

工信部 | 关于防范MuddyWater组织网络攻击的风险提示 | CN-SEC 中文网

 cn-sec.com/archives/4949464.html

admin

2026年1月27日 00:43:13 [评论](#) 63 views 字数 2388 阅读 7分57秒 阅读模式

工信部发布风险提示，MuddyWater组织近期针对政府、军事、电信、能源等机构发起网络攻击，通过[鱼叉邮件](#)投递伪装PDF和恶意宏文档，释放UDPGangster后门窃取敏感数据。建议禁用Office宏、部署邮件沙箱、监控注册表异常写入。

近日，工业和信息化部网络安全威胁和漏洞信息共享平台（CSTIS）监测发现，MuddyWater组织近期针对政府、军事、电信、能源等机构实施网络攻击，窃取系统凭证、机密文件等敏感数据。

攻击者通过鱼叉邮件投递双重伪装载荷，一类是伪装成PDF文档的可执行文件（如“xxx.pdf.exe”），另一类则在DOC文档中嵌入[恶意宏代码](#)。一旦受害者误启PDF文档，伪装文档将立即释放UDPGangster后门（MuddyWater组织的UDP后门，支持远程控制、窃密等）到本地。对于嵌入恶意宏代码的DOC文档，一旦打开，宏代码将会被静默执行并从自身解密释放后续载荷，将其保存为txt文件后重命名为装载UDPGangster的novaservice.exe可执行文件。攻击载荷成功在内存部署后门后，UDPGangster会将自身复制为SystemProc.exe，并通过写入注册表HKCU...UserShellFoldersStartup实现自动启动。同时，MuddyWater组织采用动态C2连接策略，优先读取本地配置文件，失败则回退至硬编码C2地址。后门程序会收集主机名、工作组、系统版本及用户名等数据，加密回传至服务端，最终建立对目标主机的远程控制。

建议相关单位及用户立即禁用Office宏执行策略，阻断恶意文档释放攻击载荷；部署邮件网关动态沙箱，深度检测伪装PDF的可执行文件及带宏文档；实时监控注册表路径HKCUSoftware...UserShellFoldersStartup异常写入，清除SystemProc.exe后门持久化项。

相关IOC信息

MD5：

07502104c6884e6151f6e0a53966e199

409d02d6153af220e527fd72256ee3a5

561b2983d558283c446ff674ff6138c3

7bfbc76c7eeb652d73b85c99ee83b339

9e06b36f4da737b8d699a6846c2540e9

a39f74247367e0891f18b7662c8e69b5

a546d2363a4b94e361d0874b690c853b

a9235540208fa6a25614c24a59e19199

aa75a0baebc93d4ca7498453ef64128a

bed77abc7e12230439c0b53dd68ffaf7

d84812961fc7cd8340031efd7b5508a8

dd6af28d1a03193fc76001b04d5827cc

de14abbda6a649d9ec90a816847f95db

e09a720574a6594b1444ebc1d6cca969

e5dd608292b6f421b0c108816d25fc5e

SHA256 :

7ea4b307e84c8b32c0220eca13155a4cf66617241f96b8af26ce2db8115e3d53

aea51eaafacd03ade98875b107481d46a8f79ea9d903172b2ed8458c785a8273

d766a8ff123449a8c87fb3570c885439ccfd7d6151847d6d1f44ee7a59c4845c

ff62c294a2bcfee0d291b15ff1fd1733d08ab901281acf9c089f4662b4002a69

SHA1 :

0543e6c36ca89e5d3e13656af0d1b4af0b7585c9

7bb0d162bbaa462c516502d1db56818d24ad825f

903e97ee731796fde34153c71eb718a1015ba358

d00280f07f2159adb16d8f76b7838e3e86773a7e

关联域名 :

157[.]20[.]182[.]75[::]1269

64[.]7[.]198[.]12[::]1259

关联IP地址 :

157[.]20[.]182[.]75

64[.]7[.]198[.]12

· end ·

来源 | 网络安全威胁和漏洞信息共享平台

责任编辑 | 赫敏

声明：本文由工业安全产业联盟平台微信公众号（微信号：ICSISIA）转发，如有版权问题，请联系删除。



如需合作或咨询，请联系工业安全产业联盟平台小秘书微信号：ICSISIA20140417

往期荐读

重磅 | [《自动化博览》2025年第一期暨《工业控制系统信息安全专刊（第十一辑）》上线](#)

征求意见稿 | [网络安全技术 工业控制系统网络安全防护能力成熟度模型（附下](#)

[载\)](#)

工信部 | [关于防范针对DeepSeek本地化部署实施网络攻击的风险提示](#)

干货 | [长输油气管网工控安全防护：策略、实践与展望](#)

DeepSeek分析 | [零信任安全架构在工业领域的发展现状与未来展望](#)

数字化安全 | [工信部印发《高标准数字园区建设指南》（附全文+图解）](#)

AI安全 | [人工智能安全治理框架2.0版（附下载）](#)

干货 | [工业可编程控制系统加密技术研究](#)

荐读 | [安全人视角的DeepSeek洞察与思考](#)

可信数据 | [中国城市可信数据空间行业研究报告（附全文）](#)

关注 | [网络关键设备安全检测结果（第19批）](#)

数据安全 | [国家标准支撑《网络数据安全条例》生效施行（v1.0）](#)

工信部、国家标准委联合印发 | [云计算综合标准化体系建设指南（2025版）](#)

国家标准 | [数据安全国家标准体系（2025版），附下载](#)

OICT 学院



长按二维码

全新的专家视频智库尽收眼底！

这里有你想了解的前沿科技
有你想学习的技术知识
你想探讨的产业发展
想聆听的前瞻观点
认识的业内大咖

CN-SEC | 中文网



www.ICSISIA.com

工业安全产业联盟

微信号：ICSISIA



想要驰骋工业安全圈？
带上我！事半功倍！



使命与责任
提升核心技术能力
服务工业用户

CN-SEC | 中文网



——控制网&自动化博览——

欲了解更多关于自动化、智能制造、人工智能等前沿技术及咨询，请关注我们



长按识别二维码关注 



智能制造推进合作创新联盟

公众号

网罗智能制造的新鲜事

长按二维码关注我们

设为星标 ★



边缘计算洞察

📍 精选产业报告

边缘计算 · 技术 · 实践 · 生态

CN-SEC | 中文网

具身智能产业洞察



技术 | 实践 | 生态

长按二维码关注我们

CN-SEC | 中文网

原文始发于微信公众号（工业安全产业联盟平台）：[工信部 | 关于防范MuddyWater组织网络攻击的风险提示](#)

免责声明:文章中涉及的程序(方法)可能带有攻击性,仅供安全研究与教学之用,读者将其信息做其他用途,由读者承担全部法律及连带责任,本站不承担任何法律及连带责任;如有问题可邮件联系(建议使用企业邮箱或有效邮箱,避免邮件被拦截,联系方式见首页),望知悉。

<https://cn-sec.com/archives/4949464.html>

