At-a-Glance

Cisco Ransomware Defense

Benefits

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

The Rise of Ransomware

Ransomware is malicious software that encrypts a user's files—documents, photos and music—and holds them "hostage." Attackers demand that the user pay a fee (often in Bitcoin) to decrypt them 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 into a computer or network through the web or email. On a website, ransomware may infiltrate through infected ads that can deliver malware, known as "malvertising." 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 links in phishing or spam emails 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.

In the future, ransomware will not merely target individual users, but also target entire networks. With more semi-automatic propagation methods, ransomware authors will capitalize on opportunities to breach a network and move laterally to control swaths of the network to maximize impact and probability of receiving payment.

Reduce Ransomware Risk with More Effective Security

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 for the ultimate responsiveness against ransomware.

"We have reduced ransomware by over 90%.... We have not had another ransomware event."

Global Medical Manufacturer

The solution comprises the following components:

- **Cisco Umbrella** protects devices on and off the corporate network. It blocks DNS requests before a device can even connect to malicious sites hosting ransomware.
- **Cisco Advanced Malware Protection (AMP) for Endpoints** blocks ransomware files from opening on endpoints.
- **Cisco Email Security with Advanced Malware Protection (AMP)** blocks spam and phishing emails and malicious email attachments and URLs. The technology is the same as that applied on the endpoint, but it's deployed at the email gateway.
- **Cisco Firepower Next-Generation Firewall (NGFW)** with Advanced Malware Protection (AMP) and Cisco Threat Grid sandboxing technology stops threats by containing known and unknown malware and blocking command-and-control callbacks to ransomware hosts.
- **Cisco TrustSec via the Cisco network** to dynamically segment your network, so access to services and applications stays highly secure and ransomware cannot spread laterally.
- **Cisco Security Services** provide immediate triage in the case of incident response. They also streamline deployments of AMP, NGFW, and other solution products.

Next Steps

Keep your business focused on what it does best by contacting your Cisco sales representative for more information on Cisco Ransomware Defense.

C45-737465-00 06/16