勒索软件漏洞与文件传输

ipswitch

最新的勒索软件安全威胁

网络攻击每天层出不穷，似乎永无宁日。不久前，美国有五十间银行感染了 Trickbots Trojan 木马程序。在 2016 年，网络罪犯光凭一组二手路由器，就从孟加拉国银行盗走了 81,000,000 美元。欧洲最近发生的 Wannacry 攻击事件让许多医院不得不替患者安排转院，只因为他们根本无法调阅患者的病历。

在现今的网络安全环境中，IT 团队及安全性团队不能不了解网络罪犯所利用的攻击向量，以及他们会钻的漏洞。文件传输基础架构是特别需要提高警觉的地方。

新的攻击向量

Symantec 发表的 2016 年网络安全威胁报告 (Internet Security Threat Report) 强调了网络安全方面的几项重要趋势。盗用资料仍然是一大隐忧，然而报告更指出勒索软件已经急起直追了。

变化多端的攻击向量

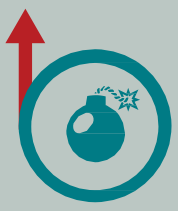
Symantec 发表的 2016 年网络安全威胁报告 (Internet Security Threat Report) 强调了网络安全方面的几项重要趋势。盗用资料仍然是一大隐忧，然而报告更指出勒索软件已经急起直追了。

NotPetya 是一场非常高调的破坏攻击行动，受害对象是 Federal Express 和 Nuance。两个受害对象均表示发生收益减少情形，原因在于对客户提供的服务发生中断。

美国财政部通货监理署 (Office of the Comptroller of the Currency, OCC) 的 2016 年半年度风险前瞻报告 (2016 Semiannual Risk Perspective) 也证实了 Symantec 的结果。关于网络安全风险，该单位特别强调“网络钓鱼仍然是入侵数据系统的主要手法... 是从事其他恶意活动的主要入侵机制。”

他们对银行发出的警告指出：“勒索活动盛行，导致数量和复杂度均有提高”，以及“攻击活动一旦得手，将会瘫痪银行的业务运作，并干扰提供服务的能力。”他们向各组织提出以下忠告：“银行若采用没有套用修补程序或不受支持的软件及硬件，就容易发生遗失数据或客户数据外泄等问题。健全的系统开发生命周期...是防范漏洞不可或缺的一环。”

