In the Boxing Ring
JUN 2023

Network Box 技术新闻

Mark Webb-Johnson
CTO, Network Box

欢迎阅读 2023 年 6 月份的 In the **Boxing Ring**

这个月，我们很高兴地宣布Network Box 管理的零信任终端安全解决方案现已向客户提供，并已在全球发布。为了配合发布，我们认为说明一些部署案例可能会有帮助。因此，在第2至3页、 我们介绍了三个案例研究，展示了不同的部署方法。

在其他新闻中，Network Box区域办事处参加了各种活动、研讨会和讲座。Network Box德国分公司参加了ComTeam路演活动，Network Box美国分公司参加了渠道合作伙伴会议，Network Box香港分公司则举办了网络安全研讨会。而在这个月的全球安全头条新闻中，ChatGPT、微软Azure、思科、WordPress、丰田、铃木和Barracuda Networks都出现了安全问题。

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
June 2023

本月摘要

托管式零信任终端安全系统

随着Network Box管理的零信任终端安全解决方案在全球发布，我们认为展示一些部署案例可能会有帮助。这个月，我们将介绍三个案例，说明白名单技术的不同部署方法。

案例1--被动型

这里的用户有一个由大约50台工作站、笔记本电脑和服务器组成的网络。所有这些都运行着传统的防病毒技术。一位销售人员在出差时把他的笔记本电脑带出办公室，感染了一些木马恶意软件。回到办公室后，远程黑客下载并执行了一个勒索软件程序--加密了他的笔记本电脑和几个网络共享的文件。网络管理员已经断开了连接并隔离了他们所能隔离的，但他们担心由于木马程序的存在，黑客可以远程访问网络进行横向传播。若所有的东西都关闭，取证成像，并逐一清理，估计需要7到10天的时间，以及相关的业务影响成本。

与Network Box SOC合作，采取了以下行动：

- 所有疑似被感染的机器都被下线并重启到安全模式。从USB安装零信任端点安全，机器重启后进入基于组的应用控制策略，只允许运行一组非常有限的预先信任的应用程序（主要是微软和一些关键的商业应用程序）。在这之后，这些机器被安全地重新上线，像正常一样使用，并提取关键数据。

- 一个Network Box设备被放置在互联网边界，以取代之前的简单防火墙（零出站策略），并制定有效的策略规则来控制入站和出站流量。受感染的局域网、IDS和IPS引擎被启用，以监测和控制出站流量

随着黑客被锁定在网络之外，受感染的机器重新受到控制，业务影响被限制，被勒索软件加密的文件可以从备份中恢复过来。

案例2--谨慎型

在这里，我们有一个由几百台工作站、笔记本电脑和服务器组成的大型网络。传统的防病毒技术在这些机器上运行，网络在外围由Network Box保护。业主和管理员担心终端用户会犯错误，点击他们不应该点击的东西--可能会导致整个网络瘫痪。

我们确定关键的高风险工作站和服务器，包括:

- 运行网络、电子邮件和协作软件的可访问互联网的服务器
- 会计工作站
- 关键决策者工作站（包括高层管理人员、财务主管等）。
- 办公室外的手提电脑

零信任终端安全系统Security被部署到所有这些高风险的机器上，并以监控模式运行两周。在此期间，Network Box的SOC人员会监控正在运行的应用程序，并在必要时将其列入白名单。一些潛在的不需要的應用程式會被發現，Network Box SOC的工作人員會與管理人員逐一解決這些問題。在两个星期结束时，未被识别的应用程序的警报数量下降到零，机器被转移到执行模式（阻止不受信任的应用程序的执行）。

这里的方法并不完美，对于没有受到零信任保护的端点所访问的网络共享需要特别注意（因为这些端点上的勒索软件感染可能会加密网络共享上的文件）。安全性不可能是100%的，在便利性、成本和安全性之间总是有一个平衡点；这种基于风险的方法试图解决这种平衡。

