Issue 1 | June | 2018

Terminus Shield

ULTIMATE SECURITY IS WHAT YOU DESERVE

Our goal is to increase the level of awareness of the audience about the latest topics on information security, so with sending your feedback and comments, help us to do it better.

info@terminus-system.com

From the Editor

In today's world which economy is globalized and threats for organizations are changing every day, the corporate partnerships are internationalized, and online business is conducted; information security plays a role more than a business enabler. Despite the continuous emerging of a variety of standards, tools and new technologies, organizations still face a lot of challenges to meet the upcoming security requirements, and management of their risks.

We in Terminus System, believe that the best way to protect organizations from all the threats they are facing to, is to increase their level of awareness about it. So we decided to issue Terminus Shield with applicable information about latest concepts and technologies in the field of information security.

One of the today's hottest topics is Block Chain. It has been said that blockchain will do for transactions what the Internet did for information. What that means is that it allows increased trust and efficiency in the exchange of almost anything. Blockchain can profoundly change how the world works. If you've ever bought a house, you probably had to sign a huge stack of papers from a variety of different stakeholders to make that transaction happen. In "What is BlockChain?" article an understanding of what blockchain is, how it works, and how it can enhance your business and the industry in which it operates, is given.

The rise of ransomware over the past few years is an evergrowing problem that has quickly become an extremely lucrative criminal enterprise. In "Malware from A to Z" article, an explanation about how malware operates and its defining characteristics will be given. Cyber resiliency is important as it gives us "the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse effects." Despite billions of dollars being spent on cybersecurity, information systems data breaches are increasing year after year. To reverse this trend, it is essential to develop metrics and processes to measure (1) threats before they become cyberattacks, (2) recovery of lost functionality after a cyberattack. "Cyber Security Metrics" article, introduces two essential metrics: Elapsed Time to Identify Failure (ETIF) and Elapsed Time to Identify Threat (ETIT). Measuring them and developing processes to lower the values of ETIF and ETIT would improve the resiliency of an information system. The article also discusses challenges associated with measuring ETIF and ETIT and proposes that the measurement and reporting of ETIF and ETIT could be transferred from companies whose systems encounter cyberattacks to companies who are in the Intrusion Detection System space.

What is Ultimate Security?

Today, most of the security measures that have been taken in organizations focus on technical and operational aspects, in which the lack of a formal framework or information security management methodology is clearly evident.

Many organizations have faced a lot of challenges in the implementation of the Information Security Management System, and most of them, however, have implemented the system and have even been successful in obtaining the ISO27001 certification, but they have not reached to the appropriate security level. There are many reasons for this problem, such as the lack of readiness of organizations to accept this system, the inability of most senior executives to understand the intangible concept of information security, the lack of indicators for assessing the level of information security, the lack of centralized monitoring and quality assessment indicators, but if we look a more deeper at it, we find that the root cause of all these challenges is the lack of a comprehensive methodology and a systematic lifecycle in the implementation of the information security management system. Several standards and procedures are in place to preserve information assets from internal and external attacks. Most of the history of literature in this field comes from case studies, validation evidences and recommendations from various industry directors, and there is not much scientific research on the relationship between business goals and information security measures, and the missing link here is a comprehensive methodology that measures it and be related to business goals.

Understanding the main features of a methodology is the key to choosing and prescribing it in different organizational situations. Some organizations compare different types of models and frameworks to their organization to select and apply appropriate information security management methodology using their own specific features and expectations, and present the result as an adaptive table. We have developed a very comprehensive and at the same tine agile for implementation of ISMS according to the organization's business objectives.

SMARTER TRAINING PLANING:

Need based vs. Training companies offers

Information Security Training is like a double sword, if right people take right training they can help to defend against attacks but if wrong people get trained, they would be a threat for organization's security. We've developed a tool for choosing right people for right training. Get Training Designer from www.terminus-system.com/tools

Our comprehensive and agile methodology has four main features:

- Process-based
- Selection-based
- Interest-based
- Cycle-based

(read more in www.terminus-system.com/ultimate-isms-solution-learn/)

What is BlockChain?

