

Full-Disclosure: RE: [Full-disclosure] RE: Computer forensics to uncover illegalinternet use

RE: [Full-disclosure] RE: Computer forensics to uncover illegalinternet use

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-09/0085.html>

From: Chuck Fullerton (cfullerton_at_fullertoninfosec.com)

Date: 09/04/05

To: "'Steve Kudlak'" <chromazine@sbcglobal.net>, "'dave kleiman'" <dave@isecureu.com>

Date: Sun, 4 Sep 2005 10:06:17 -0400

All,

I do find this like of discussion very interesting. However, there has been so much discussion that it's getting difficult to follow. Therefore, I'd like to make the following recommendation for future posts.

1. Minimize the text you to which you are replying to the pertinent info.
2. Everyone use the same method of replying.. (i.e. inline, top or bottom) I don't care which but it's really getting tough to follow.
3. Keep the discussion going as I'm really getting a lot out of this. ;-)

Sincerely,

Chuck Fullerton

From: full-disclosure-bounces@lists.grok.org.uk
[mailto:full-disclosure-bounces@lists.grok.org.uk] On Behalf Of Steve Kudlak
Sent: Sunday, September 04, 2005 1:45 AM
To: dave kleiman
Cc: 'Craig, Tobin (OIG)'; echow@videotron.ca; 'Sadler,Connie';
jbeauford@EightInOnePet.com; 'Full-Disclosure';
security-basics@securityfocus.com
Subject: Re: [Full-disclosure] RE: Computer forensics to uncover illegalinternet use

dave kleiman wrote:

Steve,

Inline..

RE: [Full-disclosure] RE: Computer forensics to uncover illegalinternet use

Full-Disclosure: RE: [Full-disclosure] RE: Computer forensics to uncover illegal internet use
Hate to play lawyer here but doesn't all of this get shot down by 3rd
Circuit Federal Court of Appeals decisions regarding the FBI's
Innocent Images project? It basically shot down the concept of "you
clicked on a hold porn link therefore you're guilty."

Well that applies to when it is determined that it was innocent. This could
be via pop-up, trojan, or malware of some kind.

This is all enshrined in Federal

Cases. No one must admit that a good prosecutor can indict a ham
sandwich and all that. But overall that doesn't happen.

Now Federal Prosecutors and Investigations staffs are very good at
sort of getting warrants and raiding someone's house or business and
going thru everything. But if the person doesn't scare and cop to
something they never did, then federal prosecutors generally have to
back off in cases where it is just things accumulating on disks etc.

Well they do not usually prosecute ham sandwiches, BLT's maybe.

I love how everyone is quick to say things just magically accumulated on
their H/D. However, they tend not back off when a file structure is found
with hundreds of images, often burned to CD's.

Furthermore in

states with a high privacy expectation like California there is a good
reason to say "We don't go through our customers data looking for
things out of the ordinary". One might argue it to be different it

RE: [Full-disclosure] RE: Computer forensics to uncover illegal internet use

Full-Disclosure: RE: [Full-disclosure] RE: Computer forensics to uncover illegal internet use
were one's employees. However if you are offering a primo privacy
service then you can legitimately scrub disks as a part of the biz
plan.

Well that may be, of course you missed the beginning of these threads, where
Mr. Combs suggested after discovering contraband on and employees H/D, to
make a copy of it take the copy to the companies attorney. Wipe the original
and "best course of action is to purposefully falsify the record of the
company's response to the incident"

The full threads can be read here:

<http://seclists.org/lists/security-basics/2005/Sep/subject.html>

<http://seclists.org/lists/security-basics/2005/Aug/subject.html>

Much of Law Enforcement and their Public Providers of services
depends on scaring people and businesses into good behavior when it is
neither necessary or ethical. My suspicion is that one can ignore this
tactic if one wishes as one is reasonably careful.. I am sure that
people will be offering "Computer Forensics Services" to find the
scary things on your compnys disks for \$500 a pop but no good reason
one has to engage in such silliness.

Yes that crazy scaring people into good behavior..... Oh wait that is
right only reasonably prudent people follow the law, criminals tend to not
care if there is law against something, they are not scared into not
committing crimes, that is why they are criminals.

Kind of like the lawlessness that is occurring in the situation you

RE: [Full-disclosure] RE: Computer forensics to uncover illegal internet use

Full-Disclosure: RE: [Full-disclosure] RE: Computer forensics to uncover illegal internet use mentioned below. Some people would say that the devastation has turned these people into criminals. Although, the reality is the people committing the crimes are the same ones that were committing them before the devastation.

