Bruce Schneier

Schneier on Security

A blog covering security and security technology.

« Friday Squid Blogging: Giant Squid Eye Preserved in a Jar | Main | LiveBlogging the Bin Laden Assassination »

May 2, 2011

Hijacking the Coreflood Botnet

Earlier this month, the FBI seized control of the Coreflood botnet and shut it down:

> According to the filing, ISC, under law enforcement supervision, planned to replace the servers with servers that it controlled, then collect the IP addresses of all infected machines communicating with the criminal servers, and send a remote "stop" command to infected machines to disable the Coreflood malware operating on them.

This is a big deal; it's the first time the FBI has done something like this. My guess is that we're going to see a lot more of this sort of thing in the future; it's the obvious solution for botnets.

Not that the approach is without risks:

> "Even if we could absolutely be sure that all of the infected Coreflood botnet machines were running the exact code that we reverse-engineered and convinced ourselves that we understood," said Chris Palmer, technology director for the Electronic Frontier Foundation, "this would still be an extremely sketchy action to take. It's other people's computers and you don't know what's going to happen for sure. You might blow up some important machine."

I just don't see this argument convincing very many people. Leaving Coreflood in place could blow up some important machine. And leaving Coreflood in place not only puts the infected computers at risk; it puts the whole Internet at risk. Minimizing the collateral damage is important, but this feels like a place where the interest of the Internet as a whole trumps the interest of those affected by shutting down Coreflood.

The problem as I see it is the slippery slope. Because next, the RIAA is going to want to remotely disable computers they feel are engaged in illegal file sharing. And the FBI is going to want to remotely disable computers they feel are encouraging terrorism. And so on. It's important to have serious legal controls on this counterattack sort of defense.

Some more commentary.

Posted on May 2, 2011 at 6:52 AM • 37 Comments

To receive these entries once a month by e-mail, sign up for the Crypto-Gram Newsletter.

Comments

I think there is a big difference between disabling a computer using the rogue command and control channel that is already on the box and hacking into the machine to install your own malware. In the case of a botnet every zombie box is capable of taking orders from a criminal enterprise. The FBI used this existing channel to shut down the enterprise. It's a pretty large leap to go from that to using Government sponsored zero day attacks to take control of arbitrary machines at the behest of the RIAA. For one such machines don't have centralized C&C so attempting to carry out such a plan would be impractical.

Posted by: Mike B at May 2, 2011 7:05 AM

From the temporary restraining order: "Identified owners of infected computers will also be told how to 'opt out' from the TRO, if for some reason they want to keep Coreflood running on their computers."

"opt out" from the TRO, if for some reason they want to keep Coreflood running on their computers.

When possession of malware, like child pornography, on a computer is made illegal -- and the RIAA would love to include file sharing software in the definition of malware -- then law enforcement will have, in those who have opted out of the Coreflood TRO, a ready-made list of criminal malware possessors.

Posted by: Alan Kaminsky at May 2, 2011 7:29 AM

I'd imagine the next step for botnet writers is a "deadman's switch", that nukes the infected computer; should control of the botnet slip from their fingers or the malware be erased in the wrong way.

One could say that the threat of this might make people more concerned about the security of their home computers. I'll take that bet.

Posted by: Jason! at May 2, 2011 7:45 AM

I share concerns about outsiders being able to remotely execute code on machines, but in this case if the targets are already infected with botnet software they're effectively already out of their owner's control and can't be trusted anyway. This is in contrast to the RIAA who's argument rests on the owner being complicit in the alleged crime(s).

That said, I agree with Bruce insofar as there must be strict legal rules about when such disabling can be executed. The first step may be to more specifically define what constitutes a botnet, given law enforcement and politicans barely even understand file sharing!

Posted by: Ruben Schade at May 2, 2011 7:46 AM

Its a tough choice, but I think having the government in control of a botnet is probably 10% better than having organized crime in control of it.

But what they should do is download a patch to de-zombie each infected client, not simply deactivate the botnet until the next reboot. This looks like what they really want is a botnet all their own.