勒索软件

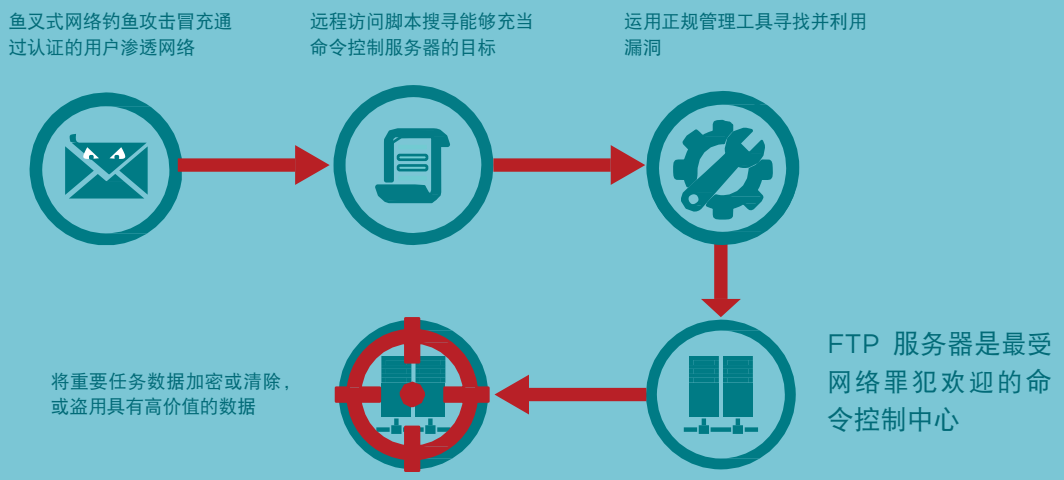


破坏行动

鱼叉式网络钓鱼

攻击手法面面观

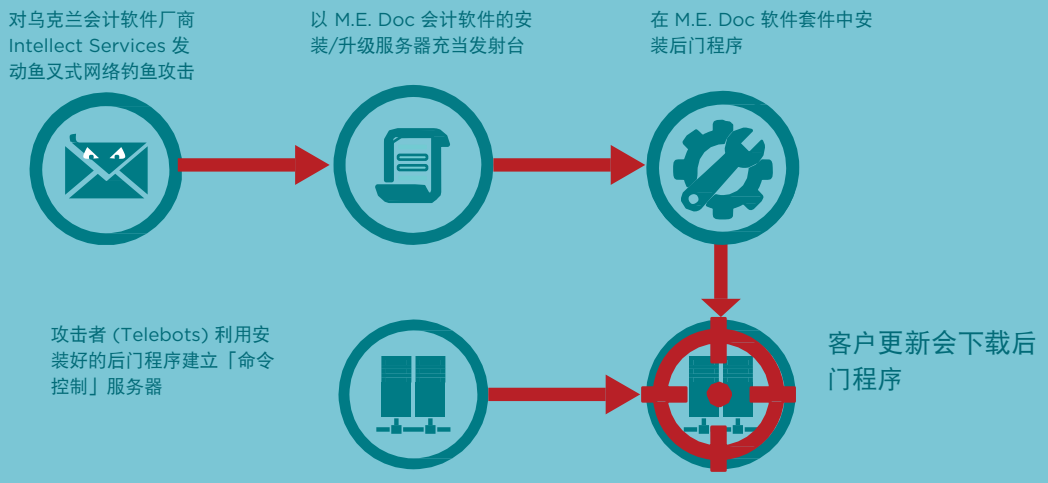
典型的攻击会分阶段进行。首先，攻击者的目标是破解防火墙并清除所有 IDP/IPS，然后冒充通过认证的用户存取使用网络。接下来的目标则是找到有漏洞的装置并夺取控制权，从而利用这一装置充当命令控制平台。最后，攻击者会设法将恶意酬载传递到网络上的重要资产中。



NotPetya 攻击

近期破坏力最强的攻击向量包括 **NotPetya**。NotPetya 源自俄国的 Telebots 团队，第一个下手对象是乌克兰的企业。之后，破坏范围逐渐延伸到美国。NotPetya 一开始是锁定 Intellect Services 为鱼叉式网络钓鱼的攻击目标，这家公司是 M.E.Doc 会计软件的乌克兰厂商。顺利入侵后，Telebots 就控制了 M.E.Doc 的升级服务器。该公司的升级服务器采用过时的 Open SSH、Web 及 FTP 服务器版本，有许多漏洞，因此成为容易下手的对象。Telebots 在 M.E. Doc 安装与升级套件的某个 .dll 档案中安装了一个后门程序。

客户只要下载了这个套件，就会安装这个后门程序。Telebots 还在 M.E. Doc 的服务器上安装了命令控制软件，以利将 NotPetya 推送到感染了后门程序的计算机中。



鱼叉式网络钓鱼

鱼叉式网络钓鱼是指假冒看似可信的个人身分寄送电子邮件，企图让内部人员信以为真而透露重要信息。其概念是诱使目标用户开启含恶意软件的电子邮件附件或网页链接。能够夺取用户装置控制权的脚本加载远程访问软件就是其中一例。

这是网络罪犯最常利用的入侵武器，近期也有几间世界数一数二的大型银行成为此类猖狂犯罪行径的受害者。

黑客可以透过黑暗的网络取得如 NECURS 之类的垃圾邮件工具，每天都能发出无数封电子邮件。这也大幅提高了他们找到不知情或未经训练的内部使用者并诱使其落入陷阱的机率。

鱼叉式网络钓鱼让网络罪犯得以破解防火墙，还能冒充通过认证的用户存取使用网络。这是其他恶意活动的前兆。

鱼叉式网络钓鱼

搜寻“发射台”

