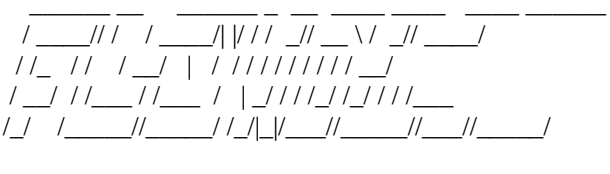
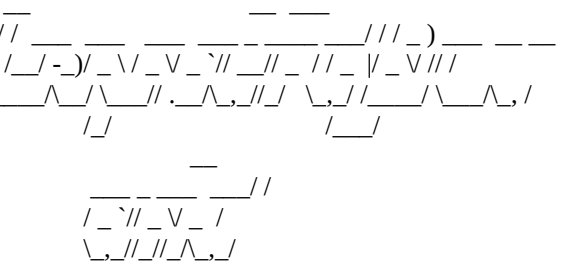
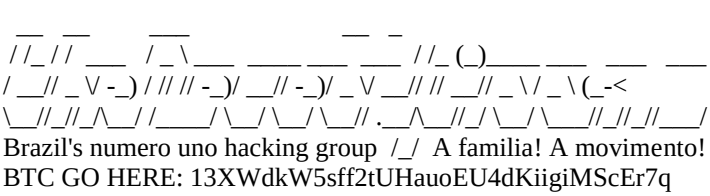


brought to you by





Brazil's numero uno hacking group /_/ A familia! A movimento!
BTC GO HERE: 13XWdkW5sff2tUHauoEU4dKiigiMScEr7q
Twitter:@fleximinx (for now)

==========

--[1: Introduction]---

Hello, all!

Since FlexiSpy burnt their entire network driving us out, we think it's time for us to release our HowTo guide for aspiring hackers, about what we did, and how you can do it, too.

This is going out there to help people learn how to hack and how to defend themselves, as is traditional after these types of hacks.

There are lots of articles out there written by other talented hackers that would serve as excellent introductions, but we'd be remiss if we didn't include Phineas Fisher's articles, which are fantastic introductions [1][2][3]. They cover things like how to stay safe and many of the basics, including many techniques we used to compromise FlexiSpy/Vervata/etc. So read them and soak them up.

[1] http://pastebin.com/raw/cRYvK4jb
[2] http://pastebin.com/raw/GPSHF04A
[3] http://pastebin.com/raw/0SNSvyjJ (the previous link, translated into Gringo)

--[2: Recon]---

Just like Phineas, our initial tactic was to run fierce against both vervata.com and flexispy.com, then do some whois lookups to enumerate the entire IP space.

You can see the output of fierce (post-hack, sadly depleted after we stole their DNS) below:

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
180.150.146.32 support.flexispy.com
75.101.157.123 test.flexispy.com
180.150.144.83 www.flexispy.com

They had several servers situated behind Cloudflare, which was a problem. Cloudflare unfortunately has a pretty effective WAF that, while nowhere near guaranteed to put an end to any fun, does almost guarantee that it'll be a lot more difficult and require a lot of configuring any automated tools to avoid setting it off. We had time, though, and looking at that list, what hostname seems immediately interesting?

Yes, that's right. It's admin.flexispy.com. Probably an admin panel.

--[3: Level 1]---

Now that we had a target, it was time to go to work.

We tried some SQL injection on the login page [1]. We didn't get anywhere, but this wasn't very surprising. It's not 2010 any more; SQL injection is a widely-known attack, and most tutorials now teach people how to not end up introducing simple vulnerabilities into software.
It still happens. You just can't rely on it.

So, out of boredom, we tried some common default credentials. admin:admin, administrator:administrator, the usual culprits. Imagine our surprise when test:test are valid.

We log in and look around. It's one user, tied to a gmail address. They have one license, which seems like a dead test device.
There's some functionality there that throws you into what appears to be the customer interface over at mobilebackup.biz using some oauth/single-sign-on functionality. There's also functionality for viewing user details, looking at license details, and editing user details like username, password, and so on.

The URL looks like this:
https://admin.flexispy.com/secure/employee/editEmployee?employeeId=1

Of course, because we're not dealing with people concerned about security, you can just change the Id=1 to Id=2. And that'll show you another user's details. And let you reset their password on the customer interface.

We played around with that for a couple of hours, and then we wrote a very simple script that just used curl to request every single ID up to

99999, which was the upper limit. We repackaged this into a nice text file and did some grepping to see if there were interesting customers (there were several), before getting bored and moving on. There's only so much you can do with customer lists, and that probably wasn't going to be enough to kill FlexiSpy.

[1] https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)

--[4: Level 2]---

Next, we decided to use nmap to scan their office ranges. We'd found these through our earlier fierce scan, and you can see them below.

58.137.119.224 - 58.137.119.239
202.183.213.64 - 202.183.213.79

There were a few SSH servers running, a Microsoft Exchange server, and some RDP, along with a few websites which mostly seemed to be hosting WildFly default pages, and one CRM instance.

Those were interesting, because it indicated there was both Linux and Windows on their internal network, which gave us options once we got inside. For now, though, we didn't have access, so we looked to see what else there was. On one server, port 8081, there appeared to be a Sonatype Nexus repository with some jar files sitting in it, which appeared to be for the command-and-control web applications. We assume that FlexiSpy put them there deliberately for resellers to take and install on their servers.

