Hakin9

PRACTICAL PROTECTION IT SECURITY MAGAZINE

VOL.16, NO. 06

RANSOMWARE AND VULNERABILITY MANAGEMENT

Ransomware and Phishing

Vulnerability Management Introduction

Simple Android Ransomware and Mrs. Major Virus

Demystifying Malware An Entry Level Introduction to Malware

AND MORE...

Hakin9

TEAM

Editor-in-Chief
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Editors:

Marta Sienicka
sienicka.marta@hakin9.com

Magdalena Jarzębska
magdalena.jarzebska@software.com.pl

Marta Strzelec
marta.strzelec@eforensicsmag.com

Bartek Adach
bartek.adach@pentestmag.com

Michalina Szpyrka
michalina.szpyrka@eforensicsmag.com

Proofreader:
Lee McKenzie

Senior Consultant/Publisher:
Paweł Marciniak

CEO:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Marketing Director:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

DTP
Magdalena Jarzębska
magdalena.jarzebska@software.com.pl

Cover Design
Hiep Nguyen Duc
Joanna Kretowicz

Publisher
Hakin9 Media Sp. z o.o.
02-676 Warszawa
ul. Bielawska 6/19
Phone: 1 917 338 3631

www.hakin9.org

All trademarks, trade names, or logos mentioned or used are the property of their respective owners.

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Betatesters & Proofreaders

Lee McKenzie

Hammad Arshed

Bernhard Waldecker

Amit Chugh

Alexandre D'Hondt

Craig Thornton

Paul Mellen

Tom Updegrove

Jeff Smith

Christopher Pedersen

Jay Kay

Steve Hodge

Jonus Gerrits

Matthew Sabin

Bhuna Salvedurai

Graham Hili

Ricardo Puga

Olivier Caleff

Dear Readers,

We decided to dedicate our June edition to a very current and recurring topic - Ransomware and Vulnerability Management. During the COVID pandemic, the ransomware industry was more powerful than ever. That's why it's so crucial to understand how ransomware and malware threatens us every day, but also how to prevent or secure vulnerabilities of our system. We prepared ten quality articles that will help you acknowledge and protect yourself from those threats. Let's dive into it!

We start off with *Ransomware Redux*, in which you'll learn what ransomware is, how to prevent its attacks and what was a "Colonial Pipeline" case. Then we swiftly drift to *Ransomware and Phishing*, in which the author explains why ransomware is so dangerous and how phishing can be used to leverage such attacks.

Later on in *Project Indigo Brick. New Pathways in Data Handling* you'll explore the landscape of problems that arise from ransomware, and also you'll learn about the newest solution for securing your data from such attacks.

In Introduction to *Vulnerability Management. How to Perform Effective Vulnerability Management* you'll learn how important is the role of effective vulnerability management and what are the best vulnerability analysis tools. If you're more interested in Android security, we suggest you take a look at *Simple Android Ransomware and Mrs. Major Virus*, in which the author explains characteristics of a simple android ransomware attack (SARA) and presents how to use the Mrs. Major virus.

Later on, in *Ransomware (Trojan Horse) Attacks Could Have Been Predicted Back in 1987 by Reading the Department of Defense's Orange Book*, the author explains how The Department of Defense's rainbow series for information security is still relevant and how Trojan Horse attacks on Windows could have been predicted by the orange book due to Windows' discretionary Access Control.

If you prefer more analytical articles, you may want to take a look at *The Darkside Ransomware Sample Analysis, Part 1*, in which the author analyses a ransomware sample using REMnux.

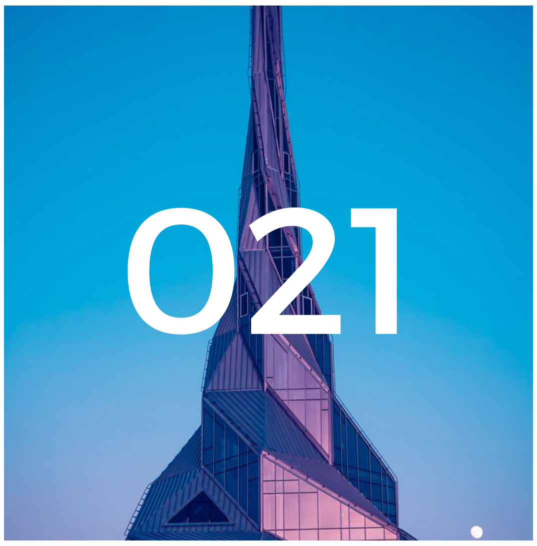
But there's more! We also prepared articles touching the topics of malware, password cracking, and mobile security, so everyone can find something for themselves.

