攻击快车道

深入了解恶意 DNS 流量

Akamai

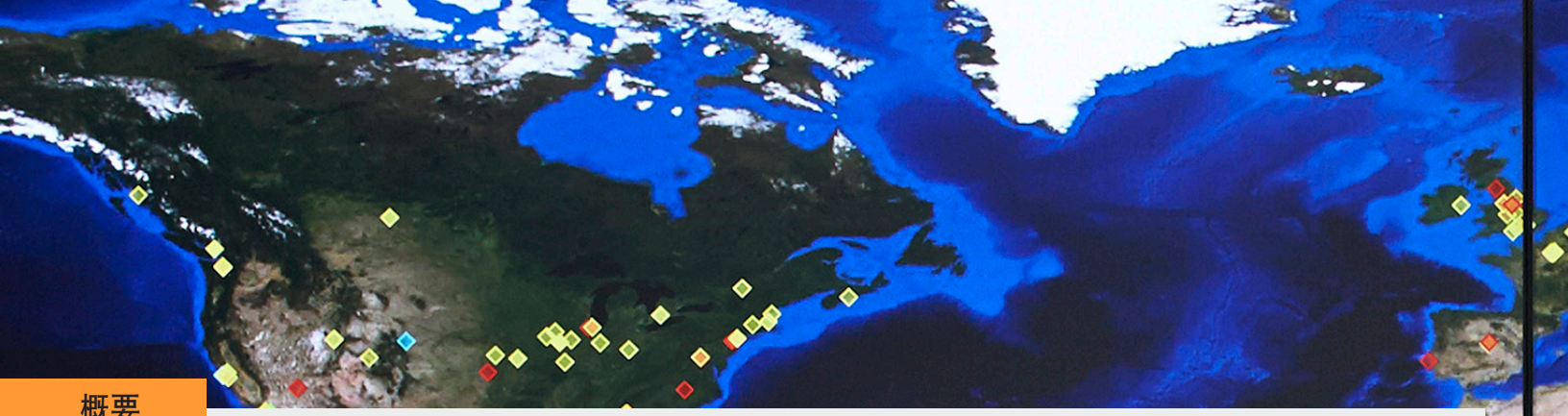
目录

域名服务器——攻击流量快车道

域名服务器 (DNS) 自问世之初就一直是互联网基础架构的重要组成部分。无论在家中还是公司，我们的大多数网上活动都要借助 DNS 的力量，这样我们才能够正确导航到万维网上的目的地。当然，攻击者往往也会选择利用这一基础架构来实施攻击，比如让攻击威胁访问命令和控制 (C2) 服务器来等候指令，或者让远程代码执行连接某个域名，以将恶意文件下载到设备中。由于 DNS 无处不在，它已成为攻击基础架构的重要组成部分。

作为一家安全公司，Akamai 具有独特的优势，我们可以观察并且保护企业和家庭用户，帮助他们抵御恶意 DNS 流量，避免由此造成系统入侵和信息被盗。在本报告中，我们将分析以全球家庭用户和企业为攻击目标的恶意流量。通过全面分析恶意 DNS 流量（包括其与攻击者团体或工具的关联），企业就能获得重要信息，了解自身面对的最为普遍的威胁。因此，这些信息可以帮助安全从业者评估其防御态势，还可以执行缺口分析，从而满足用于抵御这些威胁的技术和方法的需要。如果不这样做，攻击就有可能得逞，进而造成机密数据丢失、财务损失，或是因为不合规而遭受处罚。到 2025 年，网络犯罪造成的损失预计会激增到每年 10.5 万亿美元，企业必须做好防范攻击的准备。

在分析针对企业和家庭用户的恶意 DNS 流量时，我们观察到了数次攻击爆发和攻击活动，例如基于 Android 的恶意软件 FluBot 在世界各个国家或地区之间传播，以及各类以企业为目标的网络犯罪团伙的猖獗活动。或许最好的例子莫过于与初始访问代理 (IAB) 相关的 C2 流量泛滥，这些流量旨在入侵企业网络，让攻击者将获得的访问权限卖给其他方（例如勒索软件即服务 (RaaS) 团伙）来谋利。我们在 DNS 这条信息快车道上观察到了这些活动，并特此分享给大家，希望能给读者带来些许收获。



概要

根据我们的数据，在任意给定季度，都有 10% 到 16% 的企业的网络中出现过 C2 流量。C2 流量的出现表明网络有可能正在遭遇攻击，或者发生了入侵，而威胁可能包括信息窃取僵尸网络、IAB 等众多形式。

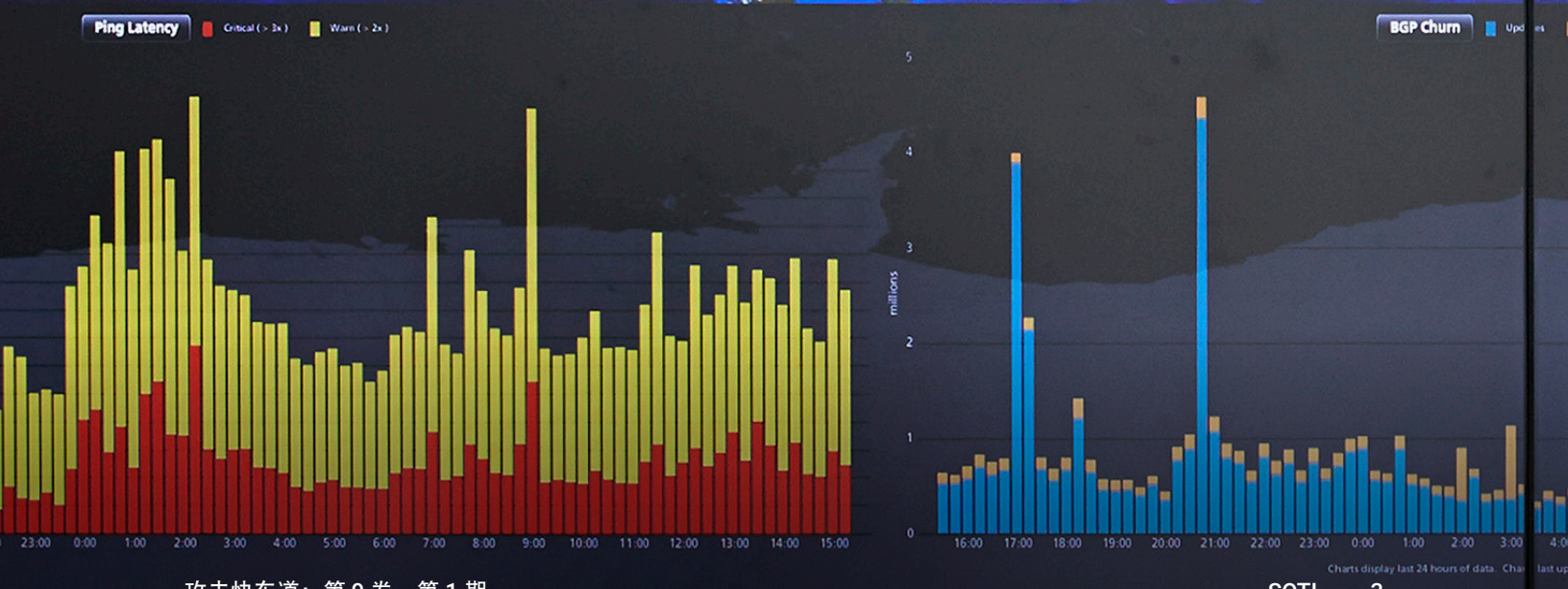
26% 的受影响设备曾连接过已知的 IAB C2 域，包括与 Emotet 和 Qakbot 相关的 IAB C2 域。IAB 的主要任务就是执行初始入侵，并将访问凭据销售给勒索软件团伙和其他网络犯罪团伙，因此会给企业造成重大风险。

网络连接存储 (NAS) 设备正中攻击者的下怀，因为这些设备不太可能安装修补程序，而且存有大量高价值的数据。我们的数据表明，攻击者在通过 QSnatch 滥用这些设备，企业网络中有 36% 的受影响设备在访问与此类威胁有关的 C2 域。

30% 的受影响企业属于制造业；这一数字是排名第二位的垂直领域的两倍，突显出网络攻击对现实世界产生的影响，例如供应链问题和对日常生活造成的破坏等等。《网络与信息安全指令 2》(NIS2) 等法规有助于遏制针对基础行业或制造业等重要行业的攻击。

针对家庭网络发起的攻击不仅会尝试滥用计算机等传统设备，还企图滥用手机和物联网 (IoT)。大量的攻击流量可能与移动端恶意软件和 IoT 僵尸网络相关。

通过 DNS 数据分析，我们发现 FluBot 恶意软件在欧洲、中东和非洲 (EMEA)、拉丁美洲 (LATAM) 以及亚太地区和日本 (APJ) 迅速爆发。促使感染量增加的部分因素可能是这种恶意软件采用了社会工程策略，并使用了多种欧盟 (EU) 语言。



Akamai DNS 流量分析术语

Akamai Edge DNS 和 DNS 基础架构每天会观察多达 7 万亿个 DNS 请求。为保护 Akamai 用户和企业，Akamai 会观察请求是否指向会传输恶意软件的域或可能窃取信息的网站，并阻止相应请求。通过检查这些恶意 DNS 事务，我们可以将这些域分为三类——恶意软件、钓鱼网站和 C2，并开展深入研究，确定当今企业和家庭用户面临的重大威胁。

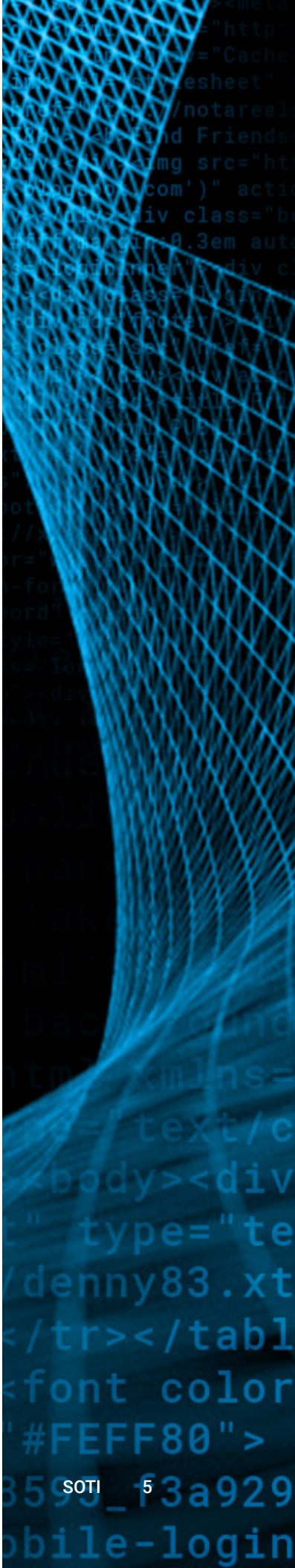
根据对恶意 DNS 流量的谨慎数据抽样，我们可以就最为普遍的威胁得出重要结论。我们的措施为两类群体提供保护：其中一个群体是企业，Akamai 为企业网络提供保护；另一个群体是在个人网络上访问互联网的家庭用户，他们面临着多种威胁，比如旨在接管其设备以达到恶意目的（如通过加密货币挖矿来谋利）的僵尸网络。

首先，我们给出*钓鱼网站*、*恶意软件*和 *C2* 这些术语的定义，并说明本报告中如何使用这些术语。

钓鱼网站是指与网络钓鱼工具包关联的域名，它们会效仿和“克隆”零售企业、银行、高科技公司和其他公司网站的外观与体验，诱骗用户泄露凭据和个人身份信息 (PII) 等重要数据。Akamai 通过 DNS 观察这些流量，保护企业和家庭用户免遭身份被盗、信息丢失的烦恼。

恶意软件是指传输或植入恶意文件的恶意域（可能是多个域）。此类别还包括：托管恶意 JavaScript 的网站，已被入侵并且投放垃圾广告的网站，或者将用户重定向到含有此类广告的网页的网站。许多现代攻击都需要从外部来源将恶意文件下载到设备上，以此作为初始攻击载荷；或者下载恶意内容，以支持持续攻击的下一阶段。观测和阻止此类流量有助于保护企业，避免初始感染或持续攻击。

在我们的 DNS 流量分析中，**C2** 是指用来与受感染的设备通信的域，它会发送命令，随后控制设备。在初始入侵后，攻击者在受感染的系统与攻击者控制的服务器之间建立 C2 通信，以发送额外的命令，比如下载和传播其他恶意软件、数据泄露、关闭和重启系统等，从而给系统或网络安全造成进一步破坏。C2 流量预示着有持续攻击，但这些攻击仍有可能被抵御，因此检测 C2 流量至关重要。此外，阻止与 C2 服务器相关的域可以防止建立 C2 通信，进而阻止恶意软件下载更多指令或命令，减少攻击者在您的网络中实施恶意活动的机会。



