绿盟威胁情报月报

2025 年 02 月

绿盟威胁情报中心（NTI）

https://nti.nsfocus.com/

2 月，绿盟科技威胁情报中心（NTI）发布了多个漏洞和威胁事件通告，包含微软 2 月安全更新多个产品高危漏洞通告、Palo Alto Networks PAN-OS 身份验证绕过漏洞(CVE-2025-0108)通告、PostgreSQL SQL 注入漏洞（CVE-2025-1094）通告等。

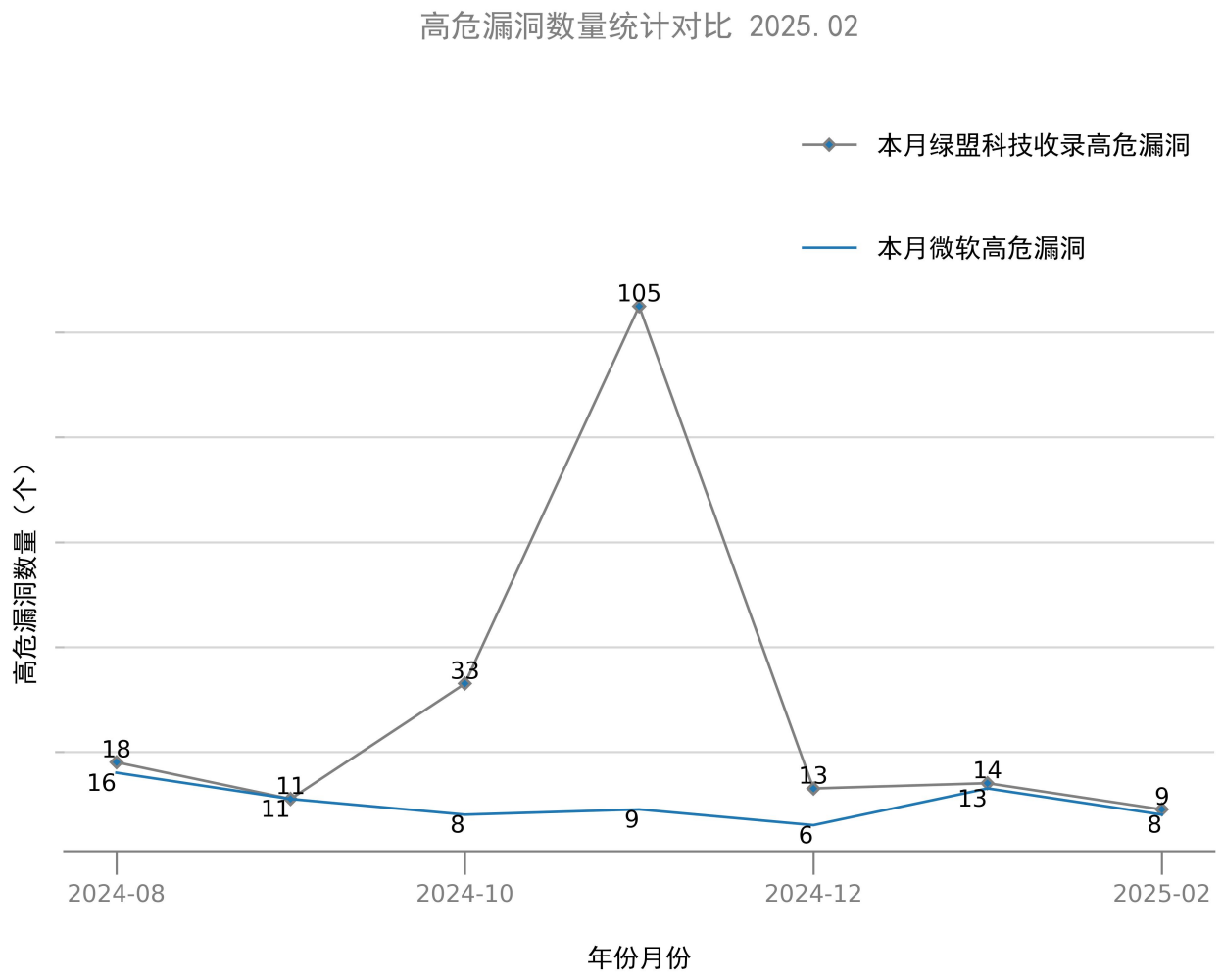
绿盟科技 CERT 监测到微软发布 2 月安全更新补丁，修复了 63 个安全问题，涉及 Windows、Microsoft Office、Azure、Apps、Microsoft Visual Studio 等广泛使用的产品，其中包括权限提升、远程代码执行等高危漏洞类型。

