白皮书

勒索软件二进制文件的实证比较分析

作者：Shannon Davis

SURGe by Splunk

splunk> turn data into doing

执行摘要

安全研究人员和网络防御者已经撰写了许多关于勒索软件的文章，但许多组织仍然对这种攻击做出战术性的反应，而不是有针对性的应对。这部分是由于缺乏关于勒索软件的基础知识。勒索软件的加密速度是一个值得进一步研究的领域。迄今为止，关于这一主题的最全面的信息来自 LockBit 勒索软件作者自己，他们在自己的网站上发布了勒索软件系列加密速度的比较结果，以宣传他们是“最快的”。 本文旨在阐明一个以前留给罪犯的研究领域。我们在受控环境中利用科学方法，测量了 10 种流行勒索病毒恶意软件在不同 Windows 操作系统和硬件规格下加密近 10 万个文件（总计近 53GB）的速度。通过这项工作，我们希望给防御者更多的知识和信心，让他们在检测过程中“防患于未然”，而不是在 Lockheed Martin 网络杀伤链白皮书中讨论的“行动目标”阶段等待检测。

为了确定勒索软件的加密速度，我们创建了 Splunk 攻击范围实验室环境的修改版本，并选择了 10 种勒索软件变种，然后在四台主机上执行每个变种的 10 个样本。两台主机运行操作系统 Windows 10，另外两台主机运行Windows Server 2019。在将勒索软件样本归因于每个变种时，我们采取的方法是在 VirusTotal 中仅选择由 Microsoft Defender Antivirus 确认的样本。我们为每台主机分配了“高”或“中”级别的资源，以测试勒索软件在不同的处理器、内存和硬盘配置下的表现。我们在每台主机上启用了 Windows 日志功能，以收集、综合和分析 Splunk 中的数据。这使我们能够测量勒索软件变种加密近 10 万个文件的速度，以及勒索软件如何利用处理器、内存和磁盘等系统资源。

在运行所有 100 个勒索软件样本后，我们确定总加密时间 (TTE) 从 4 分钟到 3 个半小时不等，平均速度为 42 分钟。由于加密时间短，在加密完成之前，留给组织做出有效响应的时间将非常有限。当在具有不同资源的系统之间比较相同的勒索软件病毒株时，我们发现一些变量会影响 TTE，例如处理器速度或 CPU 内核。然而，影响也不一致，这意味着一些勒索软件是单线程的，或最低限度地能够利用额外的资源。LockBit 勒索软件是在任何系统上加密最快的变种。这与之前的报告一致，即 LockBit 只需加密每个文件的 4KB，便可使文件无法使用，从而加快了攻击速度。“最快勒索软件”的称号也与 LockBit 开发者自己在该组织 Tor 网站上的公开宣称相吻合。

SURGe 计划在这项研究的基础上，为网络防御者提供全面而高层次的勒索软件概述。特别是，我们计划使用开源文件分析框架工具（例如 stoQ、模糊算法和 Splunk 的机器学习工具包 (MLTK)）来审查多个勒索软件样本的文件访问技术。此外，我们还计划调查现代勒索软件没有用打包程序掩盖的说法，并确定是否有可能在未知勒索软件二进制文件被“部署”时群集待确定的分类器，而不是在执行后检测它们。我们计划在 2022 年 6 月在 .conf22 上发布这项研究的数据集。我们鼓励研究人员调查该语料库，并验证我们的研究结果或在此基础上进行构建，以帮助全球蓝队队员社区。

重要研究结果

- 在我们的测试中，在 10 个勒索软件变种中，LockBit 勒索软件的加密速度最快，这与该勒索软件集团在其 Tor 网站上的声明一致。
- 勒索软件变种加密 98561 个文件 (53.83 GB) 的平均时间为 42 分 52 秒。
- 个别勒索软件样本加密速度差异很大，从四分钟到三个半小时不等。
- 改进的硬件功能为一些勒索软件样本提供了更快的加密速度。其他样本和变种无法利用增加的资源，有时它们在规格更高的系统上表现更差。额外的内存对任何样本的加密速度都没有显著影响。更高的磁盘速度可能在更快的执行中发挥作用，但最有可能的是与可以利用额外 CPU 内核的变种相结合。

简介

在 2021 年的 M-Trends 报告中，Mandiant 发现他们在 2020 年的调查中有 25% 涉及勒索软件，高于 2019 年的14%。[1]2021 年 Verizon 数据泄露调查报告 (DBIR) 指出，从 2019 年到 2021 年，勒索软件攻击的频率翻了一番。[2]尽管这种恶意软件在公众意识中相对较新，但自从 1989 年在一次 AIDS 会议上通过软盘首次出现以来，它就一直困扰着世界。[3]

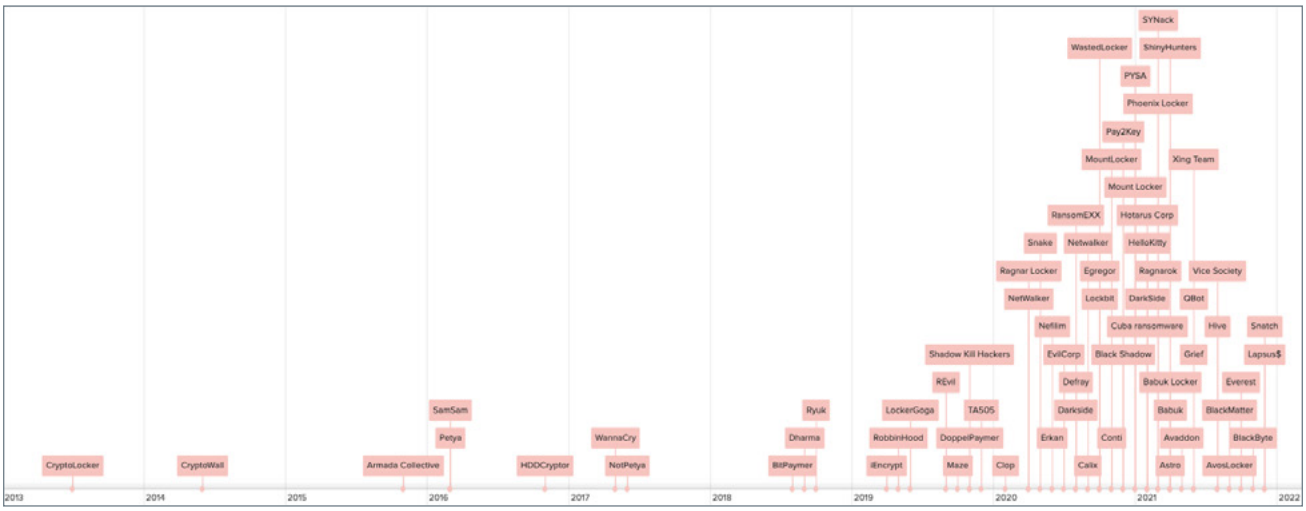

图 1.Spunk 图表突出显示了 2013 年至 2022 年勒索软件系列的增长情况。

前面提到的 M-Trends 报告指出，在美洲，勒索软件的平均停留时间为三天。[4]三天的停留时间听起来并不理想，但长期以来，人们一直认为勒索软件的停留时间更短，只有几个小时甚至几分钟。如果平均停留时间是以天而不是以小时来计算，防御者采取行动的机会很小。2021 年，CERT NZ 发布了一份白皮书，概述了勒索软件的生命周期，并提出了帮助组织应对这一日益增长的威胁的建议 (图 2) 。[5]

1. FireEye 和 Mandiant，“Fireeye-Rpt-Mtrends-2021.Pdf”，2021 年 4 月 13 日，13，https://www.mandiant.com/resources/m-trends-2021.
2. Verizon，“DBIR 2021 数据泄露调查报告”，2021 年 5 月 12 日，14，verizon.com/dbir.
3. “案例研究：AIDS 木马勒索软件”，SDxCentral，访问时间：2022 年 2 月 23 日，https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/.
4. FireEye 和 Mandiant，“M-Trends 2021”，14。
5. “勒索软件如何发生以及如何阻止它”，CERT NZ，访问时间：2022 年 1 月 29 日，https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/.

