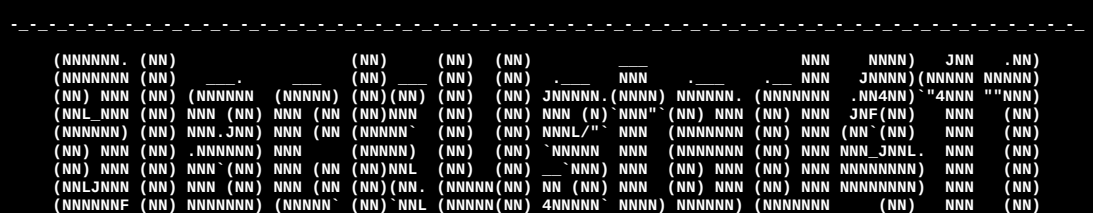


“BLACKLISTED 411 .NET”

Edition 2

11.15.2005

Table of Contents

[1] ==Introduction to Online Magazine Format==

I really do need writers in order to successfully continue the development of the online edition. As I've stated before, I believe that the online edition should be a collaboration effort supported by the community and sponsored by Blacklisted411. I don't want content to be submitted by one or two people consistently, but rather a varying variety. With this variation, BL411 .NET will be able to offer new and cutting edge views and ideas. Please don't underestimate you writing skills. If you have time, and are willing to write, please submit it to me. I am more than willing to help improve your writing style.

New Ideas:

I have some really good ideas that would really improve the quality of the online edition, but unfortunately I am unable to implement them due to previously stated problem. I'm going to go ahead and list out a few of the major ideas in hopes of getting some feedback.

Vulnerable Live CD's (Live Linux Distro with Vulnerable software thus allowing you to test your exploits in a controlled environment)
Video Tutorials (Video showing a exploit being conducted on a live vulnerable system along with some explanations)
Exploit of the month (A very detailed look at an exploit. This would include analysis of vulnerable code and some theory)
Physical Security (A look at how physical security is being implemented in the real world)

We often hear about SQL exploits and buffer overflows, but to gain a better understanding, some of us might have to actually perform or watch these exploits to fully understand them (Hence the Live CD's and Videos). The Physical Security idea would consist of looking at a few buildings and physical security methods. Of course, any pictures would be taken to protect the privacy of the Editor and the business being observed.

Any opinions on these ideas would be appreciated.

[2] ==Edition Quote==

"Those who desire to give up freedom in order to gain security, will not have, nor do they deserve, either one."

Benjamin Franklin

Editors Note: Cough Cough, "Anti-Terrorism Bill?"

[3] ==Tools==

File Recovery
File Recovery - http://www.pcinspector.de/file_recovery/uk/welcome.htm (One of my Favorite Freeware file recovery programs)
Smart Recovery - http://www.pcinspector.de/smart_media_recovery/uk/welcome.htm (Recovery program for Memory cards!)

Malware Reverse Engineering
Filemon - http://www.sysinternals.com/Utilities/Filemon.html (Monitors file actions)
Regmon - http://www.sysinternals.com/Utilities/Regmon.html (Monitors registry actions)
RootkitRevealer – http://www.sysinternals.com/Utilities/rootkitrevealer.html (Recently used to uncover XCP)

Linux Tools
RootKit Hunter - http://www.rootkit.nl/ (Used to check common programs against known good MD5 hashes)
Dsniff - http://naughty.monkey.org/~dugsong/dsniff/ - (A great little tool for sniffing out passwords, login information, and more)
Honeyd - http://www.honeyd.org/ - (Great program to keep your local script kiddies busy or at least entertain you for hours as they attempt to hack you)

[4] ==Links==
http://www.israeltorres.org – Awesome security blog from one of our authors.
http://www.seattlewireless.net/ - Very informative website on 802.11 along with wrt54g and some other APs
http://www.rootkit.com/ - Your one stop for all you rootkit needs and news

[5] ==Articles==

[a] Fun with EXIF thumbnails

Fun with EXIF thumbnails

by Unic0der

Anyone that has ever surfed the internet probably has seen censored, cropped or "Photoshopped" pictures and wondered how the original picture may have looked like (*Fig1*). In this short article I will demonstrate how you can get a glimpse onto the original picture (under certain circumstances). Requirement for this "recovery" is the existence of an embedded EXIF thumbnail. For those of you who have never heard of EXIF I will give a short introduction in the following paragraph.

