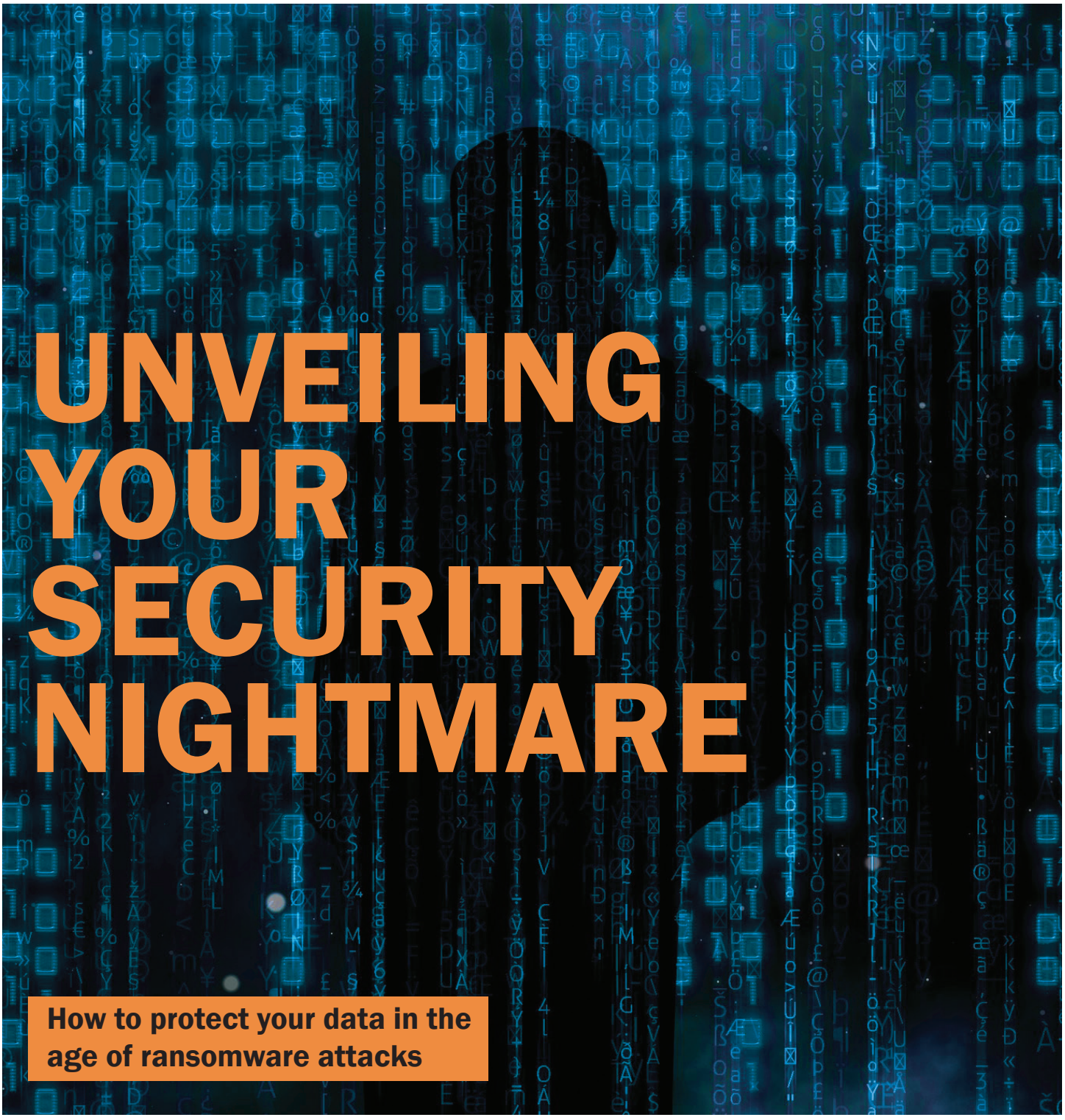
DataServ

p: 1.800.560.7378
e: info@dataservtech.com
w: dataservtech.com
t: @dataservtech

31280 Viking Parkway, Westlake, Ohio 44145

DataServ founded in 1986, is a provider of Information Systems and Technology (IST) solutions. We have provided comprehensive IT solutions to the public and commercial markets for three decades in Ohio and surrounding regions.



UNVEILING YOUR SECURITY NIGHTMARE

How to protect your data in the age of ransomware attacks

DataServ

p: 1.800.560.7378
e: info@dataservtech.com
w: dataservtech.com
t: @dataservtech

31280 Viking Parkway, Westlake, Ohio 44145

Ransomware: The Rising Threat

The FBI has been scrambling recently to contain the latest manifestation of a devastating malware attack commonly known as "ransomware." Schools, hospitals and businesses are often the target. But what is this latest malware, and what can your organization do about it?

Malware has always been a problem, but the latest strain, ransomware, is particularly nasty and problematic.

While ransomware attacks are not exactly new – the first known occurrence took place in 1989 (more on this later) – the frequency of the attacks has increased within the last few years. The Cyber Threat Alliance estimates ransomware has caused $325 million in damages worldwide since January 2015. The FBI has reported victims have paid more than $209 million in ransom payments from January through March of this year. Compare that to $25 million – the total cost of ransom payments for 2015 in the U.S. (per the FBI).