威胁当头：企业内无处不在的恶意流量

根据 Akamai 的 DNS 流量分析，我们可以看到，2022 年第四季度，13% 的设备至少有一次尝试连接与恶意软件有关的域（图 1）。此外，6% 的设备与涉及到网络钓鱼的域进行了通信。对于本报告中重点关注的 C2 领域，我们观察到其全年呈增长趋势，第四季度有极小幅度的下降。

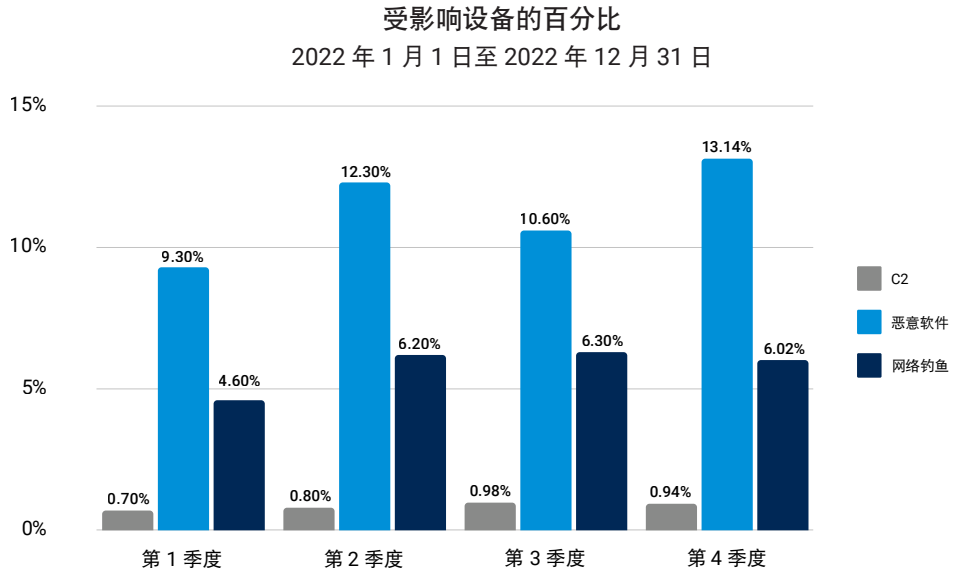


图 1：我们观察到，受保护的设备尝试连接恶意目的地的行为呈上升趋势

请注意，图 1 仅涉及到尝试与恶意域通信的单个设备。有必要指出，尝试连接恶意软件目的地（攻击者可能借此下载恶意软件）的设备，与尝试连接 C2 域的设备（通常在持续攻击中用于促进攻击者与恶意软件之间的通信，还可用于下载额外的恶意软件以推进攻击周期）之间存在差异。这种差异可代表以下三者间的不同之处：网络渗透尝试 (可能在初次尝试将恶意软件下载到设备时即被阻止)、成功渗透 (根据我们的数据，这表示可能未经过 DNS) 或正在进行的攻击 (可能联机 C2 域以执行攻击) 。

本报告主要关注 C2 流量，将此视为攻击者已成功侵入设备的一个潜在指标。为便于了解这种攻击的普遍性，我们需要通过另一种不同的视角来观察数据。我们不考虑个别设备，而是将数据按企业汇总起来，检查持续攻击（通过 C2 流量的存在确定）在数据集中出现的频率。

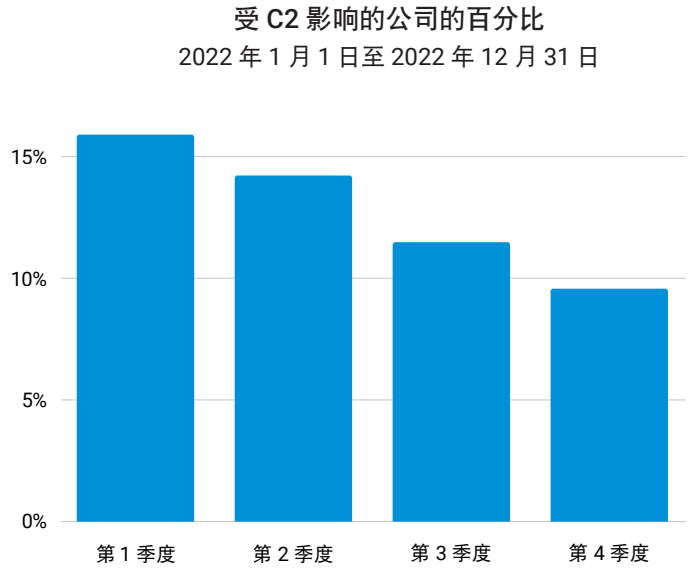


图 2：通过分析恶意 C2 流量，我们得出了全年至少有一台设备尝试连接 C2 域的企业百分比

> **根据我们的 DNS 数据，在任意给定季度，都有 10%–16% 的企业至少观察到一次 C2 流量从其网络中发出的情况。**

根据我们的 DNS 数据，在任意给定季度，都有 10%–16% 的企业至少观察到一次 C2 流量从其网络中发出的情况（图 2）。这可能表明恶意软件尝试与运营者沟通，是潜在的入侵迹象。我们的解决方案阻止了这些 C2 流量到达目的地，但攻击一旦得逞，就可能会导致数据泄露、勒索软件攻击及其他威胁。截至 2022 年上半年，共检测到 23 亿个恶意软件变种，平均每天 1,501 个。我们的研究强调了利用 DNS 防止恶意软件在网络中取得进展或造成危害的有效性。

初始访问代理对企业构成了普遍的威胁

多阶段攻击已成为现代攻击领域中的一种主力方法（图 3）。攻击者发现，如果能协同工作（或彼此雇用）或在一次攻击中结合使用各种工具，就能提高攻击的成功率。对于这些攻击的成败，C2 发挥着至关重要的作用。它们不仅可用于通信，也让攻击者能方便地下载攻击载荷，以及用于推进攻击下一阶段的恶意软件。过去几年中观察到的 Emotet/TrickBot/Ryuk 勒索软件攻击链就是最好的例证。Emotet 首先渗透到受害者的网络中，在获得初始访问权限后，它会联系一个域，下载 TrickBot 的攻击载荷，以获取个人数据和凭据等。如果根据攻击者的标准，受害者属于高价值目标，恶意软件会联系其 C2 服务器并下载最终的攻击载荷：Ryuk 勒索软件。

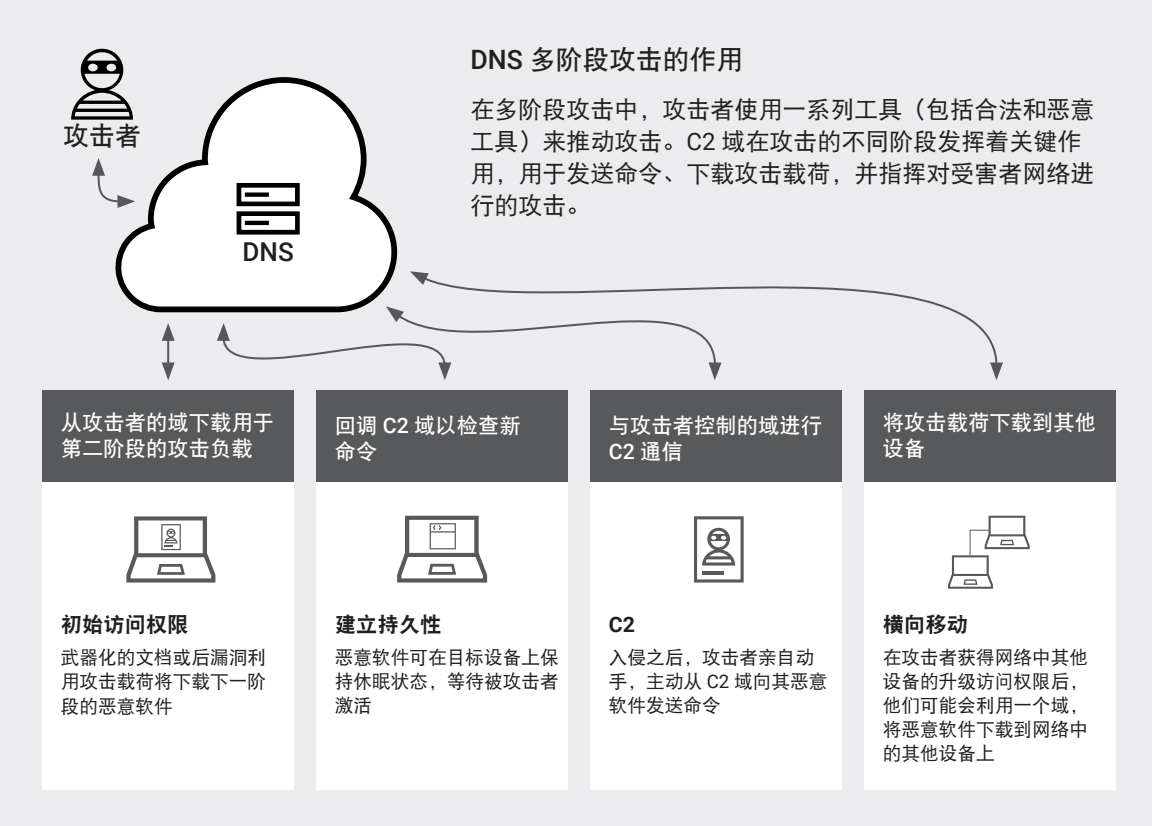


图 3：C2 在攻击各阶段的作用

在评估本报告的信息时，请务必考虑这种事件链。C2 通信可能发生在攻击的不同阶段。我们近期对现代勒索软件团伙（如 Conti 团伙）的攻击手法开展了分析，结果表明，精明的攻击者往往会安排操作人员进行“手动操作”(hands on keyboard)，以便快速、有效地推进攻击。观察和阻止 C2 流量的能力对于阻止持续攻击非常重要。

我们观察到的 C2 域可以分为两大类：一类归属于特定威胁系列或攻击者团伙的域，另一类无此归属。在本节中，我们将深入研究与威胁类型相关的 C2 域，帮助读者根据各攻击者团伙的能力和所用方法来评估风险水平。请注意，部分此类恶意软件系列可能适合多种应用场景，具体取决于攻击者在攻击中使用它们的手法。

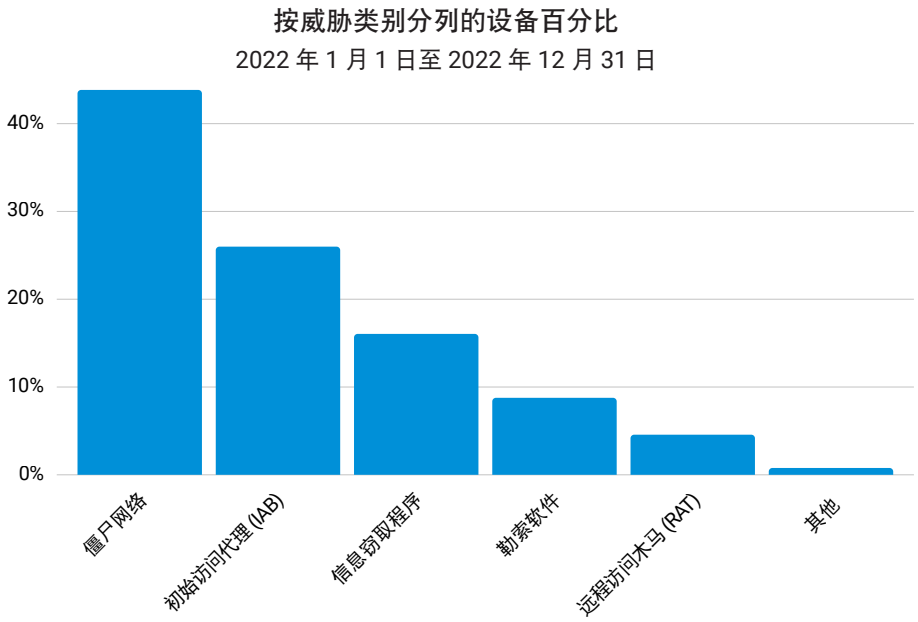


图 4：攻击目标为企业的僵尸网络比例最高，其次是 IAB 和信息窃取工具

图 4 将攻击者团伙划分成 IAB、僵尸网络和 RaaS 几个分组。我们的数据表明，IAB 是企业网络面临的一项重大威胁，以数据泄露为目标的僵尸网络同样如此。

初始访问代理
IAB 的关注重点是为其他网络犯罪分子（包括勒索软件分组）提供初始入口点，让后者能在企业网络中获得立足点。持久性、入侵后远程执行攻击载荷（勒索软件采用的就是这种方法）以及数据泄露。

