勒索软件和 COMMODITY LOADER

在此处下载完整的英文报告

勒索软件威胁态势

勒索软件攻击者群体变化多端，不断设法适应地缘政治环境变动、防御者采取的各类行动以及执法部门的打压等形势。2022 年，从规模和强度方面而言，这些形势变得更加严峻。受此影响，有些勒索软件组织停止了活动，但也有些组织通过反复更名来重起炉灶，甚至结成新的战略合作伙伴关系。Cisco Talos 观察到 2022 年出现了若干相关趋势。

Talos 跟踪了十多个勒索软件即服务 (RaaS) 组织（图 **1**）。根据我们的调查结果，LockBit 是 2022 年最活跃的勒索软件组织，超过 20% 的暗网受害者帖子都与其有关，紧随其后的是 Hive 和 Black Basta。这些调查结果表明，勒索软件攻击者的大众化程度有所提高，相较于前几年仅有少数组织垄断市场，整体情形大为不同。勒索软件组织也不再孤立运转，而是多团队协作，在这样的架构中，拥有独门手段的威胁发起者可以获得更多机会来支持多个攻击活动和组织。

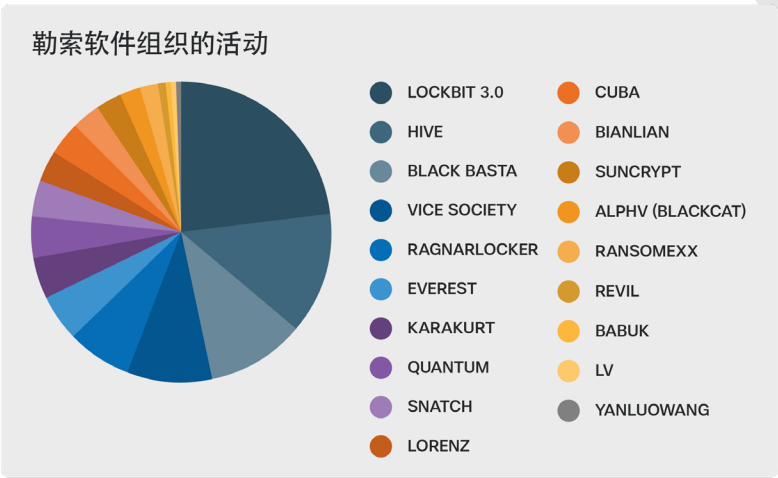

图 ***1.*** *1* 月至 *10* 月，*Talos* 跟踪到的发布于勒索软件数据泄露网站上的帖子数量。

由于俄乌战争迫使许多威胁发起者在这场冲突中选边站队，并将行动目标直指亲俄或亲乌组织，因此加剧了整个群体之间的摩擦。Conti RaaS 当属其中发声最强烈的组织，他们警告说，任何试图干预俄罗斯入侵的人都会遭到攻击。一名与 Conti 有牵连的人曾为了报复该勒索软件团伙，泄露了相关信息，其中包括恶意软件的源代码和分支组织之间的内部聊天记录。在另一起事件中，Talos 发现了一个名为“LockBitBlack”的 LockBit 3.0 勒索软件加密器的构建程序遭到泄露。一位据称是 LockBit 开发人员的人声称对此事担责，据 LockBit 表示，他们对该组织的薪酬结构心怀不满。

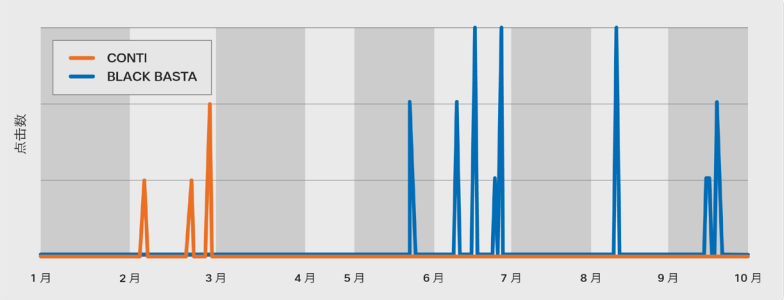

图 ***2.*** *Secure Malware Analytics* 中针对 *Conti* 勒索软件和 *Black Basta* 注册表修改的行为指标检测。

