FORTINET

白皮书

勒索软件威胁态势分析

了解威胁的范围和复杂性

要点综述

当一种网络威胁在一年中增长 35 倍时，每个组织都应引起注意。这正是对勒索软件的真实写照。黑客将攻击目标瞄准许多不同行业领域的组织，以及不同规模的企业。单点的、碎片化的安全措施已经难以阻止勒索软件攻击。在防御网络攻击时，采用将下一代防火墙、分层安全性和前瞻性威胁情报相集成的安全模式至关重要。

勒索软件即服务 (RaaS) 和其他套件类工具降低了网络犯罪的门槛，即便是新手攻击者也可以成功入侵分散的安全基础设施。而比特币等货币技术则使执法机构几乎无法跟踪赎金支付的链路。如今，支付给勒索软件黑客的赎金正在呈指数增长。未来几年内，这种趋势极有可能会延续下去，并且增长速度将会更快。

组织所遭受的财务影响远不只是向网络犯罪分子支付赎金这么简单。停机会造成数千甚至数十万计的收入和生产力损失。目前，多个行业的受害组织都可以证明这些影响。

威胁范围

从中小型企业 (SMB) 到大型企业，数据是当今大多数组织的核心。然而，随着更多公司资产的数字化以及向云端的不断迁移，网络犯罪分子开始将攻击矛头指向数据。90% 的全球数据是在过去两年中创建的，并且同期数据泄露事件增加 54%。

从 2018 年到 2019 年，检测到的勒索软件数量增加了 365%。[1]

在过去的一年中，新型勒索软件变种的数量增加了 46%。[2]

认识到数据的巨大价值后，越来越多的网络犯罪分子开始使用勒索软件来牟取非法利益。他们通过各种攻击手段渗透到 IT 系统中并访问数据，然后对文件进行加密、锁定和泄露。由于无法访问对业务至关重要的信息，被黑客攻击的组织不得不向网络犯罪分子支付赎金以解锁这些信息。随着攻击手段的不断演进，现在网络犯罪分子可以为受害者提供实时客户支持，从而引导他们完成汇款并重获对数据和 IT 系统的访问权限。

勒索软件攻击激增

勒索软件的威胁有多严重？去年，勒索软件攻击增加了一倍以上，并且黑客对攻击手段进行了修改以增加非法所得。[4] 但与此同时，只有三分之一的组织表示他们有信心可以跟踪和阻止攻击。[5]

勒索软件的财务影响也直线上升。到 2021 年，勒索软件预计将对全球产生 200 亿美元的影响。[6] 勒索软件通常索要六位数的赎金，并且一般要求使用比特币进行汇款，这无疑增加了对网络犯罪分子洗钱的追查难度。[7]

间接成本是与勒索软件攻击相关的业务中断成本。在公共部门中，42% 的组织在过去 12 个月中经历过勒索软件事件，其中 73% 的组织因此停运两天或更长时间。[8]

只是冰山一角

然而，这些数字可能无法真正说明问题的严重程度。勒索软件攻击存在严重的少报问题，被报告的事件只有不到四分之一。一份新报告揭露，网络犯罪问题可能被广泛低估。超过一半的受访者表示，他们认为大多数企业即使在必要时也不会报告网络犯罪。9

对于自认规模太小而不会成为网络犯罪分子勒索软件攻击目标的组织而言，情况已然不同。小型企业通常缺乏专门的内部 IT 专家，而且缺乏必要的控制措施来管理 IT 系统，因此更无法幸免于勒索软件攻击。在面对大型组织强大的安全控制措施屡屡受挫的情况下，攻击者正将目标锁定更下游的公司，根据小型企业的收入降低了勒索金额，但发起了更多攻击。确实，这些企业在运营时无法提供适当的数据保护来抵御、防备勒索软件并从中恢复过来，正迅速成为网络犯罪分子的主要勒索目标。对于中小型企业来说，平均停机成本为 141,000 美元，比去年的平均水平增长 200% 以上。[11]

勒索软件的业务影响

如今，因勒索软件攻击造成的系统停机以及无法访问信息的成本损失高达数十亿美元，而且随着勒索软件黑客不断将目标瞄准物联网 (IoT) 设备，这一数字可能飙升至数百亿美元。