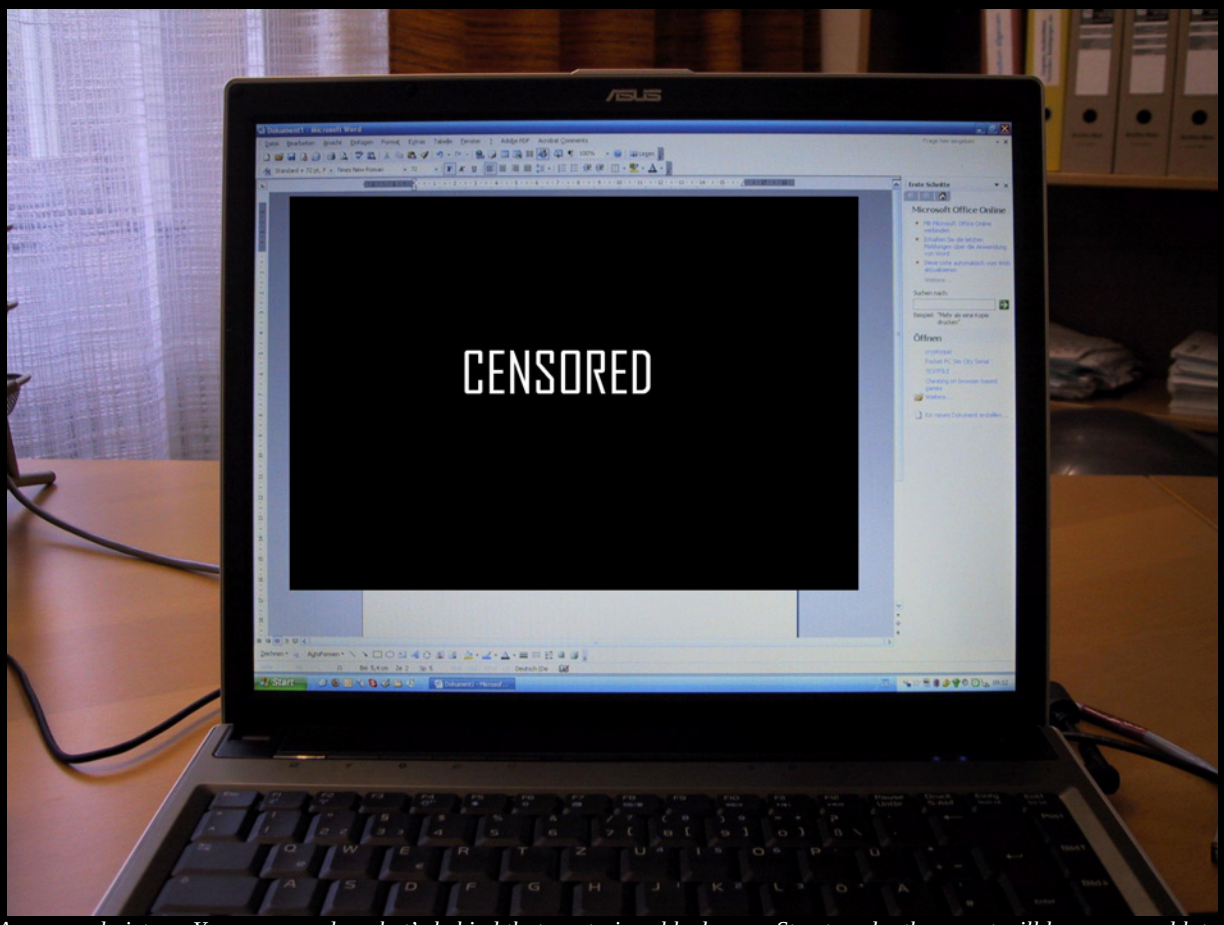


Fig 1: A censored picture. You may wonder what's behind that mysterious black area. Stay tuned – the secret will be uncovered later in this article.

What is EXIF?

EXIF (Exchangeable image file format) is a specification for the image file format used by most modern digital cameras and even some state-of-the-art camera phones. The specification uses existing file formats like JPEG or TIFF and extends them by adding a multitude of specific metadata tags covering a broad spectrum. Here is a small assortment of existing tags:

- Camera Manufacturer and Model Information
- Date and Time Information
- Camera Settings (Shutter speed, Focal length, Aperture, Orientation, …)
- Copyright Information

The latest EXIF specification written by the JEITA (Japan Electronics and Information Technology Industries Association) dated April 2002 can be downloaded from www.exif.org.

Fun with EXIF thumbnails

Another nice feature of EXIF is that it allows placing thumbnails in its header. This allows thumbs to be displayed faster because the computer doesn't have to build them from the original version each time they are requested. Unfortunately, if you edit an image and forget to

edit the thumbnail inside its EXIF header, everybody with a little know-how can still obtain the original version of the picture before the editing took place.

Let's collect some facts about EXIF thumbnails and see what we can get out of it:

- Fact is that most modern digital cameras store thumbnails in the EXIF header.
- Fact is that most expensive post 2003 image manipulation programs create and store EXIF thumbnails.
- And last but not least fact is that some cheap or old image manipulation software keeps EXIF thumbnails of the original pictures because it forgets to update them after an image was edited (Microsoft Paint provided with Windows XP is one of them).

To show you what can happen if you don't care about the thumbnails stored in the EXIF header of your images I made two photographs with my digital camera and edited them with an image manipulation program that "forgets" to update the enclosed thumbnails. Then I opened the two manipulated photos with a program called Exifer (http://www.friedemann-schmidt.com/software/exifer/) which allows viewing and editing of EXIF data, including the embedded thumbnails. Now guess what, I was able to get a glimpse of the original unedited photos – even after the editing took place. ☺ (*Fig 2*, *Fig 3*)

