概览

优势

- 在威胁尝试植入前进行阻止，从而**降低勒索软件感染的风险**。
- **即时防御**勒索软件，免除后顾之忧，让您专注于业务运营。
- **分层的集成防御**提供出色可视性和响应速度，从 DNS 层、网络到终端全方位保护。
- **动态分段**，使勒索软件远离网络。
- 思科 Talos 安全情报和研究小组提供**业界一流的情报**。

思科勒索软件防御

勒索软件发展

勒索软件是指可加密个人计算机上文档、照片和音乐等信息的恶意软件或恶意代码。用户必须支付费用（或赎金）才能解密并赎回这些文件。

勒索软件已迅速成为目前利润最丰厚的恶意软件类型之一，每年可非法获利 10 亿美元。

它们通常通过 Web 或邮件进入计算机或网络。在网站上，勒索软件可以通过提供恶意软件的受感染广告（称为“恶意广告”）潜入。用户浏览包含恶意广告的站点时，将会自动下载恶意软件或将其重定向到漏洞攻击包。在邮件中，勒索软件使用网络钓鱼或垃圾消息获得立足之地。只要用户点击网络钓鱼或垃圾邮件中的链接或打开附件，勒索软件即可进行下载并控制其命令与控制服务器。

勒索软件还可以使用漏洞攻击包控制系统。漏洞攻击包是用于识别终端系统中软件漏洞的软件套件。然后他们会在这些易受攻击的系统中上传并运行恶意代码，如勒索软件。

未来，勒索软件不会只针对个人用户，还会针对整个网络。勒索软件编写者会更多地采用半自动化的传播方法，抓住一切机会破坏网络并逐步渗透到更广泛的网络中，从而扩大影响并提高获得赎金的可能性。

使用更有效的安全方法降低勒索软件风险

由于勒索软件可以通过多种方式渗透组织，减少勒索软件感染的风险需要基于产品组合的方法，而不是单个产品。必须尽可能预防勒索软件，检测其是否已访问系统并进行控制以限制损害。

思科® 勒索软件防御利用思科安全架构来保护业务，其防御范围从网络扩展到 DNS 层、邮件以及终端。我们的解决方案由业界一流的 Talos 威胁研究提供支持，实现了针对勒索软件的终极响应速度。

“我们解决了勒索软件 Web 攻击媒介中的一个巨大风险，显著提高了用户在网络连接方面的体验。”

Octapharma

此解决方案包括以下组件：

- 无论是否在公司网络内，**思科 Umbrella** 均可保护您的设备。在设备接入托管勒索软件的恶意站点前阻止 DNS 请求。
- **面向终端的思科高级恶意软件防护 (AMP)** 可以阻止勒索软件在终端上打开。
- **配备高级恶意软件防护 (AMP) 的思科邮件安全**可阻止垃圾邮件和网络钓鱼邮件以及恶意邮件附件和 URL。AMP 技术类似于在终端中的应用，但是部署在邮件网关。
- 配备高级恶意软件防护 (AMP) 和 Threat Grid 沙盒技术的**思科 Firepower 下一代防火墙**可阻止已知威胁以及命令与控制回调，同时提供对未知恶意软件和威胁的动态分析。
- **思科 ISE** 通过思科网络对网络进行动态分段，这样一来，对服务和应用的访问即可保持高度安全，勒索软件也无法横向扩散。
- **思科安全服务**可在事件响应中提供即时分类。还可简化 AMP、NGFW 及其他解决方案产品的部署。

后续行动

联系思科销售代表了解有关思科勒索软件防御的更多信息，使您的企业能够专注于最擅长的领域。

C45-737465-00 07/16