Ransomware attacks live up to their namesake and work like a real kidnapping scenario. In short, hackers send infected links in an email to the victim, and if the victim clicks on the link, which houses a Trojan-style virus, the hackers gain access into the victim's hard drive. The hackers then encrypt the victim's data, making it inaccessible without the encryption key, and hold it for ransom, charging anywhere from hundreds to thousands of dollars in Bitcoin – a difficult-to-trace, virtual currency.

Sometimes the lethal links are offered in a pop-up window or a tempting link on a website. Regardless of the medium, the links often look like they are from a real business or organization.

Recently, hackers have targeted hospitals, school districts and other public institutions. In some instances, schools and hospitals have paid these attackers thousands of dollars to access their critical databases and information. Talos, part of Cisco's Collective Security Intelligence (CSI), discovered that millions of out-of-date devices, mainly in school districts, are at risk to ransomware attacks.

Such attacks paralyze organizations as their records, crucial software and databases are shut down. Unfortunately, the Los Angeles Times reported that the FBI has not made a single arrest in the current rash of ransomware attacks.

WHAT TO DO IF YOU ARE ATTACKED

Unfortunately, if your data is not backed up, you cannot access it again without payment to the hackers to obtain the key. After a certain amount of time, the hackers will probably destroy the key, making decryption completely impossible. Paying the ransom is highly discouraged by law enforcement as it will only encourage the operators of these schemes. What should you do, then?

Well, if your data wasn't backed up, chances are you won't see it again. So, the simple answer to this problem is, back up your data. This is your greatest weapon against ransomware attacks because it renders the entire concept of kidnapped data useless.

WHAT EXACTLY IS THIS VIRUS?

The first known instance of a ransomware-style virus occurred before the internet as we know it existed. Long story short (check out the full story from Medium.com here), a crazed doctor of biology from Harvard, Dr. Joseph L. Popp, sent out 20,000 infected floppy disks – hand copied, packed and posted – to 90 countries in 1989. The floppy disks supposedly contained AIDS education software (in fact, he sent many of the disks to medical research institutions).

But soon the victims of the floppy disks realized something else was going on when their printers spouted out a ransom note demanding a licensing fee of $189 be paid to a PO Box in Panama if they wanted to decrypt their data.

Eventually, the code was cracked, and Popp was arrested. However, he was declared insane and unfit for trial by a judge. To add to this already bizarre tale, he would later found the Joseph L. Popp, Jr Butterfly Conservatory in Oneonta, New York.

> "If your data wasn't backed up, chances are you won't see it again..."

Now let's use science to further understand this virus. There is a reason this type of malware is called a virus. The analogy to its biological counterpart is very apt, because this type of malware is delivered to your computer by carriers, or "vectors." These are the spam emails and tantalizing web page links that come across your screen, and somehow, some way, one of them was activated by a hacker. Also just like biological viruses, the malware authors routinely change their attack vectors so you have to constantly be alert to avoid clicking on the wrong thing.

At the same time, anti-virus software tries to recognize the malware itself and block its actions. But just like with real-life viruses, the malware is constantly changing itself to evade detection. This is especially the case with the crypto virus variants that are changing rapidly (because they are so lucrative to their operators). In short, despite everyone's best efforts, the odds that a crypto virus variant infects us is pretty good.

WHAT YOU NEED TO DO

Infections can be avoided by carefully inspecting every email, not clicking on weird web links and only opening emails if they are from trustworthy sources. For example, if you did not order anything from Amazon, don't open a document from an email that claims to have details of an alleged order; go to your Amazon account and verify its status independently.

While ransomware attacks are difficult to avoid, there are some things that can be done to minimize the impact of an infection:

- In a corporate environment, make sure you do not have any company-wide shared drives mapped to your computer unless you truly need them. Ransomware viruses will encrypt files there, too. If you do need access to such shared drives, consider if you need write as well as read access. The idea is to minimize the grasp of the files the virus can encrypt.
- A good Intrusion Detection System (IDS) might be able to detect the virus' communications with the ransomware operators. The sooner this is detected, the sooner the infected machine can be quarantined. Some IDS solutions automatically quarantine an infected machine.

Lastly, if you think there is even just a remote chance your computer might be infected, swallow your pride and immediately inform your help desk so they can assist in minimizing the impact not only to you, but to the rest of your organization as well.

WHAT NEXT?

In sum, the key to protecting your organization's data and technology from threats like ransomware is to have a working back up system. That way you won't need to pay a cent to ransomware hackers in the case of an attack.

DataServ offers back up and disaster recovery services, security measures (including email filtering services), and safe, secure locations to store your critical data.

Risk management is the first step in knowing if your district or business is prepared for even the most menacing malware attack. DataServ will work with you to identify the necessary procedures to avoid or minimize impact of security threats. We start by conducting a thorough assessment of your technology, which gives us an idea where your organization stands so we can show you what your next steps should be.

To discuss an assessment, contact us at 1.800.560.7378 or at info@dataservtech.com.