进入网络后，网络罪犯会开始扫描锁定不安全的装置，再以找到的装置充当用于攻击高价值目标的“发射台”。许多工具都可以帮助网络罪犯达到这一目的，而安全性团队却不见得能对这类工具提高警觉。

夺取操作系统的控制权后，网络罪犯会利用正规的管理与入侵测试工具周游网络。找到重要的业务系统后，黑客会传递恶意酬载，用于窃取数据和/或干扰业务运作。

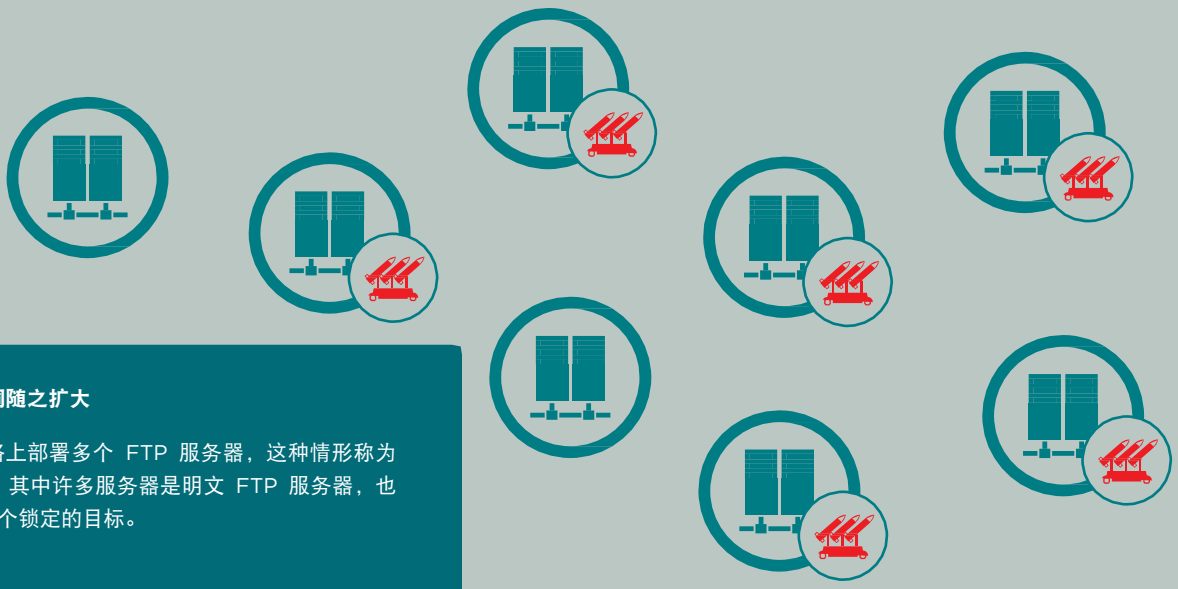
密码哈希的防御能力不高。就算没有拿到高等数学博士文凭，您也有能力破解加密密码。只要在 Google 搜寻并下载 Cain and Abel 或 John the Ripper 之类的暴力破解程序，短短 2、3 小时就能轻松破解 Windows 密码。密码哈希一旦遭到破解，多阶段验证会是成效卓著的反制措施。

建立命令控制

“命令控制”FTP 服务器

在经验丰富的黑客眼中，安全防御措施不够完善的文件传输服务器是很容易得手的目标。设定开放匿名存取功能、使用电子邮件作为登入名称，并以“password”作为密码的服务器，往往是第一个遭到锁定而且也是最容易得手的目标。匿名 FTP 服务器的隔离措施若不够完善，重要资产很容易就会经由网络外泄。

FTP 通讯协议若未加上 SSH 或 SSL 等安全机制，就会传送未加密的数据。这些服务器通常也是管理不当的服务器，其中保存了大量容易存取及使用的信息，这些信息可能十分重要，也可能助长此类攻击活动。自动化脚本及活动记录往往没有受到保护。黑客会利用这一缺陷修改记录文件，以利掩饰自己的行踪。