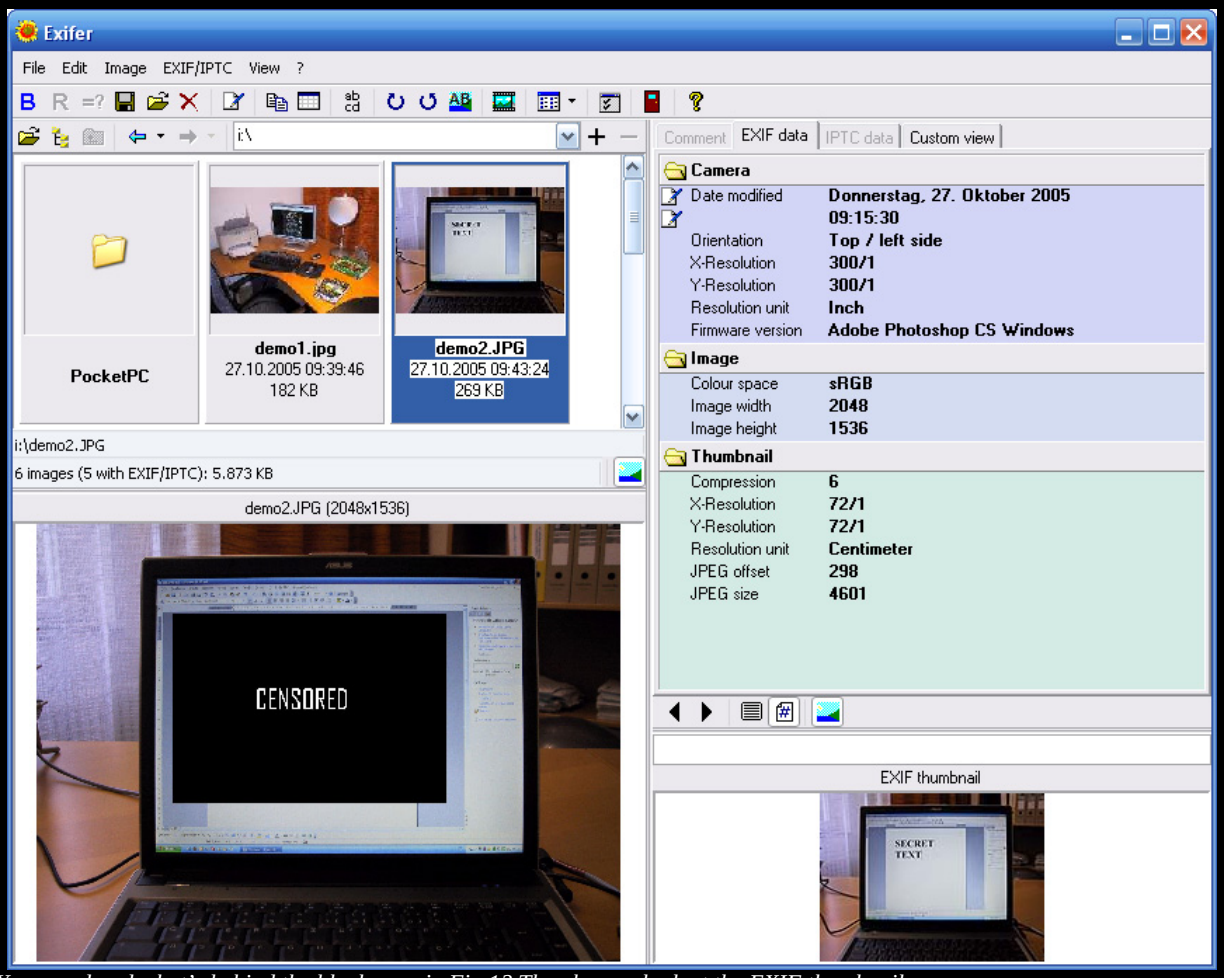


Fig 2: You wondered what's behind the black area in Fig 1? Then have a look at the EXIF thumbnail.

