McAfee Labs 威胁报告

2020 年 11 月

McAfee 威胁研究团队全心全意致力于确保您的数据和系统安全，并且首次推出了 MVISION Insights 预览信息显示板，用于展示此类威胁活动的流行情况。

此报告的研究及编写人员：
- Christiaan Beek
- Sandeep Chandana
- Taylor Dunton
- Steve Grobman
- Rajiv Gupta
- Tracy Holden
- Tim Hux
- Kevin McGrath
- Douglas McKee
- Lee Munson
- Kaushik Narayan
- Joy Olowo
- Chanung Pak
- Chris Palm
- Tim Polzer
- Sang Ryol Ryu
- Raj Samani
- Sekhar Sarukkai
- Craig Schmugar

简介

今年是不寻常的一年！2020 年第 1 季度，我们忙于抵御恶意分子利用 COVID-19 发起的来势汹汹的攻击活动，而在第 2 季度，没有迹象表明这些攻击活动有任何减弱的趋势。事实上，当我们继续在家办公，尽一切努力确保各项工作正常运行之际，不法分子似乎正绞尽脑汁企图从疫情中牟利。McAfee 遍布全球数十亿传感器组成的全球威胁情报网络，检测到第 2 季度以 COVID-19 为主题的威胁活动总数暴涨了 605%。您可以查看 McAfee COVID-19 威胁信息显示板，了解疫情相关威胁活动的最新信息。

McAfee 威胁研究团队全心全意致力于确保您的数据和系统安全，并且首次推出了 MVISION Insights 预览信息显示板，用于展示此类威胁活动的流行情况。此外，您还可以查看 Yara 规则、IoC 以及此类攻击活动在 MITRE ATT&CK 框架下的对应信息。我们每周都会更新这些攻击活动，因此实际上，伴随这份威胁报告的还有一个信息显示板，可以显示特定攻击活动的更多详细信息。

关注

分享

衷心希望您不仅可以从这份威胁报告中，而且还可以从我们的信息显示板中，看到对您有价值的内容和数据。您的反馈对我们极为重要，并且我们做的这些工作，都是为了让您既可以从宏观上了解威胁态势（这份报告），又可以从微观上掌握切实可行的情报 (MVISION Insights)，从而更好地确保安全。

希望您会喜欢这期内容丰盛的《McAfee Labs 威胁报告：2020 年 11 月》。

顺颂冬安

—Raj Samani

Twitter @Raj_Samani

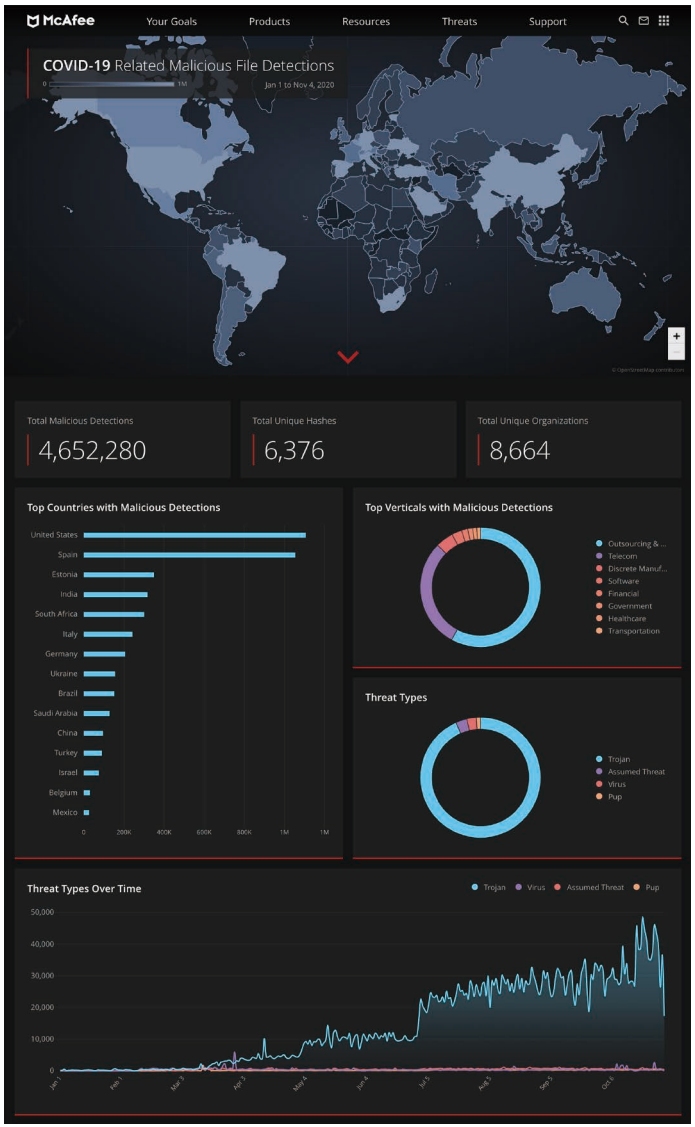


图 1. McAfee 遍布全球数十亿传感器组成的全球威胁情报网络，检测到第 2 季度以 COVID-19 为主题的威胁活动总数暴涨了 605%。

关注

分享

目录

2 简介

5 对各行业的威胁以及威胁媒介

8 恶意软件威胁统计信息

13 政府机构面临多云环境挑战

14 攻击者使用元数据攻破 AWS 中的应用程序

19 McAfee 对机器人漏洞的调查研究

21 MalBus 攻击者将攻击阵地从 Google Play 转移到 ONE Store

23 Ripple20 漏洞缓解最佳实践

25 警惕 OneDrive 网络钓鱼

26 资源

在这份报告中，McAfee® Labs 对 2020 年第 2 季度出现的安全威胁进行了仔细研读。对于各种威胁和攻击，我们的 Advanced Threat Research 团队始终保持警惕并积极进行跟踪、识别和研究，掌握最新攻击活动的来龙去脉。

2020 年第 1 季度，全球开始陷入新冠疫情大流行；2020 年第 2 季度，企业继续采取应对措施，空前数量的员工在家远程办公，因此，网络安全持续考验着新常态下的办公需求。

历时六个月之后，首席信息安全官 (CISO) 和安全团队面对的威胁，无论演化的速度还是数量和规模的增长，都是前所未见。不法分子利用日益复杂的攻击技术，有针对性地向那些仍然受困于新冠疫情限制、有可能在远程设备和带宽安全方面暴露出潜在漏洞的企业、政府机构、学校和个人发起攻击。

历时六个月之后，对员工而言，遵守安全守则并对攻击者保持警觉依然至关重要。在点击外部电子邮件附件和未经验证的链接时，应慎之又慎，因为附件和链接经常被用作网络钓鱼的切入点，是传播和启动勒索软件、RDP 漏洞及其他恶意软件的载体。

与以往一样，McAfee 研究人员的侧重点在于网络犯罪分子所采用的战术和技术。我们将一如既往地继续努力，确保客户和社群的安全。McAfee 持续监测其遍布全球的数十亿传感器，借助这个网络提供的情报和强大的洞察，协助企业抵御威胁、保护资产安全。

有关不断演化的威胁的最新信息，请访问 McAfee 威胁中心。

对各行业的威胁以及威胁媒介

2020 年第 2 季度，McAfee Labs 观测到的恶意软件威胁数量平均为每分钟 419 个威胁，每分钟的威胁数量增加了 44 个，增幅为 12%。

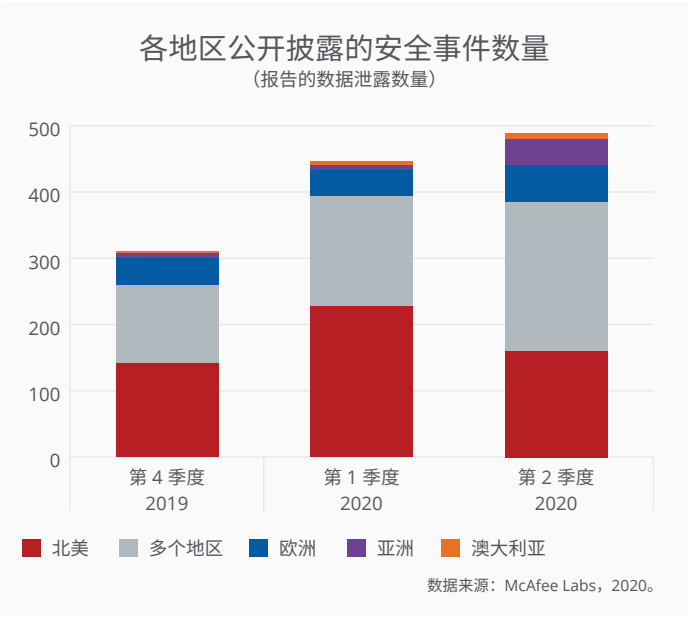


图 2. 据 McAfee Labs 统计，2020 年第 2 季度公开披露的安全事件数量为 561 起，包括地区目标不适用的事件，比 2020 年第 1 季度增加了 22%。在披露的安全事件中，以美国为目标地区的事件占总数的 29%，比上一季度降低了 30%，而以欧洲为目标地区的安全事件则占总数的 10%。

