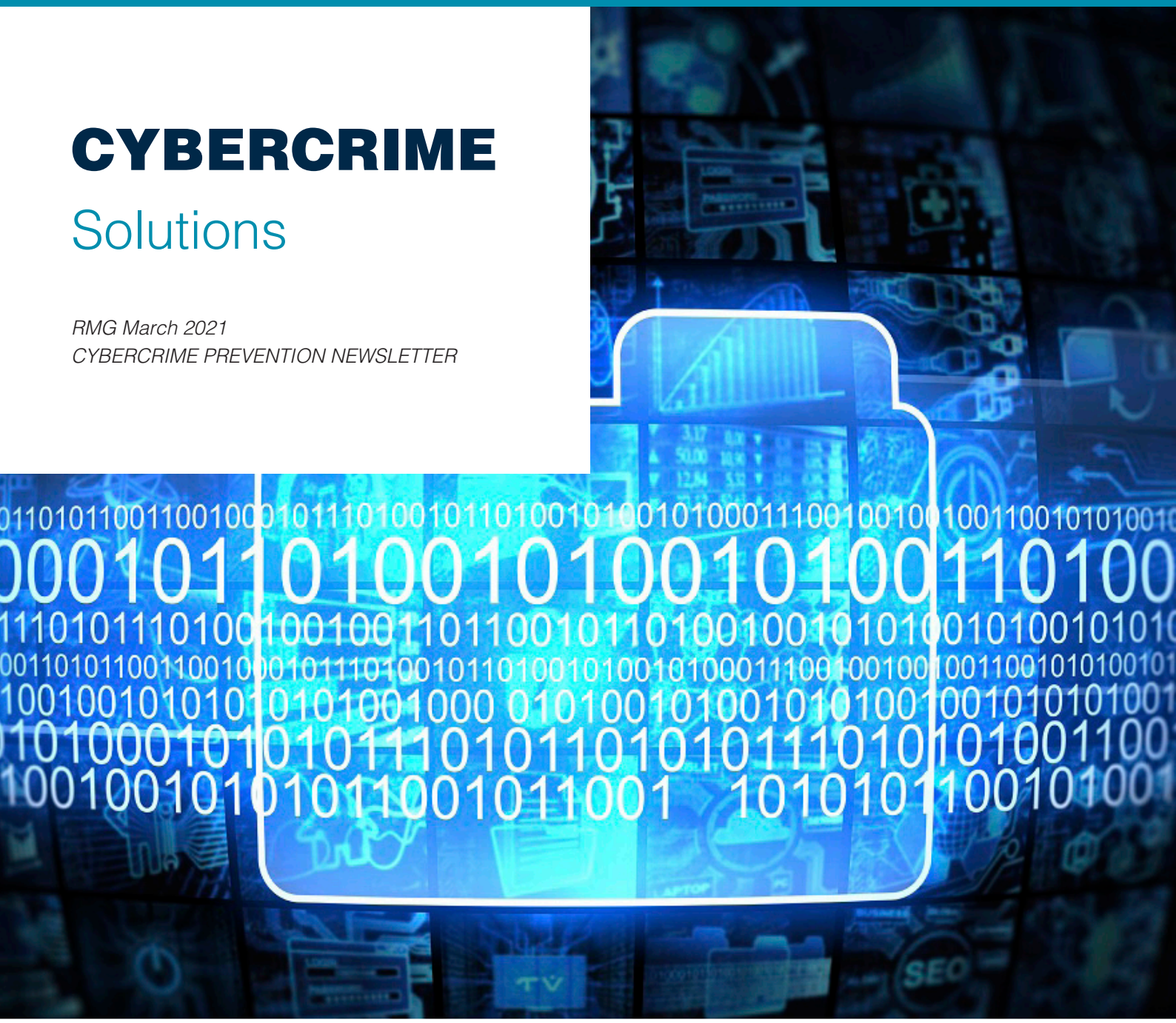
CYBERCRIME

Solutions

RMG March 2021
CYBERCRIME PREVENTION NEWSLETTER



www.rmgforensics.com

INSTITUTE OF DIRECTORS SOUTHERN AFRICA

UNASHAMEDLYETHICAL

RMG
FORENSIC SERVICES (Pty) Ltd.