“勒索软件即服务”分组
该分组的团伙允许其他攻击者（甚至是不具备专业技术知识的攻击者）成为其合作者，并有偿使用他们的勒索软件。

僵尸网络
攻击者可以利用僵尸网络达到各种目的，比如加密、DDoS 攻击、数据泄露、恶意软件部署和横向移动等。

信息窃取工具
信息窃取工具收集各种类型的数据，如用户名、密码、系统信息、银行凭据、Cookie 等。

我们还观察到，攻击者将勒索软件、远程访问工具 (RAT) 和信息窃取工具纳入攻击组合，让它们各自在不同的阶段发挥关键作用。新手级攻击者和经验丰富的网络犯罪分子如今都能通过地下交易平台获得现成的工具，因此他们能够成功完成初始入侵，藏匿在网络中并推进攻击，这让企业比以往更容易受到网络犯罪的侵扰。在梳理这些分组时，我们还会分析其运作的交叉点，以及给企业造成的潜在影响和冲击。

“初始访问代理”分组

“初始访问代理”(IAB) 这一特定类型的网络犯罪分子主要关注打通初始入口点，让其他网络犯罪分子和攻击者能借此在企业网络中获得立足点。多个网络犯罪分组都采用类似的入侵方法，比如利用 RDP 和 VPN 相关漏洞、使用暴力破解攻击、收集凭据转储，以及发送带有恶意软件的钓鱼邮件，但 IAB 擅长获得这些受感染系统的访问权限，随后将访问权限出售给其他分组的攻击者，而不会自行实施整个攻击。根据报道，LockBit、DarkSide、Conti 和 BlackByte 等威胁背后的勒索软件团伙均在其行动中利用了 IAB。2023 年的一份研究报告指出，初始访问权限的平均售价约为 2,800 美元。

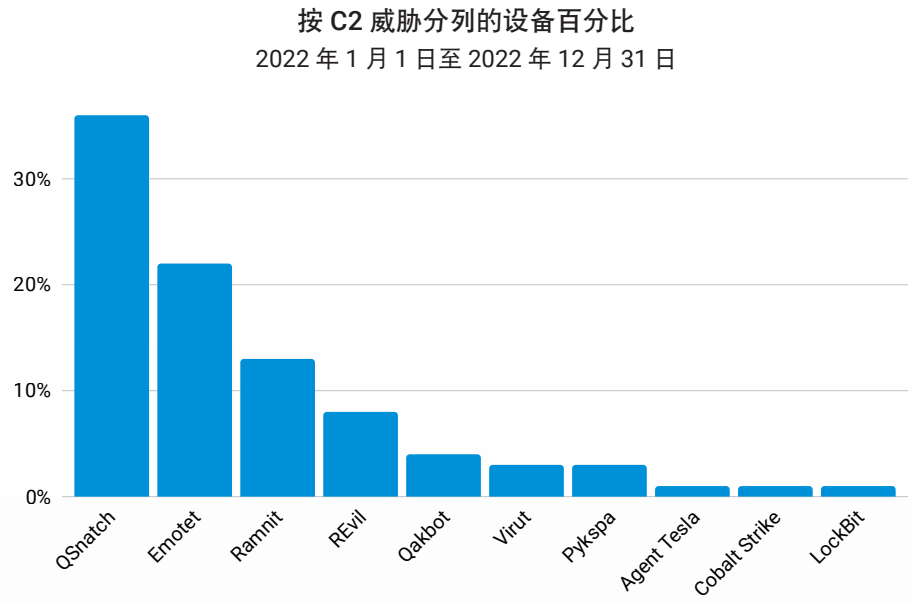
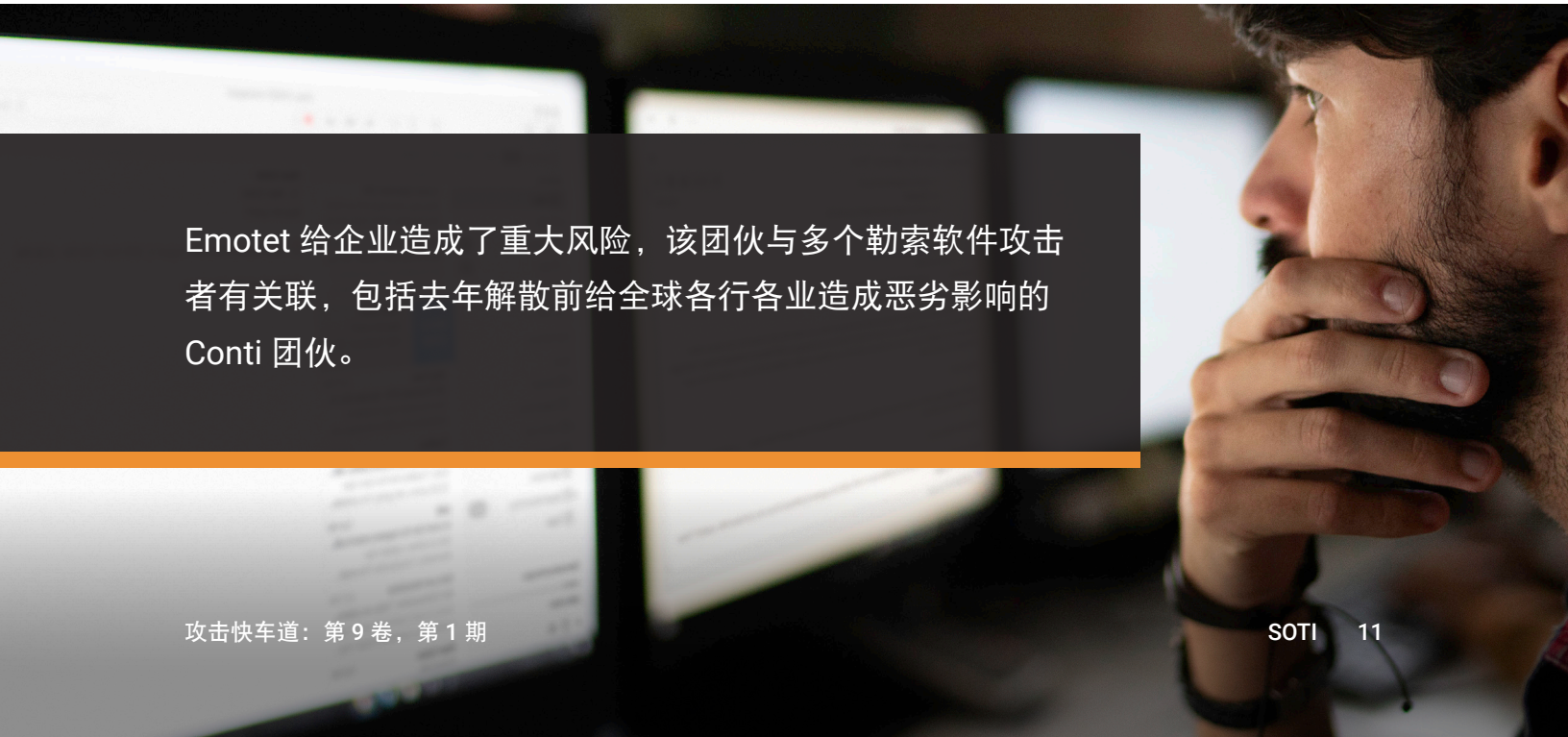


图 5：QSnatch、Emotet 和 Ramnit 是企业网络流量中出现频率较高的 C2 系列

根据我们的 DNS 数据（图 5），26% 的受感染设备连接过与 IAB 有关联的域，如Qakbot（4% 的受感染设备）和 Emotet（22% 的受感染设备）。在 RaaS 商业模式和网络犯罪领域，IAB 都有着举足轻重的作用。勒索软件攻击者和网络犯罪分子需要远程访问权限和凭据，不仅需要借此渗透到受害者网络中，还需要以此实现横向移动、建立持久性、获得访问权限并执行其他活动。攻击者利用 IAB 来完成侦查、潜在目标扫描和初始感染等耗时的任务。在地下交易平台中唾手可得的访问权限消除了这个步骤，降低了攻击者发动攻击所需的专业技能，也缩短了发动攻击所需的时间。这种局面造成企业面临大量潜在的针对性攻击，以及由此而来的勒索软件、机密和敏感信息被盗、间谍活动和数据泄露威胁。

在我们的数据中，Emotet 是极具代表性的 IAB 之一。Emotet 给企业造成了重大风险，该团伙与多个勒索软件攻击者有关联，包括去年解散前给全球各行各业造成恶劣影响的 Conti 团伙。多年来，Emotet 添加了更多模块，如分布式拒绝服务 (DDoS) 和电子邮件盗窃功能，其预期受害目标群也不断扩大。Emotet 最初是一个具有大量功能的银行木马/僵尸网络，如今已转变为恶意软件即服务 (MaaS) 威胁，传播 IcedID 银行木马、TrickBot 和 UmbreCrypt 勒索软件等威胁。根据观察，TrickBot 团伙还利用 Emotet 来分发一些勒索软件，包括 Ryuk、ProLock 和 Conti 等。关于 Emotet 所用技术的更详尽的观察，可参阅有关此主题的 MITRE ATT&CK 框架。



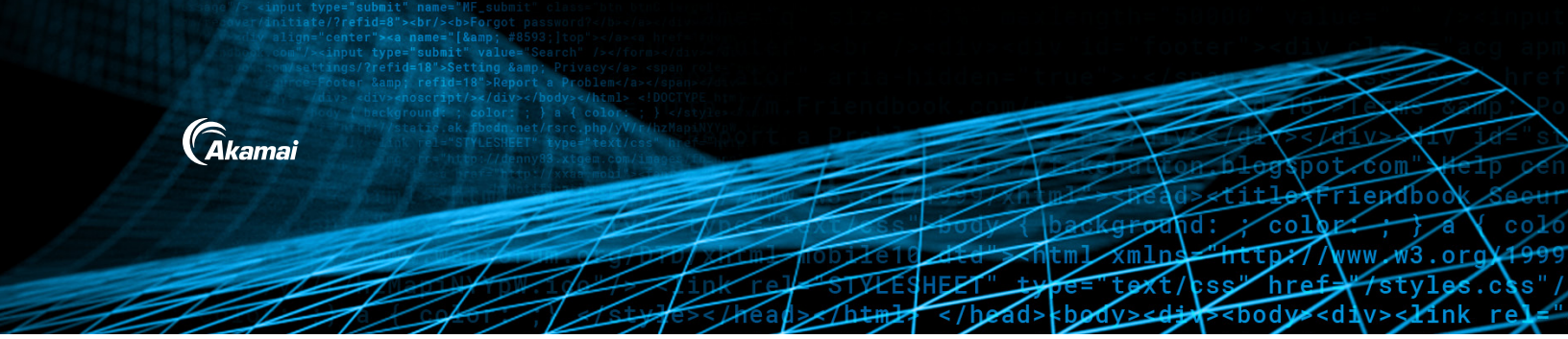
Emotet 给企业造成了重大风险，该团伙与多个勒索软件攻击者有关联，包括去年解散前给全球各行各业造成恶劣影响的 Conti 团伙。

在我们的数据中，第二突出的 IAB 是 Qakbot。我们已经确知该团伙与 Black Basta 勒索软件团伙有合作关系，后者据称已影响全球各地至少 50 家企业。Qakbot 团伙因信息窃取能力和提供第二阶段恶意软件（用于进一步破坏系统安全性）而闻名。根据研究，Qakbot 利用了 Cobalt Strike，这本是一种供红队使用的合法渗透测试工具，攻击者滥用这种工具，在入侵后开展一系列恶意活动，并在受害者环境中留下后门。这是近年来 IAB 日益频繁使用的一种技术。您可以访问 MITRE ATT&CK 框架，获得有关 Qakbot 在攻击期间利用的技术的额外情报。

“僵尸网络”分组

在我们的分析中，僵尸网络是规模最大的威胁类型分组，占所分析 C2 流量的 44%。这个分组中涵盖多种多样的攻击者，也应该注意，并非所有僵尸网络都一般无二。有害性较低的变种可能会植入加密货币挖矿程序，或利用受害者的机器发动 DDoS 攻击。虽然这些做法本身就会给受害者造成损失，但我们在企业中发现的僵尸网络可用于数据泄露和多阶段攻击，因此可能造成更重大的风险。僵尸网络可以在网络中横向扩展，并可用于部署勒索软件（TrickBot 采用的就是这种做法），也可专门用于窃取信息和收集凭据。

我们发现，企业环境中出现的大型僵尸网络 QSnatch 采用了后一种做法，造成网络连接设备中的数据泄露。根据我们的数据，36% 的受感染设备受到了 QSnatch 的影响。这种恶意软件专门针对 QNAP——企业用于备份或文件存储的一种 NAS 设备。虽然感染方法还不明确，但研究人员推测，QSnatch 可能的感染途径是利用固件漏洞，或者对具有默认用户名/密码的设备进行暴力破解攻击。强烈建议使用 QNAP 的公司及时更新其固件（一旦感染，QSnatch 将阻止安装修补程序并禁用安全产品），并立即改掉默认密码。攻击者利用 QSnatch 实现凭据抓取、密码记录、远程访问和数据泄露等目的。存储设备可能会成为攻击者的目标，因为它们含有大量高价值信息，而且入侵这些设备还能使企业在遭遇勒索软件攻击时无备份可用。这份 CISA 警报强调了战术和应对措施的细节。