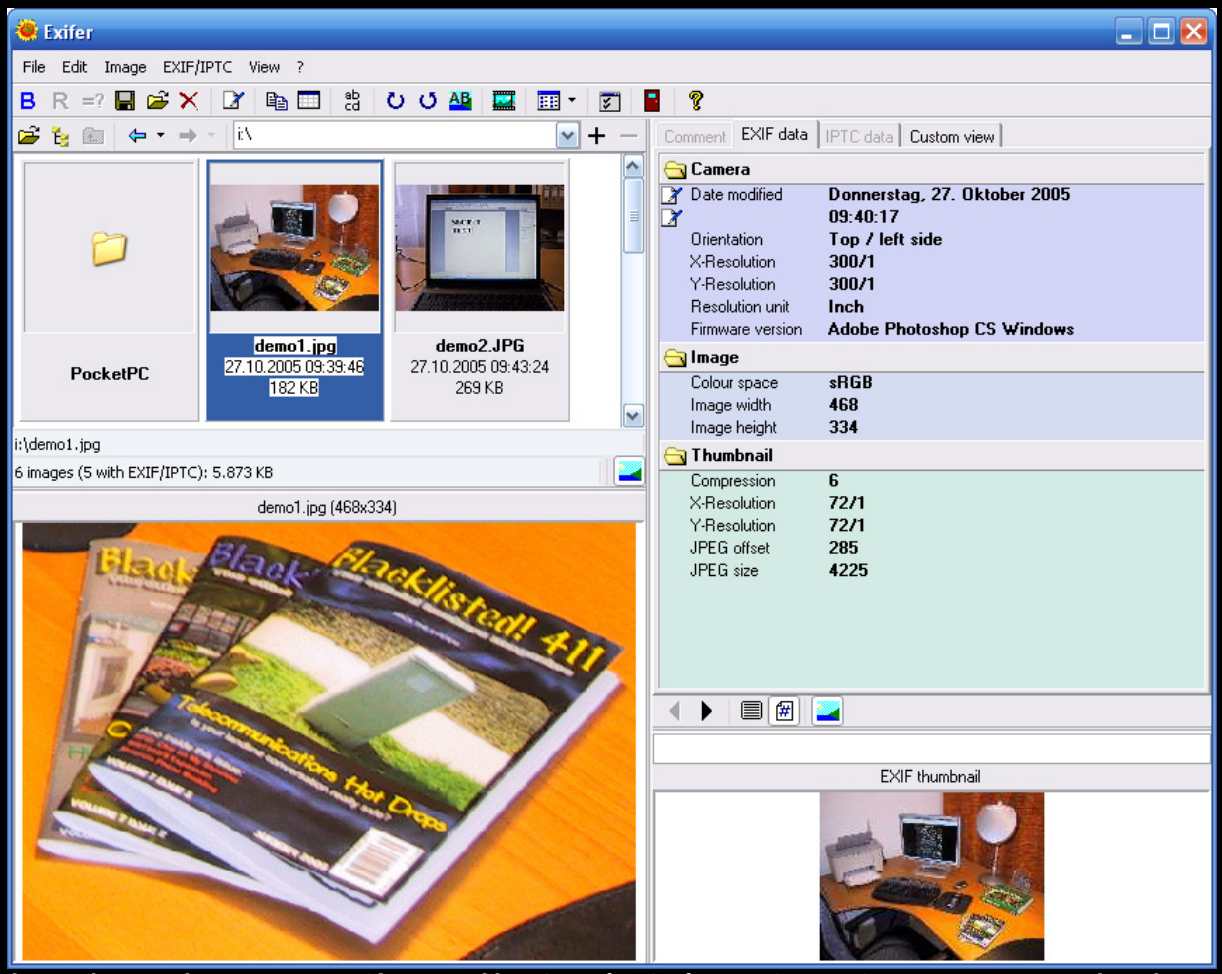


Fig 3: That can happen when you use a stupid program like Microsoft Paint for cropping your images …You can see where the picture was taken.

If you want to see another (nasty) example about what can happen when you never heard of EXIF thumbnails you should definitely have a look at the following web page:
http://wizbangblog.com/archives/000491.php

So what have you learned today? Never forget to remove or update the EXIF thumbnails trapped in your images! Otherwise folks will have fun with them. ;-)

Editors Note: This would work great for those Hacked Xbox 360 and PSP photos. Hopefully they didn't read this.

Hacking Cryptograms 101: *Rotating letters is not secure, just annoying.*

By Israel Torres < israel@israeltorres.org >

Everyday “secret” messages are being sent at the speed of the electron to people everywhere on the planet Earth. Yes, they are even sent to you and you may not even know it. No, this isn’t another paranoid theory or scheme based on the latest SETI intelligence. These cryptic whispers begin with a simple understanding of human languages. If you are still with me this far you should be good for the rest.

By nature humans are trained to read a certain way and eventually get very good at it. The more they read the better they get. The unfortunate part is that most of us stay with only one or two languages for the rest of our lives. There are others that spend a lifetime learning as many languages as they can and learn to read from left to right, from right to left, from top to bottom and from bottom to top. For those that don’t put effort into thinking outside the box may not even know this is happening right now. In fact most of the population doesn’t care. The people that do care are often categorized as hackers, terrorists, and feds. Talk about a weird party of interest. But here is why.

Let’s go with the common understanding: If you don’t see it, then it isn’t there. If it isn’t there then there is no reason to hide, therefore you can say it is hiding in plain sight. The interesting thing is that anyone that cares to read these messages can. Yes, even you. Here is how.

Let us begin with a simple and common phrase: “Hello World”
From left to right this states Hello World, as in a greeting to the world at large. You can recognize it in a sentence and even my word processor recognizes it as correctly spelled and used.

Now what happens when we reverse our phrase to: “dlroW olleH”
Whoa, my word processor doesn’t like it. You probably don’t either. At first glance it doesn’t even look like English or perhaps even any other language at all. After further analysis you may notice the capital letters and deduce it is just “Hello World” backwards.

We fix that by making them all lower case to “dlrow olleh”
Yeah at first glance it looks odd and alien to the English language. What you are saying it can’t be this easy to fool humans and computers? Well it can and it does every second of the day.

We can further obfuscate this phrase by applying any one or more implementation of simple alphabetic rotation to the phrase. Let’s give a try at rotating all the letters in the phrase one by shifting each letter once down the alphabet. For example the letter d become the letter c, l becomes k and so forth. We end up with: “ckqnv nkkdg” This is a cryptogram. It is a message that is by all definition hidden.

Chances are great that if you see this on a website or email you would just figure you didn’t have the right sort of plug-in or something wasn’t loading right and may just disregard it – especially if it was hidden in the html source of the web page you are visiting. If you are familiar with the modem days of old you would maybe even think it was line noise garbage and disregard it completely. In reality it could be a message to you, or even worse a message about you. Feds usually would be worried it was a message to a group of people indicating some type of action to be taken by the group. Do you know what your name or handle looks like backwards and rotated? Yeah, didn’t think so. Most don’t, and don’t care. Let’s just say it comes in handy if you do. Let’s move on.

Let’s throw in a little history (without the groans). If you don’t know what the USENET is you should at least understand that it is a historical method of communication among computer users to get messages to mass people around the world easily. It uses NNTP defined by RFC 977. (By the way these are all things you can google at any time – this is the online version right? (big wink)). Some messages weren’t meant to be read by all parties, or scanned by computers using filters to find information easier and faster. These messages were then encoded with a method of alphabet rotation as explained above. This then became the de facto standard of hiding communications from unintended parties. The thinking was that if you didn’t bother decoding it, you didn’t care. (Kind of how it is still like today). Rot13 is fun but it is really common sometimes too common if you know what I mean. People still wanted to hide their messages but no bother with fancy mathematical algorithms (writing them up or implementing them) so they came up with less formal implementations of how to hide ASCII data with a twist of making less common to decode unless you knew the game. Yes, knowing the game, or at least becoming familiar with it will make you a better hacker, and person in the end.

