

AntiOnline

Maximum Security for a Connected World



Table of Contents

Editorial
by MsMittensp. 3

What OS is the Best?
By Pooh Sun Tzup. 4

Cyber-monoculturism: A Discourse on
Digital Diversity
by <0p. 6

An analysis of the internet community
by Ennisp. 8

Honeypots Revisited
by alpha p. 10

Anonymizer Privacy Manager: Doing what exactly?
by MsMittens p. 13

MsMittens' Editorial

I got a treat today. A colleague had asked a representative from Iridian to visit us. They make Iris recognition hardware/software access controls. It was really interesting and eye-opening (pardon the pun). This technology ensures that the identified person is in fact that person. You can't fake it (no popping out eyeballs and using those a la Minority Report). Disease doesn't affect the iris. Even twins don't have same irises (although their DNA would be identical). In fact, the only thing holding it back was cost and general population acceptance.

Now the cost issue I'll set aside but it's the general population acceptance that I think is the bigger challenge. That is the challenge for security in general. I still hear today that ominous phrase "I don't have anything worth stealing". *gulp*. It's Murphy's Law that they will be hit with the next Outlook virus and will populate my mail box with more ingenious ways to make my body parts bigger with a simple pill pop. Yip. Eee.

Sigh. I suppose, as has been discussed on the boards recently, that people like this keep us employed. But I wonder sometimes how bad society can get. I watched the new updated TV mini-series for Battlestar Galatica (and am a regular watcher of Enterprise). Anyone notice how perfect their computers are? No security flaws. No bugs. No vulnerabilities. Who the heck programs these things anyways? Asminov's robots?

Not to be pessimistic... well, ok. I'll be pessimistic. Society sucks at times. Heck, half my security lists are now being flooded with virus messages (mostly Netsky and MyDoom these days). The other half of the lists are schmucks sending messages "Is this another phishing attempt?". D'uh! Look at the source! Geez. Maybe it's not the stupid general population I need to worry about but rather the inept security admin that's afraid to take a chance and research things on his/her own. Why is that so hard to learn about things?

meh

At least here, we're open to this (most of the time — *grin*). This issue does have the desire to learn and to teach. Pooh reminds us that OSes come in all shapes and sizes, and that perhaps the administrator has more to do with a secure OS than the OS itself. Ennis teaches us one of the important factors of AO — the community it represents. <o (lessthanzero) looks at the issue of cyber-monoculturism. Perhaps there is too much dependence on one answer to our security problems? alpha takes a good overview of honeypots. And I close with an article long promise to Tedob1 (you can have more data, Tedob1, if you want) on the privacy tool, Anonymizer. I have suspicions as to how it works... or does it??

I hope you enjoy this issue, albeit a bit small. Quality not quantity is important! I do put out a general call for future articles. Our next deadline will be **May 24, 2003**.

Enjoy!

What OS is the Best?

By Pooh Sun Tzu

Many times throughout my security years of both teaching and learning, I find that at least once every few months someone asks me "What Operating system is the best?" or "What Operating System is better/more secure/less secure/faster/cooler/easier to hack with". To each I've given the same answer and thoughts that I shall share here, as I merely feel it is time to do so. Do not expect a list of Operating Systems, nor expect biased opinions in this post. I want to offer insight to one of the most valuable peices of wisdom one can have in the security business.

The answer to the question of "What Operating system is the best?" is quite simple:

Each and every Operating System is capable of preforming and responding just as well as the next.

That's correct. Now, set aside differences, stereotypes, and your past knowledge for a moment, please. And allow me to share my thoughts with you. Here is a quote I want you to never forget, something that I have never forgotten once my mentor taught me: The OS is only as good as the Admin, and the OS can never make up for a bad admin. A veteran of a Windows Operating System can lock up any windows distro in a heartbeat, more secure than an SELinux kernel on OpenBSD running tripwire, by using their knowledge and experience of windows. A newbie of OpenBSD, however, can make it as insecure as an unfirewalled, unupdated, windows 95 distrobution. Think about this for a second, if you will for me. An Operating System can have all sorts of default safeguards and built in security functions, plus unlimited tools at the admins disposal to secure it with. But, if the admin is not familiar with that Operating System, whichever one he is using, then it is all useless to him.

There is an old adagio: "A firewall is no good if you do not know how to configure it and read the logfiles"

It holds true to Operating System security, upkeep, and usage. While so many people may argue about "LINUX IS TEH GOD!!!111 windows is INSECURE omfg!!!11FIVE" and about "LINUX IS 31337 :P yuh rght", they are forgetting how important it is to learn and master both. A good security admin doesn't just brag and become a fanboy about their OS, they dig deep into the core of it to discover how they can tweak and modify it in each and every way, so that when the time comes to modify it, they already know how. Be it mastering the Registry in Windows, which by the way is actually every single module configuration that directly links into the Windows kernel at your finger tips. Or be it learning how to use KDE, even if your past experience with it was shotty. Why is it so important to focus deeply onto your OS of choice? I'll tell you why.

When an admin is comfortable with their OS, they can begin to actually learn. Thus is the root of my entire answer. Despite what OS you are on, find the one you are most comfortable with and master it. Because when you master it, nothing can penetrate you, and you are quick to

both problem solving and prevention. Forget the stereotypes of Windows not being "leet enough", or Linux being only for "geeks". Find what you like best, and master it. This leaves me to the last part of my post here, dear friends.

When you have mastered an OS, truely knowing it inside and out, then move onto a new one. A completely different one. If you mastered Gentoo Linux to the bone, then give Windows XP a shot. Remember, shove aside stereotypes and previous bad experiences and use that to drive you even harder to make it WORK like it should. With equal knowledge of multiple operating systems, not only does that widen your "hire me" contract, but it helps build general knowledge about computers, period.

