

FLEXISPY

24/7 +1 213 810 3122

中文

产品功能兼容性感谢信搜索更多

世界上最具权威的电脑、手机和平板电脑的监控软件

无论在哪里，你都能了解电脑和手机上所发生的一切



- ✓ 监控所有手机的数码和音频通讯信息
- ✓ 监控所有电脑&Mac用户的活动
- ✓ 支持安卓、苹果, iPad, PC 和 Mac
- ✓ 比其它任何任何软件的功能更多、
- ✓ 退款保证
- ✓ 安装服务

立即接通在线客服

FS FlexiSPY 销售部
在购买之前请先了解

在线交谈已开始

FS FlexiSPY Sales
Hi! Do you have any questions I can help you with?

在这里输入您的消息

选项 登录 zendesk

请观看演示 立即

自称世界上最权威监控软件FlexiSpy被黑删库，怎么做到的？



嘶吼吼 · 1 天前

FlexiSpy是什么

FlexiSpy是一款非常知名的手机、电脑监控软件，也就是我们常说的远控。

FLEXISPY

24/7 +1 213 810 3122

产品

功能

兼容性

感谢信

搜索

更多

查看软件的所有强大功能

监控通话

- 实时监控通话
- 记录通话内容⁵
- 通话记录
- VOIP通话记录⁶
- VOIP 通话录音⁶
- 监听手机的周围环境
- 记录手机环境⁸
- FaceTime偷录³

监控文本信息

- 读取短信内容
- 读取彩信内容⁸
- 发送“发送/删除/回复”短信
- 删除包含关键词的短信⁸
- 读取电子邮件内容

监控GPS

- 查看和跟踪GPS定位

监控即时聊天内容

- WhatsApp⁶
- Facebook / FB信使⁶
- Viber⁶
- LINE⁶
- Skype⁶
- WeChat 微信⁶
- iMessage⁴
- BBM⁴
- Blackberry PIN²
- 雅虎通⁶
- 环聊⁶
- KIK¹
- Telegram¹
- Tinder⁶
- Instagram⁶
- QQ¹
- Hike¹

监控多媒体

- 视频文件
- 图像文件
- 音频文件

远程监控

- 用摄像头拍照⁸
- 重启设备⁶
- 检查设备的电池状态
- 短信远程指令

监控互联网

- 浏览过的网页⁶
- 书签⁶

监控应用程序

- 通讯录
- 日历⁶
- 便签⁴
- 已安装的程序⁸
- 程序活动

及时收到警报

- 更换SIM卡
- 呼叫特定联系人
- 警报号码

秘密监控

- 隐藏越狱痕迹⁴
- 隐藏SuperSU痕迹¹
- 设法不被程序列表/任务管理器发现

易于使用

- 易于安装
- 在线远程指令
- 升级
- 24/7 支持

4月22日，Tek在推特声称窃取了FlexiSpy的源代码和二进制文件。

Tek

@tenacioustek

正在关注

I have uploaded the source code and binaries of #FinSpy dumped by @fleximinx on github :

翻译自英文

Te-k/flexidie

flexidie - Source code and binaries of FlexiSpy from the Flexidie dump

github.com

转推

65

喜欢

79

下午3:16 - 2017年4月22日

知

首发于
嘶吼RoarTalk

写文章

登录



Flexidie
@fleximinx

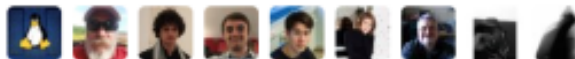
+ 關注



Hack Back! pastebin.com/raw/Y1yf8kq0

轉推
103

喜歡
130



下午1:21 - 2017年4月24日

↩ 8

↻ 103

❤ 130

入侵细节分析

第1步：信息收集

查询子域名

```
192.168.2.231 portal.vervata.com
58.137.119.230 www.vervata.com
180.150.144.84 api.flexispy.com
180.150.144.84 admin.flexispy.com
180.150.144.83 affiliate.flexispy.com
180.150.144.83 affiliates.flexispy.com
180.150.144.83 blog.flexispy.com
180.150.156.197 client.flexispy.com
180.150.144.82 community.flexispy.com
58.137.119.229 crm.flexispy.com
54.246.87.5 d.flexispy.com
216.166.17.139 demo.flexispy.com
180.150.144.86 direct.flexispy.com
180.150.144.85 ecom.flexispy.com
54.169.162.58 log.flexispy.com
180.150.147.111 login.flexispy.com
68.169.52.82 mail.flexispy.com
68.169.52.82 mailer.flexispy.com
180.150.144.86 mobile.flexispy.com
180.150.156.197 monitor.flexispy.com
180.150.144.87 portal.flexispy.com
68.169.52.82 smtp.flexispy.com
180.150.144.82 support.flexispy.com
```

知

首发于
嘶吼RoarTalk

写文章

登录

发现服务器位于Cloudflare后面，这就比较尴尬了。因为Cloudflare带有WAF，没法进行扫描、爆破等自动化的渗透。

但是发现了一个域名，是admin.flexispy.com。可能是一个管理面板。

尝试sql注入

在登录页面上尝试了一些sql注入，没发现问题。

之后尝试了下常见默认密码，admin:admin，测试的时候发现惊喜，是的，就这样登录进去了。



但是这个账户登录之后有限制，无法使用。通过后台页面查看发现某个页面可以查看用户详细信息，包括许可证详细信息以及编辑用户详细信息（如用户名、密码等）的功能。

网址如下所示：

```
https : //admin.flexispy.com/secure/employee/editEmployee?employeeId=1
```

