2016 年 4 月 11 日，星期一

勒索软件：过去、现在和未来

“凡是过去，皆为序章。”
- 威廉·莎士比亚，《暴风雨》

引言

去年兴起的勒索软件正成为一个日益严重的问题。企业通常认为支付赎金是取回数据最划算的办法，现实情况也可能正是这样。但是，我们所面临的问题是，每一个企业为了取回其文件而支付的赎金，会直接用于下一代勒索软件的开发。因此，我们看到勒索软件正以惊人的速度不断发展。

在本篇博文中，我们将探讨过去各种高效的自我传播型恶意软件的特点，以及助使恶意软件逐步渗透的工具的发展情况。这些研究非常重要，因为我们预计网络攻击者会开始在勒索软件中使用这些功能，从而使其更富攻击性。在本博文中，我们将重点放在两条思路上：首先，过去出现了很多成功的恶意软件；其次，成功的网络勒索者会根据过去的经验开发出新的和不断进化的威胁软件。

据我们现在的了解，勒索软件的使用者有一种“漫天撒网，守株待兔”的心态；他们会尽可能多、尽可能快地攻击各种目标。通常，他们通过漏洞攻击包或大规模网络钓鱼活动来发送负载。最近出现了大量互无联系的勒索软件活动，明确地以企业作为攻击目标。我们认为这是一种预兆，预示着勒索软件未来的攻击趋势。

过去，数据丢失大多只是恶意软件活动的附带危害（虽然偶有例外）；现在，恶意软件与破坏数据或拒绝访问内容的关联变得前所未有的严峻。大多数攻击者所关注的是持续性地访问数据或者获取系统所提供的资源，以达到他们的目地。勒索软件改变了这一传统模式，从破坏系统转向彻底的勒索；如今，攻击者使用勒索软件拒绝人们访问数据，如果要恢复对数据的访问，则需支付赎金。本文将讨论勒索软件的最新发展趋势以及如何保护您的企业以应对这种威胁。

目录

第 1 章：勒索软件简介

勒索软件是以通过各种手段来拒绝人们访问用户数据作为最终目标的一类恶意软件。这种软件的早期变体会使用各种技术锁定人们对计算机的访问权限或者拒绝人们访问文件（例如修改 ACL 以及禁止访问系统工具、桌面等），而较新的变体则直接使用强加密算法（例如 AES、RSA 等）来加密用户文件。勒索软件专门以用户文件为攻击目标，同时会避免破坏系统文件。其中的原因是，这一方面可以确保用户会收到相关的通知，以告知他们的文件所遭到的攻击，另一方面，用户也能够通过一定的方法支付赎金以取回他们的文件。对文件进行加密后，此类恶意软件通常会自我删除，并留下某种形式的文档。这个文档会指示受害者如何支付赎金，并重新获得对加密文件的访问权限。某些变体还会向受害者设定支付时限，并威胁如果在此时限之前未收到付款，则将删除密钥/解密工具；或者，在其他情况下，则会增加赎金的价格。

勒索软件的发送方式通常包括：漏洞攻击包、水坑式攻击、恶意广告，或者大规模的网络钓鱼活动。一旦发送成功，勒索软件一般通过某种嵌入式文件扩展名列表来识别用户文件和数据。勒索软件还会通过编程，避免影响某些系统目录（例如 Windows 系统目录或某些程序文件目录），以确保负载运行结束后，系统仍然保持稳定，以使客户能够支付赎金。如果某一位置的文件与列表中的某个文件扩展名相符，勒索软件就会对该文件进行加密。否则，就不会攻击该文件。 在文件加密成功后，勒索软件通常会向用户发出通知，说明如何支付赎金[1]。

图 1：Locky 是一种最新的勒索软件变体。这是一份文件扩展名的列表，如果勒索软件找到这些扩展名的文件就会对其进行加密 。

随着勒索软件的发展，勒索软件不断地变得越来越有针对性。为了了解勒索软件的未来趋势，我们认为探究勒索软件和高效自我传播型恶意软件的历史是至关重要的。我们还将研究最近发生的勒索软件事件，从中我们可以看出勒索软件的攻击目标似乎发生了转变，最后，我们将描述我们认为代表勒索软件最有可能的演进路线的一些情境。

第 2 章：勒索软件简史

在有案可查的勒索软件中，最早的实例之一出现在 1989 年。 它就是“PC Cyborg Corporation”编写的 AIDS 木马，这种木马病毒通过软盘进行传播[3]。 在 1996 年，针对当时称之为“密码病毒学”（即出于恶意目的使用密码）的课题，出现了相关的研究文章[4]。 研究人员创造出一种概念验证病毒，它能够使用 RSA 和 TEA 算法对文件进行加密，同时拒绝访问用于加密文件的密钥。 到了 2005 年，各种勒索软件纷至沓来，例如：Krotten、Archiveus、GPCoder 等等[5][6]。 在上面提及的恶意软件系列中，GPCoder 是最令人感兴趣的，因为在众多的勒索软件中，它在加密文件时使用的是 1024 位 RSA 加密，这就使得人们难以通过暴力破解的方法来恢复文件。

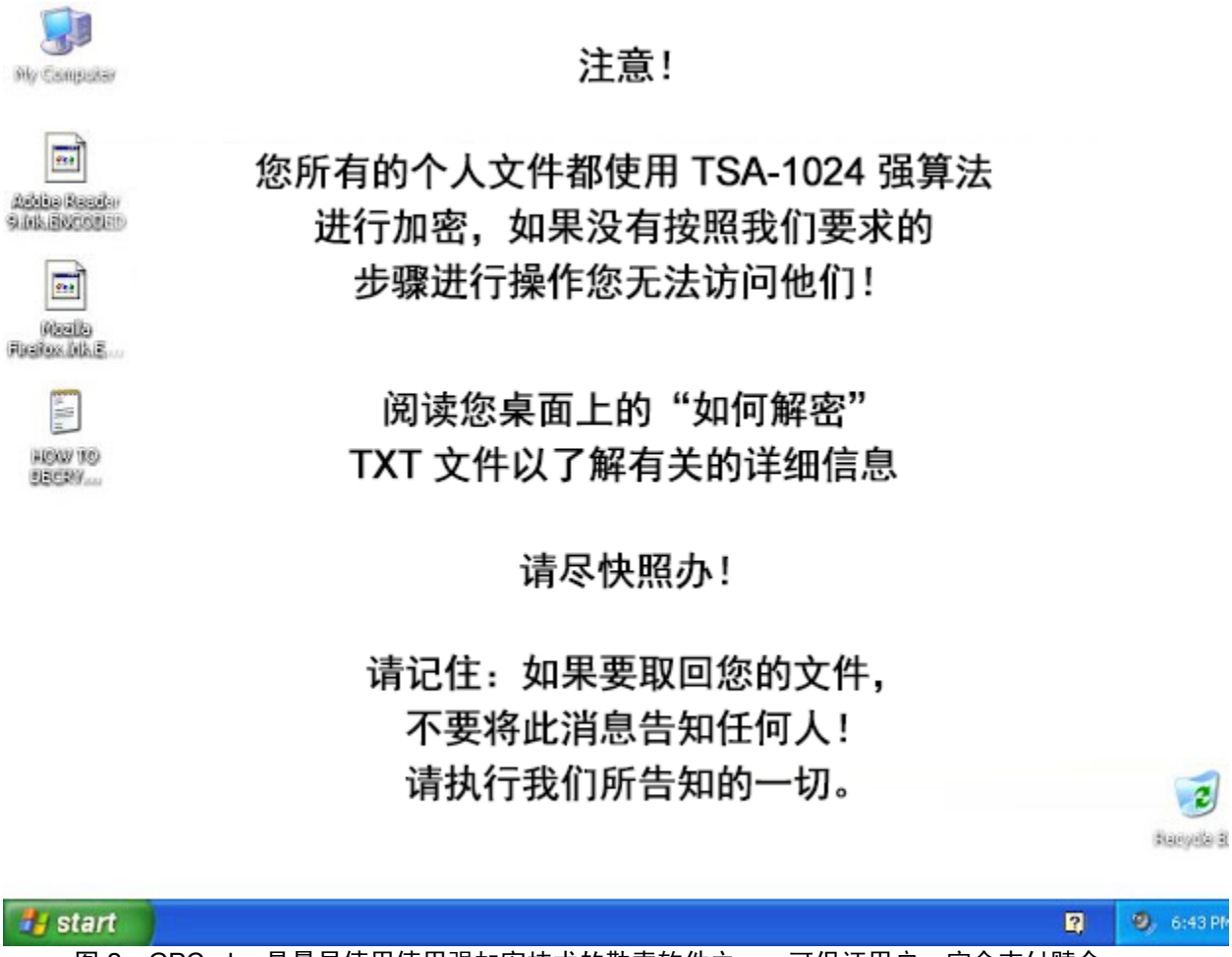


图 2：GPCoder 是最早使用使用强加密技术的勒索软件之一，可保证用户一定会支付赎金 。

在 2012 年，出现了基于 ZeuS 和 CitadelReveton 木马的 Reveton 木马病毒，这是人们发现的第一个大规模部署的勒索软件。此恶意软件会声称其代表各种不同的执法部门（根据目标区域设置）。受害者的系统里会显示一份通知，其声称某个执法部门已经锁定他们的文件，受害者需要缴纳“罚金”才能恢复相关的文件。Reveton 会提示用户购买现金卡或比特币并通过网站提交相关的支付信息，然后才能取回他们的文件。

图 3：Reveton 的诸多锁屏之一。Reveton 会显示出一个伪装成当地执法部门的通知页面，并告知用户使用预付款现金卡 (MoneyPak) 进行支付，或在某些情况下，也可以支付比特币，以解锁他们的系统。有趣的是，Reveton 并不使用加密技术锁定目标系统。

根据 Brian Krebs 撰写的一篇文章，Reveton 的确是一棵摇钱树。 该文章中提到一个数据，仅仅在一个目标国家/地区里，每天通过该勒索软件得到的赎金大约为 44,000 美元[8]。 也就是说，在一个月内即可在一个目标国家/地区获得超过 130 万美元的赎金。勒索软件取得了相当大的“成功”。

受 Reveton 的成功鼓舞，新型勒索软件变体开始涌现。 Cryptolocker[9]。 Torrentlocker[10]。 Cryptowall（及其所有变体）[11]。 Teslacrypt[12]。 Locky[13]。 如今，甚至出现了基于 JavaScript 的勒索软件负载，以及旨在攻击 Linux 和 OSX 用户的变体[14]、[15]、[16]。

第 3 章：勒索软件最新动态

ANGLER EK 为 CRYPTOWALL 推波助澜（ANGLER 分析）

如今，勒索软件仍在对全世界的用户产生威胁；这种威胁持续增长，攻击目标更为庞大，赎金也越来越高。 据我们的内部文章（其中介绍了 Angler 漏洞攻击包如何运行的详情）估计，就 Angler EK 攻击者而言，发送勒索软件负载已经构成了一个年产值达 6000 万美元的行业[17]。 也就是说，平均每月的产值达 500 万美元。请注意，这只是一个漏洞攻击包以及一组攻击者发送一套勒索软件负载所产生的收益。这种丰厚的利润意味着勒索软件将成为网络犯罪者的大买卖。

