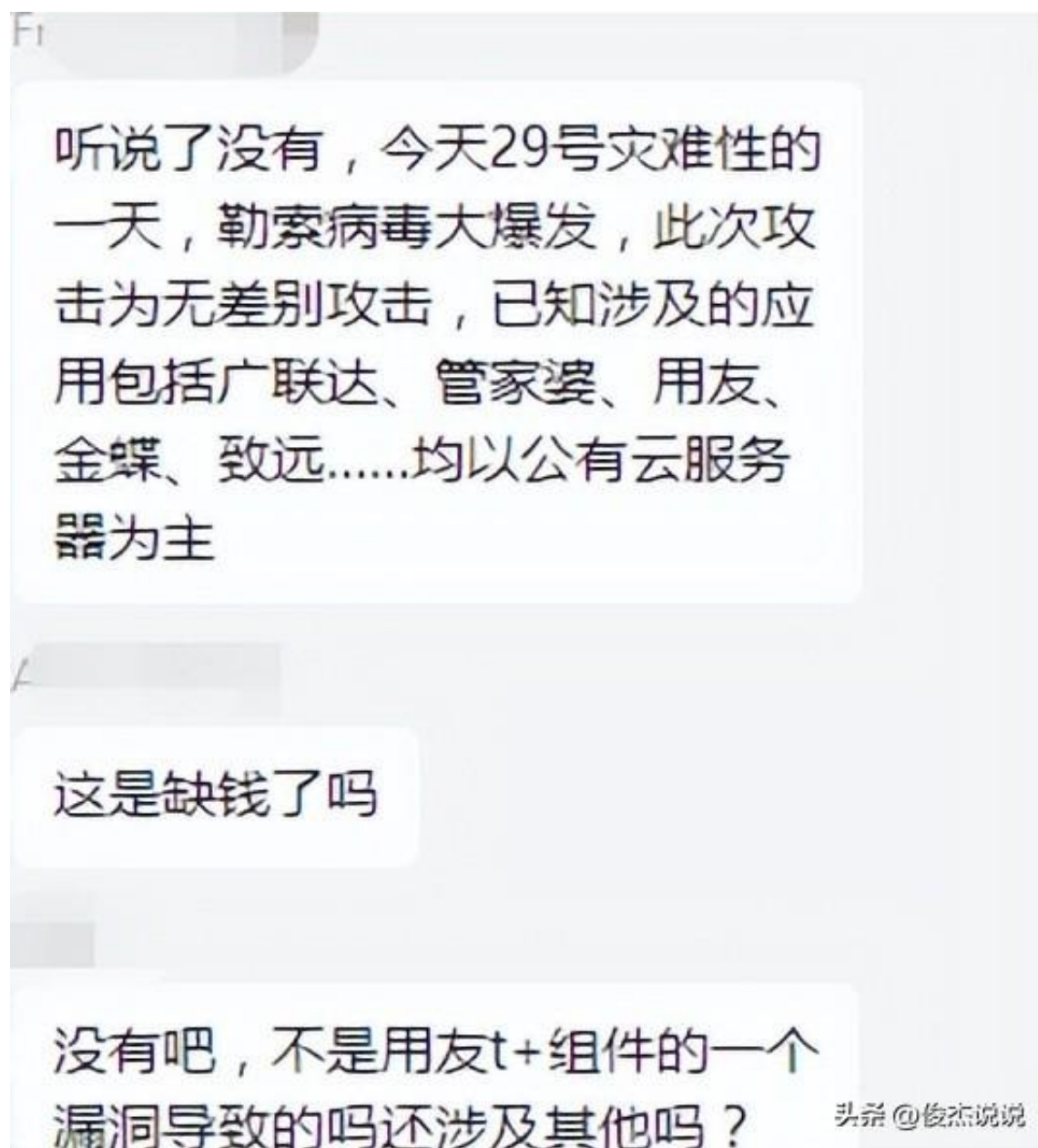


国内知名技术社区 [qldao123.com](http://qldao123.com)

最新消息，国内多个安全技术社群

传出今天针对以疑似用友为代表的国产管理软件勒索病毒大爆发 [#勒索软件攻击#](#)



昨晚勒索病毒开始大面积攻击国内领先软件厂商，请所有使用用友和畅捷通软件的客户朋友检查数据备份，把数据拷贝到移动硬盘做异机存储，防止遭受攻击后数据无法找回。当发现系统异常时，请及时与服务人员联系。已经有近很多客户反馈已发生中毒，请大家务必重！

头条 @俊杰说说



头条 @俊杰说说

通过我们远程排查，目前可以确认黑客是利用了某CRM系统漏洞，通过命令执行发起的攻击。

```
cmd /c curl -s -u user:password@192.168.1.100:8080 -X POST -d '{"username": "admin", "password": "123456"}' http://192.168.1.100:8080/api/login
```

