互联网现状
第 09 卷 | 第 04 期

勒索软件异常活跃

亚太地区及日本概况

Akamai

目录

报告的关键见解

《亚太地区及日本概况》是我们更全面的 SOTI 勒索软件报告《勒索软件异常活跃：漏洞利用技术花样翻新，零日漏洞深受黑客青睐》（仅提供英文版）的补充篇。请参阅该报告中的详细分析，了解勒索软件团伙的攻击趋势、攻击方法和攻击技术；攻击阶段描述、对应解决方案、保障贵公司安全的建议；以及我们的研究方法。

概述

勒索软件持续对企业造成重大破坏，并造成更多人深受其害，原因包括攻击者在不断升级和改变攻击技术，引入新的勒索方法，并利用不断扩大的攻击面以及受害者安全预算有限造成的防御不足。勒索软件团伙在攻击环境中占据主导地位，越来越多的相关攻击得逞，这样的现状充分体现了这些危险趋势的影响。在亚太地区及日本 (APJ)，相关的例证为：2021 年第 4 季度到 2022 年第 4 季度受害公司数量增长 50%，并且相较于 2022 年第 1 季度，2023 年第 1 季度的受害公司数量同比激增 204%。

在本期 APJ 概况中，我们分享了更多见解，帮助您更好地防范这一日益尖锐的问题并实施更好的风险管理，相关见解包括：

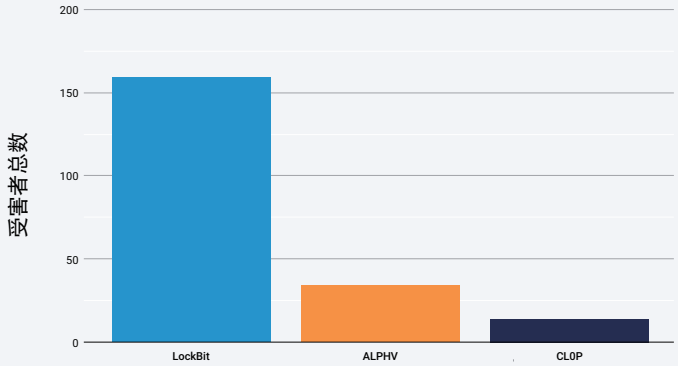
- 在 2021 年 10 月到 2023 年 5 月期间，LockBit 在勒索软件攻击活动中占主导地位，而 CL0P 因积极利用漏洞而迅速崛起。攻击技术发生变化，从网络钓鱼攻击转变为猖獗的零日漏洞和一日漏洞滥用，导致受害者数量大幅增加。
- 与全球范围的调查结果一致，制造业已成为受害企业数量最多的垂直行业，商业服务业紧跟其后。
- 勒索软件受害者大多数是规模较小的企业，收入不超过 5 千万美元。但超大规模的企业也会遭受攻击。

LockBit 成为勒索软件团伙活动中的主导

尽管人们对勒索软件的认知度不断提高，市面上可用于应对这一威胁的工具和最佳实践层出不穷，但在 2021 年第 4 季度至 2022 年第 4 季度期间，APJ 区域受害公司的数量增加了 50%，相较于 2022 年第 1 季度，2023 年第 1 季度的受害公司数量同比激增 204%。与我们全球报告中的数据结果一致，2021 年 10 月 1 日至 2023 年 5 月 31 日期间，受害者遭受的攻击以 LockBit 为主，此攻击在 APJ 区域所有攻击中占到 51% 的比例，与 ALPHV 和 CL0P 共同占据攻击排名榜的前三位（APJ 图 1）。