You can find cryptograms in newspapers, magazines, websites, heck even this zine has a cryptogram at the end! There are many different kinds and are really fun to wrap your brain around if you make the time. Do enough of them and you can start seeing the solutions the minute you open the page. Sometimes you get the solution sometimes you present yourself with another puzzle. There are even cryptogram books you can get at the local bookstore that are filled with all sorts of cryptograms (and their solutions on the back pages). In this case it isn’t the answer that is thrilling as so much is the way you got there. Were letters rotated or substituted, or even left out entirely to make the puzzle more cryptic and therefore required more time to solve? These brain building activities aren’t for everyone however. If you are still reading this they most likely are for you.

So you don’t have the time to sit down and shift letters around, but still want to know the solution to the cryptogram. That makes sense to me, except that I urge you to first understand how something works before using a tool to automate thinking. Substituting thought is always bad in every aspect. You can Google for cryptogram solvers out there and you will find thousands of them out there available in almost all scripting and programming languages. Let’s throw in a little coding here to give an example of finding the solution to the previous

cryptogram featured in the last edition of Blacklisted411.net's online zine. If you aren't into coding, I suggest you at least look it over to get a feel of the logic involved. If you simply refuse to even look at it skip the following example and **GOTO NO_CODING();**

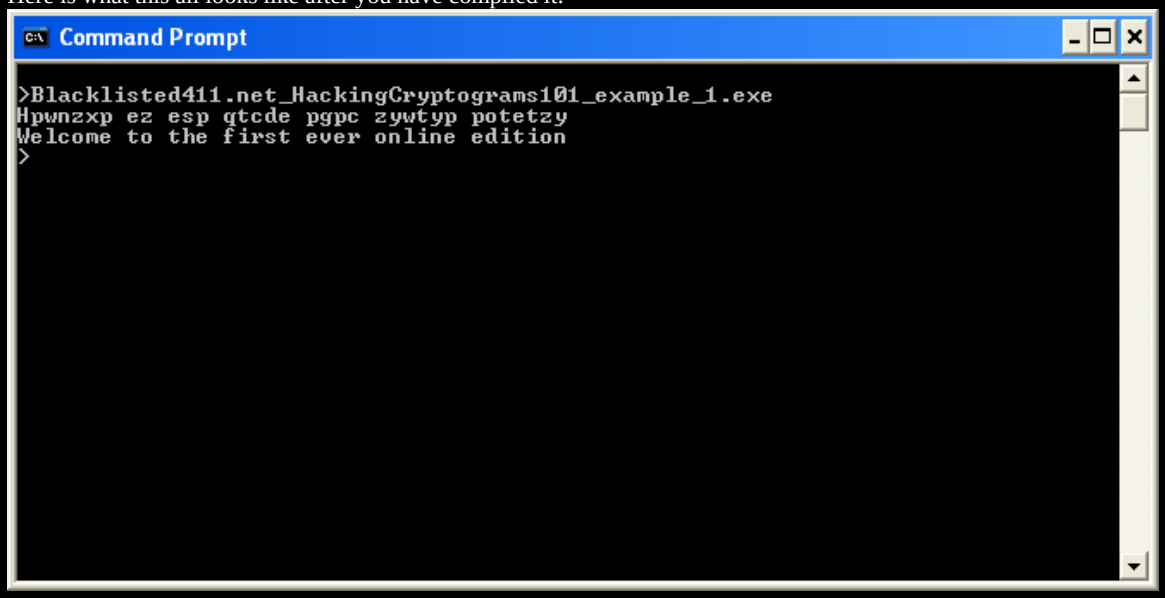
Let's take for example the last edition of the Blacklisted411.net cryptogram:
Hpwnzxp ez esp qtcde pgpc zywtyp potetzy

Here we will go throw the documented code and explain at least one approach in finding the solution to the cryptogram. Don't worry you don't have to type all this out, you can download the file from the source cited below. This is a very simple example that allows you to manually play with the idea of rotating text. Play with the values and write in your own conditions to get more out of it.

```
// Blacklisted411.net_HackingCryptograms101_example_1.cpp
// Hacking Cryptograms 101: Rotating letters is not secure, just annoying.
// By Israel Torres < israel@israeltorres.org >
//
// This example demonstrates how to brute force a suspected Caesar Cipher cryptogram.
// You may change the nrotate value from 1 to 26 if inquiring minds want to play more.
//

#include <iostream.h>
#include <string.h>

void main(int argc, char* argv[])
{
	// here we are setting up our variables for use
	char szCrypto[255]="\0";
	char szTemp[2]="\0";
	int flag_skip = 0;
	int nrotate = 11;

	// here we are copying our cryptogram into a variable
	strcpy(szCrypto,"Hpwnzxp ez esp qtcde pgpc zywtyp potetzy");

	// here we are showing what the cryptogram is to the console.
	cout << szCrypto << endl;

	// here we are finding out what the length of the cryptogram is
	int nCrypto = strlen(szCrypto);

	// here we are working for the entire length of the cryptogram
	for (int nloop = 0 ; nloop < nCrypto ; nloop++)
	{
		// here we are copying data into a variable for exclusive usage.
		szTemp[0] = szCrypto[nloop];

		// here we are comparing the value of the character to a set of ASCII conditions
		if ((int(szTemp[0]) >= 65) && (int(szTemp[0]) <= 90))
		{
			// we know that upper case letters are 26 values between 65 and 90
			// we then rotate the values accordinginly to make sure we are not exceeding the letter limit
			// and finally put the new data to the console
			cout << char(65 + (int(szTemp[0]) - 65 - nrotate + 260)%26);
			flag_skip = 1;
		}

		if ((int(szTemp[0]) >= 97) && (int(szTemp[0]) <= 122))
		{
			// we know that lower case letters are 26 values between 97 and 122
			// we then rotate the values accordinginly to make sure we are not exceeding the letter limit
			// and finally put the new data to the console
			cout << char(97 + (int(szTemp[0]) - 97 - nrotate + 260)%26);
			flag_skip = 1;
		}

		// here we are just passing anything that is not a letter directly to the console
		if (flag_skip == 0)
		{
```

```
                        cout << szTemp[0];
                }

                // here we are resetting the flag for the next time around
                flag_skip = 0;
        }
}
```