头条 @俊杰说说

此外，通过与攻击者的沟通邮件可

以肯定对方也是中文使用者，沟通全程使用中文进行对话，且语句非常自然并非“机翻”。



## 关联漏洞信息

对于此次勒索病毒传播所依赖的漏洞，推测为本月初发现的一个0day漏洞。

2022年8月5日，360漏洞云便收到漏洞情报：某

流行企业财务软件存在0day漏洞。通过对其官方已发布的补丁和漏洞细节进行反复对比，确认此漏洞尚无补丁，为0day漏洞。

相关漏洞为WEB类漏洞，漏洞触发效果为RCE，漏洞触发过程为反序列化远程代码执行。

## 受到攻击地域分布统计

此次攻击从8月28日21时30分左右开始大规模爆发，一直持续到8月29日1时左右，截至当前360安全大脑观察到有1986台机器遭到攻击，统计地域分布如下

。

# AI Ops 峰会

14:00-14:10  **出品人开场**  
熊昌伟  
用友畅捷通公司助理总裁

14:10-14:40  **AI Ops异常检查和根因分析在云上环境实践**  
周琦  
阿里云资深技术专家

14:40-15:10  **关于智能运维中算法落地的一些思考**  
王鹏  
复旦大学计算机科学技术学院教授  
融创科技首席数据科学家

15:10-15:40  **智能运维在安信证券的应用实践**  
权宁升  
安信证券智能运维负责人

15:40-16:10  **用友畅捷通如何通过智能运维来提升稳定性保障**  
文吉  
用友畅捷通SRE负责人

**时间：**  
2022年8月30日 14:00



头条 @ 智行理财网

而针对电子元器件企业的攻击也在加剧

我们期待文中提到的中国相关管理软件厂商的回应

请大家赶紧抓紧时间做

离线备份

80%的企业做不好备份/恢复

据路边社可靠线报

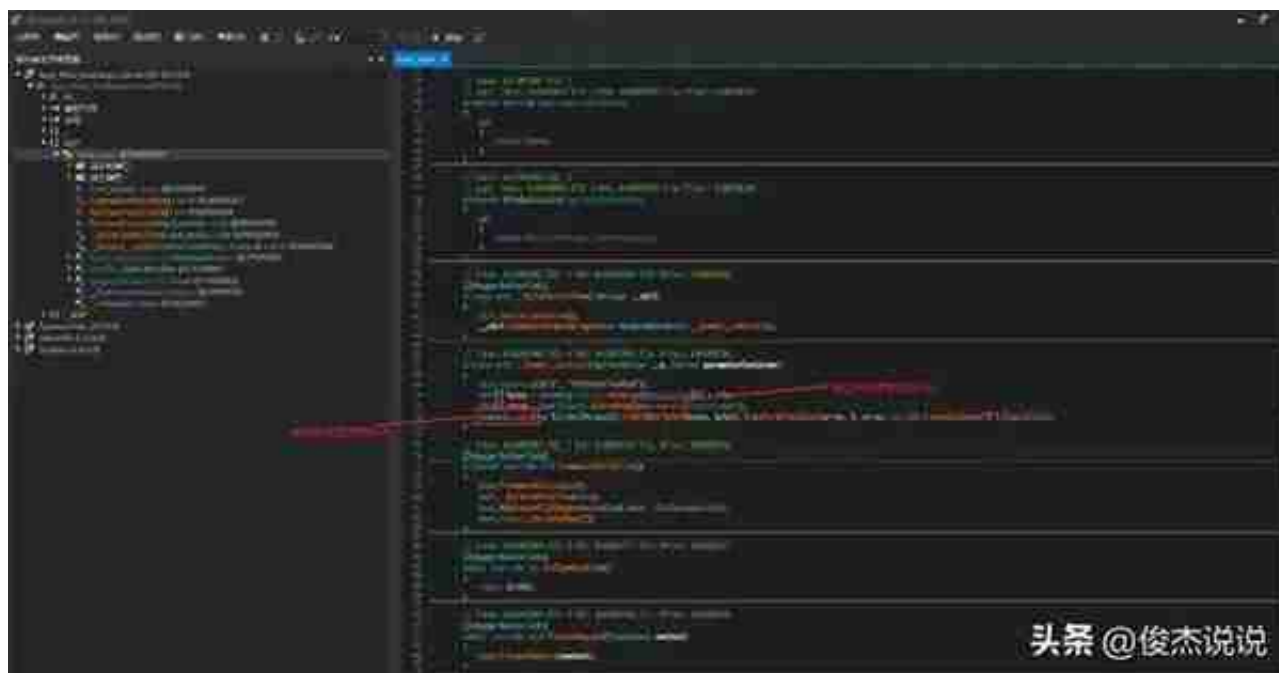
最新消息超过2000家企业已收到[#勒索病毒猖獗#](#)

[#老板,服务器中了勒索病毒,需要10万,怎么办?#](#)

火绒安全实验室监测，疑似借助用友畅捷通T+传播的勒索病毒模块异常活跃（FakeTplus病毒）。火绒工程师排查某勒索现场时发现，病毒模块的投放时间与受害者使用的用友畅捷通T+软件模块升级时间相近，不排除黑客通过供应链污染或漏洞的方式进行投毒。火绒安全软件可成功查杀该病毒。



被勒索后，需要支付0.2个比特币（目前大概27439人民币），黑客留下的勒索信，如下图所示：



，通过与攻击者的沟通邮件可以肯定对方也是中文使用者，沟通全程使用中文进行对话，且语句非常自然并非“机翻”。