SAN JUAN – How It Works: Understanding DNS Abuse
Saturday, March 10, 2018 – 13:30 to 15:00 AST
ICANN61 | San Juan, Puerto Rico

UNKNOWN SPEAKER: March 10th, 2018 How It Works Understanding DNS Abuse, Room 209BC 1:30pm. [AUDIO BREAK]

CATHY PETERSEN: Good afternoon, welcome everyone. Sorry, that was quite a start, did I just wake you up? Welcome to our second How It Works Session for the day. We will have John Crain, who will talk about Understanding DNS Abuse. John?

JOHN CRAIN: Thank you very much, you can all go back to sleep now. I'm John Crain, I'm ICANN's Chief Security Stability and Resiliency Officer, just a very long title. Basically, we deal with all things related to the security, stability and resiliency of the identifier systems and today I'm going to talk a little bit about DNS Abuse or how the DNS is abused. Hopefully our technology will work. Let's start by talking a little bit about what is DNS Abuse and DNS Misuse.

The first thing is there is no globally accepted definition of this. People hear this terminology and they think it's like something that's clearly defined because it's DNS Abuse and the answer is, well not really. Different people have different definitions of what DNS Abuse is. Some people think that all cybercrime that uses a domain name, which is pretty much all of it. Is there for DNS Abuse. Hacking of registration systems could be one or malicious conduct that uses names.

When you look at the DNS or when we look at the DNS, we tend to look at the data and the infrastructure that provides the resolution services or the name registration services and we worry about corruption of that data, denial of service against that infrastructure and some people also worry about the privacy of that data. There's a lot of discussion at the moment in the internet engineering task force about how we can protect privacy of DNS data, there's also a lot discussion about privacy of data in the how is systems or the systems we use to publish information about registrations which is not actually the DNS itself, it's a different protocol.

We tend to refer to misuses when people are being deliberately deceptive or conniving and doing unsolicited activities that use the DNS. In simpler terms, DNS Abuse pretty much refers to anything that attacks or abuses the DNS infrastructure or DNS misuse, we tend to use that term in anything that exploits the DNS, the protocol or the registration of names.

Why do people decide to abuse or attack the DNS? That's pretty straight forward. You use the DNS for pretty much everything you do online. It's also in some ways a fairly easy target. If you disrupt somebody's domain name resolution, i.e. you can no longer get the IP address from www.business.tld they have no business, you need the DNS to get to those websites, that's why it's an interesting target to exploit. You can do various things to confuse and misdirect users.

Common attacks include things like fishing, where they may use a domain name that looks very similar to another one. Various vectors for actually exploiting the DNS. You can maliciously register a name, i.e. a register a name purely for an activity that's abusive, fishing is often a case of that. You can actually highjack name resolution and there's various ways you can do that. Of course, you can always corrupt the data either on the wire or by attacking those registration services.

All elements of the DNS, hopefully some of you came to the How the DNS Works earlier, are subject to attacks, that can be the resolvers themselves, the systems that are asking and answering the questions, the authoritative name servers. It can also be the caching resolvers and it can also be the client or the stub resolver that's on your machine. Of course, it can also be the registration systems. If you think about the stub on your machine, the resolver on your machine, that can of course be affected by malware and things like that. The caching resolvers, not so much these days but in the past were occasionally hit by what we call 'cache poisoning attacks' and I'll come to those in more detail in a little bit.

We have this little chart just to give us an idea of where these various parts can be attacked. If we're looking at the resolvers, obviously if you can't access the machine, it's not going to work. We hear a lot about denial of service attacks these days, or distributed denial of service attacks, they're very scary sounding, in many ways they're actually very scary.

The latest numbers we were seeing in the news of attacks where in the 1.7 terabit of data. Who here has a couple of terabits of data into their network, bandwidth into the network, apart from you in the back there, I know you do. Most people don't. That's denial of service or prevention of getting to the system or the network, their access to the network in super large scale. A scale that most businesses can't deal with.

Of course, the actual devices themselves are subject to attack. The name serves have hardware which may have bugs. They have software on them and as well know, all software has bugs. We may not know about them all yet but eventually we'll find bugs in them. The operating system, the name server software, the cache itself, the memory ware where we remember answers is subject to attack. Then there's the administration and configuration of those systems. If people are touching them, then obviously people can be lead or mislead to make mistakes or they can just make errors that open up problems.