Excuse my flipness. I just got through friends caught up in this call people stranded and alone by the hurricane in the Southland and all these other things do ring silly right now.

Regards,

Dave

For a long time I sysop'd an open system, I dunno how much time I ended up deleting "girl with vacuum cleaner" pictures. This is getting weirder and weirder because with photoshop people can create things that do not exist in real reality. Of course you have really funny things like this one image that was from Japanese advertizing. They had a 10 year girl with this incredibly large pretty phallic looking squirt gun which she was squirting with a look of bliss on her face. It was pretty funny. It was funny how when showed this image it became a "cynicism filter". People would divide into the group that thought this was completely engineered from the get-go and those who thought it was just some weird thing that came out and no one noticed it, or that it was the product of the fact that much of Japanese Culture doesn't quite go looking for all possible suggestive variants. It really became a filter.

Now my suspicion about people in the US Southland is that it is a bit of oppurtunism in the face of despair and the feeling that "whitey has been shitting on us for centuries". Me being on the North American West Coast doesn't notice that because there were no slave quarters and slave markets in California, Washington, Oregon, British Columbia and we are apt to think a "quadron" is a small gold coin that would be nice to find in one's progenitors coin collection. I don't think it is because there is just a massive criminal element hidden from us. Now some of the behavior sounded like what I found in my tenure at a small residential hotel. From the last week of the month to the first week of the next month a number of curious items would end up for sale. It was always curious to imagine where these items came from, some were legitimately obtained, others probably not. There was always an argument among the low rent district types that

RE: [Full-disclosure] RE: Computer forensics to uncover illegal internet use

Full-Disclosure: RE: [Full-disclosure] RE: Computer forensics to uncover illegal internet use

universally almost always aligned as "crazy white guys accusing mexicans of shop lifting and reselling, whereas many of the items they had could be seen as coming from equally questionable sources.

Now if one talks to Federal Proscutors they will tell you that they feel comfortable with their "Vacuum Cleaner" approach. They feel if they do go and get everyone questionables stuff and go through it, then one will be able to determine how many folks had thing accumulating on their disk and how many actively collected it etc. Now interestingly with the Third Circuit's Decision which is close to rock solid at this point in precdent, people like journalists would sort of get wide descretion especially if they were working on stories and doing investigations etc.

Two other things come in here. In both the US Ninth Circuit and Upper Level Courts of British Columbia it has been held that one can not commit crimes against "virtual children" or "animated descriptions of children etc". This means the general belief in liberal democracies that "thought crimes" are questionable is beginning to be enshired in code and precedent. I am pretty sure this is well embedded in North American Culture and is apt not to go away even with the idea, darfe I say spectre two very conservative reversalist judges on the Supreme Court. Note I have not had time to study how things work in the EU or even Australia.

Now technoculturally want this may eventually provoke is the use of high grade encryption by more people. Right now I know even artists who hqave become more technologically saavy and who encrypt things even when legal code is on their side overall. In the 1970s and 1980s there were a number of legal razzlements of artists who used their children as nude models no matter how innocent. This went too far and eventaully what got established is the concept that "simple nudity is not obscene". It is interesting because artists are not usually seen as users or consumers of secuuity products and things like encryption.

Anyway this is all very interesting and we do live in interesting times. So it will be interesting to see how this will go and whether the bizness idea of trying to safe from all possible wrongdoing or perceived wrongdoing will win out overall. I know lots of vendors and security consultants have been hoping that "porn protection" would turn into a lucerative field but so far it doesn't compare to virus and malware protection.

Interestingly in artist circles the whole imaging thing has turned into "sousveillance" and artists have been having way too much fun turning the cameras back on the people who usually use them. It is interesting that people like Sudo Chiles House who was one of the first people to install a "cam" which in her case was a 35mm camera that took pictures regularly of her bedroom is all buit forgotten in the modern installatiion of cams in various public and private spaces. Note the UK and places in Florida have been very much into the "you are being watched" theory of crime control. I also have heard tales of "spy camera destroyers" who have been running around spray painting cameras but I think that is not widespread at this point. Hmmm, indeed these are interesting times. whether it is a blessing

RE: [Full-disclosure] RE: Computer forensics to uncover illegal internet use

Full-Disclosure: RE: [Full-disclosure] RE: Computer forensics to uncover illegalinternet use
or a curse is an open question.

Have Fun,
Sends Steve

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>