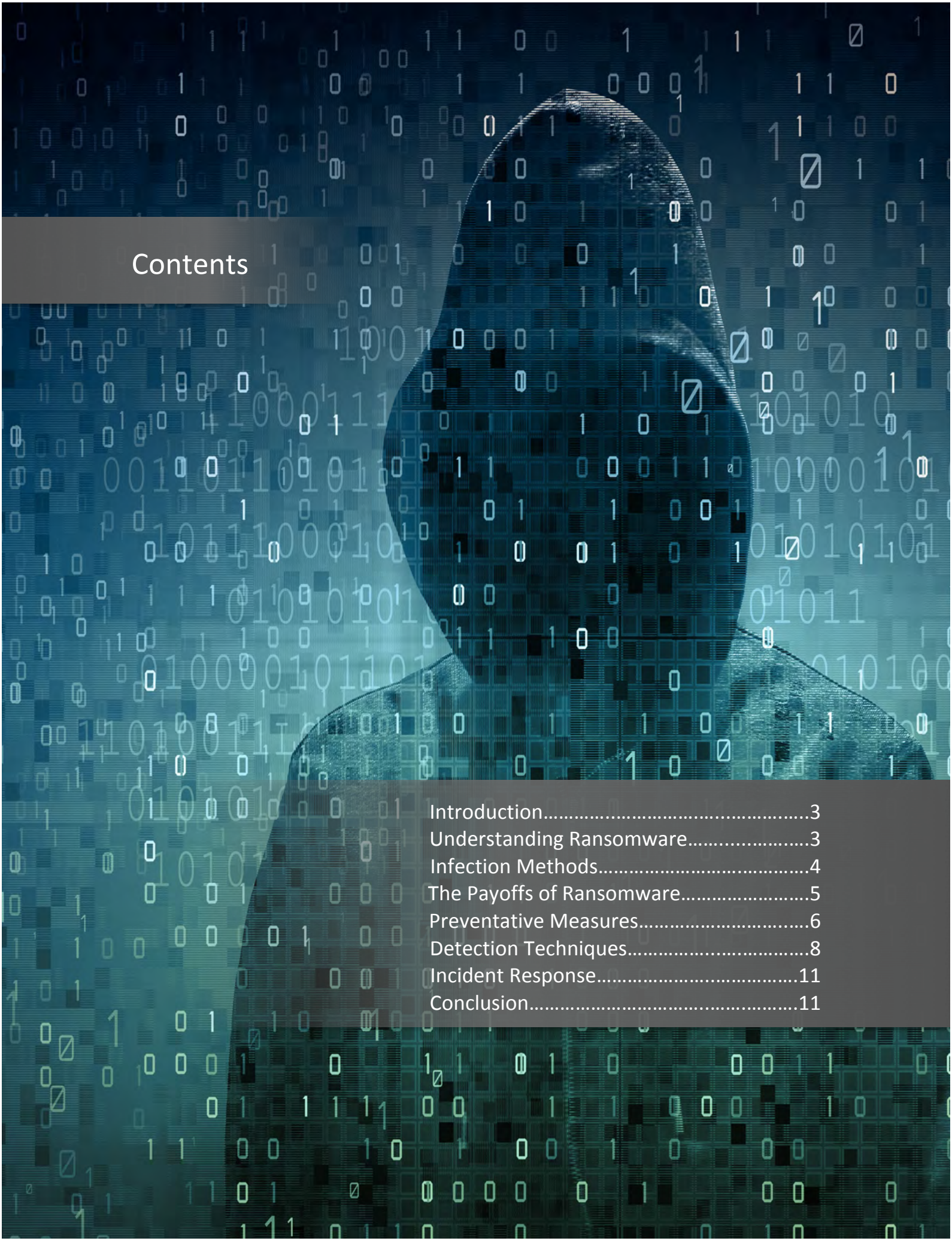
PROFICIO

Ransomware: Detection and Prevention



Contents

Introduction

Ransomware is a form of malware that restricts or prevents users from accessing their own systems, usually by means of encrypting files automatically. It requires users to provide payment through online methods before restoring access to the systems. The first observed instance of ransomware, which locked the screen and demanded payment, was in 2009 and found in Russian-speaking countries. In the past few years, ransomware has posed a very real threat to the world. There is evidence of thousands of infections, ranging from typical home users to enterprise networks. Defense measures are rapidly being developed to detect and prevent ransomware, but it's highly likely that ransomware will continue to evolve and present a danger for years to come.