本月的威胁事件中包含，Banshee macOS 窃取程序的新版本，这是一种与针对 macOS 用户的讲俄语的网络犯罪分子有关的恶意软件、Coyote 家族主要针对巴西的用户，试图从 70 多个金融应用程序和众多网站中收集敏感信息、在野黑客通过利用 DeepSeek 的声誉来进行网络钓鱼、虚假投资诈骗和伪装成 DeepSeek 的恶意软件和 SystemBC RAT 现在以 Linux 为目标，传播勒索软件和信息窃取程序等事件。

以上所有漏洞情报和威胁事件情报、攻击组织情报，以及关联的 IOC，均可在绿盟威胁情报中心获取，网址：https://nti.nsfocus.com/

一、 漏洞态势

2025 年 02 月绿盟科技安全漏洞库共收录 68 个漏洞，其中高危漏洞 9 个，微软高危漏洞 8 个。



* 数据来源：绿盟科技威胁情报中心，本表数据截止到 2025.03.05

注：绿盟科技漏洞库包含应用程序漏洞、安全产品漏洞、操作系统漏洞、数据库漏洞、网络设备漏洞等；

二、 威胁事件

1. Banshee macOS 窃取程序的新版本，这是一种与针对 macOS 用户的讲俄语的网络犯罪分子有关的恶意软件。

【标签】macOS

【时间】2025-02-08

【简介】

2025 年 1 月 9 日，国外安全平台披露 Banshee macOS 窃取程序的新版本，这是一种与针对 macOS 用户的讲俄语的网络犯罪分子有关的恶意软件。此算法与 Apple 在其适用于 MacOS 的 Xprotect 防病毒引擎中使用的算法相同。

【参考链接】

https://research.checkpoint.com/2025/banshee-macos-stealer-that-stole-code-from-macos-xprotect/

【防护措施】

绿盟威胁情报中心关于该事件提取 10 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

2. Coyote 家族主要针对巴西的用户，试图从 70 多个金融应用程序和众多网站中收集敏感信息。

【标签】Coyote

【时间】2025-02-08

【简介】

2025 年 1 月 30 日，国外安全平台披露 Coyote 家族利用类似的 LNK 文件。包含旨在执行恶意脚本和连接到远程服务器的 PowerShell 命令。这些文件是最终提供 Coyote Banking 特洛伊木马的多阶段作的一部分。该恶意软件主要针对巴西的用户，试图从 70 多个金融应用程序和众多网站中收集敏感信息。部署后，Coyote Banking

木马可以执行各种恶意活动，包括键盘记录、捕获屏幕截图和显示网络钓鱼覆盖层以窃取敏感凭据。

【参考链接】

https://www.fortinet.com/blog/threat-research/coyote-banking-trojan-a-stealthy-attack-via-lnk-files

【防护措施】

绿盟威胁情报中心关于该事件提取 10 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

3. 在野黑客通过利用 DeepSeek 的声誉来进行网络钓鱼、虚假投资诈骗和伪装成 DeepSeek 的恶意软件

【标签】DeepSeek

【时间】2025-02-05

【简介】

2025 年 1 月 30 日，国外安全平台披露在野黑客通过利用 DeepSeek 的声誉来进行网络钓鱼、虚假投资诈骗和伪装成 DeepSeek 的恶意软件

【参考链接】

https://cyble.com/blog/deepseeks-growing-influence-sparks-a-surge-in-frauds-and-phishing-attacks/