We hope you'll enjoy reading this issue as much as we enjoyed creating it. We would also like to thank our contributors, reviewers and proofreaders, without whom this edition wouldn't have been possible.

Stay safe and enjoy!

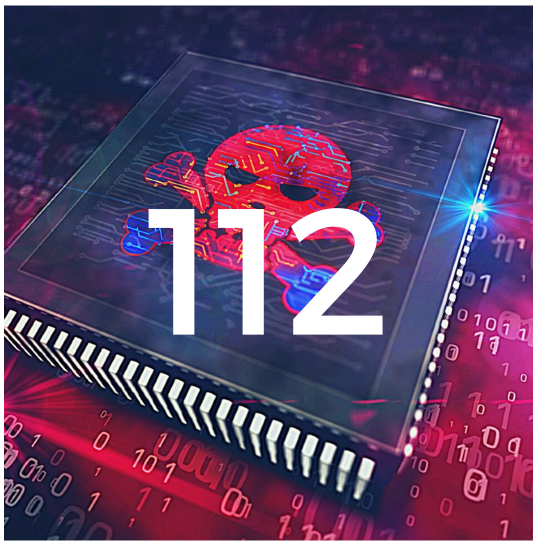
Hakin9 Editorial Team

Contents

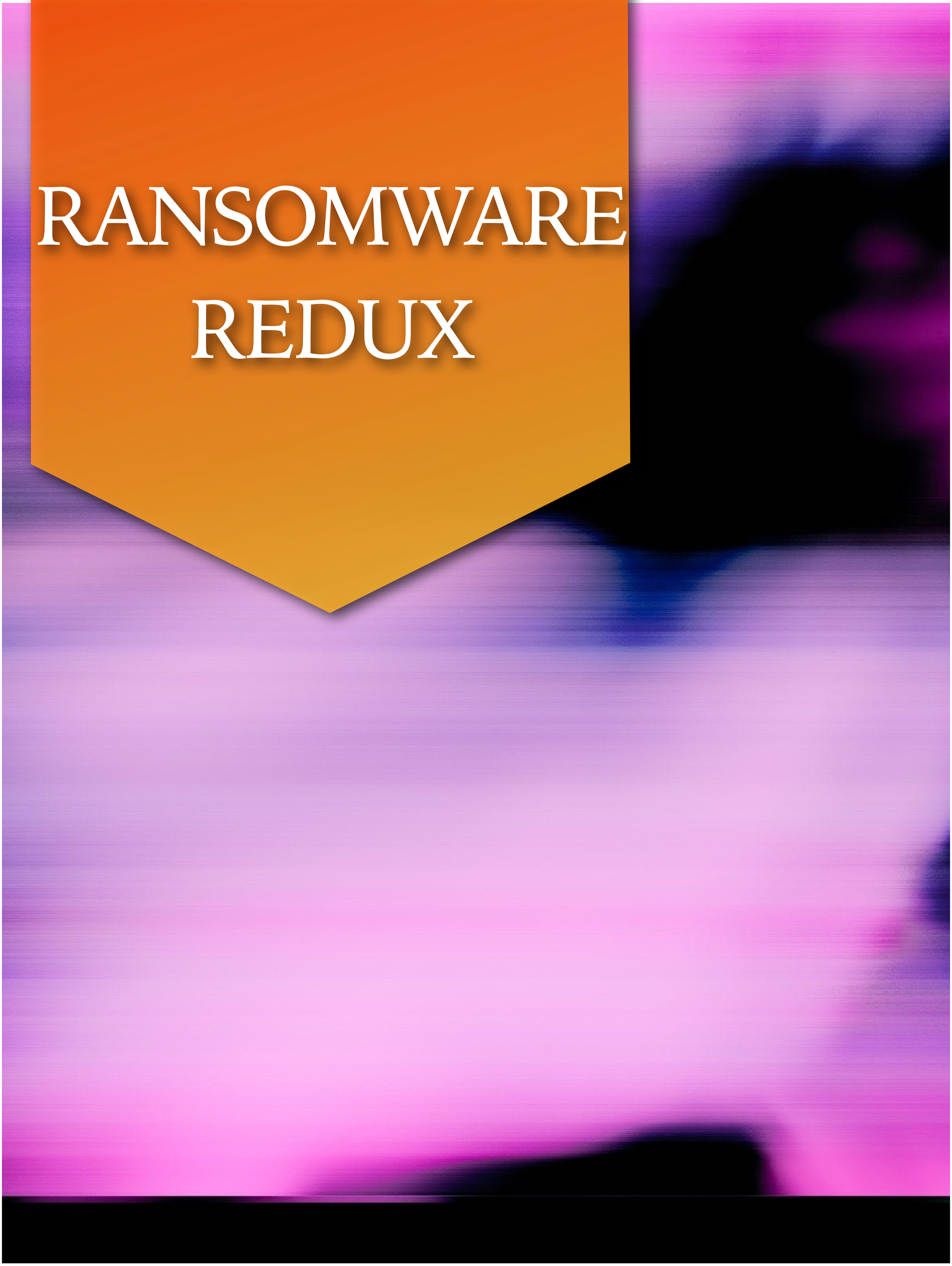


Contents

Contents



RANSOMWARE REDUX



SYED PEER

The author is a seasoned 20-year IT professional having worked in Fortune 400 companies across diverse verticals from Social Media to Banking to Cyber Security with experience managing Software Development, Engineering and Cyber Security teams.

“Go therefore, tell thy master here I am;
My ransom is this frail and worthless trunk,
My army but a weak and sickly guard

– Henry V (3:5) by William Shakespeare

Introduction

As humanity (in its billions) marches forwards in its relentless race to break new technology frontiers and mankind revels in its fruits with gadgets galore and more toys than we will ever have to time to play with, a blue-collar industry has come into existence of modern-day burglars, pirates, and ***highwaymen***.

The highwaymen of old, masked, locked and loaded, would locate themselves in green pastures and foliage for camouflage and lay in wait for their unsuspecting victims to arrive. Then at the appropriate moment they would reveal themselves on the road and stop stage coaches in their tracks while their victims stared down the barrel of a musket and were read the unforgettable command “Stand and deliver”. Theirs was a strategy of stealth and ambush that would confuse and confound their victims, ungentlemanly in its manner but lethal in its execution. Their prize would be a “king’s ransom” (or whatever was available) in return for the lives and property of their victims.

Fast forwarding to the present, a whole new industry has evolved of digital highwaymen better equipped than their forebearers and more efficient in their methods concealing their identity and leaving few traces of their pathways and steeped in a currency only the most daring can afford.