So I say again, and I leave you with this: Each and every OS is just as good as the next, and can do the same thing in different ways. The key and the challenge is finding the OS you are most comfortable with, blowing off the windows and linux zealots that will stereotype you, and actually learning. Remember, there isn't a single thing that Linux can do that I can't make Windows do just as good, and there isn't a single thing that Windows can do, that I can't make Linux do just as good.

Take care and be well.

Become famous! Send an article into the AONewsletter!!

We want articles on security tools, "hacking" tools, ideas, rants, raves, reviews, etc. Also, if you want to promote your website, send me a little note.

Send a note to msmittens@msmittens.com with AONewsletter in the subject line or send a private message to my AO account, MsMittens.

Next deadline: May 24, 2003

Cyber-monoculturism: A Discourse on Digital Diversity

by <0

The concept of a cyber-monoculture was first introduced in CyberInsecurity (Bace, Geer, Gurman, et al. 2003). The CyberInsecurity article is quite an interesting read and I would recommend it to anyone who might be curious about information security theory as the contents of the article are indeed apropos to current information security ideology. And though the article poignantly covers a breadth of issues regarding security, I would like to focus on the notion of cyber-monoculturism exclusively. Cyber-monocultures do exist (and exist outside of the MS realm despite the innuendos presented in the article) and deserve our attention in terms of discussion and analysis. This, then, is the goal of this document; to precisely explain what a monoculture of the cyber-variety is, what possible issues arise when a monoculture exists, and finally what can be done to mitigate these possible issues.

This term monoculture is borrowed directly from agricultural science, where the term is applied to the practice of planting a single species of plant (crop). Basically, it is a commentary on the lack of biodiversity in a (eco) system and is most commonly employed in the pejorative. The application of monoculturism to the digital world is a straightforward analogy- meaning, a cyber-monoculture can be defined as a component's existence in a computing system to a degree of exclusivity. The authors of CyberInsecurity specifically highlight the Windows operating system, but I do not believe we can take the risk of confining our definition to only that specific example. Whilst the supposition of Microsoft's cyber-monoculture may be accurate, the business practices such as user-lock-in via licensing agreements fact-based, this example is no more all inclusive than citing corn as the agri-monoculture. Indeed, this "degree of exclusivity" applies to any software or hardware mind you, but especially so to critical applications and operating systems that organizations' business models thrive upon. Could we include Cisco in this discussion? Sure. BIND? Most definitely. Again, it is the degree of exclusivity that defines a cyber-monoculture, not brand or manufacturer. So, we must objectively ask ourselves though, what possible perils are introduced when a cyber-monoculture develops?

Once again, the perils of cyber-monoculture mirror those in the agri-monocultural analogy. In the agricultural domain, monocultures are highly susceptible to pestilence and insect plagues. Naturally, cyber-monocultures are exposed to analogous risks. The lack of (cyber) diversity in a cyber-monoculture permits digital virii and/or worms to reach pandemic levels in very quick fashion due to the existence of susceptibility in all hosts. As well, the high-level of similarity between hosts or systems in a cyber-monoculture can create a windfall effect during coordinated exploitation (whether the attack is software based or human based- e.g., virii or human intruder). The authors of CyberInsecurity refer this phenomenon as "cascading failure"; the notion being much akin to a domino effect whereby failure(s) rapidly spread throughout the cyber-monoculture. We could easily summarize here by stating that over-specialization breeds in weakness. Furthermore, the very nature of (cyber) monocultures prevents the competition that is necessary in a system for evolution to continue. Agri-monocultures are well known for this property whereby pollination becomes limited due to the lack of

diversity and predator-prey dynamics are disrupted. This too is evidenced in cyber-monocultures in the form of monopoly and cessation of innovation and competitive alternatives through litigation. Indeed, faced with such stark realizations, certainly we must explore avenues to correct and/or mitigate these pitfalls.

Foremost, we must dissimulate ourselves of the notion that governmental dogma will resolve and/or mitigate the perils of cyber-monocultures. The forced dissection of simulated (yes, simulated) monopolies into smaller competitive factions does nothing to move the argument forward. Rather, the issue is avoided and the risk sown across a wider platform. The introduction of competitive species (or hardware or software, etc.) only serves to increase risk, to increase management. Again, the perils of cybermonoculturalism are not mitigated, merely hidden by a simulacrum of security simulation mentioned above. So, where do we begin on our quest to solve this issue?

First, we must collectively accept responsibility for the individual systems/hosts that comprise the monocultures that we participate in. I would posit that flaws are not inherited, moreover they are permitted. Meaning, the risk is ours to allow or mitigate. Doing nothing is akin to allowing; acting is akin to mitigation. Secondly, we must become aware. Causality encases this entire discussion and is more immediately perceptible in a monoculture. The effects of our causes are more butterfly-effect-like than cascading-failure-like; this supposition demands that we become aware not only of our vulnerabilities, but also aware of what possible vectors exist that may exploit these weaknesses. Passiveness and neutrality do not belong in this discussion, as it is the pro-active that succeeds (both in exploitation and defense of exploitation). Thirdly, we must act responsibly through acknowledgment of vulnerabilities, analysis of possible safeguards and countermeasures, and pro-activity in both applying these controls as well as requesting (or searching for..) new controls when those in existence are not adequate. Idleness and reliance upon third-parties (i.e., manufactures and vendors) contributes very little to the resolution. It is initiative and drive that will succeed in mitigation of the weaknesses that monocultures breed.

Indeed, monocultures surround us. Though the term has its roots in agriculture it can be extended now to the digital, online world and well beyond. Because of the high degree of exclusivity that (cyber) monocultures are part and parcel of, weaknesses develop. These can run the gamut from monopolistic business practices, to cascading failure during attack, to the death of innovation and evolution themselves. Yet, there is hope lurking beyond the binary vistas. Once we accept responsibility for our systems, once we become aware of the vulnerabilities and the methods to mitigate/resolve them, and then take a pro-active approach in the application of this new found awareness, I believe we will have taken several large steps forward in eliminating the risk(s) inherit to living in the modern, cyber-monoculturistic society.

