NETEVENTS

GLOBAL PRESS & ANALYST SUMMIT "INNOVATORS IN CLOUD, IOT, AI & CYBERSECURITY"

DRAFT

Conference Debate Session VI
The Insidious Danger of Botnets: They Are Everywhere. They Are Multiplying

Chair: Mike Spanbauer

Vice President of Research and Strategy, NSS Labs

Panellists:

Peter Brecl	Director of Product Management, Security Services, CenturyLink
Wayne Burke	Technology Research Innovator, EC Council
Cricket Liu	Chief DNS Architect, Infoblox
Arabella Hallawell	NETSCOUT Senior Director, Strategic Marketing
Michael Levin	Former United States Secret Service - Deputy Director, US Department of Homeland Security

Mike Spanbauer

So welcome back from the break, folks. I have the good fortune of introducing a topic today that has certainly made headlines for the last few years, more prominently recently due to significant service interruptions, but that topic is Botnets. So our intent today isn't to cover all aspects or facets of it. It would be impossible in this short period of time, but rather just generally educate on where we are relative to them, improve

awareness and also where are things heading and how can we all contribute in a positive way to improving the security position? So I have an incredible group of panellists, whom I will introduce here in a moment. But before we get into who's on the panel, I will set the stage with respect to some of the basics and introduce really at its root what are Botnets.

So the robot concept obviously is a bit of a joke here - is, in an individual instance, and really the concept of an infected machine that is uniquely or individually not particularly exposed or at high risk. The issue is that a Botnet is a large group of machines that are all centrally controlled, often by one threat actor or a function and through that central control can wreak great damage to any number of targets or opportunity - you know, value resources. So - and why they're an issue is because ultimately Botnets are incredibly highly distributed, right?

Infections often leapfrog from one to the next via remote access kits or other means or, as you're probably well aware, some of the vulnerabilities that have been disclosed over the last 24 to 36 months and obviously our race, as we've already talked about, with connecting devices to the internet, IoT and it's whether consumer or commercial, have revealed - and directly connected access for criminals to compromise these nodes. So in the case of Mirai or other nets, they are, at the time of installation, the consumer is basically leaving pieces unconfigured, default passwords and with the vulnerability in place that allows me to easily attach, compromise, leave it and attach it to the greater network there.

So, at its core, it becomes a sinister mechanism that's deployed globally. This is the root challenge, right? It's not that you can take one specific instance, one infected machine. It is a group of elements all connected and for one particular purpose. By way of a bit of history, the number of Botnets that have become public over the last six to - five to 10 years are varied. These are just a handful of the most prominent Botnets by name that have been both been identified and the majority taken down over the last few years. So the - you know, the activities that Botnets ultimately drive vary widely, right?

It's from simple denial of service, basically just a brute force overwhelming a particular resource and/or resources, such as the Dyn attack, where the name servers were taken offline and some very prominent websites/companies were affected by that, to cryptojacking/cryptomining, taking over the WordPress pages and the instances where they're capitalising on your resources for their own profit, their own gain, mining coins. Now, really the diversity of potential bots is any connected device that has some processor, some capability and ultimately a vulnerability with which they can install their code on and take advantage of the unit. At the bottom here, and this is particularly interesting and something we'll talk about a little bit here on the panel is the economics.

So the direct effect of what a Botnet does to a specific target is costly, but it's not just that the specific target is affected, but all the other services, indoor customers that in scope for disruption or an attack. Those costs, I mean, best measures, three, five, 10 x the direct effect and the economics are just incredibly scaled to the point where Botnets cost a great deal more than I think we even capture today. So the questions we're going

to address and talk to some degree about are - so where are we right now? How do we get here? Then also the debate on what's being done now? There are a considerable number of efforts, our panellist contribute to these today, of effective means by which Botnets are being addressed. Then we'll talk a little bit about what does the future hold and where can we go from here?

So with that, I'd like to turn over to the panel. I'll allow each of them to introduce themselves briefly and we'll start on it. So, Wayne, do you want to go first?

Wayne Burke

Yep. Good morning, folks. My name's Wayne Burke, yeah, representing EC Council as the research innovator for technology, new technology, and our focus is really to try and encourage new up and coming interns that are coming into the industry to get involved with building these new networks with neural networking, blockchaining, artificial intelligence, so it's really bringing new skills to the industry.

Mike Spanbauer

Peter.