人肉搜索

网络犯罪分子诡计多端。一些网络犯罪分子不再威胁删除锁定的数据，而是威胁要公布这些数据（也称为“人肉搜索”）。对于处理私人和敏感客户数据的组织来说，例如金融服务、医院、律师事务所等，这可能会带来严重不良后果。除了对品牌声誉的影响之外，根据《健康保险可携性和责任法案》(HIPAA) 等法规就信息保护提出的发送客户通知和其他繁琐要求，违规泄密可能会迅速造成数十万甚至数百万美元的处罚。

为“赎金”日储备比特币

勒索软件的影响不仅仅限于被黑客攻击的组织。以银行为例。由于数据丢失或无法访问数据所造成的潜在影响可以用分钟甚至秒进行衡量，因此企业无法等待网络犯罪分子数天之后才允许其访问被黑客攻击的数据。

勒索软件如何工作

勒索软件的传播

那么，勒索软件究竟如何工作呢？首先让我们看一下勒索软件的分发。勒索软件可以使用任何数字手段进行分发，包括电子邮件、网站附件、业务应用、社交媒体和 USB 硬件，以及其他数字传输机制。电子邮件仍然是第一大传输载体，而且网络犯罪分子更愿意使用链接文件，其次是附件。

- 电子邮件链接，31%
- 电子邮件附件，28%
- 网站附件，24%
- 未知来源，9%
- 社交媒体，4%
- 业务应用，1%

基于 SaaS 的主要感染：[12]

- Dropbox，64%
- Microsoft Office，47%
- G Suite，18%
- Box，6%
- Salesforce，2%

勒索软件感染的首要原因：[13]

- 垃圾邮件或网络钓鱼电子邮件，76%
- 缺乏网络安全培训，36%
- 弱密码，30%

就电子邮件而言，网络钓鱼电子邮件作为传递通知或虚假软件更新请求发送。用户点击链接或附件后，其他恶意组件通常（但最近较少）会以透明的方式下载下来，然后使用 RSA 2048 位私钥对文件进行加密，从而使用户几乎无法解密文件。在其他情况下，勒索软件作为文件嵌入在网站上，一经下载和安装，便会发起攻击。

不同类型的勒索软件

勒索软件的攻击形式不尽相同。去年，勒索软件攻击经历了迅猛发展。传统勒索软件会跟踪您的数据并锁定文件，直至您支付赎金。但是随着物联网设备的激增，新型勒索软件开始出现。它不会追踪组织的数据，而是将目标瞄准控制系统（例如车辆、生产装配线、电力系统），通过关闭这些系统索要赎金。

让我们快速浏览下现有的几种最流行的勒索软件：

商用现货勒索软件。一些勒索软件以商用现货软件的形式存在，网络犯罪分子可以从暗网市场购买并安装在自己的恶意服务器上。对数据和系统的黑客攻击和加密直接由在网络犯罪分子服务器上运行的软件进行管理。商用现货勒索软件的示例包括 Stampado 和 Cerber。

勒索软件即服务。CryptoLocker 可能是最著名的勒索软件即服务 (RaaS) 模型。自从其服务器被关闭之后，CTB-Locker 已成为最常见的 RaaS 攻击方法。另一种快速增长的 RaaS 是 Tox。其工具包可供网络犯罪分子自由下载，并产生一个可由网络犯罪分子安装或分发的专用可执行文件，其中总赎金的 20% 会用比特币支付给 Tox。

勒索软件联盟计划。RaaS 模型通过具有可靠记录的联盟黑客来传播恶意软件。

对物联网设备的攻击。勒索软件会渗透到对关键企业系统实施控制的 IoT 设备中。它会关闭这些系统，直至获得赎金才会解锁它们。

勒索软件家族和变种在 2016 年激增十倍。2016 年，FortiGuard Labs 每天都能检测到多个新变种。有趣的是，除多态代码外，勒索软件还经常使用变形代码来更改其数字身份，但攻击方式保持不变。依赖基于签名的传统杀毒解决方案的组织很难跟上勒索软件的持续快速演进。当组织确定一种变种并将其列入黑名单时，网络犯罪分子已经开始采用新的变种。举例来说， 2020 年第一季度赎金数量的增加，Ryuk 和 Sodinokibi 勒索软件家族就“功不可没”。[15]