Posted by: bob at May 2, 2011 8:10 AM

So, what happens when the botnet after next destroys all data when it detects attempts to have it disable itself?

IANAL, but as the sending of deactivation commands is a willful act by whoever is sending them, I would expect them to be liable in some way.

Posted by: Richard "RichiH" Hartmann at May 2, 2011 8:16 AM

The idea of some government agency attacking a server on behalf of the RIAA, or any large corporation, smacks of neo-neo-colonialism or cyber-neo-colonialism.

Posted by: aikimark at May 2, 2011 8:40 AM

"From the temporary restraining order: 'Identified owners of infected computers will also be told how to "opt out" from the TRO, if for some reason they want to keep Coreflood running on their computers.'"

I saw that. I just can't imagine how that sort of thing would work on any scale.

Posted by: **Bruce Schneier** at May 2, 2011 8:46 AM

It's stuff like this that made me decide to migrate all of my computing tasks to Linux some 4 years ago. I don't regret the decision (or the pain - there was some) at all.

Posted by: Spaceman Spiff at May 2, 2011 8:53 AM

How on earth could this possibly be a consideration? Getting rid of malware with a set of known network devices is hard enough, much less a sea of malware-infested computers out of the owners' control. That being said, there should be mandatory awareness classes about how to protect your computer from malware before you get an internet connection, lol. At least a basic course.

Posted by: fbm at May 2, 2011 9:02 AM

@bob: They could make a patch available, but forcibly applying it on infected computers is about as wrong as infecting them in the first place. In either case, you're covertly installing software on somebody else's computer with unknown results; only the motives differ.

Taking control of a botnet and deactivating it through its own control channel is much more reasonable. (BTW, if the government wants a botnet, I'm sure several agencies can do better than trying to grab somebody else's.)

@aikimark: I have a slight problem with your comment: where did the "neo" come from? Using military force to benefit ones' own businesses is old-fashioned colonialism. "Neo" is when you leave the other government in place, and make it do what you want through economic means. More economical, and it doesn't carry the same stigma. However, taking direct action (like attacking a computer) isn't neo.

Posted by: David Thornley at May 2, 2011 9:43 AM

The biggest concern I see is the gov. is executing code on users computers with out their knowledge. Now granted they are trying to fix a problem but what if the code they execute actually creates a larger problem for some individuals? I also do not find it acceptable right wrong or otherwise for the gov to execute any code on users computer without their knowledge. IMO this is no different than GOV agency monitoring, infecting a suspects computer without a search warrant or the individuals consent.

Posted by: jerbear at May 2, 2011 10:21 AM

This is a situation where there don't appear to be any good options (currently) on the table.

The slippery slope: just as Bruce points out, later, the RIAA will use this to shut down machines supposed to be involved in filesharing. And after that?

There can be no "serious" legal controls: as wikileaks has shown, the govt does not respect laws against kidnapping, torture, and murder. And on less serious issues, like filesharing, the govt has shown that it'll defame 84,000 totally innocent people for every 10 that may actually be involved in something nefarious.

So, the government can't be trusted to properly handle abuse. Expect lots and lots of FPs.

And what about private industry? Twiddling their thumbs. Why should abuse departments shut down paying customers? The almighty dollar commands them not to.

In the end, I agree that people who let their machines be taken over and used for abuse have signed away the "sanctity" of their machines. I just don't see a solution to the problem that I feel confident about, is all.

Posted by: Johnston at May 2, 2011 10:29 AM

Here's hoping they've done substantial testing on what this "stop" command actually does. My biggest concern is that they are trusting the malware itself to disable the malware. That seems like a risky approach given that they don't have a lot of confidence in their understanding of the reverse-engineered code.

Posted by: Brent W at May 2, 2011 10:54 AM

I'm not sure there is a legitimate slippery slope argument here. Love them or hate them, the RIAA is made up of most 50-60+ year olds who couldn't wrap their heads around selling music online in the 1990s. They understand civil suits and excessive statutory damages. They are also good at getting them at legislative and judicial levels.