【防护措施】

绿盟威胁情报中心关于该事件提取 10 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

4. TTP-Finance Report: Who Targets Financial Institutions?

【标签】APT

【时间】2025-02-25

【简介】

本报告深入分析了 Sekoia 跟踪和记录的网络犯罪团伙及国家支持的入侵组织。作为 2024 年针对金融机构的最新攻击活动的综合分析，本报告概述了这些攻击的主要威胁来源。读者可以在 Sekoia.io 平台上获取有关这些入侵组织的详细信息，包括其过往行动历史、战术、技术及操作手法。如需了解特定威胁行为体的更多信息，请联系 tdr@sekoia.io。关键发现：初始访问经纪人（IABs）在金融行业的网络犯罪活动中扮演关键角色，他们通过出售未授权的网络访问权限，推动大规模、多层次的攻击。勒索软件与敲诈团伙 持续对金融机构构成重大威胁，利用高级恶意软件、漏洞利用和双重勒索策略，导致运营中断、重大经济损失和声誉损害。银行木马运营商 越来越多地使用复杂恶意软件，利用桌面和移动设备漏洞（包括生物识别数据窃取）来攻击全球金融机构。即服务型网络犯罪（CaaS）模式的普及，使高端网络钓鱼（AiTM）攻击门槛降低，增加了针对金融机构的大规模精准攻击。国家支持的 APT 组织 也将金融行业作为目标，出于经济利益、情报收集或破坏稳定的目的实施网络攻击。主要 APT 威胁：朝鲜 APT 组织（如 Lazarus、Bluenoroff、Andariel）长期以来针对金融行业，利用网络攻击规避国际制裁，并资助弹道导弹和核武器计划。伊朗和中国的 APT 组织 也曾针对该行业，并与网络犯罪分子合作，以提高网络攻击的经济效益并掩盖国家行为的痕迹。部分 APT 组织 既追求经济利益，又进行情报收集。这种双重动机与政府将部分网络攻击外包给私营公司的做法有关。网络犯罪生态系统的复杂性：网络犯罪分子之间的分工日益模糊，“初始访问即服务（IABs）”、“恶意软件即服务（MaaS）”等模式降低了新兴攻击者的入侵门槛。由于金融机构存储大量敏感数据，网络攻击可能导致供应链被入侵，引发广泛影响。国家支持的威胁组织正日益与网络犯罪团伙合作，如 APT33（伊朗）充当 IAB，与勒索软件集团合作获取赎金。结论：金融行业正面临越来越复杂和多层次的网络威胁，攻击者既包括独立的网络犯罪分子，也包括受国家支持的高级威胁组织（APT）。这些攻击的动机涵盖经济利益、情报收集和破坏稳定，金融机构必须加强防御措施，以应对日益复杂的网络威胁格局。

【参考链接】

https://blog.sekoia.io/cyber-threats-impacting-the-financial-sector-in-2024-focus-on-the-main-actors/

【防护措施】

绿盟威胁情报中心关于该事件提取 3 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

5. SystemBC RAT 现在以 Linux 为目标，传播勒索软件和信息窃取程序

【标签】SystemBC RAT

【时间】2025-02-13

【简介】

2025 年 2 月 11 日，国外安全平台披露 SystemBC RAT 现在以 Linux 为目标，传播勒索软件和信息窃取程序

【参考链接】

https://hackread.com/systembc-rat-targets-linux-ransomware-infostealers/

【防护措施】

绿盟威胁情报中心关于该事件提取 2 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

6. Kimsuky APT 正在分发快捷方式文件包含通过鱼叉式网络钓鱼攻击的恶意命令。

【标签】Kimsuky APT

【时间】2025-02-13

【简介】

2025 年，2 月 4 日，国外安全平台披露 Kimsuky APT 正在分发快捷方式文件包含通过鱼叉式网络钓鱼攻击的恶意命令。快捷方式恶意软件伪装成带有 Office 文档图标的文档文件，例如 PDF、Excel 或 Word。执行此文件时，将运行 PowerShell 或 Mshta 以从外部源下载和执行其他有效负载。最终为控制受感染系统而执行的恶意软件是 PebbleDash 和 RDP Wrapper。

