关于 NutsBot 新型僵尸网络利用 React2Shell 漏洞传播的风险提示

本报告由国家互联网应急中心（CNCERT）与绿盟科技伏影实验室共同发布。

一、概述

近期，CNCERT 和绿盟科技伏影实验室联合监测到黑客利用 React2Shell（CVE-2025-55182）漏洞传播僵尸网络 NutsBot。

React2Shell（CVE-2025-55182）漏洞是 2025 年 12 月 3 日公开披露的一个高危安全漏洞，具备影响范围广、攻击门槛低、危害程度高等特点。该漏洞源于 React 服务器组件（RSC）协议层的不安全反序列化缺陷，允许未经认证的攻击者通过构造恶意请求在受影响的服务器上执行任意代码，进而实现完全控制、内网渗透或部署恶意软件。

NutsBot 是一款新型僵尸网络家族，该家族不仅继承了传统 DDoS 攻击能力，还集成了信息窃取、远程命令执行、挖矿牟利等多重功能，并通过动态基础设施、复杂认证协议及多种反检测技术，展现出较强的隐蔽性、抗干扰能力和持续演进特征。

近期以来，NutsBot 利用新曝光的 React2Shell（CVE-2025-55182）漏洞进行传播，并持续对国内外目标频

繁发起攻击活动，本报告旨在深入剖析 NutsBot 僵尸网络的技战术特点、传播态势及造成的现实威胁，并提供相关防范建议。

二、僵尸网络分析

（一）相关样本分析

1.核心特点

攻击者在部署该僵尸网络木马时，常使用“nuts”作为恶意软件的存放目录名。基于这一特征，我们将其命名为 NutsBot 僵尸网络家族。“nuts”一词在英文中兼有“疯狂”与“坚果”的双重含义，这一命名恰好影射了该僵尸网络的行为特征与防御特点：一方面，其传播迅速、活动猖獗，体现出“疯狂”般的攻击性；另一方面，其采用多层认证、反追踪等严密防护机制，犹如“坚果”般难以破解。该家族具备如下特点：

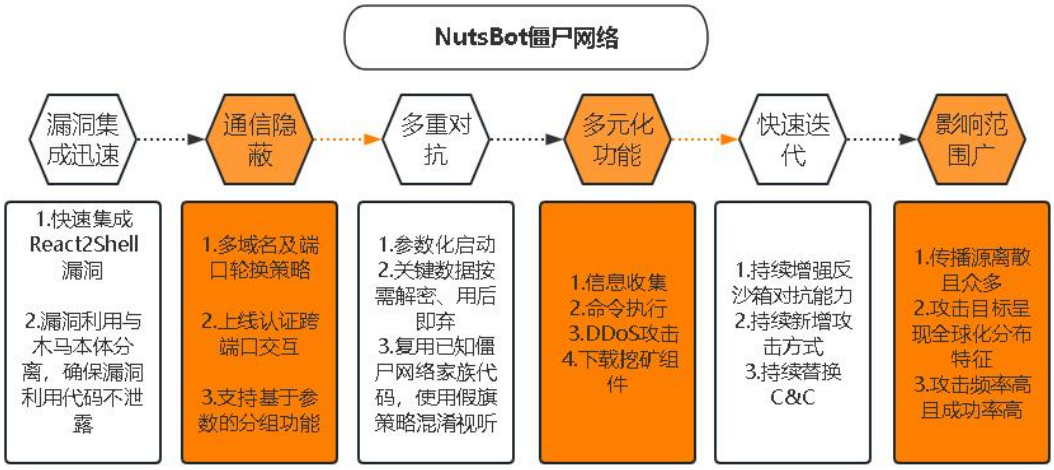

图 1NutsBot 僵尸网络特点

2.多维攻击体系

NutsBot 僵尸网络在功能上除了 DDoS 还内置多重常规 IoT 僵尸网络家族不具备的功能：

信息收集：不同于常规的 IoT 类僵尸网络家族，NutsBot 僵尸网络会收集并上传主机信息，为后续的横向移动或更有针对性的攻击提供了信息基础。

命令执行：NutsBot 僵尸网络家族具备命令执行的功能，能够执行 kill 自身，重启及远程 shell 命令，这使得其具备的威胁性陡然提升；

DDoS 攻击：其 DDoS 攻击模块复用了 Mirai 家族的核心代码结构，支持十余种攻击向量，并扩展了新的指令字段，表明其持续进行功能演进。攻击指令可通过网络动态下发，实现对指定目标的精准打击。