Let's have a look at some examples of some of the things that we've seen that can define as DNS Abuse. I'm going to go throw a few different types of attack here. The first one I'm going to talk about is DDOS as we just raised that. DDOS stands for Distributed Denial of Service Attack and basically what you're trying to do is fill somebody's pipes, their bandwidth or the resources on the server. The DNS lends itself really well to this. Because it's what we call 'UDP Transaction' you can actually send packets and pretend to be somebody else. You can say, "Hi, this is a DNS query. I'd like you to answer and I am Cathy." And then if you're the name sever, you'll send all those answers to Cathy.

Now, when it's distributed and we have hundreds or thousands or tens of thousands of machines sending these queries, that means you can send a lot of responses back to somebody who never asked the question. Of course, it doesn't't' even have to be a name server, you can send it anywhere if it's filling the pipes to that network of that service, be that a web server or whatever it is, people can't get to it anymore. As I said, we saw one of these at 1.7 terabits per second, that's a large attack and we're seeing an increase in the size of attacks, they're just completely going up all the time and of course that means that everybody has a provision for that, it's a bit of an arms race.

One of the ways you can do this is to use something called an 'open re-curser'. We have big open re-cursers that are run by large and responsible internet service providers and the most well-known one is probably 8.8.8.8, which is operated by Google and they have lots of things in place to prevent this happening with their service but there's also a lot of these open machines that will answer queries for anybody out there on the internet that are even not as well provisioned or secured or in fact in many cases the operator of that doesn't even their doing it.

If you discover these you can send them queries and they will answer back to whatever you deiced the target it. Very, very large amounts of data. This is that in a graphical representation, so you have the attacker sending DNS queries, multiple machines. If you look at the size of botnets these days, botnets a robotic network basically compromised machines with malware etcetera that have controlled from organization or individual, a bad person normally.

If you've got 100,000 of these machines sending queries, the people who own those machines don't know this is happening, sending one or two small DNS queries is not something they're even going to notice, you send them to an open re-curser and they answer with a much larger DNS response and if it's 100,000 queries, that's 100,000 responses. If it's a million queries, that's a million responses. This happens in the wild all the time. Not all attacks are of that scale, in the terabits. There's also a lot of smaller attacks. Obviously if you have a smaller network, they don't need to send 1.5 or 1.7 terabits of traffic at you, they can probably take you down with a few gigs.

Another way of doing this with TCP, if DNS is UPD, which is a sort of fire and forget mechanism, TCP requires you to actually have a handshake between the machine that sends the query and the response. If you lie when you start the TCP session in a packet or a sin, you'll get an acknowledgement back. If you're the victim in this case, you're not seeing necessarily UDP packets or DNS answers coming back to you, you're seen acts or acknowledgements from the server and that will quickly deplete your resources.

Once again, this can be in the tens or hundreds of thousands of packets coming your way. If you're doing this against DNS, you can do this with DNS message over TCP. Now people often think that DNS is just UDP but by protocol it's not and there's actually very good reasons for allowing TCP to work. It's the fall back for larger queries. It's not as common an attack type but we do see it in the wild.

Poisoning a cache can happen in a few ways. Often people think about somebody sitting on your network and trying to get in between a man in the middle of the attack if you like, on your DNS queries and sending an answer faster than the actual legitimate DNS server.

The idea in this case is that I send you a legitimate looking spam message, everyone knows I need to lose a little bit of weight, they send me the lose weightfastnow.com and that's actually a legitimate registration that the bad guy has made, just looks like a dieting page and when I do the query for that I'm of course going to go to their name servers because they have owned the name and they can send me the response and they can actually send me the records for loseweightfastnow.com but also they can include other records. At the same time, they can answer for, in this case say for Ebay.com and if I cache that answer then the next person that's for Ebay.com will get the wrong IP address. This is another way of doing cache poisoning.

You can of course poison a host. If you have managed to get malware on to somebody's system, you can actually change where they ask for DNS. You could change the cache on the machine so that the stub resolver just answers or you can change where you point them to. There's a well-documented case of this called DNS Changer which was a piece of malware that would change your default name servers, recursive name servers to name servers owned and operated by the bad people, the criminals and then every time you made a DNS query, they did decide what answer they would give.

They could very easily point you to different IP addresses, different servers. It was actually quite a nice piece of malware as malware goes, I guess nice is not the right word. It also had the ability to, if it could get into your router using default passwords, everybody here probably has a router in their house, even if they don't know it, that has often a name server on there or it points you to a set of name servers and what they would do is if they were compromised they would attempt to get into that router because many people don't change their passwords and then they would change the default name servers on that.