关注

分享

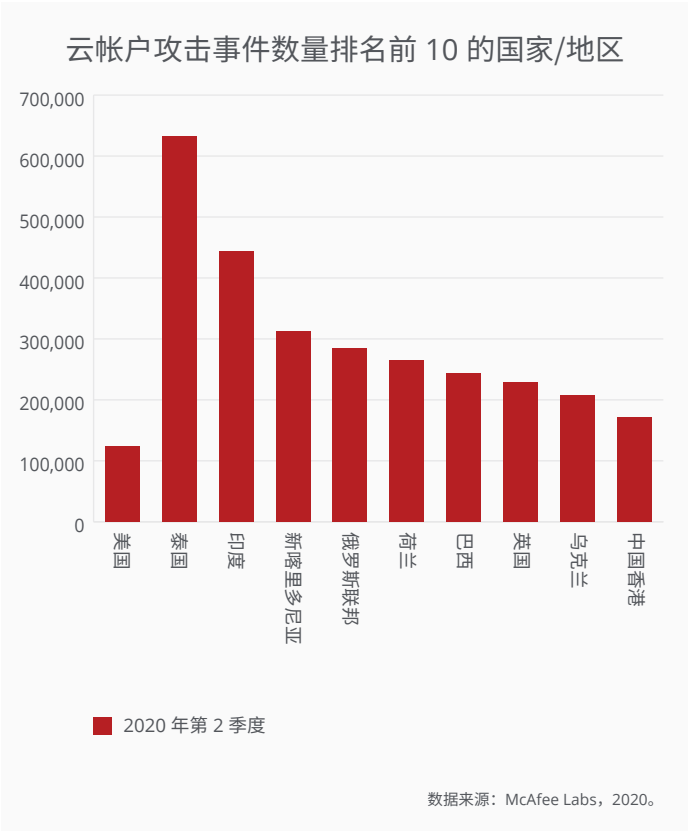


图 3. 2020 年第 2 季度，McAfee 收集并匿名处理了全球超过 3000 万 McAfee MVISION Cloud 用户的云使用情况数据，从中观测到大约 750 万次针对云帐户的外部攻击活动。这组数据涵盖的公司遍及全球所有主要行业，包括金融服务、医疗卫生、公共部门、教育、零售、技术、制造业、能源、公用事业、法律、房地产、交通运输以及商业服务。

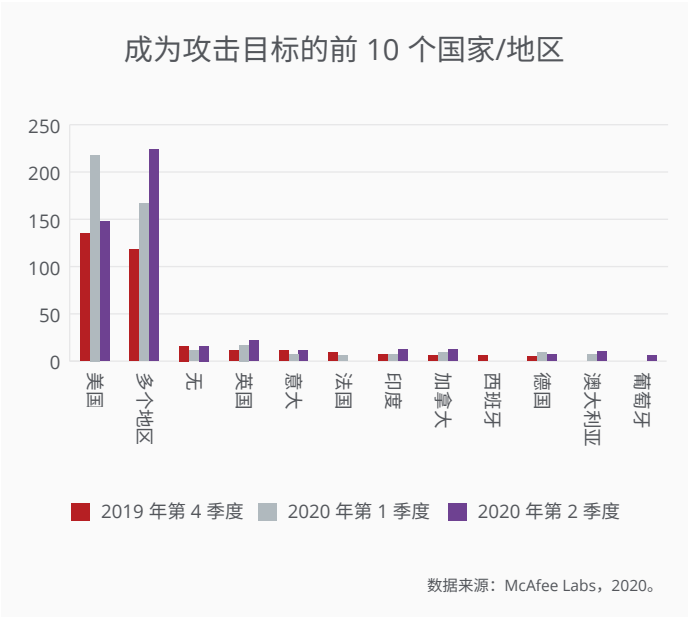


图 4. 与上一季度相比，2020 年第 2 季度披露的以美国为目标地区的安全事件降低了 47%，英国增长了 29%，加拿大增长了 25%。公开披露的所有安全事件中，近 27% 发生在美国。

关注

分享

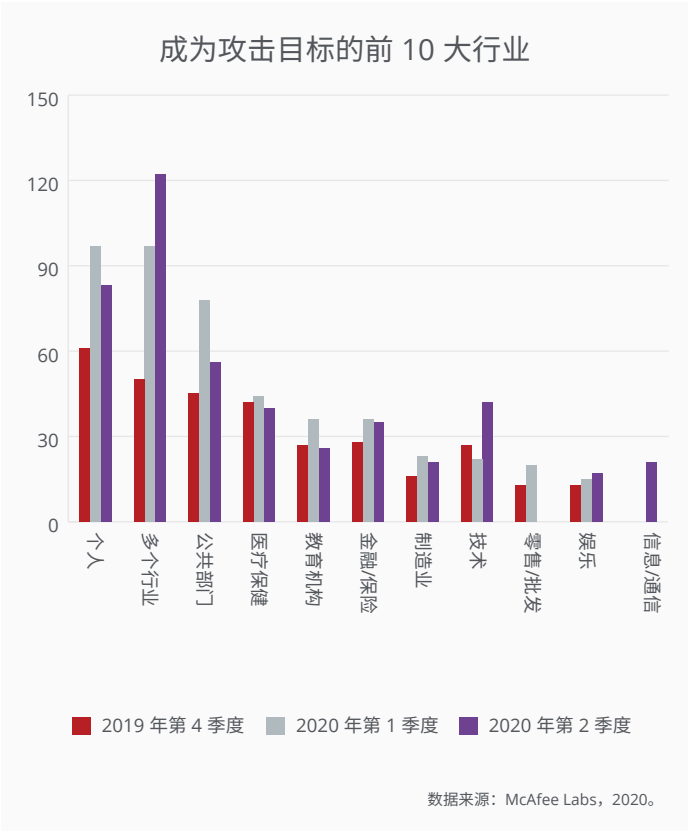


图 5. 与上一季度相比，2020 年第 2 季度披露的针对科技行业的安全事件增长了 91%。针对多个行业的安全事件增长了 25%，制造业降低了 10%，公共部门行业降低了 14%，针对个人的攻击降低了 28%。

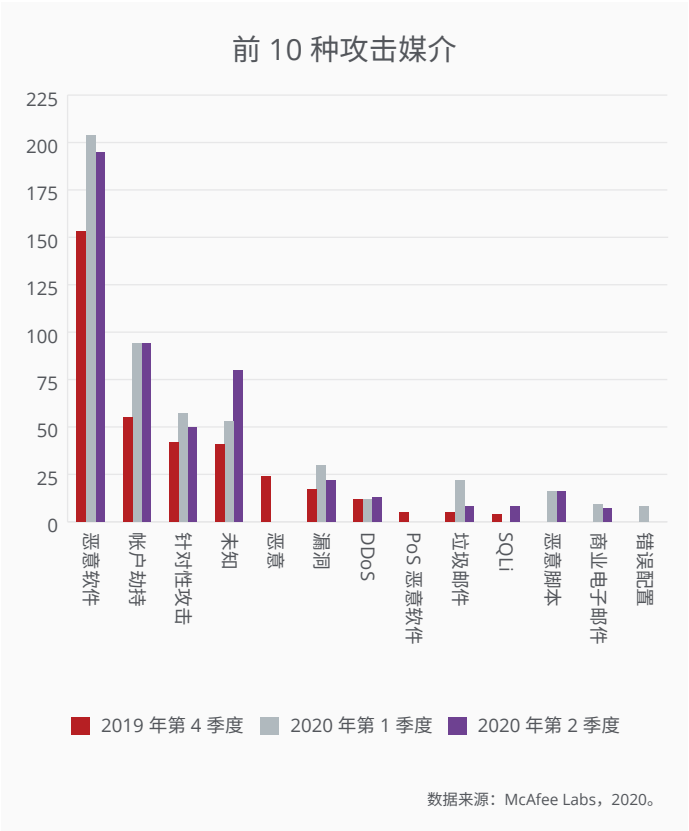


图 6. 总体而言，在公开报告的安全事件中，2020 年第 2 季度披露的攻击媒介主要是恶意软件，占比 35%。其次是帐户劫持攻击，占比 17%，第三是针对性攻击，占比 9%。