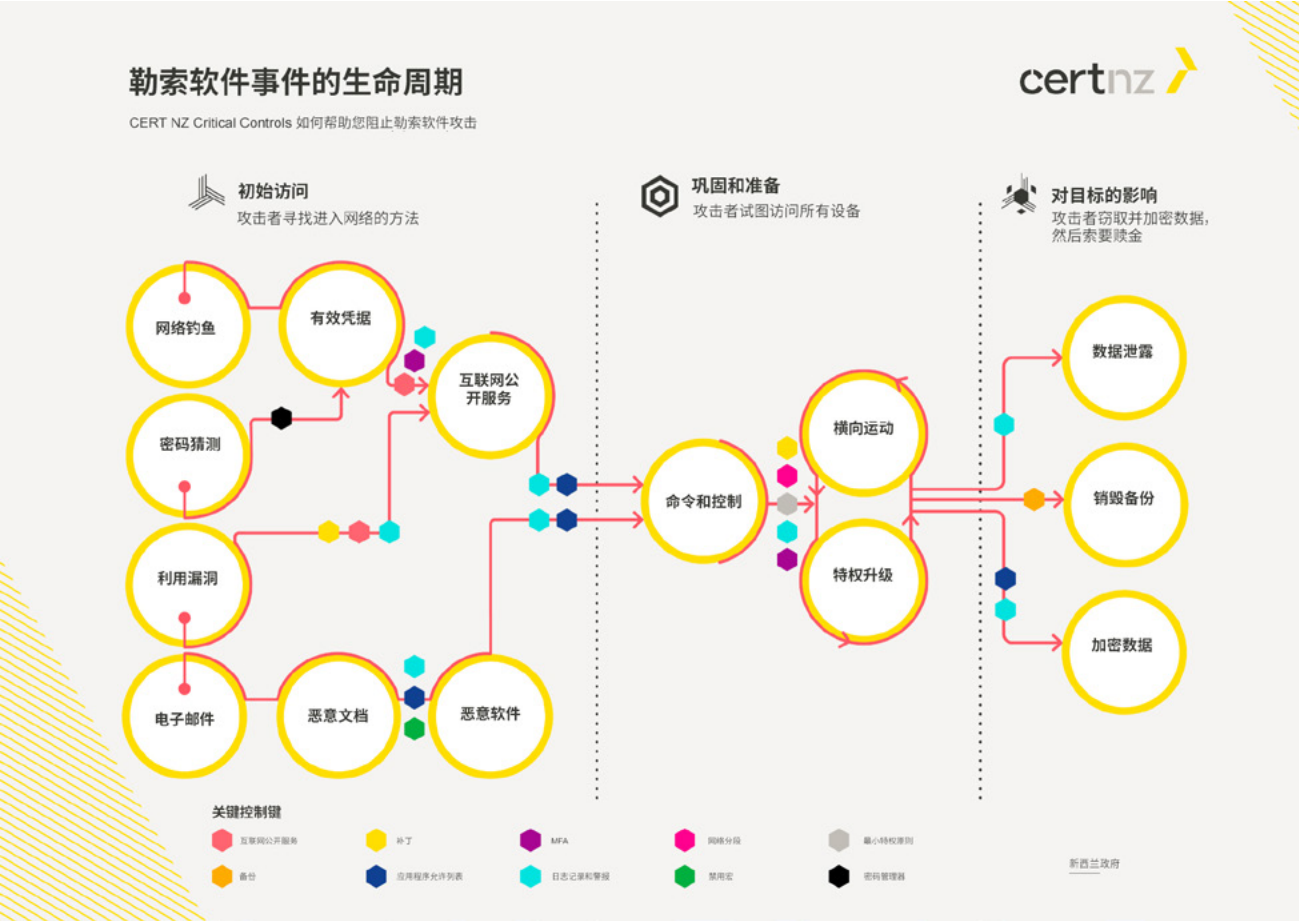

图 2.CERT NZ 发布的勒索事件详细进展。

CERT NZ 的这项工作和 Mandiant 引用的三天停留时间让我们质疑，组织如何积极防御勒索软件。在我们开始研究防御方法之前，我们决定首先研究两个问题：

- 首先，勒索软件病毒株加密一台主机需要多长时间？
- 组织能否恢复或阻止文件系统的完全加密？

逆向工程师已经做了大量工作来了解为什么一些勒索软件病毒株加密速度如此之快。除了 Lockbit 勒索软件组的一则宣传广告，我们找不到任何实证研究来比较不同勒索软件系列之间的加密速度。[6,7]本文概述了我们对 10 个勒索软件系列的动态评估加密速度的分析，并为蓝队队员提供了一些建议，以更好地通知他们的防御措施。应该注意的是，本文的目的不是创建勒索软件检测方法。相反，我们的目标是让防御者了解勒索软件加密速度的整体真相。

> 本文概述了我们对 10 个勒索软件系列的动态评估加密速度的分析，并为蓝队队员提供了一些建议，以更好地通知他们的防御措施。"

6. “LockBit BLOG”，访问时间：2022 年 2 月 13 日，http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd[.]onion.ly/conditions.
7. Gridinsoft LLC，“LockBit 勒索软件。最单纯和最快速的勒索软件”，Gridinsoft LLC，访问时间：2022 年 1 月 29 日，https://gridinsoft.com.

布置环境

我们开始用无限的问题来集思广益我们的假设，这些问题涉及勒索软件加密的速度有多快，以及如果勒索软件加密的速度比预期的快，组织如何才能“防患于未然”。[8]我们开始将我们的问题综合成一个单一的假设：**如果对手获得了系统的访问权并部署了勒索软件，那么加密的速度将会超过网络防御者实际能够阻止的速度**。Verizon·DBIR 指出，大多数组织在对手获得对系统的访问权几天后，而不是几个小时或几分钟后，才会检测到泄露行为。[9]为了测试我们的假设，我们需要创建一个实验室来进行重复测试，收集不同勒索软件二进制文件的样本，然后分析我们的研究结果。我们也希望以迎合蓝队队员的方式进行这项研究。因此，我们选择不对恶意软件二进制文件执行静态逆向工程工作，而是在受控环境中动态执行它们，并针对相同的变量对它们进行测量。我们计划在未来的博客、论文和会议报告中详细解释我们的方法和技术流程。

在白皮书的这一部分，我们将解释如何设计实验来测试我们的假设。我们还详细介绍了我们的恶意软件实验室的高级架构和配置，以及我们如何和为什么获取恶意软件。最后，我们列出了我们的研究和分析中任何已知的假设，这些假设可能会给我们的研究结果带来偏差。

方法学

为了测试我们的假设，我们需要在受控环境中执行各种勒索软件病毒株，从端点主机收集本机 Windows 性能遥测数据，并分析数据。我们选择了 10 个勒索软件系列，每个系列都有 10 个独立的二进制文件，以防止群集错觉，即倾向于看到不存在的模式，以及确认偏差，即倾向于寻找支持自己信念的信息。对于每种 Windows 端点类型和资源规格，我们为每个系列创建了单独的 Amazon Web Services (AWS) Virtual Private Cloud (VPC)，并且每个单独的二进制文件都在专门为其评估而创建的主机上运行。然后将结果转发到中央 Splunk 实例进行分析。每台主机都有 98561 个文件放在 100 个目录中。这些文件类型来源于数字语料库，并被作者视为最有可能被勒索软件二进制文件加密的文件类型。[10,11,12]这些文件在 CC0 许可证下提供，来源于美国政府的公共网站。最后，我们在 Windows 主机上启用了事件 ID 4663，以便查看文件的加密情况，并确定每个勒索软件系列的加密速度。[13]

8. John McHale，"保护国防部免受网络攻击，防患于未然 - 军用嵌入式系统"，访问时间：2022 年 1 月 30 日，http://militaryembedded.com/cyber/cybersecurity/defending-dod-from-cyberattacks-getting-to-the-left-of-the-boom.
9. Verizon，“DBIR 2021 数据泄露调查报告”，90。
10. Simson Garfinkel 等人，"用标准化的司法鉴定语料库将科学引入数字司法鉴定"，数字调查 6（2009 年 9 月）：S2–11, https://doi.org/10.1016/j.diin.2009.06.016.
11. “数字语料库下载：Corpora/Files/Govdocs1/By_type/”，访问时间：2022 年 1 月 30 日，https://downloads.digitalcorpora.org/corpora/files/govdocs1/by_type/.
12. “数字语料库下载：Corpora/Files/Govdocs1/Zipfiles/”，访问时间：2022 年 1 月 30 日，https://downloads.digitalcorpora.org/corpora/files/govdocs1/zipfiles/.
13. Microsoft，“4663(S) 试图访问对象。(Windows 10) - Windows 安全”，访问时间：2022 年 1 月 30 日，https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4663.