Now not only have they compromised your machine but they've compromised anybody who uses your network. The interesting case with DNS change was to actually disable this network, law enforcement had to figure out to how put clean name servers in the place of the criminal name servers. When they kicked down the doors of the colows, or they served their warrants, they actually had to go in and put their own infrastructure in and they relied on people from the industry to actually build those servers and take them in so that the people who were infected could once again get proper name resolution. It's not really proper name resolution because they're still going somewhere they shouldn't but at least they're getting honest answers. Once again, these are abuses of the DNS and the way DNS works that happened in the wild.

Then of course there is an entire system of registration of names. When you buy a name, you go a register that with a registrar, it goes to a registry and there's a few ways of exploiting that. Name registrations are fairly easy targets. There's a lot of automation going on and in many cases the correspondents, the discussion between the registrant, the person buying the name and therefore afterwards manning the name and the registrars, is all via email.

Who here has ever had an email compromised? If that's your email that's associated with your domain name, your domain name is now at risk. If you think about the various compromises that are being announced of email systems or even of financial logins, I think Equifax was a big one. In a lot of these cases they have email addresses and passwords, if you're using the same email and password for your name registration, you're at risk. Some of the registrars have two factorial authentications. They have more advance systems but not all of them do.

Of course, if you're a bad guy you don't necessarily have to steal name, you can also just go out and register a name. Names are pretty cheap. Sometimes you want particular strings. If you're going to do a fishing scam, fishing is where you try and get somebody to click on a link and go somewhere, you might want a name that looks like a legitimate site, maybe something very similar to a bank name or to ecommerce site. You may want to have a solid landing place for your ransomed ware payment page. Something that you control yourself rather than something that you've compromised.

Malware often have distribution sites that you want to be more solid then the comprised machine. Sometimes they register names for this, pharma sites, piracy sites, sometimes you want a recognizable name that is constant and stays up. They'll register names for that. Much the same way criminals also buy name servers and web server and all the other resources and sometimes even rents out entire racks in co locations facilities to run infrastructure. They don't always compromise things, sometimes they go out and actually buy an infrastructure.

Typically, when you look at the large malware and botnets infrastructures it's a mixture. The botnet itself may well be comprised machines but some of the controlling infrastructure might be purchased and what looks like legitimate purchases with legitimate names that they've registered.

Why would they do that? It just gives you more control of the name. When you have your own name servers. Fishing you want these strings. I can also just crack into the systems. If I want to deface or appear to deface a corporate website I can do that by attacking the actual webserver itself. Obviously if I can compromise a webserver I can get in and change the data.

Often this happens when you have data systems that are not up to date. There's a lot of platforms that allow people to build websites easily and as long as you keep the software up to date they're not too bad but if people forget to update the software. If you can't get into that way, what we've seen happen is that the perpetrators will attack the registry systems or the registrar's systems and get at the name and then they change name servers and if they can get into the DNS, they can change the IP address for that webserver.

Instead of going to the legitimate business server, you go to some other server and you get a page that says, "Hey, we have hacked large corporation X." But in fact, they've not. They've not even touch large corporation X's infrastructure, they've managed to get into their name account or into the registrar or the registry itself. They've attacked the infrastructure to take charge of a particular name. Not common but we do see that.

I talked about email and compromised emails, it's getting more and more common as we've had big attacks. Who is affected by either the Yahoo or the Equifax breech? Most of you don't know you were affected okay. There were millions of people affected by those breeches. I only saw half a dozen hands here and that really surprises me because some of these services around the world and a lot of people have accounts with them. As I said, if you were using those for your domain name registration, you might want to go and change those.

This is an interesting use of the DNS is, it's something we call 'fast flex'. Like many of the things that people often call abuse, there's legitimate reasons for doing this as well. If you think of some of the content distribution networks, they can their IP's very quickly, depending on where you're coming from to point you to a specific server. Now bad guys do this too.

One of the reasons they do this is to make it hard to track them. What they do is they have very short time to live on the DNS information and they will constantly change the IP address of the server where their malicious content is. The name may stay the same but the IP address will constantly be changing and that makes it really hard for people to mitigate this.

Now, sometime they change both the name and the address, we call that double fast flex. This infuriates people that are trying to track this stuff down. I've hear people say, "We should not allow that." But there are legitimate reasons for using this technology. If it's a good technology that people in the industry use, you can guarantee the bad guys will figure out how they can use it themselves as well.

It isn't something we here about as much about these days, it was very hot topic a couple of years ago but it still occurs and I still get the occasional complaint from law enforcement that don't understand that people can change their IP addresses and their names which is sort of the whole purpose of DNS is to officiate the IP address so that you can change it.