Peter Brecl

Right. Hi. My name is Peter Brecl and I'm a director of product management for security services at Century Link. Century Link is one of the largest internet backbone operators globally. So with that, we have a unique visibility into what's happening in the world of Botnets, command and control infrastructure, et cetera, and we are heavily involved into collecting that information, sharing that information with industry peers and then taking proactive steps in helping our users, as well as other internet users, have a better internet experience by impacting and taking those command and control infrastructures.

Mike Spanbauer

Thank you.

Cricket Liu

Hi, good morning. I'm Cricket Liu. I'm the chief DNS architect at Infoblox. I'm probably the only chief DNS architect in the room, I guess. Nobody else wanted that title. Infoblox is a DNS and DHCP company. We provide DNS/DHCP and IP address management products and infrastructure to 9000 big organisations around the world, including 90 per cent of the Fortune 100.

Michael Levin

Morning, everyone. I'm Michael Levin. I'm the CEO of the Centre for Information Security Awareness. We provide security awareness and compliance training to businesses of all sizes. I'm a former Secret Service agent, retired from the US government after 30 years of service.

Arabella Hallawell

Hi, I'm Arabella, with NETSCOUT Arbor. For those of you who aren't familiar with Arbor, the company started in 1999 actually helping the very first organisation with DDOS attacks and really helps the world's networks from service providers, enterprises, organisations around the globe with some of the most largest and most complex cyberattacks. I guess, we've seen DDOS from when it was just a baby to now with over 18 years' experience as an adult. DDOS has got a car and an apartment all of its own. So excited to join the panel and talk about some of the very exciting, as well as pretty threatening issues, around DDOS and Botnets today.

Mike Spanbauer

Well, thank you, all. So let's go ahead and start off with just sharing some thoughts with regards to what are the challenges and particularly how did we get to where we are? I mean, that - I don't want to go into responsibility and blame exactly, but I'd like for folks in the audience to understand that it's not one specific problem, one specific point. So, Mike, maybe or Peter, if you want to - you guys want to start off. Where did we get to or how did we get here today?

Peter Brecl

So let me start. So from a visibility that we have utilising the network as a sensor, we're seeing obviously continued growth of the Botnets. The way I kind of like to think about them is I would - I'm going to categorise them into two groups. The first group is just traditional, let's say, computers we have at home. I think the landscape there is getting better. We do see the growth of the Botnets, but not at the pace that we see it in the second group, which is I'm going to call the internet facing services. Think of it, IoT devices that you see in that second group. The first group, the reason why I'm making a statement is that things are getting better is you have more awareness, better patching, [UCAT / you've got] user education, you do not click on this, et cetera. So the window of the opportunity for a malicious actor to infect that machine has shortened over time.

So if you're the malicious actor, you're going to go after targets that are easier to compromise, so that brings me now to the second category, which is the - let's call it the IoTs. We've discussed already in some of the previous presentations there's an extreme growth in that area. So that's the first aspect of it, so we have the addressable targets are plentiful. Then the second part is the patching. How often do the home users thinking about, "Do I need to patch my video camera that is exposed on the internet?" et cetera.

Then if you layer on top of both of those categories, the new approach of distributing and compromising machines using worms and utilising the actual compromised machines and IoTs to spread, that gives the bad actors the - I'm going to call it the amplification factor, where they use the numbers of the compromised machines to even compromise most - more machines, so that's why you see in that second category significant growth.

Michael Levin

One of the things that I am focused on and what we try to do as far as education is the concept of what is the real risk and with IoT it's amazing to me - and when I say the

risk, I'm talking about the risk maybe to the critical infrastructure in every country throughout the world. We have so many vulnerabilities currently and we're so fixated in the EU and in the US in our senate right now about Facebook. Everybody is so worried about the data thefts occurring potentially in Facebook; we have far much more risk on IoT devices than anything that's occurring in Facebook, in my opinion, to the critical infrastructure and to the physical safety and security of our society.

So from my perspective, it's much more dangerous than the other privacy rules that we're worrying about currently.

Mike Spanbauer

I'd like for one on the panel to take the vendor challenge of the IoT devices, the consumer space, the routers that have been shipped, having to serve two masters, so the passwords default out of the box satisfying easier user installation, right? My parents won't go through reconfiguring an entire stack of technology, but the issue is that the attackers now know and can compromise us, so what can be done or how many devices out there could potentially satisfy both angles? Is there anyone…

Wayne Burke

I think if I want to just respond from the perspective of the sheer mass of people using all these different services right now, that we realise artificial intelligence is ability for a computer to be taught something. So just as we're seeing an exponential growth in attack vectors, we're also starting to see an exponential growth in Dr Watson. Right? So you're going to be using artificial intelligence to be able to consume more data, to make more intellectual responses to events that take place. So it's not all bad. It's about adapting to the new technologies by teaching the younger generation new skills. So the fundamentals are still there. Just because we're using neural networks, doesn't mean to say we're going to forget about fundamental physical networking from the good old says. We've still got to build upon that bid; we're able to do it from multiple different layers now.