“勒索软件即服务”分组

根据我们的 DNS 流量分析结果，在连接过 C2 系列的受感染设备中，有 9% 访问过与 RaaS 团伙相关的域。此类网络犯罪团伙允许其他攻击者（甚至是不具备专业技术知识的攻击者）成为其合作者，并有偿使用他们的勒索软件。一旦被勒索软件侵袭，企业要承受的后果不只有公司机密数据丢失。他们还有可能需要承担补救和恢复成本、法律费用、罚款、造成生产力损失的停机时间以及品牌和名誉损失。Cybersecurity Ventures 认为，到 2031 年，每年因勒索软件攻击而造成的损失将达到大约 2,650 亿美元。Akamai 发布的《全球勒索软件报告》也强调了勒索软件的破坏性影响，除了供应链中断等经济损失之外，在某些情况下，勒索软件还可能会危及生命。

REvil 是一个颇为“高产”的 RaaS 团伙，他们因在一次供应链攻击中攻击一家 IT 管理供应商而恶名昭著，那次攻击总计影响了 1,500 多家托管服务提供商。团伙的数名成员被俄罗斯政府逮捕后，其行动就此停止。但在团伙解散几个月后，安全研究人员观察到，REvil 的泄漏站点再度活跃，发布了最新受害者的信息，美国的一些大学赫然在列。研究人员推测，实施这一攻击活动的犯罪分子可能并非同一个 REvil 团伙，并警告说，不要让打着 REvil 团伙名号的民族国家网络犯罪分子借此隐藏踪迹。在战术方面，REvil 的指明做法就是根据目标受害者定制攻击流，这体现出该团伙对其目标的了解程度。如需进一步了解与 REvil 有关的战术、技术和过程，请阅读 MITRE 的帖子。

> **存储设备可能会成为攻击者的目标，因为它们含有大量高价值信息，而且入侵这些设备还能使企业在遭遇勒索软件攻击时无备份可用。**

在检查 DNS 流量时，我们发现的另一个 RaaS 团伙是 LockBit。在 Conti 团伙“销声匿迹”后，LockBit 团伙一跃成为最活跃的 RaaS 提供者之一。根据这份报告，在此之前（即 2019 年 11 月到 2022 年 3 月），该团伙的 RaaS 的受害企业数量仅次于 Conti 团伙。

LockBit 团伙为拥有比其他 RaaS 团伙更快的加密机制而洋洋自得，并声称其 LockBit 2.0 已经影响了 12,000 多家公司。2022 年 6 月，该团伙发布了 LockBit 3.0，增加了一些功能，还添加了一个漏洞赏金计划。据报道，他们还利用 Log4j 漏洞获得对目标的初始访问权限，这也突显出及时安装修补程序的重要意义。如果企业未能及时修补此类安全漏洞，被 LockBit 感染的风险就会更高。LockBit 还在不断重塑自身，近期增加了三重勒索战术，如果受害者拒绝支付赎金，他们会加密文件，将其发布到泄密网站上，并发动 DDoS 攻击。

攻击工具

本节中提及的工具在攻击中可能发挥特定作用，包括入侵系统、获取信息或升级特权等。根据我们的观察，各类攻击者团伙使用的攻击武器库通常都要依靠通信来发挥作用，比如信息窃取工具和 RAT 都是如此。通过了解这些工具以及攻击者团伙使用的战术，安全从业者可以了解攻击的发动方式，从而相应地做出防范规划。

信息窃取工具

信息窃取工具迄今仍是攻击中频繁使用的一种 MaaS 工具，用于获取各种类型的数据，如用户名、密码、系统信息、银行凭据和 Cookie 等。即便不具备技术知识和/技能的攻击者也能以相对低廉的价格轻松获得信息窃取工具，并发动自己的攻击。

在 C2 恶意软件系列的列表中，我们观察到 16% 的设备访问过已知的 C2 归属，并尝试连接信息窃取工具。Ramnit（13% 的受感染设备）绝不是又一个平平无奇的信息窃取工具。其优势在于高度模块化，这让攻击者能够利用各种功能，比如窃取其他敏感数据和下载/部署其他恶意软件，以达到其最终目标或推进攻击。2021 年，Ramnit 被视为顶级银行木马，近期的新闻报道提到了另一种恶意软件与 Ramnit 使用类似的代码。

网络中发现信息窃取工具预示着用户的凭据可能面临风险。攻击者可能会将收集到的被盗信息拿到地下交易平台上出售，供其他攻击者用于获得初始访问权限。勒索软件团伙可以通过网络钓鱼或僵尸网络部署信息窃取工具，从而获得有效凭据，在提供 MaaS 的地下论坛中将访问权限使用权出租给信息窃取者，或通过 IAB 购买网络访问权限。在某些情况下，信息窃取者有可能成为 IAB，并将收集到的高价值凭据（如 VPN 或 RDP 访问权限）出售给出价最高的人或其他攻击者，供其发起更为复杂的攻击。

远程访问工具

一些攻击者团伙在行动中滥用了 Cobalt Strike。攻击者通过多种方式利用这种强大的 RAT，包括侦查、特权升级、通过网络横向移动、建立持久性、入侵后远程执行攻击载荷（勒索软件采用的就是这种方法）以及数据泄露。虽然该工具主要用于入侵后的横向移动和渗透，但由于它带有鱼叉式钓鱼模块，它也能用作获取初始访问权限的攻击媒介。已知使用该工具的团伙包括 Conti、Qakbot、TrickBot 和 Emotet 等。为了帮助检测环境中的 Cobalt Strike，Google 创建了这组 YARA 规则，可确定恶意使用该工具的情形。

我们的数据还显示了 Agent Tesla C2 流量的存在。这种 RAT 在地下市场中兜售，由于价格低廉、使用简单，对于网络犯罪分子颇具吸引力。攻击者可以利用此工具从各种浏览器中获取凭据、捕捉按键操作、抓取屏幕截图，并记录按键。其著名的战术之一是表单抓取，这让攻击者能够收集 PII 和其他敏感信息。此类被盗信息可用于身份盗窃或欺诈。PCrisk 发布了有关 Agent Tesla 技术的更多细节，以及它对用户的影响。

活动形势表明，全年有零星的恶意软件活动

在一年期间，我们观察到 C2 恶意软件的活动有所波动（图 6）。典型案例：可以看到，Emotet 在 2021 年 11 月死灰复燃，随后在 2022 年 1 月和 2 月期间特别活跃。这种活动量的激增表明攻击活动的强度极大，该威胁在偃旗息鼓数月之后，借此重新树立自己的地位。在复出后的几个月里，Emotet 加强了攻击战术，包括规避 Microsoft 禁用 Visual Basic for Applications 宏的举措。一些报告指出，2022 年 7 月至 11 月期间，Emotet 活动量再度大幅下降；我们的数据观测结果表明，7 月的 C2 流量下滑，通过连接 Emotet 域的受感染设备占比降低也能看出这一点。这可能表明该团伙在全年保持活跃，也可能表明已安装的恶意软件仍在与过时的基础架构通信。2023 年的观察结果能帮我们确定 Emotet 团伙是否确实已经蛰伏。

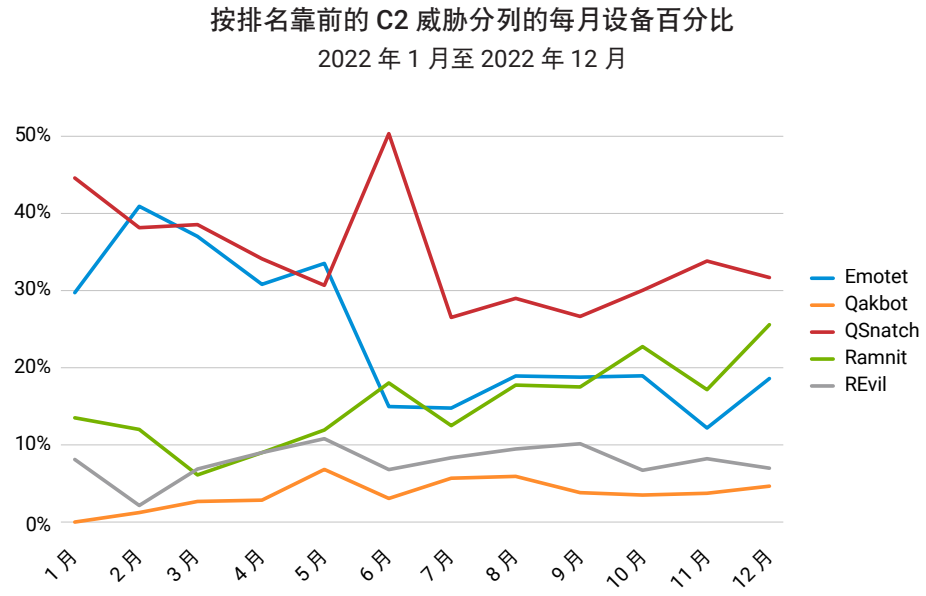


图 6：月度趋势图显示，在 2022 年全年，QSnatch 持续活跃

> **可以看到，Emotet 在 2021 年 11 月死灰复燃，随后在 2022 年 1 月和 2 月左右特别活跃。这种活动量的激增表明攻击活动的强度极大，该威胁在偃旗息鼓数月之后，借此重新树立自己的地位。**

QSnatch 全年始终保持活跃，6 月左右，其活动量达到顶峰，表明这种威胁的普遍程度。由于以下几个原因，NAS 服务器仍是攻击者的可行目标：第一，其中包含敏感数据；第二，为 NAS 服务器执行修补的几率较低；第三，这些设备在企业网络中可能更易访问，可能成为横向移动的中枢。虽然在过去几年间，情况有所变化，比如新增了内置安全解决方案，但网络犯罪分子可禁用其安装的安全产品和/或阻止设备安装新修复程序，以此规避这些举措。因此，这些设备仍然容易受到该恶意软件新变种的影响。

我们还看到，从 8 月到 12 月，Ramnit 在企业网络中的数量不断增加。这十分令人担忧，因为这种恶意软件可能会窃取一系列敏感信息，攻击者后续可能会将这些信息卖给其他威胁者，用于发起未来攻击。

QSnatch 和 Emotet：所有地区的共同威胁

为了确定各地区普遍存在的威胁，我们研究了各地区连接 C2 域的设备的百分比（图 7）。各百分比数据均表示在各地区受影响设备中的占比，各地区的受影响设备也各有不同。但有趣的是，在所有地区，我们都观察到类似的攻击趋势，仅有极少数的例外。因此，我们建议各地区遵循“结论和建议”部分中的建议，或是上文讲解恶意软件分组的各节给出的建议。

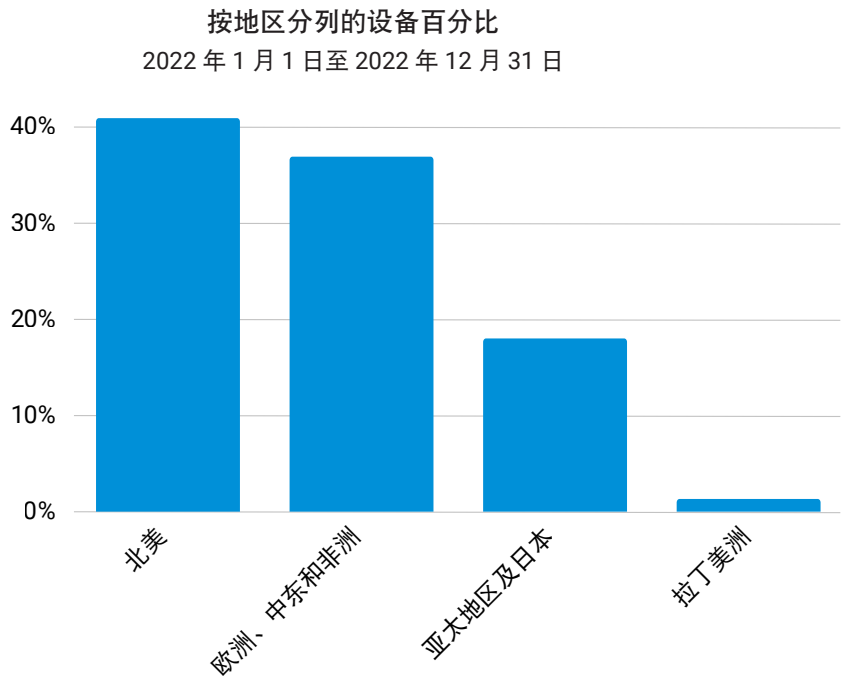


图 7：观察各地区受影响的设备数量，北美以 41% 位列第一，其次是欧洲、中东和非洲地区 (37%) 和亚太地区及日本 (18%)