Contents

Foreword

As part of the Fraud Awareness initiative of the MRG Group to its members this monthly Fraud newsletter would assist with the most current Fraud Trends detected in the industry as well as practical advice to proactively remedy this.

In this month's fraud newsletter version 4 / 2021 we cover the subject at hand: cyber security threats. We will explain the definition and these modi operandi of the fraud and provide tips on how to prevent it.

In the next edition newsletter version 5 / 2021 in the second quarter of the year we will define POPIA in the South African context.

Ransomware

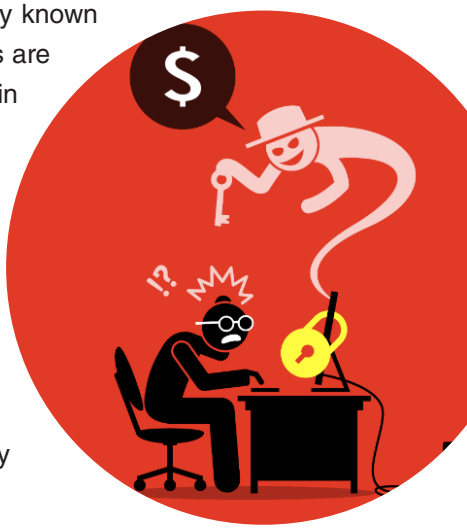
Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment.

Users are shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, usually payable to cybercriminals in Bitcoin.

There are a number of vectors ransomware can take to access a computer. One of the most common delivery systems is phishing spam — attachments that come to the victim in an email, masquerading as a file they should trust. Once they are downloaded and opened, they can take over the victim's computer, especially if they have built-in social engineering tools that trick users into allowing administrative access. Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems, or data.

Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

There are several things the malware might do once it has taken over the victim's computer, but by far the most common action is to encrypt some or all of the user's files; but the most important thing to know is that at the end of the process, the files cannot be decrypted without a mathematical key known only by the attacker. The user is presented with a message explaining that their files are now inaccessible and will only be decrypted if the victim sends an untraceable Bitcoin payment to the attacker.



In some forms of malware, the attacker might claim to be a law enforcement agency shutting down the victim's computer due to the presence of pornography or pirated software on it, and demanding the payment of a "fine," perhaps to make victims less likely to report the attack to authorities. But most attacks do not bother with this pretense. There is also a variation, called leakware or doxware, in which the attacker threatens to publicize sensitive data on the victim's hard drive unless a ransom is paid. But because finding and extracting such information is a very tricky proposition for attackers, encryption ransomware is by far the most common type.

Who is a target for ransomware?

The short answer to the question posed in the heading is 'everyone': Every small business, midsized company, enterprise, and organization is fair game, especially considering the WannaCry and Petya attacks (though the latter was an atypical ransomware example).

The long answer is more complicated. Your vulnerability to a ransomware attack can depend upon how attractive your data is to criminal hackers, how critical it is that you respond quickly to a ransom demand, how vulnerable your security is, and how vigorously you keep employees trained about phishing emails, among other factors.
Who is today's top ransomware targets?

Education

Academic organizations, especially colleges and universities, have been among the top ransomware targets. In fact, a fall 2016 ransomware study from BitSight Insights placed educational institutions as the no. 1 target, with at least one in 10 experiencing a ransomware attack.

Smaller IT teams, budgetary constraints, and a high rate of network file sharing are among the reasons educational organizations are so vulnerable, according to the BitSight Insights report. Plus, “with access to social security numbers, medical records, intellectual property, research, and financial data of faculty, staff, and students, these institutions are a prime target for cyberattacks,” the report noted.

Government

Government agencies are another prime target, ranking no. 2 on BitSight Insights’ list. The occurrence of ransomware in this sector more than tripled from fall 2015 to fall 2016, according to BitSight Insights.

