http://www.c114.net/security/4355/a983393.html

NetEvents2016 to explore the malware topic， “isolation” will end enterprise dilemma 28/11/16

NetEvents2016探讨恶意软件话题 “隔离”终结企业两难局面

http://www.c114.net (2016/11/28 15:45)

C114讯 11月28日消息（林想）9月21日至23日，NetEvents2016全球媒体与分析师峰会在美国加利福尼亚州的萨拉托加举行，汇集了全球各地IT行业100多位的IT厂商管理人员、服务提供商、行业前瞻专家、风险投资家、媒体等代表，就恶意软件话题进行了探讨，与会专家一致认为，“隔离”将终结企业两难局面。

毫无疑问，对消费者、员工和企业而言，勒索软件的攻击非常可怕。受害者必须付出可观的代价从勒索攻击中复原。美国有线电视新闻网（CNN）报道，根据美国联邦调查局2016年4月的报告，“通过敲诈企业和机构来解锁计算机服务器，网络犯罪在2016年的前三个月就收获了2.09亿美元。”典型的勒索软件可能要求支付10,000美元或更高的金额；比如好莱坞长老会医疗中心在二月份就支付了超过17,000美元的赎金 。

现场专家一致认为，勒索软件是互联网的一个祸害，不容忽视

有超过5.5亿的恶意软件变种，以及每天成千上万新的恶意软件被发现，传统检测恶意软件的方法在时间上，在人才上，并在人员配备上，以及在购买和维护安全产品的成本上有许多隐性成本。 隔离，不需安装任何软件在最终用户的台式机、笔记本，或移动设备上 ，不仅节省IT的时间和金钱，而且还消除了关于更新最终用户软件的担忧。

近年来出现的勒索软件、僵尸网络军团等网络威胁。现场网络安全专家断言，勒索软件是互联网的一个祸害，不容忽视。

经过探讨，专家一致认为隔离技术成为防范恶意软件攻击的最好方法。“隔离技术，就其性质而言，是不打开终端用户台式机、笔记本，或移动设备上的网站，而是打开基于云的平台上的安全虚拟容器内的网站。最终用户是通过能呈现与直接访问无分别的用户体验的技术来与网站互动。借由执行远离端点的会话，并且只提供安全呈现的信息给设备，用户就避免了恶意软件和恶意活动的攻击。”

恶意软件没有到达端点的路径，而合法的内容不需因安全的利益而被阻止。管理者可以开放更多的互联网给他们的用户，同时消除了攻击的风险。可以说，“隔离”终结了他们昂贵的两难局面：

· 风险：没有活跃的web内容到达端点，从而未分类的网站存在零风险。

· 消毒感染机器的成本：隔离消除了网站成为恶意软件威胁的载体，大大减少了需重新映像的机器的数量。降低了为每个浏览器和插件漏洞制作修补机的紧迫性。

· SOC成本：隔离会在传统解决方案检测到威胁之前就阻止了威胁，消除了错误或不准确的恶意软件警报。

· SOC周转：警报疲劳与SOC员工流失一起都被最小化。

· 故障派工单数目：员工生产力更高，且现在可以自由安全地探索网络而不需提交重新分类请求。

· 重新分类专家：通过消除重新分类的请求，需要昂贵专家的需求被消除。

有超过5.5亿的恶意软件变种，以及每天成千上万新的恶意软件被发现，传统检测恶意软件的方法在时间上，在人才上，并在人员配备上，以及在购买和维护安全产品的成本上有许多隐性成本。 隔离，不需安装任何软件在最终用户的台式机、笔记本，或移动设备上，不仅节省IT的时间和金钱，而且还消除了关于更新最终用户软件的担忧。 C114