北美

全球大多数企业都遭遇过这两个大型威胁：QSnatch 和 Emotet。北美地区约 29% 的受影响设备受到 Emotet 的影响，33% 受到 QSnatch 的影响（图 8）。根据 Dark Reading 的报告，Shodan 搜索显示，有 30 万台 QNAP 设备连接到互联网，这让此类设备成为颇具吸引力的目标。此外，QNAP 这样的 NAS 设备可能会用作备份，以及媒体或文件服务器。

北美地区其他值得关注的威胁包括 Ramnit、Qakbot 和 REvil。考虑到 Emotet 这样的 IAB 为其他感染（包括但不限于勒索软件）铺平道路的方式，这非常耐人寻味。

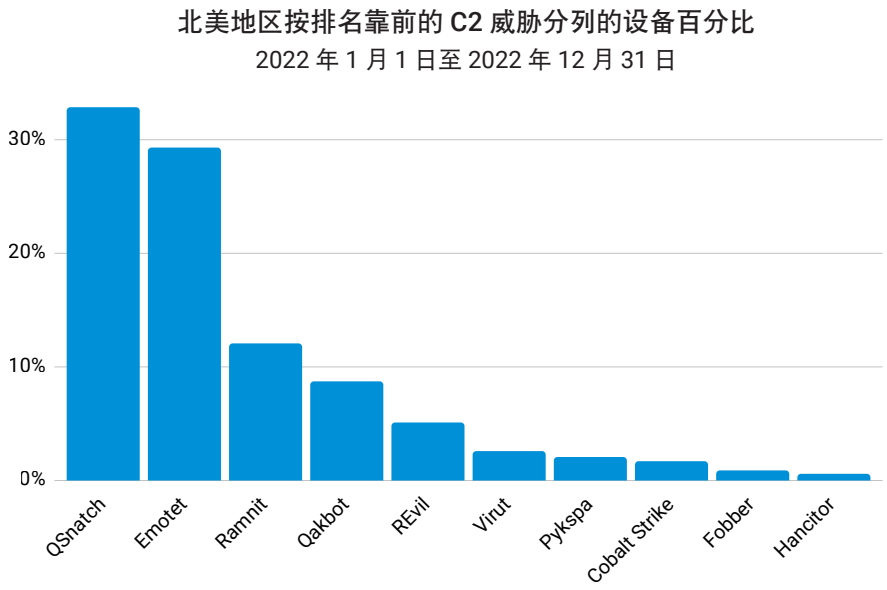


图 8：在北美企业中，大多数受影响设备都至少访问过一次与 QSnatch、Emotet 和 Ramnit 有关的域

欧洲、中东和非洲

欧洲、中东和非洲地区受影响设备的比例也非常高，仅次于北美。我们在该地区观察到的大型威胁（图 9）包括 QSnatch (28%) 和 Ramnit (21%)。Ramnit 在该地区的增加并不让人意外，因为其运营者过去曾将意大利、英国和法国的银行/金融机构作为目标。在 Ramnit 的一次迭代中，其配置将欧盟国家作为主要目标。事实上，如果比较全球受 Ramnit 影响的设备数量，欧洲、中东和非洲地区的受感染设备在 Ramnit 感染的所有设备中占比最高。除此之外，感染 Emotet 的设备在该地区也很高，达到 19%。

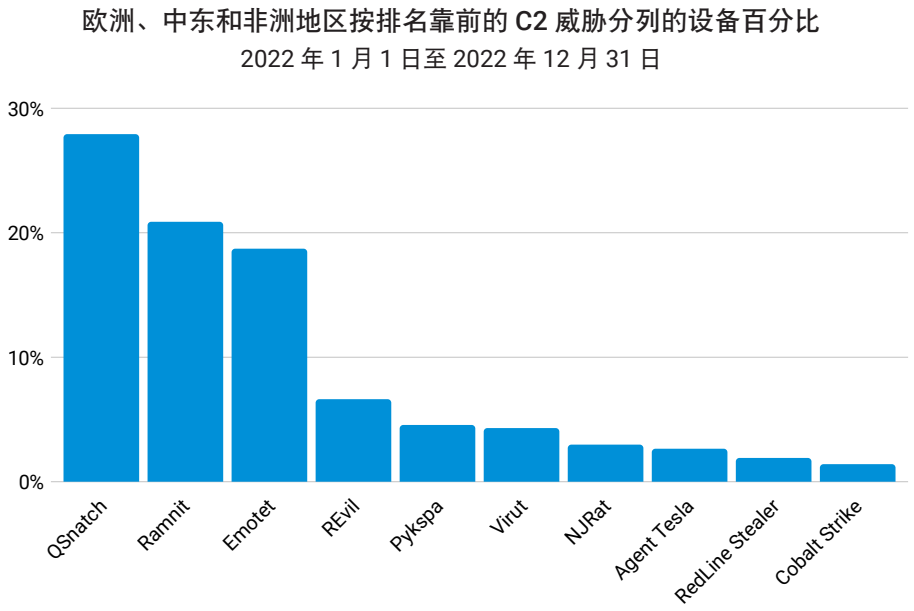


图 9：可以看到，欧洲、中东和非洲地区连接到 Ramnit C2 的数量超过其他地区，这显著增加了该地区企业的风险

亚太地区及日本

QSnatch 的感染对亚太地区及日本产生了重大影响（图 10）。如果比较各地区背后的数字时，就感染 QSnatch 的设备而言，亚太地区及日本排名第二，仅次于北美地区。另一方面，亚太地区及日本还应警惕勒索软件 REvil 和 LockBit，它们均为该地区受影响设备中的五大威胁之列。虽然 REvil 团伙成员在去年被捕，但在几个月后，我们又在现实环境中观察到这种恶意软件的活动。这或许是能获得代码的团伙原成员尝试重新启用 REvil。看到 LockBit 和 REvil 这类勒索软件威胁（主要攻击动机是经济因素）并不让人意外。随着 RaaS 运营者继续利用像 Emotet 这样的 IAB，勒索软件仍将给各行各业、各个地区的企业构成重大安全挑战。

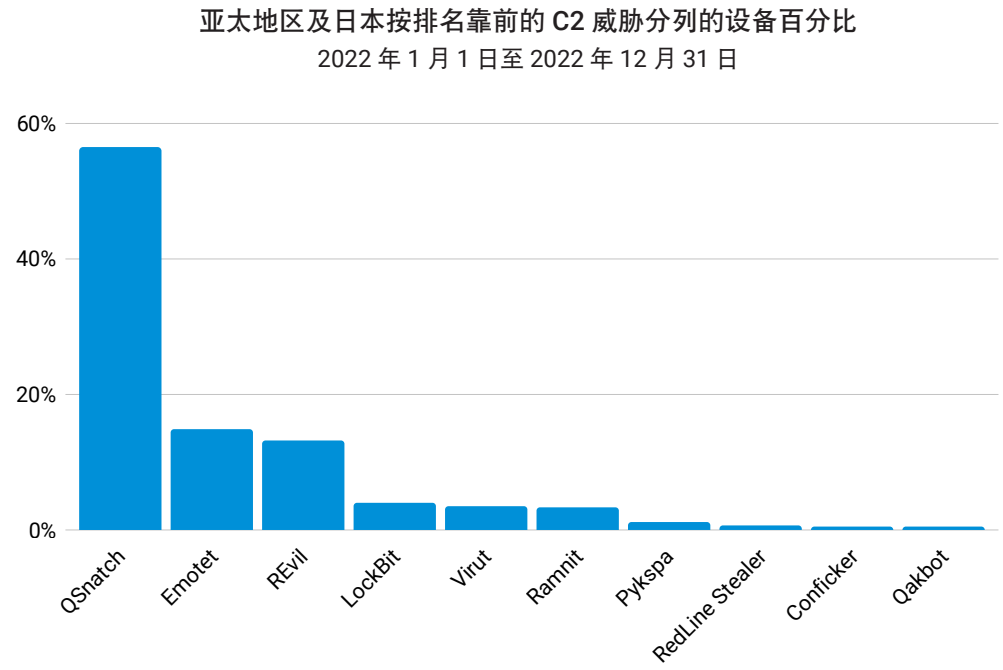


图 10：Akamai 在该地区观察到大量的 QSnatch 感染事件

拉美

再看一下拉美地区的趋势。这个地区受影响的设备数量最少，但这并不一定表示其成为目标的几率较低或受影响较小。该地区也受到了 QSnatch 和 Emotet 的影响（图 11），这与全球趋势一致。单独查看这个地区，可以看到 Agent Tesla、Virut 和 Ramnit 都非常活跃。

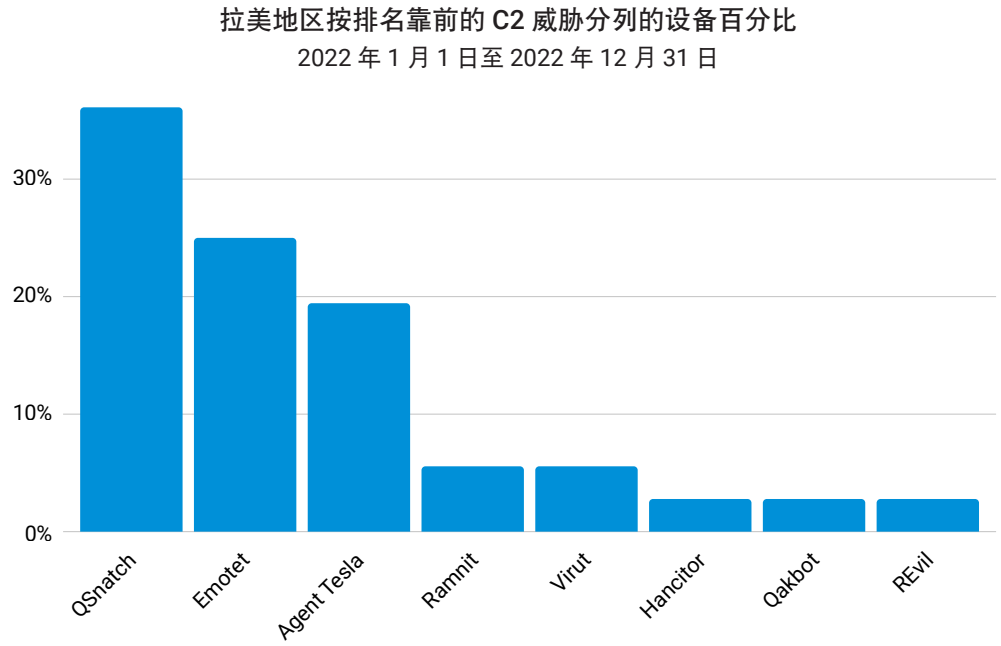


图 11：拉美地区的威胁环境与全球趋势呼应

地区细分非常有意义，这样我们不仅能看到各地区的相似之处，还能了解每个地区的独特威胁。QSnatch 一直是领先的威胁系列，但紧随其后的四大威胁（Emotet、REvil、Ramnit 和 Agent Tesla）在不同地区各有不同。在您确定漏洞管理和渗透测试团队的工作重点时，需要根据地区性的威胁情况作出调整。

行业和垂直领域趋势：制造业受到初始访问代理、僵尸网络的严重冲击

通过分析行业趋势，我们可以看到每个垂直领域的风险水平，并将其与其他行业进行对比。我们并未研究受影响设备的数量，而是按客户汇总设备，得出各垂直领域受影响的公司数量（图 12）。根据我们的 DNS 数据，我们发现，在所分析的存在 C2 流量的企业中，有超过 30% 的比例属于制造业。此外，商业服务 (15%)、高科技 (14%) 和商业 (12%) 等垂直领域的公司也受到了影响。我们的 DNS 数据中排名前两位的垂直领域（制造业和商业服务）也呼应了受 Conti 勒索软件攻击的主要行业，具体请参见我们的全球勒索软件报告。在该报告中，我们深入研究了 Conti 勒索软件的受害者，并按垂直领域、收入和地区进行了分析，说明了这一种类繁多的威胁的攻击趋势。

> **根据我们的 DNS 数据，我们发现，在所分析的存在 C2 流量的企业中，有超过 30% 的比例属于制造业。此外，商业服务 (15%)、高科技 (14%) 和商业 (12%) 等垂直领域的公司也受到了类似的影响。**

