

# SolarWinds失陷服务器测绘分析报告

阅读量 **499077**

发布时间 : 2020-12-18 16:00:27

分享到: 

## 0x01背景

美国时间2020年12月13日，SolarWinds公司的orion平台软件被爆出存在供应链后门，使用该公司产品的数百家美国核心组织机构被国家级APT组织入侵。

在此事件披露后不久，Solarwinds供应链后门的C&C开始被微软和域名服务商接管锁定，攻击者似乎已无法通过C&C控制失陷的SolarWinds服务器。但在360威胁情报中心发布的SolarWinds供应链攻击揭秘报告中，明确指出了此次事件相关的核心后门程序外，攻击者还在SolarWinds服务器中植入了另外的WebShell后门程序。

据悉，SolarWinds公司为全球30万家客户提供了产品服务，SolarWinds失陷服务器有可能仍然遍布网络空间，相关组织机构仍然存在极大的安全风险。依靠360安全大脑的全网安全能力，360Quake团队联合360高级威胁研究分析中心对全网的SolarWinds服务器进行了分析调查。

## 0x02Solarwins WebShell后门分析

Solarwinds orion平台的Web控制台和IIS等Web中间件是无缝绑定的，因此攻击者可以从外网直接访问服务器。



### 360Quake空间测绘系统

系统地址: <https://quake.360.cn/>

文章 **12**

粉丝 **1**

### TA的文章

360Quake V5.0新版上线，文末福利满满等你来体验！

2021-07-23 18:30:27

活动 | 360QUAKE年度活动限时大放送最后一波啦！

2021-04-30 18:00:58

Quake新功能更新：一键C段查询与数据去重

2021-04-19 18:00:38

浅析Cobalt Strike Team Server扫描

2021-04-16 15:30:28

360Quake红蓝对抗新功能更新

2021-04-12 17:27:18

### 相关文章

虚假 Meta 广告劫持 Facebook 帐户以传播 SYS01 信息窃取程序

2024-10-31 10:43:35

网络钓鱼者通过Eventbrite服务接触目标

2024-10-30 15:47:51

摩根大通在病毒式“无限金钱故障”后起诉诈骗者

2024-10-29 11:01:39

BeaverTail 恶意软件在针对开发人员的恶意 npm 包中重新出现

2024-10-29 10:52:05

臭名昭著的黑客组织 TeamTNT 启动新的加密货币挖矿云攻击

2024-10-28 11:11:32

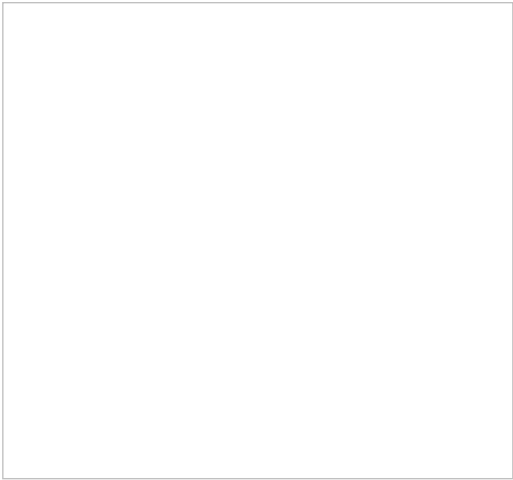
加密劫持警报：黑客利用 gRPC 和 HTTP/2 来部署矿机

2024-10-23 15:40:58

Meta 利用面部识别技术打击欺诈和账户接管行为

2024-10-23 15:31:54

### 热门推荐



在此次solarwinds供应链攻击事件中，攻击者在后渗透阶段针对特定目标solarwinds服务器的Web控制台植入了Webshell后门组件，该组件的原厂功能是根据网络请求数据给管理平台网页返回显示logo图片，而在后门组件中对原功能增加了一段后门代码。



