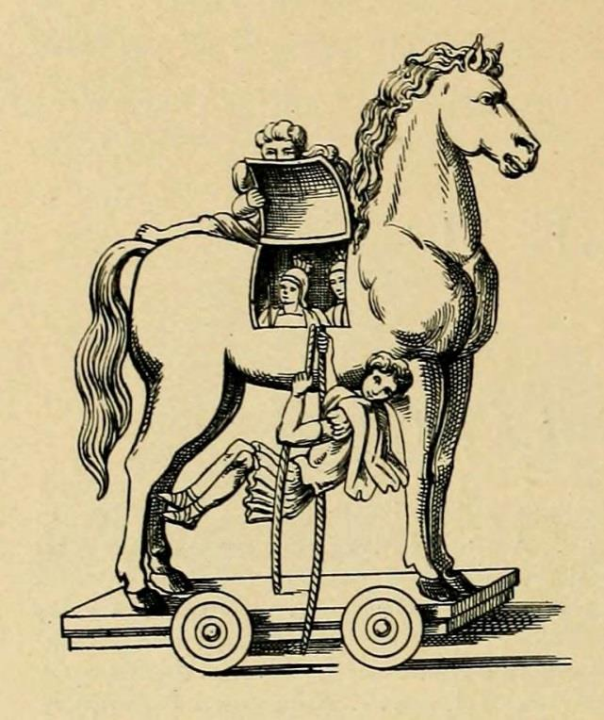
Show me the money! Ransomware…The billion dollar nightmare

Practical steps in taking charge of your life and business from malware!



The world just witnessed one of the biggest ransomware outbreaks to date, affecting more than 200,000 organizations in 150 countries from the NHS in the UK to Renault factories in France, Telefónica in Spain as well as Russia's second largest mobile operator, MegaFon.

The success of the current ransomware attacks has meant that cyber criminals are going to continue to expand and improve their approaches. It is our bad luck that still we are not fully prepared to handle these outbreaks in a timely fashion. The malware attack was briefly stopped when a security researcher identified an obscure domain name in the malware's code and bought the domain. However, this may have just been a temporary solution as the hackers behind the attack could easily just change the domain and re-release the malware.

Let's briefly examine the motives behind these attacks and how IT security teams must be prepared to address and overcome these attacks.

First what is 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.

It is one of the fastest-growing malware threats today and is already an epidemic. The FBI reported a tenfold increase in ransomware crimes which putting ransomware on track to be at least a $1 billion crime. According to a report, an average of more than 4,000 ransomware attacks has occurred daily since January 2017. More than $200 million have been paid in ransom during the first three months. As per research, the financial impact of this brand of cybercrime starts in the range of $75 billion each year.

But what are the drivers and motives in rise of the ransomware?

Ransomware is not a new threat. The earliest known ransomware was PC Cyborg back in 1989. Since that time, ransomware has evolved and become far more sophisticated. Other key developments that have made ransomware more pervasive and lucrative such as the:

- Release of the mobile computing including Android phone and Apple iOS
- Rise of Bitcoin: Bitcoin enables easy and virtually untraceable payments to anonymous cybercriminals.
- Emergence of Ransomware-as-a-Service (RaaS): RaaS can be purchased for a small fee and/or a percentage of the ransom payment which makes it easy for practically anyone to use ransomware.

How Ransomware operates?

Ransomware is commonly spread through email attachments; infected programmes; drive-by infections on compromised websites; direct network connections that exploit operating system vulnerabilities; exploit kits; waterhole attacks (in which one or more websites that an organization frequently visits is infected with malware); or malvertising (malicious advertising).

Once delivered, ransomware typically identifies user files and data to be encrypted through an embedded file extension list. It is also programmed to avoid interacting with certain system directories (such as the windows system directory, or programme files directories) to ensure system stability for delivery of the ransom after the payload finishes running.

Files in the specific locations that match one of the listed file extensions are then encrypted. Otherwise, the file(s) are left alone. After the files have been encrypted, the ransomware typically leaves a notification for the user, with instructions on how to pay the ransom.