Now because DNS is everywhere and everybody uses it for everything, it's also often not filtered. If you have a file there's a very good chance that port 53 which is the domain name system port is not looked at. Some firewalls will block on TCP but won't necessarily block them on UDP. The other thing with the DNS is we have things called text records, which you can query for and you can put anything that's text in there, so you can put any kind of data. Y ou could actually take data out of a network and bring it back to the bad guy. Lot of proof of concepts but we actually saw this used in the wild about three weeks ago where the perpetrators were doing point of sales devices, so credit card readers in stores and the way there were moving the credit card details was as records in the DNS because those point of sale services actually use DNS and there's legitimate traffic and they were hiding the exfiltration in the DNS packets. We've actually seen this recently in the wild.

The other thing that the DNS is used for in a very similar fashion is for command and control for that malware, for the botnets. Because the firewalls allow inbound responses with the DNS, you can send commands to your controlled machines and this is fairly common on modern malware is that they use the DNS, they tend to do two things, they tend to peer to peer command and control but they tend to also in the background to have a DNS channel to be able to send signals to the compromised machines to for example, start a DDOS attack, send those DNS queries that we saw in the distributed denial of service attack. Plenty of examples in the wild, moto, there's dozens and dozens of these systems out there.

One of the other things that's not in the slides that they will do is the way control those systems or the rendezvous point if you like of the way that they get the DNS queries to start is they will use something called domain generation algorithm. That's a piece of the code which based on a timestamp and the algorithm will generate a random looking name.

Now, they're not random because every machine is generating the same list of names and then they call home, they use the DNS to try and call home to that machine and if that bad guys register those names and point it to an IP address, the malware will try and do a DNS query to get to its command and control server and do what DNS is supposed to do, it will give them the IP address and they'll be able to connect.

That's interesting because often they will generate hundreds or thousands of names that they could possibly use in a single day but they only need to register one for it to work so most of this malware barrens will stop, the first name on the list and they will work their way through. I think configure C was doing about 50,000 names per day and if you're trying to block this activity, if you're on the good guys side and you say, "I want to block this." You actually have to prevent them from registering all 50,000 of those names.

Has anybody here heard of Operation Avalaunch or Andrometer? These were law enforcement activities to disrupt botnets. These botnets aren't only used for DDOS they're used for all kinds of malicious activity. If you go and read up on those, you'll see things like they blocked 800,000 names. People often get that confused with what they did is they took away 800,000 name registrations, that's not the case.

The majority of these names have not been registered by anybody yet because they are random looking eight or twelve-character length strings that make no sense. What they're doing is they're blocking the registration of the names not taking the registration of the names. It was about 800,000 I believe in Avalaunch. Quite a bit of work and law enforcement are constantly working to try and take down these botnets and these malware families. As they have DGAA's in them that may talk or may have lists of names that spam many top-level domains, many distractions, it makes it quite complex for law enforcement to actually take action against these.

Once again, Avalaunch, I can't remember how many M LAT's they sent out, Mutual Legal Assistance Treaties, it's something that law enforcement used to basically translate a court order from their jurisdiction to another jurisdiction and somebody in a different jurisdiction to take action but it was dozens and dozens and dozens of these legal documents they had to do a round the world to have people take action against this. It's a bit of a losing battle but they are using the DNS and the way the DNS is supposed to work to their advantage. They're abusing the system in many ways, not just through DDOS but also for the way they register and use names.

JAY PAUDYAL: I am an ICANN fellow and member of Neo-Brahmi Generation Panel under IDN programs. I want to intervene by saying DSN misuse or abuse which costs many frauds like fishing, malware, distribution, spamming, http attacks, etcetera. In my opinion we can make a policy where it will be mandatory to give photo id's any national identification, driver's license, passport, etcetera to change or set DNS entry and details of ID should match with the Whois profile of the said domain name.

If you argue this will require human resource to handle it, then my point is, in the era of block chain technology and artificial intelligence we don't need any humans to verify things and software bot will do. As all of you are aware the moment advertisement platform like Facebook and Google detects any kind of fraudulent activity, they ask for the photo id of the user and disables their account temporarily then why can't we do it at ICANN, since ICANN is managing DNS records of the internet and DNS abuse misuse is affecting the user of the internet?

JOHN CRAIN: Thank you for that intervention, Jay. There's few misconceptions in there. ICANN is a -- for the DNS, the most part a policy development organization. We don't actually manage much of the DNS. We do implement the root, which is the top level of the DNS and for those who have been -- if you have not been to the DNS Primer, the 101, it will be on again on Monday at 5pm, so do come to that.

Because we manage the root of the system, the ICANN community sets policy for the root of the system. We can set some policy towards the contracted parties, which are for example the gTLDs and that's an ICANN community thing, so we could discuss and we do discus in the community if you're following it many of these issues around abuse and how we handle it.