An analysis of the internet community

by Ennis

It's has been a long time since I first came across AntiOnline, September 2001 in fact. The place has changed but it is still Generally the same, in fact I have come to realise that most internet communities follow a general pattern. And since my Studies have taken me into a new direction from computer security I wanted to give something back to the internet community that gave me the greatest pleasure to be a part of.

The most important component of any internet community is the sense of belonging among dedicated members, the usual faces that are guaranteed to post every day be it Christmas day to post their newly acquired box or even New Years eve in a drunken stupor. AntiOnline has always had a general core of dedicated users, when I joined the member names that stick with me are Negative, Souleman and MsMittens although many more begin to enter my mind with the more effort I put in. These people have put more into this tiny piece of cyberspace than one generally expects from its full time staff be it the elusive JP or the moguls that be in JupMedia. In fact some of these members have indeed become members of the site earning a nifty paypacket from something I have always enjoyed doing for free. The difference is the do more than I could ever bring myself to do, daily pruning of the forum and the mundane tasks associated with it Such are our deserving moderators.

There is also among those grey forums the makings of much amusement for anybody who has any kind of interest on how people will act anonymously. Although the standards of trolling have seriously declined since the days of Oblio and Chemical there is nothing more likely to pass a dull hour than watching the reactions of people to what is essentially a screenname. That is where internet forums get interesting to people like me, the amateur psychologist, it is a playground for people's created identities and thus provides a little insight even if the aim of the forums is simply to provide answers for the security inept.

I have since wondered what the appeal of these forums are and whether it is somehow related to this kind of alternate identity. Forgive me if I sound pretentious or seem to be taking something as simple as a forum serious but my mind began to wander and I felt compelled to offer something to the illustrious newsletter since my rate of tutorials for AntiOnline has deteriorated to nil. I think I have done my fair share for AntiOnline, the Newsletter was my idea, I produced the first edition but if you have a look at it the superiority of MsMittens for the job is quite clear. I also feel I have produced a good quantity of tutorials especially those aimed at newer members, quality of course is judged by the reader. Now since I will no longer be writing tutorials or contributing to AntiOnline anymore in any real sense I want to offer this little 'insight' of my own. I think this is justification.

Now for those of you who don't appreciate some of the improvements of AntiOnline here is a list of them which I hope makes some new users aware of the abilities of AO:

AntiPoints - Like them or not antipoints are what make AO unique. Self moderating of members by members is something you wont find anywhere else. For all the criticisms

antipoints are a feature that I believe have done nothing but good for AntiOnline. Although the days of no antipoints didnt seem to have as many problems it was a hassle waiting for JP to ban a member whilst they proceeded to post rubbish continually.

Conference Rooms- Underutilized resource that allows users to create their own little rooms for debates.

Security/Non Security Tutorials - An amazing resource not to be matched eslewhere plus I am pretty sure that in a few years AO tutorials will begin to find their way all over the net such is its nature but I think I would be proud of that, sincerist form of flattery and all that.

Addicts Forum- We are plotting our takeover in there, dont tell Jup...;)

There is so much more but I feel that we need to highlight just what kind of kick ass forum we have at our disposal and to keep this mind as new members and oldies strive forward to make it even better. mIRC issomething that has changed since my first year or so here, the loss of AO IRC is something I still believe has caused a deterioration at AntiOnline. Although many good efforts have been made to make a new IRC community it hasn't got the same buzz or appeal as the good old AntiOnline IRC.

Anyway I feel I have ranted on enough and I have just written this over the last half hour but if I start rewriting or editing I feel it might turn into a monster so I'll finish here. I just wanted to leave something at AntiOnline, a message about how great a tool it is and how we should all use it to its full potential. Maybe such a message is a waste of time and nobody will listen but sometimes a little nudge can change things.

So thank you all, need I name you? You know who you are and for those I haven't talked to in a while I am sorry but maybe one day I'll pot into IRC under my alternate guise which some of you may know, others not.

Become famous! Send an article into the AONewsletter!!

We want articles on security tools, "hacking" tools, ideas, rants, raves, reviews, etc.

Send a note to msmittens@msmittens.com with AONewsletter in the subject line or send a private message to my AO account, MsMittens.

Next deadline: May 24, 2003

Honeypots Revisited

by alpha

alpha_betarian@yahoo.com

Originally, this was written as a response to an article in 2600 that I saw and didn't think did justice to honeypots. Upon closer inspection, I decided that, judging by the way it was written, it was more suitable for the AntiOnline crowd. I'll try and grace 2600 with a different article. Most of my information for this little tutorial came from a book entitled, "Honeypots: Tracking Hackers" by Lance Spitzner. Those interested in the honeypot field should check it out as it is an excellent, excellent book filled with a wealth of information. It's also a great place to start out from.

What exactly is a honeypot you ask?? According to Spitzner, it is "a security resource whose value lies in being probed, attacked or compromised (p. 40)." In other words, it's a machine you want to be attacked so you may look over the logs, or any other data generated by the attack, in an attempt to learn exactly how the attacker got in and what techniques he/she may have used. Now, there are many different kinds and classifications of honeypots, but they all have at least one common trait. Honeypots have no production value so no communication should be taking place with them. Therefore, anything that does go their way, should be questioned. Most likely, it's a scan, probe or attack of some sort. It may also be possible to install a packet sniffer on the physical honeypot machine in order to see the actual keystrokes of the attacker. If it is, then not only would you know that something is happening, you'd know exactly what. I'm not totally sure on that though.