实验室

如前所述，该研究是针对在受控环境中执行的勒索软件二进制文件进行的。我们使用本机 Windows 审计和日志记录功能收集勒索软件的性能，并将结果转发回 Splunk 实例。实验程序部分更详细地描述了关于遥测设置的详细信息。每个勒索软件样本都在一个独立、自包含的环境中运行。每个勒索软件环境中的 Splunk 实例将事件转发到单个 Splunk 实例进行比较、分析和报告。我们通过为我们的实验修改 Splunk 的开源攻击范围工具来创建实验室（图 3）。[14]攻击范围允许网络防御者在 AWS 中使用 Splunk 软件动态创建小型网络，并使用 Terraform 和 Ansible 的组合预先配置日志记录。

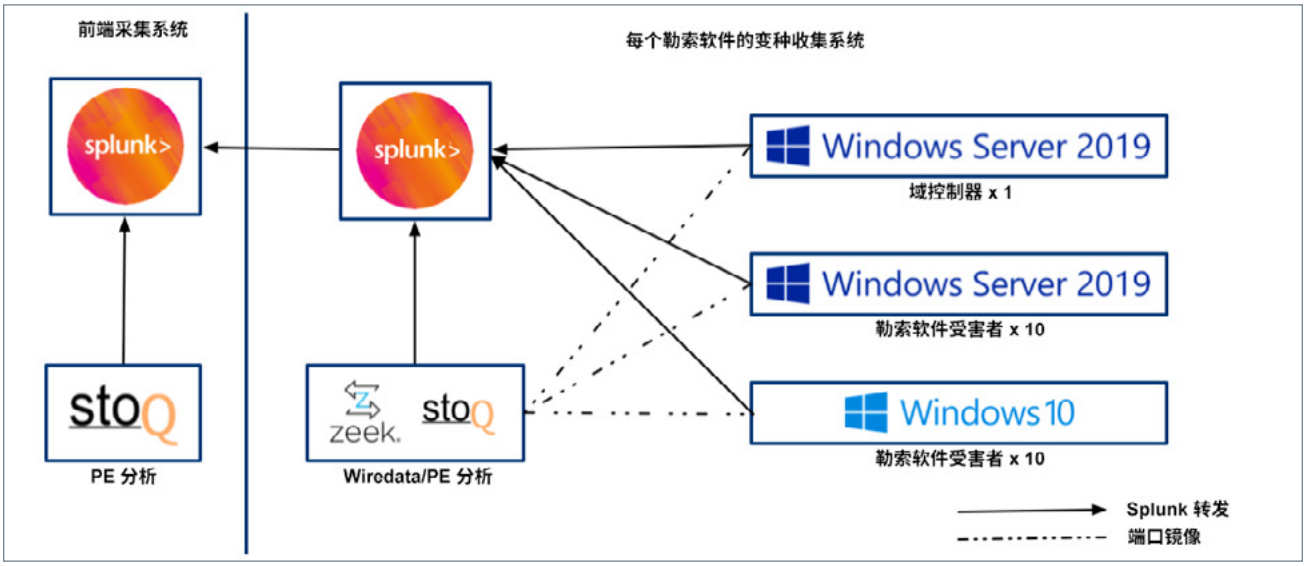

图 3.我们的自定义攻击范围的高级概述。

根据我们从组织和流行网站（例如 PC Mag）收集的轶事反馈，此范围内的主机规格符合许多现代笔记本电脑或服务器版本。[15]这些主机卸载了 Microsoft Defender，并且没有安装其他防病毒 (AV) 或端点检测和响应 (EDR) 工具。我们安装了额外的工具，包括 Splunk 代理，用于将信息发送回 Splunk 和 Microsoft 应用程序 Sysmon。[16] 最后，为了检测任何蠕虫或远程映射文件加密，我们这些主机加入到一个 Windows 域，在域控制器上有一个开放的网络共享（C 盘）。有关主机规格和日志记录配置的更多信息可在附录 A 和 B 中找到。为了捕获文件加密事件，我们对测试目录和所有子目录启用了对象级审计，包括成功和失败的访问尝试。通过启用对象级审计，每当勒索软件二进制文件试图加密文件时，都会生成事件代码 4663 事件。最后一个 4663 事件表明文件成功加密是“删除”，我们用它来跟踪加密速度。虽然在我们测试的所有系列中都发现了此事件，但此删除事件可能不会出现在其他系列中。在这种情况下，可能需要不同的标记来测量 TTE。

14.Splunk 攻击范围，Jinja（2019 年；再版，Splunk GitHub，2022 年），https://github.com/splunk/attack_range.
15.“Dell Latitude 7420 审查 | PCMag”，访问时间：2022 年 1 月 30 日，https://www.pcmag.com/reviews/dell-latitude-7420.
16.markruss，“Sysmon - Windows Sysinternals”，访问时间：2022 年 2 月 25 日，https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

实验程序

为了最好地模拟现代勒索软件活动，我们通过位于Windows Server 2019 域控制器上的远程 PowerShell 脚本，在 10 台 Windows 10 主机和 10 台 Windows Server 2019 主机上执行勒索软件。该远程 PowerShell 方法用于启动勒索软件感染，而不是用户必须手动执行二进制文件。该方法还有一个额外的好处，就是模拟了现代勒索软件活动，其中勒索软件是由操作员通过脚本执行的，而不是由受害者在桌面上执行。此外，它还减少了一些"人工交互"的开销，这使得勒索软件可以利用比其他方式更多的系统资源。当执行勒索软件时，我们没有向它传递任何标志。我们以不同方式执行的唯一勒索软件变种是 Babuk，因为它无法使用远程 PowerShell 方法可靠地运行，因此我们在每台主机上交互启动 Babuk。每个操作系统的两个不同硬件配置文件用于评估勒索软件的性能。附录 B 中提供了这些配置文件的准确规格。

PowerShell 脚本允许我们选择想要运行的勒索软件样本。然后，该脚本将遍历域中 Windows 10 或 Windows Server 2019 主机的数量，并通过远程 Web 服务器启动勒索软件二进制文件的下载。每次测试均在 Windows 10 或 Windows Server 主机上进行，不会同时在这两个主机上进行。

当每个主机上的下载完成时，PowerShell 脚本远程启动每个勒索软件二进制文件，Babuk 除外。然后，我们能够使用 Windows 安全事件日志分析每个变种加密文件的速度。需要事件代码 4663（试图访问对象）来可靠地捕获加密事件。我们对 Windows 10 和 Windows Server 2019 主机上的 100 个测试目录启用了文件系统审计，以便生成所需的事件日志。

勒索软件二进制文件

跨 10 个勒索软件系列的 100 个勒索软件样本来自 VirusTotal。我们仅利用了来自 VirusTotal 的 Microsoft Defender 检测来确定勒索软件系列的归属。选择这些勒索软件系列是因为它们在过去 12 到 24 个月中非常普遍（图 4）。