Now, the DNS is a hierarchy called system and you delegate to the next level down, just like ICANN delegates the roots and then you also delegate responsibility. You could probably argue that there could be some policy elements between registries and their registrants and there are, some of these are policies some of them are acceptable use policies. Then you've got a level below that. How do you then start policing that and the level below?

It's not as straight forward as ICANN can stand up and set a policy. As an organization we don't have that power and due to the distributed nature of the system, the way it's designed, it wouldn't be that straight forward. I think, Michele, you want to intervene as well. Before I go forever I should let you talk to this because you operate a registrar and have operational knowledge of this.

MICHELE NEYLON: Thanks. Michele Neylon for the record, CEO and founder of Black Knight the largest hosting provider and registrar in Ireland, chair of the Internet Infrastructure Collation and a bunch of other things. While I'm always interested here ideas around how we can better mitigate DNS Abuse, what that person is suggesting is completely unworkable for a multitude of reasons. If you would like to have domain names cost say $500 or Euro per year, I will happily implement a system where I will take a blood sample for every DNS change but unless and until people are willing to pay that kind of money that's just not going to work.

Secondly, I will use the buzz word 'dajour', GDPR, if you expect registrars and hosting providers to start collecting huge amounts of personal information, which are not related to the service that's being provided, in other words changing a DNS record, that's going to render the entire thing unusable.

Now, if you want to go down this route, I would really recommend that you don't, go off and get some national legislation and do it within your own country but bear in mind the internet is global and most of us operate cross boards and we are not going to implement this and I feel fairly confident in saying, the most of my fellow registrars would find this unworkable.

Now, having said that, there are certain registrars who operate in totally different, who are targeting specific markets. If you are a fortune 100 or a fortune 500, you are probably using their services and all of the DNS changes and other things that they would provide to you, would be validated but the issues that I believe this panel is talking about is related to general DNS Abuse which is a completely different kettle of fish. Thanks.

JOHN CRAIN: Thank you, Michele. You actually covered a few of the topics that I was going to cover. For example --

MICHELE NEYLON: I was trying to save you time, John.

JOHN CRAIN: Thank you. For example, the issues around the Who is data and privacy and all these kinds of issues. It's an interesting intervention and, Jay, if you become a fellow for a future ICANN meeting, I will happily have conversations about this. Do we have anything else there?

CATHY PETERSEN: Not yet.

JOHN CRAIN: Not yet, okay. So I will move on to the next slide.

CATHY PETERSEN: This session is fun according to the --

JOHN CRAIN: According to…?

CATHY PETERSEN: We've got a comment that this session is fun.

JOHN CRAIN: Well, we're not supposed to have fun so we will stop that, that's very bad of me, I'm sorry. Let's talk a little bit about how the landscape is evolving and of course just like anything on the internet, stuff always evolves. I'm not sure if better is the good term but certainly more efficient botnets. I work closely with law enforcement in my roll at ICANN as subject matter expert on issues like this, so I'm seeing some of this first hand.

The size and the complexity of malware and botnets is increasing, people get smarter all the time, including the bad guys. We are definitely seeing a lot more what we call DDOS as a service. You don't actually have to own a malware variant you can go buy a malware variant or a piece of their botnet. They have amazing graphical, web interfaces where you can go and purchase the poison of your choice or the botnet of your choice, the malware of your choice and the number of machines you want and pick a target and somebody will do it for you and it's not expensive.

I recommend that nobody does this, that is probably criminal activity and I will hunt you down and I will send my law enforcement friends to you but these things are sold as commodities these days. You do not need to know anything about the internet apart from how to get a website and probably on to some of the dark web stuff, which isn't hard, to go and purchase these things. That's the normally the kind of stuff that law enforcement goes after, this commercialization of abuse.

We're still seeing plenty of fast flex and double flex, it's back again, it comes and it goes. Spam is just getting worse, now their hosting a lot of their infrastructure in the cloud, it's a salesman's term for distributed computing, but you can go buy spam services just like you can buy DDOS services. An example is the Avalanche malware infrastructure, Avalanche was the project name, it was multiple variants of malware were involved and they were buying selling various services and it's everything from DDOS to moving money around to sell elicit goods and it's all using this DNS infrastructure that the criminals have built up. We call it the internet of threats or the internet of venerable things.

We are seeing a proliferation of cheap devices going to people's homes. I like playing with these, I have many, many threats inside my own home network. If you have heard of something called the Miraii botnet, which attacks some DNS infrastructure, I'd like to say it was a year ago but it was probably much longer, time gets shorter as you get older. That was using various devices on the internet that weren't quite secured how they maybe should have been.