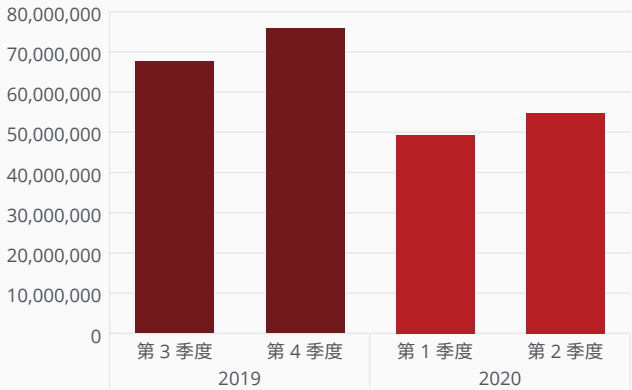
关注

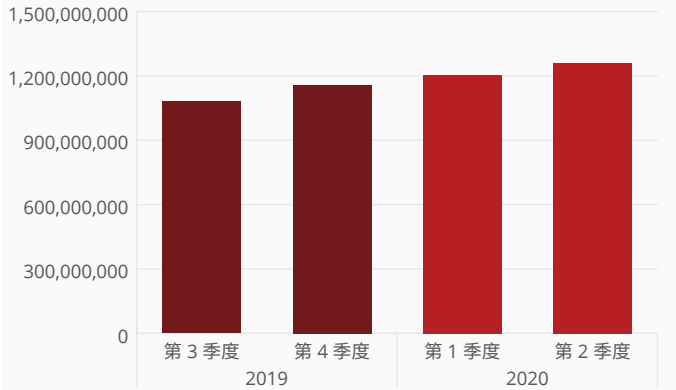
分享

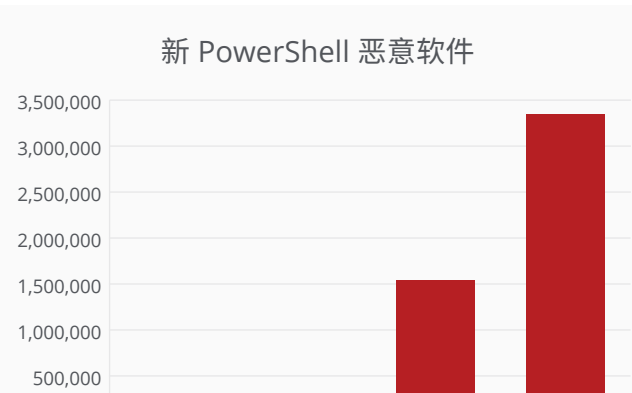
恶意软件威胁统计信息

2020 年第 2 季度，多个类别的威胁数量显著增加：

- McAfee Labs 在 2020 年第 2 季度观测到的数据是每分钟 419 个威胁，比上一季度增长近 12%。
- 新的 PowerShell 恶意软件比上一季度增长 117%，包括 Donoff PowerShell。
- 新的 Microsoft 365 恶意软件比上一季度增长 103%，其中相当一部分增长归因于可以启动 PowerShell 的 Donoff 文档。
- 新的恶意签名二进制文件比上一季度增长 25%，其中部分增长可能是由 Android Mobby 广告软件所造成。
- 新的货币挖矿恶意软件比上一季度增长了 25%，原因主要在于挖矿应用程序的流行（数据不含 Hashbuster）。
- 新的 Linux 恶意软件比上一季度增长 22%，部分原因在于 Gafgyt (IoT) 和 Mirai (IoT) 僵尸网络。
- 新的移动设备恶意软件比上一季度增长 15%，部分原因在于 Android Mobby 广告软件。
- 新的物联网 (IoT) 恶意软件增长 7%，包括因 Gafgyt 和 Mirai 僵尸网络导致的增长。
- 与 2020 年第 1 季度相比，观测到的勒索软件数量保持稳定。
- 新的 iOS 恶意软件降低了 77%，其中 Tiniv 在第 1 季度飙升后也有所回落。
- 新的漏洞利用恶意软件比第 1 季度降低 21%，其中 Exploit-CVE-2010-2568 数量有所减少（数据不含寄生兽漏洞）。
- 新的 JavaScript 恶意软件比上一季度降低 18%，其中 JavaScript 挖矿程序也有所减少。
- 新的 MacOS 恶意软件比上一季度降低近 8%，其中后门程序 Shlayer 和广告软件 Bundlore 均有减少。


新恶意软件
80,000,000
70,000,000
60,000,000
50,000,000
40,000,000
30,000,000
20,000,000
10,000,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。

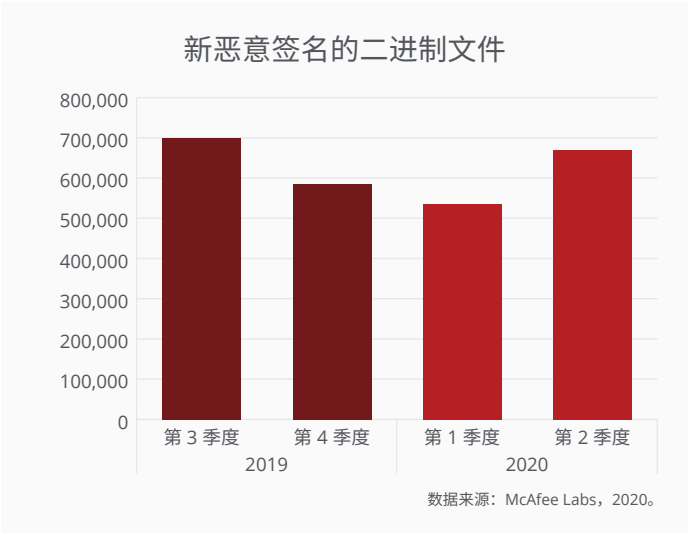

恶意软件总计
1,500,000,000
1,200,000,000
900,000,000
600,000,000
300,000,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。