经发现，一台健康的服务器在一个月的时间段里监控着 147 个代理服务器，并产生超过 3,000,000 美元的收益。经我们观察，大约一半的 Angler 活动是这一个网络攻击者造成的，仅仅从勒索软件感染中每年获得的收益就超过 30,000,000 美元。

图 4：直接从 Talos 的“Angler Exposed”（Angler 分析）研究中摘录的数据。这些统计数据是对单个 Angler 漏洞攻击包操作的统计。

LOCKY：从银行木马病毒转变成勒索软件

正如我们上文中所暗示的，Angler EK 操纵者并不是唯一的勒索软件发送源。最近，出现了一大波来自一种新的勒索软件变体“Locky”的攻击活动。我们提供的数据证明，Locky 是一个攻击性很强的勒索软件变体。Locky 可能是由“Dridex”银行木马的操纵者编写并传播的。 最近的研究似乎还表明，Locky 具有一个实际分销该勒索软件的附属系统，其中管理员/制作者从受害者支付的赎金中获取分红[18]。 至于每天究竟会产生多少 Locky 受害者，目前尚未有一致的看法。下面列出的数值只是一个非常粗略的估算，并不能保证精确；Talos 小组对这些数据不承担任何责任。

根据《福布斯》的数据，Locky 每天能够危及 90,000 名受害者[19]。 根据 Talos“Angler Exposed”（Angler 分析）研究的统计数据，我们假设 2.9% 的受害者支付了赎金。Locky 的平均赎金金额通常在 0.5 比特币和 1 比特币之间。

赎金价格	受害者/天	付款的人数/天	当前比特币价格（2015 年 2 月 3 日）	每天的利润	每月的利润	12 个月的利润
1 比特币	90,000	2,610	419.00 美元=1 比特币	$1,093,590	$32,807,700	$393,692,400
0.5 比特币	90,000	2,610	419. 00 美元=1 比特币	$546,795	$16,403,850	$196,846,200

图 5：此表显示的是，假设 Locky 每天感染 90,000 名受害者，其中 2.9% 的受害者选择支付赎金，那么平均每天、每 30 天和每年，Locky 可能赚取多少赎金（以美元计）。以每位受害者支付 0.5 比特币和 1 比特币的赎金为标准。

在传送机制方面，Locky 似乎使用与 Dridex 相同的 TTP（工具、技术和流程），首先利用恶意 Office 文档执行网络钓鱼活动，然后通过被入侵的网站和/或防弹主机进行第二阶段传送（真正的攻击性可执行文件）。除此之外，还有证据似乎表明，Locky 是通过漏洞攻击包来传送负载的。这种观点是有道理的；毕竟网络的范围越广泛，所产生的利润越大。

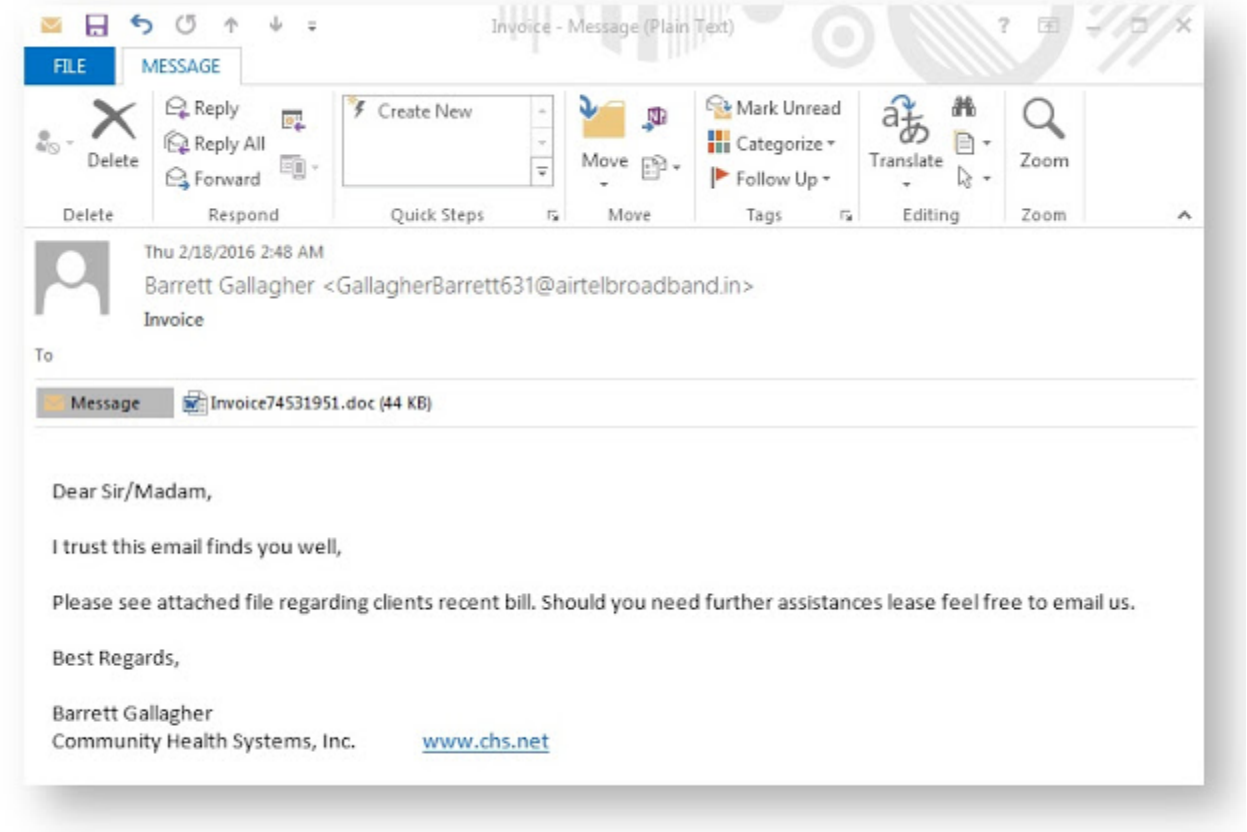


图 6：一个典型的勒索软件网络钓鱼邮件，在其附件中含有 .doc 文件。此示例中，.doc 文件里嵌有 VB 宏，用于抓取第二阶段的负载（通常，这就是勒索软件真正的可执行文件）

最近，有消息表明，一些勒索软件操纵者正在扩大他们的攻击目标。勒索软件操纵者开始转向攻击更庞大的目标，他们认为不仅这些目标安全防护很薄弱，并且可以从中获得更大的收益。

2016 年 2 月，一家医院遭到了勒索软件的攻击。 在这次攻击中，医疗评估和诊断设备、患者记录以及其他电子通信都受到了勒索软件的影响[20]。 这也是第一个公开披露的针对医院的勒索软件攻击。最初据称（或据传言），攻击者要求医院支付 300 万美元的赎金，但是院方最终支付了 17,000.00 美元。现在，攻击者最初索要的 300 万美元这个数额是否真实，以及双方是否通过协商降低了赎金金额，这些都不得而知。该医院与 LAPD 和 FBI 都取得了联系，以寻求如何处理这种情况的建议。 他们的建议是，不断修补系统的漏洞，使用最新版本的杀毒软件，在手边保留备份，如果这一切都无效，那就支付赎金[21]。

遗憾的是最近的报告指出，这种情况正在发展为一种趋势。在德国，也有医院报告感染了影响标准操作的勒索软件。 幸运的是，在报告的案例中，勒索软件影响甚微，并且院方能够通过备份成功地恢复系统[22]。 更近的一个案例是，美国东北部的一家大型医疗保健机构也遭到了类似勒索软件的攻击[23]。

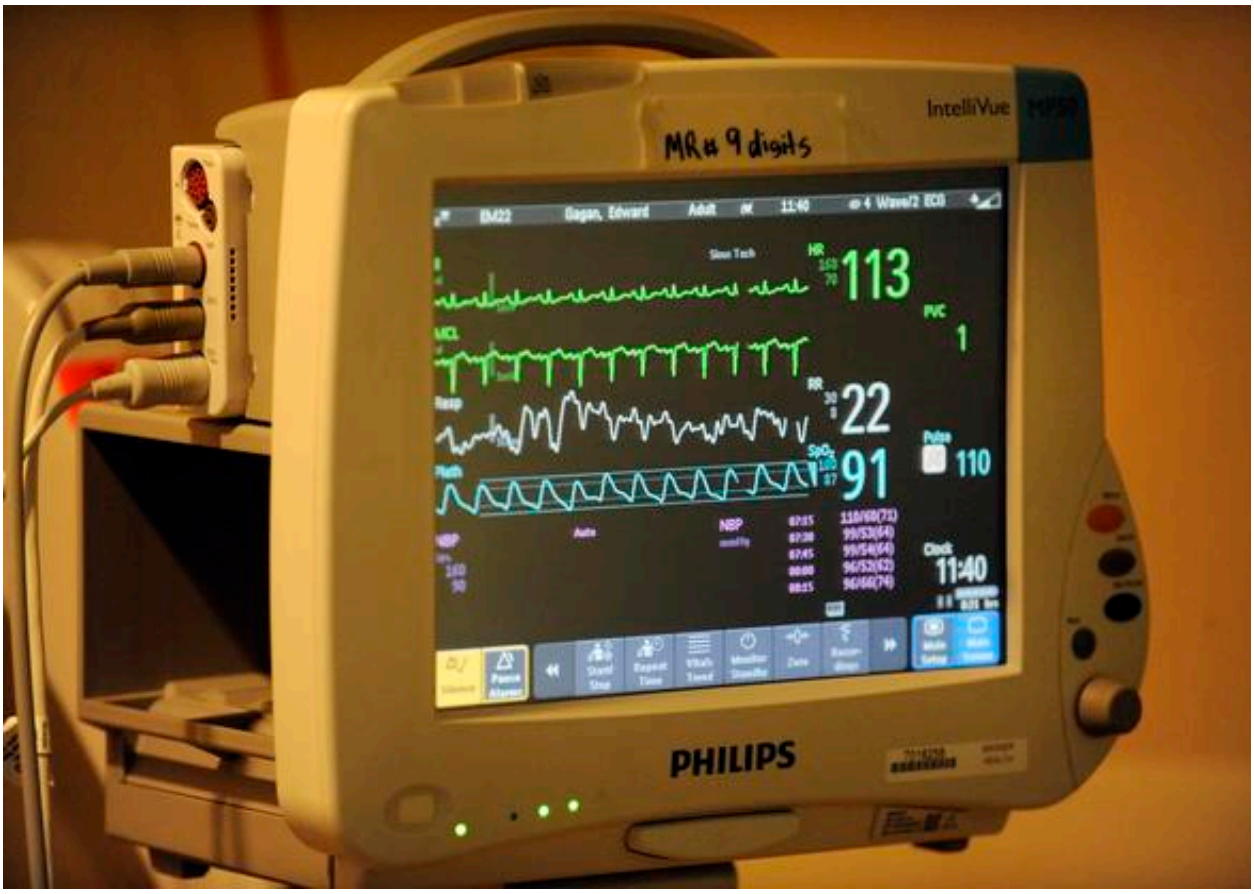
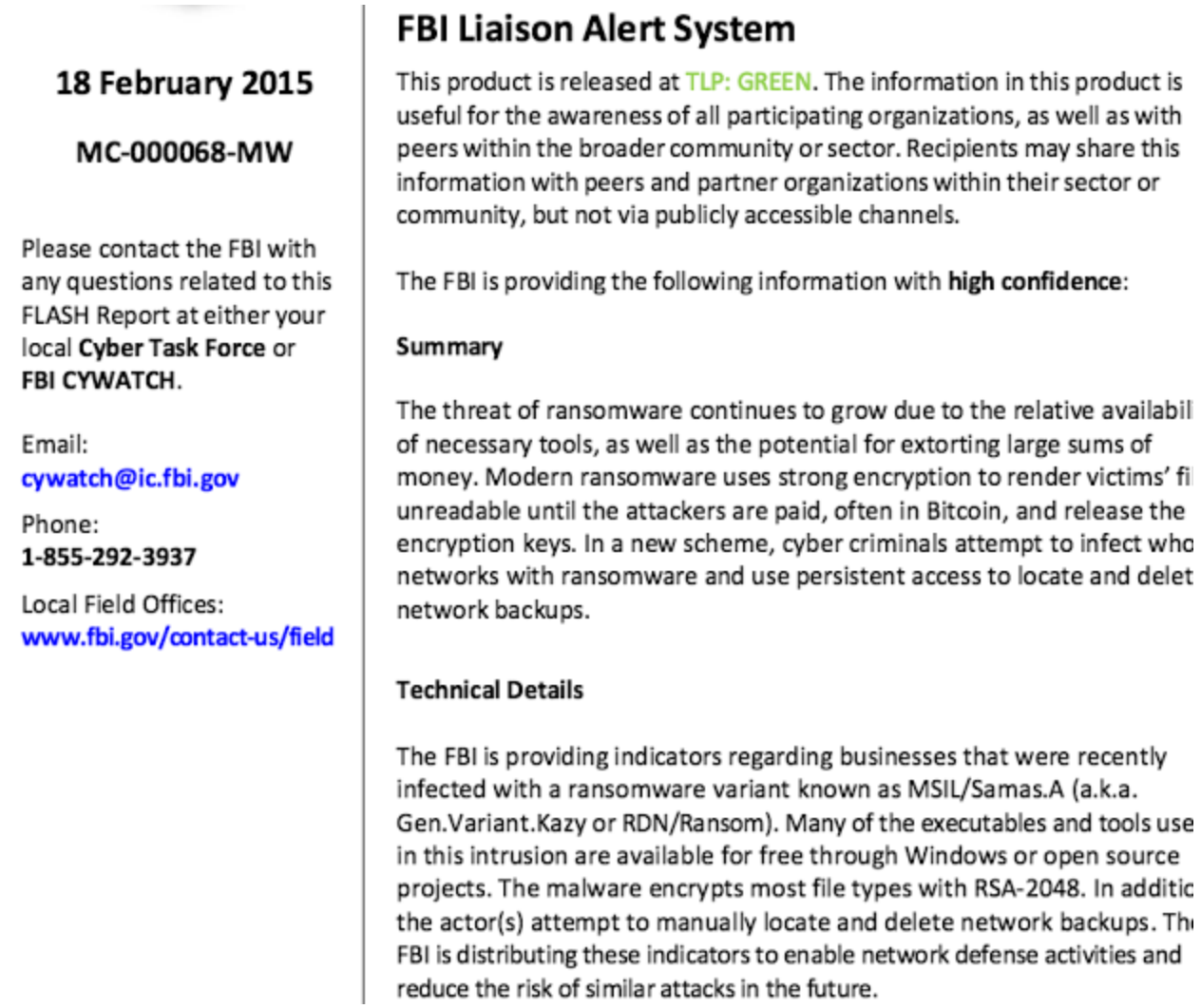