Understanding Ransomware

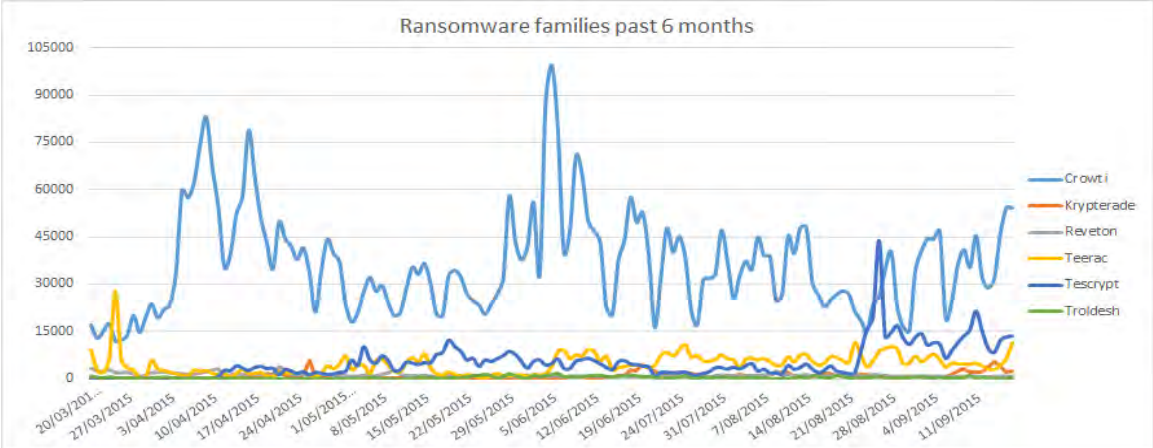
There are two main types of ransomware: locker ransomware and crypto ransomware.

Locker ransomware prevents users from accessing the interface of their computer. It simply modifies the machine to make normal usage impossible. There are a number of ways locker ransomware can accomplish this, but in all of them the user is given some limited ability in order to interact with the ransomware. This allows the user to provide payment for unlocking the machine.

Crypto ransomware prevents users from accessing the files on their computer. It accomplishes this by encrypting the files present on the machine – as well as any network-shared files the machine may have access to – without presenting the encryption key to the user. The ransomware then demands a payment from the user in exchange for the decryption key, which would be used to decrypt the files and allow the user to access them again.

Recently, crypto ransomware has become more popular because it's generally more successful at coercing victims into paying the ransom. Because locker ransomware does not modify the files of the machine, it can potentially be removed and allow for restoration of the machine to a previous uninfected state. Locker ransomware is, however, still successful on devices that may have more limited user interfaces, such as wearable devices. Crypto ransomware, on the other hand, has been effective for many different targets, and is computationally infeasible to remove as it would require breaking established encryption algorithms to do so.

There are six large families of ransomware, largely dominated by the “Crowti” family (otherwise known as CryptoDefense or CryptoWall):



Source: [Microsoft Threat Report]

These families differ in their implementation of crypto schemes, the destinations they communicate with, and the exploitation mechanisms they use to limit user access. But at a high level, they all operate the same way – once a machine is infected, user access is severely limited and a ransom demand is made.

Infection Methods

How might a computer be infected with ransomware? Ransomware is a type of malware and as might be expected, ransomware uses the same delivery mechanisms that other forms of malware do.

Spam email is one of the most common avenues of infection for ransomware. Spam email is sent out through botnets or spamming services. The contents of the mail will typically include either a link to a site with an exploit kit or an infected attachment. Often times, some form of social engineering will be used to try and trick the recipient into opening the infected attachment, following the link(s) provided, or downloading and installing the malware some other way.

