TA585 组织利用 ClickFix 钓鱼技术部署 MonsterV2 RAT 的深度技术分析

APT1天前发布 admin 58 0 0

事件概述

2025 年 2 月，Proofpoint 首次发现了一个新的网络犯罪组织 TA585，该组织利用美国国税局(IRS)为主题的钓鱼邮件，包含指向恶意 PDF 的链接，诱导受害者访问使用 ClickFix 技术的假验证页面。这些钓鱼活动主要针对金融和会计行业的中小型企业。

到 2025 年 3 月，TA585 的活动扩展到冒充 IRS 和美国小企业管理局(SBA)，继续针对金融和会计公司。随后在 2025 年 4 月，该组织演变为完全自主的运营商，注册并维护自己的恶意基础设施，被研究人员标识为 CoreSecThree。这种基础设施托管网页注入和过滤系统，确保只有真实用户才能接收恶意载荷。

TA585 的独特之处在于其高度自主性，控制着从基础设施到恶意软件部署的整个攻击链，这与大多数依赖初始访问代理或第三方传递服务的恶意软件分发者形成鲜明对比。该组织使用的主要恶意软件是 MonsterV2 RAT，这是一款功能丰富的远程访问木马、窃取器和加载器，具有信息窃取、隐藏虚拟网络计算(HVNC)和剪贴板劫持等多种高级功能。

攻击技术与攻击链分析

攻击链概览

TA585 的攻击链是一个多阶段的复杂过程，从初始访问到最终的命令与控制。完整的攻击流程展示了 TA585 组织如何通过多种初始访问途径引导受害者访问恶意 URL，经过 CoreSecThree 基础设施的过滤和 JavaScript 注入，使用 ClickFix 社会工程学技术诱导用户手动执行恶意命令，最终部署 MonsterV2 RAT 并建立与 C2 服务器的连接。整个过程展现了攻击者精心设计的多层次攻击策略，每个阶段都有特定的技术手段确保攻击的成功执行。

初始访问技术

TA585 采用多种初始访问技术，主要包括：

1. 钓鱼邮件：伪装成美国国税局(IRS)或小企业管理局(SBA)等政府机构的邮件，包含指向恶意 PDF 的链接。这些 PDF 会将受害者重定向到使用 ClickFix 技术的假验证页面。
2. GitHub 通知滥用：创建假 GitHub 问题并标记合法用户，触发包含恶意缩短 URL 的自动 GitHub 电子邮件。这些 URL 指向行为者控制的站点，托管假 GitHub 验证页面。
3. 恶意广告：第三方研究人员还观察到 TA585 通过恶意广告进行活动传递。

ClickFix 社会工程学技术

ClickFix 是 TA585 使用的核心社会工程学技术，该技术诱导访问者手动在 Windows 运行框或 PowerShell 终端中执行恶意命令。ClickFix 技术的执行流程如下：

1. 用户被引导到受感染的网站，这些网站显示假验证页面。
2. 这些网站被注入恶意 JavaScript，加载恶意脚本，创建网站覆盖层，呈现假 CAPTCHA。
3. 页面指示用户验证他们是人类，需要在 Windows 运行框或 PowerShell 终端中手动运行提供的命令。
4. 如果用户按照提示操作，PowerShell 命令会触发 MonsterV2 恶意软件的下载和执行。
5. 一旦执行，受感染的系统会被验证并重定向到合法网页，最大限度地减少怀疑。

这种技术之所以有效，是因为它规避了传统的安全保护机制，如宏禁用和恶意附件检测，转而专注于”入侵人的大脑、情绪和行为”，通过精心设计的社会工程学让用户自己感染系统。

CoreSecThree 基础设施

架构与基础设施概述

CoreSecThree 是 TA585 威胁行为者使用的专有恶意基础设施，其命名基于其域名和基础设施特征。该基础设施是 TA585 完全自主运营的关键组成部分，使其能够控制从初始访问到恶意软件部署的整个攻击链。

TA585 拥有并维护自己的域名，使用 Cloudflare 托管基础设施，这使其能够隐藏真实的服务器 IP 地址，增加追踪和分析的难度。整个攻击链由 TA585 自主控制，不依赖第三方流量分发系统，这与大多数依赖初始访问代理或第三方传递服务的恶意软件分发者形成鲜明对比。此外，该基础设施支持多种恶意软件投递，包括 MonsterV2 和 Rhadamanthys，展示了其技术灵活性和适应性。

已知的 CoreSecThree 基础设施域名包括 intlspring[.]com，该域名被用于传递 MonsterV2 和 Rhadamanthys 两种不同的恶意软件。通过 Cloudflare 托管服务隐藏真实基础设施，使用多个域名进行 C2 通信，支持 IP 地址和域名形式，增加了检测和阻断的难度。