图 7：现已出现很多针对医疗保健行业的勒索软件攻击。目前尚不清楚这些攻击是专门针对医疗保健行业策划的，还是偶然进行的。

发展趋势：SAMSAM.EXE

最近在医疗保健行业发生的攻击事件预示着勒索软件的发展趋势。 最近发布的一份报告似乎也证实了我们的观点：勒索软件正在铤而走险，开始进攻特定的目标，希望获得巨额收入[24]：



18 February 2015

MC-000068-MW

Please contact the FBI with any questions related to this FLASH Report at either your local **Cyber Task Force** or **FBI CYWATCH**.

Email:
cywatch@ic.fbi.gov

Phone:
1-855-292-3937

Local Field Offices:
www.fbi.gov/contact-us/field

FBI Liaison Alert System

This product is released at TLP: GREEN. The information in this product is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector. Recipients may share this information with peers and partner organizations within their sector or community, but not via publicly accessible channels.

The FBI is providing the following information with **high confidence**:

Summary

The threat of ransomware continues to grow due to the relative availabil of necessary tools, as well as the potential for extorting large sums of money. Modern ransomware uses strong encryption to render victims' fi unreadable until the attackers are paid, often in Bitcoin, and release the encryption keys. In a new scheme, cyber criminals attempt to infect wha networks with ransomware and use persistent access to locate and delet network backups.

Technical Details

The FBI is providing indicators regarding businesses that were recently infected with a ransomware variant known as MSIL/Samas.A (a.k.a. Gen.Variant.Kazy or RDN/Ransom). Many of the executables and tools use in this intrusion are available for free through Windows or open source projects. The malware encrypts most file types with RSA-2048. In additic the actor(s) attempt to manually locate and delete network backups. Th FBI is distributing these indicators to enable network defense activities and reduce the risk of similar attacks in the future.

图 8：有关 SamSam.exe 详细情况的一份 FBI FLASH 报告摘要

根据该报告和最近发生的攻击事件，可以看出勒索软件已经开始针对企业进行攻击。勒索软件有针对性地对企业进行攻击已经开始成为主流。

如上所述，SamSam.exe（亦称 MSIL/Samas.A 和 RDN/Ransom）正在成为一个严重的问题。大多数勒索软件或通过漏洞攻击包，或通过大规模的网络钓鱼活动和恶意 office 文档，来将最终用户作为攻击目标。有时他们会对网络共享进行加密，但这并不是攻击活动的主要目标。Locky 勒索软件的不同之处在于，它的攻击目标是映射和未映射的网络共享，而不是集中攻击目标企业的网络。SamSam 在攻击目标和策略上都发生了改变。相比于攻击个人用户，这些攻击者转向攻击企业网络：他们会将能接触到的所有数据都进行加密，从而索要一笔更大数额的赎金。

尽管围绕 SamSam 众说纷纭，但它的攻击方法和负载其实非常简单。首先，攻击者会获取访问权限。根据一些报告显示，获取这种访问权限的一个常用方法就是采用一种称为“Jexboss”的开源工具，寻找流行的 JBoss 应用平台的未修补部署实例作为攻击目标。Jexboss 会采集 JBoss 服务器上的指纹码并进行扫描，以确定其所使用的攻击方法中，是否有易于攻击该目标的某种方法。如果经检查发现，该服务器易于进行攻击，攻击者就会对 JBoss 服务器展开攻击，并向系统上传基于 JSP 的后门。一旦攻击者在服务器上获得一个立足点，就会继续上传能够进一步危害系统的工具，例如“regeorg”。Regeorg 是一种用于在服务器上设置代理的工具，然后可以通过它获得目标网络的进一步访问权限。人们将这种技术称为“支点攻击”。

攻击者通过这个初始访问权限逐渐深入目标网络，并搜索凭证以增强自身的权限。这一阶段的终极入侵目标是，向网络上能够访问的尽可能多的系统大量植入勒索软件之前，查找和破坏联网的备份。在找到备份系统并销毁所有的本地备份或者拒绝对上述备份的访问后，网络攻击者会扫描并收集尽可能多的 Windows 主机。在收集到各个主机后，攻击者使用批量脚本、psexec 及其勒索软件负载的简单组合，通过半自动化的方式向网络中散播勒索软件（需要注意的是，这种散播方法与合法的系统管理员在行使其职责过程中所使用的方法相同）。其真正的可执行文件中内嵌了一个由 sysinternals 制作的能够安全删除的可执行文件，从而确保删除负载并且不能通过磁盘调查分析进行恢复。 尽管散播此恶意软件的方法较为原始，但其结果不容置疑：这些攻击者目前获得了大约 275 比特币 - 超过 115,000.00 美元[25]、[26]。

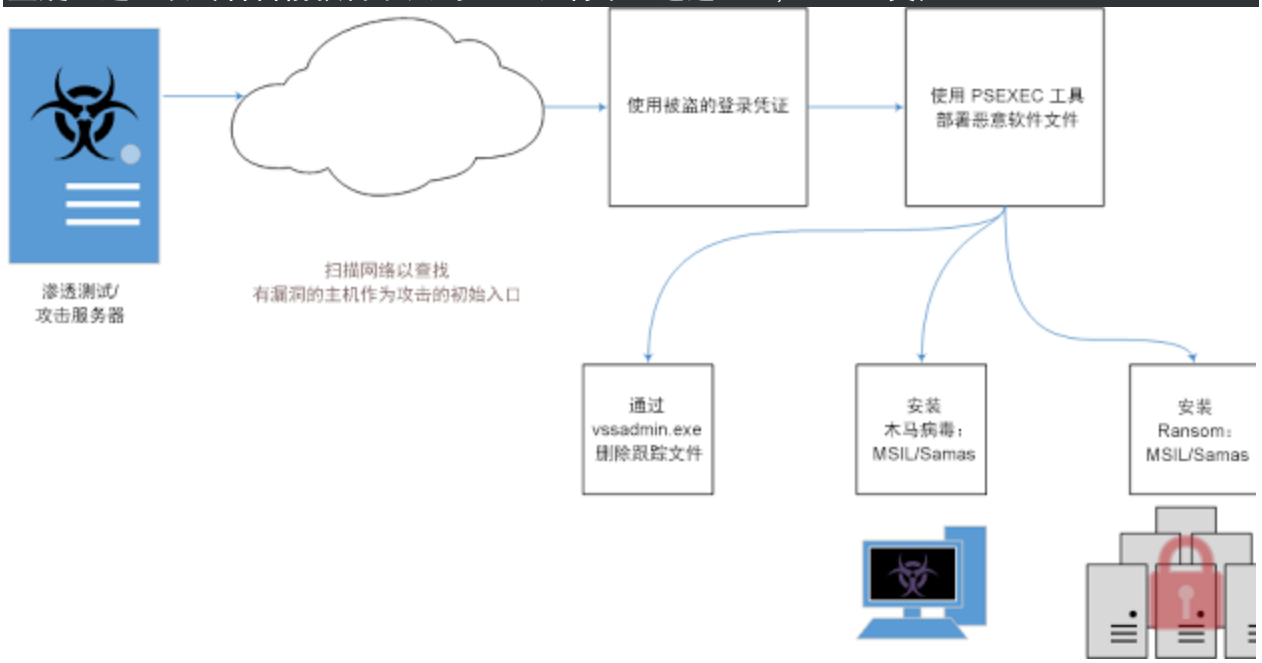


图 9：下图显示的是负责部署 MSIL/Samas（又称为“samsam”）的攻击者所采取的操作流程，本图来自 Microsoft 恶意软件防护中心。

标准勒索软件攻击似乎能够获得数万亿的收入，但是为什么攻击者仍然会选择攻击企业网络，获取一次回报？原因在于：为了进行持续性的攻击，需要花费相当多的成本维护基础设施 - 例如漏洞攻击包所需的代理和网络钓鱼所需的中继站。这些成本不仅包括金钱的支出，还包括避免被检测到所必需花费的人力成本。勒索软件的操纵者必须不停地切换 IP 地址、域和托管基础设施，以避免安全研究人员发现他们的负载并将 C2 站点列入黑名单，或者以其他方式被托管服务提供商关闭服务或者卸载。此外，勒索软件操纵者必须避免泄漏他们的真实身份以免遭到拘捕；只要他们在执行勒索软件活动，执法部门就会寻找他们并将其逮捕，从而阻止他们的违法活动。这些工作都必须在长期的时间里持续进行，如此才能确保勒索软件产生收益。