Downloaders and botnets are other means of distributing malware. After a machine is infected, a downloader will download more malware onto the already infected machine. A downloader effectively spreads the infection in two phases as a means of bypassing host-based defense measures. The first infection needs only to bypass defenses and download the second instance of malware, which could be a well-known variant that is normally stopped by the defense measures in place. Trojan botnets have been observed to download ransomware on infected machines as well.

Malvertisement, or malicious advertisements, can sometimes be placed on otherwise trusted websites. Once there, they can redirect traffic to a site hosting an exploit kit. This "drive-by-download" method of delivery can be difficult for a user to notice during their normal activity.

The Payoffs of Ransomware

Ransomware has become incredibly popular in the past several years and for good reason – it continues to generate a massive amount of profit. Cryptowall 3.0 is the most successful ransomware of all time, causing an estimated $325 million in damages so far, and millions of dollars in profit for cybercriminals.

The average ransom demand is slightly over $300. The amount of the ransom demand has been noted to change based on a number of factors. Most notably, geography plays a key role in determining the sum of money that is demanded. The goal of ransomware authors is ultimately to be paid by infected users; as such, the amount they demand must be reasonably affordable to their target. If the amount is too large, it is unlikely that any payment would be received, as the loss of files is unlikely to be life threatening.

The type of target can also influence the ransom amount demanded by cybercriminals. In particular home users typically face smaller ransom demands than business users. Home users typically face demands much closer to the $300 average, while businesses can see demands for thousands of dollars. It has been observed that $10,000 is a common price point for ransom demands made to businesses as it is an amount they are sometimes willing to pay, while also being too small of an amount for law enforcement to treat the investigation as a high priority.

Source: Symantec

Ransomware employs many psychologically proven techniques to coerce infected users into paying the ransom demands. Some variants of ransomware will display a fake law enforcement notice to masquerade as a trusted authority, demanding payment from the user. This often includes references to “illegal content” found on the machine – an additional tactic that may persuade the user into quietly paying the ransom without seeking outside help for fear of embarrassment.

Other variants of ransomware typically include a time limit on the ransom. If the user does not pay within this time frame (usually a few days), the ransomware states that the decryption key will be deleted and the files will be lost forever. This promotes a sense of anxiety and urgency in the user.

Screenshot of CTB-Locker ransomware; Souce: "Kafeine"

Preventative Measures

Despite the large number of variants and its seeming ubiquity as a threat, ransomware heavily targets a few threat vectors. Here are steps you can take to harden your network against this type of threat:

1. Create backups of your files

This is essential in protecting yourself against ransomware infections. Properly maintained backups of files allow you to wipe an infected machine completely with little to no data loss. Ransomware operations target users who are not prepared enough to have this option. Note that this backup should be stored separately – some ransomware

variants will delete Windows shadow copies of files in an attempt to remove local backups from the infected machine.

2. Keep your security solutions as up-to-date as possible
Cybersecurity is often described as only being as strong as the weakest link. Typical enterprise environments will employ numerous security solutions including firewalls, antivirus, intrusion prevention systems, webfilters, and more. Ensuring each of these are fully updates goes a long way towards providing protection capabilities offered by the vendors of each of these solutions.

3. Keep your operating system and other software as up-to-date as possible
Updating the operating system and applications on the machine will help provide protection against drive-by download attacks as well as help prevent the exploitation of software vulnerabilities. Both are common avenues for ransomware infection.

4. Exercise caution when following links through email and opening attachments
Most ransomware arrives through email – either spam or phishing – and is installed on a machine once the email links are followed or the attachments are opened. Email antivirus scanners may provide enhanced protection for this however a well-trained user is the best defense against emails from malicious sources.

5. Block binaries running from %APPDATA% and %TEMP% paths
The majority of ransomware utilizes these locations during the infection process. Blocking the execution of binaries in these locations would provide an additional defense measure against ransomware infections.