What's a group of shadowy, amorphous internet vigilantes to do but sit and spend a little bit of time reversing them? We pulled out our copies of procyon, a fantastic decompiler for Java [1] and got to work.

We pulled our several interesting utilities; the first would be their Mailchimp API key. This was fun, and let us see them sending out emails to new customers (with nice, fresh, default passwords they encouraged the customers to change). We had a look for vulnerabilities that might let us do some SQL injection (again) or exploit the API somehow, but the code didn't easily hand over any 0days to us.

What it did hand over, though, was a password, fairly simple, that looked like it might be a shared, default password: tcpip123.
We sprayed this around against the SSH servers and the WildFly servers, but didn't have much luck.

Finally, we decided to try the CRM. Amazingly, we were able to compromise an administrator account using the password we found. From there, we were able to manipulate certain module installation functionalities into, eventually, letting us get remote code execution, and uploaded our shell.

[1] https://bitbucket.org/mstrobel/procyon/wiki/Java%20Decompiler

--[5: Level 3]---

So, there we were, sitting on a server inside FlexiSpy's internal network. We weren't root, and the kernel was relatively new. We could have tried using DirtyCow [1], but many of the publicly available exploits had a high risk of frying the server, and the more reliable methods would require creating a development VM identical to the CRM server, which would take time which we were not sure we had.

We dropped a simple tool that allowed us to proxy onto the internal network, and we also placed a port scanner and an automated credential-checking tool onto the server, and started scanning quietly for

port 22, 3389, and 23.

Once we had a list of these, the first thing we did was deploy our SSH scanner against them to test for the simple combination of root:tcpip123, admin:tcpip123, and Administrator:tcpip123.

We were in luck. We had managed to compromise three of their NAS servers. These were all Linux x86-64 machines, too, which meant we could deploy our tools on them with relative ease. We backdoored the NAS servers using some code of our own devising, which we left running in-memory hidden as one of the existing services to avoid bringing any unwarranted attention down on our heads.

From there, we spent several days scouring the systems. On one, we found source code backups, on another, we found backups of home directories, HR documents, corporate files, some SSH keys, password backups, internal network diagrams, you pretty much name it, we had it. Many of these files were quite out of date, but we were able to glean the password/username combination to several servers (services:tcpip123 and services:**tcpip!23) which also had sudo privileges.

We stole SSH keys from a number of them, and tasked the Jenkins server to start pulling down all of their repositories, and send them off to a server on the internet we controlled afterwards.

We also noticed we had access to the Domain Controller for all of the Windows domains, so we dropped some malware on that, and started slowly infecting devices and pulling credentials from memory. One of those sets of credentials belonged to a member of staff in charge of IT, which gave us access to the internal SharePoint server, which is always a house of fun.

By this point, we realised that FlexiSpy didn't give a crap about security, and in order to give us as many different points of access as possible, we deployed Tor across the Linux infrastructure, setting up each server's SSHd as a Hidden Service. We siphoned out as much as we could, stopping for a few weeks to attempt to transfer the EDB files from the Exchange Server, which were over 100GB in size. Eventually, we gave up, after trying several times to exfiltrate them, because we felt if we kept going, we'd eventually cause an alert loud enough that even FlexiSpy would notice.

Once that was done, we contacted Motherboard, gave them the interesting files, and sat back with some popcorn.

[1] https://dirtycow.ninja

--[6: BONUS LEVEL]---

Wiping their servers was mostly a case of dding /dev/urandom all over all their drives, but we did have to do that across several RAID devices on their ESXi servers, which was one of the most frustrating things we've attempted.

Not even several hackers, armed with years of knowledge of UNIX, could enjoy trying to use ESXi. Eventually, after entering several long and arcane enchantments, we were able to reformat and dd over the RAID devices. The rest was fairly simple.

We used the stolen credentials from the SharePoint, NAS devices, and other places to log into Cloudflare, drop their account, then log into Rackspace, and destroy their servers there, and log into their multiple Amazon accounts, deleting as many S3 buckets of backups as we could find, before killing all of those.

Finally, we redirected their domains to Privacy International, and went on our merry way, pausing only to hijack a few twitter accounts and laugh at FlexiSpy.

--[7: Hack Back!]----------

Firstly, we'd like to dedicate this to everyone who has ever been a victim of Gamma, or FlexiSpy, or other surveillance tools.

We've stolen every a great deal of source code, going back years. We are hoping that signatures are going to be distributed, tools written to identify and remove infections, and we also hope that people will see that this industry is really out there, is worth money, and that it's terribly, terribly evil.

We're just, like, this group of guys, you know? We can hack these people, and we can expose their secrets, but it's up to everyone to make a difference.

If you have reverse-engineering skills, please, put them to use here. And not just with FlexiSpy. Take apart other malware samples, from other vendors of the same scumware.

If you have contacts in the antivirus or threat intelligence industry, push your colleagues to spend a little more time on these things.

If you're a hacker, hack back.

If you're an ordinary person, stay safe. Watch how things progress, and see what people are saying about how to detect FlexiSpy and protect yourselves. Several researchers, such as Hacker Fantastic [1], Tek [2], and Ben [3] are doing really good work.

If you're a spouseware vendor, we're coming for you. Stop, rethink your life, kill your company, and be a better person.

Otherwise, you'll be seeing us soon.

[1] https://twitter.com/hackerfantastic
[2] https://twitter.com/tenacioustek
[3] https://twitter.com/Ben_RA