另一方面，对于 SamSam.exe 之类的勒索软件，在使用的时候并不需要大量的昂贵基础设施，可以通过开源工具快速有效地进行部署。这意味着对企业展开勒索软件攻击所需的成本更低。根据攻击者能够多快地在受害者的网络里进行操作，一般在一两周内就会收到赎金。更低的基础设施成本使得攻击者使用较少的代理服务器就可以隐藏他们的真正位置。这类基础设施成本低廉，并且可以在攻击者的要求得到满足后轻易地销毁/删除。在收到付款后，攻击者能够隐藏他们的真实身份以避开调查员的追踪，同时，他们可以选择风险相对较低的付款方式（通常是比特币）来将他们的非法收益洗白，这一点对他们更为有用。

第 4 章：高效自我传播型恶意软件的特性

SamSam 令人感兴趣的地方在于，它标示着攻击重点所发生的转变，即从以个人最终用户为目标转向以整个网络为攻击目标。此外，其半自动传播方法虽然简单，但很有效。勒索软件制作者由此开始看到攻击企业网络的机会。他们很可能开发出更快、更有效的传播方法，从而最大化地扩大影响以及提高收到赎金的概率。自我传播型恶意软件已经以蠕虫和僵尸网络的形式存在了几十年的时间。通过探究过去存在的这些高效自我传播型恶意软件示例，能够为我们带来启示：这些制作者将来可能会使用哪些方法来赋予恶意软件持久性和自我传播性。

蠕虫是指能够在系统之间自我传播的恶意代码片段。这意味着无需用户干预，它就可以在系统之间自我复制。一旦蠕虫被释放，并且具有可行的传播方法，那就几乎不可能控制蠕虫的感染，更不用说根除蠕虫。 多年前甚至是几十年前释放的恶意软件，如今仍然存在并且继续危害人类[27]。

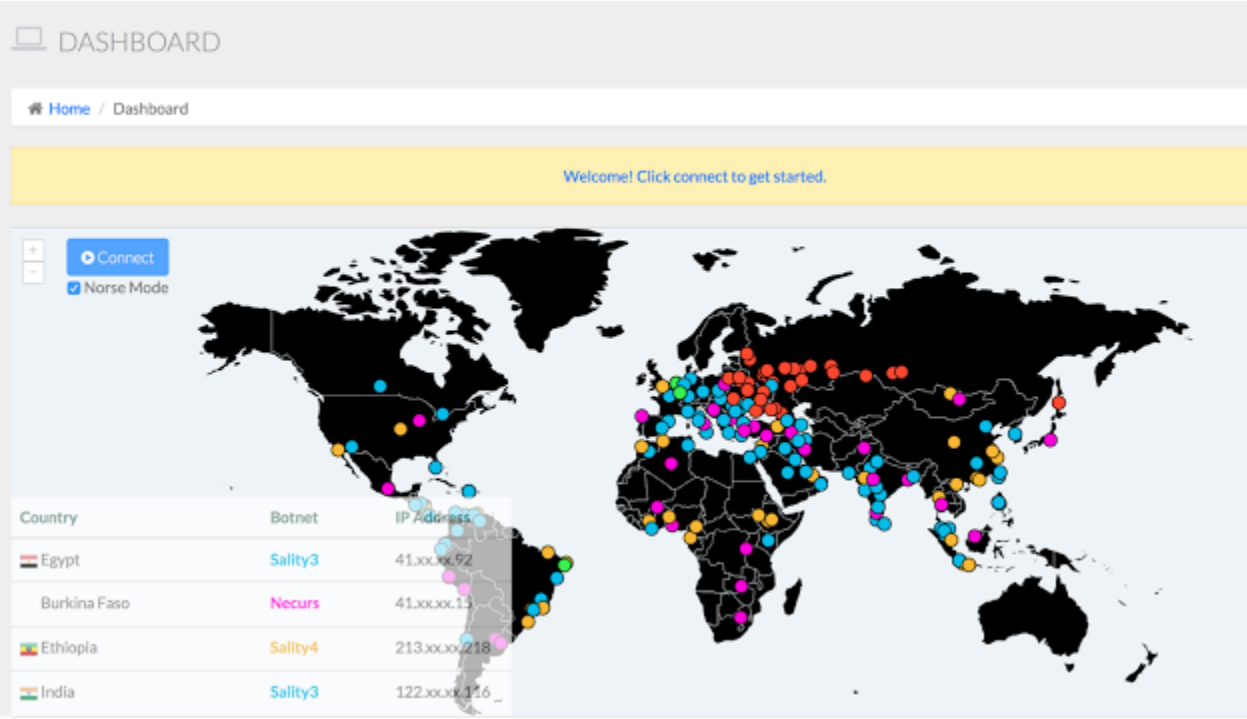


图 10：这是僵尸网络/蠕虫病毒跟踪器的控制面板。这些数据是通过被动和主动的网络监控解决方案收集到的。所跟踪的僵尸网络和蠕虫病毒中，有一些存在时间已达十多年之久，并且仍然十分强大。

当谈起强大的自我传播型恶意软件时，您会想到哪些呢？Nimda？Sasser？Code Red？SQL Slammer？Sality？Conficker？这些流行的、具有弹性的恶意软件有哪些共同特征？我们不妨一起来分析一下它们的某些传播特点：

利用广泛部署产品里的漏洞 - 在过去取得成功的蠕虫病毒大多数都是利用在互联网中所使用的产品的漏洞。直到今天，Microsoft Windows 系统一直很流行，因此，这些蠕虫病毒自然就以 Windows 系统作为感染和传播的目标。这其中有些蠕虫可能会在漏洞被发现/修补之后短短 17 天即已发布，有的则可能会在漏洞首次被公告之后六个月甚至更长时间之后才发布。

自我复制到所有可用的驱动器（网络驱动器、USB 驱动器等） - 某些种类的恶意软件能够收集本地和远程的驱动器，并自我复制到这些驱动器里，以进行散播和/或存留。（例如，恶意软件会自我复制到所有本地驱动器的根目录中，并成为具有隐藏属性和系统属性的可执行文件，也可能作为带有 autorun.inf 文件的隐藏系统可执行文件自我复制到所有 USB 存储设备里，当 USB 存储设备连接到另一个系统时，此 autorun.inf 文件就会尝试执行此恶意软件）。这样，即便通过公共互联网和/或离线系统无法访问的系统也可能被感染。 如同 Sality 一样，Conficker 也是利用这种功能，并通过受感染的 USB 驱动器进行传播[28]，[29]。

文件感染模块 - 以文件为感染目标的恶意软件会将自身附加到文件前面或者后面。具体来说，它们会附加在未受 Windows SFC/SFP（系统文件检查器/保护器）保护的可执行文件上。这样就可确保，每次在系统上运行可执行文件时，系统不会将其视为受保护的操作系统文件，从而使系统可能会再次遭到感染。有些蠕虫病毒还可以自行粘附，并且通过非可执行文件进行传播。

有限暴力破解 - 令人惊讶的是，在过去只有很少的蠕虫病毒尝试使用这一方法。Conficker 的某些变体含有一个限定词表，通过该词表这些变体能够尝试访问隐藏的“ADMIN$”共享文件，从而扩散到其他主机上。 Conficker 的独特性在于，在所研究的自我传播型恶意软件变种中，它是唯一使用此功能的恶意软件[30]。

弹性命令和控制 - 有些蠕虫病毒会考虑到那些通常用来中断“命令-控制”（或简称为“C2”）基础设施的操作。这些蠕虫会实施一些避免发生此类中断的预防措施，例如在无法访问 C2 的情况下执行的一系列操作，或者采用非标准网络架构发出命令。许多蠕虫病毒没有 C2 基础设施 - 它们所使用的只是一个简单的默认操作，从而尽快地进行传播。此类蠕虫的一个示例就是 SQL Slammer 蠕虫病毒，它快速传播的性质会在其活动的高峰期显著地减缓网速。此蠕虫病毒通过非常流行的 MS SQL 服务器里所发现的一个广泛可用的漏洞进行传播。 此外，病毒的感染载体和后续指令都很小，只需要单个数据包即可，并且在当时很常见的扁平化公司网络中，它能够轻易地找到攻击目标，这些都有助于病毒的传播。[31]。 另一方面，Sality 拥有基于 P2P 网络的 C2 基础设施，这种网络与文件共享等程序所使用的网络属于同一种类，它无需通过可能遭受攻击的中央服务器，就可以在客户端之间传播[32]。 最后，除了刚才讨论的 P2P 方法之外，Conficker 蠕虫病毒还使用一种被称为“域生成算法”(DGA) 的技术确定从哪些主机上接收指令。DGA 是一种能够生成大量域名的编程方法，恶意软件制作者由此能够提前购买以防止遭受防御者的黑名单限制。 当每个域依次被阻止、列入黑名单或删除时，攻击者可以移至下一个域，如此能够不断移转并持续地增加威胁，以应对人们阻止蠕虫病毒而采取的措施[33]。

使用其他后门 - 一些恶意软件制作者意识到其他的感染可以已经在系统上留下了后门，他们其实可以直接利用这些后门来传播自己的恶意软件。Nimda 蠕虫病毒巧妙地利用了这种方法：它可以扫描之前的蠕虫病毒“Sadmind”和“Code Red II”所留下的后门。 如果任一个后门可以使用，Nimda 就会通过这个后门来访问并感染系统。[34]，[35]。