Here is what this all looks like after you have compiled it:



NO_CODING()
Once you figure out what is going on you can even build a super tool yourself to assist you with solving future cryptograms faster. Before you know it secret messages unveil themselves to you in the flash of the eye. Depending in what type of circumstance you figured out the message you may not want to let the parties know you can read them like a coloring book on a sunny day especially if they think they are getting away with the golden egg.

Keep in mind there are many variants of cryptograms and half the fun is finding out how to approach it. This particular cryptogram is using rotated text (namely Rot11) to encode the message. With each variant there is a different way to play with it to find the message so do not expect just rotating text will work all the time.

This ends the lesson for this issue. Hopefully the crypto guys back at Blacklisted411.net aren't cursing me for showing you guys how to play this game. I am sure they will make the next cryptogram a lot more difficult to play with (and probably give me more ideas to play with too) ;)

Keeping it 'rael,
Israel Torres

Here are the sources for the non-googlers out there.
http://en.wikipedia.org/wiki/Usenet
http://www.rfc-editor.org/rfc/rfc977.txt
http://dictionary.reference.com/search?q=cryptogram
http://en.wikipedia.org/wiki/ROT13

Source code can be downloaded here:
http://www.israeltorres.org/blacklisted411/Blacklisted411.net_HackingCryptograms101_example_1.cpp
MD5 hash of the source code can be validated at:
http://www.israeltorres.org/blacklisted411/Blacklisted411.net_HackingCryptograms101_example_1.cpp.md5.txt

Hacking, Privacy, and the Eternal Need for Remaining Vigilant

- by Erik Giles

The recent revelation that Sony Corporation secretly violated the privacy of their own customers when they used legally purchased music CD's to install a stealthy and difficult to remove spyware program, came as a shock to many. Most ironic in this case was the fact that this spyware was only installed on the computers of those who had legitimately purchased these CDs! Thus, only those who didn't get their music from an illegal file sharing system were subject to its limitations.

But some watchful people weren't shocked at all, and the more I thought about it, the less surprised I was as well. In a way, we might well thank Sony for this, because the incident served as a bloodless reminder of the importance of the principal of 'checks and balances', upon which the American system of government is built. Our founding fathers understood this. As Thomas Jefferson said more than 200 years ago:

"In questions of power...let no more be heard of confidence in man, but bind him down from mischief by the chains of the Constitution." --Thomas Jefferson: Kentucky Resolutions, 1798.

The man who discovered that Sony was doing this was, in his own way, acting as a 'check and balance' for Sony. Of course I am not saying that Sony has the same kind or amount of power that the government does, but clearly, they and other large companies do have enough power to assume some measure of control of individuals computers. Without this 'check and balance', which came from a private citizen, what would be next? Would our PC's eventually become nothing more than the marketing and customer tracking platforms, in effect sales robots, for the world's biggest corporations?

This is one of the ways I think that the hacking community, and their colleagues who work in computer security, can really serve society. By remaining watchful and acting as a last-ditch 'check and balance' in cyberspace, all our freedoms can remain protected. It's one of the reasons I find the subject of hacking so interesting, and the reason I support Blacklisted 411.

We really need this watchfulness to continue. In cyberspace, who else is really watching? I know that the FBI has a cyber crime function, but compared to the rest of the world outside of cyberspace, law enforcement efforts and consumer protection efforts are limited. Could your local or state police force do anything about this program that Sony made? Do they have the will or the skill to look for it? Certainly, nearly all of them do not.

Right now, I think that cyberspace is very much like the old 'wild west', in that it's a very new world, and like the ranchers and cattlemen of old, sometimes hackers and others have to assume some of the responsibility of policing this space. An example of this is the Spam vampire program that Goldfinger recently wrote of. Lacking a fast and effective means for law enforcement to track down and arresting spammers, we can use vigilante cyber tactics to police them ourselves.

This leads me to another topic, the Real ID Act of 2005. Many people are very concerned about this new piece of legislation and it's impact on privacy and human rights, particularly for immigrants and asylum seekers. Before the Sony incident reminded me of the never ending need for 'checks and balances', I would have considered these concerns to be valid in an abstract sense, but in practice, I would have asked, what bad could really come of it?

In light of the recent terror arrests in Australia, where a group of Islamists were discovered to be allegedly probing the security of a nuclear plant, I can understand the need to have a legal method to cut through all the bureaucracy to address terrorists who use our own immigration laws against us. We can't afford to be wrong. If a nuclear plant were ever melted down by a terror cell, the devastation would be unimaginable. The Chernobyl accident made thousands of miles of Russian land uninhabitable.