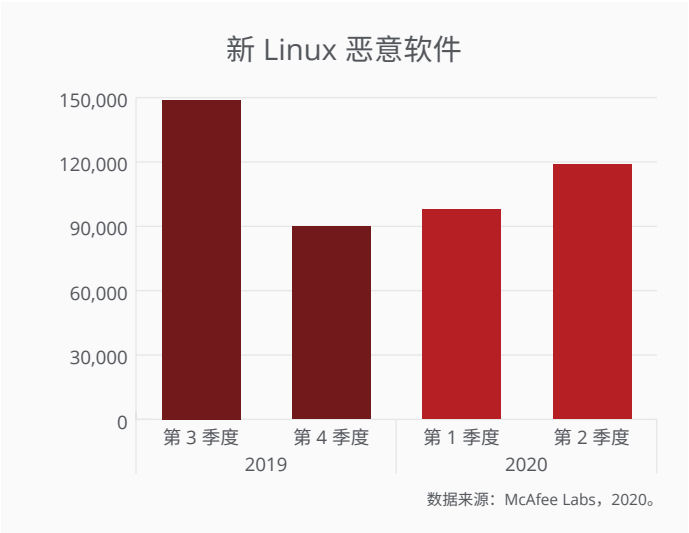

新 PowerShell 恶意软件
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。

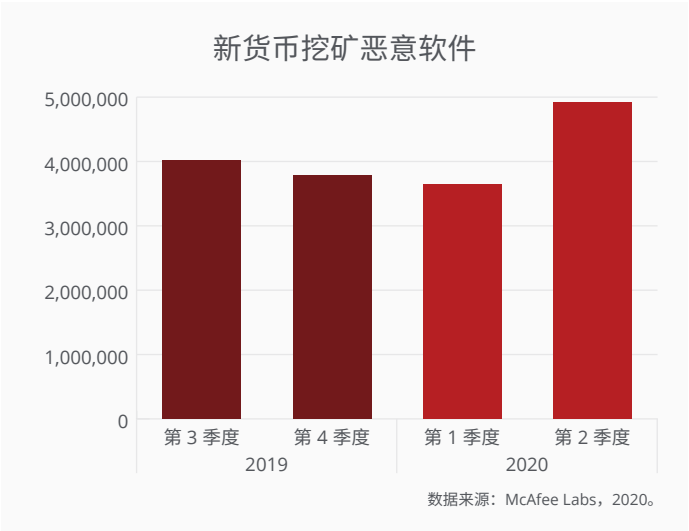

新 Microsoft 365 恶意软件
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。

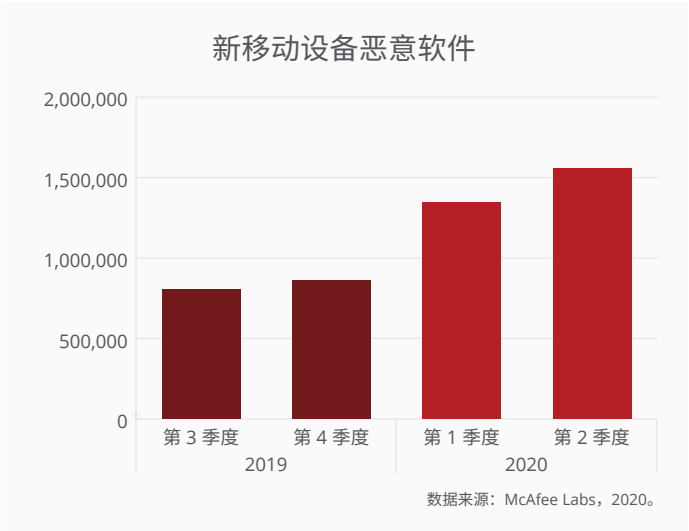
关注

分享


新恶意签名的二进制文件
800,000
700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。

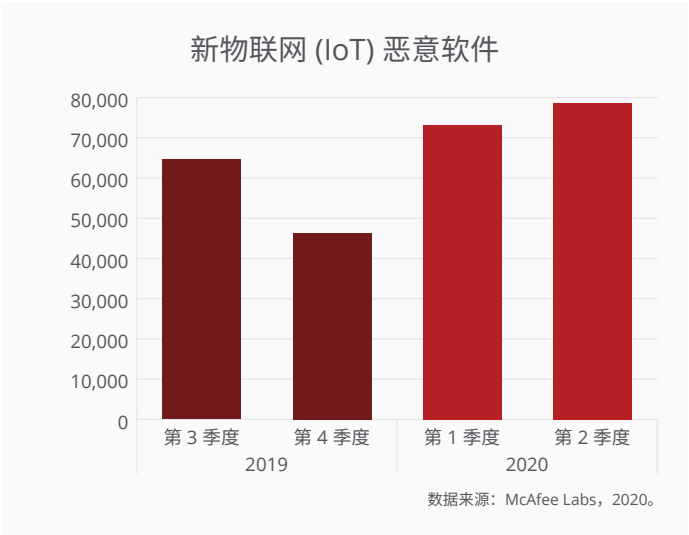

新 Linux 恶意软件
150,000
120,000
90,000
60,000
30,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。


新货币挖矿恶意软件
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。

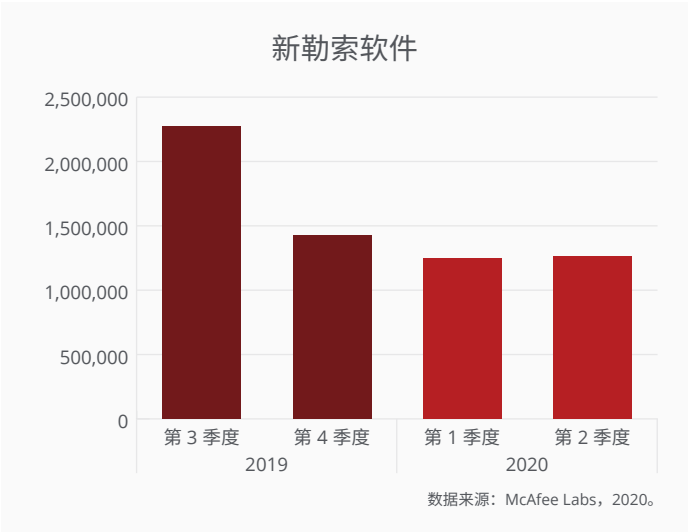

新移动设备恶意软件
2,000,000
1,500,000
1,000,000
500,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。

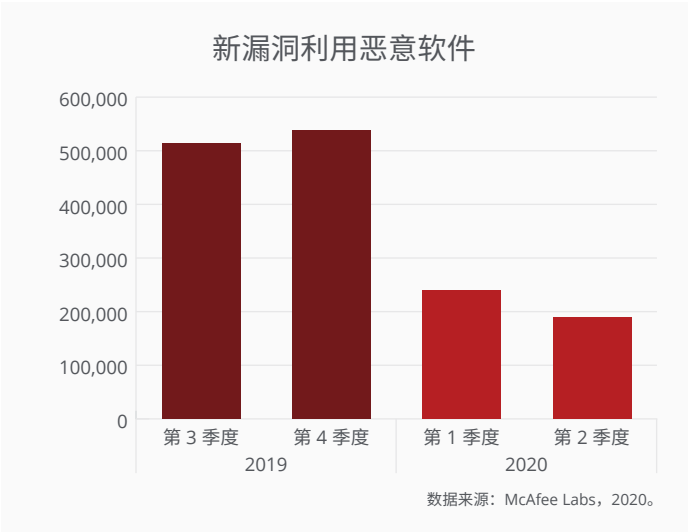
关注

分享

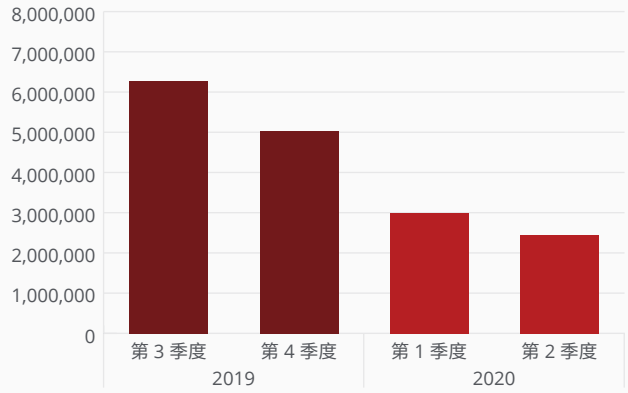

新物联网 (IoT) 恶意软件
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。

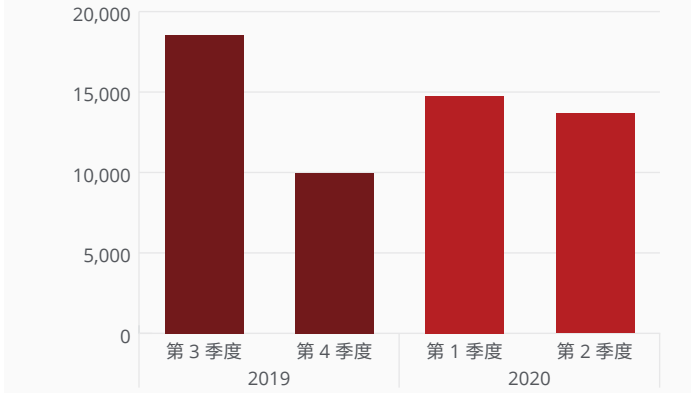

新 iOS 恶意软件
3,500
3,000
2,500
2,000
1,500
1,000
500
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。


新勒索软件
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。


新漏洞利用恶意软件
600,000
500,000
400,000
300,000
200,000
100,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。

关注 分享


新 JavaScript 恶意软件
8,000,000
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。


新 Mac OS 恶意软件
20,000
15,000
10,000
5,000
0
第 3 季度
第 4 季度
第 1 季度
第 2 季度
2019
2020
数据来源：McAfee Labs，2020。

关注

分享

政府机构面临多云环境挑战

今年一到四月，美国政府部门的企业云使用量增长 45%，并且随着在家办公和保持社交距离的措施继续施行，团队合作还将需要更多基于云的协作服务。

混合云和多云架构可为政府机构提供足够的灵活性、增强的安全性以及所需的容量，满足当前和未来现代化办公要求。然而，围绕多云架构和混合云架构的实施，仍有许多问题尚待解决。跨机构的基础设施实施云智能方法是一个非常复杂的流程，联邦机构的 CISO 们面临着相应的挑战。

在近期的“Securing the Complex Ecosystem of Hybrid Cloud”（确保混合云复杂生态系统安全）网络研讨会上，McAfee 美国公共部门业务部首席技术策略师 Ned Miller 有机会与云技术领域的一些公共和私营行业领袖坐在一起讨论相关问题。这场网络研讨会由美国公共政策创新中心 (CPPI) 和国土安全部对话论坛 (HSDF) 联合主办。

与会人员一致认为，尽管近年来支持混合云和多云环境的技术性基础设施取得了长足的进步，但要确保政府机构在更加安全的环境下运行，仍有大量工作有待进行。

在制定多云和混合云的实施策略时，联邦机构 CISO 需要考虑三个关键概念：

1. **不存在普适的、可以通用的混合云环境。**各组织采用的功能各不相同，都有自己必须要填补的独特缺口。要出台一套明确的系统让组织了解如何才能成功填补这些缺口，这个过程需要一些时间。话虽如此，对于希望在其基础设施中实施云方法的组织而言，并没有一种普适的、可以通用的混合云或多云环境技术。
2. **“零信任”的定义将会继续演变。**“零信任”的说法由来已久，其定义将会继续发展演变。在概念上，“零信任”是指一种要求组织对现有架构进行全面彻底检查的方法。它不是一项具体技术，而是一套必须应用于组织基础设施方方面面的功能集，以便组织实现混合云或多云环境。
3. **必须为数据保护策略制定连贯一致的实施政策。**连贯一致的实施政策是维护易于识别的数据保护和威胁管理策略的关键。对于组织来说，要完全实现基于云的跨团队协作，对数据实行有条件访问和情境访问至关重要。