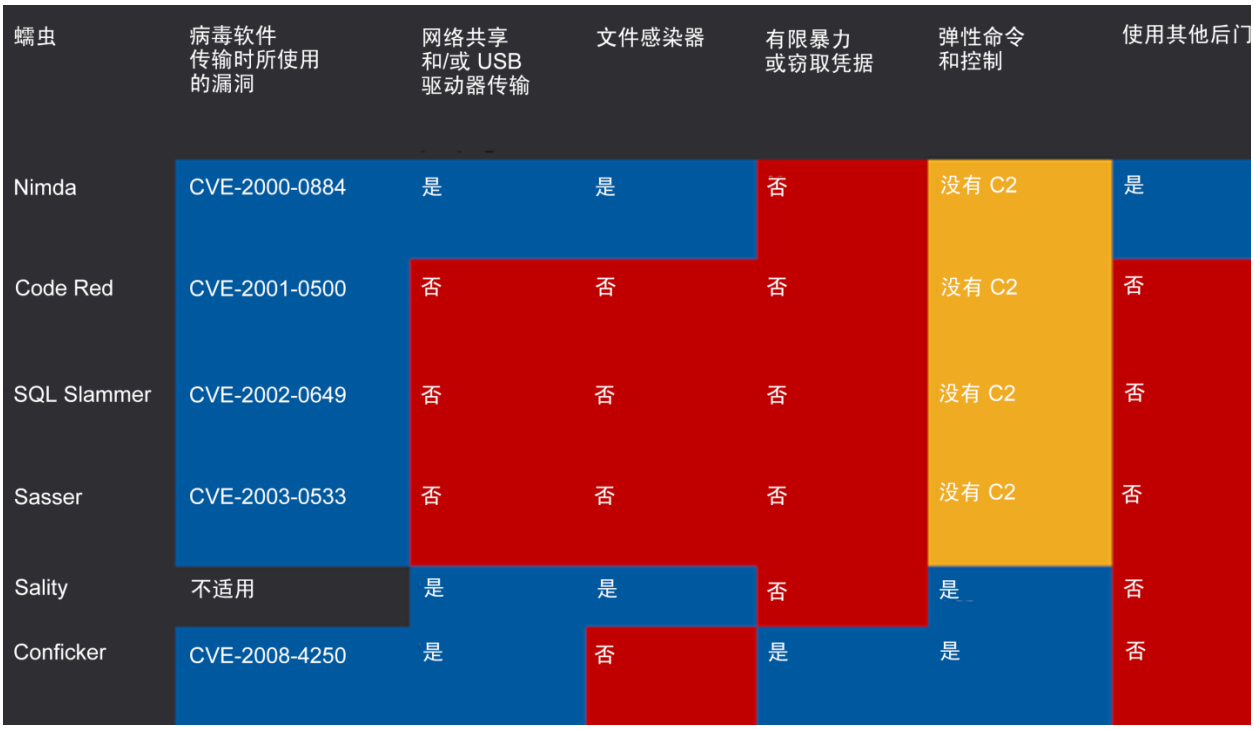


图 11：这些僵尸网络和/或蠕虫病毒通过多种机制全身而退，从而确保它们继续存在并持续进行传播。它们传播很快，并且适应性极强。即便在今天，其中一些僵尸网络仍然在运行。

请注意：我们谈论的所有蠕虫病毒都未使用上述讨论的全部方法。过去的大多数恶意软件都以快速感染作为其唯一目的。一些蠕虫病毒其实并没有进行特别的设计以使其能够长期存活，但是，他们确实在相当长的时间内设法存活了下来。如果这些蠕虫病毒的制作者以勒索软件为制作目的，情况将会如何？

第 5 章：未来的勒索软件

目前为止本文回顾了勒索软件的历史，有关勒索软件的最新事件以及过去一些臭名昭著的僵尸网络和蠕虫病毒的传播特点。回顾的目的是为了思考这个问题：下一代勒索软件将是什么样的？当有经验的攻击者使用强大的、内置的、自我传播的方法来开发勒索软件时，会产生什么后果？本章将介绍勒索软件的下一代架构。然后我们将使用该架构来分析一个模拟情景，从而回答这个问题：如果这种勒索软件存在于今天并且释放到了网络中，会产生什么样的后果？

主流勒索软件框架

我们假设是一位高级攻击者实施本次模拟攻击，例如技术高超的渗透测试员和熟练的威胁攻击者，他们一般都倾向于使用采用模块化设计的软件。模块化设计使他们可以按照需要使用某些功能，这样可以实现更高的效率，并且在发现一种方法无效后，可以按照需要转换策略。在很多流行的开源渗透测试套件中都能找到这种架构，例如 Metasploit（由 Rapid7 提供支持）、Armitage（Raphael Mudge 提供的一个开源框架）以及 Cobalt Strike（由 Strategic Cyber 有限公司提供支持）等等。

在我们假设的框架里，将使用我们前面示例中所取得的经验教训。我们想采用以下功能：

- 对用户文件的标准位置进行加密（例如 C:\Users）以及提供自定义的目录和文件类型，允许按目标进行自定义。
- 标记哪些系统和文件已经加密，以确保避免我们在执行程序的过程中以及在必须进行恢复时，不慎将已加密的文件再次加密。
- 提供联系攻击者的有效方式以及相关的说明，要求您将来之不易的金钱换成您所选择的半匿名货币并发送给攻击者。对此，攻击者常常要求使用比特币，但是，没有理由限制仅可使用比特币进行支付，毕竟还存在其他类似的货币。
- 允许攻击者设定赎金的数额，并指定双重期限：一个是提高支付金额的期限；另一个删除加密数据的密钥之前的期限。

除了这些核心功能外，该框架还应支持不同的模块。这使得攻击者可以对不同的环境进行定制，并且在能够使用漏洞时，改变方法从而以更大肆地进行传播。以下是这类模块的一些示例：

文件感染模块：此模块将扫描目标系统里没有得到内置安全功能（例如 Windows SFC/SFP）保护的可执行文件。它将尝试将自身添加到可执行文件上，从而试图进一步进行传播，并且指望在人们从系统中清除了原始感染病毒后，还可以重新执行此文件。

Autorun.Inf/USB 大规模存储传播本模块将搜索受感染的系统，以查找本地和远程的映射驱动器。然后它将自我复制到这些驱动器的特定位置，并对文件属性进行设置，从而使人们更难以发现和删除这些复制文件。随后，它会将“autorun.inf”文件写入这些驱动器中，从而使之后与该驱动器连接的所有计算机都运行这些感染程序。这是一个经典传播方法，最早出现的一些计算机病毒使用的就是类似这种的方法，该模块的目的是劫持授权员工的访问，从而安全通过防止感染的那些区域。

身份验证基础设施漏洞：本模块将利用作为很多公司网络组件的常见身份验证基础设施中（例如 Kerberos）已知的一些漏洞进行攻击。有许多可以使用的工具，例如“Mimikatz”，这些工具使用各种凭证齐全的方法来攻击这类基础设施。然后，可以利用这些凭证访问其它系统，有时甚至以管理员的身份进行访问。

命令和控制（简称“C2”）/报告感染：为了降低被发现的风险，勒索软件可以通过配置使其丧失命令和控制的功能。本模块将简单地向命令和控制域传送一个附有 GUID（全局唯一标识符）的标志，以尝试通过通用协议/服务（如HTTP、HTTPS或DNS ）访问该域，从而能够传送该数据。然后，C2 可以收集这些 GUID，以统计出目标网络里受感染/加密的系统的数量。攻击者可以使用此类信息确定他们攻击活动的效率。

速度限制器：限制速度：此模块可以确保勒索软件“友善”地对待系统资源，从而使用户不太可能发现有勒索软件正在运行。这意味着它将限制 CPU 的使用率，并减缓网络的使用率，以确保尽可能微妙地执行操作。

RFC 1918 目标地址限制器：如果主机有一个 RFC 1918 地址，所设计的植入程序将只攻击和植入目标主机；即 10.0.0.0/8、172.16.0.0/12，或 192.168.0.0/16 地址。这些地址在内部网络中使用，而不属于互联网地址。

场景示例

一组熟练的、以获取赎金为目标的攻击者一直在收集一家大型公司的相关信息，准备对其发动攻击。机会出现了，攻击者获得了对其网络的初始访问权限。网络攻击者现在需要升级其授权并确定网络中的关键目标，他们需要取得对这些目标的控制以增加获得赎金的可能性。

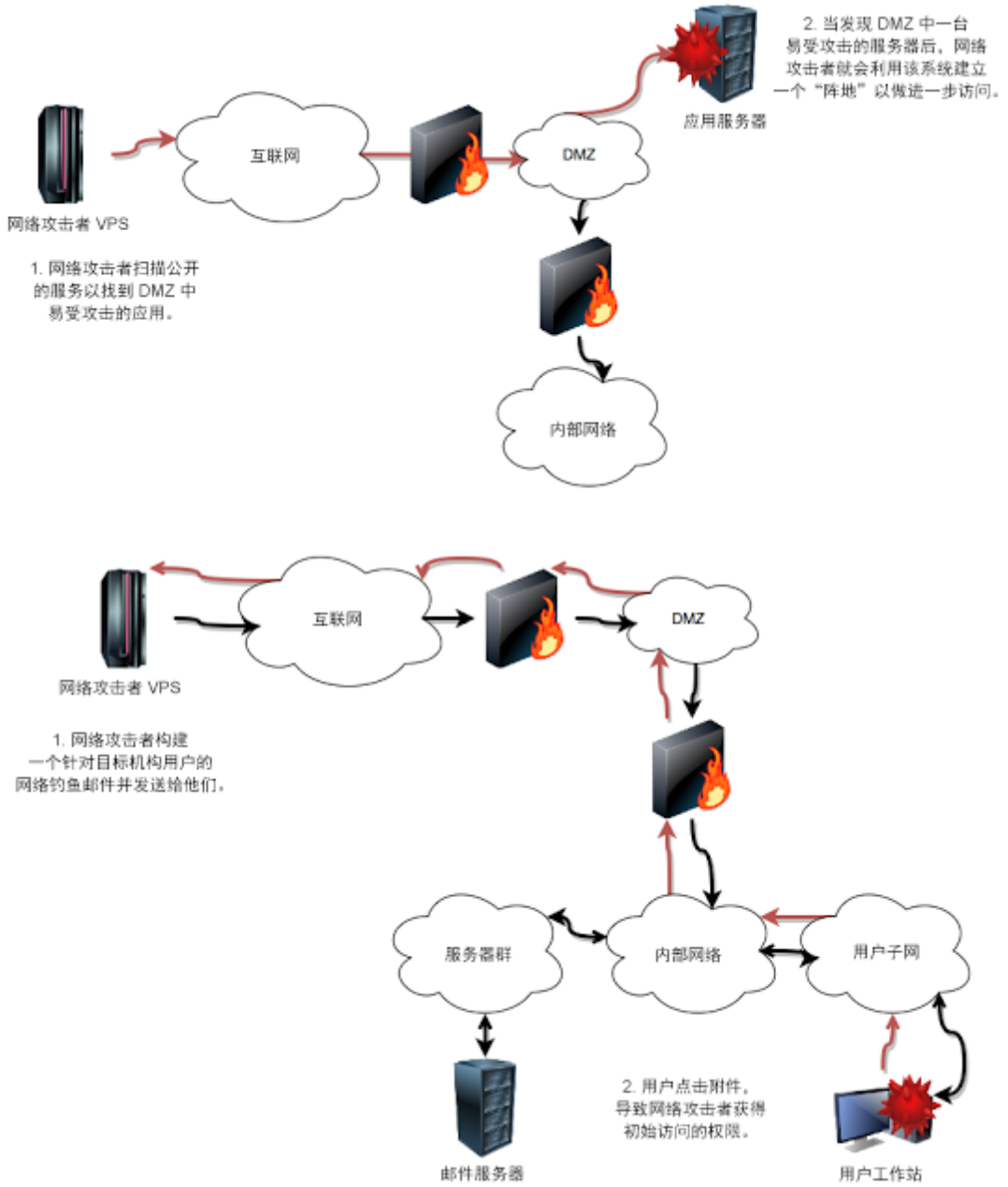


图 12：图中描述的是渗透测试员和其他网络攻击者建立对目标网络的初始访问的常用方法。

攻击者正在尝试利用系统中的本地功能以在目标网络里逐步渗透，同时降低被发现的风险。在许多操作系统里，攻击者可以利用其中很多的远程访问工具从而在系统间逐步渗透。使用本地工具进行逐步渗透，不会向磁盘引入任何内容，并且也不会被视为异常操作，这就降低了人们发现攻击者的可能性。尽管发现这些活动并非是不可能的，但是我们所面临的现实是：大多数安全运营中心 (SOC) 或 MSSP 对此视而不见。这不是我们的主观看法，现实就是如此。 从发生初始攻击到发现攻击所需的平均时间仍然长达四个月以上[36]。