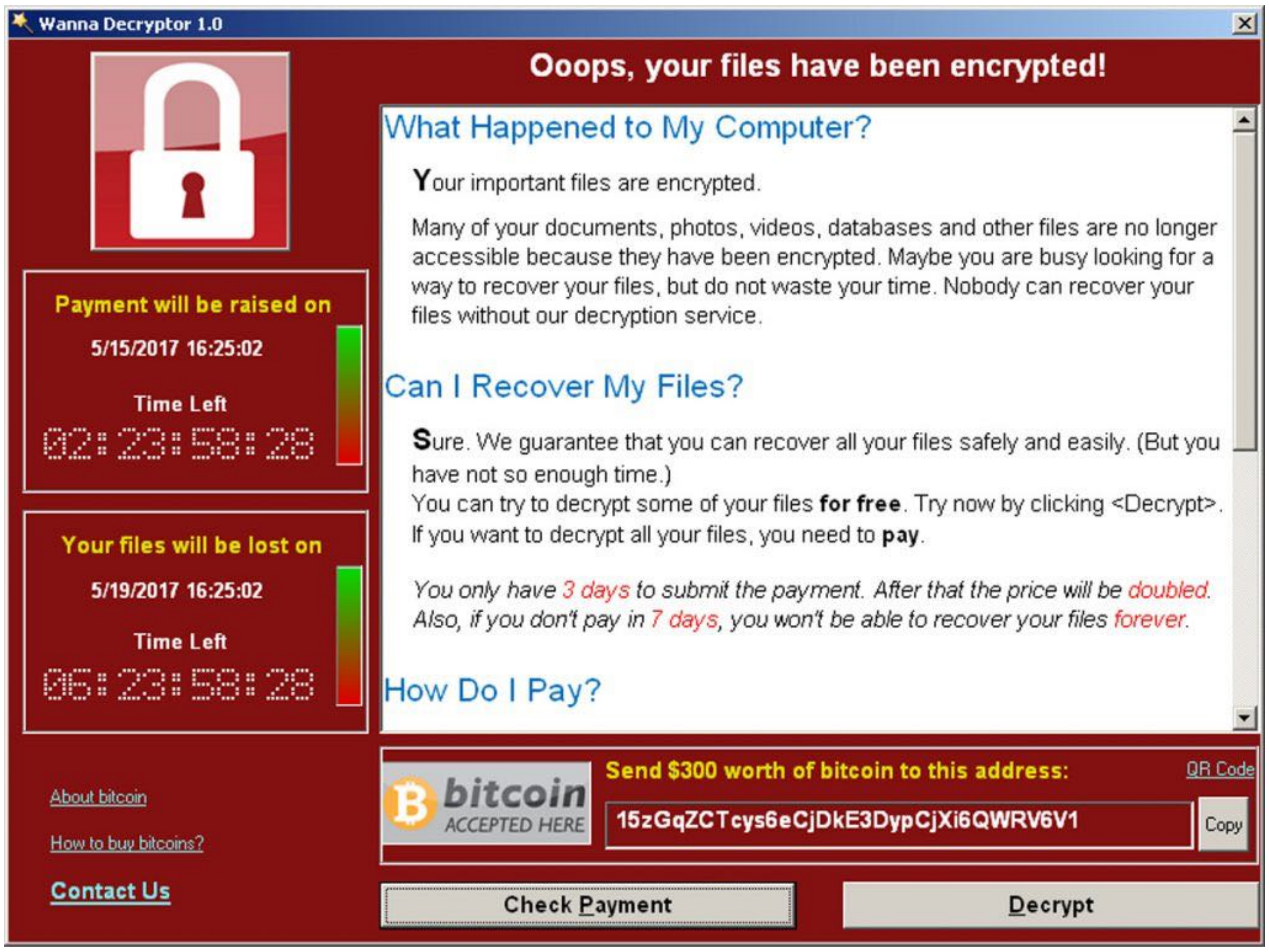
Ransomware Definition

As defined by Wikipedia *"Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them”.*

Background

Ransomware has been a “thing” since the mid-2000’s and has affected enterprises of all sizes and verticals and even touched the lives of individuals. In 2017 alone the FBI’s Internet Crime Complaint Center (ICC) received almost 2000 complaints that cost the victims over 2 million dollars in payments. Those were only the officially reported cases. We may surmise that