FTP 扩张让漏洞随之扩大

IT 经常会在网络上部署多个 FTP 服务器，这种情形称为“FTP 扩张”。其中许多服务器是明文 FTP 服务器，也是网络罪犯第一个锁定的目标。

IT 经常会在网络上部署多个 FTP 服务器，这种情形称为“FTP 扩张”。这类 FTP 多采用匿名模式，透过明文 FTP 服务器传送和储存档案，或者必须采用脚本；通常会是网络罪犯首先锁定的目标。

美国联邦调查局 FBI 在今年稍早之时公布了一则警讯 (FBI PIN 170322-001)，内容指出黑客会锁定采用匿名模式的明文 FTP 服务器并以此发动网络攻击。现在许多企业安全性团队、风险管理团队、法遵团队以及 IT 团队纷纷开始主动移除其环境中的明文及匿名 FTP 服务器。

勒索软件

建立命令控制服务器后，网络罪犯就能锁定可以让其顺利得逞的资产。

去年勒索软件攻击事件层出不穷。其攻击战略是找到重要资产并让人们无法使用这类资产。网络罪犯利用加密操作系统或数据文件、变更重要业务系统密码等手法瘫痪业务运作，不但造成巨大的损失，也暴露了法规方面可能出现的漏洞。Petya 就是勒索软件攻击的一个例子，这次的攻击将档案加密，然后提醒使用者必须以比特币 (bitcoin) 支付赎金才能收到密钥。组织急于让业务恢复正常运作，因此往往会在一两天内付清赎金。

破坏行动

破坏行动同样越来越猖獗。这类行动的目的其实是要破坏遭到攻击的企业，其手段就是摧毁该企业所重视的资料资产。近来，破坏攻击行动运用清除磁盘的方式消除所有数据，并让数据无法复原。由于此类攻击并不能直接让罪犯得到金钱，因此目前有关当局认定破坏行动是有国家在背后撑腰的组织，或是一群俗称“黑客激进分子”(hactivist) 的组织。

防护文件传输环境

要做好文件传输环境防护措施，必须遵循三个非常重要的步骤：合并、防护、管理。

合并文件传输活动

FTP 服务器扩张是相当基本的安全漏洞。这类服务器通常安装于不同的操作系统、执行不同的脚本语言，即使有进行管理，通常也是采用独立管理模式。无论就安全性或管理性而言，都毫无一致性可言。从安全性角度来看，每一台服务器都代表一个攻击向量。即使每一个系统都管理得当，也有完整的活动与存取稽核记录，但由于没有单一稽核记录，仍然是个令稽核人员感到棘手的问题。

防护文件传输环境

最低限度是将所有服务器全数升级为 SFTP 或 FTPS。无论采用 SFTP 或 FTPS，两者皆能加密传输中的数据，也不接受明文密码。额外采用 OpenPGP 还能发挥加密功能，进一步保护服务器目录中的闲置档案。不过，SFTP 不见得具有合并功能。只要无法合并，仍然会出现多个攻击向量，也会提高黑客顺利入侵的风险。