Mike Spanbauer

Arabella, you mentioned earlier around that it's not just about the distributed service attacks. The resilience and the ones that are high profile, that are, I know, aggregate but rather also the application layer in threats and attacks and the risks that they pose to businesses. Do you want to add some colour around that?

Arabella Hallawell

Yeah. Sure. I think it sort of goes back to Michael's comment about risk. For many organisations and even consumers, when we talk about IoT devices that we have in our home, many people think that DDOS and Botnets are someone else's problem. Someone else will deal with that. We're not really responsible. I think as we have this discussion, it's - I think what's clear, and as Michael talked about, it's a - very much a global problem, as we will get into, but in terms of specific vectors of attack, we often hear about things, like Dyn, which obviously was a watershed moment in terms of exposing the fragility of all these organisations that use key infrastructure services. We saw some recent attacks.

The memcaching attacks, which were huge big, what are called, volumetric attacks that obviously again threatened core infrastructure that we often rely on. But what's interesting when you look at the DDOS attack landscape is the biggest change is really around application layer attacks being the biggest new source of these DDOS attacks, as well as what are called multi-vector attacks. So enterprises today experience almost half of their DDOS attacks of this vector and the majority of them really aren't protected against them. So I think this goes back to Michael's point around does everyone really know their risk and also their responsibility in the ecosystem and what they need to do to potentially have better practices, not just to protect their own organisation or their own, but our global connected world.

Mike Spanbauer

Thank you. So let's shift then to successes we've seen at combating Botnets to date, as well as from those promises what might the future hold. So I want to start with you, Cricket, just with regards to what are the actions and your company's intent? I mean, you've got a fair interest in helping combat this, so go ahead and please share with the audience.

Cricket Liu

Well, it'll surprise no one that we take a DNS centric approach to addressing this, but one of the things that you can capitalise on is that any Botnet, regardless of how the Botnet came into being and how the devices that are part of the Botnet were originally infected - all Botnets want to communicate with commanding control infrastructure, because they need to figure out what it is that they're supposed to do. Who it is that they're supposed to attack, whether they're supposed to mine Bitcoin or attack their neighbours or scan the file system for interesting looking files that might contain credit card information or whatever. There's a lot can you do there, because the primary method of communication between any infected device in the internet is DNS, right? That bootstrap is basically all of that CNC communication.

To the extent that the Botnets reuse a lot of the same command and control infrastructure, a lot of times we activity have reputational data. We know, for example, that certain domain names are the Botnet infrastructure for a particular Botnet or a particular IP addresses are or we understand, for example, the domain generation algorithm that a particular species of malware uses to communicate with its command and control infrastructure. So we've been working on instrumenting DNS infrastructure to attack those queries and to say, well, if you get a query for a domain name that's obviously somebody's command and control infrastructure, you shouldn't answer it, which is what DNS servers have been doing for the last 30 years. So we're beginning to change that.

Mike Spanbauer

All right. So I know that others on the panel have an interest in what you've seen, what you've already implemented and how you're approaching it and perhaps, Peter, I know you play a fair role in this endeavour as well, so…

Peter Brecl

Yeah, absolutely. We take a very active role in that space and maybe just adding to what Cricket stated. So obviously there's the IP based and the domain reputation associated and that's only one of the fundamental elements on how we tackle the problem, but as we use the network as a sensor, we actively engage with the parties that are potentially hosting those malicious command and control infrastructure, notify them and if the notification, the takedown of that infrastructure, is not successful, we do take proactive steps and we disrupt the communication between the compromised machines on the internet and that command and control servers, so that - we refer to that as a C2 takedown and we've on average in a given month we are now taking down somewhere in the neighbourhood of 40 command and control infrastructures every day.

That could be IP based. It could be domain reputation based and the attackers will then react to that and move, for example, to a different command and control infrastructure. But if you think about from a security space, everyone always says the attacker has to be right once to compromise your network. You have to be right 10,000 times or whatever the number, pick the number, right? So when we take proactive steps by taking down the command infrastructure, it's actually a very painful exercise for the attacker. If you've aggregating, let's say, 10,000, 100,000, 200,000 compromised machines and all of a sudden you've lost communication to that, that cost them resources and money, so it's an effective way to disrupt their activities. Yeah.