如今，几乎每个操作系统都是勒索软件的攻击目标。攻击范围还扩展到了云和移动设备。到目前为止，勒索软件尚未大举进攻云，对于黑客来说，这是一个全新的市场机会。[16]

勒索软件黑客近期的另一项策略是瞄准并入侵易受攻击的企业服务器。通过定位服务器，黑客可以识别并瞄准主机，这导致网络上可能受感染的服务器和设备数量成倍增加。此类攻击压缩了攻击时间，比针对最终用户的攻击更具传染性。这一演进可能会导致受害者为解密密钥支付更高的费用，并延长恢复加密数据的时间。

现实攻击

几乎每个行业和每种规模的组织都受到了勒索软件的影响。2019 年，勒索软件攻击影响了 113 个政府机构、市政府和州政府，764 个医疗服务提供者以及 89 个大学、学院和学区，多达 1,233 所学校受到波及。[17]

以下是勒索软件对其中一些主要行业领域的影响研究。这部分将列举企业遭遇黑客入侵的具体示例，这些企业不仅支付了高额赎金，而且还受到了严重的财务和运营影响。

医疗

医疗行业的勒索软件问题备受关注。医疗行业中的许多 IT 系统和数据都与患者护理相关，因此意义重大。任何系统停机或信息无法访问都可能危及生命。即便勒索软件攻击不影响用于患者护理的系统和数据，医疗机构也会因丢失患者病例而受到处罚并且需要投入时间来修复损坏。

在人肉搜索中，网络犯罪分子威胁发布而非删除私人信息，这已成为勒索软件网络犯罪分子的一种策略，而且其后果更加严重。针对患者护理 IoT 设备上发起的勒索软件攻击会危及生命。

2019 年下半年勒索软件攻击占据了医疗新闻头条，在第四季度增加了 350%，对 IT 厂商的攻击造成了数百家牙科和护理机构的服务中断，还有许多医院、卫生系统和其他实体报告称因这些针对性攻击而蒙受业务中断。[18]

近年来这样的例子不胜枚举。例如，黑客窃取了对 MongoDB 数据库的访问权限，该数据库中包含一家大型健康中心 20 万患者的健康信息。该数据库被黑客清空，受害者必须支付 18 万美元赎金才能安全地恢复这些数据。

到 2024 年，网络安全市场规模将达到 3,000 亿美元。[19]

电子邮件

去年，90% 的恶意软件感染通过电子邮件传播给受害者。恶意软件最常用来藏身的文件类型是：[20]

- Microsoft Office 文件，45%
- Windows 应用，26%

隐私

在对超过 2,000 名安全专业人员的调查中，90% 的受访者认为，无论自己多么谨慎，其个人数据还是随时会被犯罪分子窃取。[21]

公用事业和能源行业

公用事业和能源行业遭受的网络攻击在数量上与其他行业大致相当。用于管理和运行公用事业和能源公司的关键基础设施的工业控制系统 (ICS) 为网络犯罪分子，包括勒索软件黑客带来了新机遇。

制造业

制造业正迅速成为勒索软件黑客的高价值目标。制造商比其他行业面临着更高的风险，因为它们不受金融服务等其他行业的监管和合规性约束。

除了包含知识产权和专有信息的 IT 系统之外，制造商还高度重视高效的流程和运营。勒索软件攻击可能会导致停机，从而削弱财务收益。对于制造商而言，时间就是金钱。因此，在制造商看来，更明智的选择是支付赎金以尽快恢复系统正常运行。

一家混凝土制造商在一名员工点击感染 CryptoWall 勒索软件的电子邮件附件后，经历了一周的停机。该勒索软件扩散到了公司的整个网络，并加密了对几个生产系统至关重要的会计数据和文件。工作日第一天，工作人员无法访问生产文件来启动制造时才发现该勒索软件。即便该公司在两天后支付了赎金，其一些会计文件仍未能解锁。如果没有这些数据的备份，该公司则将需要进行冗长的会计恢复项目。

去年，勒索软件病毒 LockerGoga 袭击了一系列工业和制造业，带来了灾难性的后果。安全研究人员表示，最近发现的这个恶意软件变种极具破坏性，它会彻底关闭计算机并锁定用户，使得受害者甚至难以支付赎金。[22]