JavaScript 注入与网页覆盖技术

CoreSecThree 基础设施的核心功能之一是在被入侵的合法网站上注入恶意 JavaScript 代码。这些注入的脚本创建网站覆盖层，显示假冒的 CAPTCHA 验证(“ClickFix”)，提示用户执行”Win+R”操作以”验证他们是人类”。一旦用户按照指示操作，将启动 PowerShell 命令下载并执行恶意软件。页面会重复向诱饵服务器发送信标，直到 PowerShell 脚本完成下载和运行。

Proofpoint 的研究揭示了 TA585 使用的 JavaScript 注入代码的技术细节。该代码是一个异步函数，使用 async/await 来处理网络请求，包含大量的字符串混淆和编码，通过 encodeURIComponent 和 escape 函数对 URL 进行编码，增加了代码的隐蔽性。代码的主要功能包括数据收集与发送、浏览器与操作系统检测、本地存储检查、图标链接提取和重定向逻辑。

数据收集与发送方面，代码通过 fetch 函数向一个远程服务器发送 HTTP 请求，收集当前页面的域名、主机名、查询参数等信息。请求的 URL 中包含了动态生成的参数，如 wsid（可能表示会话 ID）和 domain（当前域名）。

在浏览器与操作系统检测方面，恶意代码会检测用户的浏览器类型和操作系统，包括检测是否为 Windows 10 系统以及是否为特定版本的 Edge、Chrome、Firefox 浏览器。

此外，代码还检查 localStorage 中是否存在”verified”键，如果存在且值为”true”，则跳过某些操作。如果”verified”键不存在或未设置，代码会继续执行后续的逻辑。

在重定向逻辑方面，如果满足特定条件（如浏览器类型不符合预期），代码会执行 window.replace()，将当前页面重定向到一个新的 URL。重定向的 URL 通过模板字符串动态生成，包含收集的参数。

该 JavaScript 代码使用多种混淆与隐蔽技术，包括字符串混淆（关键的 URL 和数据通过 atob（base64 解码）和 encodeURIComponent 进行编码和解码，增加了代码的混淆程度）、条件渲染与短路运算（使用逻辑运算符（如&&和“）来简化条件判断，使代码更加紧凑但难以理解）以及正则表达式匹配（使用复杂的正则表达式来匹配浏览器用户代理，以确定用户使用的具体浏览器和操作系统版本）。

这种 JavaScript 注入代码的潜在恶意行为包括数据泄露（收集用户的域名、主机名、浏览器信息、操作系统信息以及图标链接，这些信息可能被用于用户跟踪或指纹识别）、重定向攻击（如果用户不满足某些条件，代码会将用户重定向到其他 URL，这可能用于流量劫持或恶意网站引导）以及绕过验证（通过检查 localStorage 中的”verified”键，代码可能试图绕过某些安全验证机制）。

高级过滤与反沙箱机制

CoreSecThree 基础设施实施了复杂的过滤系统，确保只有真实用户才能接收恶意负载，避免安全研究人员和沙箱环境。该系统能够检测并响应用户的”Win+R”活动，提供网站的”反应”，使用持续性信标(beaconing)技术，直到确认恶意软件已在目标 IP 上安装运行。只有当恶意软件从同一 IP 地址检查到有效负载服务器时，才会将用户重定向到实际网站。

过滤机制的工作流程如下：

1. 当用户访问被入侵的网站或恶意链接时，CoreSecThree 基础设施首先收集用户的浏览器信息、操作系统版本、IP 地址等数据。
2. 系统使用这些数据进行初步过滤，排除来自已知安全研究机构的 IP 地址范围、虚拟机环境和沙箱分析系统。
3. 对于通过初步过滤的用户，系统会展示伪装的验证页面，通常模仿 Cloudflare 的安全检查界面。
4. 当用户按照指示执行操作（如在 Windows 运行框中输入命令）后，系统会持续向后端服务器发送信标，确认恶意软件是否成功下载和执行。
5. 一旦确认恶意软件已在目标系统上安装并运行，系统会将用户重定向到带有”/?verified=true”参数的实际网站，以减少用户的怀疑。

这种高级过滤机制使 CoreSecThree 基础设施能够精准地将恶意负载投递给真实目标，同时避开安全研究人员和自动化分析系统，大大提高了攻击的成功率和隐蔽性。

通信协议与数据传输

CoreSecThree 基础设施使用原始 TCP 连接与 C2 服务器通信，实现类似 SSL/TLS 的加密密钥交换和双向认证。如果连接丢失，恶意软件会尝试重新连接。系统使用 ChaCha20 加密算法和 ZLib 压缩技术保护配置数