Our immigration infrastructure is clearly broken; the bureaucracy does not seem to be able to handle the millions of immigrants here from Mexico and other countries. And it's natural for Americans to expect reasonable border control. It's probably just as easy for an illegal immigrant to pass through the border of Mexico into Texas as it is for him to pass through the border of Virginia into North Carolina.

But in my opinion, the Real ID Act does little to address the problems in the immigration system. Many believe that the biggest problem with this legislation is that it allows the Department of Homeland Security to 'waive all legal requirements' in dealing with an illegal alien. This would concern Thomas Jefferson, because puts an awful lot of power into the hands of one person (the Secretary of the Department of Homeland Security), but at least they amended the legislation to include a judicial review, within a 60 day window, so there is a check and balance built into it. Even so, the Sony incident reminds us we must continue to be watchful of our own government, even as we continue in our efforts to prevent the unimaginable.

In closing, as we make legislation which may help us combat terrorism, the Sony incident should serve as a reminder to be watchful. I will never again make the mistake of dismissing the concerns of the watchful as the ravings of the paranoid who think everything is a government plot to enslave us all. In our efforts to prevent large scale terror attacks, and keep enemies from easily infiltrating our country, we must remain eternally watchful of our own government. As Jefferson said:

"I sincerely wish we could see our government so secured as to depend less on the character of the person in whose hands it is trusted. Bad men will sometimes get in and with such an immense patronage may make great progress in corrupting the public mind and principles. This is a subject with which wisdom and patriotism should be occupied." --Thomas Jefferson to Moses Robinson, 1801.

Links and sources:
http://www.pfaw.org/pfaw/general/default.aspx?oid=17851
http://etext.virginia.edu/jefferson/quotations/jeff4.htm
http://www.techworld.com/security/features/index.cfm?featureid=1931
http://www.smarthouse.com.au/Entertainment/Industry/?article=/Entertainment/Industry/News/Q7P7L4N2
http://www.cnn.com/2005/WORLD/asiapcf/11/07/australia.terror/
http://www.mipt.org/terrorism-news.asp?feed=Nuclear%20Terrorism

Editors Note: Wait, everything isn't a government plot?? (Just kidding) I do agree. One of my greatest fears is the implication of the Real ID system for use on the internet. Just imagine "logging on" to some government mainframe before accessing the internet. Of course the politicians would argue "You have to show an I.D. when you enter a bar, or caught speeding. Why shouldn't the Internet be any different?" – And to them I would say, "What pocket are you in?"

[6] ==In the News==

Sony's Emulation of Big Brother

By Dr. Fibes

Sony has caused quite a uproar lately with their "anti-piracy technology". This so called technology was nothing more than a resident program that was always running on your computer. It would report in to Sony when it felt like it. It would refuse to let you copy songs onto your IPod. Best of all they didn't even tell you they were installing it.

Yesterday Sony said that they were going to discontinue using their "XCP" technology as a precautionary measure. "We also intend to re-examine all aspects of our content protection initiative to be sure that it continues to meet our goals of security and ease of consumer use," Sony said in a statement.

That was after weeks of criticism. But the thing that really killed it was the virus that was discovered on Thursday by a British anti-virus firm, Sophos. Some malware, downloaded as an email attachment, would hide out amongst the Sony "spyware" stuff. At least that's what many people thought of the Sony "copy protection" ah, software, that it was spyware.

It certainly acted like spyware. It was able to cloak itself and become invisible using what the developer, First 4 Internet, called DRM rootkit technology. This is the same method employed by many malware hackers, no big technology secret here. Hackers exploited this advantage by naming their files with similar names as the Sony cloaked files. The Black Hats discovered that this way they too would be invisible. Soon many of these malwares were being discovered.

How ironic that the Black Hat hackers by utilizing this strength (weakness?) in Sony's software, contribute to bringing down this very nasty overbearing media strong-arm tactic upon the general populace.

But that wasn't the only negative feelings generated by this software. Leading antivirus companies updated their data files earlier this week to detect the Sony-Baloney ware. They would then kill it and refuse to allow it to be reinstalled. I think that demonstrates just about everybodys attitude about this intrusion. Computer experts had been warning for over one week that the poorly written software was a major security hazard, for just the reasons that popped up just a few days ago.

It was another one of those difficult to remove pieces of software. And they would use it to transmit who knows what whenever they chose. I really don't want anything like that on my machine. They certainly have the right to protect their product, but not sipping on the power of my machine doing it. Or clandestinely installing SPY software on my computer used to spy on ME. Hire some Private Eyes or something.

It had many great features I haven't mentioned. For example, it installed itself as soon as someone put the CD into your computer. It then keeps track of your usage of their product by spending your computer time watching you and reporting this and who knows what data back to Sony. It changes the configuration of your system so that all CD drive data must pass through the DRM rootkit technology before being

played. People who have tried removing the software or changing the settings have found they have made their CD drive useless because the data stream is interrupted by way of control of the now non-functioning Sony software.

Another big plus was that fact that after it was installed, it would only allow your CD to playback with Sony software.

It was discriminatory. You could play the CD all you wanted with no problem on an ordinary CD player. Same with a Mac. Don't Macs have CD burners too?

The consumer and marketplace have spoken on Sony's unfortunate attempt to monopolize some of YOUR computer's time and have your computer spy on you. Forcing you to allow it to transmit whatever they want, whenever they want from your machine, or you just don't play your CD on your computer. And all without even telling you.

They (Sony) blast their media into my house. Now they want to set up my computer like Big Brother, checking in, but you never know when he's looking, or what he's looking at. And all the while slowing my machine down while it takes care of it's business. And it's set up to do that every time I start my computer, so it's always running.