I actually own of the variants of video server that was used for this and had disconnected it from my network and reported problems in as far as I could back to the manufacturers about a year and a half before Miraii, you actually couldn't update these systems. It was literally impossible as a user and I like to think I know a little bit about networks and how to update systems, to actually put better code, more secure code on these devices and if you did get it on, you had a power outage and it rebooted, it came back to what it was.

We're seeing more and more devices going out there and these devices are cheap and cheap and security generally don't go together, that's just a reality of life. People want cheap devices, given the option of a $10 light bulb and a $100 light bulb that you can both control and make flash and do funky things from your telephone, most people will take the $10 one, they're not going to sit there and say, does this one has better security, that's not how humans work. We're seeing more and more of these devices. I predict that's not going to get better any time soon but awareness of this issue is getting higher.

Obviously, people are going to the manufactures and saying you shouldn't have done that but we will see more and more, this year its light bulbs, it's toasters, it's coffee machines, sensor networks, very popular that the moment alarm systems for your home, although why you would put your alarm system online I don't know but people are.

The internet of threats or the internet of things is not promising, especially for the botnet environment where think there are millions of these devices, maybe billions of these devices in a few years. An interesting thing we saw in that some of the ways the code writers use the DNS is really interesting, we actually saw some people refer to as an ignition key or a kill switch where they had a particular name that it tried query and expected not to get an answer and if it got an answer it would turn itself off. We believe that they done this to prevent people working in labs and figuring out what was going on with a code.

A researcher discovered this, registered the name and turned off the malware variant, which was pretty cool to see that they built in a flaw using the DNS, I guess they hadn't really thought it through. That was WannaCry by the way. Has everybody hear of WannaCry and WannaCrypt? It kind of got in the news.

So volumetric or DDOS attacks continue to increase. As I said, 1.7 terabits, that was this month, next year it may be double that. These are levels of data that most systems cannot deal with. We're talking terabits not megabits or gigabits, it's interesting and as I said attack kits are very easy to obtained, there are many, many out there.

One of the things that people think about when they think about fishing and abusive types of that is their bank accounts and people impersonating their bank's website. You can buy a kit with websites of the most common banks. You don't have to go an impersonate their bank anymore, you can just go out and you buy the kit. It's like do it yourself fishing kits around there. Pretty much all of this malicious behavior has become commoditized and become a business. Rather depressing really when you think about it.

You may see the term a booter or a stressor, these are businesses that will stress test somebodies network for you. Stress test is nice terminology for DDOS attack. There's argument that there's a legitimate service of testing your network by stress testing it. Well, they'll happily stress test you and if you pay them enough they'll stop stress testing you. It's extortion and fraud and there are people that sell these services. It's quite stunning.

More on the Avalanche stuff. The bad guys had a lot of their own infrastructure. Originally it was sort of a malware for botnet but then it actually became a botnet to deliver malware. Once you've compromised a machine, they would actually deliver specific types of malware to specific machines on requests from clients, not pretty. They had what we call, bullet proof hosting.

There are folks in the ecosystem, they're not people you would ever see here that will actually sell hosting, the criminals will build their own co-lo's and they will actually sell hosting on that for other people and say, we'll guarantee this stuff stays up. A lot of financial fraud attacks. Obviously, it's all about the money, just like fishing it's often about the money.

One of the things we say, it was like a cloud experience, you could just log in and buy the bits you want and have machine where you wanted them. It's quite fascinating to watch how this has all evolved over the years. Here's the 20 families you could choose. As I said Avalanche wasn't a piece of malware anymore it was many different malware and you could literally go in and you'd have a drop-down menu. It's just like buying anything else online, you go in, you have a drop-down menu and you chose which malware variant you want and how many infected hosts you want. I'm almost speechless on it.

The other thing about dealing with some of the abuse is the timeframe involved. If you look at this graph, what you'll notice is the very thing underneath is we're not talking about months or days, we have some dates in there but we're talking about years. We're talking about timeframes to dismantle this malware and this infrastructure that takes years. Taking down Avalanche was a multiyear effort, multi-jurisdictional, hundreds if not thousands of law enforcement officers and industry subject matter experts working to dismantle this. The new guys can bring up a new one in a couple of days. It's pretty easy to get new malware and adapt malware.

It's interesting, some stats here from Avalanche, it was 30 countries, 64 top level domains operated by 40 registry operators, we didn't have the number of M Laps here but it was a lot and this is still going on. In fact, if you've heard of Andromeda, what an Andromeda is, is really a follow from Avalanche, it's some of the same malware variant plus some new ones.