挖矿：监测发现，攻击者利用同一传播渠道分发挖矿木马，并主动清除宿主机上已有的其他挖矿程序（如 XMRig），以独占系统资源。这揭示了攻击者不仅追求直接的破坏性攻击，更致力于将受控设备“变现”为可持续牟利的资产。

3.通信机制与隐匿手段

NutsBot 在设计上着重强化了其通信链路的隐蔽性与生存能力。

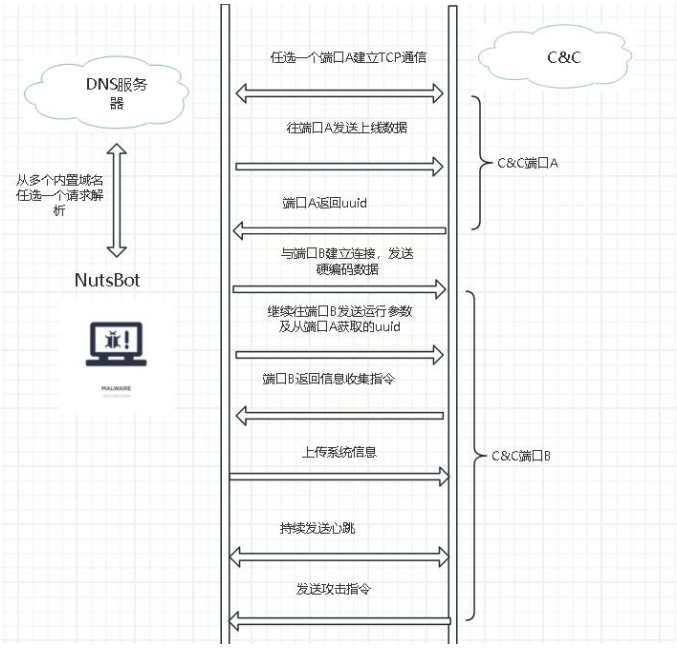

图 2 通信过程

动态基础设施：该僵尸网络内置了多个备份的 C&C 域名与端口列表，并采用加密形式存储。在通信时随机选择，当某个节点被阻断时可无缝切换至其他节点，保证了控制通道的持续性。

复杂认证协议：上线认证过程被设计为需在同一 C&C 服务器的不同端口间完成多步交互（如先于端口 A 获取令牌，再于端口 B 完成校验）。这种设计打破了传统僵尸网络单端口、明文通信的模式，有效干扰了基于简单流量监听和协议逆向的追踪分析。

4.对抗与规避检测

NutsBot 僵尸网络家族集成了多种规避安全检测的技术手段：

对抗沙箱：木马主体运行依赖于启动参数，在无参数环境下不会运行，以此规避自动化沙箱系统的检测。

数据加密：同时，其核心配置信息（如 C&C 地址）均经过加密处理，仅在内存中动态解密使用，关键数据按需解密、用后即弃增加了静态分析的难度。

人为参与对抗：攻击者在短时间内对 NutsBot 僵尸网络进行了多轮更新迭代。与早期版本相比，当前变种在反沙箱对抗能力、核心攻击功能以及内置 C&C 基础设施等方面均有所强化。

