如何应对加密勒索软件的威胁

2016年12月27日

序号	问题	回答
1	如果已经被勒索方加密数据，有办法解开么？还是只能交出1比特币了？	要想对加密文件进行解密是很困难的，最有效的方式是通过之前的备份进行恢复。此外，对于某些类型的勒索软件，如TeslaCrypt类型，思科提供了一个解密程序，可以尝试使用一下，但是不能保证可以成功。下载地址：http://www.talosintelligence.com/teslacrypt_tool/
2	桌面文件加密，解锁需要付钱吗？	要想对加密文件进行解密是很困难的，最有效的方式是通过之前的备份进行恢复。此外，对于某些类型的勒索软件，如TeslaCrypt类型，思科提供了一个解密程序，可以尝试使用一下，但是不能保证成功。下载地址：http://www.talosintelligence.com/teslacrypt_tool/
3	有几台服务器及工作站文件被加密，但是没有发现任何提示信息，如何判断源头？	恶意代码的轨迹跟踪，需要已经部署了类似思科NGFW或NGIPS的安全设备，这样才能够做到在恶意软件进入企业网络时，进行跟踪和拦截。
4	nomoreransom網站上所提供的工具，能否解除所有的勒索軟件? 或是理解為被動防禦的手段之一?	要想通过工具去实现所有的勒索软件的解密，应该是不可能的。
5	是否有安装防毒软体就可避免这种问题？	防病毒软件能够部分解决终端的风险，但是不能彻底解决问题。
6	什么是DNS Security，对应的产品？	这里提到的DNS Security，主要对应的是OpenDNS服务，简单的说，就是通过DNS过程中，判断要解析的域名和地址是否可信，这是一种Service as a Security的安全解决方案。
7	请问，web security或email security怎么检测出勒索软件？有什么显著特征吗？ 还是靠经验库？	通过Email Security，利用到了几个方面的技术，包括Sender Reputation, Outbreak Filtering, 和AMP，依靠特征库的拦截效果非常有限。关于详细介绍，请参考：http://www.cisco.com/c/m/zh_cn/offers/sc00/security-ransomware-whitepapers/index.html

8	恶意软件夹带的附件档案，档案类型会是安装档.exe，还是会伪装成文件档案.doc	各种类型可能有。
9	AMP是什么？	Advanced Malware Protection
10	cisco的解决方案是软件的吗？	思科提供的安全解决方案是基于架构式，覆盖了从边界，内网到终端的解决方案。
11	特别关注已经中了病毒，但是没有安装思科的产品，这个时候怎么解决？还有没有办法挽救？	具体需要确定是中了什么病毒，最好还是通过备份恢复来解决。
12	是否可以这样理解，思科提供的解决方案为更全面的防毒？	不能这样理解。关于详细介绍，请访问：http://www.cisco.com/c/m/zh_cn/offers/sc00/security-ransomware-whitepapers/index.html
13	如何让邮件服务器防止病毒攻击了	我理解您提到的是如何防御病毒邮件，如果是这样的话，我们建议您部署思科ESA邮件安全网关来实现病毒邮件的防御。
14	请问，我们公司使用的是Office365云邮件系统，那么ASA NGFW/NGIPS 能够拦截威胁吗？如果可以，采用什么样的部署形式？	在使用Office365的情况下，也可以考虑部署ESA来实现邮件中恶意代码的拦截。
15	S系列设备可以搭载今天提及的防护措施吗？	是的，思科WSA已经集成了AMP恶意代码防护。
16	Threat Quarantined 什么意思？如何做到quarantination?	我理解您提到的应该是Cisco Rapid Threat Containment。关于这方面的详细的介绍，请参考：http://www.cisco.com/c/en/us/solutions/enterprise-networks/rapid-threat-containment/index.html
17	20頁提到的ESA方案，是否與cellpoint功能相同?另外自動更新功能，需要購買MA才能繼續嗎?	思科ESA是思科的邮件安全网关产品，详细信息请参考：http://www.cisco.com/c/en/us/products/security/email-security-appliance/index.html