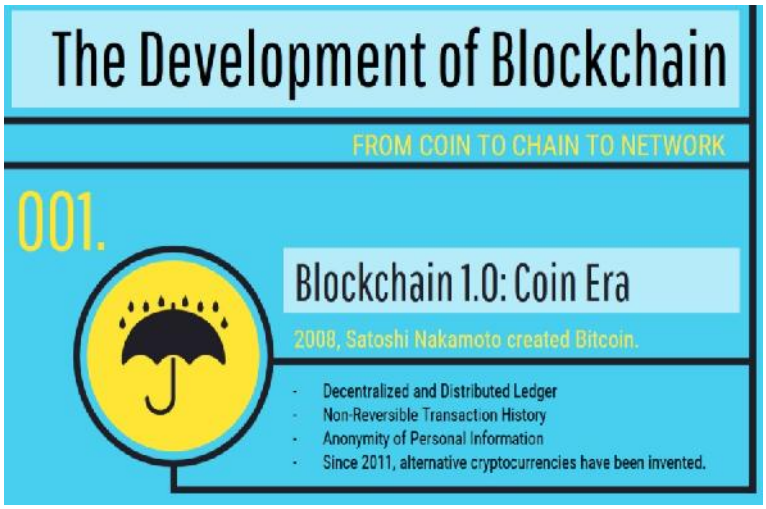
Introduction

Blockchain is one of the most exciting technologies emerging right now. Beyond cryptocurrency, it is redefining how we store, update and move data across networks. It is enabling a new way to write and deploy applications. It has the potential to improve online security and trust. It may even enable the creation of a new type of organization that is without hierarchy and centralized decision making. There is a new technology to store and manage data across the internet and other computing networks, it is called Blockchain or distributed ledger technology. A Blockchain, originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography. It was created as a result of the Bitcoin cryptocurrency.

Today, the application of Blockchain and its potential for exceed its genesis in Bitcoin. It supports not just digital money and trusted data movement and storage, but the exchange of value, an internet of value. At a fundamental level, it is not complex technology, but it can enable complex solutions. It can help solve some difficult computing challenges around security and it introduces capabilities that are disruptive to the status quo. For example, Bitcoin effectively eliminates the need for banks and a whole host of financial middle men that is disruptive.

Taken further, Blockchain technology can be used as a foundation for a new generation of software that distributes code and enables transactions between individuals and machines without the need for complex server infrastructure.

It is a peer-to-peer network architecture meaning that all participants are equal in their role on the network and its topology is flat, in other words, unlike for example a client-server, it is without hierarchy. Just as internet enabled new services such as the World Wide Web, email, and FTP and all benefits those solutions have created, it is increasingly apparent that the Blockchain will enable new computing platforms that ride on top of it too, such as Ethereum, Rootstock, and Tezas. Blockchain forces us to think differently about technology and it presents exciting opportunities in a significant number of use cases and industries. Today, the internet plays a significant role in how we communicate, learn, work, and play, and so much more. It has decimated industries like the newspaper business, reinvented others, like how we manage our money, and created new industries such as social media, but this vast network of networks has some stubborn problems, we face ongoing questions such as, is the person you are doing business with online, really who they say they are? Is a service real? And are only authorized people being granted access to private systems. Healthy ecosystems rely on trust. Innovators have worked hard to solve these challenges, and we have come a long way and yet, we still get hacked, our systems and databases are compromised, money and identities are stolen, and our confidence to further innovates using the internet is stifled and at worst impeded.



The Blockchain, however, solves almost all of these challenges. Let's discuss how it does this. The Blockchain is a new type of database. Instead of one single database residing on a single server in a datacenter, a Blockchain database is installed on individual computers used by the people who used the database. If we want ironclad online voting, workable digital currencies, confidence in machines talking to machines, self-driving cars that securely negotiate with each other, improved methods to authenticate identity, and more, we are going to need a more secure and trustworthy Internet. It is going to need to begin with how we manage data and databases. A core characteristic of a traditional database is that it has essential authority and governs it. For instance, typically any database that is created and owned by an organization has total rights to that database. They can decide who has access and what type of access they can have. They decide what is stored in it, what is deleted and what is archived. However, this has at least two potential flaws to it. First with one master database with one major key holder for each organization need this can result in a single point of failure.

