effectively managed to crash the internet in 15 quick minutes.

Cost of the malware: Estimated to be around $1 billion.

8. Stuxnet: Stuxnet is easily the scariest virus on the list as it was built by government engineers in the US with the intention of obstructing nukes from being built in Iran. Yes, you read that right. Who needs to target email when they can gun for nukes? Stuxnet spread by a USB thumb drive and targeted software controlling a facility in Iran that held uranium. The virus was so effective it caused their centrifuges to self-destruct, setting Iran's nuclear development back and costing a lot of money. Stuxnet is the first real venture into cyberwar and it definitely asks the question as to what will come next. The idea of digital weaponry is pretty scary, isn't it?

Cost of the malware: Unknown?

Source: Norton Anti-Virus Software Company

In Conclusion: Be Totally Aware of Your Vital Data at All Times!

Today we are all experiencing new malware and spyware threats such as Stuxnet which we now know has the ability to destroy an entire buildings' electronic controller equipment. More specifically; in Nuclear development plants as well as critical infrastructure like other types of power plants, water utilities and even power grids. One word: "Scary!" This virus was first seen in 2010 and has yet to be addressed by hardware manufacturers and could possibly be the worst virus in history to date. The source code is easily available for download on the Internet and can be reprogrammed to perform even more harmful tasks. If you're not aware of the U.S. military drone program, you should be. In recent months, the U.S. military has lost several drones due to hackers seizing control of these multi- million dollar war machines and now nowhere to be found.

Noble 8 Revolution's proprietary "Digital Business Platform", if used for e-Commerce purposes only, will have the capability of protecting all of your vital data. Can you imagine an online drone being flown into an unsuspecting neighborhood, like a "Digital Business Platform" originating domestically or from a foreign country and then start firing its powerful malware weapons at IBL's and blaming it on the management of Noble 8 Revolution? Not going to happen!

The Pakistani Brain virus was first introduced in 1996 and has now become part of everyday e-Commerce business. Seemingly legitimate enterprisers use a form of this virus as adware to infect your computer and a pop-up window, looking professional and e-Commerce legitimate, tells you that your computer is infected and they will charge you only $49.95 to clean the infections off of people's computers. Wow, what a deal! Even Apple is mum on their operating software's security because of a recent rash of breaches. Fighting off these malicious malwares is almost impossible unless you're somewhat of a guru like an experienced garage mechanic. The viruses built to extract your hard earned cash and vital data, gives these entities the ability to inform you that you'll have web page access and communication to pay for the "Adware Virus Preventer" and that illegitimate vendor will clean the infection and then on to your bank account!

So there you have it! While viruses and malware might seem like a myth drummed up by tech companies, they are a very real threat that have caused billions of dollars in damage. The Noble 8 Revolution founders, management and group committees declare that we are all now "Independent!" Yes independent business

leaders who are operating within a safe and secure virtual environment complete with enough tools to achieve “Independence” and “Freedom” both virtually and physically!

In closing, without Noble 8 Revolution’s “custom developed software technology,” these malware and nefarious software problems would have existed from the very beginning of a global launch. Noble 8 Revolution founders and management are wishing the entire Noble 8 Nation a Happy Independence Day 2018.

Happy Independence Day!

Blaine Williams, Co-Founder and CEO
Mark Campese, Co-Founder and CMO
Robert Morales, CTO

Visit Noble 8 now at: www.noble8revolution.com