6. Block Tor traffic
Ransomware often uses Tor to disguise its outbound communication from infected machines. Adding block rules to your next generation firewall can limit this and provide an indicator of compromise, allowing you to remove an infected machine from the network to contain the threat and perform remediation.

7. Review write permissions on network shared files
Ransomware on a single machine could represent a large loss of data if that machine or user has write permissions on files shared across the network. These permissions should be limited wherever possible, as they represent a potential avenue through which a ransomware infection can increase its damage done to the network.

8. Disable RDP
Remote Desktop Protocol (RDP) is a utility that allows others to remotely access your desktop. Many forms of malware access target machines using RDP. Ransomware is no exception to this. If RDP is not required, it can be disabled to protect your machine from

many types of malware and from all RDP exploits. The instructions are different depending on your version of Windows:
Windows XP RDP disable
Windows 7 RDP disable
Windows 8 RDP disable

9. Filter EXEs in email
Consider automatically blocking emails sent with executables as attachments. It is not uncommon for spam emails to have executable attachments as a means of infecting the target machine. If you do still need to email executables, you can continue to do this by compressing them (in password-protected ZIP files), or through the cloud.

10. Show hidden file extensions
As previously mentioned, ransomware will often infect a machine by means of a malicious attachments. Sometimes, the default Windows behavior of hiding known file extensions can make it difficult to notice that type of file is being opened. You can change your Windows settings so that the full file extension is displayed, making suspicious files easier to spot.

Detection Techniques

Detection mechanisms and processes for ransomware are similar to those used for other forms of malware. There are two types of evasion techniques that make detecting common ransomware difficult.

Packing/Crypting
Antivirus is the most common defense mechanism that cybercriminals encounter when attempting to infect a machine. Traditionally, antivirus has been a signature-based solutions that looks for patterns in a file at rest to determine if it is malicious. Recently, many antivirus vendors have begun to supplement their offerings by developing heuristic detection capabilities.

To bypass this, cybercriminals will compress and encrypt the binary of their malware to avoid detection by antivirus solutions. This process is known as “packing” or “crypting”, and the encryption can be repeated several times to generate a binary that performs the same function but avoids detection of current signatures.

Whitepapers dealing with the cybercriminal economy have described attackers repacking the same type of malware multiple times each day. Antivirus vendors create new signatures each day, but often these signatures will simply detect previously known malware that has simply been repacked more times.

Changing Command and Control Indicators
The second most common countermeasure cybercriminals encounter when attempting to infect a machine with ransomware is blocking or blacklisting IP addresses. Several technologies such as firewalls, IDPS, host-based firewalls, and other products will block malicious IP addresses known to be involved in cybercriminal command and control activity. In order to prevent command and control communication, early designs of common ransomware products such as Crytpolocker used domain generation lgorithms to randomize the IP addresses they communicate with each day. Cryptowall leveraged Tor to anonymize the command and control severs being used for the ransomware activity.

New variants of ransomware will likely use similar, or more advanced techniques to prevent being blocked at the IP level through simple IP blacklisting. Knowing the common techniques built in to evade countermeasures such as antivirus and blacklisting command and control activity, we evaluate below some current security solutions and how they can detect ransomware.

Firewall logs:
Firewall logs are great for detecting a variety of threats. With ransomware at the network layer, you want to detect the process of installing the malware or the command and control communication.

ProSOC Threat Intelligence Profiler (TIP) is a database for IP addresses and domains that collects reputation information on blacklisted addresses and domains from publicly available threat intelligence sources. Network traffic is checked against this for suspicious communication with domains or IP addresses that have a poor reputation. Additionally, ProSOC maintains a domain watchlist and an IP address watchlist based on previously detected compromises and employs correlation logic to check for traffic to and from any of these previously detected indicators:

ProSOC Destination Domain Watchlist
Outbound traffic to a destination IP address that has been designated as a network indicator of compromise.

ProSOC Destination IP Watchlist
Outbound traffic to a destination domain that has been indicated as a network indicator of compromise.