The second major flaw is that all power is held by the central authority. In general this is okay. For example, if you run an e-commerce website, you probably want total control over it. Your own control authority, perhaps you as a CEO, decide all aspects of that environment, including shutting down. What central power can do, however, is exert authority that is subject to bias, such as limiting access for subjective reasons. When databases power important and influential systems in the private and public sector rights to access becomes a complex topic.

In most cases, people remain the final arbiter of the validity of a transaction. We see this in contract work. A contract between two entities completed over the Internet still requires one or more central authorities to validate data. For example, with a mortgage bank must validate savings and approve loans. Title companies must validate properties and legal professionals must validate signatures and other contractual requirements. Each one of these central authorities has unique power that levies considerable overhead in a mortgage transaction. The transactions in the varied databases all take time to process, cost money, are vulnerable to hacking, provide limited participation from those involved, requires special skills and can be error prone. Up until now we have generally been okay with this.

In fact, the identical database is installed in every computer of every user who uses that database. We call it a distributed database because of this. Now in order to create a new entry in this distributed database all participating computers must agree to the change. Consensus must be reached. For example, if we use the metaphor of payment, if a person attempts to make a payment from one user to another and does not have sufficient funds in their account the Blockchain participants will not permit the transaction. In addition there are participants in the network called miners who contribute processing power to the network to solve mathematical problems in exchanging for a reward. That is used to ensure that only valid new transactions may be added to the database.

What makes Blockchain technology compelling is not just that it offers a new way to manage databases and support trust but it creates new opportunity. Let's take a simple example of the challenges of proving ownership of a digital product. While digital products such as photos or music have become simple to acquire, store, and move across devices, the same advantage makes it really easy to copy them and dare I say it, steal them. Artists and media organizations have had to largely accept this fate, resulting in the loss of billions of dollars of lost value. If you are a valid owner it is hard to prove. If we could register our creation and ownership of digital products in a Blockchain database, it is possible we could attain immutable proof. For example, if you are a professional photographer and you register your photographs on a Blockchain, it will be difficult for someone else to claim that they took the picture. Your ownership record will be stored on the Blockchain and it will be nearly impossible to change that fact.

The Blockchain would also enable trustworthy mechanism to support transfer of digital ownership. Blockchain technology is still a work-in-progress. It is open-source and is evolving as we speak. For this reason, it has some significant short-term challenges, including transaction speed, verification, data management, a lot of data is granted and needs to be stored on the Blockchain, and despite a promise of high security, and there are still security and privacy challenges. We will also need to overcome the complexities of integration. If Blockchain is going to co-exist with other technologies, which will be necessary, a lot of innovation is still needed to make that happen. Integration will also require a way for different distributed ledgers to talk to each other. We need a set of standards that is uniform engineering or technical criteria, methods, processing of practices, a prerequisite for any global adoption of new technology. We don't yet have them for the Blockchain, but fortunately work is underway. Bitcoin the digital currency, both the reason Blockchain exists and the biggest current utilizer of it, means that it is financial organizations who are on the front lines of its near-term impact. What might that mean in terms of risk? Let's face it, banks, for example, make huge profits on financial transactions. They are motivated to exert control. There is little incentive for massive disruptive innovation. Financial organizations also have huge investments in their technology infrastructure, so there is less appetite for more investment that could make their systems obsolete. It is not an easy sell to convince the millions of stakeholders in the global financial ecosystem to upend what they do and worst yet, make much less money doing it. *(continued in page 6)*

Malware from A to Z

Introduction

Malware (short for **malicious software**) is any software intentionally designed to cause damage to a computer, server or computer network. It is a malicious software that damages or disables computer systems and gives limited or full control of the systems to malware creator for the purpose of theft or fraud. Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software. The code is described as viruses, worms, Trojan horses, ransomware, adware, spyware, scareware, besides other terms.

Protection against malware involves the prevention of malware software gaining access to the target's computer, and for this purpose antivirus software, firewalls and other strategies can be used to try to protect against the introduction of malware, to check for the presence of malware and malicious activity, and to recover from attacks. These categories are not mutually exclusive, so malware may use multiple techniques. This section describes different types of malware with stress on ransomware.

Viruses

A *virus* is a self-replicating program that produces its own copy by attaching itself to another program, computer boot sector or document. It is usually hidden within another seemingly innocuous program that can produce copies of itself and insert them into other programs or files, and that usually performs a harmful action (such as destroying data).