（二）传播方式分析

通过跟踪监测，我们发现 NutsBot 主要通过 React2Shell 漏洞（CVE-2025-55182）传播。React2Shell 漏洞源于 React 服务器组件（RSC）所采用的“Flight”协议中存在不安全反序列化缺陷。在处理客户端提交的 RSC 载荷时，服务端未能对传入数据实施有效的验证与过滤。攻击者可据此构造包含恶意 JavaScript 代码的 HTTP 请求，发往启用 RSC 功能的任意端点。由于漏洞存在，服务器会将恶意载荷错误识别为可执行的代码逻辑予以解析并运行，从而实现攻击绕过。

此漏洞影响范围广泛，涉及以下核心框架版本：React 19.0.0、19.1.0、19.1.1 及 19.2.0。由于其利用过程无需身份认证且稳定性高，成功利用可导致以下严重后果：

完全控制服务器：攻击者能够执行任意系统命令，窃取服务器敏感数据与凭证。

横向移动渗透：以受控服务器为跳板，对内网其他系统进行进一步渗透。

部署恶意软件：在实际攻击中已观察到攻击者借此植入挖矿程序、后门、勒索软件等高危远控恶意代码。

监测显示，CVE-2025-55182 在公开曝光仅一天（12 月 4 日）后，NutsBot 僵尸网络就成功将其武器化，迅速进入实际攻击阶段。

三、僵尸网络感染规模

通过监测分析发现， 2025 年 12 月 16 日至 21 日期间，NutsBot 僵尸网络在我国境内已确认的活跃“肉鸡”规模约 1.14 万台，境内日上线肉鸡数量最高达 3626 台，肉鸡 C2 日访问量最高达 86.3 万次。主要控制服务器情况如下：

图 3 境内日上线肉鸡数量分布情况

四、防范建议

请广大网民强化风险意识，加强安全防范，避免不必要的经济损失，主要建议包括：

（1）梳理已有资产列表，及时修复相关系统漏洞，包括历史漏洞和最新曝光的漏洞。

（2）加强口令强度，避免使用弱口令，密码设置要符合安全要求，并定期更换。建议使用 16 位或更长的密码，包括大小写字母、数字和符号在内的组合，同时避免多个服务器使用相同口令。

（3）尽量不打开来历不明的网页链接，不要安装来源不明软件。

（4）建议通过官方网站统一采购、下载正版软件。如无官方网站建议使用可信来源进行下载，下载后使用反病毒软件进行扫描并校验文件 HASH。

（5）安装终端防护软件，定期进行全盘杀毒。

（6）当发现主机感染僵尸木马程序后，立即核实主机受控情况和入侵途径，并对受害主机进行清理。

五、相关 IOC

样本 MD5：

3BA4D5E0CF0557F03EE5A97A2DE56511

0BA11AF560B518E89F9D16F960D9E567

DA8036683C31844AFD2ECD987E9997A6

0BEE4906B5F233842BB2BA1FF85639AA

49051A130E9C30705D5A46E0CD00D800

4F214639E82779B623D14BAD7856E646

0BA11AF560B518E89F9D16F960D9E567

DA8036683C31844AFD2ECD987E9997A6

0BEE4906B5F233842BB2BA1FF85639AA

49051A130E9C30705D5A46E0CD00D800

4F214639E82779B623D14BAD7856E646

下载链接：

http://31.56.27.76/n2/aarch64

http://31.56.27.76/n2/tbk

http://31.56.27.76/n2/armv5l

http://31.56.27.76/n2/lterouter

http://89.144.31.18/nuts/x86

http://89.144.31.18/nuts/x

http://89.144.31.18/nuts/armv7l

http://89.144.31.18/nuts/arm4

http://5.255.121.141/nuts/x86

http://5.255.121.141/nuts/x

http://5.255.121.141/nuts/lc

http://5.255.121.141/nuts/bolts

http://193.34.213.150/nuts/x86

http://193.34.213.150/nuts/bolts

http://185.14.92.152/nuts/lc

http://45.61.157.12/nuts/bolts

控制 IP：

185.14.92.55

5.253.188.173

77.110.104.193

69.169.104.2