成功集成多云环境是所有行业都面临的非常现实的挑战，尤其是像联邦政府一样复杂的大型企业和机构。对于 IT 员工而言，跨不同云环境管理安全性是一件极其复杂的事，也正因如此，他们亟需一些得力的工具，可以帮助他们自动执行任务并持续保护云中或云外敏感信息的安全。

有关多云环境威胁的更多信息，请访问此处。

攻击者使用元数据攻破 AWS 中的应用程序

将企业应用程序迁移到云原生架构可以带来巨大的业务价值，不仅可以增加规模和提高敏捷性，还能减轻繁琐的任务负担，例如修补和升级服务器基础设施。

然而，无论是在 AWS、Azure、GCP 还是其他任何云环境中，都存在一种新的风险类别。新的上下文以及您在云环境中的配置要求，滋生了新的云原生威胁。过去，诸如可公开访问存储对象之类的默认设置，使敏感数据呈开放状态，这让企图利用这些弱点的任何人都可以轻易窃取敏感数据。

在新环境中很容易犯错，因为云提供商会不断加入新的功能，因此新的设置也会随之持续引入。对云环境进行配置始终是企业自己的责任。AWS 和其他提供商无法控制您如何使用他们的服务。他们只提供配置模板以供参考。如果不了解各项配置会得到什么样的结果，不清楚如何构建云原生应用程序，可能会带来灾难性后果。

在今年的 RSA 会议上，McAfee 首席技术官 Steve Grobman 演示了如何利用 AWS 的“实例元数据”这项功能来窃取敏感数据。下面，我们一起来看一下这个攻击情景，重点指出一些重要的经验教训，并讨论如何防范自己遭受此类攻击。

实例元数据攻击

所有云提供商都具备管理云原生应用程序中的资源凭据的功能。如果正确使用这些功能，则可避免将凭据存储在明文或源代码存储库等易受攻击的地方。AWS 中的实例元数据服务 (IMDS) 提供与计算实例相关的信息，包括该实例所在的网络以及存储容量等，且这些信息可由实例上运行的软件获取。IMDS 还会为分配到该实例的任何 IAM 角色提供经常轮换的临时凭据。例如，分配到某个实例的 IAM 角色，可以定义该实例以及实例上运行的软件可否访问 S3 存储桶中的数据。

我们来看一个常见情景。

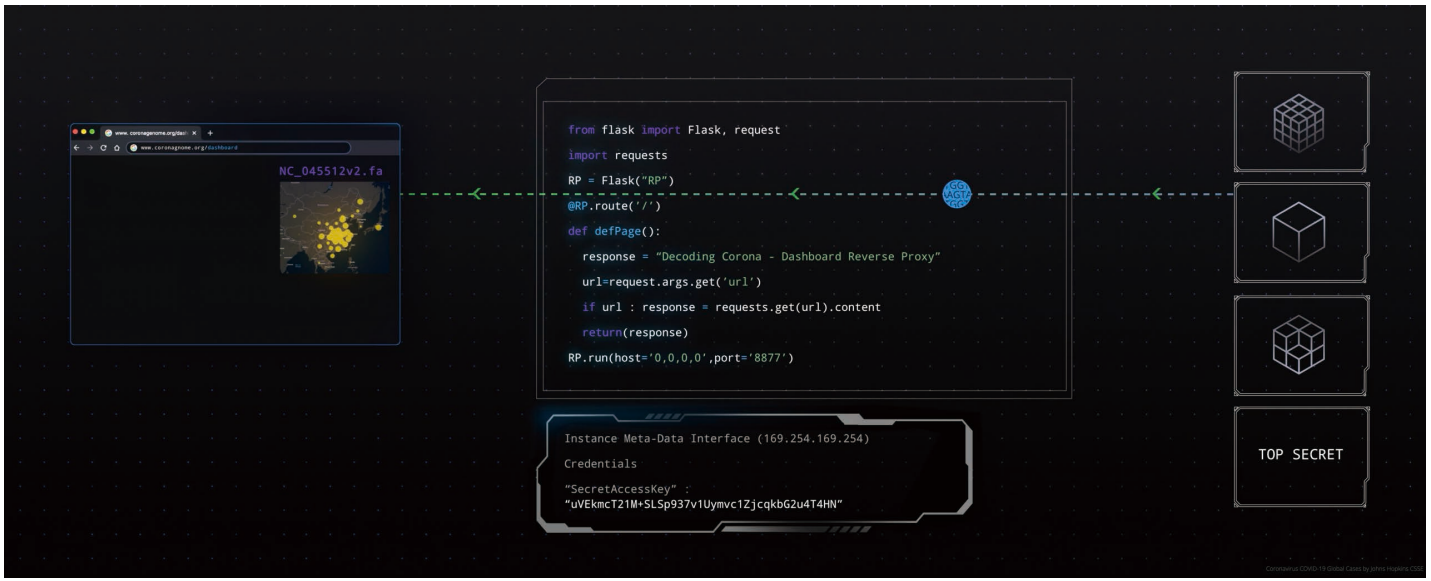
某流行病学专家团队在 AWS 中构建了一个云原生应用程序，尝试使用一个公共的信息显示板，通过可视化图表来呈现数据，以显示团队在病毒基因组分析方面的进度。

关注

分享

在这个应用程序的开发阶段，团队遇到了一项挑战。他们的虚拟私有云 (VPC) 中的大多数资源原本都应在互联网上隐藏。VPC 中可供公众查看的唯一资源是信息显示板。

用来托管其数据的 S3 存储桶需要保持私密状态，不对外公开。为了将数据从 S3 提取到公共信息显示板，他们添加了一个反向代理作为中间媒介。要实现这一目的所需的操作非常简单，只需快速搜索一下 Google 再添加几行代码，这一功能即可添加到他们的应用程序中。



关注

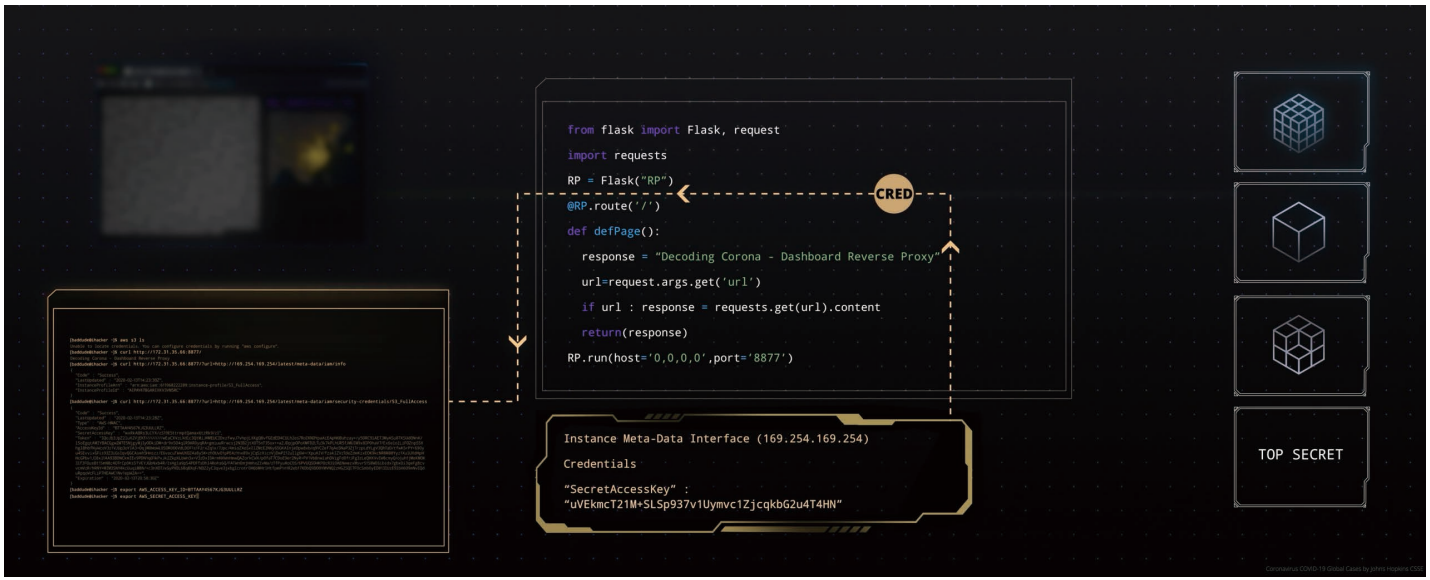
分享

对于这个流行病学专家团队而言，反向代理是一个既简单又有效的解决方案，完美适用于他们的用例。他们没有意识到的是，反向代理使他们陷入了大规模的泄露风险。

运行反向代理的计算实例分配到了一个 IAM 角色，该角色有权访问专家团队的私密 S3 存储桶。从实例元数据中可获得反向代理访问 S3 的凭据。

访问该网站并且对他们的数据感兴趣的攻击者注意到，该团队在信息显示板中引用了反向代理的 IP 地址。于是，攻击者检查了一下是否可以连接到该地址。确认连接正常后，攻击者又检查是否可以通过反向代理访问实例元数据。大获成功。