APJ 区域：按受害者数量排名的前三大勒索软件团伙

2021 年 10 月 1 日 – 2023 年 5 月 31 日



APJ 图 1：在 APJ 区域，勒索软件攻击受害企业中大多数遭受的是 LockBit、ALPHV 和 CL0P 的攻击

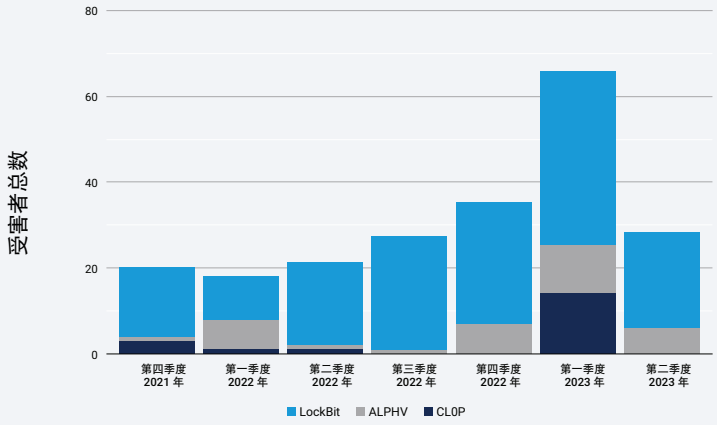
季度分析

在 2021 年第 4 季度至 2022 年第 2 季度期间，LockBit 堪称猖獗，但 CL0P 勒索软件的活跃度也非常高，这类勒索软件在 2023 年第 1 季度出现激增，缩小了与 ALPHV 的距离，而该勒索软件团伙也因此在 APJ 区域活跃度排名榜上跃升至第三位（APJ 图 2）。CL0P 活动量激增可归因于它利用各种零日漏洞作为切入点。在过去六个月中，攻击技术从网络钓鱼攻击转变为猖獗的漏洞滥用，导致受害者数量大幅增加。尽管如此，在本报告撰写之际，我们只能获得 2023 年第二季度* 的部分数据，而截至 2023 年 5 月 31 日，我们尚未记录到任何 CL0P 攻击活动，这可能表明 2023 年第一季度存在异常之处。但有必要说明，2023 年 6 月，由于 MOVEit 漏洞利用攻击，CL0P 受害者数量有所增加，包括一部分位于 APJ 区域的公司。

**此处 2023 年第 2 季度的数据并不完整，数据截至 2023 年 5 月 31 日。*

APJ 区域：按受害者数量排名的前三大勒索软件团伙

季度数据：2021 年 10 月 1 日 – 2023 年 5 月 31 日



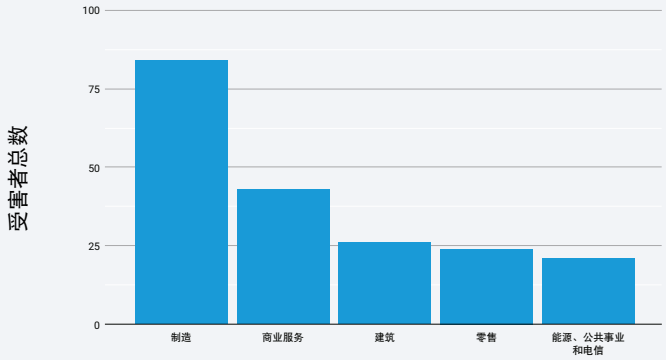
APJ 图 2：APJ 区域前三大勒索软件团伙的季度受害者数量比较：LockBit、ALPHV 和 CL0P

关键行业身陷风险

APJ 区域面临勒索软件风险的五大关键行业是：制造业、商业服务业、建筑业、零售业和能源业（APJ 图 3）。这与全球整体趋势相符，但不同之处是，在全球范围内，排名第五位的是教育业。这大体与去年的全球勒索软件报告一致，当时制造业和商业服务业也排在前两位。当时，这些行业深受 Conti 勒索软件困扰。在 Conti 消失后，LockBit 顶替了 Conti 的位置。此外，我们还注意到，这与我们先前的 DNS 主题报告《攻击快车道：深入了解恶意 DNS 流量》中的主要受影响行业存在重叠，体现出恶意命令与控制 (C2) 流量和勒索软件攻击之间的联系。

APJ 区域：按勒索软件团伙受害者数量排名的前五大行业

2021 年 10 月 1 日 – 2023 年 5 月 31 日



APJ 图 3：在 APJ 区域的勒索软件攻击中，制造业受害企业数量最多

**此处 2023 年第 2 季度的数据并不完整，数据截至 2023 年 5 月 31 日。*

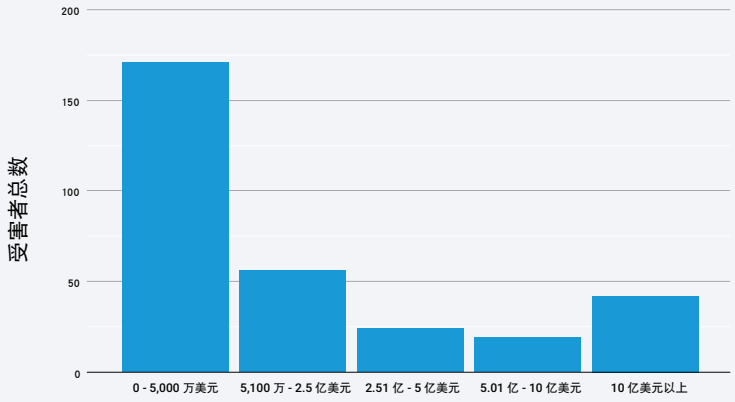
还有必要说明，LockBit 并未区别对待任何行业：在 APJ 区域各行各业中，它都是最为猖獗的勒索软件，在针对制造业的攻击中占 60%，在针对商业服务业的攻击中占 55.8%，在针对建筑业的攻击中占 57.7%，在针对零售业的攻击中占 45.8%。即使在针对能源行业的攻击中，LockBit 也占到 28.6% 的比例，剩余比例由数个不同的勒索软件团伙构成，但任何团伙在攻击中的占比都不超过 14.3%。