Honeypots are grouped by the amount of interaction they allow the attacker to have, either low, high, or medium. Low interaction honeypots are generally port listeners which occasionally emulate, but do not provide, actual services. Usually, there is little risk, both to other networks and the network on which the honeypot resides since there is nothing for the attacker to truly interact with, just a script pretending to be an actual service.

High-interaction honeypots tend to offer actual operating systems for the attacker to interact with. As you can see, the amount of risk high-interaction honeypots produces is great, so they are most usually in some sort of controlled environment. Usually, this environment is behind a firewall which allows attackers to compromise a honeypot sitting behind it, but does not allow the attacker to attack other machines from the honeypot (Spitzner p. 82).

Medium-interaction honeypots fall into a grey area between its low and high interaction counterparts in that they are home-made and not some off-the-net/out-of-the-box pre-made solution. Medium-interaction honeypots can range from a simple port listener created with netcat listening on a particular port to a complete Red Hat 9.0 machine just sitting on a network somewhere waiting to be attacked. Basically, these types of honeypots are built and completely customized by those who will be administering them.

An example of a low-interaction honeypot is one called Back Officer Friendly (BOF). Originally written to listen for Back Orifice attempts, BOF would listen on port 31337 and pretend to be a

machine infected with the BO trojan. As time passed, capabilities to listen on other ports, like FTP, telnet, and SMTP, were added. As of this writing, BOF is currently capable of listening on seven ports. Honeytrap software called ManTrap is an example of a high-interaction honeypot and runs on Solaris machines. ManTrap runs on top of the operating system and creates up to four exact, yet separate, copies of the operating system with each copy being unaware of the others. Each copy acts as a cage, which contains the attacker and records all of his/her actions. Records of the events are sent to an administration GUI where the logs of all the cages/copies can be viewed.

But what can a honeypot do for me, you ask? Think of this. Firewalls have the have the wonderful ability to create upwards of gigabytes of data per day, containing entries of both hostile and non-hostile activity. Honeypots, since they have no production value, should not get any traffic at all. The traffic they do get, not only is significantly less, but is also automatically questionable.

Say a Linux honeypot mimicing a webserver was compromised. You have the log entry generated by the honeypot, along with the offending IP. Now you can reference the date and time of that event with the firewall to significantly narrow your search of the event in the firewall's log. Once you know what it looks like in the firewall, you can then look for other potential attacks against your actual webserver from the same offending IP. You then can also see what kind of other traffic is coming from that offending IP to your network. Same ideas holds true for desktop/workstation machines, and other machines of value, as well. Obviously though, the honeypot must mimic the production machine either exactly, or as close as possible in order to look like an actual machine of value.

However, the most valuable purpose a honeypot has is research. Honeypots are currently used to learn the tricks and the trades of the black-hat "hacker". They also can catch previously unknown, day-zero, exploits in the wild and discover vulnerabilities that they exploit. In January 2002, a ManTrap honeypot running on Solaris discovered a previously unknown exploit in use targeting the dtspcd service. More recent than that, in April 2003, an exploit against Samba was discovered by a machine that was "essentially a honeypot (Lemos)." While some people are figuring out ways to break into systems and developing tools to do so, others are figuring out how the first group got in, and are developing tools to aide them in this process. Honeypots happen to be one of them.

As wonderful as honeypots may seem to some, a huge legal and privacy debate rages on. It isn't quite clear where honeypots fall in terms of legality in the United States. Our legal system here in the U.S. is based on precedent, and since honeypots have only recently begun to gain popularity, there currently is no precedent that I know of. Entrapment is also a concern among some, but since entrapment involves getting someone to committ a crime they otherwise would not have, and crackers are most likely out looking to break into something anyway, an entrapment defense might not work. However, I'm no lawyer (thank god!!), so talk with someone who is before deploying one.

On the other hand, honeypots spark an intense privacy debate as well. Here, honeypots may also fall under various other laws like the Fourth Amendment of the U.S. Constitution, The Wiretap Act, The Pen/Trap Statue, and the Electronic Communications Privacy Act (Spitzner p.

372 - 376). A major concern among some is that attackers, once they break in to a honeypot, may not know that they are being monitored. Apparently, they would then go chat with their buddies and others, on IRC or whatnot, thinking they have secure communications.

Suggestions have been made to add disclaimers on log-in screens that basically say "On this system, you'll be monitored and by logging in you agree to let yourself be monitored" so that attackers may have a chance to know that they're being monitored. But like I said earlier, for you security professionals out there, consult a lawyer before deploying a honeypot on your organization's network. It could save you a mess of legal headaches later on.

Honeypots are available to install on a wide variety of operating systems, including Windows, and the various Linux and Unix flavors. They are quickly gaining popularity in many organizations and I am sure that we will see them again in the near future. Soon, deceiving a potential attacker will be just as important as detecting and preventing one. Like anything though, in order for them to operate with maximum efficiency, they must be carefully maintained and administered.

**** Works Cited ****

Lemos, Robert. "Honeypots Get Stickier for Hackers". CNET News.com
<http://news.cnet.com/2100-1009-996574.html>. April 11, 2003

Spitzner, Lance. "Honeypots: Tracking Hackers" Addison-Wesley. 2003.

