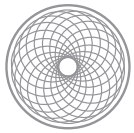

TADPO

Call of Privacy: Modern Spyware by PlayStation Network

The Anonymous Data Protection Officers

Table of Contents

Prologue

Due our objective research of the SONY PlayStation Network, we decrypted nearly 100% of the traffic transferred over proxies, http and https to and from the PSN. Just out of curiosity, not to harm anyone or anything and not like SONY may want people to see it.

As SONY calls the scene hackers "evil", we surely do not address pirates and skiddies, we wondered how SONY is treating the users' privacy and rights (remember the Music CD/DVD and USB stick rootkits). After we noticed a few badass functions they have built into the PSN/PS3 functionality, we just call it the "Call of Privacy: Modern Spyware" case.

Below we list and explain a few of the shady PSN functions and data mining stuff. And remember: EVERYONE has a right to know about YOUR OWN PRIVATE data being transferred over the networks !

Sensitive data

Even if a connection is SSL encrypted, companies are aware of the big risk behind custom CA files and it's possibilities. SONY seems not to care about those known vulnerabilities. It is a big company and a HUGE network. With huge we mean a magnitude of hundreds and even thousands: the PSN utilizes thousands of servers, handled by a very small group of administrators and quality assurance people. The IP ranges and domains of these servers are retrievable by anyone, cause this is how the Internet works ! It is all public data and information !

An example is the credit card information and the login authentification itself. Take a look at the traffic:

creditCard.paymentMethodId=CC_COMPANY&
creditCard.holderName=EXAMPLENAME&
creditCard.cardNumber=1234567890123456&
creditCard.expireYear=2012&creditCard.expireMonth=2&
creditCard.securityCode=123&
creditCard.address.address1=EXAMPLESTREET%2024%20&creditCard.address.city=EXAMPLECITY%20&
creditCard.address.province=EXAMPLEREGION%20&
creditCard.address.postalCode=12345%20

The credit card information should ALWAYS be encrypted. In ANY case. At least the security code. SONY is only relying on it's https connection. With all those CFWs spreading around, this is not secure anymore.

Same goes for the user details:

serviceid=IV0001-NPXS01001_00&
loginid=example@mail.com&
password=examplepassword&
first=true&
consoleid=EXAMPLEID123

Such sensitive data can now be captured by anyone who builds his own custom firmware with custom certificates. There are enough n00b-friendly tools by now. Means, little scriptkiddies can spread their little CFWs and phish user data.
As many of these people are using a third party DNS, they are a potential victim of phishing.
At the beginning of the PS3 launch, this user data was even transferred over http !

That being said, we continue with...

Information gathering

The PlayStation Network agreement states that SONY is allowed to collect nearly any data that is connected with your privacy.It is clear, that SONY won't tell you WHAT they are collecting in the TOS etc., as many people would never accept that TOS.

The Anonymous Data Protection Officers

A few month ago we noticed the TOS silently beeing updated without a new user agreement request. It was about that you have the right to contact a "Data Protection Offier" at SCEE, who can can give you details about what data is collected. So we phoned SCEE. Beeing forwarded to many people, it turned out that there is no so called "Data Protection Officer". Funny right? Shortly after this call, the clause was removed from the TOS.
SONY itself told us, that they do not know, what we are talking about regarding this Officer. They told us, that there was never such a position inside SONY, neither a phone number. Even the address was non existing !

Still it is an impudence what huge amounts of data they are collecting. One example is an information list which is transfered everytime you login the PSN as well as at some random time. A few short quotes:

<info category="76">TFT-TV</info><info category="77">

This is a string sent to SONY which includes your TV model. The list is long and contains a lot more like information about attached USB devices, your home network, your playtime behaviour, installed games, apps, homebrews or their so called "circumvention devices" and so on. Details about your Home network, statistics etc.

Modern user tracking we guess ;-) They try to make every PSN user transparent like a glass figurine. It seems that not only the governments are going for such plans.

The BANHammer

Now SONY is swinging the "mighty" banhammer. Some users are banned, some are only warned. But who warns SONY? Their semi-legal tactics against the enduser are a joke. We again remember their rootkits on Audio Media and USB Sticks.

Just for your interest, we quote a guy from SONY:

Thomas Hesse, President of Sony's Global Digital Business, literally says: "Most people, I think, don't even know what a rootkit is, so why should they care about it?"

This is not an urban legend -> http://www.techdirt.com/articles/20051108/0117239_F.shtml

So we could take this for an example and say: "Most people inside SONY don't even know what security is, so why should they care about it?"

If SONY cares about their customers, why are they treating them like totally douchebags ? Of course the quote does not reflect the view of the company itself, but HELL, this was not from a Jon Doe inside SONY, it was from a Department's President !

The PSN is a core feature of the PlayStation3, like OtherOS was. So why do they ban the PSN of users who LEGALLY run homebrew (not backups!) on their consoles? Just because they do not like it?

It is a fact that reversing a system is legal in most countries all over the world, and if someone who really only wants to run his own code (no, not backups!), which he legally signed and coded without any SONY libraries or documentation, would sue SONY, they would may lose.
Reverse engineering is also allowed for analysing purposes. E.g. is a software/hardware implementing/running, rootkits, spyware, malicious code, security flaws, transferring privacy data and so on.

Imagine if this wouldn't be legal, any antivirus software would brake the law ! The companies of antivurus software are reverse engineering virus code, that is NOT copyrighted by them !
So why are those companies allowed to RE and even PUBLISH their findings to the public but not people like fail0verflow etc. ?

By studying the PSN since it's launch we know it's vulnerabilities pretty good right now and unbanning consoles might be as easy as banning consoles. It is an infinite circle of "who-is-better".

The Anonymous Data Protection Officers

Sony just can not, or just don't want to, make a clear distinction between pirates&skiddies and hackers, who only want to OWN and UTILISE what they OWN and PAID for.

Hackers are responsible for creating stuff like the PC, Unix, Windows, Macs, the Internet, the WWW, AAA games etc.

Guess what IBM is calling their Cell/Hypervisor docs ? Make an educated guess: Hackers Guide.
Research Hypervisor Hackers Guide:
This document is intended for programmers who wish to discuss the code of the Research Hypervisor Project. It also attempts to introduce the hopes and dreams of the maintainers of the code that, hopefully, will make those dreams a reality.
http://www.research.ibm.com/hypervisor/HackersGuide.shtml

One last thing:
Our research is based on PUBLIC information, Hardware/Software we OWN and PAID for and the right for our PRIVACY to be PROTECTED !

- The Anonymous Data Protection Officers