【参考链接】

https://asec.ahnlab.com/en/86098/

【防护措施】

绿盟威胁情报中心关于该事件提取 8 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

7. 关于 RapperBot 的僵尸网络恶意软件分析

【标签】RapperBot

【时间】2025-02-13

【简介】

2025 年 2 月 5 日，国内安全平台对于 RapperBot 的僵尸网络恶意软件分析

【参考链接】

https://mp.weixin.qq.com/s/NvlVuA5urPG_r6attAiXsA

【防护措施】

绿盟威胁情报中心关于该事件提取 10 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

8. TTP-GhostSocks-Partner In Proxy

【标签】GhostSocks

【时间】2025-02-28

【简介】

GhostSocks 是一种基于 Golang 开发的 SOCKS5 后连代理恶意软件，最早于 2023 年 10 月在俄语犯罪论坛上被发现，并支持 Microsoft Windows 和 Linux 系统。2024 年 7 月，该恶意软件在英语犯罪论坛上开始传播，采用“GhostSocks”这一名称进行推广。GhostSocks 主要与 LummaC2（Lumma）信息窃取恶意软件捆绑使用，

并以“恶意软件即服务”（MaaS）的方式出售，使攻击者能够轻松利用受感染系统进行非法牟利。其与 Lumma 的深度集成，包括自动配置功能和针对 Lumma 用户的折扣定价，表明攻击者意图增强感染后的滥用能力，提高凭证窃取的成功率，并规避反欺诈检测机制。GhostSocks 的代理通信机制 GhostSocks 的核心功能是 SOCKS5 后连代理，允许攻击者远程控制受害者设备，并将其变成恶意代理节点。它采用 多层代理架构，隐藏攻击者的真实 C2 服务器，主要包括以下步骤：受害者初始感染 GhostSocks 运行后，加载本地配置文件并联系 Tier 1 中继服务器（代理 C2）。中继服务器（Tier 1 Proxy）转发流量受害者不会直接连接到攻击者的真实 C2，而是先与 Tier 1 服务器 建立 SOCKS5 代理隧道。该中继服务器充当转发节点，接收受害者的流量，并进一步传递至 Tier 2 或真实 C2 服务器。真正的攻击控制中心位于 Tier 2 服务器或更深层的基础设施，并通过多个代理层隐藏其位置。受害者的所有流量都被 GhostSocks 代理隧道重定向，攻击者可通过受害者 IP 进行网络活动，如访问银行账户、绕过地理限制、执行欺诈交易等。如果某个 Tier 1 服务器被安全团队发现并封锁，GhostSocks 可通过新的 Tier 1 服务器 自动重新连接，保证持久性。此外，攻击者可通过 C2 下发新指令，动态调整受害设备的代理配置。GhostSocks 的危害隐藏攻击来源：攻击者通过受害者设备发起连接，使恶意活动看似来自合法用户。绕过地理限制与安全防护：金融机构和在线服务通常依赖 IP 识别，GhostSocks 代理可帮助绕过这些机制，提高非法交易成功率。增强攻击链的灵活性：支持远程执行命令、下载额外恶意软件，并可修改 SOCKS5 代理凭证。

【参考链接】

https://infrawatch.app/blog/ghostsocks-lummas-partner-in-proxy

【防护措施】

绿盟威胁情报中心关于该事件提取 10 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

9. 威胁行为者滥用 Gophish 提供新的 PowerRAT 和 DCRAT

【标签】Gophish

【时间】2025-02-14

【简介】

2024 年 10 月 22 日，监测发现一个由未知威胁行为者使用名为 Gophish 的开源网络钓鱼工具包的网络钓鱼活动。

【参考链接】

https://blog.talosintelligence.com/gophish-powerrat-dcrat/

【防护措施】

绿盟威胁情报中心关于该事件提取 6 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

10. Akira 勒索软件不断发展

【标签】Akira

【时间】2025-02-14

【简介】

2024 年 10 月 21 日，监测发现 Akira 不断迭代发展

【参考链接】

https://blog.talosintelligence.com/akira-ransomware-continues-to-evolve/

【防护措施】

绿盟威胁情报中心关于该事件提取 10 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

11. Earth Simnavaz（又名 APT34）对中东发起高级网络攻击

【标签】APT34

【时间】2025-02-11

【简介】

2024 年 10 月 11 日，研究人员发现一个名为 Earth Simnavaz（也称为 APT34）和 OilRig 的网络间谍组织，该组织一直在积极针对中东的主要实体。