The FBI should be commended for attacking a real threat to commerce - a bot net. If however, in their haste to kill it, they take down a couple of infected machines, they may have to deal with the civil liability. The RIAA doesn't need this type of liability - they already have thousands of winnable cases of copyright infringement to pursue. The Feds may be in charge of enforcing copyright (as all of my DVDs remind me) but I don't see too many "joint operations" in the near future...

Posted by: Sean Patrick Burke at May 2, 2011 11:02 AM

The ISP's have had the ability to cut off machines they knew were part of a botnet. I listened to AT&T argue at a public conference why they didn't want to start doing that. Someone asked them why they couldn't at least notify the person who was sending all the spam etc., that they were part of a botnet. They still didn't want to do it. And they know it's eating up bandwidth and that it threatens others on the network. But they wouldn't do it for several reasons - it's a can of worms. And now the FBI is actively and intrusively getting control of a botnet? There's a lot more to it than what's presented.

Posted by: Jack at May 2, 2011 11:35 AM

I remember reading about similar case a while ago where researchers were able to hijack control of a botnet by predicting and purchasing domain names that the client software would try to connect to. They ended up not disabling the malware (on instruction from legal department) due to liability concerns, and lost control of the botnet when the domain registrations becase too expensive.

Though I've also heard of researchers and rivals who have been able to decommission botnets. I imagine the reason the FBI can "get away" with it is that they have considerably more immunity (implied or actual) from liability, and secondly, they don't care.

Microsoft Corporation has been using remote update functionality to actively remove malware for quite a while now; the MSRT (Malicious Software Removal Tool, mrt.exe) is delivered to Windows clients every month. Apple is known to have an app blacklist for their iDevices, and Google recently used their Cloud-to-Device Messaging to push their "Android Market Security Tool" DroidDream malware cleaner to affected Android devices, in real time. The C2DM remote install capability is unique to Android among the smartphones, as far as I know (BES can push bits to enterprise berries, but RIM doesn't use this AFAIK).

I imagine that the trend of OS/hardware vendors baking in killswitches, along with other functionality, will be seen more and more in the future as mobile & embedded devices shift to a managed user experience (and managed "security") as part of a centralized ecosystem model. In fact I think it's not be too long before updates go seamless, transparent and completely devoid of user interaction, Kindle-style. On many platforms there's no opt-out or prompting already, just patches and version checks every time it connects to the online service.

It still amazes me how major botnet controllers aren't using authenticated control channels. Just like IRC botnets: completely insecure.

Posted by: Seiran at May 2, 2011 12:54 PM

@Sean Patrick Burke:
"The FBI should be commended for attacking a real threat to commerce - a bot net. If however, in their haste to kill it, they take down a couple of infected machines, they may have to deal with the civil liability. "

The first time they zap a machine in another country, that liability may turn from civil to criminal. Most developed countries have criminal computer "hacking" laws these days, and they generally don't have a blanket exemption for foreign law enforcement agencies, no matter how well intentioned.

Posted by: Tony H. at May 2, 2011 12:55 PM

Coreflood exploits a Windows OS vulnerability and has been around for years. Which stakeholder should fix it: OS vendor, anti-virus vendor, ISP, end-user, FBI?

Probably should be the OS vendor, because it caused the software flaw and is more capable than the FBI to fix it. Are we going to nationalize anti-spyware the same way we are nationalizing health care?

Posted by: [illegible] at May 2, 2011 1:09 PM

Posted by: ant at May 2, 2011 1:00 PM

@David

Since America was a colony of the original set of colonial European powers, our efforts are 'new', thus the "neo" prefix. I wasn't ascribing/asserting methods, motivations, or results with the "neo".

Posted by: aikimark at May 2, 2011 1:10 PM

As I've said before, this is NOT a technological issue.

It is very easy to remotely remove a root kit from a machine.

It is a legal issue. As is demonstrated in the article that Bruce linked to.

So all the "cyber war" doomsday scenarios about zombie networks that have been brought up here in the past can be shown to be flawed (again).

And still some people will claim that it cannot be done. And they will cite their limited understanding of Turing machines and such.