图 4.我们选择了 10 个勒索软件系列及其各自的毒株进行研究。

在附录 C 中，我们提供了在每个系列中测试的每个二进制文件的 VirusTotal 检测字符串和 SHA256 哈希。

结果

对于我们最初提出的勒索软件加密速度有多快的问题，答案显示了勒索软件系列之间的巨大差异。我们希望了解每个样本的加密速度和持续时间，以及各个系列本身的平均速度和持续时间。使用中值而不是平均值可以防止少数异常值扭曲特定系列的整体结果。

当我们在测试期间收集 Windows Perfmon 数据时，我们观察到一些系列比其他系列更好地利用了增加的系统资源。一些系列非常高效，而另一些则倾向于利用大部分 CPU 时间和非常高的磁盘访问率。使用大量系统资源的样本与更快的加密速度之间没有直接关系。 当部署在更快的测试系统上时，一些勒索软件系列的性能会变差，甚至崩溃。

在每个样本的基础上，在观察的 98561 个测试文件中，最快的加密时间是 4 分 9 秒。该加密操作由 lockbit-9.exe (133adb408a4837d3a20634d79baf01151061c49cd936e9a8787b91df8997b6b0) 在 Windows 2019 Server 高规格实例上执行 (图 5) 。

Variant	Endpoint	process_name	Duration	Encryptions_Per_Second
Lockbit	Server-2019-High	C:\ransom\lockbit-9.exe	00:04:09	396

图 5.来自 Windows 2019 Server 上部署的 lockbit-9.exe 示例的数据。

相反，对于相同的测试文件集，观察到的最慢加密时间是 3 小时 35 分 8 秒。该加密操作由 babuk-5.exe (1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff8c17032aa017f6075c02) 在 Windows 10 中等规格实例上执行 (图 6) 。

Variant	Endpoint	process_name	Duration	Encryptions_Per_Second
Babuk	Win-10-Mid	C:\ransom\babuk-5.exe	03:35:08	8

图 6.来自 Windows 10 实例上部署的 babuk-5.exe 示例的数据。

当我们查看每个测试系列的平均加密持续时间时，我们发现，尽管 Babuk 的单个样本是加密速度最慢的勒索软件，但 Babuk 系列作为一个整体是第二快的，持续时间为 6 分 34 秒。LockBit 速度仍然最快，为 5 分 50 秒。在每个系列的平均加密时间方面，最慢的是 Mespinoza(PYSA)，平均持续时间为 1 小时 54 分 54 秒。总体而言，所有勒索软件系列的平均加密持续时间为 42分 52 秒 (图 7) 。

系列	中值持续时间
LockBit	00:05:50
Babuk	00:06:34
Avaddon	00:13:15
Ryuk	00:14:30
Revil	00:24:16
BlackMatter	00:43:03
Darkside	00:44:52
Conti	00:59:34
Maze	01:54:33
Mespinoza (PYSA)	01:54:54
中位数的平均值	**00:42:52**

图 7.10 个勒索软件系列的加密持续时间中位数。

平均中值持续时间表明，一旦加密过程开始，对勒索软件攻击作出响应的时间窗口有限。考虑到最大的灾难可能来自于单个关键文件被加密，而不是受害者的全部数据被加密，这可以证明应对的时间更加有限。考虑到这些因素，一旦加密过程开始，对于大多数组织来说，减轻勒索软件攻击可能会非常困难，甚至不可能。虽然检测和防御能力超出了本研究的范围，但对于那些希望防御勒索软件攻击的组织来说，还有一线希望。

我们极力确保我们获取这些数据的方法不会影响我们收集的数据的结果。然而，对于这些工具（例如 Sysmon 和受约束的对象级审计）可能引入的延迟，我们对它们进行测量的能力有限。我们认为，这些工具不会导致任何显著的延迟，所以，也不会极大地改变我们的研究结果。未来专注于勒索软件加密速度的研究可能希望确保有一种方法来测量工具可能引入的延迟。最后，我们认识到，将勒索软件样本归属于“系列”可能很困难。为了确保本次研究在样本选择方面的一致性偏差，我们将每个样本的哈希与从 VirusTotal 获得的 Microsoft Defender 结果进行了比较。提取签名名称，然后进行规范化。然后，我们使用生成的规范化值来识别特定的勒索软件系列。

结论和进一步的工作

这项研究的目标是，根据经验评估常见勒索软件系列在各种操作系统和硬件规格下的加密速度，以确定组织是否能够及时做出反应，从而实现有效的缓解。根据我们的中值结果，我们的发现表明，通过勒索软件加密，在 43 分钟之内便会导致全部数据丢失。数据的加密和丢失是前面提到的 Lockheed Martin 网络杀伤链的“行动目标”。正如 Mandiant M-Trends 报告所发现的那样，43 分钟是一个极其有限的采取措施进行缓解的机会窗口，特别是考虑到检测入侵的平均时间是三天。因此，我们假定，许多组织不太可能防止勒索软件造成的数据完全丢失。如果组织希望防御勒索软件，很明显，他们需要在网络杀伤链上防患于未然，对入侵和漏洞进行检测，而不是针对行动目标。我们希望这项研究的发现可以帮助网络防御者更好地探索和识别潜在的缓解机会。还应注意的是，尽管我们将实验室配置为检测勒索软件样本的蠕虫行为，但大多数样本都没有这种行为。未来的研究将更深入地探索蠕虫行为。

我们的研究并不仅限于这项工作。我们计划在 Splunk BOSS 平台上发布这些信息，以支持值得探索的其他研究领域。更具体地说，我们希望评估勒索软件在加密文件时表现出的模式，勒索软件蠕虫行为，如何基于模糊哈希算法聚类相似的勒索软件二进制文件，以及未来随着时间的推移对勒索软件系列归属的分析。

鸣谢

像这样的研究不仅仅需要主要和次要调查人员去创造。特别感谢 Allie Mellen、Mark Harris、David French、Ryan Kovar、Audra Streetman、Marcus LaFerrera、Mick Baccio、Dave Herrald、Drew Church、Johan Bjerke、John Stoner、Tamara Chacon、Kelcie Bourne、Scott Roberts、Adam Swanda、Michael Haag 以及 Splunk 威胁研究团队 (STRT) 的《Splunk 攻击范围》一书的作者。

参考文献

- SDxCentral。“案例研究：AIDS 木马勒索软件。” 访问时间：2022 年 2 月 23 日。https://www.sdxcentral.com/security/definitions/case-study-aids-trojan-ransomware/.
- “Dell Latitude 7420 审查| PCMag” 访问时间：2022 年 1 月 30 日。https://www.pcmag.com/reviews/dell-latitude-7420.
- “数字语料库下载：Corpora/Files/Govdocs1/By_type/.” 访问时间：2022 年 1 月 30 日。https://downloads.digitalcorpora.org/corpora/files/govdocs1/by_type/.
- “数字语料库下载：Corpora/Files/Govdocs1/Zipfiles/.” 访问时间：2022 年 1 月 30 日。https://downloads.digitalcorpora.org/corpora/files/govdocs1/zipfiles/.
- FireEye 和 Mandiant。“Fireeye-Rpt-Mtrends-2021.Pdf”，2021 年 4 月 13 日。https://www.mandiant.com/resources/m-trends-2021.
- Garfinkel、Simson、Paul Farrell、Vassil Roussev 和 George Dinolt。"用标准化的司法鉴定语料库将科学引入数字司法鉴定。" 数字调查 6（2009 年 9 月）：S2–11. https://doi.org/10.1016/j.diin.2009.06.016.
- CERT NZ。“勒索软件如何发生以及如何阻止它。” 访问时间：2022 年 1 月 29 日。https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/.
- LLC, Gridinsoft。“LockBit 勒索软件。最单纯和最快速的勒索软件。” Gridinsoft LLC。访问时间：2022 年 1 月 29 日。https://gridinsoft.com.
- “LockBit 博客。” 访问时间：2022 年 2 月 13 日。http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion[.]ly/conditions.
- markruss。“Sysmon - Windows Sysinternals.” 访问时间：2022 年 2 月 25 日。https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.
- McHale, John。"保护国防部免受网络攻击，防患于未然 - 军用嵌入式系统。" 访问时间：2022 年 1 月 30 日。http://militaryembedded.com/cyber/cybersecurity/defending-dod-from-cyberattacks-getting-to-the-left-of-the-boom.
- Microsoft。“4663(S) 试图访问对象。(Windows 10) - Windows 安全。” 访问时间：2022 年 1 月 30 日。https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4663.
- Microsoft 安全情报。“木马：PowerShell/Redearps。威胁描述，“2021 年 3 月 24 日。https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:PowerShell/Redearps.A&threatId=-2147189091.
- Splunk 攻击范围。Jinja。2019 年。再版，Splunk GitHub，2022 年。https://github.com/splunk/attack_range.
- Symantec。“在攻击中对 POWERSHELL 的使用增加” Symantec Corporation，2016 年。https://docs.broadcom.com/doc/increased-use-of-powershell-in-attacks-16-en.
- Verizon。“DBIR 2021 数据泄露调查报告”，2021 年 5 月 12 日。verizon.com/dbir.