**Become famous! Send an article into the
AONewsletter!!**

**We want articles on security tools, "hacking"
tools, ideas, rants, raves, reviews, etc.**

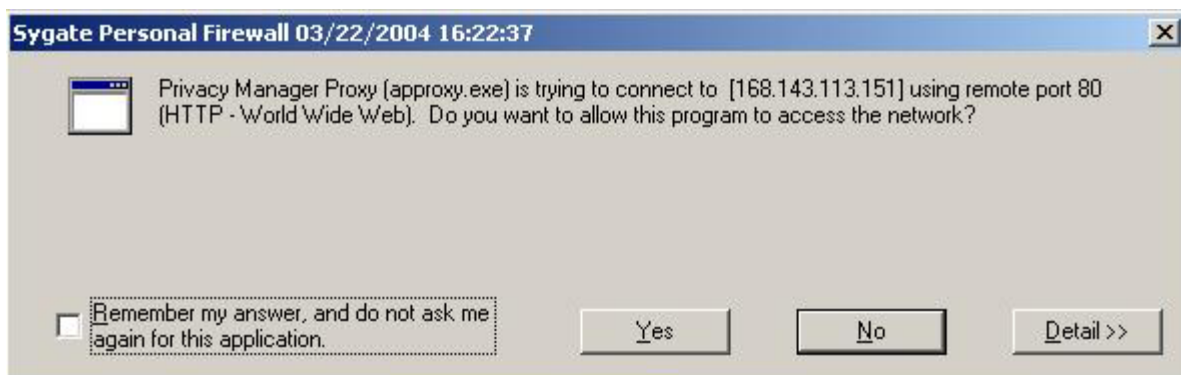
**Send a note to msmittens@msmittens.com
with AONewsletter in the subject line or send
a private
message to my AO account, MsMittens.**

Next deadline: May 24, 2003

Anonymizer Privacy Manager: Doing what exactly? by MsMittens

Privacy. It's dear to us on the Internet because we know there is an inherent lack of it on the Internet. Many people who surf around and visit various websites like to ensure a certain amount of privacy. It helps avoid some of the spam emails and can help keep us protected from the prying eyes of the government (although, if you talked with the US Government in particular the impression is that no one should be anonymous). That said, one of the front-running tools in helping individuals keep their privacy is Anonymizer (<http://www.anonymizer.com>).

It's an interesting tool that caught my eye late last year. intmon, AO's admin, had forwarded an email from a new user trying to visit AntiOnline. Apparently, everytime they connected to the main page while using Anonymizer, they would get Document contains no data as an error. It struck me as odd at the time. So I began a little search and investigation into what might have caused this. I visited their website. Directly from the website one is allowed to visit any website they want anonymously by entering the URL in the provided box — except Antionline. As Spock used to say... "Fascinating."



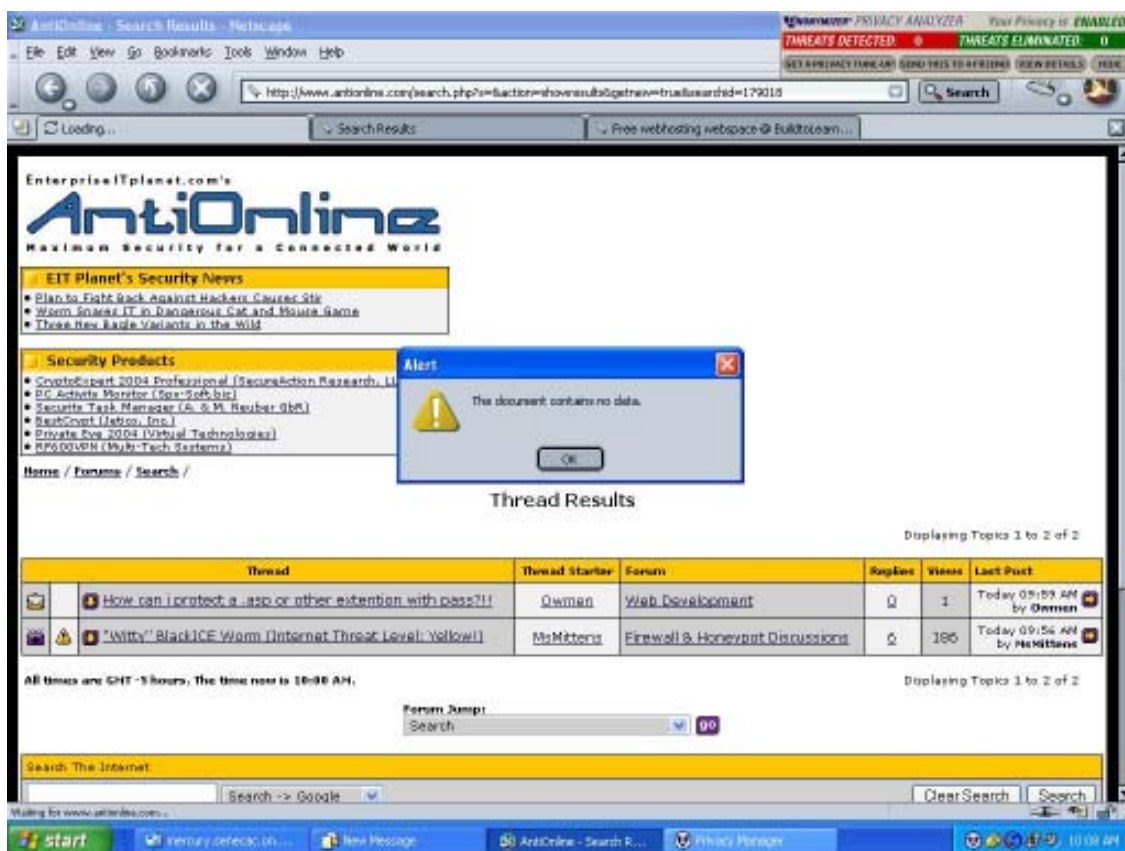
I began to wonder why this would be. I had originally speculated that perhaps Antionline had been "associated" with other "hacking" websites it might be part of a special exempt list. This proved to be a false assumption since I could happily visit <http://www.astalavista.com> and other "suspect" websites. Ok. That theory out the window.

Maybe it was a leftover from the "hacker wars" of the mid-90s, when many took objection to Antionline's creator, JP, doing some activities with federal authorities. Now that might hold some. Time to do some research, me thinks. And with that I shelled out the \$30USD for the product and flip from Linux to Windows for a while. I did attempt to get anonymizer working in Linux but wine just didn't want to cooperate on this (plus I had re-mangled my Slackware install so I think I lost something somewhere...).