案例3 - 准备型

这是一个相对较小的网络。一家金融服务公司，有少数高薪员工提供咨询服务。主要决策者担心勒索软件攻击或网络入侵会泄露敏感的客户数据（特别是考虑到大多数员工使用的笔记本电脑在办公室网络保护之外的时间）。

零信任终端安全系统被部署在所有工作站、笔记本电脑和网络服务器上，并处于监控模式。在两到三周的时间里，Network Box SOC的工作人员会监控正在运行的应用程序，必要时将其列入白名单，直到这些机器可以被转移到强制模式（阻止所有不受信任的应用程序的执行）。

在部署和随后的几个月里，一些不需要的和有潜在危险的应用程序被阻止在网络上运行。Network Box SOC的工作人员提醒办公室经理对最终用户进行跟踪。关键决策者对他们可以获得的报告印象深刻，这些报告显示了哪些应用程序是由哪些用户在什么时间运行的。

结论

从黑名单（反病毒）到白名单（零信任）的方法需要转变思维方式。每种方法都有其优势和劣势，最好的总结是：

白名单与黑名单的利与弊

指标	白名单	黑名单
对已知恶意软件的有效性	100%	接近100%
对新出现的恶意软件的有效性	100%	或许90%至95%
误报	更新，以及新的安装	很少
名单维护	管理员或SOC管理	供应商
阻断行动	在执行时	下载/扫描时
使用应用程序的可视性	全面报告	通常没有
应用程序使用的政策控制	完全控制	通常没有

你可以看到，白名单方法的最大缺点是，它需要最终用户/管理员维护白名单。同时，最重要的区别（除了反恶意软件的有效性）是改进报告和控制哪些应用程序被允许在网络上运行。通过简单地不信任（或添加到白名单）未经授权的（而不是恶意的）应用程序，可以实施有效的政策控制。白名单让终端用户完全控制和报告哪些应用程序在他们的终端设备上实际运行。

Network Box的方法解决了終端用戶維護白名單的管理負擔問題，把這個功能轉移給Network Box的SOC工程師和我們的管理服務。我们提供自管理，SOC管理，以及混合组合。换句话说，我们提供所有零信任的优点，而没有任何缺点。

Network Box HIGHLIGHTS

Network Box全球 活动、研讨会和讨论会

对于Network Box的区域办事处来说，这是一个繁忙的月份。Network Box德国分公司参加了在汉堡、盖尔森基兴和达姆施塔特举行的各种ComTeam路演活动。美国Network Box参加了在拉斯维加斯举行的渠道合作伙伴会议。而Network Box香港举办了一个网络安全研讨会，讨论Network Box的服务产品： 云SIEM+，移动SIEM+，云UTM+，持续安全扫描，渗透测试，以及Network Box的24x7x365 SOC管理。



月刊主办	联系方式
Mark Webb-Johnson 主编	Network Box CNNOC cnnoc@network-box.cn
Michael Gazeley **Kevin Hla** 产品支持	或者上门到: 深圳市福田区深南大道 竹子林求是大厦西座920
Network Box HQ **Network Box USA** 贡献者	+86 (755) 3336 1581 www.network-box.cn

全球 安全头条

安全情报
ChatGPT发生数据泄露事件，引发安全担忧
LINK: https://bit.ly/3qlpGgs

Dark Reading
微软修补了严重的Azure云安全漏洞
LINK: https://bit.ly/43eWR3R

Bleeping Computer
思科警告说，关键的交换机漏洞已被公开利用
LINK: https://bit.ly/43DgS3E

黑客新闻
流行的WordPress插件的新漏洞使超过200万个网站受到网络攻击
LINK: https://bit.ly/3oGe07v

Dark Reading
丰田披露长达十年的数据泄漏，暴露了215万客户的数据
LINK: https://bit.ly/43f11Zx

BitDefender
铃木摩托车厂因网络攻击而停工
LINK: https://bit.ly/3qfivWV

The Hacker News
黑客利用Barracuda电子邮件安全网关的零日缺陷达7个月之久
LINK: https://bit.ly/43zp0SN