攻击者并非盲目地在网络上进行活动，他们有明确的目标。假设他们获取了至少一台攻击目标工作站的本地管理员凭证，（如果还没有获得凭证，那么通常来讲这是攻击者的第一个目标），那么之后的目标依次是：

1. 获取域管理员级别的凭证和 NTDS.dit - 通过域管理员凭据他们能够访问域控制器。连接到域控制器后，攻击者能够获得 NTDS.dit 的副本，并使用 kerberos 金牌通行证轻松地控制网络。它还向攻击活动授予本域里每一个帐户的所有密码散列表，由此他们可以开始进行破解或简单地“使用散列表”即可。
2. 识别备份系统和/或（可能的情况下）灾难恢复系统（NAS、SAN、磁带机器人控制、Sungard 等）- 网络攻击者获得域控制器和 NTDS.dit 后，就可以自由地查看网络。下一个目标是找出备份系统和服务器，并确认所使用的平台和软件，以及如何能够最好地禁用/削弱它们。此外，如果拥有相关凭证并访问到恢复站点（热站或暖站，例如能够在遭受攻击后进行恢复的 Sungard 系统），对其进行识别和攻击或者拒绝对其进行访问，以确保对方支付赎金。至此我们并没有对系统展开攻击，只是在确认相关目标以供将来植入勒索软件。
3. 识别具有关键性数据和服务的系统（数据库、CMS、编码存储库、文件共享等）- 此时我们的攻击者已经拥有整个系统的密钥，同时确认了备份和灾难恢复系统。下一个逻辑步骤是画出整个网络环境和确定高价值目标。网络上的关键任务型系统是什么，位置在哪里？数据库在哪里？Web 应用？HR 系统？薪资系统？文件共享？如果攻击者发现备份系统和备用网络未分段（尽管不太可能），就会获得一些提示，从而了解公司会将备份存储于其他哪些位置。
4. 识别邮件服务器 - 除了关键任务系统外，识别所有的邮件系统。VOIP、电子邮件、Enterprise Messenger 应用等。在攻击期间，它能够连接到任何人和坐标的硬件，因此使用时间越长，攻击者越能够最大化地散播勒索软件。
5. 识别负责执行软件应用推送的系统：SCCM、WSUS、允许您将软件包进行推送的某些 A/V 厂商、GPO 等 - 在最近有记录的少许攻击事件中，针对企业网络使用的就是这种恶意软件传播方法：它能够危害程序发行平台并使用它来传播负载。鉴于我们的恶意软件具有自我传播的能力，当利用这些应用分发平台时，我们的勒索软件能够成倍扩散，人们也就更难控制我们的攻击。

攻击者能够访问域控制器和根据需要映射网络。目前即已获取备用系统、任务关键型系统、邮件服务器、应用发布平台的访问连接。攻击者从 NTDS.dit 获取散列表，并使用硬编码凭证发现工具/脚本，再结合其他的方法，来找到其他重要域帐户的密码。然后将其作为模板，并结合 rockyou 密码破解词表，就可以破解许多密码。攻击者决定现在即可展开攻击，使用勒索软件框架来生成勒索软件负载，并对其进行下列设置。

核心功能

生成的负载要求对方在 8 天内支付相当于 100 万美元的比特币，如果超过 8 天仍未支付，则赎金将增加到 300 万美元。说明中会提到一个 .onion 地址（隐藏的服务），并告知对方如何使用 tor2web 或 ToR 浏览器捆绑包，以及如何购买比特币。由于攻击者知道所有重要应用、驱动器和数据的位置，因此他们使用勒索软件将自定义目录和文件扩展名进行加密，并作为核心植入的一部分。

安装模块

- RFC 1918 地址限制器：对于这种扩散到目标网络之外的植入，攻击者不感兴趣。
- 速度限制器：这可以确保恶意软件不会因网络或 CPU 的使用异常而被发现。
- PSexec：攻击者获取 NTDS.dit 从而有权访问网络上所有的 NTLM 散列表，同时破解一些散列表，并找到能够访问网络资产的密码列表文件。将词表与 PSexec 结合使用，就可以向整个网络上传并执行负载以实现快速的自我复制。
- 文件感染模块：在执行的时候，负载会确定目录中的执行文件（dll、cpl、scr、exe）是否受到 windows SFC/SFP 是否受到保护和/或目录中的这些执行文件是否进行了加密，如果既无保护，也未加密，则会向其所发现的可执行文件前面附加此负载的副本。这也包括已映射的网络驱动器。

负载传送和传播

攻击者可以修改组策略和域的 GPO 并传送一个自定义勒索软件植入的破解版本 MSI。然后他们就离开网络，然后等待对方支付赎金。正是由于被盗用的散列表（和/或用户名/密码）和通过 GPO 进行软件推送（这会传播和执行恶意软件），最终导致恶意软件呈指数级扩散。通常，大多数公司网络缺少网络分段，这会进一步促进勒索软件负载的传播，甚或扩散到更多的系统里。即便备份磁带未受感染（在原位或不在原位置），但是由于备份管理系统受到感染，因此也无法恢复备份。当勒索软件继续传播时，核心应用和系统开始一步步崩溃。系统很快就会出现遭受攻击的症状，但是，由于对邮件系统和应用的攻击，以及只有宽带通信（移动电话、外部托管聊天系统）是可用的，调度很缓慢，这就为勒索软件提供了更多的时间进行传播。

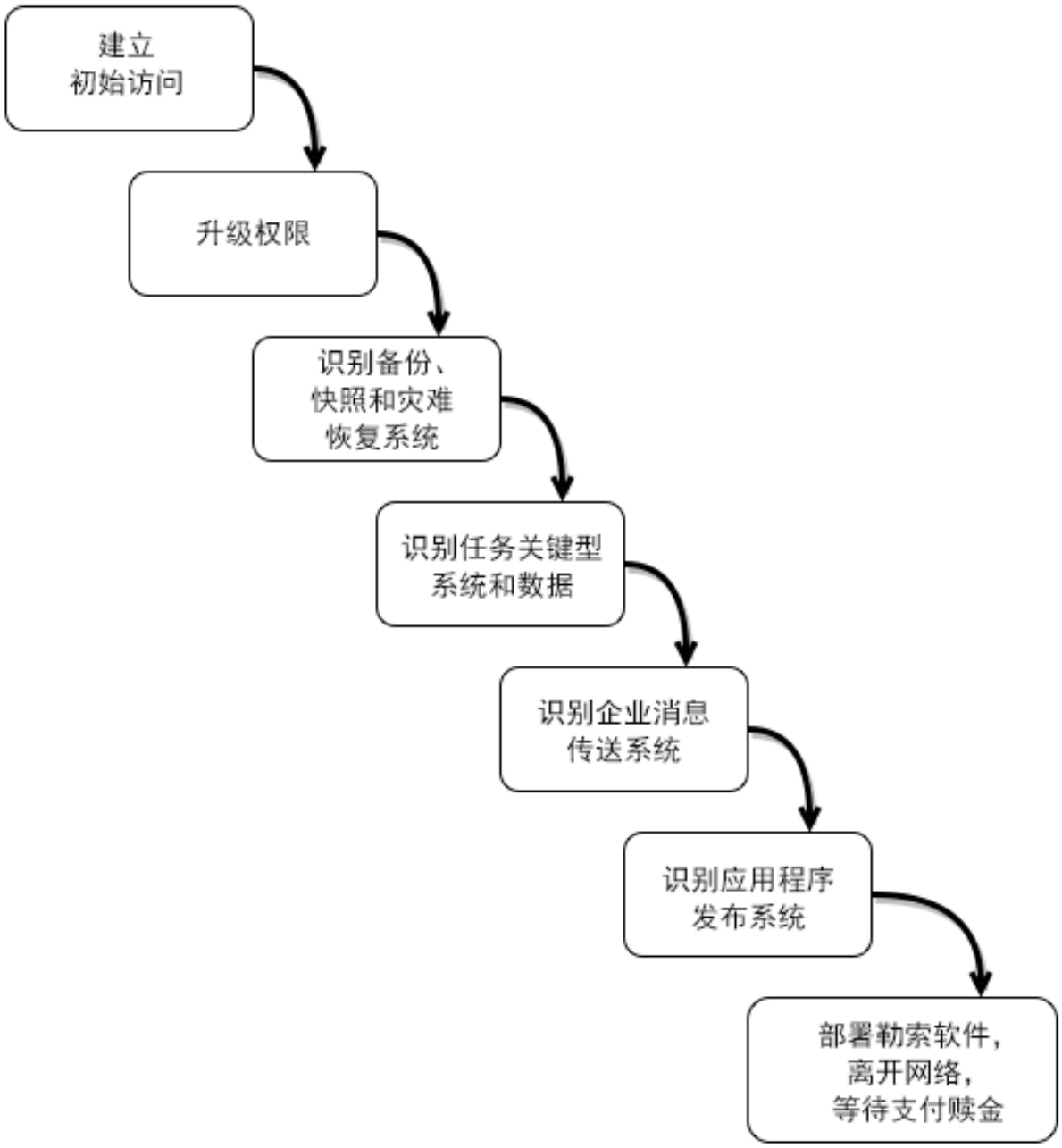


图 13：描述的是我们虚构网络攻击者使用勒索软件彻底地破坏目标网络的攻击流程。

攻击的影响

一旦勒索软件发动攻击，几乎是无法阻挡的。在 1 小时的时间里，800 多台服务器和 3200 台工作站受到了危害；目标组织一半的数字资产和公司绝大多数的数据都被加密。尽管启动了灾难恢复模式，但是，由于共享的凭证和很少的分段，DR 环境也遭到了危害。此时，目标组织仿佛回到了 20 世纪 80 年代，只能使用数字打字机、笔记本电脑、传真机、便条纸，纸质支票等等。受害者面临着一个选择：是首开支付赎金的先例以求得快速恢复，还是拒绝支付赎金（这种情况下可能会使恢复时间拖得更长、难度也更大，并且很可能发生数据丢失）？

无论作何选择，都涉及恢复数据的成本问题。例如，需要使用外部的应急响应力量来帮助确定事故的根源和/或支持内部应急响应，还包括安全和 IT 员工全天候进行工作以将系统恢复至运行状态所需支出的资本和运营费用等等，如果您成为上述攻击的受害者，那么会有许多量化/质化的附带损失。我们还未探讨受害者是否决定支付赎金的问题。

作为恢复过程的一部分，受害组织需要决定是否支付赎金。这会涉及到有关备份的重大问题：受害组织在多大程度上能够接受数据的丢失？当系统遭到彻底破坏的时候，这种接受程度将决定受害组织是否会支付赎金。需要考虑的因素包括如下几个方面：

- 本地备份是否可用，或者磁带库、SAN 里的内容是否都被删除或以其他的方式导致不可用？
- 如果磁带库或 SAN 里的内容被删除或不可使用，非现场的备份是否可用？
    - 异地备份频率如何？
        - 每周一次？
        - 两周一次？
        - 每月一次？
- 数据的重要性如何？
    - 在备份不可用的时间段里，受害组织会因数据丢失遭受多大的总收入损失？
    - 是否有方法可以手动恢复数据？
    - 手动恢复的费用是多少？

