Tackling the Growing Botnet Threat
Transcript

Part 1: The Threat

Julia Allen: Welcome to CERT's podcast series: Security for Business Leaders. The CERT program is part of the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. You can find out more about us at cert.org.

Show notes for today's conversation are available at the podcast website.

My name is Julia Allen. I'm a senior researcher at CERT working on security governance and executive outreach. Today I'm pleased to introduce Nick Ianelli, a member of the CERT Coordination Center. Today Nick and I will be discussing a growing threat that is reportedly more damaging than viruses, worms and other forms of malicious software, and what business leaders can do about it. So, welcome, Nick, glad to have you here today.

Nick Ianelli: Hey, thanks. I appreciate the opportunity to talk with you guys, as well as talk with everybody else out there.

Julia Allen: Great. Well, so let's talk about botnets, which I understand is short for robot networks. Could you tell our listeners what these are and why they're on the rise?

Nick Ianelli: Sure. Well, a botnet is made up of compromised hosts, which are commonly referred to as bots or zombies, or whatever moniker you want to give to these things. But the real point is, it's a bunch of compromised hosts, centrally managed or managed from multiple points, but they're logging into a location that's easily manageable.

It's hard to say with absolute certainty, why these things are ongoing and ongoing and ongoing, and rising. The simple fact is the code is out there, it's very easy to use, and if anybody has any questions, there's a free support staff – you can find them anywhere – to assist in trying to get these things to run, operate or exploit vulnerable machines.

Julia Allen: So when you say "compromised hosts," and you talk about the code, what that means to me is basically someone's taken a piece of software, one of these bot software packages, and actually installed them on a whole bunch of computers. Do I have that right?

Nick Ianelli: Yes.

Julia Allen: And then have an ability to control that in some fashion upon request.

Nick Ianelli: Probably the most popular command and control method that's being used is what's commonly referred to as IRC, internet relay chat. It's a text-based chatting program that's been around for years and years and years and years, and what they do is they have them log into these IRC servers, go into specific channels, and you can see all of the users within that channel by issuing a command in that channel. All of the compromised hosts that are there will respond and do the action requested of it by the person issuing the command.

Julia Allen: So is that one of the things that makes botnets so dangerous, this command and control structure, and why attackers find them so appealing?

Nick Ianelli: Yes, it's very easy to have them log into a central location, issue one command, and if you have a botnet of 1000 compromised hosts, have them all do the same exact thing at the same exact time.

Julia Allen: So how would an attacker find a compromised host to install one of these bot packages on?

Nick Ianelli: Well, they could buy compromised hosts from other attackers. There's what's commonly referred to as the "underground economy," where they have just a smorgasbord of items for sale – compromised hosts, stolen accounts, malware, botnet source code – I mean, you name it, they have it for sale. So there's the opportunity to purchase the stuff. Some of these guys even start with infecting their own machine or infecting a friend's machine, and then get that particular machine to start scanning the network for other vulnerable hosts. And once they have one, they just keep trying to look for other ones, and then once those get compromised, they're instructed to look for other ones, and it's just a ongoing repeatable process for them to gain more hosts for their botnet.

Julia Allen: So, it sounds like there's a fair amount of information sharing that goes on within the intruder community about this partic(ular) – I mean, obviously about many topics, but this topic in particular. Is that correct?

Nick Ianelli: Oh, heck yeah, it's amazing. These guys have no qualms about sharing information with other people, whether they're direct competitors or they're newbies or they're just your senior guys are out there. If somebody knows the answer to the question, or if multiple people know the answer to a question that's being asked, they don't hesitate to assist, provide information, to provide pointers, to even provide code to do what the person's asking to do.

Julia Allen: That's remarkable. Well, without disclosing specific cases, could you describe some of the impacts of a successful botnet attack?