这个页面存在平行越权漏洞，只需将id = 1更改为id = 2，就能显示另一个用户的详细信息，并允许在界面上重置密码。

于是我写了个脚本，指定id值的范围是1-99999，把遍历结果存储为文本文件。搜索下有没有感兴趣的用户，倒是找到了那么几个，但是没太多用，对FlexiSpy启不到致命的打击。

第2步：继续打破边界

58.137.119.224 - 58.137.119.239
202.183.213.64 - 202.183.213.79

有几台服务器运行着ssh服务，还有一个Microsoft Exchange服务器和一些开放着rdp服务的服务器，以及运行着WildFly(Jboss)默认页面的网站跟CRM网站。这些信息收集表明，FlexiSpy内部网络里有Linux和Windows，不过这时候我没有访问权限，还需要继续看。

发现有个服务器上开放了端口8081，似乎是一个Sonatype Nexus存储库，其中存在一些jar文件，可能是用于命令和控制Web应用程序。或许里面存放的文件是FlexiSpy故意放着的，以便其客户安装？

我下载了一份，并使用procyon(Java反编译器)开始逆向查看审计java代码。

我下载了几个有趣的公共项目，第一个是他们的Mailchimp API密钥，可以看到他们向新客户发送的电子邮件（他们鼓励客户改变默认密码）。

这个密码看起来应该是共享的默认密码：tcpip123。我尝试用这个密码登录ssh、WildFly，但是没有成功。

最后我决定试试登录CRM，效果很赞，登录成功了并能操作某些模块的安装，最终上传了shell。

<https://bitbucket.org/mstrobels/procyon/wiki/Java%20Decompiler>

第3步：内网渗透

通过第2步拿到的webshell，我们已经进入到了FlexiSpy的内部网络。

拿到的主机权限是低权限，内核版本较新，可以使用DirtyCow提权，但是许多公开的漏洞利用风险较高，更可靠更稳定的方法是创建与CRM服务器相同的虚拟机，这将需要很长的时间。

放弃了以上的方法，我通过代理进入内网，把一个端口扫描器跟弱口令扫描放在服务器上，开始扫描22、3339和23端口。

我做的第一件事是部署SSH扫描器，来测试root:tcpip123、admin:tcpip123和Administrator:tcpip123等简单组合。

通过扫描，我拿到了三台NAS服务器，都是Linux x86-64机器。之后把自己写的工具上传到其中的一台服务器，继续搜集内网的信息。通过几天的分析，我发现了备份主目录、HR文档、公司文件、一些SSH密钥、密码备份、内部网络图等等。大多数文件已经过时，但是我将密码/用户名组合，收集到了几个具有sudo权限的服务器（servicescenterip123 and servicescenterip123）

我从其中一台服务器窃取了SSH密钥，对Jenkins服务器进行了控制，将所有存储库下载回来，并将其发送到随后控制的互联网上的服务器上。

我留意到现在可以访问所有Windows域的域控制器，于是开始删除了一些恶意软件，并慢慢从入侵到的设备中从内存中提取凭据。这些凭证中的一个属于IT负责人员，这使我能够访问内部SharePoint服务器。

到目前为止，我认识到FlexiSpy的安全就是胡扯。为了尽可能多地提供不同的访问点，我将Tor安装到Linux基础设施部署，将每个服务器的SSHd设置为隐藏服务。我尽可能地离开，停止几个星期渗透，尝试从Exchange Server传输EDB文件，这些文件的大小超过了100GB。最终，我尝试多次渗透他们后放弃了，因为我觉得如果继续弄，FlexiSpy会发现。

第4步：格式化FlexiSpy数据

格式化内部服务器；之后通过从SharePoint、NAS设备和其它地方拿到的账号密码登录Cloudflare，删除了他们的帐户；后登录到Rackspace，注销其服务器；并登录到他们的多个Amazon 帐户，删除了亚马逊云服务上的备份。

攻击手法还原

1. 老外通过Sonatype Nexus下载到文件，逆向文件，找到了一个密码
2. 通过拿到的密码进入登录CRM，获取到了webshell
3. 内网渗透，搞定了源代码。

本文翻译自pastebin.com/raw/Y1yf8k...，如若转载，请注明原文地址：[自称世界上最权威监控软件FlexiSpy被黑删库，怎么做到的？](#) 更多内容请关注“嘶吼专业版”——Pro4hou

信息安全

☆ 收藏 📄 分享 ⚠ 举报

👍 14


知 首发于
嘶吼RoarTalk

📝 写文章

登录

4 条评论


写下你的评论

- 

DL MARK


删裤跑路

1 天前

2 赞
- 

ggff ss


整天被吹上天的 linux 的安全性 也不过如是

1 天前
- 

gty0ng 回复 ggff ss

难道不觉得这只是对一些人来说

1 天前

查看对话
- 

shiyang

删裤跑路。

1 天前

1 赞

文章被以下专栏收录



嘶吼RoarTalk

回归最本质的信息安全。

进入专栏

推荐阅读

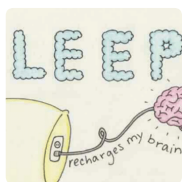


通过自动化机器学习对抗Java恶意软件

PINLogger：通过移动传感器窃取智能手机PIN码

嘶吼吼 · 1 天前

发表于 嘶吼RoarTalk



边睡边记？----睡眠中记忆的巩固

insoulter · 2 个月前 · 编辑精选

发表于 行为与认知神经科学



保罗·乔治：涅槃重生之后，他还是曾经那个他

氩的世界 · 8 天前 · 编辑精选

发表于 氩的世界