附录 A: Windows 日志记录配置

- 在 C:\Files\ 和所有子目录（目录 0-99）上启用 Windows 文件系统审计（事件代码 4633）。对修改文件的失败和成功尝试均启用该功能。
- 启用命令行日志记录的 Windows 进程创建（事件代码 4688）
- 安装 Sysmon，并使用 Olaf Hartong 提供的详细配置进行配置

附录 B: 主机规格

- Win-10-高- Windows 10, AWS m5.2xlarge (8 CPU/32GB RAM) 300GB HDD（3000 IOPS/125MB 吞吐量）
- Win-10-中- Windows 10, AWS m5.xlarge (4 CPU/16GB RAM) 300GB HDD（3000 IOPS/125MB 吞吐量）
- Server-2019-高- Windows Server 2019, AWS m5.4xlarge (16 CPU/64GB RAM) 300GB HDD（10000 IOPS/500MB 吞吐量）
- Server-2019-中- Windows Server 2019, AWS m5.2xlarge (8 CPU/32GB RAM) 300GB HDD（3000 IOPS/125MB 吞吐量）

附录 C: 勒索软件系列和二进制文件

二进制文件	SHA256 哈希	VirusTotal Vendor	VirusTotal 检测
avaddon-0.exe	078de7d019f5f1e546aa29af7123643bd250341af71506e6256dfee8f245a2a7	microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-1.exe	18c1ad49bf46b44df5926851ca30f00f6675c535b6826a3c779099643327ea33	microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-2.exe	288165763637cda27304d90bb7ec47e103dfb69fdf6c009d113b1f6852c091a0	microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-3.exe	3a040105b3cb704c838a87061dba6b03712d308636a438004300ec154de2d4d6	microsoft	Ransom:Win32/Avaddon.PD!MTB
avaddon-4.exe	4adc6cac6071cd67773c9cefab479f0ffde370c4cedac31b6db4de065c3ec7af	microsoft	Ransom:Win32/Avaddon.PD!MTB
avaddon-5.exe	572610a5033a2060afa67ddbfd7345013e82c6904dd7ace22cb6f0b0bedcb550	microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-6.exe	743079700007b64647d9ea4a0c361e6e981518ed06a5902ab9f275c38aa45c7b	microsoft	Ransom:Win32/Avaddon.MK!MTB
avaddon-7.exe	b9e62cb99e71c856cc41edfd837689993b7fc63c780e5786c34b2a8f63ef37b6	microsoft	Ransom:Win32/Avaddon.P!MSR
avaddon-8.exe	cc95a8d100f70d0fbf4af14e852aa108bdb0e36db4054c3f60b3515818a71f46	microsoft	Ransom:Win32/Avaddon.C!MTB
avaddon-9.exe	d8acd139f4f99b3137ab4cea9ef9e515e3a560f25a79666ac302f21d468340f8	microsoft	Ransom:Win32/Avaddon.PD!MTB
babuk-0.exe	04126b30c1c2663cdf2b6386781aedbfce2ef418a0b01de510bd536903f577e3	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-1.exe	049e53f72c8afa5ccb850429d55a00e2fbe799e68247fd13f5058146cf0f4cf8	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-2.exe	106118444e0a7405c13531f8cd70191f36356581d58789dfc5df3da7ba0f9223	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-3.exe	12c561ac827c3f79afff026b0b1d3ddec7c4b591946e2b794a4d00c423b1c8f8	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-4.exe	1b04e1fbddfcdb16a3d103e50261937815668d92d4909a15352dd5e2615adbf4	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-5.exe	1b9412ca5e9deb29aeaa37be05ae8d0a8a636c12fdff8c17032aa017f6075c02	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-6.exe	1f37064ff61211d7a0d0428af856323bafb734b3f8b0e44d04e8e0db872349ee	microsoft	Ransom:Win32/Babuk.MAK!MTB

二进制文件	SHA256 哈希	VirusTotal Vendor	VirusTotal 检测
babuk-7.exe	245e191bfe998ad9ef2d6b169af22f3c290e9950234f8ddd0f4a03cb3eebf761	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-8.exe	2509e5a4535d25110663a698410847aa0cb9ce734722076ada4c651532f318a5	microsoft	Ransom:Win32/Babuk.MAK!MTB
babuk-9.exe	25835a890a218fd26bfd8b23696576402b5eb8a4c9af4a51529e14c4f00a9cce	microsoft	Ransom:Win32/Babuk.MAK!MTB
blackmatter-0.exe	8eada5114fbbc73b7d648b38623fc206367c94c0e76cb3b395a33ea8859d2952	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-1.exe	26a7146fbed74a17e9f2f18145063de07cc103ce53c75c8d79bbc5560235c345	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-2.exe	2aad85dbd4c79bd21c6218892552d5c9fb216293a251559ba59d45d56a01437c	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-3.exe	496cd9b6b6b96d6e781ab011d1d02ac3fc3532c8bdd07cae5d43286da6e4838d	microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-4.exe	b4b9fdf30c017af1a8a3375218e43073117690a71c3f00ac5f6361993471e5e7	microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-5.exe	6d4712df42ad0982041ef0e2e109ab5718b43830f2966bd9207a7fac3af883db	microsoft	Ransom:Win32/BlackMatter.MAK!MTB
blackmatter-6.exe	be5bc29f58b868f4ff8cd66b4526535593e515a697bb8951c625bdfed13cccb7	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-7.exe	ed47e6ecca056bba20f2b299b9df1022caf2f3e7af1f526c1fe3b8bf2d6e7404	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-8.exe	7a223a0aa0f88e84a68da6cde7f7f5c3bb2890049b0bf3269230d87d2b027296	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
blackmatter-9.exe	9bae897c19f237c22b6bdc024df27455e739be24bed07ef0d409f2df87eeda58	microsoft	Ransom:Win32/BlackMatter.PAB!MTB
conti-0.exe	004ede55a972e10d9a21bcf338b4907d6eed65bf5ad6abbbd5aec7d8484bdedf	microsoft	Ransom:Win32/Conti.SD!MTB
conti-1.exe	17ac91a36237d8f37dcee961ba74c9310a45c009780ea092c3a1e428870ff8a1	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-2.exe	34366c9a9ac34dd9016abd406cffe713a3e8606e8600e6cb07e0242904f91a5b	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-3.exe	49dc5a243d322cd4d467e5f24b61ff749869564ddcf6a2f700839cf5ae9e37ea	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-4.exe	0b0b902af452e1c949a609a3b29a9de21dac639846c77427de06e6e63c1fe904	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-5.exe	73bd8c2aa71f5dcd9d2ddd79e53656c6ae3db2535e08cf9dab1cd13bdd6d5ea3	microsoft	Ransom:Win32/CONTI.DC!MTB
conti-6.exe	8df9b346bf591629a9eb0bf9f32c545a1266873495ceec9ba990be1dd22b9aa9	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-7.exe	0ffbc914e3bb09df586a93e5a5a557d03c5fcce7e8ee4a36bd3a09b8ed429c7a	microsoft	Ransom:Win32/Conti.SD!MTB
conti-8.exe	d43b52e3453ce77d2694a239232f39341a98fa704954a558125e74a85f22a346	microsoft	Ransom:Win32/Conti.MAK!MTB
conti-9.exe	1201e76d42f85feb89d64e6fd497144ed3afe66281b2464e84f3b889f2867c9b	microsoft	Ransom:Win32/Conti.MAK!MTB
darkside-0.exe	22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6	microsoft	Ransom:Win32/DarkSide!MSR
darkside-1.exe	2c323453e959257c7aa86dc180bb3aaaa5c5ec06fa4e72b632d9e4b817052009	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-2.exe	45ecce9dfec886e2b092a996f6affb9e7417d6121e58b0ec643be7e36a03106d	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-3.exe	7f6dd0ca03f04b64024e86a72a6d7cfab6abccc2173b85896fc4b431990a5984	microsoft	Ransom:Win32/DarkSide!MSR
darkside-4.exe	84af3f15701d259f3729d83beb15ca738028432c261353d1f9242469d791714f	microsoft	Ransom:Win32/Darkside.PAB!MTB