the actual numbers are much higher considering that in 2020 alone there were over 180 million ransomware attacks reported.

Relying solely on the internet alone, these modern armchair highwaymen have wrecked the lives and business of so many and made a permanent place in the annal of cybercrime.



Wanna Decryptor 1.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

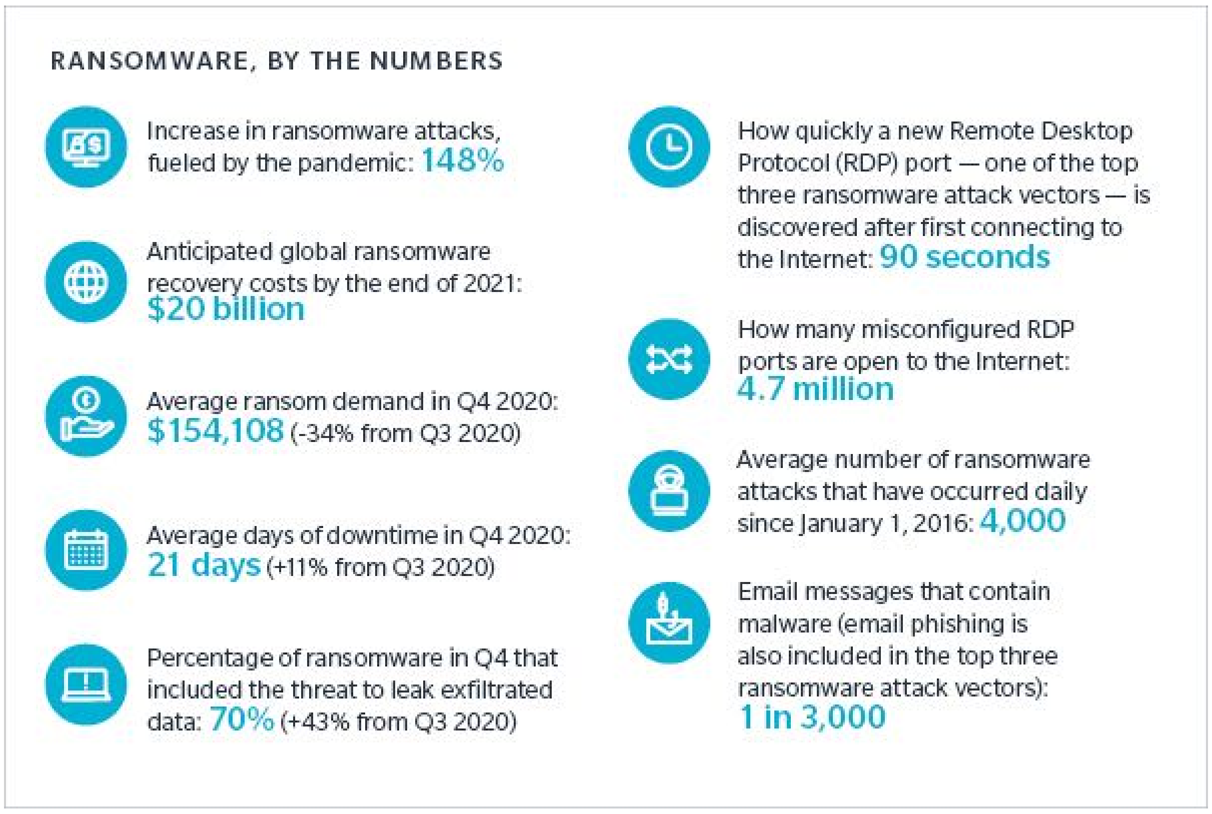
Send $300 worth of bitcoin to this address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Wannacry screenshot