The Chief Software Architect at Winternals Software, Mark Russinovich discovered the hidden copy-protection "technology" on Holloween. He was testing a new winternals product, RootkitRevealer, and discovered that his machine had a rootkit malware program running. This greatly surprised him as he was very cautious about what was installed on his machine. Sony tried to pull the silent treatment on the subject, but it just wouldn't go away. Russinovich stated yesterday concurrently with Sony's announcement about discontinuing use of the rootkit that "This is a step they should have taken immediately."

Sony produced a patch that removed the program's ability to avoid detection after Russinovich criticized them. Sony also gave easier access to instructions on completely removing the program. However you can no longer listen to your CD on your computer. And their new found second thoughts over not using the "technology" are temporary, what does that mean? Until the big stink has blown over in the news and they can quietly begin loading it on computers again? Probably.

The Italian ALCEI-EFI, equivalent to the Electronic Frontier Foundation has filed suit against Sony charging that the DRM is a virus. They have also asked the Italian Police to investigate criminal charges. The (American) Electronic Frontier Foundation is currently collecting up stories, they are considering a class action suit against Sony for this software.

This was a tremendous public relations blunder for Sony. Hopefully they'll just do the right thing and throw in the towel on DRM. Nobody likes it, nobody wants it and they now have egg on face big time. And probably some hefty court losses in the future as well.

The stranglehold of the major corporations continues to grow and grow. New technology has contributed to that in a big way. Starting with computers themselves. Even newer technology is coming along constantly as well. RFID tags are going to revolutionize many things, many not for the better.

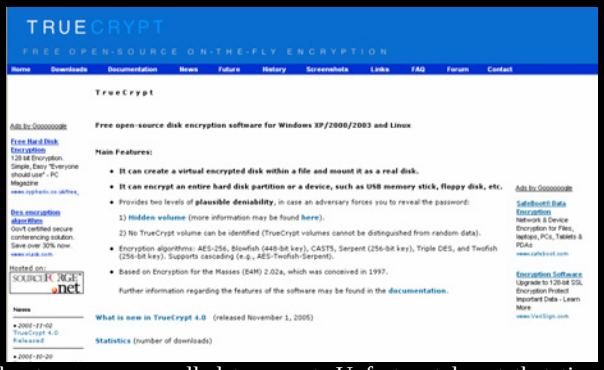
For sure though, they can't have my machine. It's like my castle, my cyber home and I should be able to decide who enters and goes, just like at my actual home. Don't tell me I have to install spyware to play some media that I PURCHASED. I don't want that junk on my machine.

[7] ==Product/Service Reviews==

DD-WRT: Quick Update

If you recently read my article about hacking the Linksys WRT54G/S, you probably are familiar with the DD-WRT firmware. As I mentioned before, DD-WRT is by far one of the best firmware images available. Thanks to BrainSlayer, we now have a feature that hasn't been offered in ANY consumer product on the current market. To my knowledge, the only other AP that offers this ability is the Cisco Aironet Access Points (Which are rather expensive). The ability I'm referring to is the ability to create multiple SSIDs . And these aren't just aliased SSIDs. These are fully featured SSIDs, meaning that you could make one SSID which is on its own VLAN for your hotspot, and have your laptop on a totally different SSID which would be aliased on another VLAN. Also, all SSIDs support their own separate encryption method (WPA, WEP, WPA2, RADIUS, ETC). Unfortunately, this feature is in the early Alpha stage (Public Alpha). When development is finished, DD-WRT will offer 16 simultaneous SSIDs. I HIGHLY suggest you closely watch the developments and consider purchasing a WRT54GS if your in need of a router/access point. Now I know it might be tempting to purchase one of the Pre-802.11N routers/access points, but I would highly encourage you to wait a little bit longer. Nothing would be worse than purchasing a Linksys SRX router only to find out that newer 802.11N network cards don't support the proprietary SRX technology, thus forcing you to upgrade.

TrueCrypt: Revisited



In the last online edition we talked about a program called truecrypt. Unfortunately, at that time, the program was built for Windows exclusively. I am very happy to announce the release of a new version which includes support for Linux. Also, with the release of version 4.0, we now have the option of using keyfiles. With the combination of a password, we now have two-factor authentication (Authentication = What you have + What you know). Support for x86 has also been added. The only improvements I would like to see in a future release, is the ability to encrypt keyfiles with a additional password (Since keyfiles appear to be stored in clear-text), support for RSA dongles, and biometric device support (Fingerprint, Retina, etc). A full list of improvements can be found at http://www.truecrypt.org/history.php .

NOTE: Next edition will have more tool reviews. Had a few technical problems.

[8] ==Cryptogram==

I was going to write an explanation about how to solve the last cryptogram, but since Israel Torres already did an excellent job of explaining how to break it, Ill refrain from restating the solutions.
This cryptogram should be relatively simple. No functions (Such as XOR, AND, etc).

Clues – It's a combination of a substitution cipher along with another trick (Which is done in binary).

000100100101110000011001011001011010000100100011100010110011100 11

Special Thanks to Unic0der for the lifesaving cryptogram.

[9] ==Favorite Photo==

Pictures like this really scare me. Nice little Photoshop trick though. Unfortunately for us, this may become a reality someday. Just imagine someone breaking your door down and yelling "Police, Drop your MP3 Player and move away from you keyboard".

[10] ==Credits==

Chief Editor: Zachary Blackstone

Online Edition Editor: Ustler

Authors: Unic0der, Dr. Fibes, Erik Giles, Israel Torres