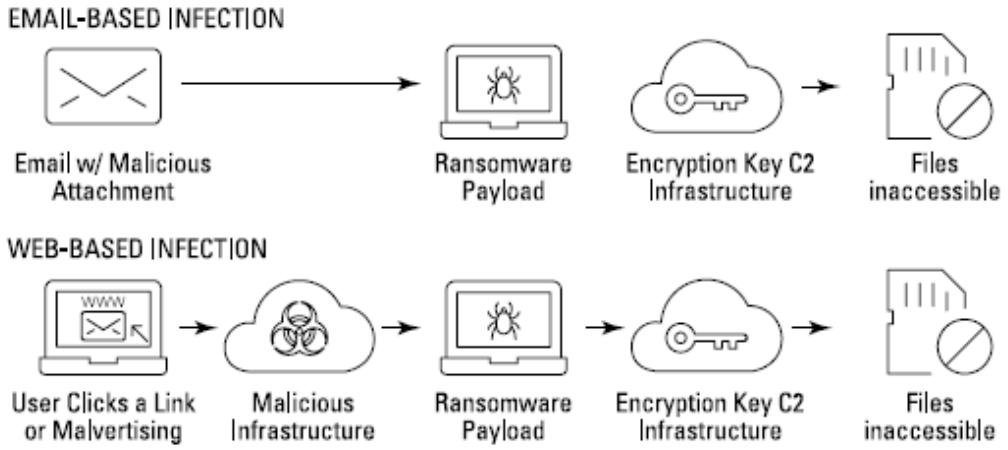


Figure 1: How ransomware works.

Figure 2: Screenshot of WannaCry's Ransom Demand.

Let's talk about whether you want to pay the ransom or not?

There is no honor among cyber criminals. Ransomware works for criminals only when their victims pay the ransom. Although an attacker will usually provide the decryption key for files if victim pays the ransom, but there is no guarantee that they haven't already installed other malware and exploit kits on endpoints or other networked systems, or that they won't steal data for other criminal purposes or to extort more payments in the future.

Ransom amounts may also increase significantly the longer a victim waits. Like any blackmail, cyber criminals try to limit a victim's options and get the victim to pay the ransom as fast as possible.

The victim often believes that paying the ransom is the most cost-effective way to get their valuable data back and, unfortunately this may be true.

Let's talk about how to implement best practices to reduce Ransomware risks

There are a number of best practices that organizations can proactively implement before, during and after targeted by an attacker. Ransomware attacks can be opportunistic. The attacker's motive is often profit, with as little risk and effort as possible. Preventing an attacker from gaining entry to the network with an architectural approach is the most effective way to prevent a ransomware attack from succeeding in the first place.

Attackers usually achieve initial access to a target through one of two methods:

- Social engineering/phishing to get an unsuspecting user to expose his network credentials or install malware
- Exploiting a vulnerability in a public-facing (Internet) application or service

Before an Attack:

The following best practices should be implemented to prevent attackers from gaining access to an organization's network and systems.

- Conduct regular and continuous security awareness and training for end users and employees
- Perform ongoing risk assessments to identify any security weaknesses and vulnerabilities in your organization, and address any threat exposures to reduce risk

- Ensure that your existing incident response plan is able to address a ransomware incident
- Enforce tried and tested backup and recovery processes
- Keep up to date with software patches and updates across the IT and security infrastructure
- Remove the use of administration rights where possible
- Institute a privilege management programme to eliminate unnecessary data access privileges to minimize the data at risk
- Implement endpoint controls, particularly for remote and roaming users
    - Keep antivirus current
    - Deploy an endpoint tool to block bad applications
    - Implement web security for off-network endpoints
    - Consider User Behavior Analytics (UBA) to identify and shut down suspicious activity on key endpoints, even when operating off-network
- Implement controls at network egress points
    - Firewall rules to block command and control traffic as well as counter evasion techniques that may be used to deliver malicious payloads
    - Advanced threat protection controls, including sandboxing, to defend against zero-day and other highly evasive malware techniques
    - Web security solutions to block unknown/uncategorized destinations and perform real-time analysis of web content
    - Email security solutions to block incoming email-borne threats

During an Attack:

If your organization is under attack, fast and effective incident response is required to limit any potential damage. The specific action steps and remediation efforts to be undertaken will be different for each unique situation. However, the time to learn the breadth and extent of your organization's incident response capabilities is not during an attack. Your incident response efforts should be well understood and coordinated before an attack and should be documented and repeatable, so that you can reconstruct an incident after an attack and identify lessons learned and potential areas for improvement.