Now, in addition to the standalone software, I needed tools to try and track what the software was doing. For that I employed Proximitron and Achilles. I also later got Process Explorer to try and track memory allocation. I began by experimenting at work on my Windows XP box

there. The admin had given me full rights on my work machine to play with (and because I had complained I was tired of popups and wanted to deal with them more effectively). What I didn't expect is that when I went to connect to Anonymizer to do the final licensing and authentication, it was blocked! It did make sense. The College would want to know who did what when someone else comes to complain. Ah well.

So I installed it home on my Windows 98 box. Now, I do want to point out that I had McAfee Anti-Virus enabled along with BlackIce defender. I did remove defender as I didn't want it to interfere with my experiments. My first test was to see if I could mimic the error that the user had complained about. Anonymizer allows for default settings from Low (allow everything) to Maximum (basically block everything). It was kind of nifty. I could choose whether scripts would run, whether you would see the title of the webpage you were visiting (avoids nosy bosses learning you are good at various games), allowing or disallowing cookies and a myriad of other features. It is a pretty good tool actually. But like the user, no matter what setting I put it on, I would get Document contains no data. The only way I could visit AO was to shut off Anonymizer. Well, that seems silly.



A few days later I discovered that the College had finally allowed access to Anonymizer. I guess my email requesting access did work! Excellent. So I re-installed the product at work and gave it a go there. On that machine I actually had no firewall installed (school does apparently provide something since certain websites are blocked). But I did have anti-virus (Symantec) installed. And things certainly got interesting.

I began by experimenting with Anonymizer by itself. The same issue as the one I experienced

on my home machine reappeared at work. This time, however, I was on XP. So I was able to eliminate the OS at least. I fired up the ol' packet sniffer, WinDump, so I could see what Anonymizer was doing on the network at least. What I found interesting was that Anonymizer would connect back to specific proxies setup by the company. This is how you remain anonymous: basically, you proxy through their servers to connect to various locations. This would mean, technically, if someone wanted to find you, knew you were using Anonymizer and had enough legal leverage (ie., warrants) they could track you down. As TheHorse13 commented to me once, there is always a way to track someone down. This would certainly be the case. But I wasn't sure that this was the reason why I would be blocked from seeing Antionline. It just didn't make sense still — unless the proxies were designed to deliberately block AO. My 2nd theory about it being a leftover of the past was feeling stronger.

So now I fired up Proximitron to see what was going on as far as modifying pages between Anonymizer and the website being visited. And the weirdest thing happened: Now, I could see AO without problem. Eh? Now that was a head scratcher. So I tried Achilles instead. And this time, I got blank pages. I suppose that's better than Document contains no data but it strikes me that it's kinda the same. Now, this was interesting. This sort of shot my 2nd theory down a bit. One of two things might have been going on: a script that runs on AO could be interfering with Anonymizer or it could be because the proxying by Proximitron/Achilles was blocking AO to Anonymizer that Anonymizer didn't pick up that AO was there (follow me?).

Now I fired up Process Explorer to see if I could find out what Anonymizer was actually doing. One of the things I did determine was that Anonymizer uses a lot of memory threads. I counted about 20-25 different threads. But there wasn't one that stood out specifically. Add to that having to cut my experiment short because of an impending potential strike. Time to continue the experiment at home.

Now, the home machine had changed. I had re-installed both Slack and Windows. And the Windows wasn't 98 but rather XP. But I decided not to renew my subscription with McAfee because I wanted to use the Windows box for an abuse box. I installed Anonymizer and Process Explorer and.. it worked! Not a single problem connecting with AO at all. Now this was weird. Maybe my conspiracy theory wasn't accurate. Could it be that the anti-virus was actually interfering with Anonymizer's ability to interpret a script? More experimentation. I installed Panda Anti-Virus but no change was noticed. Interesting.

Now as I write this I did some final tests. I opened up ProcessExplorer and set Anonymizer to Maximum. Then I refreshed the AO page. I got the appropriate page but ProcessExplorer crashed. Weird. Did it again. Same thing. I set Anonymizer to Medium and no problem. There does seem to be issues with how the memory is managed in my opinion and noobish guessing (I'm not a programmer but I do get the idea as to how things should work generally).

I suspect that Anonymizer and the virus software are running into conflicts. The reaction of ProcessExplorer would also help support this theory. It does make me wonder however if someone could create an exploit to crash Anonymizer and thus remove the anonymity that it provides. Perhaps something worth exploring by someone here.

Note: I've left the appendices pretty much unaltered in hopes that someone might see something worthwhile to add.

Appendix 1: ProcessExplorer Threads when attempting to access AO

Process	PID	CPU	Description	Company Name
System Idle Process		0	84	
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4			
smss.exe	560		Windows NT Session Manager	Microsoft Corporation
csrss.exe	608	3	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	632		Windows NT Logon Application	Microsoft Corporation
services.exe	676	3	Services and Controller app	Microsoft Corporation
svchost.exe	872		Generic Host Process for Win32 Services	Microsoft Corporation
svchost.exe	952		Generic Host Process for Win32 Services	Microsoft Corporation
Smc.exe	988	1	Sygate Agent Firewall	Sygate Technologies, Inc.
spoolsv.exe	1324		Spooler SubSystem App	Microsoft Corporation
svchost.exe	1652		Generic Host Process for Win32 Services	Microsoft Corporation
DefWatch.exe	1684		Virus Definition Daemon	Symantec Corporation
inetinfo.exe	1716		Internet Information Services	Microsoft Corporation
nmapserv.exe	1736			
Rtvscan.exe	1752	1	Symantec AntiVirus	Symantec Corporation
svchost.exe	2292		Generic Host Process for Win32 Services	Microsoft Corporation
lsass.exe	688		LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	500		Windows Explorer	Microsoft Corporation
VPTray.exe	596		Symantec AntiVirus	Symantec Corporation
bxOEPlugin.exe	900			
ctfmon.exe	916		CTF Loader	Microsoft Corporation
HOTSYNC.EXE	1100		HotSync® Manager Application	Palm, Inc.
devldr32.exe	1524		DevLdr32	Creative Technology Ltd.
msimn.exe	1572		Outlook Express	Microsoft Corporation
Netscp.exe	2884		Netscape	Mozilla, Netscape
privmgr.exe	1780			
procexp.exe	2448	8	Sysinternals Process Explorer	Sysinternals
aproxy.exe	3796			