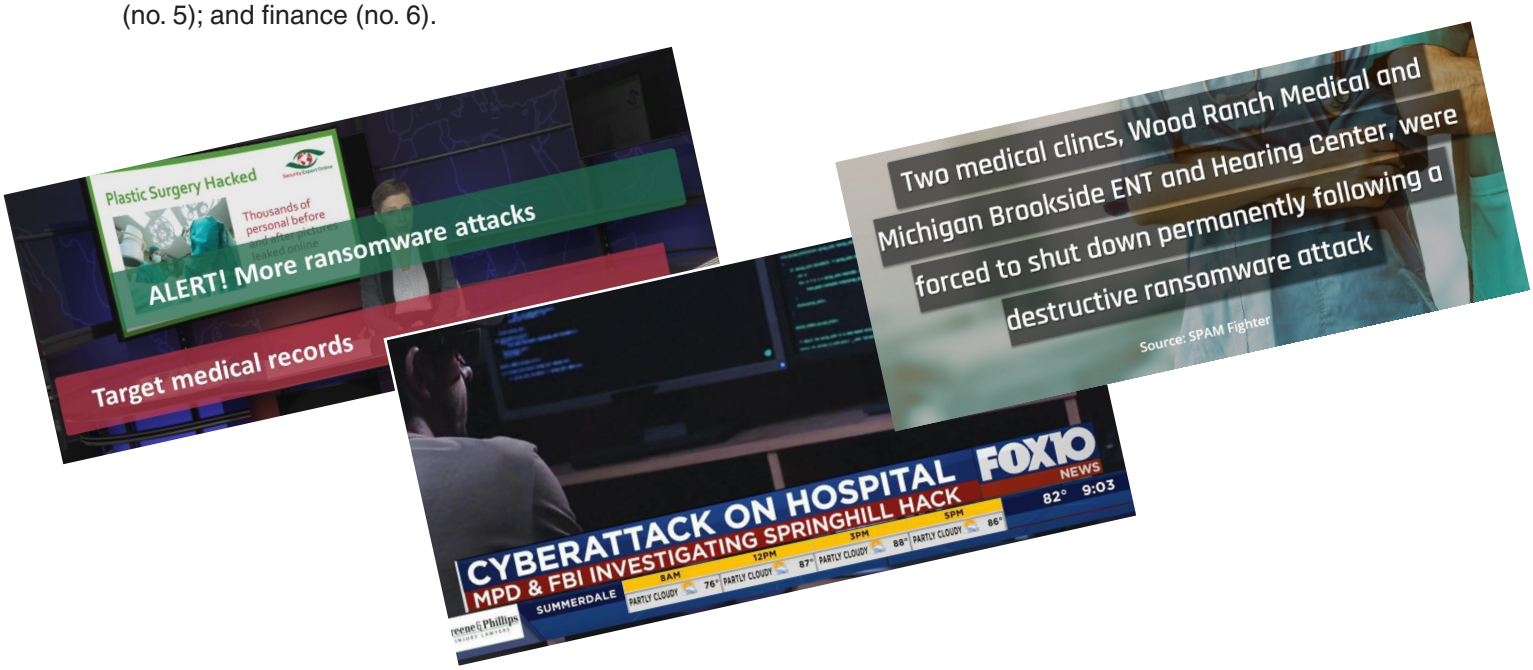
An example occurred in September 2016, when a new ransomware threat, Marsjoke, targeted state government agencies, according to Kaspersky Lab’s Threat Post blog.

Some government agencies may be targeted because the services they offer, such as police protection, are time-sensitive and crucial; because such agencies often need to respond quickly, they have a greater sense of urgency in recovering their data and thus may be more willing to pay the ransom under duress.

Healthcare, energy/utilities, retail, finance

Healthcare organizations ranked no. 3 on BitSight Insight’s top list of ransomware targets. “Hospitals, in particular, may pay the ransom because their patient data is critical in life-or-death situations,” the report noted. One such example was the Hollywood Presbyterian Medical Center, which paid a $17,000 ransom in 2016 to hackers who had locked some of the hospital’s critical data.

The sectors rounding out the BitSight Insights list include, in descending order, energy and utilities (no. 4); retail (no. 5); and finance (no. 6).



HR departments

We are seeing more ransomware attacks targeting enterprise human resource departments where criminal hackers pose as job applicants, hoping that HR professionals will open emails and attachments from unknown senders — which will then spread the ransomware.

Mobile devices and Macs

Ransomware is not just a PC threat. A Kaspersky Lab Malware Report released in May 2017 found that 218,625 mobile ransomware files were detected in the first quarter of 2017 vs. 61,832 in the previous quarter.
Ransomware does not exclusively target Windows computers, either.