将上述问题（或者更多）全部计入在内，最后做一个简单计算：如果支付赎金的相关成本少于非现场备份之间的时间间隔内丢失数据的相关成本，那么受害组织很有可能会支付赎金。否则，该组织将接受数据丢失，并开始进行恢复。

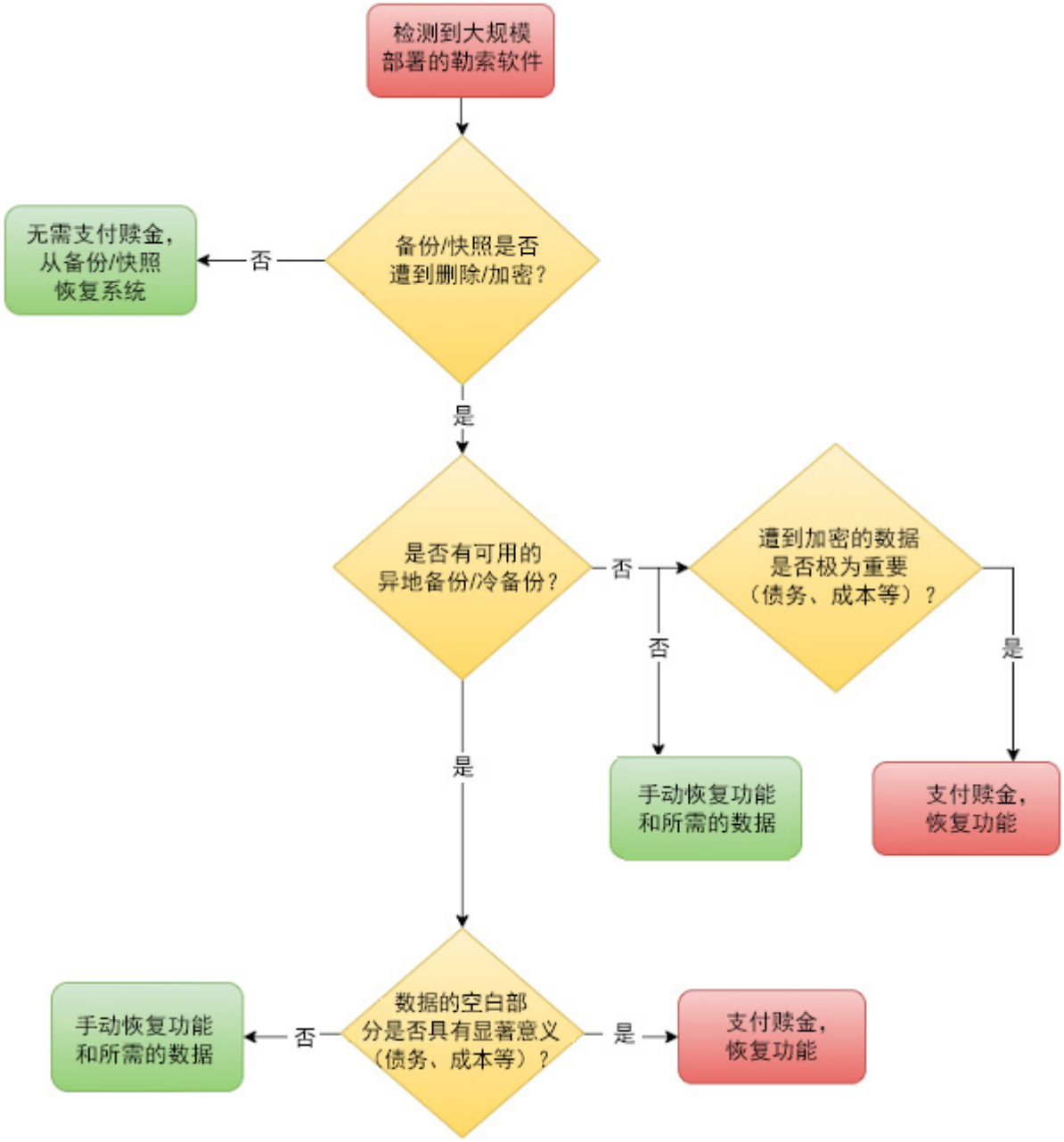


图 14：在遭到勒索软件攻击时，此流程图可以最终决定受害者是否会支付赎金。

作为恢复过程的一部分，如果受害组织投保了网络保险，那么可以申请保险理赔。但是网络保险是较新的产物，尚不成熟。此时还必须考虑一些问题，包括：

- 网络保险提供商是否会对索赔进行核查？
  - 他们是否会发现受害者存在过失[37]？
  - 保险单上是否附有相关条款，对于勒索软件或“网络敲诈勒索”造成的损失进行赔偿[38]？
- 保险单是否足以赔偿损失[39]？

在大多数情况下，网络保险要么不足以覆盖全部的风险范围，要么并未附带适当的附加条款以赔偿特定的损失[40]。

第 6 章：防御

正如在本文我们所描述的那样，在有经验的攻击者手里，具有自我传播功能的勒索软件将会成为受害者的一场噩梦。但是，尽管可能发生上述情形，但是并不代表它必然会发生。总体来说，大多数企业网络都以大致相同的方式构建，因此所描述的场景大体相同。这意味着无论具体目标是谁，上述场景几乎都普遍适用。鉴于企业的网络设计具有相同特性，针对“当攻击者以我们为目标的时候，会发生什么”这个问题，答案是相同的：如果没有坚实的外围防御，那么攻击者就能够进行初始访问。如果攻击者可以进行初始访问，而且受害者允许这种威胁在网络内逐渐渗透，攻击者所得到的授权就会逐步升级，最终他们就会映射网络，以访问帮助他们达到目的的相关资产。如果允许权限升级，在攻击者部署勒索软件后，就会对目标组织产生彻底危害，并造成服务的丧失。这时问题会变成：当攻击者不再满足于投机性地攻击医院，而是将他们的目标设定在其他组织或者其他垂直行业，情况会怎样？电力、燃气、水、运输、空中交通管制？与以往相比，深度防御已经不再是数十年间所宣传的一个概念或词语，如今，它更成为一项必须进行的实践工作。

下面列出的是一些降低风险的策略。尽管这些都不是新出现的方法，但是当组合使用的时候，这些防御技术和策略能够灵活地阻止初始访问，并且如果攻击者成功地获取初始访问，他们具有限制相关威胁的作用。

防止初始访问

在攻击尚未开始之前，我们就可以采取措施来预防进攻的发生。如果攻击者在目标网络无法轻易地建立初始访问，那么攻击者更可能转向其他较为容易进攻的目标。攻击者也是机会主义者，他们希望花费尽可能少的代价来取得相应的收益。如果无法轻易地建立初始访问，这会增加他们寻找其他更容易进攻目标的可能性。获得初始访问通常采用如下两种方式中的一种：公共服务的漏洞或者网络钓鱼/社交工程。

DMZ 强化技巧

DMZ 强化包括几个关键性的管理和维护任务：

- 定期进行端口扫描：端口扫描可以用来映射您的 DMZ，并且在组织连接互联网的时候，可以更好地查看实际的服务和操作系统的情况。如果您有一些服务连接到互联网，您可以将公共地址映射到私有地址，以确定谁拥有那些资产和/或是否确有必要将这些服务连接到互联网。连接到公共互联网的服务数量越少，攻击者的攻击范围就越窄。
- 漏洞扫描/补救：一旦确定有公开暴露的服务，应使用漏洞扫描工具对其进行扫描。尽快修复扫描结果。

- 常规系统维护：
  - 查找并遵循系统强化指南，例如 DISA 的 STIG[41]
  - 确保定期执行补丁维护。
  - 确保 DMZ 系统日志连接到日志采集器/SIEM。
  - 需要身份验证的所有公开系统/服务都应当使用强密码；并可以考虑实施双因素身份验证（如果可能）。
  - 需要身份验证的所有公开系统/服务都应具有限速功能，或者可以基于失败的猜测次数中断系统/服务，从而阻止暴力破解攻击。

缓解网络钓鱼/社交工程

若要防止攻击者通过网络钓鱼或社交工程获得初始访问则要困难得多，具体可以采取下述措施来缓解相关风险：

- 考虑建立一个公司管制的文件共享程序，组织的用户和/或公司合作伙伴之间可以通过该程序交换文件。使用一个文件共享解决方案，并指示用户不得共享或接收来自邮件的文件，这样做几乎就可以完全缓解利用附件的网络钓鱼攻击。指示用户不得使用邮件服务器进行文件交换，也不得将其用于文件归档。
- 通知用户不必经常使用启用宏的 office 文档，甚至永远不要启用宏。 实际上，您大多数的基础用户无需使用宏，可以通过组策略禁用 office 宏，并只为有特定需要的业务部门而启用宏[42]。 对于必须使用 Office 宏的那些业务部门，可以考虑使用数字签名的宏，以进一步降低该风险。
- 有些网络钓鱼攻击是通过传送 PDF 文件来进行的，专门针对某些 PDF 阅读器应用（例如 Adobe Reader）的漏洞来达到执行代码的目的。可以考虑使用其他 PDF 阅读器并禁用额外的功能（例如 PDF 上的 JavaScript）。
- 确保邮件扫描网关禁止发送和接收可执行文件（exe、dll、cpl、scr）、带有宏的 JavaScript（.js 文件）office 文档，以及扫描 .zip 文件的内容。
- 对 SPF 记录进行检查/验证，以减少欺骗性电子邮件。
- 确保您拥有邮件网关解决方案，并使用最新的网络钓鱼域信息对其进行更新（如 senderbase 等）
- 通常，由于新的 gTLD 和动态 DNS 域价格低廉，因此在恶意软件活动中出现了严重的滥用。在大多数情况下，几乎可以无所顾忌地将这些域列入黑名单；毕竟它们与业务的相关性往往非常低。将动态 DNS 和 gTLD 默认为黑名单，并且只有在特定业务确有需要的情况下，将单个域根据需要加入白名单。
- 提示用户，即便信任也要进行验证，特别是对于来自公司外部的带有附件的任何邮件。进行验证时，只需简单地询问发送方“您发送过此邮件吗？”在打开附件之前，都应首先通过电话进行确认。

- 在任何情况下，如果用户怀疑他们遭到了网络钓鱼攻击，指示用户报告该事件。不应让用户畏惧您的 SOC 或安全部门，并且不应因为用户报告安全事件而对其施加惩罚。
- 通知用户，IT 和/或安全部门从不会要求其提供他们的密码，从而降低网络钓鱼攻击的有效性，他们在攻击的时候会尝试收集用户的凭证。
- 禁止安装 USB 驱动器。这将减少“由于帮助别人打印其 USB 驱动器中的简历而感染恶意软件的场景”，同时可以缓解试图通过已感染病毒的 USB 驱动器躲避防御的自我传播型恶意软件。如果无法在整个企业都禁用可移动介质，至少要禁止可移动介质通过 GPO 自动运行，并且指示员工决不可接受或使用来自不受信任源的闪盘。指示用户在插入闪盘以及访问文件之前，应当对所有的闪盘进行病毒扫描；可以考虑配置相应的杀毒软件，从而在任何 USB 驱动器插入系统时，杀毒软件会自动进行即时扫描。如果需要在敏感的物理分隔区使用闪盘，可以考虑单独留存一批闪盘，将其标记为公司资产并在每次使用时进行签名登记。
- 确保访客在前台进行登记、签名，并始终对其进行跟踪监控。访客进行访问时，应始终有陪同人员在旁。
- 近距尾随，即未获授权的个人跟随已获授权的个人进入限制区，可能会成为一个严重的问题。大多数人都有避免冲突的倾向，因此就使得实施防止近距尾随的策略更加困难，对于似乎“手头工作很忙”的人提出上述要求则尤为困难。解决办法是将下述要求列入安全政策：员工必须佩戴工牌并随时可以让人们看到。此外，所有授权访客、供应商等都需要遵守本政策，进入所有门户时都必须携带工牌并且始终应由员工陪护/陪同。