Worms

A *computer worm* is a malicious program that replicates, executes, and spreads across the network connections independently without human interaction. Most of the worms are created only to replicate and spread across a network, consuming available computing resources; however, some worms carry a payload to damage the host system.

Trojan horses

A *Trojan horse* is a harmful program that misrepresents itself to masquerade as a regular, benign program or utility in order to persuade a victim to install it. A Trojan horse usually carries a hidden destructive function that is activated when the application is started. Trojan horses are generally spread by some form of social engineering.

Rootkits

Once malicious software is installed on a system, it is essential that it stays concealed, to avoid detection. Software packages known as *rootkits* allow this concealment, by modifying the host's operating system so that the malware is hidden from the user. Rootkits can prevent a harmful process from being visible in the system's list of processes, or keep its files from being read.

Backdoors

A *backdoor* is a method of bypassing normal authentication procedures, usually over a connection to a network such as the Internet. Once a system has been compromised, one or more backdoors may be installed in order to allow access in the future, invisibly to the user.

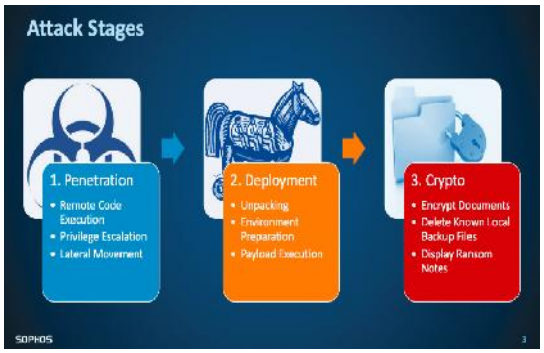
Backdoors may be installed by Trojan horses, worms, implants, or other methods.

Ransomware

Ransomware is malicious software (malware) used in a cyberattack to encrypt the victim's data with an encryption key that is known only to the attacker, thereby rendering the data unusable until a ransom payment (usually cryptocurrency, such as Bitcoin) is made by the victim.

Spyware

Spyware is a program that secretly record what you do on your computer. They can be used for some perfectly legitimate purposes, but the majority of spyware is malicious. Its aim is usually to capture passwords, banking credentials and credit card details - and send them over the internet to fraudsters. It is a software that aims to gather information about a person or organization without their knowledge that may send such information to another entity without the consumer's consent, or that asserts control over a device without the consumer's knowledge.



Trends

Four major trends stood out in 2017 and will likely dominate in 2018:

1. A ransomware surge fueled by RaaS and amplified by the resurgence of worms;
2. An explosion of Android malware on Google Play and elsewhere;
3. Continued efforts to infect Mac computers; and
4. Ongoing Windows threats, fueled by do-it-yourself exploit kits that make it easy to target Microsoft Office vulnerabilities.

Ransomware continues to make organizations suffer, as evidenced by the persistence of Cerber and outbreaks of WannaCry and Petya (also known as NotPetya, since it was a variant of the original but with new behaviors). Looking at the raw numbers, WannaCry bested Cerber as the most prolific ransomware family, remaining active since its initial outbreak in mid-May. But that doesn't make Cerber any less of a threat. If we narrow the scope to which ransomware appeared on the most computers, Cerber remains the most pervasive.

Ransomware as a service (RaaS) – malware kits available to anyone, regardless of skill – is a growing problem, and Cerber is an example of that. Looking at affected industries, hospitals and universities have been particularly hard hit.