If law enforcement takes years, the attackers -- firstly they're not bound by regulation and rules and morals like the guys on the good side are. Their timeframe is hours or days, they operate in internet speeds. A botnet operator needs to register a name, well that takes him five minutes. Anybody here ever registered a domain name? If it's available it's pretty quick. Michele, you could tell me a domain name in a few minutes? Yeah, it's not hard.

Leasing that out, that doesn't take any time either because they have the platforms, they have pretty websites with drop down things. Then they need to go and actually start infecting people. Well that normally like a fishing campaign or a drive by malware or something like, be slow at this and say it's like 12 hours. Then maybe in a day victims will start notifying security companies or law enforcement, assuming they notice. Then weeks, months, sometimes years later the final action of taking this stuff eventually takes place because of that law enforcement and operational security speed or timeline. Do you have a question?

LENDON TELESFORD: Yeah, my name is Lendon from Grenada. Question/curiosity. You mentioned a lot of the bad guys purchase legitimate domains for the wrong reasons, so as a TLD what mechanisms are there in place to track what percentage of your domains are used for legitimate versus illegitimate uses?

JOHN CRAIN: That's an interesting question. We're trying to do some statistics on this but defining what is legitimate and illegitimate is not always straightforward. There are certain types of abuse that we are measuring and what we're looking at is what we call reputation lists that are published and used by the security industry to protect networks and the names they put in there. They don't catch all the abuse but we're using it as an indicator but we're not the registry operator, so we're doing this from a purely put data into the policy perspective.

It's not as easy as it sounds. You've got to identify good reputable and trustworthy list providers and then you've got gather various other forms of information, associating for example a name of a registrar requires doing Whois queries because you're looking for the registrar id and you've got to create that data and manage that data. Then look at what that means, data gives you questions not answers most of the time. We have some percentages and we've published some data and it's preliminary because we're still working this system but we know that a large portion of the abuse types spam, botnet, command and control, malware and fishing sit with a small number of registries.

We have anecdotal data that suggests that pricing drives this abuse towards different registries, registrars and kind of logical when you think about it. I think Michele pointed to this, if you're $500 a name, you can afford to do a lot of security work. If they're $10 a name or $1 a name, they're more attractive to the bad guys and don't have the funds to do that kind of work and Michele you can intercede if you wish.

MICHELE NEYLON: Just on that query which in an interesting one. At the registry level as John points out there are various data feeds you can use, at the registrar level ultimately, it's not our job to be the internet police but at the same time a fraudulent registration is going lead to a charge back and a charge back costs me more than I would have made from the domain name so I don't want the charge back.

Do you understand what the charge back is? Credit card charge back, so essential if I steal John's credit card and I go to Amazon and I buy a book or a CD or a phone or whatever, he will eventually realize that the order on his credit card is not valid, that I've stolen his credit. He'll go to his bank, his bank will cancel the credit card, give him a new one and then they will send a message to the merchant, the shop or the registrar or the hosting provider and reverse the payment.

When they reverse the payment, as the merchant we get kind of fined as it were, if the order for $10, it'll got me maybe $50. If I have to challenge the charge back because that happens all the time, people decide to use charge back as a way of getting a refund, that will cost me money as well. The kinds of things we would do, like my company does is we do things like we will check to see if the IP address is a proxy, if the IP address for a user network or is for a server, there is no valid reason why a webserver should be on my order form for example. There are no valid reason why particular networks should be anywhere near an order form.

For example, I don't sell much to China, so therefore Chinese IP addresses have a bad reputation on our system. We're an Irish company, so Irish IP addresses have a good reputation and so on and so forth. As a registry it's a bit more complicated because obviously as John says, you're dealing with other things but the certain patterns you can look at. The price one is something that people can debate it but if you look at the date, there's usually a correlation of some kind. There's a ccTLDs that have given away lots of domains and they had to take certain actions to deal with that. Anybody wants to talk further about it, please, I'm sure John will be happy to take it offline.

JOHN CRAIN: Thanks for lining me up to take up more questions offline, Michele, you're too kind. There are things you can measure and there are actions you can do, all of which have a cost. There's a lot of discussion in the ICANN realm, especially with public safety working group and the registrar and the registries around what exactly is the role of the industry to deal with this abuse.

As ICANN Organization Staff we don't operate much infrastructure we don't operate registries and registrars, we tend to look at it more from can we measure this to give input and insight into the policy discussion. It's a problem, everybody knows it's a problem. Nobody wants these registrations in their system, they cost them money and they hurt their reputation. I think there is definitely a incentive for people in the industry to take action and they balance that against all the normal business things of cost and whether or not this is their role, taking action against a name also has risks associated with it, such as liability if you make mistakes.