阻止逐步渗透和传播

如果攻击者突破您的初始防御，您的目标就是尽可能地让他们难以在网络里逐步渗透。通过周密的架构和密码管理，您可以使攻击者的逐步渗透变得非常困难。

- 企业大部分的网络是“一马平川”的，在业务部门之间、用户和数据之间、特定数据和业务部门之间等，几乎很少甚或没有分段。在大型组织里，您通常看不到网络分段的原因是这需要大规模的协调和规划。大多数网络随着容量需求的增加而随之增长，同时只有很少甚或根本没有考虑进行分段。进行企业兼并时，他们通常关注的是如何快速集成其他资源，而这和安全的要求是相反的。除了这些之外，对网络进行适当分段的好处是不容否认的。通过分段可以终止和/或减缓逐步渗透，并控制所产生的威胁。分段网络有多个组件，但是不应只是将其视为一份详细清单，而是应当考虑具体实施以下事项：

    - VLAN 和子网分段：每个业务部门都应拥有各自的 VLAN 和子网，从而对各自访问的数据进行逻辑隔离。另外，分段不应该仅限于业务部门。用户工作站与本业务部门所需的服务器/服务，以及跨业务部门所使用的服务（例如，消息、文件共享、邮件等）同样需要进行分段。VLAN 和子网的列表应当由 IT 和安全人员进行精心维护并供其使用。如果您由于疏忽而未获得这些信息，或者正在尝试找出对用户、服务器和业务部门进行逻辑分隔的方法，可以考虑查找 DHCP 范围配置并且将其用作进行子网和 VLAN 分段的准则。
    - 专用防火墙/网关分段：防火墙是网络分段的另一个重要部分，但是在进行内部网络设计时，它常常为人们所忽视。了解哪些业务部门有彼此直接通信的需求，哪些没有这种需求。了解业务部门间进行通信时需要哪些服务和端口。对入口和出口进行过滤（这需要了解服务数据流的方向）。定期审查防火墙策略。IT 和安全人员应当可以使用防火墙策略，并应参与策略审查的决定。
    - 配置入口/出口过滤的主机型防火墙。再次强调 - 入口和出口均需进行过滤。主机彼此之间应当不能通过 SMB（139/tcp、445/tcp） 进行通信。如果设置了文件服务器，实际上就不需要进行这种通信。如果您可以有效地禁用主机间的 SMB 通信，您就可以防止攻击者使用“通过散列表”所进行的逐步渗透。SMB 通讯应仅限于应用分发平台，文件共享和/或域控制器。
- 应用程序管制/白名单：应用程序白名单是 windows 的内置功能，可以通过软件限制策略来实施这种功能[43]。 但是，如同网络分段一样，它需要大量的时间进行实施和测试，尤其当不同的业务部门有不同程序需求的时候。 因此作为一种临时措施，使用它来阻止试图在特定位置（例如 Windows 系统的 %TEMP%或%APPDATA% 目录）运行的可执行文件，可能较为容易，同时可以对某些有必要运行可执行文件的应用程序做出例外设定[44]。 如同网络分段一样，白名单的设置也需要花费大量的时间，但是对于控制和防止初始访问和逐步渗透，它能够为我们带来巨大的帮助。
- 基于角色的网络共享权限（最小权限）：在网络上多个业务部门、文件夹权限和共享权限之间的文件共享往往极其复杂。应用程序的文件共享权限如果限制在最小范围，就可以防止对单个用户的攻击所导致的网络文件共享上的大部分数据发生丢失，也可以防止攻击者使用被侵害帐户来访问不同业务部门的数据；如果密码安全管理不善，攻击者可能使用被侵害的用户帐号来收集文件共享中该用户所不应拥有的凭证。
- 适当的凭证管理：应当对用户进行培训，从而要求其使用密码管理器和强密码来存储网络凭证。要求客户不得重复使用密码

恢复

面对攻击者的赎金勒索，备份恢复是您的最后一道防线；在最坏的情况下，它将是您最后的堡垒。您是否能够以最少的数据丢失和/或服务中断而从攻击中得以恢复，取决于系统备份和/或灾难恢复站点作为攻击者攻击对象的一部分，是否遭到破坏。您的备份是否遭到破坏又取决于备份系统的完善程度和/或网络、恢复站点是否与您的主网络充分进行了分段。即便您根本不使用现场备份，而是选择使用云备份解决方案（例如 Amazon Glacier），但是如果这些云备份凭证保存在易于获取的位置，或者，如果重复使用密码，那么我们假设的网络攻击者就可以轻易地删除所有的备用，此时如果不没有其他适当的备份解决方案，就会造成 100% 的数据丢失。自认为安全、非现场的企业备份解决方案，如果存在密码重复使用的现象和/或密码管理不善，实际上可以轻易地被攻破。

对于使用备份解决方案的企业，有各种各样的备份方法供其选择；SANS 阅览室里有一个关于磁带循环方案的综合性文档，它对于审查不同的磁带循环方案非常有帮助[45]。 通常来讲，作为磁带循环策略的一部分，人们会将这些磁带的一部分发送到离站存储设备。这么做的目的是为了进行灾难恢复；如果存放组织数据的站点发生灾难性故障，存储设备里的磁带仍然完好地保存在那里，并可以通过备份设备进行恢复。如果本地备份被删除、撤除或被攻击者使用其他方式导致不可用，如果想不支付赎金，非现场备份通常是恢复服务的唯一希望。您将备份发送至离站的频率，将决定有多少数据（如有）可能发生不可访问或丢失。

总结

在过去几年里，在全球范围内勒索软件变体及其部署呈明显的上涨趋势。网络犯罪分子发现了一个获取收益的好机会。这些网络攻击者必然会留意在过去取得成功的那些恶意软件，以期提高勒索软件的有效性。结合锁定目标的新方法，我们预计勒索软件的发展趋势是 - 它将能够在整个网络里进行自我传播和半自主的渗透，并造成毁灭性的后果。

为了强调这一点，大家只需观察一下 SamSam.exe - 这个在多个互无联系的企业网络中发现的以医疗行业垂直部门为主要目标进行破坏的恶意软件样本 - 就会发现这个趋势。SamSam 并不复杂，亦不具有完全的独立性，但是它显示出一个成功的蠕虫病毒的诸多特征 - 快速传播、传送负载（勒索软件）和削弱系统的恢复能力。自我传播型勒索软件（或者称为“加密恶意软件”）的时代即将到来。

长期以来，有关企业网络安全的关键性安全控制和最佳实践做法得到了广泛赞誉，但是在私底下他们却被忽略了。插入式设备和安全解决方案只能在其力所能及的的范围内保护网络，而如果人们没有从内心重视起来，未对网络的构建和扩展建立深度防御，那么在防止威胁方面他们只能起到很小的作用。如果企业不立即开始架构防御性措施，那么有可能导致今后不得不支付大量的赎金。

参考资料

1. https://en.wikipedia.org/wiki/Ransomware
2. http://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/
3. https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b
4. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=502676
5. http://www.networkworld.com/article/2314306/lan-wan/files-for-ransom.html
6. http://voices.washingtonpost.com/securityfix/2008/06/ransomware_encrypts_victim_fil.html
7. https://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Ransom%3AWin32%2FGenasom.BQ
8. http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/
9. http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/
10. http://www.welivesecurity.com/wp-content/uploads/2014/12/torrent_locker.pdf
11. https://www.cryptowalltracker.org/
12. http://www.pcworld.com/article/3045206/security/teslacrypt-ransomware-now-impossible-to-crack-researchers-say.html
13. http://www.bleepingcomputer.com/news/security/the-Locky-ransomware-encrypts-local-files-and-unmapped-network-shares/
14. http://krebsonsecurity.com/2015/11/ransomware-now-gunning-for-your-web-sites/
15. http://www.computerworld.com/article/3018972/security/ransom32-first-of-its-kind-javascript-based-ransomware-spotted-in-the-wild.html
16. https://blog.opendns.com/2016/03/10/17123/
17. http://www.talosintel.com/angler-exposed/
18. http://community.hpe.com/t5/Security-Research/Feeling-even-Locky-er/ba-p/6834311#.VsacC_IrJhF
19. http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#22a04c7e75b0
20. http://www.engadget.com/2016/02/19/hospital-ransomware-a-chilling-wake-up-call/
21. https://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise
22. http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030
23. http://bigstory.ap.org/article/cf41601903fd4cc492718c12b01d9d1c/fbi-probing-virus-behind-outage-medstar-health-facilities

24. http://eweb.cabq.gov/CyberSecurity/Security%20Related%20Documents/FLASH%20MC-000068-MW.pdf
25. http://blog.talosintel.com/2016/03/samsam-ransomware.html
26. https://blogs.technet.microsoft.com/mmpc/2016/03/17/no-mas-samas-whats-in-this-ransomwares-modus-operandi/
27. https://intel.malwaretech.com/
28. https://isc.sans.edu/forums/diary/Conficker+autorun+and+social+engineering/5695/
29. https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Win32%2FSality
30. https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm%3aWin32%2fConficker.B
31. https://www.sans.org/security-resources/malwarefaq/ms-sql-exploit.php
32. https://www.sans.org/reading-room/whitepapers/detection/60-seconds-wire-malicious-traffic-34307
33. https://www.icann.org/en/system/files/files/conficker-summary-review-07may10-en.pdf
34. https://www.sans.org/security-resources/malwarefaq/sadmind_iis.php
35. https://www.sans.org/reading-room/whitepapers/malicious/code-red-worm-45
36. http://www.scmagazine.com/companies-quicker-to-detect-breaches-hackers-more-aggressive/article/479415/
37. http://www.businessinsurance.com/article/20150515/NEWS06/150519893
38. http://www.irmi.com/online/insurance-glossary/terms/c/cyberextortion-coverage.aspx
39. http://www.privacyanddatasecurityinsight.com/2015/03/cyber-insurance-do-i-really-need-it/
40. https://c.ymcdn.com/sites/www.coloradobankers.org/resource/resmgr/Education/03-23-15_Weekly_Risk_Summary.pdf
41. http://iase.disa.mil/stigs/Pages/index.aspx
42. https://www.microsoft.com/en-us/download/details.aspx?id=18968
43. https://www.nsa.gov/ia/_files/os/win2k/application_whitelisting_using_srp.pdf
44. https://bluesoul.me/2016/03/18/ransomware-is-the-future/
45. https://www.sans.org/reading-room/whitepapers/sysadmin/backup-rotations-final-defense-305

WILLIAM LARGENT 上午 9:01发布

标签：CRYPTOWALL,网络钓鱼,勒索软件,SAMSAM,社交工程