二进制文件	SHA256 哈希	VirusTotal Vendor	VirusTotal 检测
darkside-5.exe	c6e2ef30a86baa670590bd21acf5b91822117e0cbe6060060bc5fe0182dace99	microsoft	Ransom:Win32/Darkside.PAB!MTB
darkside-6.exe	2c1e20a4b38634b97de398246bc3c8082d47663702a46bb885dc7fcc5f71daa1	microsoft	Ransom:Win32/DarkSide!MSR
darkside-7.exe	43e61519be440115eeaa3738a0e4aa4bb3c8ac5f9bdfce1a896db17a374eb8aa	microsoft	Ransom:Win32/DarkSide!MSR
darkside-8.exe	533672da9d276012ebab3ce9f4cd09a7f537f65c6e4b63d43f0c1697e2f5e48d	microsoft	Ransom:Win32/DarkSide.DA
darkside-9.exe	5da3e6b4bea1eaceddb048a4a6bd702291189f42d15c4b2670de78984329b0a9	microsoft	Ransom:Win32/DarkSide.DA
lockbit-0.exe	00ad914476509f84b40f2dbe804dc7c37a1a24ef3472674574d3367079bf0a2a	microsoft	Ransom:Win32/Lockbit.STA
lockbit-1.exe	04f65270c92dda82c759c1eee49cf8f4c98a2ed0071272e49132331fda482dba	microsoft	Ransom:Win32/Lockbit.STA
lockbit-2.exe	082f91d85c437f415cea44b36afb4198da07b78593c836a398cd96365166e7d8	microsoft	Ransom:Win32/Lockbit.STA
lockbit-3.exe	50d08c974f7abce2da5c2a8976d3c6017334a418359d7bb031bd0914b848b24a	microsoft	Ransom:Win32/Lockbit.STA
lockbit-4.exe	0cd33e6b180862072a00a0c2f897afa754df071bcec3d13e581c41a5c27a3102	microsoft	Ransom:Win32/Lockbit.STA
lockbit-5.exe	7a1fb0eac9b62ce510030f9ff983d9d6225fd8dad6f05c1051c335aca87ffa24	microsoft	Ransom:Win32/Lockbit.STA
lockbit-6.exe	0d4966b4724f141adb7a7db1d9ae48f5c293c6049cc7f949220256c2e72ab5ac	microsoft	Ransom:Win32/Lockbit.STA
lockbit-7.exe	bb736c8d3dd2b3ebcacd3e2a61f95b20d23bc981cc22888dff88cfd2e720ee99	microsoft	Ransom:Win32/Lockbit.STA
lockbit-8.exe	d68cad561a949648a84ffc2f2db186f585cd4a90951eea91c1c100d996cb3688	microsoft	Ransom:Win32/Lockbit.STA
lockbit-9.exe	133adb408a4837d3a20634d79baf01151061c49cd936e9a8787b91df8997b6b0	microsoft	Ransom:Win32/Lockbit.STA
maze-0.exe	f03172bd32ed16df6dda8e8146d24b073b864da59d669218fcc5e97835a5e956	microsoft	Ransom:Win32/Maze.PA!MTB
maze-0.exe	f03172bd32ed16df6dda8e8146d24b073b864da59d669218fcc5e97835a5e956	microsoft	Ransom:Win32/Maze.PA!MTB
maze-1.exe	0b9c99276ed36110afc58b3fb59ada135146180189c25d99618ca5897537ee21	microsoft	Ransom:Win32/Maze.PA!MTB
maze-2.exe	2a6c602769ac15bd837f9ff390acc443d023ee62f76e1be8236dd2dd957eef3d	microsoft	Ransom:Win32/Maze.PA!MTB
maze-3.exe	b3473d205ba722e229f49002093b61fc35902e1a67bcd558bf9a7811278e5cb2	microsoft	Ransom:Win32/Maze.PA!MTB
maze-4.exe	5a06ae8540d5a0d7fb88e80d3e61c3a6079f3abdafe998ce70ffdcac9e940520	microsoft	Ransom:Win32/Maze.PA!MTB
maze-5.exe	877c439da147bab8e2c32f03814e3973c22cbcd112d35bc2735b803ac9113da1	microsoft	Ransom:Win32/Maze.PA!MTB
maze-6.exe	9d86beb9d4b07dec9db6a692362ac3fce2275065194a3bda739fe1d1f4d9afc7	microsoft	Ransom:Win32/Maze.PA!MTB
maze-8.exe	e45eacf5158bb2aa11f29f0675b4cb68dbf7e376569516fe33f84be524c67763	microsoft	Ransom:Win32/Maze.PA!MTB
maze-9.exe	ecd04ebbb3df053ce4efa2b73912fd4d086d1720f9b410235ee9c1e529ea52a2	microsoft	Ransom:Win32/Maze.PA!MTB
mespinoza-0.exe	0433efd9ba06378eb6eae864c85aafc8b6de79ef6512345294e9e379cc054c3d	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-1.exe	0f0014669bc10a7d87472cafc05301c66516857607b920ddeb3039f4cb8f0a50	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-2.exe	164cb8e82d7e07cca0409925cadd8be5e3e8e07db88526ff7fe87596c6a6bd07	microsoft	Ransom:Win32/Aurora.SIB!MTB