While the biggest ransomware attacks affect Windows users using different techniques – for example, WannaCry exploited a vulnerability in the Windows Server Message Block (SMB) service – an ever-increasing volume targets Android as well. A lot of it was found in apps on Google Play, and while Google diligently purges the bad apples, it's all but impossible to keep pace with the bad guys. Android malware intercepted by SophosLabs is designed for many purposes, from sending text messages to stealing data, disabling security software, installing unwanted apps and snooping. For a long time, Cerber has been the most prolific ransomware family, but its power was overshadowed for a few months – beginning in mid-May – when WannaCry stormed the planet on the back of a worm exploiting an old Windows vulnerability. Attackers used NSA code leaked by a group of hackers known as the Shadow Brokers. The NSA attack tool was the EternalBlue exploit, which took advantage of the Microsoft flaw to spread the worm that ultimately dropped WannaCry on computers. From there, WannaCry used strong encryption on such files as documents, images and videos. It also went after servers, trying to encrypt SQL server databases and Microsoft Exchange data files. Though Cerber dropped to second place, accounting for 44% of all ransomware, it remains a potent force to be taken seriously. As noted above, it still remains the most pervasive of all ransomware attempting to infect customer computers, and it's undergone many mutations to circumvent sandboxes and antivirus. It's also an example of ransomware as a service (more on that below). Cerber's creators are particularly nurturing when it comes to this ransomware, constantly updating it and making improvements. This is why it remains so prolific. In March, Microsoft released a patch for a flaw in Windows SMB, which allows computers to share files and printers across local networks. Unfortunately, organizations were slow to install it and left the door wide open for WannaCry, which accounted for more than 45% of all ransomware intercepted from customer computer lookups between April and October. Sophos investigation revealed a three-stage attack, starting with remote code execution and the malware gaining advanced user privileges. From there, the payload was unpacked and executed. Once computers were hijacked, it encrypted documents and displayed ransom notes.

(continued in page 6)

Cyber Security Metrics

Introduction

Preventing cyberattacks is an important objective. Cyberattacks, data breaches, and spending on cybersecurity are increasing year over year. These cyberattacks resulted in the exposure of over 80 million components of personally identifiable information (PII) including social security numbers, driver's license numbers, medical records, etc.

The flexibility, scalability, availability, lower cost, etc., are driving the corporate information infrastructure to migrate to the cloud from local servers and the operational assets information such as financial, human resources, production, logistics, etc., are being stored remotely. The cloud services could introduce new cyberattack vectors due to lack of direct control of cloud service providers on the shared infrastructure and dependency on third party developed capabilities, ease in procuring and accessing cloud services allows nefarious users to hack into data of other users in a multi-tenant cloud architecture, and Man In Cloud Attack. These new attack vectors would not only compromise the information assets but also result in a detrimental impact to the operations of the whole enterprise.

The cyber ecosystem is non-discriminant in the sense that good and harmful information coexists harmoniously. The internet and transmission protocols by which the information travels within the cyber ecosystem is also non-discriminant in the sense that good and harmful information is transmitted across cyberspace without discrimination as to priority or hierarchy. Thus, the opportunity to discriminate between good and harmful information would not occur in the cyber ecosystem. Discrimination must occur within one's own Information Technology/Operational Technology (IT/OT) infrastructure, and must occur in the security infrastructure layers.

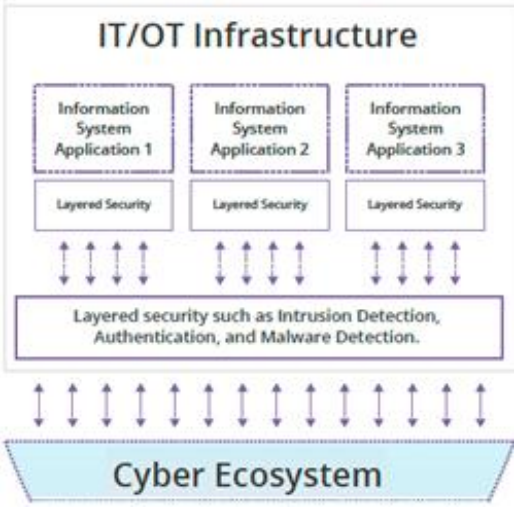


Figure 1

As shown in Figure 1, the first opportunity to discriminate between good and harmful information occurs at the security layers between the cyber ecosystem and IT/OT infrastructure. The second opportunity occurs at the security infrastructure layers part of the information system.

If a cyberattack is identified and captured at the security layers in the IT/OT infrastructure, then the information system is protected. However, if a cyberattack is identified by the security layers residing in the information system (i.e., harmful information already past the IT/OT infrastructure), then the information system is compromised. The loss of function resulting from a cyberattack depends on the kind of function that the attack targets (logistics, tactics, etc.) and on the type of information that is available and exposed (trade secrets, personally identifiable information, etc.). For example, a 2014 cyberattack on Sony Pictures (NYSE:SNE) disabled computers, leaked upcoming movies, and completely paralyzed the operation for a short period of time whereas a cyberattack on the Pentagon's Joint Forces e-mail system resulted in the shutdown of the e-mail system for a short period of time but only locally, without affecting rest of the Pentagon's e-mail systems.