这种摩擦是导致勒索软件团伙更名或滋生新勒索组织的常见原因。当 Conti 停止运营并将其基础设施下线时，我们发现我们的遥测检测数据普遍下降，但此后不久，Conti 便更名为“Black Basta”粉墨登场。研究人员认为，这两个组织的支付和泄密网站以及通信方式颇为相似（图 **2**）。

COMMODITY LOADER

Commodity Loader（即部署第二阶段恶意软件的商业木马）是一项持续性威胁，会在全球范围内不断产生影响。这种恶意软件一开始是作为银行木马而开发的，用于入侵实体以谋取经济利益，但随着时间的推移，它们已适应了更严格的安全控制措施，并发展成为更复杂的

勒索软件和 COMMODITY LOADER

威胁。它们现在主要作为具有模块化功能的加载程序而运行，使网络犯罪分子能够灵活地使用一系列开源工具和新开发的恶意软件。根据我们对多个网络和终端遥测集的分析，2022 年最活跃的四种 Commodity Loader 为 Qakbot、Emotet、IcedID 和 Trickbot（图 **3**）。

虽然我们的遥测检测到了与 Trickbot 相关的活动，但我们评估大部分此类活动可能是在检测旧的受感染终端，因为自 2022 年初以来该恶意软件的操作者一直处于非活动状态。同样，Emotet 虽然仍可使用，但与 2021 年 1 月上旬执法部门清除该僵尸网络之前相比，它的活跃程度已大大降低。其他恶意软件（例如 Qakbot 和 IcedID）日益猖獗，填补了这一空白。

根据我们在 2022 年观察到的一个总体趋势，恶意软件操作者更频繁地使用 ISO、ZIP 和 LNK 文件类型来传送 Qakbot、Emotet 和 IcedID，这可能是为了防止 Microsoft 阻止启用宏的文档。另一个趋势是，Talos 观察到 Qakbot、Emotet 和 IcedID 操作者使用在受害者环境中发现的离地攻击二进制文件 (LoLBins) 来下载并启动恶意负载。在某些情况下，Qakbot 和 Emotet 分支组织还曾通过试验不同的 LoLBin 来改进其攻击序列，以提高它们在组织内不被发现的几率。

虽然我们的遥测检测到了与 Trickbot 相关的活动，但我们评估大部分此类活动可能是在检测旧的受感染终端，因为自 2022 年初以来该恶意软件的操作者一直处于非活动状态。同样，Emotet 虽然仍可使用，但与 2021 年 1 月上旬执法部门清除该僵尸网络之前相比，它的活跃程度已大大降低。其他恶意软件（例如 Qakbot 和 IcedID）日益猖獗，填补了这一空白。

查看完整报告可深入了解每种 Commodity Loader。

Commodity Loader

	Qakbot	IcedID	Emotet	Trickbot
别名	Quackbot、Qbot、Pinkslipbot	BokBot	Geodo、Heodo	不适用
分支组织	可能由欧亚网络犯罪分子开发的商品恶意软件	未知	由与俄罗斯结盟的网络犯罪组织 Mummy Spider 开发的商品恶意软件	由与俄罗斯结盟的网络犯罪组织 Wizard Spider 开发的商品恶意软件
开始活跃的时间	2007 年	2014 年	2017 年	2016 年

目标

- 获得初始访问权限并建立持久性攻击路径，以便于进一步实施入侵活动。
- 部署下一阶段的恶意软件，包括勒索软件。

受害者群体

- 面向全球所有行业。
- 自俄乌战争以来，Trickbot 一直扬言要对俄罗斯民众遭受的袭击进行报复

典型 TTP

- 网络钓鱼、恶意垃圾邮件、社交工程、漏洞利用、盗窃数据（例如财务数据），以及凭证式和蠕虫式传播。
- 高度模块化，使得操作者能够进行各种攻击

恶意软件和工具

- 这些恶意软件变体既可部署其他各种恶意软件，也可由其他各类恶意软件系列进行部署，彼此相容。
- 在攻击生命周期的各个阶段使用 Cobalt Strike 等商业工具以及 LoLbin

图 ***3.*** *Commodity Loader* 威胁列表。