A key component of effective incident response that is often overlooked is information sharing, which includes the following:

- Communicating timely and accurate information to all stakeholders
- Automatically sharing new security intelligence throughout the architecture. Bringing together critical data from disparate systems, such as SIEM, Threat Intelligence and

sandboxing tools, enables the incident response team to quickly surface and effectively triage high-impact security incidents.

After an Attack:

Important actions after an attack has ended include the following:

- Resuming normal business operations, including restoring backups and reimaging systems, as necessary
- Collecting and preserving evidence for law enforcement and auditing purposes
- Analyzing forensic data to predict and prevent future attacks, for example, by identifying related domains and malware with the associated IP addresses, file hashes, and domains
- Performing root cause analysis, identifying lessons learned, and redeploying security assets, as necessary

It is highly recommended to improve existing security architecture to leverage an integrated, portfolio-based approach that is simple, open, and automated, rather than traditional point products to safeguard businesses against ransomware and other modern threats.

As more organizations get smarter with their protection mechanisms, the profitability of ransomware will decline, so there is no harm in sharing your 'best practices' and 'lessons learned' with professional network.

These attacks also raise significant questions about whether or not countries that are developing and stockpiling cyber weapons can do more to protect those tools from being stolen and turned against their own population.

The real damage caused by the devastating cyberattacks is becoming clearer. Its impact will be felt for a long time to come, like the World Wars' which impacted the generation before us.

So what is the solution? How can you protect yourself?

I would like to conclude with the following important comments on ransomware defense;

1. Ransomware is the fastest-growing malware threat and it is evolving at an alarming rate with new and more sophisticated variants and exploits. Attackers are adjusting their lures to the local language of their targets to smooth the payment process.
2. Ransomware-as-a-Service has emerged as a new threat that makes it as easy as "one, two, three" for practically anyone with limited technical skills to become a cybercriminal.

3. Paying a ransom doesn't solve security problems. It directly funds and perpetuates future cybercrime and other criminal activity. Once you get caught in this 'spider web' by paying ransom, it will leave you trapped and vulnerable to future ransom demands.
4. Build a layered security architecture based on good practices that allow new and existing security technologies to be easily integrated into a comprehensive security solution.
5. Deploy integrated and best-of-breed portfolio-based solutions that reduce complexity in their security environment and improve their overall security posture.
6. Embed security throughout the network environment, throughout the data center, on endpoints on mobile devices, and in the cloud.
7. Reduce complexity and minimize unnecessary interfaces in the security environment as security technologies should be simple to deploy and use.
8. Leverage cloud-based, real-time threat intelligence as it enables IT teams to deploy the most up-to-date countermeasures as quickly as possible when new threats emerge, and leverage security expertise that extends well beyond their organization.
9. Automate security actions to reduce response time including dynamic access control lists (ACLs), domain and website whitelisting / blacklisting, and firewall rule creation and distribution and installation of anti-malware and intrusion prevention system (IPS) signature files.
10. If you see something then say something. There is no harm in reporting infection details, which will in turn give authorities more comprehensive view of ransomware's spread and impact in the event of attack.

Protect yourself through the Centre of Excellence in Cyber Security, Governance, Risk & Compliance (CGRC) services.

CGRC's cyber security business and technical services are delivered by a team of experienced consultants and penetration testers who have a deep understanding of the range of cyber risks faced by organisation's today, enabling you to implement the best possible security solutions to fit your budget and requirements.

A ***Cyber Health Check*** to understand the overall view of how effective your security plan is. Are the right IT security controls in place to protect the information that is critical to your business?

An ***ISO 27001 Consultancy***, whether your organisation has the necessary security controls to monitor, review and protect organisation's information assets

Penetration testing services to assess your organisation's vulnerability to attack as well as the value and exploitability of critical assets

A ***Cyber incident response plan*** to support your response time and the resumption of business activities after a ransomware attack

A ***Phishing staff awareness course*** to ensure your staff has the knowledge and awareness to rebuff phishing attacks that distribute ransomware.

CGRC
Risk. Managed.

Centre of Excellence In Cyber Security, Governance, Risk and Compliance (CGRC)
Park Road
(Adjacent Abasyn University),
Chak Shazad,
Islamabad
Phone : 051 – 8732472

Fax : 051 – 8448227

Email : info@cgrc.edu.pk

Web : www.cgrc.edu.pk