While ransoming has been around for centuries whether for goods or captives taken in battle or as part of conquest, modern day digital ransomware varieties have grown exponentially with increasingly advanced capability to spread laterally across the organization, to avoid detection, to encrypt files and folders and to apply measured coercion to exact payments. Modern day ransomware proponents will even make use of legitimate system level features such as Microsoft's CryptoAPI, thereby avoiding the need for calling an external Command and Control (C2) point and avoiding detection by any in-house Data Leakage Prevention (DLP) solution.

Ransomware: Modus Operandi

The term "ransomware" is somewhat misleading as it points to the endgame of customer extortion rather than the mechanics of what is actually happening under the hood. The first step always has to be a means to access the target systems files and folders and this is often facilitated by a targeted phishing attack. Some sobering 2020 ransomware stats are shown below.



RANSOMWARE, BY THE NUMBERS

Increase in ransomware attacks, fueled by the pandemic: 148%

Anticipated global ransomware recovery costs by the end of 2021: $20 billion

Average ransom demand in Q4 2020: $154,108 (-34% from Q3 2020)

Average days of downtime in Q4 2020: 21 days (+11% from Q3 2020)

Percentage of ransomware in Q4 that included the threat to leak exfiltrated data: 70% (+43% from Q3 2020)

How quickly a new Remote Desktop Protocol (RDP) port — one of the top three ransomware attack vectors — is discovered after first connecting to the Internet: 90 seconds

How many misconfigured RDP ports are open to the Internet: 4.7 million

Average number of ransomware attacks that have occurred daily since January 1, 2016: 4,000

Email messages that contain malware (email phishing is also included in the top three ransomware attack vectors): 1 in 3,000

Courtesy marsh.com

The “Colonial Pipeline” Case Study

The ransomware attack on the Colonial pipeline is a case study in what should and should not have happened. Organization need to review the information and take a pragmatic look at their own IT and OT systems in place.

- Though spear phishing is the flavor du jour for most breaches, in this case hackers gained access to a legacy VPN account password and started their work in earnest. How they obtained access to the that legacy VPN profile is unclear and still under investigation.

- Although the attack was significant in its reach and disruption it was NOT “nation-state” sponsored but executed by individuals and private criminal teams intend on extortion. This only demonstrates how fragile our systems have become and how careless our security practices by those who operate them.

- In the year 2018 an external Audit of Colonial discovered “*atrocious*” information management practices and a “*patchwork of poorly connected and secured systems*”. Probably not alone in the energy industry for such poor findings, it still surprises that even 3 years after such a report they fell victim to such an attack and one can only assume that their “information management practices” have not improved significantly to allow orphaned VPN accounts to be still available for exploits.

- Most worrying, without an advanced Trojan Horse or a focused spear phishing campaign or malware specifically engineered “fit for function” or the Colonial network, hackers simply used a redundant (yet active) orphaned VPN credential login password to gain access into Colonial’s secured systems and achieved the necessary lateral movement of malicious software.