The National Academy of Sciences (NAS) defines resiliency as "the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse effects". Bruneau et al.9 developed a framework to quantitatively assess the resiliency of a community after an earthquake by measuring Quality of Infrastructure, Q(t), over a period of time. The value of Q(t) ranges from 0% to 100% where 0% means no service available and 100% means no degradation in service. At time t0, an earthquake event occurred and dropped Q(t) from 100% to 50% instantaneously. It took time t1 to fully recover, Figure 2. This approach is based on the notion that Quality of Infrastructure, Q(t), of a community is affected after an earthquake and it takes a certain amount of time to fully recover from it.

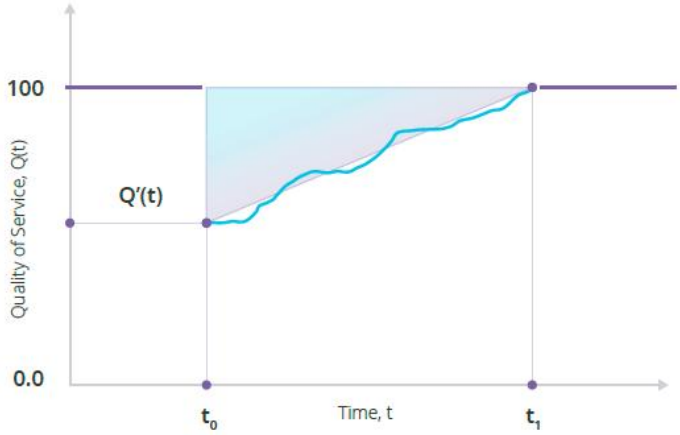


Figure 2

Zobel et al. applied the resiliency of community after an earthquake framework to quantify cyber resiliency after a cyberattack. They analyzed many types of cyberattacks: (1) slow-onset single event, (2) sudden-onset single event (3) slow-onset multi event, (4) sudden-onset multi event. An information system performs many functions; they were all combined into a single function defined as Quality of Service, Q(t). The functional value for Q(t) ranged between 0 and 1; value of zero (0) represents unable to perform the intended function and value of one (1) represents fully performing the intended functions.

This paper expands the cyber resiliency model presented by Zobel et al. 10. It introduces two new variables, namely Elapsed Time to Identify Failure (ETIF) and Elapsed Time to Identify Threat (ETIT) and qualitatively presents a compelling case that the measurement and publication of ETIF and ETIT would spur innovation in the IDS space, and aid in the overall improvement of the resiliency of information systems.

Modified Cyber Resiliency Model

Figure 3a graphically represents the Zobel et al. characterization of a resiliency profile for a slow-onset single-event cyberattack. In this case, the loss of quality of service occurs gradually over time, a virus gradually propagating across the system unnoticed. The start of the cyberattack in the timescale is represented as t0 start, the end of cyberattack is presented as t0 end, and the corresponding of loss of functionality is Q'(t). The time to recover the full functionality from t0 start is T. The triangular area with the base as T and the height as Q'(t) represent the loss of resiliency.

The smaller the area under the resiliency curve the system is more resilient. That is, the cyberattack did not impact the functional performance, or the system recovered quickly and/or a combination of both.

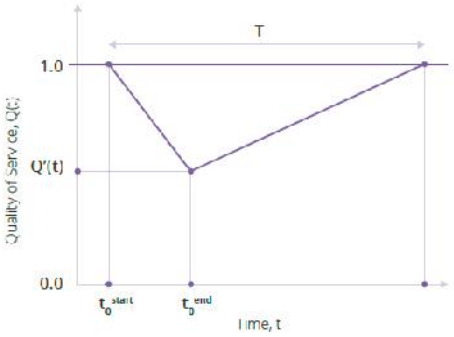


Figure 3a

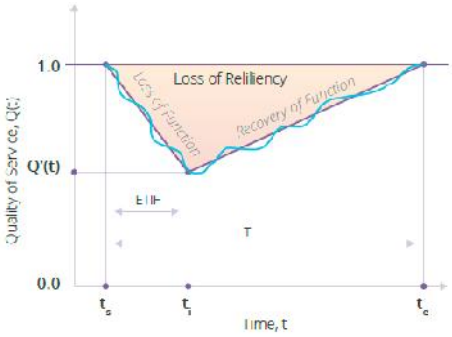


Figure 3b

(to be continued in next issue)