Process: aproxy.exe Pid: 3796

Type	Name
Desktop	\Default
Directory	\Windows
Directory	\BaseNamedObjects
Directory	\KnownDlls
Event	
Event	
Event	
Event	
Event	
Event	
Event	
Event	

Event
Event
Event
Event \BaseNamedObjects\crypt32LogoffEvent
Event \BaseNamedObjects\REAPSITES_LOCK_1
Event \BaseNamedObjects\MXAPSITES_LOCK_1
Event \BaseNamedObjects\AP_PROXY_TERMINATE
Event
Event
Event
Event
Event
Event \BaseNamedObjects\APPROXY_ALIVE_SSL
Event \BaseNamedObjects\APPROXY_ALIVE
Event \BaseNamedObjects\AP_CONFIG_CHANGE_EVENT
Event
Event \BaseNamedObjects\AP_CONFIG_CHANGE_EVENT
Event
Event
File \Device\Afd\Endpoint
File \Device\Afd\Endpoint
File \Device\Tcp
File \Device\Tcp
File \Device\Afd\Endpoint
File \Device\Tcp
File \Device\Tcp
File \Device\Afd\Endpoint
File \Device\Afd\Endpoint
File \Device\Tcp
File \Device\Tcp
File \Device\Tcp
File \Device\Tcp
File \Device\Tcp
File \Device\Ip
File \Device\Ip
File \Device\Ip
File \Device\Tcp
File \Device\Afd\Endpoint
File \Device\WMIDataDevice
File \Device\WMIDataDevice
File \Device\NetBT_Tcpip_{3DCD127F-95DC-4F29-A7B4-046036794EA7}
File \Device\Tcp
File \Device\Tcp
File \Device\Afd\Endpoint
File \Device\Tcp
File \Device\Tcp
File \Device\Afd\Endpoint
File \Device\Tcp
File \Device\Tcp
File \Device\Afd\Endpoint
File \Device\Tcp
File \Device\Tcp
File \Device\Afd\Endpoint
File \Device\Tcp
File \Device\Tcp


```
IoCompletion
IoCompletion
Key HKLM\SYSTEM\ControlSet001\Services\Tcpip\Linkage
Key HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters
Key HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters\Interfaces
Key HKLM\SYSTEM\ControlSet001\Services\NetBT\Parameters
Key HKLM
Key HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32
Key HKCU
Key HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
Key HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
Key HKU
KeyedEvent \KernelObjects\CritSecOutOfMemoryEvent
Mutant \BaseNamedObjects\WMAPSITES_LOCK_1
Mutant \BaseNamedObjects\SITES_GUI_OR_PURGE_MUTEX
Mutant \BaseNamedObjects\AnonProProxyStarted
Mutant \BaseNamedObjects\tcpmoncfg_LOCK_MUTEX
Mutant \BaseNamedObjects\DBWinMutex
Mutant \BaseNamedObjects\IP_LIST_LOCK_MUTEX
Mutant \BaseNamedObjects\dnsCache_LOCK_MUTEX
Mutant \BaseNamedObjects\IP_LIST_LOCK_MUTEX
Mutant \BaseNamedObjects\dnsCache_LOCK_MUTEX
Port
Process approxy.exe (3796)
Section
Section \BaseNamedObjects\SITE_LIST_SHM_1
Section \BaseNamedObjects\tcpmoncfg_SHM
Section \BaseNamedObjects\ip_list_SHM
Section \BaseNamedObjects\dnsCache_SHM
Section \BaseNamedObjects\ip_list_SHM
Section \BaseNamedObjects\dnsCache_SHM
Semaphore
Semaphore
Semaphore
Semaphore
Thread approxy.exe (3796): 3856
Thread approxy.exe (3796): 3800
Thread approxy.exe (3796): 3800
Thread approxy.exe (3796): 3860
Thread approxy.exe (3796): 3856
Thread approxy.exe (3796): 3856
Thread approxy.exe (3796): 3860
WindowStation \Windows\WindowStations\WinSta0
WindowStation \Windows\WindowStations\WinSta0
WmiGuid
```