The technology is available. The legal precedent is under discussion. Which leaves the next issue of "how to prevent future zombie infections of those (and other) machines".

Posted by: Brandioch Conner at May 2, 2011 1:15 PM

@ ant : "Probably should be the OS vendor, because it caused the software flaw"

What flaw? That general purpose OSs should be able to run any program which the user desires? You do realize that it's infeasible to solve the general problem of identifying malware, don't you? Oh, and you didn't know that malware ends up on people's computers via a mixture of OS flaws, third-party software flaws (Adobe, anyone?), and naive users actually downloading and running Trojans?

Posted by: Ron Kaminsky at May 2, 2011 2:08 PM

To me, this looks like some proof of concept both in terms of technological capability as well as a test case for the amount of legal flak such an action could draw. Short: I think they're creating a (dangerous) precedent.

Posted by: Dirk Praet at May 2, 2011 2:31 PM

Put me down on the list of people who don't like the idea of the FBI trying to shut down or running the botnet.

It seems to me there is no reason to issue a stop command to the zombie machines. Once the botnet controller is out of the hands of the people benefiting from the botnet, the only risk is that some other server might re-assume control. It would be more logical to monitor the botnet and use it to track down those servers and nail those guys rather than disable the botnet entirely.

What should be done is track down the zombie machines and send notifications to the owners (most of whom probably are easily identifiable via the IP addresses - these are almost all personal, university and some corporate machines, after all) and let the owners do the cleaning.

The remaining machines which are either not cleaned or not tracked down can be used as trojan horses to track down anyone who tries to re-assert control of them with another server or IRC channel.

As for the RIAA getting the FBI to do their dirty work, they already do. And the RIAA is known to have hired "security consultants" who hack into other people's machines and who spike P2P networks with false material. So, yes, I can fully believe they could do such a thing.

The FBI already uses a ham-handed method to seize domains they believe are used for "piracy". Anyone who doubts the FBI would love to be able to control every personal and corporate computer in the country is just naive.

Posted by: Richard Steven Hack at May 2, 2011 4:58 PM

Posted by: Richard Steven Hack at May 2, 2011 4:58 PM

The analogy is to public health. There are three methods of handling highly communicable diseases: preventive vaccination, quarantine, and forced treatment of infected persons. Vaccination is the least intrusive, quarantine is quite intrusive, and forced treatment is very intrusive and rarely done in the USA.

In this botnet situation, quarantine won't work because we cannot readily exclude infected computers from the internet. Thus, the choices are vaccination (installation of software that prevents botnet infections) or forced treatment of infected computers. Most computer users already have chosen vaccination, so why does the FBI believe that forced treatment is required? Also, how does it have jurisdiction over all the infected computers? Surely some of them must be located outside the USA.

Posted by: Dr. T at May 2, 2011 5:27 PM

I agree with Richard Steven Hack: stop the server and notify owners of the infected machines. Once the exact threat is known, it is not that hard to clean it.

Posted by: NZ at May 2, 2011 8:56 PM

@ Ron Kaminsky: "What flaw? That general purpose OSs should be able to run any program which the user desires? You do realize that it's infeasible to solve the general problem of identifying malware, don't you?"

Coreflood was identified in 2004 or earlier so the difficulty to solve the general problem of identifying malware is not related to this specific known OS vulnerability that is now being patched in 2011 by the FBI instead of by Microsoft.

Posted by: ant at May 3, 2011 2:11 AM

"I just don't see this argument convincing very many people."

I think it's a question of culpability. If Coreflood damages their machine, it's the hackers fault. If the FBI code damages the machine, it's the FBI's fault.

"The problem as I see it is the slippery slope." Absolutely. Or in other words, here we go again.

Posted by: bob at May 3, 2011 3:47 AM

This needs a legal basis. One comparison I can think of is that if somebody breaks into your house, the police is allowed to secure the door/windows/whatever. Another one I see is that firefighters are allowed to enter houses without explicit permission in order to fight fires. At least firefighters are also allowed to do substantial damage if needed. So some precedent exists.