Emerging ransomware targets and threats

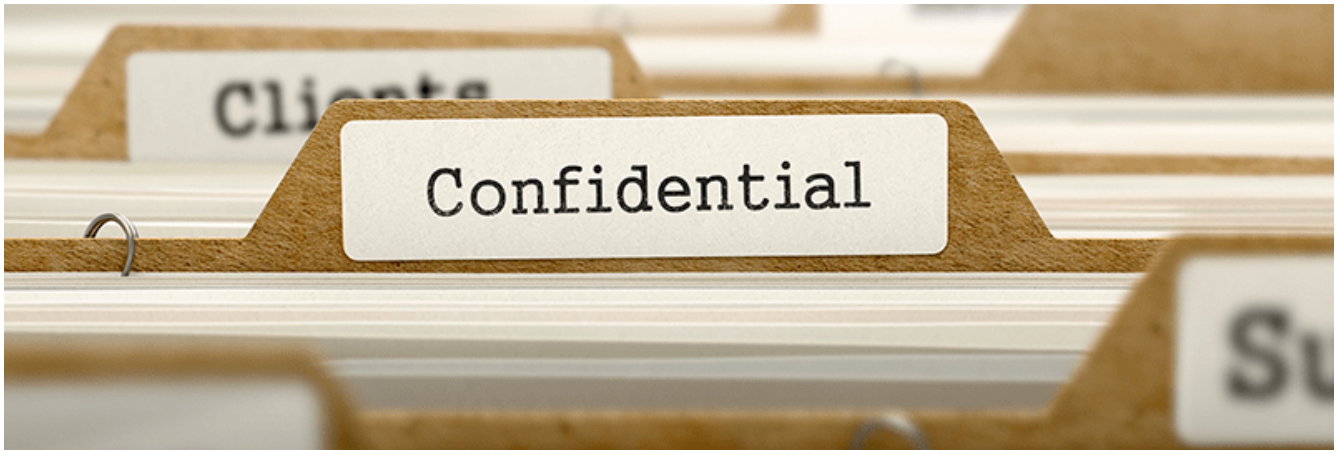
At a high level, any organization that has critical data, and where team members need to make quick decisions, will remain prime ransomware targets.

The sensitivity of an enterprise's data will also be a factor. For example, along with the sectors cited in the BitSight Insights report, you can expect to see law firms among targeted businesses soon. Legal firms have client data that is highly sensitive, and typically have the resources to pay a ransom.

The next phase of ransomware is not just about holding data hostage; it is becoming about threatening to publish data online if the enterprise that owns it does not pay the ransom. In that scenario, law firms — and many other types of organizations — are attractive targets. Criminal hackers might block your ability to access your data, then put the data up for sale online to the highest bidder. Celebrities could be subject to such tactics, as well as organizations with sensitive data and lots of competitors — some of which might be willing to pay to get access to your data.

There are several different ways attackers choose the organizations they target with ransomware. Sometimes it is a matter of opportunity: for instance, attackers might target universities because they tend to have smaller security teams and a disparate user base that does a lot of file sharing, making it easier to penetrate their defenses.

On the other hand, some organizations are tempting targets because they seem more likely to pay a ransom quickly. For instance, government agencies or medical facilities often need immediate access to their files. Law firms and other organizations with sensitive data may be willing to pay to keep news of a compromise quiet — and these organizations may be uniquely sensitive to leakware attacks.



How to minimize the ransomware threat

As much as possible, keep current database backups stored on air-gapped storage, where the backed-up data resides on a device with no network connection.

Phishing emails continue to be one of the most common ransomware attack vectors. As a result, it is important to keep email filtering rules always updated and to provide ongoing employee education. Teach team members how to identify suspicious email and links.

Be cautious about admin credentials, too. Eventually, someone will click on a link in a phishing email and (the malware) will make it into your system. If the person (clicking the link) has wide open access to your network, like admin credentials, the ransomware will have an easier time accessing important files.

As always, use layered security with regular security software patches, vulnerability management, system hardening, and always-updated endpoint protection suites.