据，确保通信的安全性和效率。

通信流程包括以下步骤：

1. 恶意软件建立与 C2 服务器的初始连接。
2. 双方交换加密密钥并进行双向认证，确保通信的安全性。
3. 恶意软件发送系统信息，包括操作系统版本、地理位置、用户名和外部 IP 等。
4. C2 服务器发送命令，恶意软件执行并返回结果。
5. 如果连接中断，恶意软件会自动尝试重新连接。

这种通信协议设计确保了攻击者与受感染系统之间的安全、稳定通信，同时最大限度地减少了被检测的风险。

MonsterV2 RAT 恶意软件分析

基本信息与技术架构

MonsterV2 是一款功能丰富的远程访问木马(RAT)、窃取器和加载器，于 2025 年 2 月首次在网络犯罪论坛上出售。与同类恶意软件相比，它价格昂贵，标准版每月 800 美元，企业版每月 2000 美元。该恶意软件使用 C++、Go 和 TypeScript 编写，具有先进的架构，内置 RAII 包装器、线程安全性和 ChaCha20 加密。

MonsterV2 RAT 的技术特性包括基本信息（如首次发现时间、价格、编程语言等）、核心技术架构（如内存管理、线程安全性、加密算法等）、主要功能模块（如信息窃取、远程控制、HVNC 等）、防御规避技术（如 SonicCrypt 自定义加密器、反调试功能等）和执行流程（如初始化、配置解密、系统信息收集等）。从中可以看出，MonsterV2 是一款技术复杂、功能全面的高级恶意软件，其设计注重内存管理和线程安全，同时采用多种加密和混淆技术来保护自身和通信过程，使其成为一个强大且难以检测的威胁。

功能与能力分析

MonsterV2 具有多种高级功能，使其成为一个全面的网络攻击工具：

1. 信息窃取：能够窃取浏览器数据、登录凭证、信用卡信息、加密钱包等敏感信息。
2. 远程监控：支持屏幕录制、网络摄像头访问和键盘记录，使攻击者能够全面监控受害者的活动。
3. HVNC（隐藏虚拟网络计算）：允许攻击者建立隐蔽的远程桌面连接，提供图形用户界面访问，而不会提醒受害者。
4. 剪贴板劫持：能够替换受害者剪贴板中的加密货币地址，将资金重定向到攻击者控制的钱包。
5. 命令执行：支持通过 PowerShell 或 CMD 执行命令，给予攻击者对受害系统的完全控制权。

防御规避技术

MonsterV2 采用多种技术来规避检测和分析：

1. SonicCrypt 自定义加密器：用于混淆恶意软件代码，增加静态分析的难度。
2. ChaCha20 加密：保护其配置和 C2 通信，防止网络流量分析。
3. 地理限制：避免感染独联体(CIS)国家的计算机，包括俄罗斯、白俄罗斯、乌克兰等，这是许多恶意软件的常见做法，旨在避免这些国家的执法机构的注意。
4. 反调试和反沙箱功能：帮助恶意软件检测分析环境，并在检测到时改变行为。

配置与通信机制

MonsterV2 的配置解密过程包括：读取配置前 32 字节作为密钥材料，与硬编码主密钥结合，解密配置。配置包含多个值，如 anti_dbg、anti_sandbox、autorun、build_name、disable_mutex、C2 IP 和端口等。

通信方面，MonsterV2 使用原始 TCP 连接与 C2 服务器通信，顶层有小型附加组件，用于交换加密密钥和双向认证（类似 SSL/TLS）。连接到 C2 服务器后，它会传输详细的系统元数据，包括操作系统版本、地理位置、用户名和外部 IP，然后等待进一步指令。

已知样本与 C&C 地址

根据可获取的信息，已知的 MonsterV2 相关指标包括：

1. 互斥体模式： Mutant-5B7C3E6F9D8A1F42BCDE0347FA8C9E12D13A4597628F6BD57C4E81A9670D3F5A Mutant-A8F1D32C497EB560C9A21D87F34EB70591D2C864EAF53BD7906C12F8D4E39BAF Mutant-93D8FE2065BCA71BEF2486AD7FA0C935ECC27104ABF9E6531875F22CB40D9E8F
2. 已知 C&C 基础设施： intlspring[.]com 域名被用于传递 MonsterV2 使用 Cloudflare CDN IP 连接 C2 服务器，将恶意流量伪装成合法服务

TA585 攻击者组织分析

组织概况与特点

TA585 是 Proofpoint 于 2025 年 2 月首次发现的网络犯罪组织。该组织的独特之处在于其高度自主性，控制着攻击链的每个环节，从基础设施和传递到有效载荷部署。这与大多数依赖初始访问代理或第三方传递服务的恶意软件分发者形成鲜明对比。