教育行业

有关勒索软件攻击的新闻头条通常围绕医疗、金融服务和其他行业领域的安全事件。但是，教育在勒索软件目标组织中的排名也很高。为什么呢？教育机构拥有教师、教职员工和学生的社会保险号、病历、财务数据和知识产权，因此是非常有利可图的目标。此外，K-12 学校和专科学校行业细分对网络安全准备工作的重视程度不够，这就不难理解为何网络犯罪分子将它们视为攻击目标了。

金融服务和银行业

信息金融服务和银行存储着广泛的客户信息，这使其成为了勒索软件攻击的首要目标。网络钓鱼和勒索软件攻击是金融服务公司[23]报告最多的网络攻击类型。此类事件的最常见原因通常被描述为“第三方故障”（这或许反映了 IT 基础设施之间的关联性），占报告总量的 21%。19% 的事件归咎于硬件和软件问题，18% 归因于变更管理。[24]

信用合作社和小型银行的勒索软件黑客行为正在急剧增加。去年第一季度，勒索软件攻击激增，针对客户的勒索软件攻击通知数量与去年第一季度相比增加了 105%。[25]

制造业

制造业正迅速成为勒索软件黑客的高价值目标。制造商比其他行业面临着更高的风险，因为它们不受金融服务等其他行业的监管和合规性约束。

除了包含知识产权和专有信息的 IT 系统之外，制造商还高度重视高效的流程和运营。勒索软件攻击可能会导致停机，从而削弱财务收益。对于制造商而言，时间就是金钱。因此，在制造商看来，更明智的选择是支付赎金以尽快恢复系统正常运行。

一家混凝土制造商在一名员工点击感染 CryptoWall 勒索软件的电子邮件附件后，经历了一周的停机。该勒索软件扩散到了公司的整个网络，并加密了对几个生产系统至关重要的会计数据和文件。工作日第一天，工作人员无法访问生产文件来启动制造时才发现该勒索软件。即便该公司在两天后支付了赎金，其一些会计文件仍未能解锁。如果没有这些数据的备份，该公司则将需要进行冗长的会计恢复项目。

去年，勒索软件病毒 LockerGoga 袭击了一系列工业和制造业，带来了灾难性的后果。安全研究人员表示，最近发现的这个恶意软件变种极具破坏性，它会彻底关闭计算机并锁定用户，使得受害者甚至难以支付赎金。[22]

教育行业

有关勒索软件攻击的新闻头条通常围绕医疗、金融服务和其他行业领域的安全事件。但是，教育在勒索软件目标组织中的排名也很高。为什么呢？教育机构拥有教师、教职员工和学生的社会保险号、病历、财务数据和知识产权，因此是非常有利可图的目标。此外，K-12 学校和专科学校行业细分对网络安全准备工作的重视程度不够，这就不难理解为何网络犯罪分子将它们视为攻击目标了。

金融服务和银行业

信息金融服务和银行存储着广泛的客户信息，这使其成为了勒索软件攻击的首要目标。网络钓鱼和勒索软件攻击是金融服务公司[23]报告

最多的网络攻击类型。此类事件的最常见原因通常被描述为“第三方故障”（这或许反映了 IT 基础设施之间的关联性），占报告总量的 21%。19% 的事件归咎于硬件和软件问题，18% 归因于变更管理。[24]

信用合作社和小型银行的勒索软件黑客行为正在急剧增加。去年第一季度，勒索软件攻击激增，针对客户的勒索软件攻击通知数量与去年第一季度相比增加了 105%。[25]

政府机构

由于系统中包含至关重要的信息，政府机构对网络犯罪分子来说别具吸引力。去年，俄亥俄州向当地市政政府警告称勒索软件攻击正呈激增趋势，当地市政当局需要通过建立正确的技术和流程来防范这些威胁。

到 2021 年，勒索软件预计将对全球产生 200 亿美元的影响。

要点

随着勒索软件的发展和变异，对几乎各种规模的组织所构成的威胁与日加剧，组织要特别注意以下几点：

拦截已知威胁。寻找一款网络安全解决方案，以阻止所有攻击媒介中已知的勒索软件威胁。这需要使用分层安全模型，其中包括由前瞻性全球威胁情报提供支持的网络、端点、应用和数据中心控制措施。