【参考链接】

https://www.trendmicro.com/en_us/research/24/j/earth-simnavaz-cyberattacks.html

【防护措施】

绿盟威胁情报中心关于该事件提取 10 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

12. 国家网络安全通报中心公布重点防范境外恶意网址和恶意 IP

【标签】恶意网址

【时间】2025-02-14

【简介】

2025 年 2 月，中国国家网络与信息安全信息通报中心发现一批境外恶意网址和恶意 IP，境外黑客组织利用这些网址和 IP 持续对中国和其他国家发起网络攻击。这些恶意网址和 IP 都与特定木马程序或木马程序控制端密切关联，网络攻击类型包括建立僵尸网络、挖矿木马、远程控制、后门利用等，对中国国内联网单位和互联网用户构成重大威胁。

【参考链接】

https://mp.weixin.qq.com/s/szInvRwcOcs62eBYqWRr2A

【防护措施】

绿盟威胁情报中心关于该事件提取 10 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

13. 新型 APT 组织 DarkGaboon 攻击俄罗斯财务部门

【标签】DarkGaboon

【时间】2025-02-11

【简介】

2025 年 1 月 22 日，据国外安全技术公司 (PT SEC) 专家披露，APT 组织 DarkGaboon 使用携带 Revenge RAT 恶意软件的俄罗斯财务文件作为诱饵，对俄罗斯的财务部门发起攻击。

【参考链接】

https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/dark-gaboon-rossijskie-kompanii-atakuet-ranee-ne-izvestnaya-apt-gruppirovka

【防护措施】

绿盟威胁情报中心关于该事件提取 10 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

14. APT-C-08（蔓灵花）组织 WebDAV 行动分析

【标签】APT-C-08

【时间】2025-03-04

【简介】

2024 年 10 月 21 日，监测到多起通过 searchconnector-ms 文件结合诱饵话题的钓鱼攻击活动，邮件附件压缩包内携带恶意 searchconnector-ms 样本文件，诱导用户打开。通过对攻击者所使用的技战术和相关资源进一步分析，确认为蔓灵花组织发起的钓鱼攻击。

【参考链接】

https://mp.weixin.qq.com/s/kkl0jh14M9DtDGtSGQ4gag

【防护措施】

绿盟威胁情报中心关于该事件提取 10 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

15. PSLoramyra：无文件恶意软件加载程序的技术分析

【标签】PSLoramyra

【时间】2025-03-04

【简介】

2024 年 11 月 27 日，发现一种称为 PSLoramyra 的恶意加载程序。这种高级恶意软件利用 PowerShell、VBS 和 BAT 脚本将恶意负载注入系统，直接在内存中执行它们，并建立持久访问。

【参考链接】

https://any.run/cybersecurity-blog/psloramyra-malware-technical-analysis/

【防护措施】

绿盟威胁情报中心关于该事件提取 6 条 IOC，绿盟安全平台与设备已集成相应情报数据，为客户提供相关防御检测能力。

绿盟威胁情报中心

绿盟威胁情报中心（NSFOCUS Threat Intelligence），作为绿盟科技智慧安全 3.0 战略的重要组成部分，统筹公司的威胁情报生态和能力建设，对外提供威胁情报产品和服务。其依托公司专业的安全团队和强大的安全研究能力，对全球网络安全威胁和态势进行持续观察和分析，以威胁情报的生产、运营、应用等能力及关键技术作为核心研究内容，推出了绿盟威胁情报平台以及一系列集成威胁情报的新一代安全产品，为用户提供可操作的情报数据、专业的情报服务和高效的威胁防护能力，帮助用户更好地了解和应对各类网络威胁。

绿盟威胁情报中心：https://nti.nsfocus.com/

绿盟威胁情报云：https://ti.nsfocus.com/

总部：北京市海淀区北洼路 4 号益泰大厦
绿盟科技（股票代码 300369）

邮编：100089
电话：010-68438880
传真：010-68437328
邮箱：NTI@nsfocus.com