勒索软件团伙关注投资回报率

无论公司规模或收入如何，任何企业都不能避开勒索软件攻击的风险。但数据表明，攻击者成功针对 APJ 区域的小型企业发动了攻击（APJ 图 4），这呼应了全球趋势。根据新加坡网络安全局发布的一份报告，在新加坡报告的大多数勒索软件受害者都是制造业和零售业的中小型企业。我们推测，规模较小的公司应对勒索软件威胁的安全资源有限，因此更容易遭受攻击、更容易被渗透，而且他们也有支付赎金的能力。然而，规模最大的企业也受到了攻击，研究表明，受影响企业的收入越高，攻击者索要的赎金就越高。

APJ 区域：勒索软件团伙受害者数量（按受害者收入范围分列）

2021 年 10 月 1 日 – 2023 年 5 月 31 日



> 无论公司规模或收入如何，任何企业都不能避开勒索软件攻击的风险。

APJ 图 4：在 APJ 区域，大多数勒索软件受害企业的收入不超过 5 千万美元

APJ 区域概况的相关结论

勒索软件持续对企业造成重大破坏。在全球和地区范围内，各国政府正在结成统一战线，共同应对这一威胁，并着重强调可帮助安全防御者保障其企业安全的技术。澳大利亚外长、印度外长和日本外长及美国国务卿发表的一份声明指出，抵御勒索软件对国家安全和所有行业的影响已成为一项迫在眉睫的任务，并加强了制定相关计划的承诺，以帮助各界企业加强网络安全、提升抗风险能力。今年早些时候，“国际打击勒索软件特别工作组”成立，由澳大利亚担当工作组行动领导者，旨在推动由 36 个成员国和欧盟组成的联盟加强合作，共同应对勒索软件的传播和影响，其举措包括共享网络威胁情报。2022 年 10 月，新加坡也成立了自己的首个机构间特别工作组，多个政府机构参与其中，旨在保护企业和关键基础设施，抵御愈加猖獗的勒索软件攻击。

随着监管机构出台加强网络安全标准的倡议和政策，您有必要了解您所在地区的报告要求，从而将其纳入您的行动手册/危机管理计划，并了解您利用多层防御措施降低风险的机会。

如需了解更多信息，请参阅全球勒索软件 SOTI 报告《勒索软件异常活跃：漏洞利用技术花样翻新，零日漏洞深受黑客青睐》。

方法

勒索软件数据

该报告中所用的勒索软件数据从大约 90 个不同勒索软件团伙的泄漏站点收集而来。这些团伙通常会公开其攻击详情，如时间戳、受害者名称和受害者域名。值得注意的是，此类对外公开的信息仅限于每个勒索软件团伙希望公之于众的内容。这些公开的攻击的成功性不在本次研究的范围内。

本次研究重点关注所报告的受害者。在每次分析中，我们都会测算每个组别中的不同受害者数目。通过将这些受害者数据与从 ZoomInfo 获得的数据相结合，可得知有关每个受害者的更多详细信息，如所在位置、收入范围和所属行业。

所有数据均为 2021 年 10 月 1 日至 2023 年 5 月 31 日这 20 个月内的数据。

致谢名单

编辑与创作

Ori David
Badette Tribbey
Charlotte Pelliccia
Lance Rhodes

审稿和主题撰稿

Moshe Cohen
Shiran Guez
Ophir Harpaz
Reuben Koh
Richard Meeus
Steve Winterfeld
Maxim Zavodchik

数据分析

Chelsea Tuttle

营销与发布

Kimberly Gomez
Georgina Morales Hampe
Shivangi Sahu

更多《互联网现状/安全性》报告

《互联网现状/安全性》报告由 Akamai 精心呈献，获得了各界的广泛赞誉，您可以回顾往期报告，并关注即将发布的新报告。**akamai.com/soti**

更多 Akamai 威胁研究

关注最新的威胁情报分析、安全报告和网络安全研究的动态。
akamai.com/security-research

此报告中的 Akamai 数据

查看本报告中引用的图片和图表的高画质版本。这些图片可免费使用和引用，但前提是注明转载来源，并且保留 Akamai 徽标。**akamai.com/sotidata**

进一步探索 Akamai 解决方案

如需详细了解 Akamai 的勒索软件解决方案，请访问我们的**安全解决方案**页面。