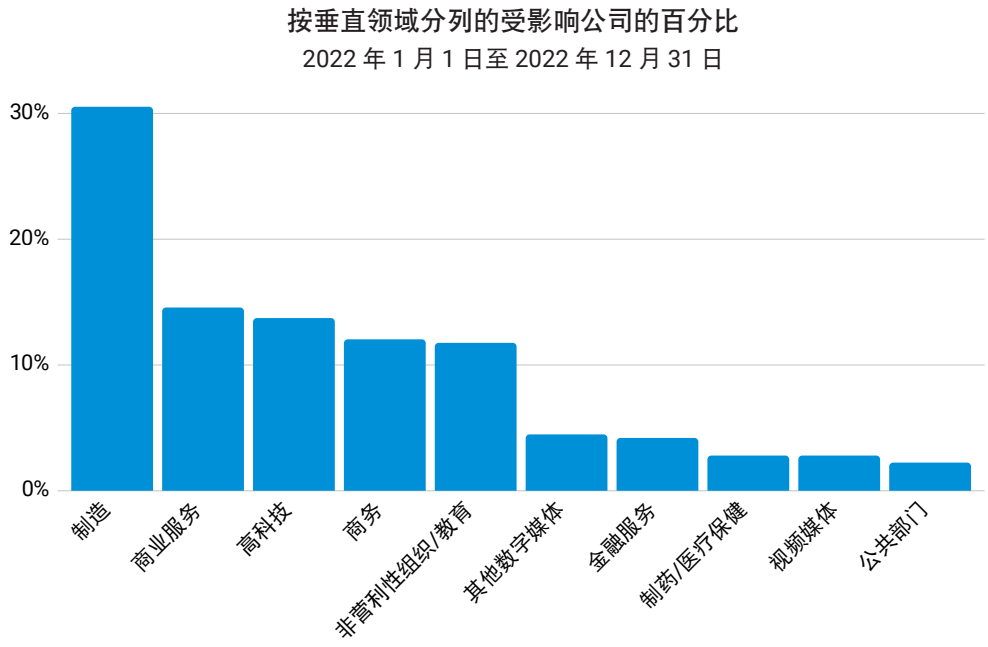


图 12：制造业、商业服务和高科技是受 C2 感染影响最大的行业

我们看到，制造业受各种 C2 攻击的严重侵扰，这让人倍感担忧，因为制造业属于重要行业，如果攻击者得逞，其后果可能会波及现实世界，例如供应链中断。数据无法体现制造业受影响如此之深的具体原因，但更深入地探究这个行业中的威胁类型或许可以让我们一探究竟。

我们看到，一些国家/地区正通过法规加强制造业等关键行业的安全性。面向整个欧盟的 NIS2 立法加强了网络安全标准和安全要求，如风险分析和信息系统安全政策、供应链安全，以及重要实体（如能源、运输、银行、医疗等）的事件处理。它还扩大了受影响的垂直领域的范围。

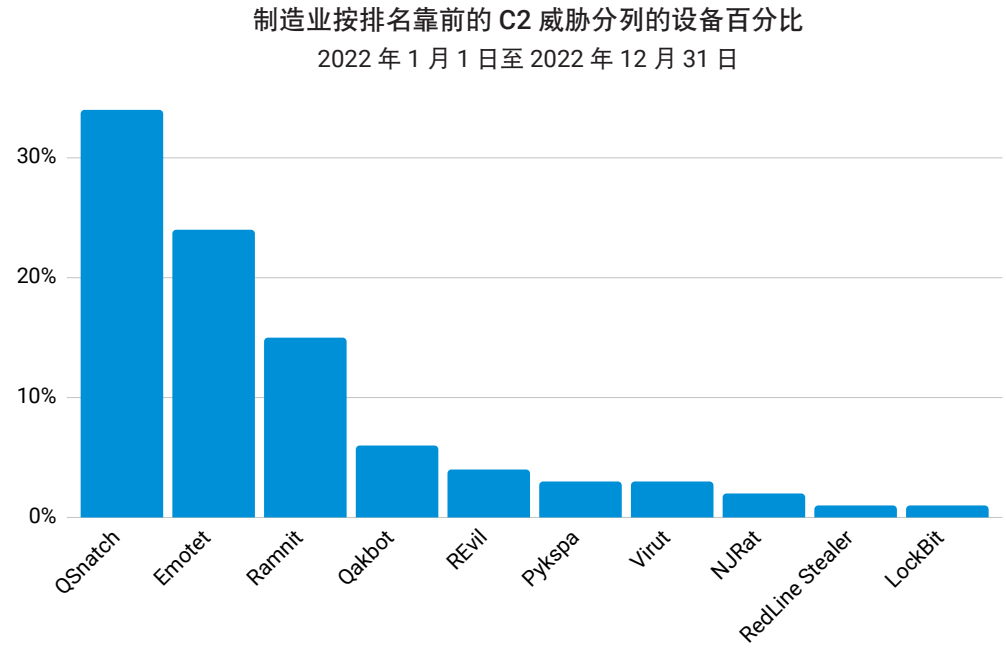


图 13：在制造业中发现的排名靠前的 C2 威胁系列是 QSnatch、Emotet 和 Ramnit

对制造业的深入研究表明，在该垂直领域的企业访问的 C2 相关域中，排名靠前的包括 QSnatch、IAB 和 Ramnit 域（图 13）。其网络中出现 IAB 可能表明攻击者在收集有关其潜在目标的情报，一旦获得所入侵设备的访问权限，攻击者即可将这些数据出售给其他网络犯罪分子，比如 RaaS 团伙。此外，在威胁该行业的 C2 恶意软件列表中，我们还能看到信息窃取工具的身影。需要警惕的一项威胁是 RedLine Stealer，它能收集浏览器信息，如凭据和信用卡详细信息，而且目前以 MaaS 的形式出售，每月订阅费用为 100-150 美元。根据 Group-IB 的研究，在 2021 年下半年至 2022 年上半年期间，这种信息窃取工具估计获取了 35,585,412 份日志，其中可能包含单点登录帐户。此外，仅在 2022 年第三季度，与这种信息窃取工具有关的 C2 域名就激增 409%。

跟踪行业趋势总是让人兴趣盎然。在一个垂直领域发生的情况往往只是垫脚石，网络犯罪分子的目标是整个行业中的所有垂直领域。有时，我们会看到攻击者侧重于一个行业内的某项突出技术。其他时候，他们会去寻找更有可能付钱的受害者，或者有可能支付最多赎金的受害者。我们也观察到，他们会对历来不注重网络安全投资的行业下手。这里的启示是，如果您看到隔壁冒烟，最好也检查一下自己家的消防系统。

家庭用户面临攻击威胁

攻击者将目标投向企业的原因不言自明，成功入侵企业网络可给他们带来更高的回报。他们使用广泛的工具和战术渗透到企业周边，维系持久性，并在某些情况下泄露机密信息。因此我们会在企业网络中看到了上一节所讨论的信息窃取工具和 IAB 等威胁。但在家庭网络中则是另外一番景象，所利用的威胁和目的都有所不同。

家庭用户的安全防护措施通常没有企业环境完善，但这个群体能给攻击者带来的经济回报也不如企业。攻击者甚至这一点，并设法通过简化感染家庭设备的能力变现。例如，他们发起大规模的活动，通过“广撒网”的战术入侵尽可能多的设备，而对于企业的攻击则具有高度的针对性。在这些家庭设备成为大规模僵尸网络的一部分后，攻击者即可调动这些僵尸设备，在用户不知情的情况下开展不计其数的网络犯罪活动，如发送垃圾邮件，以及对企业发动 DDoS 攻击。僵尸网络要想取得成功，网络犯罪分子要想出租其僵尸网络，前提就是感染尽可能多的设备。在影响家庭用户时，攻击者还可通过另一种方式获得经济利益，即利用受感染设备的计算资源进行加密货币挖矿。

> **在这些设备成为大规模僵尸网络的一部分后，攻击者即可调动这些僵尸设备，在用户不知情的情况下开展不计其数的网络犯罪活动，如发送垃圾邮件，以及对企业发动 DDoS 攻击。**

家庭网络显示出大量来自僵尸网络的流量

在将关注重点转移到家庭用户时，我们将分析一组匿名样本，其中包含过去六个月间数亿项识别为恶意的查询，从而审视家庭网络的恶意 DNS 流量，指明用户应该关注的威胁。您可以一目了然地看出，最大的威胁与僵尸网络有关，这可以解释攻击者如何利用 IoT 设备达到不同的目的，后续几节将讨论这个主题。

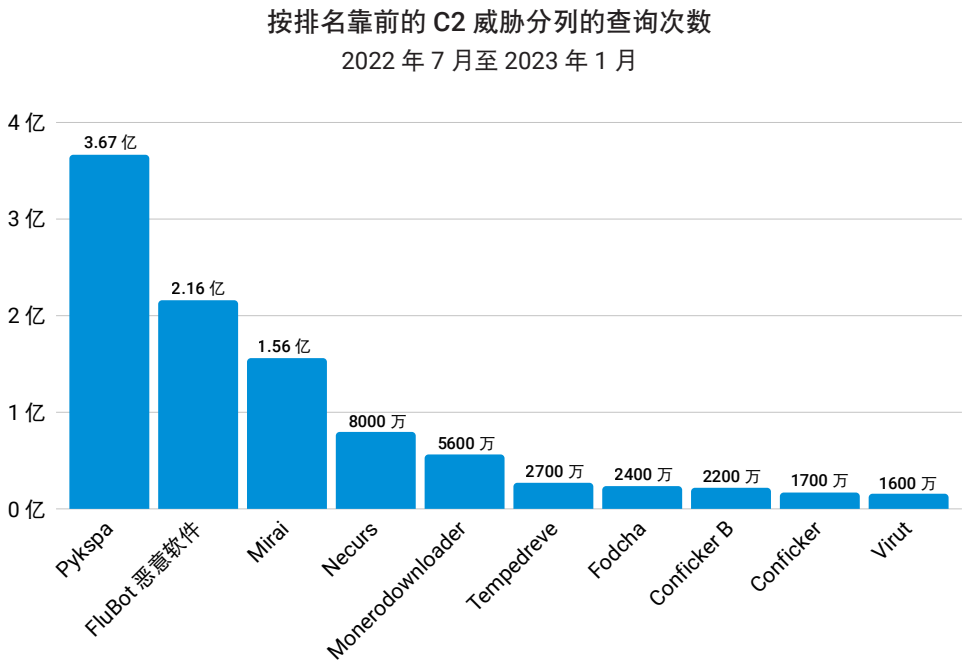


图 14：在家庭网络的 DNS 流量中观测到的僵尸网络中，排名前三位的分别是 Pykspa、FluBot 恶意软件和 Mirai

Pykspa：通过社交媒体传播

根据我们的数据结论，在全球识别出的恶意 DNS 查询中，Pykspa 的数量多达 3.67 亿项（图 14）。这种威胁的传播方式是通过 Skype 向受影响用户的联系人发送恶意链接。在某些情况下，用户在浏览器标签页中打开 Twitter 网站时，它还会创建一个带有恶意软件下载链接的推文。此外，它使用域生成算法 (DGA) 建立 C2 通信。先前的 V2 版使用其 DGA 的一个子集来规避检测，并在网络内藏匿更长时间。

其后门功能允许攻击者连接到远程系统并执行任意命令，如下载文件、终止进程，并通过各种方式（如映射驱动器、网络共享）进行传播等。Pykspa 还会查询 Skype 配置，收集受影响用户的个人信息。它还会阻止用户访问某些网站，特别是包含某些与反恶意软件解决方案有关的字符串的网站。有趣的是，这一恶意软件会检查受影响用户的 Skype 语言界面，如果是其监测的众多语言之一（包括英语、德语、法语、西班牙语和意大利语），它会相应地调整垃圾邮件。

FluBot：Android 恶意软件僵尸网络

FluBot 恶意软件是继 Pykspa 之后的又一个热门 C2 恶意软件系列。它主要通过短信感染 Android 手机，诱使用户点击恶意链接，随后下载恶意软件。作为其传播策略的一部分，FluBot 恶意软件会将受影响用户的联系人名单上传到 C2 服务器，并且向受害者的联系人发送同样的社会工程诱饵。对于用户来说，设备上存在 FluBot 会给他们的银行和财务信息造成危险，因为这种恶意软件能在用户访问合法银行应用程序时显示一个伪造的页面叠加层。因此，用户凭据可能会被用于身份盗窃或欺诈交易。

这种恶意软件使用各种社会工程诱饵。例如，它可能会建议用户点击某个链接来检查包裹配送状态；还可能告诉用户有语音留言，并欺骗用户下载伪造的语音邮件应用程序。它也可能伪称有安全更新，催促用户点击链接。一旦用户点击该链接，它就会指示他们下载一个应用程序。这个应用程序会要求联系人名单和拨打电话等授权。导致该威胁更加危险的是，它还要求获得无障碍服务权限，这让攻击者能够控制屏幕点按操作，有可能会因此而安装更多应用程序。建议用户将其设备重置为出厂设置，以删除此恶意软件。

Mirai：利用物联网的力量造成大规模破坏

在我们的研究中，识别出的 Mirai DNS 查询量达到 1.56 亿次，仅次于 FluBot 恶意软件。Mirai 以攻击开放 telnet 端口的 IoT 设备而闻名，曾对最大的 DNS 供应商之一发起 DDoS 攻击，并因此恶名昭著。这种具备自我传播能力的蠕虫病毒会寻找使用默认用户名和密码组合的易入侵设备。其聚集的僵尸设备数量一度超过 10 万台，攻击者利用这些设备对高知名度的目标发起了 DDoS 攻击。在其早期的一次攻击中，Mirai 利用 14.5 万台设备攻击了一家科技公司。这个例子表明，不安全的设备可能成为网络攻击的武器，给企业造成大规模破坏。