18	这些功能是不是ASA 55xx-X自动提供的？	ASA5500-X是思科的NGFW产品，能够提供NGFW的全部功能。
19	基于终端的AMP能否检测到终端本身、或网络的攻击	关于AMP的详细介绍，请参考：http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html
20	对整个局域网有没有能检测到某个终端或交换机出现攻击包的应用软件	通过思科Stealthwatch解决方案，利用网络设备提供的Netflow对所有的内网行为进行记录、分析和告警，对于异常行为还可以进行修复和隔离，详细信息请参考：
21	企业如果需要思科的解决方案，是购买一个呢，还是一套？	要根据企业的实际情况进行选择。
22	AMP防火墙、TALOS是旁路接入吗	关于AMP的详细介绍，请参考：http://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html 关于TALOS的详细介绍，请访问：http://www.talosintelligence.com/
23	请问思科安全设计指南在哪里下载？	请通过下面链接下载：https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=0ahUKEwjutqfew6XRAhVJNI8KHbXLDacQFghBMAM&url=http%3A%2F%2Fwww.cisco.com%2Fc%2Fdam%2Fen%2Fus%2Fsolutions%2Fcollateral%2Fenterprise%2Fdesign-zone-security%2Fransomware-defense-dig.pdf&usg=AFQjCNFmUht_TFXmqcgmTflariaA10-HOg
24	针对SDN控制器的攻击防护与传统服务器对攻击的防护措施一样吗？有什么区别？ 谢谢！	这个要看一下具体的应用场景，从本质上来说都属于安全防护的范畴，具体的防护措施要结合实际场景。
25	是否可以这样说，若员工没有安全意识，则使用任何解决方案都无法保护资讯安全？	应该说要想实现真正的安全，人员、流程和技术三者缺一不可。
26	请问，amp是不是有客户端软件？	AMP支持网络部署，也支持终端部署，详细信息请参考：http://www.cisco.com/c/zh_cn/products/security/fireamp-endpoints/index.html

27	思科的ESA 是指ironport设备吗	是的。
28	我们公司主要是移动用户被感染勒索病毒 我害怕这个病毒在公司内部传播 请问目前这个病毒应该无法内部传播吧？	从演化趋势上来看，未来的勒索软件有可能会议蠕虫传播的方式进行传播，因此存在这种风险的。
29	2017年的Ransomware預測將會流行哪些?	根据一些研究显示，在2017年勒索软件有可能会议蠕虫传播的方式进行传播，因此危害可能会更大。
30	是否有技術防止檔案被加密?	从整个信息安全的范围来看，有一些终端的安全方案能够防止文档被加密，事实上完全依赖终端也不够完整，也需要一整套的安全解决方案。
31	Cisco的FireAMP能检测到勒索软件的运行吗?	部署在终端的AMP程序能够利用回溯跟踪的方式，检测到已经发行的恶意软件，并给出其传播的轨迹。
32	业界现在有不少产品都针对这类威胁，机制都雷同，思科的产品相对其它业界产品（如checkpoint，Symantec等)有什么突出优势？	思科的安全解决方案，涵盖了从边界、终端以及内网异常行为的各个层面，并且安全设备之间能够进行协作和联动，这是与其他基于单点的安全的最大的区别。
33	哪些云供应商应用了思考的这套防护产品？	思科的安全解决方案包含了边界、终端和内网等多个产品组件，对于用户来说，有的部署了全部，有的根据需要部署了相关的产品。
34	OpenDNS是，思科DNS安全产品？	这里提到的DNS Security，主要对应的是OpenDNS服务，简单的说，就是通过DNS过程中，判断要解析的域名和地址是否可信，这是一种Service as a Security的安全解决方案。
35	有關esa 的功能是一個怎麼樣的機制? 有相關的技術資料?	关于ESA的产品资料，请访问：http://www.cisco.com/c/en/us/products/security/email-security-appliance/index.html
36	如何选择，NGFW、NGIPS？	这是一个比较大的话题，要结合您的实际情况来进行分析，下面有一个详细的介绍，供您参考：http://www.cisco.com/c/zh_cn/products/security/firewalls/index.html

37	如果代码文件基于密码有保护，如何知道是否属于该类恶意代码？	关于如何检测Malware的原理，请参考：http://www.cisco.com/c/zh_cn/products/security/advanced-malware-protection/index.html
38	怎么解决办公网内安装的一些软件自动向外发送信息？	一方面需要适当的准入控制策略，另一方面需要在边界、终端以及内网部署有效的产品和方案，从而最大限度的发现异常流量的行为。
39	APT活動可以被百分之百制止及防護?	事实上任何安全解决方案都无法做到100%的安全防护，部署了安全解决方案，带来的价值是增大攻击者入侵的难度，降低被入侵和感染的机会。
40	关于netflow,如果基于一个混合网路（非完全思科交换），如何基于交换层进行数据收集，并进行机器学习和大数据分析？	思科Stealthwatch对网络行为的记录、分析和告警，不仅仅基于Netflow，此外也支持其他的Flow格式，同时也可以通过FlowSensor设备，对无法生成Flow记录的流量，转换为Netflow的格式。
41	现在很多勒索软件会针对一些软件。比如数据库勒索内容被加密后，你们有方案拦截吗？	思科针对勒索软件的防御，专门给出了一份设计指南，详细介绍，请访问：http://www.cisco.com/c/m/zh_cn/offers/sc00/security-ransomware-whitepapers/index.html
42	AMP客户端只支持Windows？	AMP在终端部署，除了Windows还支持MacOS，Apple iOS等，详细内容请访问：http://www.cisco.com/c/zh_cn/products/security/fireamp-endpoints/index.html
43	请问思科现在安全产品哪些是可以在国内买到的，和国外版本有什么功能区别吗？	没有。
44	如果感染后，切断感染的客户端与服务器主机连接，是不是解决方法？	不一定能够有效，这也要看是哪种类型的勒索软件。