L5 CONSULTING
BUSINESS OPERATIONS ... REIMAGINED

L5 Consulting Provides Your Best Defense Against Ransomware.

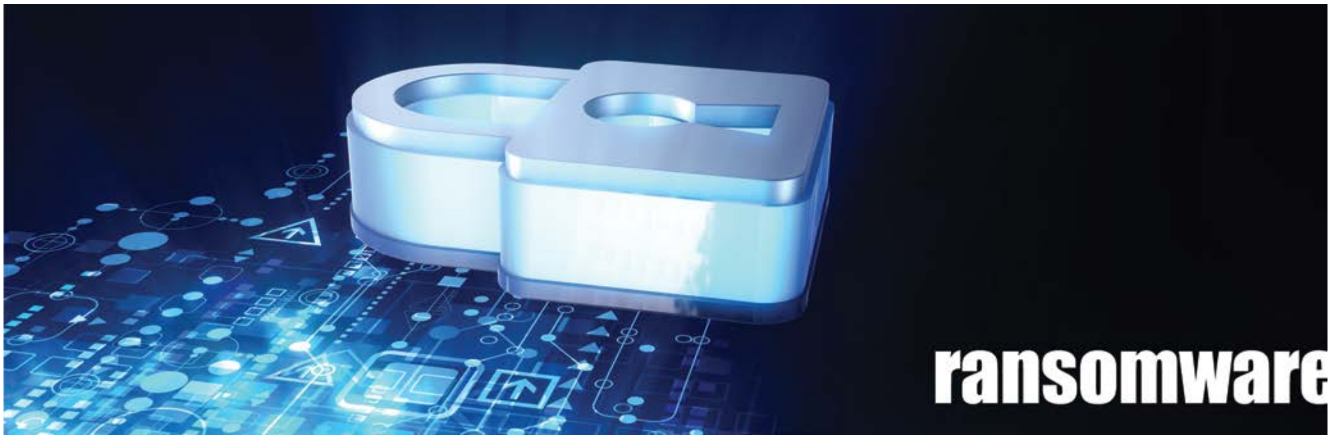
Ransomware is computer malware that holds your data hostage, or threatens to publish your data until you pay a ransom. It typically demands payments in the hundreds, if not thousands, of dollars. When ransomware blocks access to your data you'll receive a demand for payment through an anonymous system like Bitcoin to restore access. Ransomware is the fastest-growing malware threat today. It's become a lucrative criminal enterprise that is spreading and evolving at an alarming rate.

Ransomware is the fastest growing malware today, with an average of more than 4,000 ransomware attacks occurring each day in the U.S.

The Pace of Ransomware and Its Evolution is Accelerating

The rapid growth and evolution of ransomware is due to the:

- Increase in **Android** use (a popular vector for attack).
- Expansion of **Bitcoin** (that promotes virtually untraceable payments to cybercriminals).
- Emergence of **Ransomware-as-a Service** (RaaS). Cybercriminals can purchase RaaS software for a small fee and/or a percentage of the ransom payment, making it easy for almost anyone to use ransomware.



The most lucrative and far-reaching form of ransomware, CryptoWall, has infected billions of files worldwide. Since its beginning in 2014, three more versions have been developed, each one more sophisticated than the one before.

Advanced malware like ransomware evolves so quickly that it can evade detection even after it's compromised your system.

Losses Due to Ransomware

Locky is another example of an aggressive ransomware that affects as many as 90,000 victims per day. Locky could potentially infect as many as 33 million users over a 12-month period, resulting in between $287 million and $574 million in losses due to ransom payments.

Plus, loss estimates are even greater when you consider overall costs such as:

- Regulatory fines and penalties
- Legal fees
- Loss of business due to business interruptions, brand reputation damage, and loss of customers
- Remediation including incident response and recovery, public relations, breach notifications, and credit monitoring services for those affected

Cyber-criminals collected $209 million in the first three months of 2016 by using ransomware to extort money from businesses and institutions.

How Ransomware Infects Your System

Ransomware is typically delivered through:

- **Exploit Kits** — Software that's designed to run on web servers that locates vulnerabilities in machines communicating with it.
- **Waterhole Attacks** — Where websites that you visit often are infected with malware.
- **Malvertising** — Malicious online advertising that spreads malware.
- **Email Phishing** — Where cybercriminals try to trick you into giving out personal or business information such as bank account numbers, passwords and credit card numbers.