Nick Ianelli: Sure. Probably the biggest impact is data theft or data exfiltration. Once a botnet gets on your machine, or compromises your machine, whatever you as the user has access to or whatever that system has access to, that malicious code now has access to. And these guys that are running these botnets understand that, so they've built in features that permit them to access all of the resources on that system. They put in key loggers, they look for specific files, they'll look for .doc (Microsoft Word) extensions, spreadsheet .xls (Microsoft Excel) extensions, and then what they'll do is, once they find this information, they'll upload it to a location, or they'll steal that information and send it to a central site where they can go and parse through it, and decide what they want to do with the information.

Julia Allen: So pretty much anything that I would be doing on my laptop, be it at home or in the office, if there is a botnet installed on my computer, they can see or access everything I'm doing.

Nick Ianelli: That is correct. And whatever you have access to – if you have access to network shares where other people store their back up their files, that particular piece of malicious code has the capability to potentially access that network share and have access to all those other files. All of your mail contacts, your address book, botnet malware has the ability to capture all of that. In addition, they have the ability to send email from your machine, as you, to the people that are in your contact address book.

Julia Allen: Boy, some pretty scary thoughts here, wouldn't you say?

Nick Ianelli: I'll say. I'll say.

Part 2: How Do I Know If There's a Botnet on My Computer?

Julia Allen: So, why is the infiltration of botnet agents on our computers so hard to control? It seems to me that, couldn't firewalls or anti-virus or intrusion detection systems be used to find these agents on our computers and eradicate them?

Nick Ianelli: In most cases I would say yes, as long as everything is properly configured and everything is patched, secured, hardened, and up-to-date. But if you think about it, botnets tend to propagate in two ways. The first way is like vulnerability exploitation, so they're actually going out looking for vulnerable hosts on the internet. Once they find one, they'll go ahead and try to exploit it. Now, what we see in analyzing botnet malware is that the vast majority of vulnerabilities they attempt to exploit have had patches out for them for the past, I don't know, three-four-five years. I mean, we're talking back in (20)03. They're attempting to still exploit vulnerabilities that came out in 2003-2004-2005. If people were to patch their systems, that wouldn't be an issue, those vulnerabilities would no longer work for them.

And the other way that we're seeing is just straight social engineering. If you remember before how I said I could send email as you to somebody within your address book.

Julia Allen: Right.

Nick Ianelli: Well, sending email as you adds an extra layer of confidence in the person receiving that message. So if I send something and say, "Hey, check out this attachment," or "Check out this Word document," and you do that without thinking about it, and you just double-click on that, there's a chance that you are going to get exploited or you're going to run a piece of code that could install a botnet on your machine, and now you're infected and you're owned.

Julia Allen: Right, because I assume since, let's say in our case, I'm assuming the email came from you, and so I trust it.

Nick Ianelli: Correct.

Julia Allen: And proceed from there without realizing that I've just done myself some serious damage.

Nick Ianelli: Right. Right, I mean, you have to in that particular case, you're probably wondering, "Well why didn't my AV catch that. There was malicious code in that email." You have to think of it in a way that attackers are in an arms race with the folks in the anti-virus community. What they'll do as an attacker is they will take a piece of code and they will try to obfuscate it in a way that anti-virus doesn't detect it.

There are sites out there, both public and private, where an attacker can upload his malicious code, get the AV results from ten, twenty, thirty-five different AV engines. He may be only concerned with a couple of them, but as long as they pass those couple, he'll go out and submit, or try to exploit with that piece of malicious code. Now if the majority of the AV's detect his code or the attacker's code, what he'll do, or what the attacker will do, is attempt to obfuscate it in another manner so that those anti-virus engines don't detect it.

Julia Allen: Right, so effectively it flies under the radar screen and no one's the wiser.

Nick Ianelli: Oh, exactly, and that's just trying to obfuscate it. Let's just say that this is a brand new piece of malware – the AV, anti-virus, community has never seen it. First off, they need to get a copy. If their existing signatures or heuristics don't detect it, they need to get their hands on a copy of this malicious code. They need to analyze it and then they need to make a determination, "Do I adjust an existing signature? Do create a new signature? Or do I adjust one of the heuristics to try to catch this?" Once they make those changes, then they need to push those updates down to all of their end users. And all that takes time, but all that time that that took, that botnet malware was now propagating, or just malware in general.