检测新威胁。随着现有勒索软件的持续演进和新型勒索软件的不断发布，必须使用正确的沙箱及其他先进的检测技术以锁定使用相同载体的不同变种，这点至关重要。

规避未知威胁。必须在不同的安全层（通常是厂商产品）之间共享实时可行的情报，甚至扩展到组织外部的更广泛网络安全社区中，例如计算机应急响应小组 (CERT)、信息共享和分析中心 (ISAC) 以及网络威胁联盟等行业联盟。这种快速共享是快速响应攻击并在其变异或传播到其他系统或组织之前打破攻击链的最佳方法。

为意外做好准备。安全的网络分段有助于防御勒索软件蠕虫行为，例如 SamSam 和 ZCryptor。数据备份和恢复同样重要。拥有最新数据备份的组织可以拒绝支付赎金的要求，并快速轻松地恢复系统。

备份关键系统和数据。尽管恢复加密系统可能是一个非常耗时的过程，而且会中断业务运营并降低生产力，但是与支付赎金相比，恢复备份是一个更好的选择，因为支付赎金后也不能保证您的数据和系统就会被解锁和还原。在这种情况下，您需要正确的技术、流程甚至是业务合作伙伴，以确保您的数据备份满足业务需求，并且可以快速恢复。

1 Lucian Constantin, "More targeted, sophisticated and costly: Why ransomware might be your biggest threat," CSO, February 10, 2020.

2 "Ransomware Facts, Trends & Statistics for 2020," Safety Detectives, April 22, 2020.

3 Nick Parkin, "Businesses will need to be more data savvy in 2020 to reap rewards of big data," ITProPortal, January 9, 2020.

4 Jessica Davis, "Ransomware Attacks Double in 2019, Brute-Force Attempts Increase," HealthITSecurity, September 3, 2019.

5 "New Study Reveals Cybercrime May Be Widely Underreported – Even When Laws Mandate Disclosure," Financial Post, June 3, 2019.

6 "Ransomware Facts, Trends & Statistics for 2020," Safety Detectives, April 22, 2020.

7 Danny Palmer, "Ransomware is now the biggest online menace you need to worry about—here' s why," ZDNet, April 22, 2020.

8 Yotam Gutman, "What is the True Cost of a Ransomware Attack? 6 Factors to Consider," SentinelOne, January 8, 2020.

9 "2019 State of Cybersecurity," ISACA, 2019.

10 Alfred Ng, "Ransomware froze more cities in 2019. next year is a toss-up," CNET, December 5, 2019.

11 Yotam Gutman, "What is the True Cost of a Ransomware Attack? 6 Factors to Consider," SentinelOne, January 8, 2020.

12 "Ransomware Facts, Trends & Statistics for 2020," Safety Detectives, April 22, 2020.

13 "Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2019," Statista, 2020.

14 "Ransomware Facts, Trends & Statistics for 2020," Safety Detectives, April 22, 2020.

15 David Bisson, "Increase in Ransomware Demand Amounts Driven by Ryuk, Sodinokibi," Tripwire, May 4, 2020.

16 Corey Nachreiner, "Why Ransomware Will Soon Target the Cloud," Dark Reading, February 11, 2020.

17 "The State of Ransomware in the US: Report and Statistics 2019," EMSISOFT, December 12, 2019.

18 Jessica Davis, "Ransomware Attacks on Healthcare Providers Rose 350% in Q4 2019," HealthITSecurity, March 9, 2020.

19 Casey Crane, "80 Eye-Opening Cyber Security Statistics for 2019," The SSL Store, April 10, 2019.

20 "2019 Data Breach Investigations Report" Verizon, 2019.

21 "Privacy in an open world: How much do Americans care about online privacy?" Nixplay, June 6, 2019.

22 Andy Greenberg, "A Guide to LockerGoga, the Ransomware Crippling Industrial Firms," WIRED, March 25, 2019.

23 Steve Ranger, "Phishing, ransomware are top cyberattacks on financial services firms," ZDNet, July 1, 2019.

24 Ibid.

25 Gene Fredriksen, "Ransomware—A growing credit union threat and the unified solution," CUInsight, October 9,