Appendix 2: Proximitron Results when Using Anonymizer

(note: personal info removed)

```

+++RESP 167+++
HTTP/1.1 200 OK
Date: Tue, 10 Feb 2004 12:52:42 GMT
Server: Apache/1.3.29 (Unix) PHP/4.3.4
X-Powered-By: PHP/4.3.4
Set-Cookie: sessionhash=fadce0478e9bc1e284cef38b5671259c; path=/;
domain=.antionline.com
Set-Cookie: bblastvisit=1076417246; expires=Wed, 09-Feb-05 12:47:26 GMT; path=/;
domain=.antionline.com
Content-Length: 20766
Content-Type: text/html
X-Cache: MISS from proxy51.anonymizer.com
Connection: close
<start> 167: Kill pop-up windows
<start> 167: Suppress all JavaScript errors
<start> 167: Stop browser window resizing
Match 167: Frame Jumper-Outer
Match 167: Frame Jumper-Outer

+++GET 168+++
GET /aoimages/antilogo-sml.gif HTTP/1.1
Host: images.antionline.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4) Gecko/20030624
Netscape/7.1 (ax)
Accept: video/x-mng,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Referer: http://images.antionline.com/aoimages/antilogo-sml.gif
Cookie: bbuserid=xxxxx; bblastvisit=1075810754; bbpassword=xxxxx;
sessionhash=65e224b85985d1efe214dc16bcec6f80;
http://www.antionline.com/aoimages/antilogo-sml.gif
If-Modified-Since: Wed, 05 Nov 2003 19:06:12 GMT
If-None-Match: "29d7-f06-3fa94a24"
Cache-Control: max-age=0
Connection: keep-alive
Match 167: Frame Jumper-Outer
Match 167: Frame Jumper-Outer

+++GET 169+++
GET /aoimages/corner.gif HTTP/1.1
Host: images.antionline.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4) Gecko/20030624
Netscape/7.1 (ax)
Accept: video/x-mng,image/png,image/jpeg,image/gif;q=0.2,*/*;q=0.1
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Referer: http://images.antionline.com/aoimages/corner.gif
Cookie: bbuserid=xxxxx; bblastvisit=1075810754; bbpassword=xxxxx;
sessionhash=65e224b85985d1efe214dc16bcec6f80;

```


Appendix 3: WinDump results

```
10:32:05.246391 IP my.special.ip.2962 > 168.143.113.153.80: . ack 1 win 64240 (DF)
10:32:05.248987 IP my.special.ip.2962 > 168.143.113.153.80: P 1:1194(1193) ack 1 win 64240
(DF)
10:32:05.353195 IP 168.143.113.153.80 > my.special.ip.2962: . ack 1194 win 7158 (DF)
10:32:05.545877 IP 168.143.113.153.80 > my.special.ip.2962: . 1:731(730) ack 1194 win 7158
(DF)
10:32:05.546979 IP 168.143.113.153.80 > my.special.ip.2962: P 731:1461(730) ack 1194 win 7158
(DF)
10:32:05.547220 IP my.special.ip.2962 > 168.143.113.153.80: . ack 1461 win 64240 (DF)
10:32:05.668961 IP 168.143.113.153.80 > my.special.ip.2962: . 1461:2191(730) ack 1194 win 7158
(DF)
10:32:05.670409 IP 168.143.113.153.80 > my.special.ip.2962: P 2191:2921(730) ack 1194 win 7158
(DF)
10:32:05.670435 IP 168.143.113.153.80 > my.special.ip.2962: . 2921:3651(730) ack 1194 win 7158
(DF)
10:32:05.670716 IP my.special.ip.2962 > 168.143.113.153.80: . ack 2921 win 64240 (DF)
10:32:05.792939 IP 168.143.113.153.80 > my.special.ip.2962: . 3651:4381(730) ack 1194 win 7158
(DF)
10:32:05.793015 IP 168.143.113.153.80 > my.special.ip.2962: P 4381:5111(730) ack 1194 win 7158
(DF)
10:32:05.793055 IP 168.143.113.153.80 > my.special.ip.2962: . 5111:5841(730) ack 1194 win 7158
(DF)
10:32:05.795238 IP my.special.ip.2962 > 168.143.113.153.80: . ack 4381 win 64240 (DF)
10:32:05.795245 IP my.special.ip.2962 > 168.143.113.153.80: . ack 5841 win 64240 (DF)
10:32:05.910411 IP 168.143.113.153.80 > my.special.ip.2962: P 5841:6571(730) ack 1194 win 7158
(DF)
10:32:05.910451 IP 168.143.113.153.80 > my.special.ip.2962: . 6571:7301(730) ack 1194 win 7158
(DF)
10:32:05.910470 IP 168.143.113.153.80 > my.special.ip.2962: P 7301:8031(730) ack 1194 win 7158
(DF)
10:32:05.910873 IP my.special.ip.2962 > 168.143.113.153.80: . ack 7301 win 64240 (DF)
10:32:05.938840 IP 168.143.113.153.80 > my.special.ip.2962: . 8031:8761(730) ack 1194 win 7158
(DF)
10:32:05.938879 IP 168.143.113.153.80 > my.special.ip.2962: P 8761:9491(730) ack 1194 win 7158
(DF)
10:32:05.938901 IP 168.143.113.153.80 > my.special.ip.2962: . 9491:10221(730) ack 1194 win
7158 (DF)
10:32:05.939329 IP my.special.ip.2962 > 168.143.113.153.80: . ack 8761 win 64240 (DF)
10:32:05.939381 IP my.special.ip.2962 > 168.143.113.153.80: . ack 10221 win 64240 (DF)
10:32:06.023027 IP 168.143.113.153.80 > my.special.ip.2962: P 10221:10951(730) ack 1194 win
7158 (DF)
10:32:06.023070 IP 168.143.113.153.80 > my.special.ip.2962: P 10951:12411(1460) ack 1194 win
7158 (DF)
10:32:06.023456 IP my.special.ip.2962 > 168.143.113.153.80: . ack 12411 win 64240 (DF)
10:32:06.024744 IP 168.143.113.153.80 > my.special.ip.2962: . 12411:13871(1460) ack 1194 win
7158 (DF)
10:32:06.046810 IP 168.143.113.153.80 > my.special.ip.2962: . 13871:15331(1460) ack 1194 win
7158 (DF)
10:32:06.047099 IP my.special.ip.2962 > 168.143.113.153.80: . ack 15331 win 64240 (DF)
10:32:06.048494 IP 168.143.113.153.80 > my.special.ip.2962: P 15331:16791(1460) ack 1194 win
7158 (DF)
10:32:06.048746 IP my.special.ip.2962 > 168.143.113.153.80: . ack 16791 win 64240 (DF)
10:32:06.061377 IP 168.143.113.153.80 > my.special.ip.2962: . 16791:18251(1460) ack 1194 win
7158 (DF)
(1194 win 7158 (DF))
```