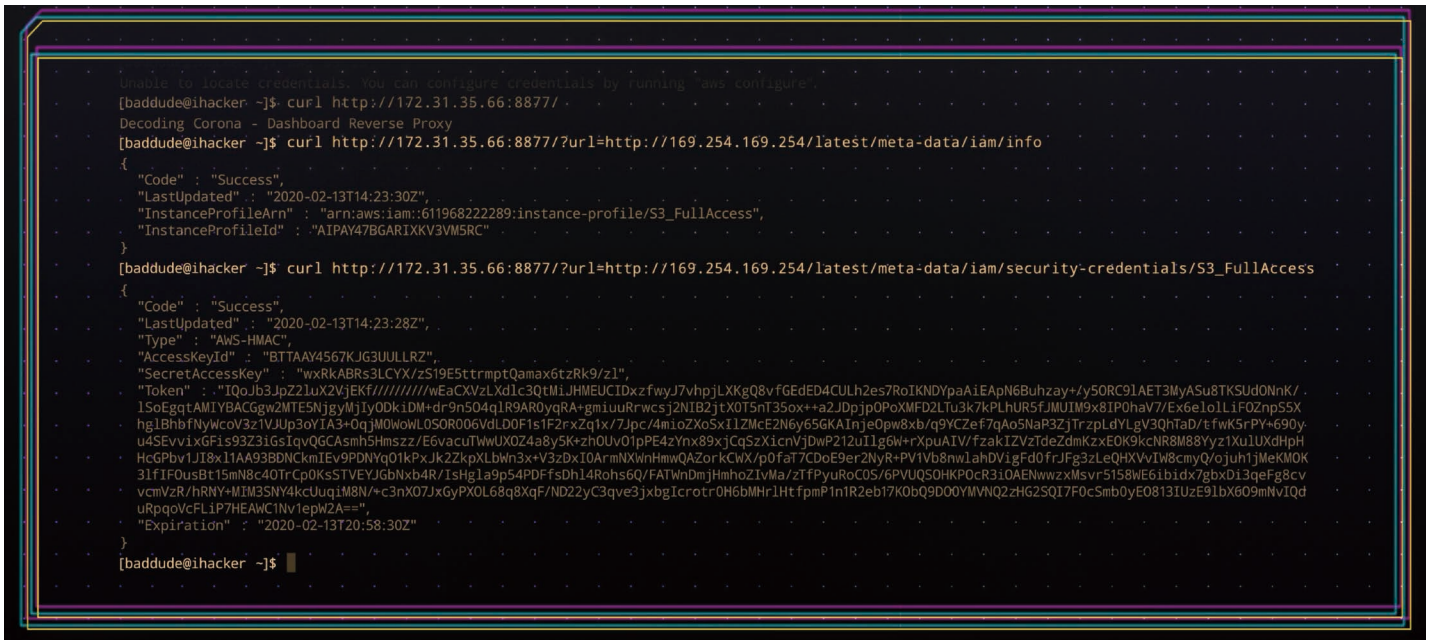
通过反向代理和实例元数据，攻击者发现了团队用来访问其私密 S3 存储桶的凭据。



关注

分享

现在，因为能够访问 S3 存储桶，攻击者即可窃取该团队为应用程序存储的高度敏感的数据。攻击者只需将目标 S3 存储桶内的数据同步到另一个 AWS 账户中自己的 S3 存储桶，那么这些数据就是他们的了。



这种类型的攻击只是 MITRE ATT&CK 框架针对云环境所述的 43 种攻击技术中的一种：https://attack.mitre.org/matrices/enterprise/cloud/

有关 AWS 如何化解实例元数据攻击的更多信息，请访问此处。

关注

分享

McAfee 对机器人漏洞的调查研究

协助开发人员为企业和消费者提供更加安全的产品是我们一贯的目标，为此，McAfee Advanced Threat Research (ATR) 团队近期对 *temi* 进行了一项调查，这是一款由 Robotemi Global Ltd. 公司生产的电话会议机器人。我们在研究后发现，temi 机器人中存在四个不同的漏洞，我们的调查文章对此进行了非常详细的介绍。这些漏洞包括：

1. CVE-2020-16170 - 使用硬编码凭据
2. CVE-2020-16168 - 源验证错误
3. CVE-2020-16167 - 关键功能缺少身份验证
4. CVE-2020-16169 - 使用替换的通道路径绕过身份验证

恶意分子可利用以上这些漏洞，监听 temi 视频通话、拦截拨给其他用户的呼叫，甚至远程操作 temi — 所有这些行为都无需任何身份验证。

根据 McAfee 的漏洞披露政策，我们在 2020 年 3 月 5 日向 Robotemi Global Ltd. 公司报告了我们的研究结果。很快，他们做出了响应并开始了与 ATR 团队的持续交流，同时还积极采用我们在披露报告中所述的化解措施。截至 2020 年 7 月 15 日，在 temi Robox OS 版本 120 中，以及在 temi Android 应用程序 1.3.7931 之后的所有版本中，这些漏洞均成功修补和化解。对于 Robotemi 的快速响应和他们在整个过程中积极合作的意愿，我们深表赞赏。可以说，这是 McAfee 有幸与之合作的响应最迅速、最主动和最高效的供应商之一。

关注
分享

什么是 temi?

机器人。未来的终极前沿领域。

temi 机器人身高 4 英尺，头部是一个 Android 平板电脑式的“大脑”。temi 小巧的外形下封装了大量传感器，具体包括：一个 360° 激光雷达 (LIDAR)，三个不同的摄像头，五个近距离传感器，以及一个惯性测量装置 (IMU) 传感器，它是加速仪、陀螺仪和磁力仪的三合一传感器。所有这些传感器共同作用，使 temi 能够在一定空间内自主移动，同时避开任何障碍物。如果不是受限于阶梯和路牙，temi 或许可以不受阻挡地自由“行走”。

Robotemi 在推广机器人时，主打用途是电话会议。temi 官网链接的一些文章介绍了这款机器人在各种不同行业中的应用案例：Connected Living 最近与 temi 合作，将这款机器人用于老年护理；纽约市的 Kellog's 咖啡采用 temi 来“改善零售体验”；企业人力资源公司 Collabera 使用 temi 来“优化不同办事处之间的沟通”。尽管其产品定位宣称是“个人机器人”，但 temi 的设计似乎同时面向消费者应用和企业应用，正是后者使 McAfee Advanced Threat Research 团队真正有兴趣将其作为研究目标。鉴于远程医疗的需求显著增加，temi 的创造者为此将产能扩大到每月生产 1,000 台，它在医疗领域的存在感不断增加尤其引人关注。那么，被感染的 temi 对其用户，无论是出差在外的母亲，还是通过机器人代理就诊的患者，意味着什么？我们下单订购了一台 temi，准备找出这个问题的答案。

有关 McAfee 对 temi 漏洞研究的更多信息，请访问此处。

关注 分享

MalBus 攻击者将攻击阵地从 Google Play 转移到 ONE Store

McAfee Mobile Research 团队在一位韩国开发人员开发的一款教育应用程序中，发现了 MalBus 的另一种变体。在之前的 MalBus 案例中，作者通过 Google Play 分发恶意软件，而新的变体几乎是以相同的手段通过 ONE Store 进行分发。ONE Store 是韩国三大主要电信公司的合资企业，并且是在韩国销售的大多数 Android 手机上的一款预安装应用程序。它拥有 3500 万用户（接近韩国总人口的 70%），并且自 2018 年年底以来已经超过了 Apple App Store 的销售额。