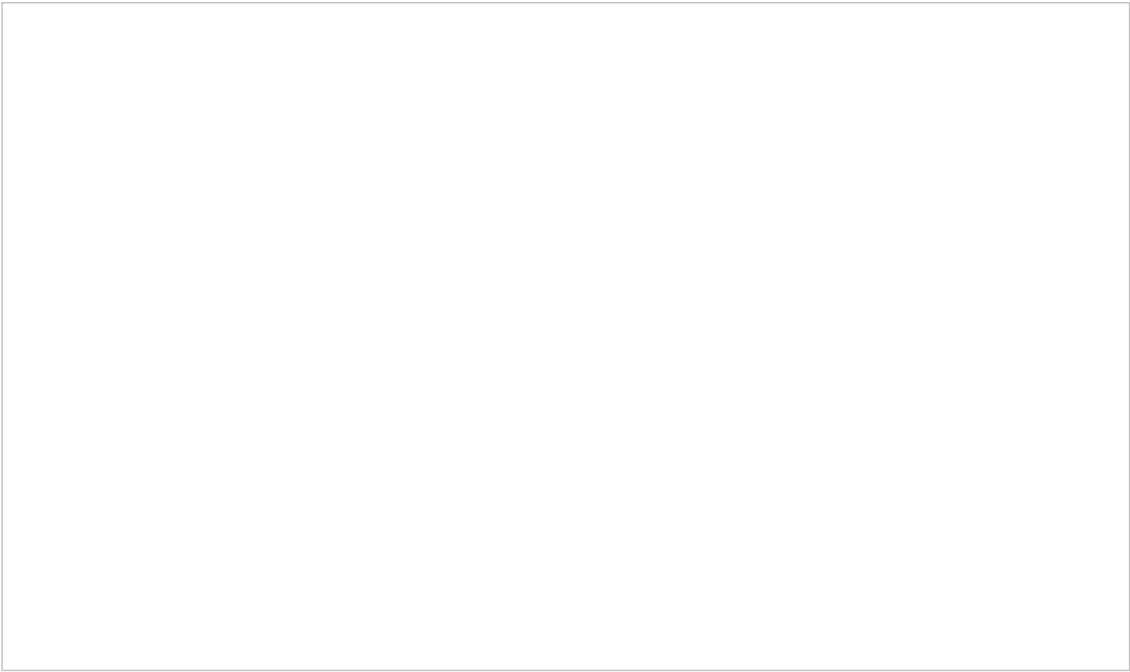
该处新增的后门代码为原文件新增了codes、clazz、method、args这四个额外的HTTP请求参数。

### 文章目录

- 0x01背景
- 0x02Solarwins WebShell后门分析
- 0x03SolarWinds服务器存活情况
- 0x04Solarwins WebShell抽样排查
- 0x05总结
- 0x06参考文章



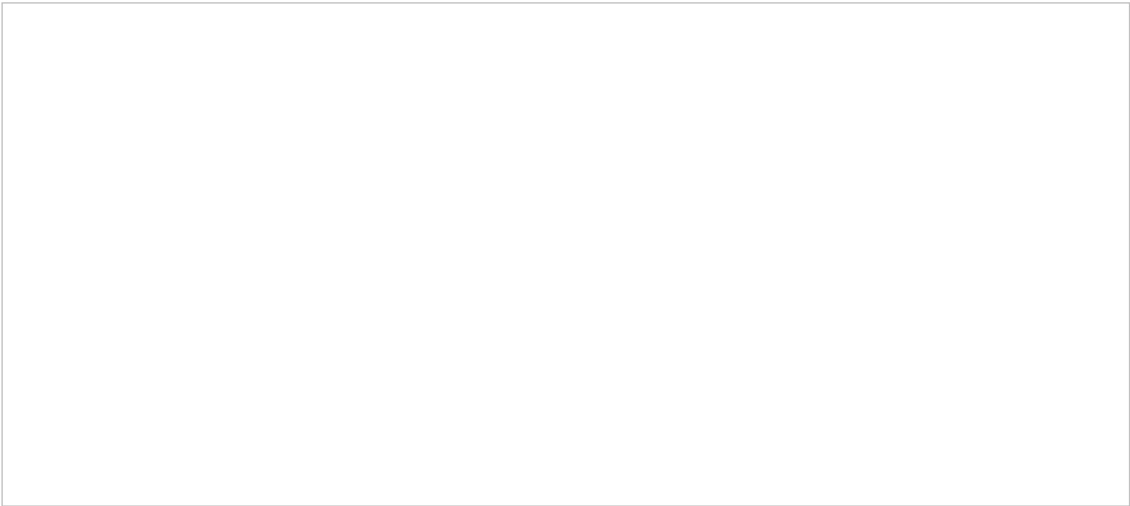
攻击者通过HTTP请求传入的任意自定义代码，最终会被后门代码动态编译执行。



0x03SolarWinds服务器存活情况

根据Quake 的搜索语法：app:“Solarwinds-orion”

我们发现SolarwindsOrion 的一年内资产数据为3146条，独立IP数量为1414个。国家分布和国内各个省份分布如图所示：





利用Quake搜索：app:“Solarwinds-orion”AND response:“2019.4”