Julia Allen: Right, and that's a reactive solution because you're analyzing it after the fact, correct?

Nick Ianelli: That's correct.

Julia Allen: How can business leaders in particular determine if botnet agents are on their computers or their organization's computers and networks, and if they do locate them, how can they get rid of them?

Nick Ianelli: What they need to make sure that they have running is logging, and they need to have logging on all of their critical systems, all of their systems that may touch the internet or have internet activities pass through it. A primary example is if you have a router, you want to make sure that you're logging net flow data from that router, and then you want to see if you can correlate that data with any of your other, say your mail server, or your DNS (domain name system)server.

And see if you can correlate that data or even visualize that data, because there's a good chance that if there's a botnet or an infected host on our machine that's in a botnet, if you can quickly look at some net flow data, you have the potential of quickly seeing that there's a potential infection on your network. And generally what we see is once a computer's infected, it will attempt to try to scan for other computers and looking at that in net flow data visually, you'll be able to pick that out right away.

Julia Allen: In other words, if there's an infected computer in my network and it's trying to scan other computers, I'm going to see a real up-tick in the number of messages or the types of messages that that computer is sending out, right.

Nick Ianelli: You got it.

Julia Allen: Okay.

Nick Ianelli: Another thing that you might be able to look at doing is if your company has an authoritative DNS server – so if you're machines are configured to ask your company's DNS server first how to resolve a DNS name or a host name, what you could do is you could set up some type of logging there, where you're looking for anomalies, or oddly looking domain names, and you can alert on them. You don't have to drop the request but you can alert on them and then just manually review them.

What we see with botnets – their DNS requests, the DNS names, the host names are quite odd and obvious. So seeing a list of today's DNS names that people looked at minus the obvious ones, and you can create a baseline and just move those out of way, but that's a pretty good indicator of a potential infection as well.

Julia Allen: Okay, so taking that kind of preventive monitoring action before things get out of hand.

Nick Ianelli: Yep.

Part 3: And What Can I Do About It?

Julia Allen: Let's say that I have found this kind of activity through my logging or using an authoritative DNS kind of service. How can I get rid of these guys?

Nick Ianelli: Well, your best bet is going to be to try to locate all the critical files on the system and pull them off or back them up, and then you're going to want to scan those files that you want to keep. And your best bet to ensure that your computer's clean, there's nothing else on there, is really to just wipe it and start from scratch. Rebuild the operating system and then load all of your applications, or load all of your files back onto the system after you ensure that they're clean and they're not infected. I mean it's really the only way that you're going to know that your machine is no longer infected.

Julia Allen: Okay, well that makes good sense, so basically doing a thorough house cleaning.

Nick Ianelli: Yes, yes.

Julia Allen: So, we've talked a little bit about this, but are there any actions that business leaders and other users can take to get in front of this a little bit, to both prevent and to detect further infection? I mean, you had mentioned, obviously have your patches be up to date.

Nick Ianelli: Sure. I mean, if you take the whole defense-in-depth approach that's a great starting point. So you want to raise awareness both with your upper management, senior management, as well as your employees. You want to make them aware that this type of activity is occurring and when this type of activity occurs, what are the potential losses that both the organization and the individual can suffer, because not only can the organization suffer, but if the individual is going to a website and a key logger's turned on, and that website just happens to be their personal bank account, well now that information could be exfiltrated off the system and the attacker could have their hands on that.

Provide education and training classes. They don't have to be anything in-depth – maybe a lunch training, just to continue to keep this fresh in the people's minds. If they're doing the right thing at work, they're generally going to do the right thing at home. So again, that just makes the internet a better place for people to surf and visit.

And as you already mentioned, making sure all of your patches and your software are in place and up-to-date. And if you need to test before you apply a patch, just know that. Come up with a plan, or have a plan ready, so that you can secure that system, lock it down as tight as possible, so that until you get that patched, your services aren't down but you're actively monitoring this to make sure that nobody's actually exploiting it.