存在问题的这款应用程序同时通过 Google Play 和 ONE Store 分发。恶意应用程序会下载并运行具有恶意功能的加密有效负载。

McAfee® Mobile Security 将这种威胁检测为 Android/MalBus，并提醒移动端用户注意防范（如果存在），同时保护用户不丢失数据。

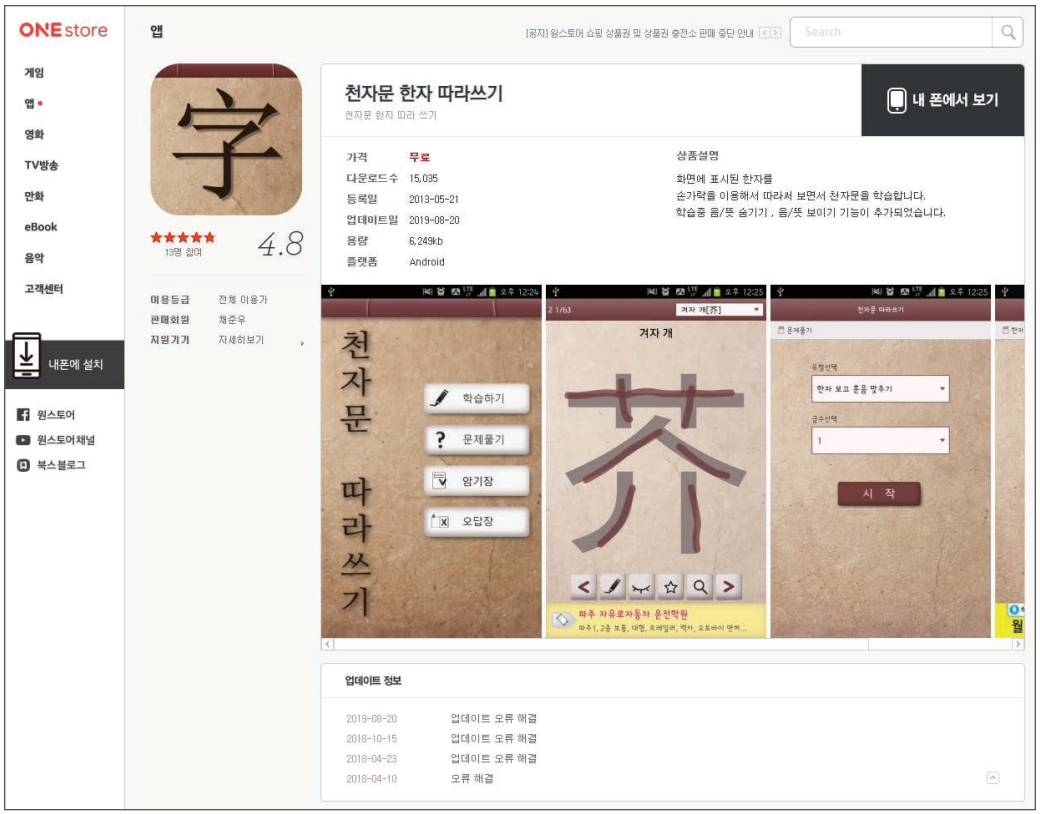


图 7. ONE Store 中应用程序页面的屏幕截图

关注 分享

攻击活动

我们发现，攻击者通过开发人员的帐户，将恶意代码注入通过 ONE Store 分发的应用程序版本 27 和 28。从 ONE Store 分发的版本 26 到 29 的应用签名证书均相同。在 ONE Store 中没有找到同一作者开发的其他应用程序。ONE Store 现在上架的是版本 29，该版本不包含恶意代码。Google Play 仍提供版本 26，此版本也未受到任何感染。

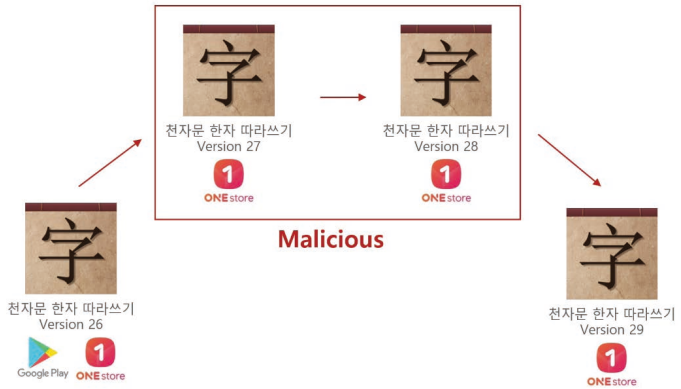


图 8. 受感染的应用程序历史版本

下图是此应用程序的总体流程，主要说明的是其恶意功能：

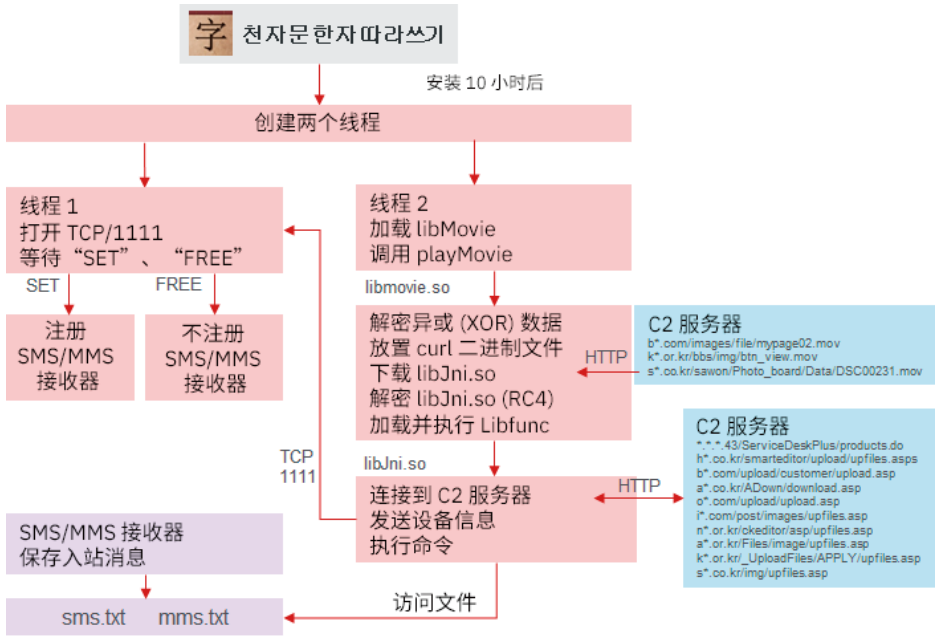


图 9. 恶意行为概览

安装恶意软件后，恶意代码会潜伏 10 个小时，以避免被动态分析发现。

```
public boolean isCheck(Context mAct) {
   long installd = 0;
   try {
      installd = mAct.getPackageManager().getPackageInfo(
                  new String(Base64.decode("Y29tLmpvb2phbmcuQ2hhcmFjdGVyQ2xhc3NpYw==", 0)), 0).lastUpdateTime;
   } catch (PackageManager.NameNotFoundException e) {
   }
   if (System.currentTimeMillis() - installd > 36000000) {
      return true;
   }
   return false;
}
```

有关 MalBus 威胁的这种变体的更多信息，请访问此处。

Ripple20 漏洞缓解最佳实践

6 月 16 日，美国国土安全部和 CISA ICS-CERT 发布了一份重要的安全公告预警，提及多个新发现的漏洞，这些漏洞对多个供应商制造的联网设备均有影响。JSOF 研究人员将这组在 Treck 开发的底层 TCP/IP 软件库中发现的 19 个漏洞称为“Ripple20”。

网络堆栈是一种软件组件，可通过标准的互联网协议提供网络连接。在这个特定案例中，协议包括 ARP、IP（版本 4 和 版本 6）、ICMPv4、UDP 及 TCP 等通信协议，以及 DNS 和 DHCP 这两种应用层协议。Treck 网络堆栈广泛用于不同行业的众多设备制造商（医疗、政府、学术、公用事业等），并且每个制造商都需要独立于所有其他制造商为自己的设备推送更新，这无疑扩大了这些漏洞的影响力和影响范围。换句话说，由于供应链和设计链的复杂性，影响会在整个行业内蔓延开来。

识别网络上易受攻击的设备，是评估企业和机构遭受 Ripple20 攻击风险的关键步骤。一次简单的 Shodan 搜索“treck”显示了大约 1000 台设备，这些很可能是面向互联网的易受攻击的设备，但是，这只占受影响设备的一小部分。在对问题设备进行网络扫描所得结果的基础上，要识别 Treck 网络堆栈与其他网络堆栈（例如原生 Linux 或 Windows 堆栈），还离不开详细的分析和指纹识别技术。