What is BlockChain? (Continue)

Financial firms must also tread carefully around some of the most robust regulations, laws, so even innovating carries risk. However, major risks lies with doing nothing, standing by and hoping that digital currency such as Bitcoin or the Blockchain itself, will pass as novel fad could be fatal. This is why financial organizations are researching the Blockchain & keeping it on their agenda. Some are already exploring active Blockchain projects. For them it seems it is better to participate than to stand idle and face the risk of obsolescence. More likely, over the long-term, financial organizations will evolve and embrace Blockchain innovation. They will find a way to work with it and prosper, rather than avoiding it. Already we see the emergence of interesting new ideas and Blockchain partners, such as Ripple and the Inter ledger Protocol, ready to enhance and improve existing payment systems. In supporting the emergence of a digital currency, Blockchain presented the world with a new way to think about database technology. A way to better secure data that has opened up whole new world of opportunity. We are left with the conclusion that, this is a disruptive technology that is worth knowing and understanding much more about and it is exactly what we want to do.

It has been said that Blockchain will do for transactions what the Internet did for information. What that means is that, it allows increased trust and efficiency in the exchange of almost anything. Blockchain can profoundly change how the world works. If you've ever bought a house, you probably had to sign a huge stack of papers from a variety of different stakeholders to make that transaction happen. If you've ever registered a vehicle, you may understand how painful that process can be. I won't even get started on how challenging it can be to track your medical records. Blockchain, most simply defined as a shared, immutable ledger, has the potential to be the technology that redefines those processes and many others. In this article an understanding of what Blockchain is, how it works, and how it can enhance your business and the industry in which it operates, is given. You learn the fundamentals of Blockchain and how this technology will revolutionize transactions and business networks.

(to be continued in next issue)

Malware from A to Z (Continue)

Attackers used NSA code leaked by a group of hackers known as the Shadow Brokers. The NSA attack tool was the EternalBlue exploit, which took advantage of the Microsoft flaw to spread the worm that ultimately dropped WannaCry on computers. From there, WannaCry used strong encryption on such files as documents, images and videos. It also went after servers, trying to encrypt SQL server databases and Microsoft Exchange data files.

Though Cerber dropped to second place, accounting for 44% of all ransomware, it remains a potent force to be taken seriously. As noted above, it still remains the most pervasive of all ransomware attempting to infect customer computers, and it's undergone many mutations to circumvent sandboxes and antivirus. It's also an example of ransomware as a service (more on that below). Cerber's creators are particularly nurturing when it comes to this ransomware, constantly updating it and making improvements. This is why it remains so prolific.

The third most active ransomware family, Locky, barely accounted for 4% of all ransomware stopped by SophosLabs. But it showed signs of resurgence over the summer. Since the beginning of August Locky returned using four different extensions: .diablo6, .lukitus, .ykcol, .asasin. The new variants displayed the usual Locky behavior, using the same ransom note and Tor payment site. Locky is spreading by spam email and coming with a script file (JS, WSF, VBS) or PDF that is compressed inside of an archive (ZIP, 7-zip, RAR) or an MSWord document containing an embedded malicious macro.

Ransomware is big business on the dark web. Its creators realized they could make more money not just by extorting currency from their victims, but by selling kits buyers could use to make and distribute their own.

We've seen a number of different services and pricing models in the past year, and expect to see many more in 2018. One of the biggest examples, as mentioned above, is Cerber. Other examples include Satan, malicious software that, once opened in a Windows system, encrypts all the files and demands a ransom for the decryption tools, and Philadelphia. The latter was notable for its marketing technique, which included a slick YouTube video advertisement on the open web.

Since ransomware became such a well-paying business, authors are paying more attention to developing features, like robust encryption and antivirus evasion techniques. They've also worked more variety into available payment options. Spora, for example, offered victims several options. They could:

- Decrypt two files for free
- Decrypt a selection of files for $30
- Have the ransomware itself removed for $20.
- Buy what they call immunity for $50.
- Get everything on the computer restored for $120.

(to be continued in next issue)