Once your system is infected, ransomware identifies files and data to encrypt. After your files have been encrypted, you'll receive a notification with instructions on how to pay the ransom.

Ransomware can infect your computers and network devices, as well as your Android phones, laptops and other wireless devices.

Why You Should Never Pay a Ransom

Many believe that the quickest and easiest way to deal with ransomware is to pay the ransom. However, there are many reasons why you shouldn't:

- There's no guarantee that you'll get access to your files.
- If the encryption key doesn't work you can't just call someone for assistance.
- The perpetrator may have installed other malware that triggers future cyberattacks against your business.
- A copy of your files may have been sold to criminals on the dark web.
- Paying a ransom doesn't remediate security breaches that occurred against your business as a result of the attack.
- When you pay a ransom, it funds and perpetuates future ransomware attacks.

According to the FBI: ***"Some individuals or organizations are never provided with decryption keys after paying a ransom. Paying a ransom emboldens the adversary to target other victims for profit, and could provide incentive for other criminals to engage in similar illicit activities for financial gain."***

L5 Consulting Provides Your Best Defense
Against Ransomware

Zero-day attacks that exploit unknown computer security vulnerabilities on your network are the most threat to your business today. Because ransomware is always evolving, you can't rely on just one solution for defense. You may think that deploying multiple, standalone security products is enough. It's not. Too many standalone security products don't provide the complete visibility that's needed across your entire network.

Plus, there's no integration with standalone products. Security is about managing risk through layers. Many cloud-based services (such as Salesforce.com and Office 365) can be conveniently accessed without a VPN connection, leaving them with only basic security. Your best defense demands sophisticated, automated solutions that prevent attacks early in the cycle, and block Internet connections to malicious sites.

L5 Consulting prevents ransomware attacks by first detecting them, and then containing potential damage before it infects your entire system. We provide a layered, automated, and all-inclusive approach of defense that covers your entire enterprise, and extends well beyond the network perimeter. Our security solution is pervasive throughout your organization's entire computing environment, including:

- Your Network
- Data Center
- Endpoints and Mobile Devices
- The Cloud

Additionally, to prevent damage from a ransomware attack we'll continually maintain backups of your data, both in-house and on the Cloud. (Some cloud systems don't back up data. L5 Consulting is always your best advisor where this is concerned.)

L5 Consulting will implement the most current, sophisticated and automated security solutions that keep pace with threats that can spread throughout your entire network within minutes or seconds.

Our solutions reduce complexities that improve your overall security, including errors that hide breach indicators on your network and other devices. With cloud-based, real-time intelligence L5 Consulting deploys the most up-to-date solutions as quickly as possible when threats appear. Plus, our solutions are automated to stay ahead of threats that could otherwise spread throughout your network within minutes or seconds. Our protection blocks requests to malicious destinations before a connection is even established, as well as threats over ports before they reach your network and endpoints.

You Must Employ Best Practices to Prevent Ransomware Attacks

L5 Consulting will help you implement best practices to prevent attackers from gaining access to your organization's network and systems in the first place. We'll ensure that you:

1. Conduct regular security awareness and training for your employees.

2. Reinforce company policies regarding:
   - Not sharing or revealing user credentials (even with IT and/or security)
   - Strong password use
   - Authentication (so you know who did what and when)

3. Encourage the use of file-sharing programs to exchange documents rather than emailing them, to prevent phishing attacks containing malicious attachments.

4. Consider using non-native document rendering for PDF and Microsoft Office files in the Cloud. (Desktop applications such as Adobe Acrobat Reader and Microsoft Word often contain vulnerabilities that can be exploited.)

5. Instruct employees who don't regularly use macros to never enable them in Microsoft Office documents. Macro-based malware uses sophisticated obfuscation techniques to evade detection.

6. Provide details on incident reporting procedures so that employees feel comfortable reporting security incidents.

7. Implement physical security, and visitor escort policies without which threaten employees' personal safety, as well as information security.

8. Perform ongoing risk assessments to identify security vulnerabilities in your organization, and address any threat exposures.

Unfortunately, despite your best efforts, employees will make mistakes. In this case, we are always here to help. For more information about ransomware and how we can provide your best defense against it, contact L5 Consulting at:

Call (888) 727-1994, ext. 3 or email info@L5Consulting.com