Personally, I believe that the analogy between a hacked machine and a house/flat on fire is sound. The machine represents a serious risk to public safety. Of course the scale is different, but not the nature of the issue.

Posted by: Gweihir at May 3, 2011 4:41 AM

> next, the RIAA is going to want to
> remotely disable computers they
> feel are engaged in illegal file sharing

If the computers in question are infected with malware without the users knowledge and participating in a botnet at the behest of someone other than the computer's owner, and the RIAA wants to hit the malware's kill switch, I say sure, let them. I don't much care what their motives are. Shutting down malware is okay. I'm good with that.

If the computers in question were *not* already infected, and the RIAA wanted to conspire to surreptitiously infiltrate them (with, presumably, malware of their own) in order to stop non-malware-initiated behavior, then that would be a different scenario entirely.

Posted by: Jonadab at May 3, 2011 8:09 AM

@Gweihir "legal basis"

Once the FBI or any other LEA has access to a botnet and the end points that make it up they have access to the data the network processes and to the data on those machines.

Any data they uncover 'in the lawful exercise of their duty' that could point to criminal, or suspected criminal, activity would be a) acceptable to a judge to issue search warrents and b) admissable.

I think the temptation to exceed the 'just shutting down a botnet' scope for their mandate would be too strong and the SAs would fish around.

Say they came across a machine compromised in criminal activity. Would they shut down the RAT that is giving them access? I think not.

Posted by: BF Skinner at May 3, 2011 9:46 AM

@ant: Microsoft has been releasing Malicious Software Removal Tool with various coreflood removal mechanisms for years now. The trojan has mostly blocked it from running and also immediately updated itself with more undetectable code. When the FBI took control, Microsoft immediately released a new update that removed the current version, now that it will no longer be patched - but of course if it can't run, it won't work.

So the OS vendor _has_ already fixed it and it wasn't enough, now what?

Posted by: foxyshadis at May 3, 2011 8:27 PM

@ foxyshadis

You may defend Microsoft, and I'm familiar with all the tools you mentioned, but I feel it's incongruous for the FBI to be patching Windows servers. Next, the FBI will send someone around to repair my TV or refrigerator.

:-)

Posted by: ant at May 4, 2011 3:28 AM

@ ant

If your TV or refrigerator creates a risk for a large number of other people in multiple countries around the world then I would expect your government to take action to mitigate the risk.

Remotely updating a computer seems a lot nicer than the way most governments work when it comes to protecting public safety.

Posted by: Bruce Clement at May 4, 2011 6:38 PM

Read the novel This Is Not A Game for some discussioin of this tactical strategy.
We need a new word for a ubiquitous action prsuing ubiquitous local results.
Tactegy? Stractic? Anyone?

Posted by: Peter E Retep at May 5, 2011 1:38 PM

As noted, there appear to be 4 actors: End User, Botnet Operator, FBI and Anti-Virus provider. Without a clear onus for responsibility, I can easily contemplate using the command and control (seized) server/computer to simply distribute a dialog box to the effect "This is a Zombie machine in urgent need of re-imaging." It places the onus on the End User, but it doesn't crash these imagined essential service type boxes. If this doesn't steal away the peace of mind afforded by ignorance, it certainly alerts a majority of users adequately... doesn't it? OK, now that the candle IS lit, whose problem is it in a perfect world?

Posted by: pointless_hack at May 8, 2011 6:31 PM

The should fix the OS,if cyber criminals use bot-nets and the FBI tries to stop them, what stops a large group putting coreflood on there computer to find the f bi's IP address(monitor the software and large bandwidth) to target them.
The OS is probable the weakest link, but that would stop criminals and governments

Posted by: asd at May 15, 2011 5:44 PM

Subscribe to comments on this entry

Post a comment

Name:

Email Address:

E-mail is optional and will not be displayed on the site.

URL:

Remember Me? Yes No

Comments:

Allowed HTML: <a href="URL"> • <em> <cite> <i> • <strong> <b> • <sub> <sup> • <ul> <ol> <li> • <blockquote> <pre>

Preview **Post**

Powered by Movable Type. Photo at top by Geoffrey Stone.