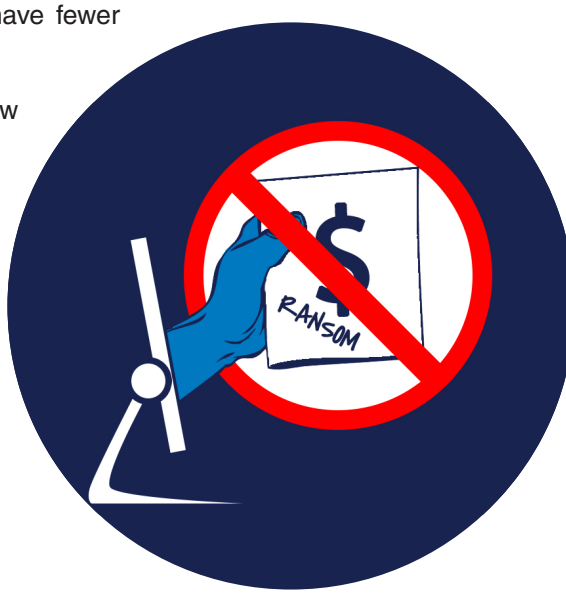
Be clear on the security measures and technologies in place at any cloud services your organization uses. Every day we hear about some massive security breach, and there are many more you don't hear about. If you or your business puts everything in the cloud, you might feel safe from a local attack like ransomware. But think again. What is protecting your company's data on these services? Is it a username and password or something more? What about the employees at these cloud companies since they have physical access to the servers? What could they do to your data?.

In the event of a ransomware attack, having strong security and well-protected backups can help you avoid the worst-case scenarios — paying the ransom, which only encourages more ransomware attacks, or losing big chunks of data.

How to prevent ransomware

There are several defensive steps you can take to prevent ransomware infection. These steps are good security practices in general, so following them improves your defenses from all sorts of attacks:

- Keep your operating system patched and up to date to ensure you have fewer vulnerabilities to exploit.
- Do not install software or give it administrative privileges unless you know exactly what it is and what it does.
- Install antivirus software, which detects malicious programs like ransomware as they arrive, and whitelisting software, which prevents unauthorized applications from executing in the first place.



And, of course, back up your files, frequently and automatically! That will not stop a malware attack, but it can make the damage caused by one much less significant.

Ransomware examples

While ransomware has technically been around since the '90s, it's only taken off in the past decade, largely because of the availability of untraceable payment methods like Bitcoin. Some of the worst offenders have been:

- CryptoLocker, a 2013 attack, launched the modern ransomware age and infected up to 500,000 machines at its height.
- TeslaCrypt targeted gaming files and saw constant improvement during its reign of terror.
- SimpleLocker was the first widespread ransomware attack that focused on mobile devices
- WannaCry spread autonomously from computer to computer using EternalBlue, an exploit developed by the NSA and then stolen by hackers.
- NotPetya also used EternalBlue and may have been part of a Russian-directed cyberattack against Ukraine.
- Locky started spreading in 2016 and was "similar in its mode of attack to the notorious banking software Dridex." A variant, Osiris, was spread through phishing campaigns.
- Leatherlocker was first discovered in 2017 in two Android applications: Booster & Cleaner and Wallpaper Blur HD. Rather than encrypt files, it locks the home screen to prevent access to data.
- Wysiwye, also discovered in 2017, scans the web for open Remote Desktop Protocol (RDP) servers. It then tries to steal RDP credentials to spread across the network.
- Cerber proved highly effective when it first appeared in 2016, netting attackers $200,000 in July of that year. It took advantage of a Microsoft vulnerability to infect networks.
- BadRabbit spread across media companies in Eastern Europe and Asia in 2017.
- SamSam has been around since 2015 and targeted primarily healthcare organizations.
- Ryuk first appeared in 2018 and is used in targeted attacks against vulnerable organizations such as hospitals. It is often used in combination with other malware like TrickBot.
- Maze is a relatively new ransomware group known for releasing stolen data to the public if the victim does not pay to decrypt it.
- RobbinHood is another EternalBlue variant that brought the city of Baltimore, Maryland, to its knees in 2019.
- GandCrab might be the most lucrative ransomware ever. Its developers, which sold the program to cybercriminals, claim more than $2 billion in victim payouts as of July 2019.
- Sodinokibi targets Microsoft Windows systems and encrypts all files except configuration files. It is related to GandCrab
- Thanos is the newest ransomware on this list, discovered in January 2020. It is sold as ransomware as a service, it is the first to use the RIPlace technique, which can bypass most anti-ransomware methods.