

工信部：关于防范GhostPenguin恶意软件的风险提示

 secrss.com/articles/88040



[病毒木马](#) [网络安全威胁和漏洞信息共享平台](#) 2026-02-26

一种针对Linux服务器的新型恶意软件GhostPenguin持续活跃，可导致Linux服务器被远程控制并引发数据泄露等严重风险。

近期，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，一种针对Linux服务器的新型恶意软件GhostPenguin持续活跃，可导致Linux服务器被远程控制并引发数据泄露等严重风险。

GhostPenguin是一个使用C++开发的多线程Linux后门恶意软件。该后门执行时先完成环境自检与初始化，通过调用系统函数（getpuid()和readlink("/proc/self/exe"））获取用户主目录及自身路径，并从指定临时锁文件加载PID值后，利用kill(pid,0)系统调用验证对应进程的活跃状态，实现进程互斥以避免多实例冲突。在通信层面，GhostPenguin采用UDP协议，通过53端口伪装成DNS流量与C2服务器建立信道，首先发送未加密UDP包向C2服务器请求16字节会话密钥，该密钥将作为RC5对称加密算法的密钥对后续通信加密。此外，GhostPenguin核心功能仅在收到C2服务器的“SetStatusActive”（设置状态为活跃）数据包后才会被激活，大幅提升检测难度。一旦核心功能被激活，GhostPenguin可通过多线程处理含远程Shell、文件系统操作等在内的约40种指令，攻击者借此可远程控制受感染设备，窃取敏感数据、破坏系统完整性，严重威胁系统安全可用性及网络环境安全。

建议相关单位及用户加强监测，排查临时锁文件与异常PID验证操作；及时修补Linux系统及应用漏洞，封堵潜在入侵途径；加强账号权限管控，禁用弱密码与违规登录行为；部署终端检测工具扫描匹配GhostPenguin特征的恶意代码；关闭UDP53等非必要端口或设置ip地址白名单，拦截异常加密通信流量等方式防范攻击风险。

相关IOC信息

SHA256：7b75ce1d60d3c38d7eb63627e4d3a8c7e6a0f8f65c70d0b0cc4756aab98e9ab7

SHA1：145da15a33b54e0602e0bbe810ef6c25f2701d50

MD5：7d3bd0d04d3625322459dd9f11cc2ea3

关联域名：

[www\[.\]jiytesti\[.\]com](http://www[.]jiytesti[.]com)

关联IP地址：

124[.]221[.]109[.]147

65[.]20[.]72[.]101

声明：本文来自网络安全威胁和漏洞信息共享平台，版权归作者所有。文章内容仅代表作者独立观点，不代表安全内参立场，转载目的在于传递更多信息。如有侵权，请联系
anquanneican@163.com。

[病毒木马 监管](#)

相关资讯

- [真实案例：苹果手机间谍软件“捕食者”攻击全过程](#)

[病毒木马 黑鸟](#) 2026-02-19

[依旧是iphone间谍软件的话题。](#)

- [安卓手机间谍软件正利用生成式AI进入一个新阶段](#)

[病毒木马 黑鸟](#) 2026-02-20

[全新的安卓恶意软件家族 PromptSpy，这是首个在执行过程中直接调用生成式 AI 实现上下文感知型 UI 操控的移动威胁，标志着安卓恶意软件正式迈入生成式 AI 赋能的新纪元。](#)

- [CNCERT：关于RCtea僵尸网络大范围传播的风险提示](#)

[病毒木马 国家互联网应急中心CNCERT](#) 2026-02-10

[该家族目前正处于快速传播与能力构建阶段，具备极强的对抗与反检测反追踪意识，已具备成熟的DDoS攻击能力，且主要针对物联网（IoT）设备。](#)