Mike Spanbauer

So it brings me to the question of should we wait for government to regulate or does private industry play a role here? There was a fair number of opinions and certainly there's no one right answer, but I'd like to start with perhaps Wayne, if you want to comment at the beginning and just regards to who do you think should take action or what's perhaps the best next step, you know?

Wayne Burke

I think it's pretty clear that the government are making some pretty large initiatives already with incentivising new programs, STEM programs for kids to get involved in computer programming with Raspberry Pis and smaller computers. That - that's how they did it in England, right? A lot of the English were losing interest in going to university and getting a degree in programming, so as the ecosystem in the United Kingdom is very reliant on programmers for the gaming industry, we started seeing how they were incentivising the younger generation to come to enrol in university programs. So building a Raspberry Pi that you could then go along and pretty much add everything you want to, to do so many different things, it's changing how we all went to school 15, 20, 25 years ago. When we were at school, it's completely different now with the younger generation. So we've got to basically be educating them with the assistance of the government, and I believe they're doing a fair about of work, but there's obviously always more room for extra work.

Michael Levin

I'll just jump into this. From my perspective, we obviously need a multipronged approach with governments providing the direction and guidance to help the public and

private sector to tackle these issues. I think the talent is obviously there. We have the ability to solve these problems. Then the next piece of the puzzle is the end users, right? The people that are connecting the devices, how do you educate them to make sure that they understand the risks and vulnerabilities. And then lastly the process has to be continuous. We can't just say today that we now understand how to protect all the IoT devices. We have to have an ongoing process where there's this collaboration amongst the organisations to move forward to protect the critical infrastructure.

Cricket Liu

I think that - I'm sorry. Go ahead, Arabella.

Arabella Hallawell

Yeah, no. I was just going to just quickly jump in, because there is some recent work that's been done actually here in the United States. About a year and a half ago, an executive order came out around protecting the internet against Botnets and basically distributed threats. It was pretty interesting, so the Department of Commerce and DHS issued their initial draft report at the beginning of the year and if you look at their core points, they really reinforce this concept that (a) it takes a village. They didn't just talk about obviously there are some effective tools out there for protection and mitigation, but few people use them. But they also mentioned things like the role of the SDLC, making sure you actually design better security in, as well as the fact it's a global problem.

So I think just one point is it is important. I think that regulations can put in place new market forces; sometimes there's new incentives, even just for the government to maybe show best practice, but DDOS and Botnets by their very nature, and as Michael said, really is a global problem, given all the devices out there, all the infrastructure out there, that always needs to be protected. One organisation and one government alone can't solve the problem.

Mike Spanbauer

Right - and Cricket.

Cricket Liu

I was just going to say that I think that there is really room for regulation, if not legislation, particularly in the area of getting a grip on IoT security. I think that the manufacturers who are responsible for general purpose computers, for regular IT equipment, pretty well have a handle these days on system security. It's not perfect. I mean, there are always going to be flaws. I think one of the real opportunities is to address these IoT manufacturers who may be have not traditionally been in the business of producing internet connected devices. So they're just getting into the game. It's an industrial application control company that feels like they have to compete with Nest, for example, so they hire some folks to slap a TCPIP stack into an existing device. They have no idea how to deal with out of the box security. They don't know what sort of threats they're going to face on the internet.

There, I think, has to be some sort of regulations that control that and that as a result give the consumer hopefully the ability to choose devices that actually have good out of the box security, that have randomised passwords, rather than the same default password that all of the CCTV cameras and DVRs that were enlisted in the Mirai Botnet had. That way, at least, you could pick up a box at Fry's or Best Buy or whatever and you could look at it and you could say, oh, okay, this meets at least these minimum standards and I can expect that if I put it on my network it's not going to be compromised in five or 10 seconds.

Mike Spanbauer

Right. This brings up, in fact, a point that you brought up earlier, Arabella, which is this [unclear] developmental lifecycle, sharing best practices from secure coding vendors, folks that have been doing this for a long time, building more robust, hardened technologies and sharing that with the IoT community and vendor [ecosystems], so they can not have to reinvent the wheel and take advantage of practices that ensure that that thought is [applied] at the beginning of the SDLC as opposed to now we've shipped all these devices. They don't have enough memory to actually upgrade; that vulnerability will persist until that device ages out, which leads to a different challenge. So all very, very good points. So, with that, we're going to offer folks a bit of closing comments and then we'll open it up for a couple of questions. Anyone want to sort of take the final closing bit or…

Michael Levin

One of the things that I deal with every day is the end user and we cannot rely on the end users to take the initiative to solve this problem. We - it's almost like in the US we have these warnings on cigarette packs and do we have to put a warning on every IoT device that says, warning, this will - this device will cause you risk if you don't pay attention and upgrade firmware or turn off the wifi or the Bluetooth if you're not using it. Our users don't understand that and until we figure out a mechanism to educate people better, the problem will continue. Unless the manufacturers are voiced, which will never happen, to do certain things, the end user is still left holding the bag trying to figure this out.