- Whether by luck or intent Colonial managed to have sufficient warning time to disable their OT systems that supplied gasoline to most of the Eastern Seaboard states.
- Ransomware often avoids anti-malware detection tools and morphs so rapidly from attack to attack that fresh variants may be unrecognizable and prevention tools totally ineffective.
- Even though they had the necessary backups, the lack of a robust recovery execution plan forced Colonial to cut a Bitcoin check (to the tune of 5 million dollars). Again, this highlights poor or inadequate practices in place and even poorer defense and public communications strategy. The money trail led the FBI to an Eastern Europe outfit known as "Darkside" who have since been very apologetic for their actions but have not returned the money.
- Enforcing Federal Regulatory compliance energy providers may be a viable solution, but with up to 80% of power generation, distribution, refining etc. being privately owned in the US – there may be a long wait for the end game.

In short, there was ample time (3 years) and early warnings (from the 2018 audit) to have taken necessary measures but Colonial still fell victim to a 5th graders attack vector (credential compromise).

Mitigations

Organizations need to looking at some of the following steps as a minimum requirement if they are to prevent embarrassing repeat attacks due to VPN vulnerabilities.

1. **VPN Known Exploits:** If there are known vulnerabilities with VPN providers and equipment, then a strategy needs to be urgently formulated for how their systems can be patched or if unpatched how they can be a part of a High Availability solution that provides for other devices to fail over. This is NOT a casual budget expense but may be necessary as a last resort if the Colonial style damage is to be avoided. VPN should be included as a critical attack vector and organizations should prepare for continuous patching and monitoring as necessary.

2. **Build Resilience:** Organizations need to have policies and procedures in place already for regular data backups, air gap enablement including necessary and better password and credential management tools to flag for archived or orphaned logins that may still work for outsiders and supply chain partners.

3. **Redraw and Remap the Network**: In the search for better security, business owners must review and possibly remap their network configuration allowing for rigorous **segmentation** to keep the critically impacted areas within their control and containment strategy. After saving lives (which remain their first priority) Firemen rarely try to save the whole building, they are only interested in preventing the spread of the fire to adjoining homes and businesses in the surrounding areas. Computer networks are no different and need some TLC (tender loving care) every few years is needed to be sure that networks are reviewed and optimized for security and "containment".

4. **Use Multi-Factor Authentication (MFA)**: Every login to systems should require a secondary degree of validation that MFA can provide. Although some customers are loath to use it, due to its so called an inconvenience, the technology

has been around for a number of years and provides the additional security to trust any login credential. How far would the Colonial hack have reached if MFA been implemented on all VPN logins?

5. **Audit:** Continuously ask for an audit of accounts with heightened privilege for both Super Users and Networks Admins. Ensure that a “least privilege” approach is established and all deviations from the same require manager approvals. Internal Audit will be all to ready to help IT / OT with this so it should not be a burden to do regularly with a rotating schedule.

6. **Enforce More Rigid Email Restrictions:** Disable hyperlinks contained within received emails to prevent spear phishing and malware spread. Improve email filtering and ensure that antivirus and anti-malware software are current and up to date.

7. **Awareness Training**: Build out the employee awareness and training program and ensure that they are current with respect to recent attack vectors. Employees are the first line of defense and their education should remain a priority.

8. **Password Policy**: Require complex passwords and ensure that they are changed regularly based on an agreed schedule. Disable all unused credentials for any type of remote access/RDP and ensure that necessary ports and logs are reviewed regularly.

Conclusion

As we can see clearly now, the ransomware threat is not going away anytime soon. Quite the opposite is to be expected. As long as there are pliable targets (such as Colonial) all too ready to part with the cash after the event rather than invest in better training and threat monitoring and due diligence before the attack, there will remain an army of ready and able actors to continue this trend.

Separately, the dependence on private energy providers and infrastructure who are not necessarily beholding to government regulatory edicts will further cloud the affair with few government agencies ready to take on the energy suppliers. To face the modern threat though every government needs to re-asses the private sector dependency curve and how it can strengthen its cyber security net without stifling private investment and job creation.

References:

1. Wikipedia Definition: https://en.wikipedia.org/wiki/Ransomware

2. Ransomware Stats:
https://www.marsh.com/us/insights/research/ransomware-stats-every-business-needs-to-know.html