二进制文件	SHA256 哈希	VirusTotal Vendor	VirusTotal 检测
mespinoza-3.exe	4dc802894c45ec4d119d002a7569be6c99a9bba732d0057364da9350f9d3659b	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-4.exe	1e2009549452ed6b524b94ed683079ee60c2b9542b1bfd5b9ee42e9161d5e7c8	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-5.exe	327934c4c11ba37f42a91e1b7b956d5a4511f918e63047a8c4aa081fd39de6d9	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-6.exe	425945a93beb160f101d51de36363d1e7ebc45279987c3eaf5e7f183ed0a3776	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-7.exe	44f1def68aef34687bfacf3668e56873f9d603fc6741d5da1209cc55bdc6f1f9	microsoft	Ransom:Win32/Aurora.SIB!MTB
mespinoza-8.exe	4770a0447ebc83a36e590da8d01ff4a418d58221c1f44d21f433aaf18fad5a99	microsoft	Ransom:Win32/Filecoder.PD!MTB
mespinoza-9.exe	48355bd2a57d92e017bdada911a4b31aa7225c0b12231c9cbda6717616abaea3	microsoft	Ransom:Win32/Filecoder.PD!MTB
revil-0.exe	d74cd044351030290f6ad8f70f91d51b6c39675ca3c70c45b5b0c5bd09589ff6	microsoft	Ransom:Win32/Revil.A
revil-1.exe	338e8f24eeb38b5ef67ef662b65d592c816eba94dfaaac856021dac407daf294	microsoft	Ransom:Win32/Revil.A
revil-2.exe	ab53e6823e47b446a245374c7760006ee84c8ea457a5fe9ca9df4732bf55a32a	microsoft	Ransom:Win32/Revil.A
revil-3.exe	73dd3cb487dfb863304d9f6d79f60b2ab4adbd162e460a2210b4a6abf049ea53	microsoft	Ransom:Win32/Revil.B
revil-4.exe	151271bf05310f94cd33cba3eb90be264edc4828c04e4e82f492b8e2576ee7a6	microsoft	Ransom:Win32/Revil.B
revil-5.exe	97f905bb24c5054d09fe79a20e04fe84042ad985b5c6e09afad21efa83dcd7a0	microsoft	Ransom:Win32/Revil.A
revil-6.exe	19f1a30555b83f23acc245ef6fe745f3292ef015c71abef8daa077e31f259179	microsoft	Ransom:Win32/Revil.B
revil-7.exe	1f7b15f6cf07c5943ce8ab5bfd0700e4919808fca4260ffd2a509100d45fadaf	microsoft	Ransom:Win32/Revil.B
revil-8.exe	1fb842e87f23e37ab39e201a024845c323c3d239331768db694dca96ed53d8c7	microsoft	Ransom:Win32/Revil.B
revil-9.exe	21bcb9c0095424a179399379939f6ebdf1dfe202825c1ca5acdd25a8f751402f	microsoft	Ransom:Win32/Revil.A
ryuk-0.exe	487d4698c6c938ca3e9251827a5813ddd21e26584b3459d768e457ddd4e8c4d4	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-1.exe	4cb0bf61d61ad3383636df11b3e4da8e67bb0acea03e981ecdd48d08ed8c796c	microsoft	Ransom:Win32/Ryuk.AA
ryuk-2.exe	dea1b54618643ffe59506398f0f131300abe0988da89b5414955843ae5b53fee	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-3.exe	0cf36731f5b8651d53fc651607c3fccac24b631c08dca4493d8e07d2fbff1db3	microsoft	Ransom:Win32/Ryuk.AA
ryuk-4.exe	8027a5e9dfcb379592868fb61fd8ed5f1605f0e4460db53d23a859d2a9743b91	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-5.exe	d4b8cbfa94bac3dbd58452fcc6c4e0b56b65a54a671a2184d9fb6e3694a0266f	microsoft	Ransom:Win32/Ryuk.DB!MTB
ryuk-6.exe	ba595e53ea6b0ef7f3332c2fec6a644c3cbc9756d2978c49e69eba92526904d8	microsoft	Ransom:Win32/Ryuk.B
ryuk-7.exe	fc4d44faf906e7a6ba133dae5f33ce22b8569943574ffccadd0292b12abcc8fa	microsoft	Ransom:Win32/Ryuk.AS!MTB
ryuk-8.exe	fe55650d8b1b78d5cdb4ad94c0d7ba7052351630be9e8c273cc135ad3fa81a75	microsoft	Ransom:Win32/Ryuk
ryuk-9.exe	568d73074880063d4d2b3e9d3ddb938685de8ec8e24974ff32f5f47d55a2dcb0	microsoft	Ransom:Win32/Ryuk

附录 D: 可加密文件类型语料库

扩展名	计数	总大小 (MB)
html	25364	1,589.66
pdf	25185	15,116.11
txt	14856	12,632.61
doc	7955	5,019.95
jpg	7095	1,020.12
ppt	5576	11,044.64
xls	4238	4,384.81
gif	2010	114.83
ps	1186	2,024.57
csv	1005	224.24
xml	918	137.19
gz	794	435.43
log	514	622.12
unk	433	63.2
png	317	19.12
text	184	136.18
dbase3	170	3.03
f	129	14.11
rtf	128	31.35
eps	67	14.23
pps	65	164.05
swf	43	20.41
wp	42	4.2
fits	39	58.58
tex	36	2.25

扩展名	计数	总大小 (MB)
java	36	1.24
kml	32	4.03
kmz	28	2
pptx	21	75.78
troff	21	1.9
bmp	13	5.23
docx	13	0.85
sgml	9	0.22
sql	7	0.46
hlp	7	0.02
dwf	5	0.56
gls	5	0.02
tmp	4	0.9
data	2	0.77
无扩展名	1	124.94
zip	1	0.84
vrml	1	0.32
wk1	1	0.31
py	1	0.23
ttf	1	0.12
g3	1	0.12
xlsx	1	0.05
pub	1	0.000049
	98,561 个文件	**总计 53.83 GB**

附录 E: 端点性能研究结果

Windows Server 2019 高规格

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Server-2019-High	95.52	96.18	61.64	628.67	67.62	8	167890.42	54246.70	55118.46	17.28	227.62	26.13
Babuk	Server-2019-High	34.82	99.74	99.36	452.19	67.89	8	3853.88	28099.74	26860.70	25.72	178.65	19.27
Blackmatter	Server-2019-High	8.25	11.90	5.47	313.81	35.74	10	1962.33	10263.18	10283.99	12.70	117.03	16.99
Conti	Server-2019-High	6.88	12.97	8.59	257.58	18.58	8	343.72	11532.70	11492.30	164.83	237.50	17.46
Darkside	Server-2019-High	6.94	21.29	16.21	311.21	35.54	10	1670.40	8721.45	8731.53	12.00	113.81	16.41
Lockbit	Server-2019-High	27.02	41.55	15.94	502.12	28.07	8	1531.18	1237.26	1399.21	7.79	110.66	19.06
Maze	Server-2019-High	4.29	5.88	4.40	365.64	3.38	8	2086.59	13216.13	4831.49	4.19	86.45	16.28
Mespinoza	Server-2019-High	5.76	7.54	4.97	153.03	2.03	8	64.42	8191.90	6142.31	3.48	47.67	8.07
Revil	Server-2019-High	7.06	18.38	13.29	243.36	35.16	8	2425.00	14108.76	14068.99	11.61	105.26	15.01
Ryuk	Server-2019-High	53.31	86.33	20.02	171279.74	53.82	8	2931.32	62045.03	82201.84	181.45	296.14	102.16

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Server-2019-High	43868	7.58	5787.00	53.9
Babuk	Server-2019-High	98560	5.55	17760.00	166
Blackmatter	Server-2019-High	98553	37.41	2635	24.55
Conti	Server-2019-High	98560	64.07	1538	14.34
Darkside	Server-2019-High	98553	43.60	2260	21.07
Lockbit	Server-2019-High	98548	5.30	18622	173
Maze	Server-2019-High	98560	86.53	1139	10.62
Mespinoza	Server-2019-High	97080	102.55	946.70	8.824
Revil	Server-2019-High	98553	27.25	3618	33.71
Ryuk	Server-2019-High	89521	8.92	9266	93.6