Julia Allen: Right. Because it occurs to me as the attacker or the intruder community are looking for vulnerable machines, if my machine is well-patched, up-to-date, securely configured, they're going to go somewhere else, right?

Nick Ianelli: Sure. Sure, I mean, that's the beauty of botnets. Once a botnet logs into whatever command and control mechanism that's in place, and as I mentioned before, IRC is one, HTTP is another. These things go over a port 80 TCP, so you've got to filter both inbound and outbound requests. And then you have the infamous peer-to-peer malware, such as the Storm worm, which operated on what appeared to be an edonkey peer-to-peer traffic.

So, yeah, you need to watch that because when these things log in to their command and control server, if the command is to scan for a particular vulnerability, they'll continue to scan for as long as they're programmed to, and that generally can mean hours, days, weeks, whatever. So as soon as that machine is compromised, they log into this IRC server; next thing you know, they're out scanning the entire internet, whether they start with your network or somewhere else, they're just scanning away.

Julia Allen: Right, so one of the best preventative measures is to make sure that they don't stop at my computer in the first place, right?

Nick Ianelli: Right. Right, and again, if you're raising awareness and providing education to your employees, the chances that they're going to get infected at work are slimmer, and the chances they're going to be infected at home are slimmer as well.

Julia Allen: Okay, well so if I do get in trouble, are there certain organizations I can contact and where are some good places to learn more about this?

Nick Ianelli: Well, the first thing you want to make sure that you have contact with, or relations with, is your upstream internet service provider (ISP). You want to make sure – you want to know who to call and when to call before you actually have a problem. Because when you have a problem, the last thing you want to do is fumble around and be like, "Oh, man, where is this number? Who do I call? What line?", because the important thing is time. If a machine on your network has been instructed to perform a DDoS (distributed denial-of-service attack) against another company, you're going to want to get that shut down; or if there's a DDoS against you, you're going to want to make sure you get that shut down and your ISP is going to be your best friend in that case.

Knowing where to submit malicious code – so let's say you found malware, botnet malware on your machine. Well, now what do you do with it? Because the anti-virus companies that you have in your network don't detect it, but you know something's fishy, something is going on with that code. So where do you send this, what do you do? Knowing what to do with that information, again, it's all about time.

Another thing is, I'm not aware of any specific companies, but if you don't have an in-house shop, again, you're going to want to look externally, and you're going to want to do that before you get into a crisis, because again it's all about time. In a time of a crisis you want to make sure you have a game plan already set, or at least something flexible that allows you to move around, but just some milestones, so to make sure that you hit them.

Julia Allen: Right, so again, another good preventative measure is to have these kind of incident response contacts and procedures in place, so that you can use them when you need them.

Nick Ianelli: Exactly. Being prepared ahead of time is going to save you a lot of time in the long run.

Julia Allen: So do you have some sources you'd recommend where our listeners can learn more about botnets?

Nick Ianelli: Sure, if you visit www.cert.org, there's a keyword search – you can search for botnets, spyware, and phishing. www.us-cert.gov has some information for various audiences: technical, non-technical, the sysadmin (system administrator). They also have a current activity section that highlights some of the big things that's going on on the internet. Honeynet website, which is www.honeynet.org, has some great papers in a series titled "Know Your Enemy," where they try to

highlight some of the big things like botnets and phishing and such. And then you can find some general situational awareness if you monitor popular blog sites like Websense or Sunbelt. Arbor has an atlas dashboard which gives you a general summary of what's going on. And the SANS Diary is more like a current activity as well. So those are some good resources to check out, just to try to grasp what's going on, on a daily or weekly basis.

Julia Allen: Well, Nick, this has been very insightful and educational. I've learned a lot just in the short time we've been talking. I know you've passed on lots of good comments and ideas to our listeners and I look forward to talking with you again.

Nick Ianelli: Great. I thank you very much. I appreciate the opportunity.