关注 分享

这些漏洞影响范围广泛，从拒绝服务到通过互联网完全远程利用代码，并且其中至少有一种不需要进行任何身份验证（CVE-2020-11901）。JSOF 研究人员发现，传统设备和物联网设备都会受到这些漏洞的影响。客户应仔细查阅来自 Intel 和 HP 等供应商发布的公告，因为非物联网设备运行的固件可能会使用 Treck 网络堆栈。

相对于堆栈仅暴露在本地的设备而言，受 Ripple20 影响最严重的是堆栈暴露在网络的设备（通常是采用 Treck 网络堆栈的物联网设备）。我们建议您审核所有联网设备，以确定这些设备是否易于遭受这些漏洞的攻击。

可能有数以千万计的设备易受至少一种 Ripple20 漏洞的攻击。缓解漏洞攻击的影响，需要设备拥有者和设备供应商的共同重视。

根据 CISA 建议，（在可能的情况下）适用于易受攻击的设备用户的缓解措施如下：

- 如果供应商已发布相关更新，请为所有适用设备打上更新补丁。
- 坚持原则，仅赋予所有用户和设备最小权限（即：设备和用户只能访问完成其工作所必需的功能集）。在这种情况下，最大限度地降低所有控制系统设备的网络暴露风险和互联网可访问性。
- 找到隐蔽在防火墙后面的控制系统网络和远程设备，并将其与业务网络隔离。
- 需要进行远程访问时，使用安全方法，例如虚拟专用网络（VPN），同时认识到 VPN 可能存在漏洞，应及时将其更新为可用的最新版本。此外，还应认识到 VPN 的安全程度还取决于连接到 VPN 的设备的安全。VPN 解决方案应使用多重身份验证。
- 在组织中使用缓存 DNS 服务器，禁止将 DNS 查询直接发送到互联网。理想情况下，缓存 DNS 服务器应利用 DNS-over-HTTPS 进行查询。
- 结合使用防火墙和入侵防御系统来拦截异常 IP 流量。

警惕 OneDrive 网络钓鱼

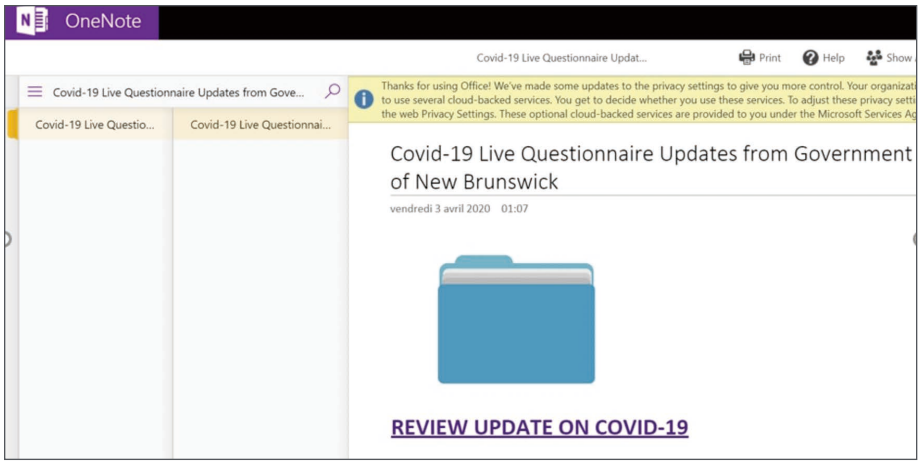
骗子会使用多种方式来针对个人信息发起攻击，目前的一个示例就是，他们利用公众对新冠疫情的恐慌情绪，向 Microsoft OneDrive 用户发送网络钓鱼和欺诈邮件，企图借助冠状病毒/COVID-19 牟利。他们会伪装成是从政府机构、咨询公司或慈善组织发出电子邮件，以窃取受害者的 OneDrive 详细信息。骗子会窃取 OneDrive 帐户的敏感信息，例如用户名和密码。我们希望引导 McAfee 用户和公众了解这些欺诈行为的潜在风险。

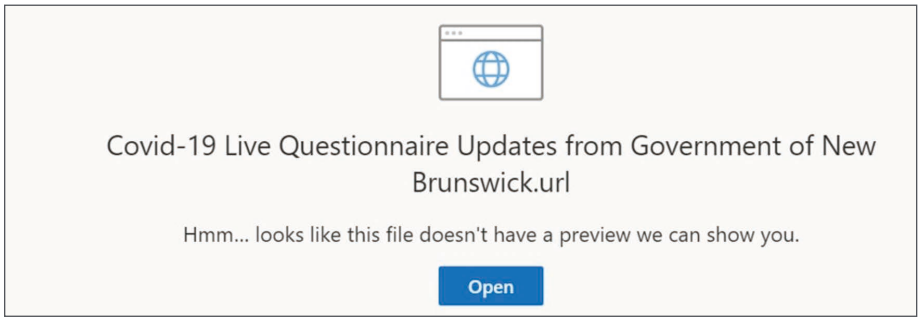
不法团伙企图窃取用户凭据

下面我们将为您介绍此类攻击的几个示例，分别来自托管在 **OneDrive** 上的政府机构、咨询公司和慈善组织，它们的目的都是让这些邮件在用户眼中看上去更加真实可信。正如下面的屏幕截图所示，目标就是窃取用户的 OneDrive 凭据。

伪装政府电子邮件诱骗受害者

骗子伪装成政府工作人员发送文档，文档内容是关于新冠疫情的最新实时问卷调查。请谨记：一般情况下，政府不会通过电子邮件向广大群众发送未经请求的文档，因此用户可检查电子邮件标题中的发件人电子邮件地址和位置来进行验证，并访问合法的政府网站来了解该网站是否有 COVID-19 相关信息。





关注 分享

"*Hmm… looks like this file doesn't have a preview we can show you*"这条警告信息的目的是诱使访客单击"打开"按钮。单击该按钮后，访客会被带到以下 OneDrive 屏幕截图所示之处，并提示访客输入其个人信息。

可以看到，该链接将用户带到了一个易受攻击的 WordPress 网站，该网站的登陆页面是一个凭据网络钓鱼页面。用户应始终谨记：合法的 OneDrive 登录页面永远不会托管在非 Microsoft 域上。对于用户而言，这应该是一个危险信号，表示这可能是欺诈或网络钓鱼攻击。

如果正中骗子圈套，那么用户无法访问 OneDrive 文档以查看最新的政府问卷调查，而是会收到一则错误消息提示稍后重试。

到了这个阶段，骗子可能已经窃取了用户的 OneDrive 个人信息。

骗子还试图伪装成招募志愿者的慈善组织，来诱骗用户相信其文档和电子邮件的安全性。

有关 McAfee 对 OneDrive 网络钓鱼研究的更多信息，包括最佳实践清单，请访问此处。

资源

若要了解最新威胁和研究结果，请参阅以下 McAfee 资源：

McAfee COVID-19 威胁信息显示板 — 更新了与 COVID-19 相关的恶意文件检测信息，包括遭受攻击的国家/地区和行业，以及威胁类型。

MVISION Insights 预览信息显示板 — 预览和探索唯一一款主动式解决方案，能够让您在面对新兴威胁时始终领先一步，掌握主动。

McAfee 威胁中心 — 我们的威胁研究团队已成功识别多种当今影响最大的威胁。

McAfee Labs 和相关研究人员的 Twitter 帐户

McAfee Labs

Raj Samani

Christiaan Beek

John Fokker

Steve Povolny

Eoin Carroll

Thomas Roccia

Douglas McKee

关注

分享

关于 McAfee

McAfee 是专注于从设备到云的网络安全公司。在协同工作思想的启迪下，McAfee 研发出了适用于企业用户和家庭用户的解决方案，让网络环境变得更为安全。通过构建与其他公司产品集成的解决方案，McAfee 能够帮助企业部署真正集成的网络环境，通过协作的方式即时进行威胁检测和纠正，从而保护网络安全。通过保护用户的所有设备的网络安全，McAfee 能够随时随地为他们的数字化生活提供安全保障。McAfee 与其他安全参与者同心协力，致力于打击网络犯罪分子，以保护所有用户的利益。

www.mcafee.com/cn

关于 McAfee Labs 和 Advanced Threat Research

McAfee Advanced Threat Research 团队领导的 McAfee Labs 是威胁研究、威胁情报和网络安全先进理念的全球领先来源之一。利用从跨主要威胁媒介（文件、Web、消息和网络）的数百万传感器获取的数据，McAfee Labs 和 McAfee Advanced Threat Research 团队可提供实时威胁情报、关键分析和专家意见，以便增强保护并降低风险。

https://www.mcafee.com/enterprise/zh-cn/threat-center/mcafee-labs.html

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，100013
电话：8610 8572 2000
www.mcafee.com/cn

2020 年 11 月