Cisco Ransomware Defense

The rise of ransomware

Ransomware is malicious software, or malware, that encrypts documents, photos, music, and other information on a person's computer. It will not release these files until the user pays a fee – or ransom – to unlock these files and get them back.

Ransomware has quickly become the most profitable type of malware ever seen, on its way to becoming a $1 billion annual market.

It commonly makes its way onto a computer or network through the web or email. On a website, ransomware may infiltrate through infected ads. known as "malvertising," that can deliver malware. Users surf sites with malicious ads that automatically download malware or redirect them to exploit kits. In email, ransomware uses phishing or spam messages to gain a foothold. Users merely have to click a link in a phishing or spam email or open an attachments for ransomware to download and call out to its command-and-control server.

Ransomware can also take control of systems by using exploit kits. Exploit kits are software kits designed to identify software vulnerabilities on end systems. They then upload and run malicious code, such as ransomware, on those vulnerable systems.

Ransomware does not merely target individual users but also attacks entire networks. With more semiautomatic propagation methods, ransomware authors capitalize on opportunities to breach a network and move laterally to control swaths of the network to maximize impact and the probability of receiving payment.

Benefits

- **Reduced risk** of ransomware infections through security that can block threats before they attempt to take root
- **Immediate protection** from ransomware that allows you to stay focused on running your business
- **Layered, integrated defenses** that give you unmatched visibility and responsiveness from the network to the endpoint
- **Dynamic segmentation** to keep ransomware cornered on the network
- **Industry-leading intelligence** delivered by the Cisco Talos Security Intelligence and Research Group

“We have covered a great risk in the web attack vector of ransomware and greatly improved our user experience in regards to Internet connectivity.”

– Octapharma

Next steps

Keep your business focused on what it does best by contacting your Cisco sales representative for more information on Cisco Ransomware Defense. Visit our webpage at: https://www.cisco.com/go/ransomware.

How to reduce the risk of ransomware

Given that ransomware can penetrate organizations in multiple ways, reducing the risk of ransomware infections requires a portfolio-based approach, rather than a single product. Ransomware must be prevented where possible, detected if it gains access to systems, and contained to limit damage.

Cisco® Ransomware Defense calls on the Cisco security architecture to protect businesses, using defenses that span from networks to the DNS layer to email to the endpoint. It is backed by industry-leading Talos threat research that shares threat information across all products to reduce time to prevent, detect, and contain automatically.

The solution comprises the following components:

- **Cisco Umbrella**, which protects devices on and off the corporate network and shares information with endpoint and email security products. It blocks network requests before a device can even connect to malicious sites hosting ransomware.
- **Cisco Advanced Malware Protection (AMP) for Endpoints**, which blocks ransomware files from opening on endpoints and shares information with web and email security products.
- **Cisco Email Security with AMP**, which blocks spam and phishing emails along with malicious email attachments and URLs, and shares information with web and endpoint security products.
- **Cisco Security Services**, which provide immediate triage in the case of incident response. They also streamline deployments and help ensure the solution is configured correctly for your environment.

Cisco products are designed to work together

The ultimate advantage that Cisco Ransomware Defense brings to customers is the ability to share threat intelligence across all products, regardless of the threat vector that they are protecting. At the heart of this unified architecture is Talos, that brokers the exchange of information across products. If a brand new threat is initially seen in an email, information about the threat is shared with web and endpoint products, and vice-versa. This reduces the window of opportunity of new ransomware variants, and prevents the lateral movement of files across a network.

Beyond the three core ransomware defense products, deeper integration with Cisco firewall, policy and access controller, and network visibility monitoring technologies increase visibility, introduce automation, and create a more effective security solution by sharing context, alerts, threats, and policies.

C45-737465-01 12/17