管理文件传输环境

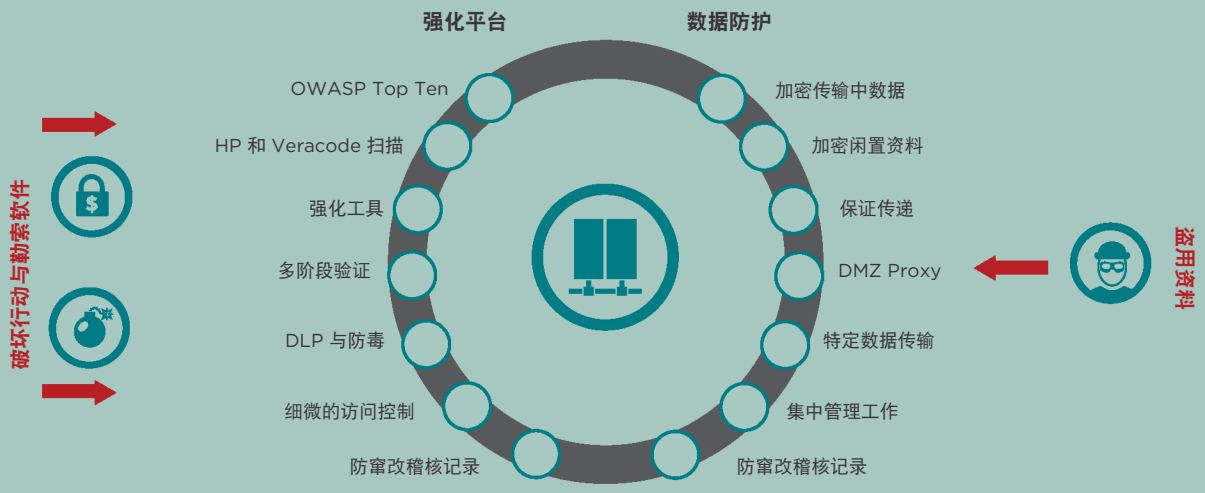
运用合并系统集中管理能够大幅提升采用强式存取及验证控制的能力、能够保护高风险数据及传输中的数据、能够降低以文件传输服务器充当命令控制平台的可能性，而且能够实行更好的档案管理措施。

Ipswitch MOVEit® 安全管理文件传输

MOVEit 不仅符合成本效益，能取代明文 FTP，还能合并您的文件传输基础架构。这款产品能够运用不使用明文 FTP 或 SFTP 软件的强化平台，因此能够妥善抵御「发射台」攻击向量。这是唯一通过 OWASP Top Ten 测试与验证的文件传输解决方案，能够防范最重要的应用程序安全性风险。

每个版本的 MOVEit 均经过 HP 及 Veracode 动态与静态扫描。这些工具运用两种不同的软件测试方法评鉴应用程序的安全性。动态测试采用的是入侵测试，这类测试会检查执行中的应用程序，并确认该程序因应各类输入的方式。静态测试则会审查与稽核应用程序的原始码是否包含任何漏洞。

MOVEit 安装套件包含 SecAuxNET 公用程序之类的平台强化工具。此套件能够为执行 MOVEit 的 Windows Server 平台预做准备，以利在公开使用因特网的网络区段进行部署。SecAuxNet 的功能包括：



参阅运用 MOVEit 防护数据与 IT 基础架构电子书，深入了解 MOVEit 如何合并、防护与集中管理文件传输环境。

关于 Ipswitch

Ipswitch 专注于设计与研发能够跨云端、虚拟及内部环境轻松发挥 24 小时全天候效能与安全性的业内顶尖软件，用户人数超过 100 万，分属 116 个国家的 42,000 间不同的公司，负责管理超过 150,000 个网络。全球 IT 团队均依靠 Ipswitch 25 年的优良创新经验，利用 Ipswitch MOVEit® 安全文件传输、Ipswitch WhatsUp® Gold 网络监控及 Ipswitch WS_FTP®，在各自的岗位上发挥商业交易、应用程序与基础架构的最大效能，并提供出色的安全保障。Ipswitch 的产品组合丰富广泛，可以直接运用，也可透过与一流 IT 厂商建立的策略联盟及 Ipswitch 不断扩大的全球合作伙伴生态系统取得，这些产品组合能够提升应用程序与网络的效能、监控各种 IT 环境，并确保在遵循 PCI、HIPAA、GDPR 和其他产业及政府资料安全与法令规范的前提下保障数据交换的安全。

本公司在美国、欧洲、亚洲及拉丁美洲均设有办事处。如需详细信息，请造访 http://www.ipswitchcn.com/ 或透过 LinkedIn 与 Twitter 保持联络。若要了解 Ipswitch 的策略联盟或全球合作伙伴服务网，请造访 http://ipswitchcn.com/partners/。

ipswitch

如何轻松面对勒索软体安全威胁

下载 Ipswitch MOVEit Transfer 30 天免费试用版 ›