Windows Server 2019 中等规格

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Server-2019-Mid	95.42	97.16	51.46	467.96	35.69	8	166866.12	44362.49	45706.62	14.84	140.11	23.97
Babuk	Server-2019-Mid	29.07	160.58	147.78	380.75	36.21	8	2985.14	21796.16	20907.03	17.95	133.61	16.87
Blackmatter	Server-2019-Mid	7.40	9.33	4.55	313.49	19.62	10	1688.89	8863.80	8850.98	11.45	95.38	16.49
Conti	Server-2019-Mid	7.10	12.33	7.93	241.00	10.41	8	117.35	10851.88	10881.95	83.15	145.91	16.57
Darkside	Server-2019-Mid	6.23	18.67	14.12	332.28	19.48	10	1495.22	7732.50	7725.44	10.86	95.34	16.22
Lockbit	Server-2019-Mid	22.40	33.26	13.45	458.79	18.10	8	1205.07	975.23	1092.23	7.02	96.55	18.76
Maze	Server-2019-Mid	4.02	4.94	3.95	333.54	4.46	8	1572.07	10751.79	3887.37	3.46	68.76	13.73
Mespinoza	Server-2019-Mid	5.39	6.70	4.65	153.03	2.02	8	80.30	6782.18	5023.70	3.55	47.27	8.11
Revil	Server-2019-Mid	6.62	17.54	12.86	254.25	19.30	8	2147.04	12687.87	12605.01	11.11	86.37	15.27
Ryuk	Server-2019-Mid	41.19	59.49	14.45	218856.14	53.61	8	1965.13	38545.07	56935.97	182.73	300.70	102.88

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Server-2019-Mid	50307	8.75	5749.00	53.6
Babuk	Server-2019-Mid	98560	6.51	15140.00	141
Blackmatter	Server-2019-Mid	98553	43.18	2283	21.27
Conti	Server-2019-Mid	98560	67.60	1458	13.59
Darkside	Server-2019-Mid	98553	50.47	1953	18.20
Lockbit	Server-2019-Mid	98548	6.76	14594	136
Maze	Server-2019-Mid	98560	114.75	858.94	8.006
Mespinoza	Server-2019-Mid	97080	124.55	779.48	7.265
Revil	Server-2019-Mid	98553	29.56	3336	31.07
Ryuk	Server-2019-Mid	93014	12.67	7289	68.4

Windows 10 高规格

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Win-10-High	68.96	77.37	31.62	457.12	37.10	8	88500.41	28297.32	28647.71	15.05	168.35	23.63
Babuk	Win-10-High	38.54	94.00	93.48	376.90	37.86	8	3189.90	21838.42	21783.18	19.83	151.92	17.53
Blackmatter	Win-10-High	6.74	8.91	4.58	299.34	21.56	10	1598.82	8358.30	8351.87	10.45	108.34	15.39
Conti	Win-10-High	7.95	15.24	9.83	228.03	11.32	8	261.15	12402.19	12389.49	83.23	167.86	15.25
Darkside	Win-10-High	6.90	20.24	15.05	393.16	23.78	10	1665.17	8488.67	8470.35	10.75	114.21	17.02
Lockbit	Win-10-High	28.78	44.13	17.42	498.25	24.38	8	1440.13	1251.17	1417.23	9.20	119.75	20.38
Maze	Win-10-High	4.10	5.00	3.91	323.62	5.11	8	1564.34	10369.55	3806.94	3.70	85.59	14.08
Mespinoza	Win-10-High	6.23	7.29	4.68	144.07	2.24	8	147.27	7219.82	5397.70	3.58	61.30	8.30
Revil	Win-10-High	8.09	21.70	15.75	252.97	19.27	8	2732.09	17054.07	16986.81	10.48	100.22	14.25
Ryuk	Win-10-High	43.93	56.51	11.68	106061.45	64.46	8	1941.94	33521.11	41399.72	182.68	326.10	103.71

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Win-10-High	98560	14.10	6990.00	65.2
Babuk	Win-10-High	98560	6.52	15130.00	141
Blackmatter	Win-10-High	98553	45.23	2179	20.31
Conti	Win-10-High	98560	58.30	1691	15.76
Darkside	Win-10-High	98553	45.38	2172	20.24
Lockbit	Win-10-High	98548	5.40	18259	170
Maze	Win-10-High	98560	115.45	853.71	7.957
Mespinoza	Win-10-High	97080	115.60	839.83	7.828
Revil	Win-10-High	98553	23.70	4160	38.76
Ryuk	Win-10-High	98284	17.17	5740	53.37

Windows 10 中等规格

Endpoint Specifications

Endpoint	OS	CPU Cores	GB RAM	Disk IOPS	Disk Throughput MB/s
Win-10-Mid	Windows 10	4	16	3000	125
Win-10-High	Windows 10	8	32	3000	125
Server-2019-Mid	Windows Server 2019	8	32	3000	125
Server-2019-High	Windows Server 2019	16	64	10000	500

Median Resource Utilization

Variant	Endpoint	%_Privileged_Time	%_Processor_Time	%_User_Time	Handle_Count	Thread_Count	Priority	Page_Faults/sec	IO_Read_KBytes/sec	IO_Write_KBytes/sec	Private_MBytes	Virtual_MBytes	Working_Set(MBytes)
Avaddon	Win-10-Mid	84.53	88.58	35.93	376.26	21.10	8	109298.88	31681.35	31810.25	8.82	145.11	18.33
Babuk	Win-10-Mid	28.88	92.38	91.30	342.77	21.67	8	2573.52	18024.88	17406.98	14.48	124.84	15.87
Blackmatter	Win-10-Mid	7.09	9.93	5.65	299.84	14.13	10	1713.94	9098.79	9079.02	9.82	98.72	14.88
Conti	Win-10-Mid	8.03	15.45	9.92	219.44	7.29	8	67.98	12578.51	12631.15	42.55	122.58	14.83
Darkside	Win-10-Mid	7.05	21.41	15.69	393.82	15.86	10	1647.89	8560.02	8550.47	10.30	104.35	16.85
Lockbit	Win-10-Mid	28.65	42.79	15.75	533.11	16.01	8	1319.68	1149.89	1246.13	10.74	111.46	20.72
Maze	Win-10-Mid	4.29	5.31	4.06	318.91	5.09	8	1561.72	10573.49	3707.72	3.63	82.95	13.79
Mespinoza	Win-10-Mid	6.39	7.56	4.79	144.08	2.23	8	137.56	7402.86	5527.32	3.58	61.26	8.23
Revil	Win-10-Mid	8.44	22.78	15.96	253.35	12.48	8	2710.56	16585.00	16521.51	9.70	91.44	14.05
Ryuk	Win-10-Mid	43.86	54.72	12.19	126006.82	63.22	8	1599.03	33496.12	41261.27	182.21	322.15	95.17

Median Encryption Speeds

Variant	Endpoint	Total_Encryptions	Duration_In_Minutes	Encryptions_Per_Minute	Encryption_Speed_MB_Per_Second
Avaddon	Win-10-Mid	98560	12.63	7804.00	72.7
Babuk	Win-10-Mid	98560	7.84	12580.50	117
Blackmatter	Win-10-Mid	98553	42.92	2297	21.40
Conti	Win-10-Mid	98560	59.34	1661	15.48
Darkside	Win-10-Mid	98553	44.72	2204	20.54
Lockbit	Win-10-Mid	98548	5.84	16881	157
Maze	Win-10-Mid	98560	115.12	856.19	7.980
Mespinoza	Win-10-Mid	97080	114.20	850.09	7.924
Revil	Win-10-Mid	98553	23.67	4166	38.81
Ryuk	Win-10-Mid	87739	16.98	5270	48.15

关于 SURGe

SURGe 成立于 2021 年 10 月，是 Splunk 的战略网络安全研究部门，致力于研究、应对和宣传影响世界的网络威胁。作为值得信赖的顾问，SURGe 通过研究论文、会议论文和网络研讨会中的响应指南和深入分析，在高知名度、时间敏感的网络攻击期间为组织提供技术指导。组织可以依靠 SURGe 提供适当的背景信息和及时的建议，自信而明智地应对全球安全事件。了解更多信息。

Splunk、Splunk> 和 Turn Data Into Doing 是 Splunk Inc. 在美国和其他国家/地区的商标和注册商标。所有其他品牌名称、产品名称或商标均属于其各自所有者。©2022 Splunk Inc.保留所有权利。

22-23023-Splunk-EmpiricallyComparativeAnalysisofRansomwareBinaries-A4-WP-101