TA585 的主要特点包括：

1. 完整攻击链控制：拥有并管理整个攻击链，包括基础设施、传递方式和恶意软件安装。
2. 自有基础设施：注册并维护自己的恶意基础设施 CoreSecThree，用于托管网页注入和过滤系统。
3. 社会工程学创新：对 ClickFix 技术的熟练使用展示了其在社会工程学方面的创新能力。
4. 精准定向攻击：主要针对金融和会计行业的中小型企业。

历史活动与攻击轨迹

TA585 的活动轨迹可以追溯如下：

1. 2025 年 2 月：Proofpoint 首次发现 TA585 活动，使用美国国税局(IRS)为主题的钓鱼邮件，包含指向恶意 PDF 的链接。
2. 2025 年 3 月：TA585 的活动扩展到冒充 IRS 和美国小企业管理局(SBA)，继续针对金融和会计公司。
3. 2025 年 4 月：TA585 演变为完全自主的基础设施运营者，注册并维护自己的恶意基础设施 CoreSecThree。
4. 2025 年 5 月初：开始使用 MonsterV2 作为主要恶意软件。

5. 2025 年 8 月：利用 GitHub 通知传递 Rhadamanthys 恶意软件。

攻击目标与战术演变

TA585 的攻击主要针对金融和会计行业的中小型企业，每波活动通常发送少于 200 条钓鱼信息，这可能是为了避免引起安全研究人员的注意，或者反映了其精准定向的攻击策略。

在战术演变方面，TA585 展示了从简单的钓鱼邮件到复杂的多渠道攻击的进化：

1. 初期阶段：主要依赖 IRS 主题的钓鱼邮件。
2. 扩展阶段：增加了 SBA 主题，并开始建立自己的基础设施。
3. 成熟阶段：利用多种初始访问技术，包括钓鱼邮件、GitHub 通知滥用和恶意广告。
4. 技术创新：熟练使用 ClickFix 社会工程学技术，通过诱导用户手动执行恶意命令来绕过传统安全防护。

总结与安全建议

威胁总结

TA585 代表了网络犯罪威胁的演变，展示了威胁行为者如何通过控制完整的攻击链和利用创新的社会工程学技术来提高攻击成功率。该组织的自主性和对 ClickFix 技术的熟练使用使其成为一个值得关注的新兴威胁。

CoreSecThree 基础设施的技术复杂性和创新性使 TA585 能够有效地绕过传统的安全防护机制，精准地将恶意负载投递给目标用户。该基础设施的 JavaScript 注入技术、高级过滤机制和通信协议设计展示了现代网络犯罪组织的技术能力和资源投入。

检测与缓解建议

基于对 TA585、CoreSecThree 和 MonsterV2 的分析，以下是一些检测和缓解建议：

1. 网络安全措施： 实施强 URL 过滤和网页分类系统，阻止已知的恶意域名和新注册的可疑域名 监控网络流量，寻找与已知 C2 服务器的通信或可疑的加密通信模式 监控 DNS 请求，识别与已知恶意域名或新注册域名的通信
2. 终端安全措施： 实施 PowerShell 执行策略，限制未签名脚本的执行，并启用详细日志记录 部署基于行为的终端保护解决方案，能够检测可疑的系统活动 实施应用程序白名单，限制未经授权的可执行文件运行
3. 用户教育与意识： 教育用户识别社会工程学攻击，特别是那些要求他们手动执行命令或在系统上进行更改的攻击 鼓励用户在执行任何系统命令或访问可疑链接前验证请求的合法性 建立明确的流程，让用户能够轻松报告可疑邮件、链接或网站

未来趋势展望

随着 TA585 等威胁行为者继续发展其战术和技术，我们可以预期以下趋势：

1. 社会工程学技术的进一步创新：ClickFix 已经展示了社会工程学攻击的创新潜力，未来可能会出现更多绕过传统安全防护的技术。

2. 自主性威胁行为者的增加：TA585 的成功可能会激励更多威胁行为者建立自己的完整攻击链，减少对第三方服务的依赖。
3. 恶意软件功能的持续增强：MonsterV2 等高级恶意软件将继续发展，增加新功能并改进其防御规避技术。
4. 针对性攻击的精细化：随着威胁行为者获取更多关于潜在目标的信息，攻击将变得更加精准和定制化。

组织应保持警惕，不断更新其安全策略和防御措施，以应对这些不断演变的威胁。特别是，应该重视用户教育和意识培训，因为社会工程学攻击如 ClickFix 主要针对的是人类因素，而不是技术漏洞。

点击阅读原文至**ALPHA 8.3**

即刻助力威胁研判

本篇文章来源于微信公众号: 奇安信威胁情报中心

上一篇

空中投放与隐蔽突防——A2PT组织对iOS手机的两起攻击案例的对比解析

下一篇

EtherHiding：APT恶意软件隐藏区块链里

相关文章