2016 年，Mirai 背后的团伙公开了源代码，或许是为了防止执法部门顺藤摸瓜找到原作者，避免牢狱之灾。此后，其他团伙开始使用 Mirai 的代码，对其进行修改和增强，并添加了更多功能，例如感染系统的功能。其代码公开的影响之一是催生了新变种，如 Okiru、Satori、Masuta 和 PureMasuta，其目的同样是发起 DDoS 攻击。重启受感染的设备确实有所帮助，但该恶意软件会不断扫描设备，因此除非用户更改密码，否则很有可能再次感染。

Necurs：恶意软件经销商和访问权限卖家

Necurs 僵尸网络最初发现于 2012 年，在过去六个月中，识别出的相关查询量达到 8,000 万。它能传输其他恶意软件的攻击载荷，如 Dridex、TrickBot 和 Locky 等，因此给家庭用户和企业造成了严重风险。有必要指出，该僵尸网络还通过僵尸网络出租服务向其他团伙出售受感染计算机的访问权限。类似于大多数僵尸网络，它使用 DGA 为其 C2 服务器动态生成多个域，保证在域名被封锁的情况下继续工作。

除了用于分发勒索软件和银行木马外，Necurs 还被广泛用于分发多种垃圾邮件攻击，如俄罗斯约会诈骗、医药诈骗等。在一次调查中，Microsoft 监测了该僵尸网络的活动，发现它在短短 58 天内发出了大约 380 万封垃圾邮件。2020 年，执法部门和安全界携手合作，端掉了 Necurs 僵尸网络。

Monerodownloader：挖矿僵尸网络

攻击者通过许多方式谋利，其中之一就是利用被入侵的设备进行加密货币挖矿。我们观察到许多专为门罗币挖矿打造的僵尸网络，其原因之一就是门罗币在网络犯罪分子中越来越受欢迎。门罗币的区块链风险敞口不是太高，而且有着匿名机制；因此无法追溯到他们个人。虽然我们目前对于 Monerodownloader 知之甚少，不过它所执行的一些战术包括收集信息，并连接到 C2 服务器以获得实际攻击载荷。

不及时修补会让系统对门罗币加密货币挖矿程序等威胁大开门户。其他类似的门罗币挖矿程序利用漏洞，冒充成免费软件引诱用户下载，还能够通过网络横向移动、感染其他设备，以获得尽可能多的收入。虽然横向移动这种说法本身更适合企业，不太适合家庭用户，但我们可以借此了解加密货币挖矿程序如何尽可能提高感染率。

各地区的头号威胁：在家庭网络中，僵尸网络依然排名第一

我们来仔细看一下地区数据，根据家庭网络的 DNS 流量解析各地区盛行的僵尸网络有哪些，并探究可能促成这类趋势的一些可能因素。

北美

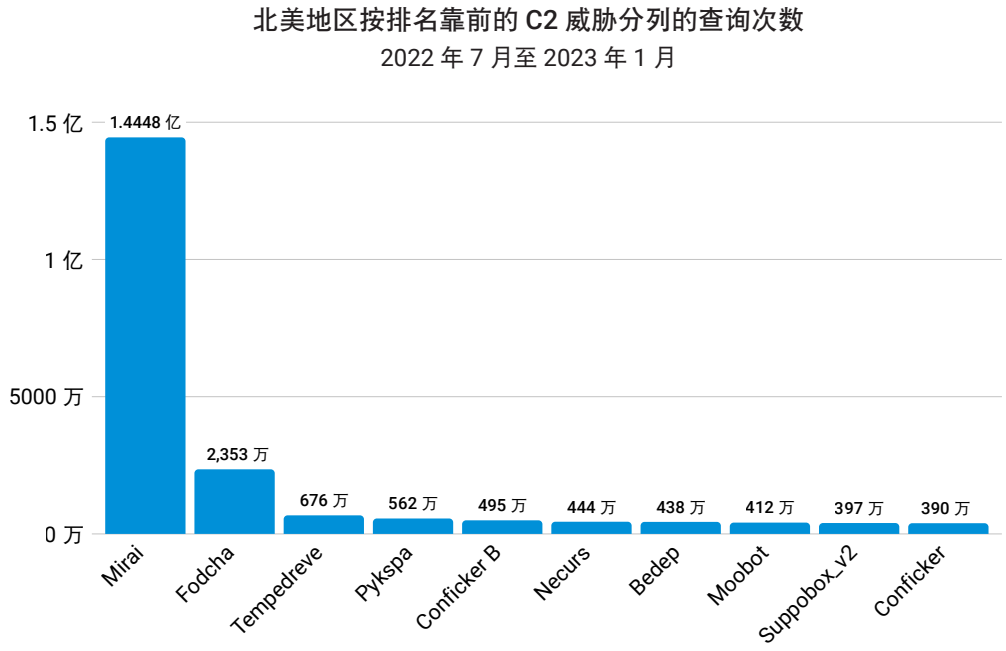


图 15：Mirai 依然在北美兴风作浪，原因或许是不安全的 IoT 设备

在北美地区，家庭网络中与 Mirai 僵尸网络有关的查询超过 1.44 亿次（图 15）。该僵尸网络的目标是仍在使用默认用户名和密码的易入侵 IoT 设备。来自该地区的查询数量较大，或许是因为 IoT 设备在该地区家庭中的普及率或使用率较高。据报道，在 2022 年，美国家庭的联网设备平均拥有量是 22 台，比上一年的 25 台略有下降。IoT 连接量在北美预计还会增加（到 2025 年达到 54 亿），未来很有可能出现更多类似于 Mirai 或近似变种的威胁，滥用不安全的 IoT 设备。

这种威胁会给家庭用户造成的影响是，网络犯罪分子可以利用其设备实施犯罪，而他们本人毫不知情。但 DDoS 攻击乃至 Mirai 等僵尸网络发起的恶意垃圾邮件也会给企业带来困扰。比较理想的做法是遵循最佳实践，改掉设备的默认用户名和密码，避免其受到 Mirai 和其他类似攻击。

欧洲、中东和非洲

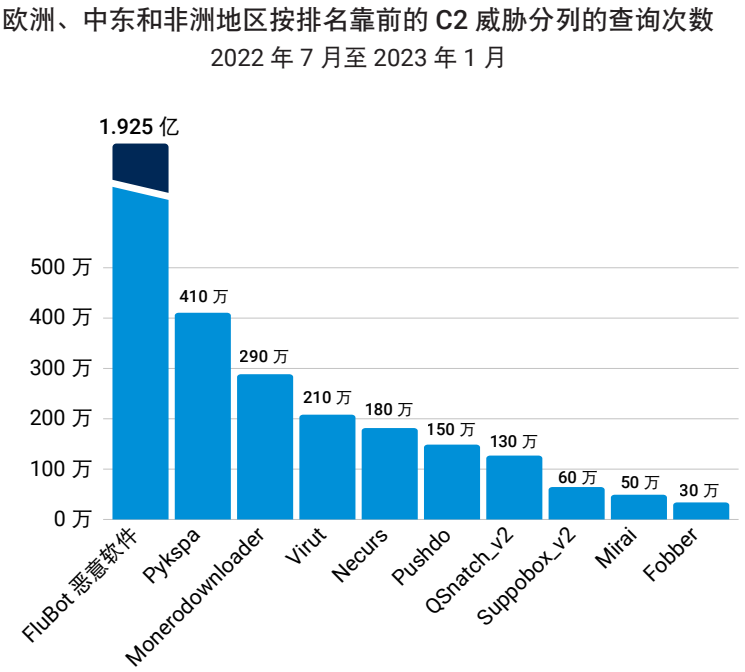


图 16：我们观察到，FluBot 恶意软件在欧洲、中东和非洲地区出现爆发，原因或许是其传播策略，及其社会工程诱饵中使用了数种欧洲语言

用“野火”来形容 FluBot 恶意软件在欧洲、中东和非洲地区的肆虐也只能说是轻描淡写。在该地区观察到了令人惊叹的庞大 DNS 查询量（约 1.93 亿）。通过审查 DNS 流量，我们确定了这些感染确实发生在欧洲、中东和非洲地区（图 16）。一个促成因素是其采用了短信网络钓鱼的战术，在这种形式的网络钓鱼中，攻击者向受害者的联系人名单发送短信。此外，它还会哄骗用户下载一个与包裹物流或语音邮件有关的应用程序，但这个应用程序实际上是恶意软件。除此之外，FluBot 还要求获得额外的权限，并在用户不知情的情况下秘密记录下用户的银行/财务凭据。根据报告，其针对的用户位于西班牙、德国、芬兰和英国等国家和地区。短信还使用其他多种欧盟语言，如德语和匈牙利语，这或许是这种恶意软件在欧洲激增的众多因素之一。

拉美

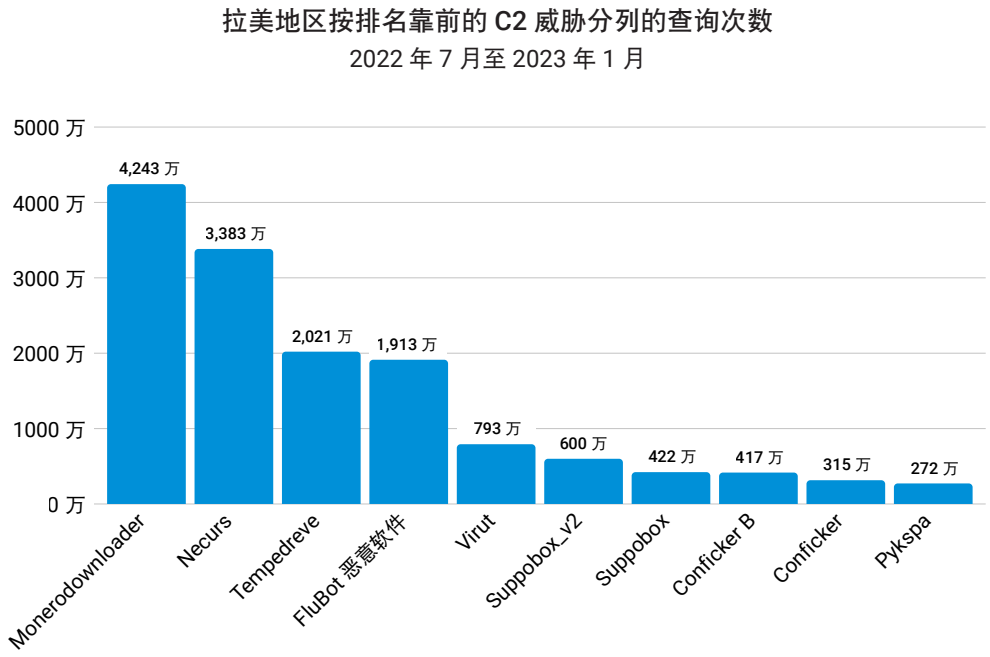


图 17：Monerodownloader 加密货币挖矿僵尸网络成为拉美地区的头号威胁，原因或许是该地区对加密货币的使用率较高

不同于北美地区以及欧洲、中东和非洲地区，拉美地区的僵尸网络分布更加多样化（图 17）。Monerodownloader 是一种加密的僵尸网络，识别出的查询量达到 4,200 万次，并因此在活跃的僵尸网络分组中位居榜首，其次是 Necurs（3,400 万）和 Tempedreve（2,000 万）。在高通胀和高汇款额的推动下，该地区的加密货币采用率很高，正因如此，像 Monerodownloader 这样的僵尸网络才能位列榜首。在用户不知情的情况下，网络犯罪分子可能将用户设备的资源用于加密货币挖矿，从中谋利。另外值得注意的是，在 DNS 流量的观察结果中，FluBot 是一个极其重要的威胁，也就是说，除了我们观察到大量相关流量的 EMEA 地区之外，这种僵尸网络的活动也很猖獗。