Unfortunately, firewalls have difficulty detecting both the process of installing the malware or the command and control communication. It is almost impossible to detect phishing threats through firewall logs, which is one of the most common vectors ransomware will come into an environment. Additionally, cybercriminals change their IP

addresses so frequently, blocking or detecting the IP addresses that may change on a daily basis may not be practical for a number of ransomware variants.

Network IDPS:
Mature network based IDPS products update their signatures that detect activity based on known patterns of command and control activity regardless of the IP address it is communicating with. Although ransomware will encrypt a lot of communication, malware authors usually slip up and some type of pattern is commonly observed in network traffic that will be common with a family of ransomware. ProSOC monitors these types of signatures for many of IDPS products as a primary detection mechanism for command and control. Within your environment, we can have a correlation rule specifically designed to detect signatures based on behavior indicative of this type of infection.

ProSOC employs numerous correlation rules to detect specific signatures associated with ransomware, as well as Trojan and virus events known to have connections to ransomware. We have content around these kinds of alerts for IDPS solutions from Cisco, FireEye, Juniper, Palo Alto, Snort, Symantec, and TippingPoint.

Antivirus:
Although antivirus traditionally can be bypassed by ransomware if the malware is fresh, antivirus definitions do update and the malware may eventually be detected on the system. ProSOC monitors antivirus data sources for anomalies that can recognize larger security incidents that network administrators need to know about.

ProSOC has antivirus correlation use cases to look for ransomware or other indicators of compromise. These include detections of virus outbreaks, in which multiple systems report the same infection and therefore indicate a threat spreading through the network, as well as repeat infections indicative of an incomplete threat remediation on a system. We have content around these kinds of alerts for antivirus solutions from McAfee, Sophos, Microsoft, Symantec, and TrendMicro.

Webfilter:
Webfilters work at the application layer and provide ProSOC a variety of additional information beyond what is available in layer 3 firewall logs. This can include the domain, URL, request method, user agent, and also a reputation of the domain. Many webfilter vendors such as Blue Coat or Websense have strong reputation and heuristic based classification that has a good rate of detecting emerging command and control.

We have seen these products repeatedly detect and prevent command and control of common ransomware variants. ProSOC then leverages this data to put the command and control indicators into watchlists to enable future detections for clients that are firewall only.

Incident Response

You have been infected with ransomware. Now what?

The first step towards remediation is containment. Containment is essential to prevent lateral propagation of malware to additional devices and shared files. Immediately remove any infected machine from the network. Disabling internet access for an infected machine will prevent the infection from spreading – and, if performed early enough for some variants of ransomware, can actually prevent the encryption process from being successful (but this is unlikely).

At this stage, the most common questions is: *should I pay?* Once containment has been completed, if the infected machine(s) files are still unencrypted, the threat can be removed through standard malware removal procedures. In this case the files can be recovered without payment. However, due to the threat posed by ransomware, it is recommended that you wipe the machine anyway.

Otherwise, the files that have been encrypted by the ransomware should be considered destroyed. Providing payment to the cybercriminals does not come with any guarantees. It is unlikely that the decryption key will be provided, and even then, reinfection is more likely to occur. Organizations that provide payment to cybercriminals are considered a success and can become a specific target for future cybercrime operations.

Conclusion

In the above paper, we examined the characteristics of ransomware and what makes it such a powerful threat. Its high profitability and remarkable success virtually guarantee its presence as a threat in the coming years as the security landscape continues to evolve at a rapid pace.

Despite the invention of many different variations and families, the main formula behind ransomware remains the same. And, in parallel, many detection and prevention measures that apply to one of these will apply to all of them.

The greatest defense against ransomware continues to be a functional and regular backup of important files. If nothing else, ransomware has taught us that we must constantly remain vigilant in the face of ever changing threats in the security world.

About Proficio

Proficio is an award-winning cloud-based cyber security company providing 24x7 security monitoring, advanced threat detection, and breach prevention services. We are changing the way organizations meet their IT security and compliance goals by providing the most advanced security solutions without the need for added headcount or costly software and hardware systems. By providing accurate actionable intelligence, we help our customers reduce their mean time to detection, response, and remediation from days or hours to just minutes.