Mike Spanbauer

Yes, no. Accountability.

Wayne Burke

I think Google are doing some good things at least. When you look at Android, the vendors themselves are really very poor in updating their systems, so Google are now changing the entire architecture to almost force the vendors that are building their products on Android as an OS, they're actually forcing them to update their products much quicker now. So the entire Google architecture within Android, they're making it very much more compartmentalised so you can update your Android older device much quicker. The vendors in the past were too oblivious to, well, it's not going to be updated, because it's an old phone or a tablet and so why do we want to waste more

money on it? But you'll see where Google are actually making the changes to almost force the manufacturers to come to the table.

Mike Spanbauer

Yeah.

Arabella Hallawell

Yeah. I think just real quick, kind of based on that and I think going back to the other point that especially with things like IoT devices, which really are a game changer in terms of the vulnerability they can cause for this kind of problem, I mean, essentially it's very hard just for (a) manufacturers to get those types of regulations put in place, but we talked about Best Buy, which is mostly - obviously here in North America, but when you think about all the manufacturers that are basically global, I think one of the earlier panellists talked a little bit about Amazon and Jeff Bezos, but it client have to be something like if something is going to be sold on an Amazon marketplace, are there any warranties around security, because IoT devices are that much of a problem, I think, for a lot of consumers.

Mike Spanbauer

Very good points. So with that, let's see if there's any questions in the audience. Obviously a diverse topic, so, please.

Audience Q&A

Davey Winder, The Times SC Magazine

Hi, Davey Winder from the UK. I write for The Times SC Magazine, amongst others. I'm interested in the panel's opinion on Botnet evolution, bearing in mind that the Fortinet Q1 report just came out and suggested that 58 per cent of Botnets are done in a day and gone. Yet, also at the same time, we've got things like Hide and Seek and the Wicked Mirai variation that have brought persistence to the party. Can the panel discuss maybe how persistence changes how you look at mitigation for Botnets.

Mike Spanbauer

So just to clarify the question, you're looking for guidance or feedback on persistence and its influence on securing and taking them down. Okay. Time to take down and so forth. So, Peter or Cricket, do you want to take first crack and/or - Peter?

Peter Brecl

Yeah, I can start. So we focus on a specific Botnet tracking. In terms of persistence, what we've seen and we've published that in the 2017 report is, for example the Mirai Botnets, the persistence of a given Botnet is anywhere from one day to in the 80 days range, whereas, for example, there's another variant called [Gafget] Botnet. We've seen

persistence of that Botnet being roughly 50 per cent higher, even though it's an older variant from 2014.

Davey Winder

I'm thinking more about these new variants that now survive [unclear] Wicked Mirai variant.

Peter Brecl

Got it. So you're saying if the end point that is compromised survives a reboot, what's the persistence on that? Yep. So from a global service provider perspective, when we do a command and control takedown, the survival of that reboot does not necessarily matter, because we insert ourselves in between the communication, between the compromised machines and the command and control and disrupt that communication. Now, what that actor is going to do is going to move that to a different infrastructure and try and re-establish communication again. Now, based on using the network as a sensor and the visibility around that, you can clearly see the patterns of compromised machines that you know about from before re-establishing communication to [unclear] so we basically repeat the same takedown there.

So some of that persistent malicious actors may force us to do a lot more than 40 takedowns a month that I was talking about, but it's really kind of an ongoing exercise. It's not going to necessarily go away, but we can impact their ability to operate and so we use that, for example, as one of the layers of, coming back to your DDOS comments, one of the layers of mitigation against denial of service attacks is rather than sending it through a scrubbing centre and analysing what's good, what's bad. It's just take down the command and control infrastructure that is attacking the particular user.

Mike Spanbauer

I want to be sensitive to time, so I don't mess up the schedule today, so - I just got the cane mark, sorry. So I want to thank the esteemed panel for sharing with us their perspectives on this rather challenging issue we face, but there is a future. So thank you all. Please give them a round of applause.