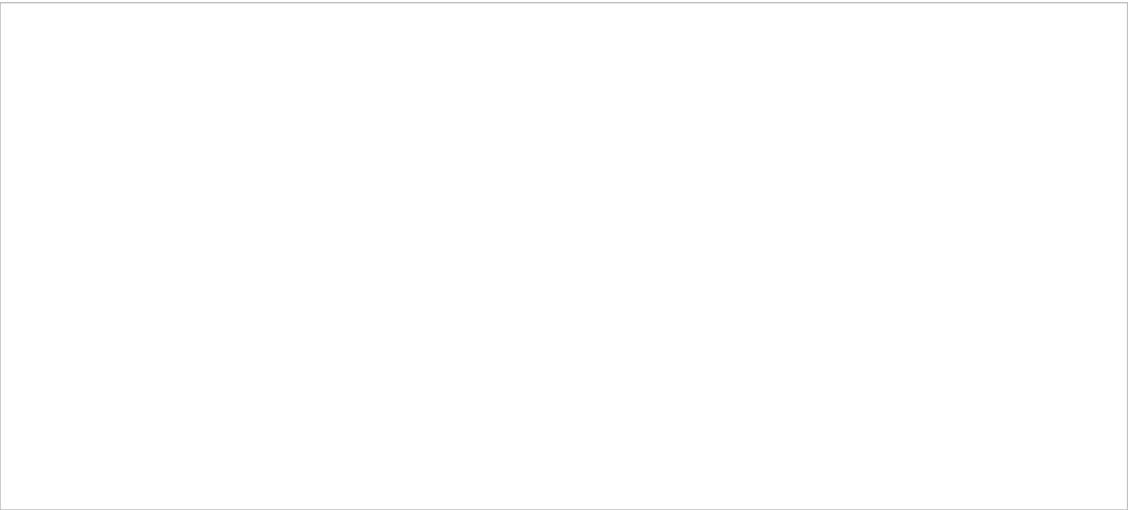
发现受影响的 2019.4版本的有485个，

利用Quake搜索：app:“Solarwinds-orion”AND response:“2020.2.1”

发现受影响的2020.2.1版本有218个。



在对Solarwinds orion平台进行探测的同时，我们统计了搭建Solarwinds orion平台的windows server版本。根据探测的结果，可以发现Solarwinds服务器环境占据前五的主要是：



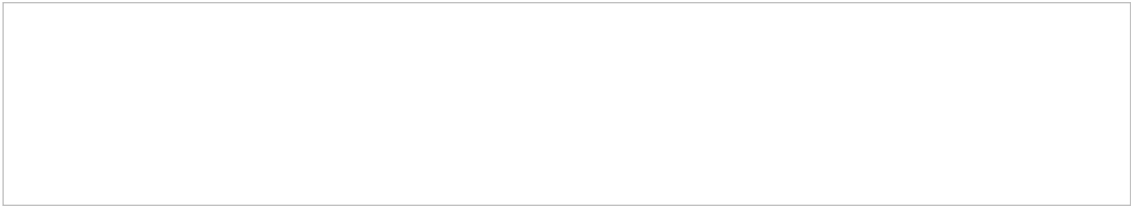
因为iis8.0和iis8.5同属于WindowsServer 2012，所以前四的windows服务器版本环境分别对应的是WindowsServer 2016， WindowsServer 2012， WindowsServer 2008， WindowsServer 2003。

### 0x04Solarwins WebShell抽样排查

结合Webshell的分析特征，我们发现请求Orion/LogolmageHandler.ashx响应文件类型会被强制设置“text/plain”。



我们针对该特征对全球的Solarwinds orion平台进行抽样分析，发现了多台疑似被植入WebShell后门的服务器。部分后门服务器列表如下：



### 0x05总结

本次探测结果可知，全网视野下存在安全隐患的Solarwinds服务器数量仍是以美国地区为最多，而国内也存在少部分隐患资产。

目前，Solarwinds供应链后门的C&C已被安全厂商和域名服务商接管锁定，但攻击者除开使用C&C控制失陷服务器外，很可能再通过其他预置的后门，利用外网失陷Solarwinds服务器再次入侵目标，请相关的组织机构提高警惕。

更多网络空间测绘领域研究内容，敬请期待~

Happy hunting by using 360-Quake.


### 0x06参考文章

[https://mp.weixin.qq.com/s/lh7y\\_KHUxag\\_-pcFBC7d0Q](https://mp.weixin.qq.com/s/lh7y_KHUxag_-pcFBC7d0Q)

本文由 **360Quake空间测绘系统** 原创发布  
转载，请参考 [转载声明](#)，注明出处：<https://www.anquanke.com/post/id/226029>  
安全客 - 有思想的安全新媒体

恶意活动

6赞 ☆ 收藏

 360Quake空间测绘系统

分享到：

### 发表评论

您还未登录，请先登录。

登录



### 安全客

- [关于我们](#)
- [联系我们](#)
- [用户协议](#)

### 商务合作

- [合作内容](#)
- [联系方式](#)
- [友情链接](#)

### 内容需知

- [投稿须知](#)
- [转载须知](#)
- [官网QQ群：568681302](#)

### 合作单位