亚太地区及日本

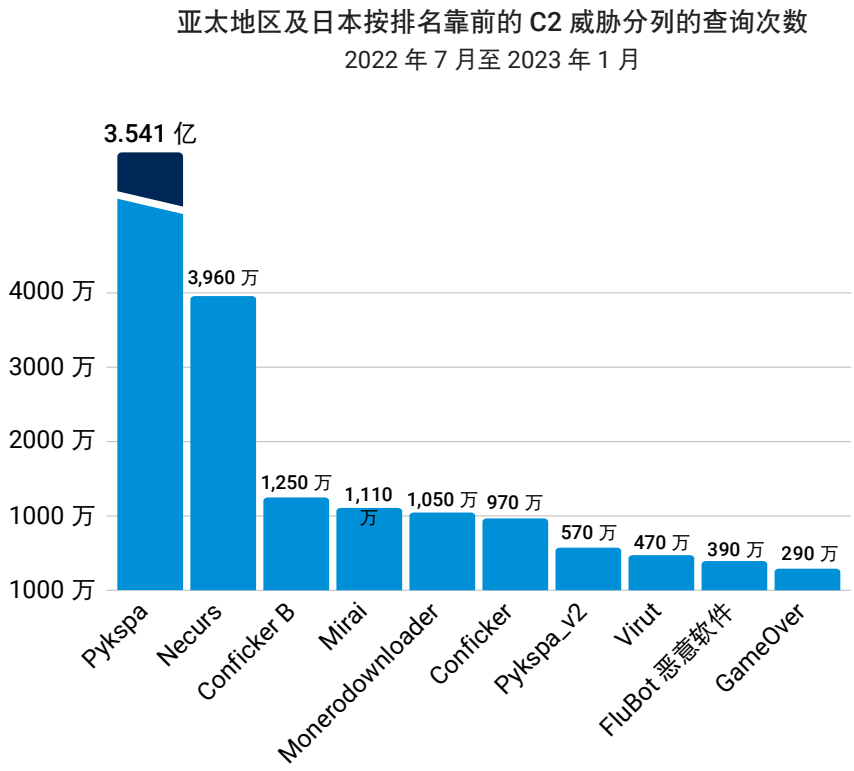


图 18：亚太地区及日本的主要威胁包括 Pykspa 和 Necurs

在亚太地区及日本，我们观察到超过 3.5 亿次与 Pykspa 有关的查询（图 18）。在 2019 年的一篇博文中，我们指出 Pykspa 使用了一种选择性的 DGA 机制，可以达到长时间藏匿的效果。那份报告中强调的领域主要集中在东亚。我们还观察到与 Necurs 等僵尸网络有关的查询，这是一项表明系统被其他恶意软件感染的有力指标。

网络钓鱼现状概述

在 DNS 流量分析的最后一部分，我们研究了网络钓鱼工具包及其在网络钓鱼活动成功中的关键作用。攻击者使用的战术不断演变，而且网上可获得的个人信息越来越多，因此网络钓鱼仍然与我们息息相关，甚至比以往更相关。如今的攻击者使用社会工程来更好地伪装其网络钓鱼，使其看起来更加合法，证据也表明，这些攻击的成功率仍然很高。Akamai 对假日钓鱼诈骗的研究表明，攻击者正在利用新的技术和战术逃脱检测。新战术包括在诈骗中使用虚假的用户荐言，还有新发现的使用 HTML 锚定的技术，确保只有有效用户才能登陆诈骗网站。

新冠疫情促使远程办公普及，这加大了检测和预防网络钓鱼攻击的难度，因此个人和企业更有必要保持警惕，并采取措施来保护自己。此外，社交媒体兴起，接入互联网的设备不断增加，这都给攻击者创造了更多机会。

网络钓鱼活动影响金融服务业

调查哪些品牌正在被网络钓鱼骗局滥用和模仿时，我们可以使用大量方法收集数据。我们收集了攻击活动总数量与受害者数量。方便评估给定攻击活动的成功率，了解每个行业中成为攻击目标的比例。

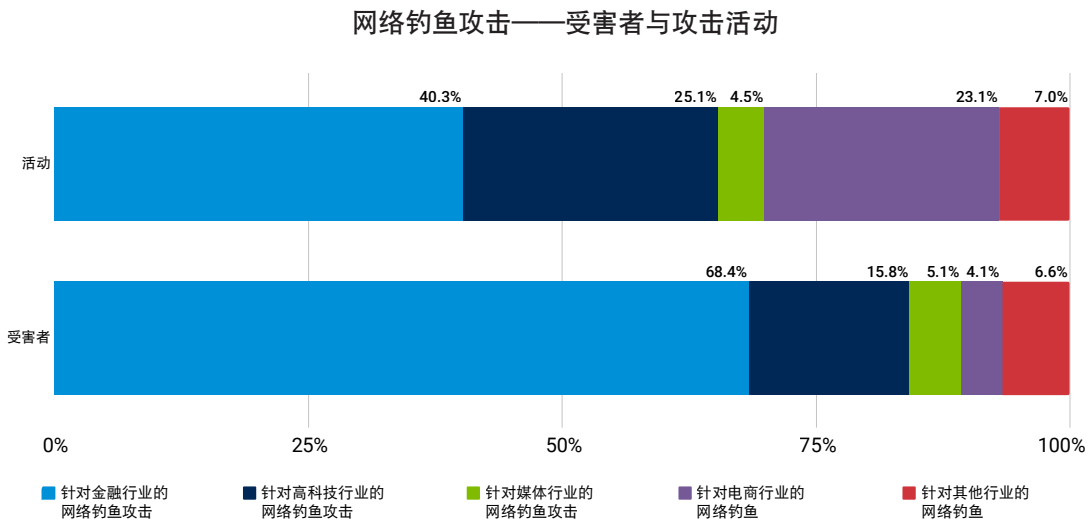


图 19：大多数网络钓鱼活动将金融服务行业作为目标（2022 年第四季度）

我们的研究发现，金融和高科技品牌在攻击活动数量和受害者数量上都排名靠前（图 19）。我们看到，针对金融服务客户的攻击占发起的攻击活动总数的 40.3%，相应的受害者数量占受害者总数的 68.4%。这表明针对金融服务的攻击在 2022 年第四季度影响巨大。在我们的金融服务业相关报告《兵临城下：针对金融服务领域的攻击分析》中，我们强调了网络钓鱼攻击是如何谋取财务收益为动机，将金融服务业及其客户作为主要攻击对象。这类攻击的潜在影响包括品牌及其名誉蒙损，以及客户信任丧失。网络钓鱼还可能导致企业需要耗费大量资源来修复问题。

2022 年第四季度，有 23% 的网络钓鱼活动针对电商领域。我们看到的攻击活动数量多余实际受害者数量，但同样应该引起注意，这表明该行业成为攻击者的目标，用户必须保持警惕，避免网络犯罪分子窃取其个人信息或银行信息。

网络钓鱼工具包：助纣为虐

网络钓鱼工具包的存在使得网络钓鱼规模庞大、日益严重。网络钓鱼工具包支持部署和维护钓鱼网站，甚至支持非技术型诈骗者加入网络钓鱼攻击者行列，实施网络钓鱼骗局。

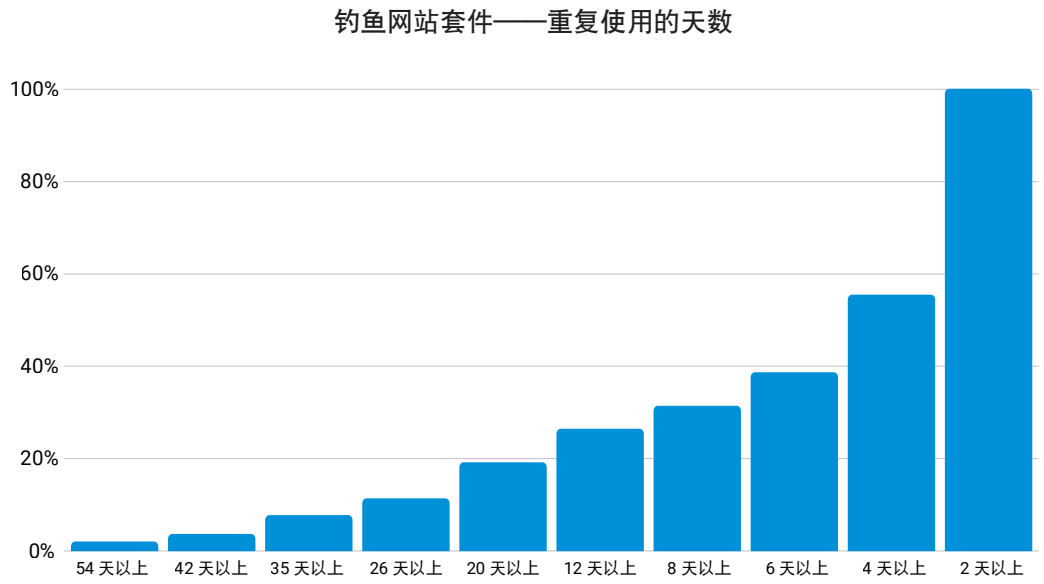


图 20：网络钓鱼工具包（按 2022 年第四季度重复使用的天数列出）

根据我们跟踪现实环境中使用的 300 多种不同网络钓鱼工具包（用于发动新的攻击活动）的研究，可以看出 2022 年第四季度，2.04% 的受跟踪工具包至少有 54 天（同一天内多次使用时，仅按一天统计）得到了重复使用（图 20）。此外，55.5% 的工具包被重复使用了至少四天，以发起新的攻击活动，所有受跟踪的工具包在 2022 年第四季度均被重复使用了不少于两天（同一天内多次使用时，仅按一天统计）。

结论和建议：主动出击，应对现代攻击

我们已经介绍了威胁分组和攻击者采用的方法，下面谈谈如何利用所有这些信息。首先是如何管理 DNS，具体方法可以是在内部管理，也可以是外包给第三方。对于规模较大或较为复杂的企业，请一家专门管理 DNS 的提供商代劳是比较合理的方案。无论如何，务必要监测 DNS 的性能和保护情况。接下来，您应该考虑需要的各种控制措施。DDoS 防护、恶意软件攻击、抓取、横向移动和渗透都是抵御工作中需要关注的重要领域。在这段数据之旅的每一步中，寻找您可以阻止的安全漏洞——这其实是一种通常称为“网络击杀链”的网络安全模型。

考虑制定行动手册，以应对本报告中介绍的攻击技术。与您的渗透测试团队或红团核对，确定他们是否（在实验室环境中）使用与 Qakbot 和 Emotet 等 IAB、QSnatch 等爬虫程序、LockBit 等勒索软件相同的工具和技术，并且使用 Cobalt Strike 等工具。务必确保您的安全控制措施能够有效地就这些类型的攻击发出提醒，有效地加以阻止，还要确保您的团队接受应对这些攻击的培训。

如果在您的网络中检测到 Cobalt Strike，比较谨慎的做法是立即创建事件报告并开展调查。虽然有可能是您的红队在使用该工具（即便如此，也应调查和报告），但只要存在这种流量，就应该提起警惕，因为这可能表明其他 RaaS 攻击团伙或攻击者入侵，也表明您仍有抵御的机会。

考虑您的安全运营中心的运营方式，确定如何跟踪可能表明 IAB 相关威胁在您网络中侦查的进程（如 BITS、Wget 或 cURL）。关键的环节是弄清有哪些下载的运行，并及时阻止正在进行的下载。然后，调查触发 IAB 的原因——是 LNK 文件、宏还是 VScript？随后探究入侵的源头。

敬请访问我们的安全研究中心，随时了解我们的最新研究资讯。

方法

命令和控制攻击流量

本报告中的数据由我们的 Secure Internet Access (SIA) 产品生成，描述了命令和控制 (C2) 攻击流量。SIA 是一种云端安全 Web 网关，旨在帮助用户安全、轻松地将其设备连接到互联网。本报告中使用了两组不同的数据，分别反映了来自拥有大量用户的企业及具有个人家庭用户的互联网提供商的安全警报数据。此数据的衡量依据是受影响的设备数量和查询数量。受影响的设备定义为：至少连接过已知、确定的 C2 域一次的设备。类似地，C2 查询的定义是：连接过已知、确定的 C2 域的查询。我们的安全团队在内部使用这些数据来研究攻击、识别恶意行为，从而向用户发布相关通知，并为 Akamai 安全解决方案提供额外的情报。

致谢名单

编辑与创作

Or Katz

Eliad Kimhy

Badette Tribbey

审稿和主题撰稿

Tanya Belousov

Shiran Guez

Ophir Harpaz

Stiv Kupchik

Grace Wang

Steve Winterfeld

数据分析

Ronan Ballantine

Gal Kochner

Chelsea Tuttle

营销与发布

Georgina Morales Hampe

Shivangi Sahu

更多《互联网现状/安全性》

回顾往期报告，并关注 Akamai 备受好评的《互联网现状/安全性》后续报告。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

访问此报告中的数据

查看本报告中引用的图形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 为应对针对企业的威胁提供的解决方案，请访问我们的 Secure Internet Access Enterprise 页面。面向消费者和中小企业市场的服务提供商可访问面向 ISP 的 Secure Internet Access 服务。

Akamai 支持并保护网络生活。全球各大优秀公司纷纷选择 Akamai 来打造并提供安全的数字化体验，为数十亿人每天的生活、工作和娱乐提供助力。Akamai Connected Cloud 是一种大规模分布式边缘和云平台，可使应用程序和体验更靠近用户，帮助用户远离威胁。如需详细了解 Akamai 的云计算、安全和内容交付解决方案，请访问 akamai.com 和 akamai.com/blog，或者扫描下方二维码，关注我们的微信公众号
发布时间：2023 年 3 月