Although it sounds like a very straight forward, this is bad, therefore we must do something conversation, in the real world there is all kinds of other things you have factor into and this what the policy discussion around this and should follow this discussion, I encourage that here at the ICANN meetings.

Once again on the timeline, the bad guys just get to act much faster than the good guys do. The good guys are bound by policy and process and regulation and morals that the bad guys don't have. For example, technically speaking we could probably, not we, not I, but somebody had probably send data to the infected machines because we know where they are, to have them clean themselves up.

Theoretically that sounds like a brilliant idea, except that's illegal in most places. You're actually touching somebody's machine without their permission. Although technically that might be an interesting idea, it's not something that law enforcement and governments can go and just do. There's a bit of balance in favor of the bands unfortunately. I think that's the same in the real world too.

Staying on Avalanche, five people were arrested. One of them was just re-arrested last week or the week before. There were 37 searches that took place in 7 countries, this is law enforcement going into buildings and taking machines and people. 39 servers in 13 countries and 221 servers were actually taken offline. 67 TLD's, 830,000 domain names were blocked, remember not taken away from people but actually prevented from being registered.

What law enforcement and industry are doing now is what they always end up doing, which is going out, telling people about it and trying to remediate, to try an actually fix the system and the work with ISP's and certs to do that and it's a lot harder to clean things up then it's to get them infected. The sad thing is often when you get machines cleaned, they get re-infected again later because it's just bad hygiene that's just the way people are. People don't update their machines.

Miraii is the other well-known botnet out there. We call this a lesson that we didn't learn. There's all this new hardware out there and developers etcetera just aren't securing the systems the way they probably should do and we've done this in the past. This isn't new, we come with a new technology, we need to get to the market pretty fast. Security is never the highest priority, we know all these things. Unfortunately, I just think this is human nature and the nature of some of these technology businesses. I don't predict this getting any better anytime soon.

As I said earlier, Miraii was really one of these issues where clearly saw it was IoT devices. A lot of these botnets we know have touched on video servers and web cameras and we seen infections in medical devices, all kinds of things, anything with an operating system is of course venerable but default. In Miraii, this is exploitation of well know variabilities, like I said, I had one of these devices that I'd reported the venerability. Arguably it's more of lack of hygiene in the way they maintain things then an actual venerability. This isn't anything that was unknown.

These things are listening on Telnet, does everybody know what Telnet is? No, I can see people shaking their head, that's because you're not supposed to be using it anymore. We deprecated this, we got rid of this and told everybody it was a bad idea sometime in 90's. It's basically what tend to do when we connect to a machine, is we do what we call a secure shell, or SSH, it's a way of connected over an encrypted and authenticated channel to a machine to manage it.

Telnet was the stuff before that, where you just connected with, if you're lucky a password and there was no encryption. Why is this the default on machines that are being released in this century? Because we got rid of it last century? This would be like deploying a brand-new automobile designed without a seatbelt. And you're about to tell me why you love Telnet.

UNKNOWN SPEAKER: [Inaudible]. One thing here is that Telnet itself isn't a problem here because it could as well be SSH but hard coded administrative credentials on a publicly available firmware is a problem itself. It could as well be on some IoT devices that there's a web interface which is HTTPS with all the certificate stuff but it's still hard coded credentials and in case of [inaudible] with Miraii at least about 20% for like millions of devices, so this is a main issue. Basically, what IoT is bringing us is the amount of technical debt, which is just built into the infrastructure and basically nobody cares about how to resolve it.

JOHN CRAIN: There was many different problems with these devices, Telnet was one of them, we just used that -- this is ages, but what we see very, very frequently on devices is standard passwords that are published on lists. If you look at DNS changer, the one that talked about earlier, the way it got into those routers, it just used the standard password that you can download from a list, you can Google it, if you have a device at home, you can literally Google the passwords.

UNKNOWN SPEAKER: I'm not going to use microphone for long but another funny example of this is the built in Apple OS six-password generator, not the one in Safari but the other which it can be used to generate a password for you App store account which actually by default generates passwords which are too easy [inaudible] a nice vocabulary, like minutes or something.

JOHN CRAIN: So, the message is we're all doomed, unless you're in the security field, in which you're employed. As our friend here was saying, there were lots of issues with Mirai, default credentials not being the least of them. These devices have been used again and again, these types of devices. When there are tens of thousands or even hundreds of thousands of these devices out there, it allows you to have pretty large botnets and depending on the type of device, they may be actually designed for high through put.

If you think of a video server, that's a machine that's actually designed to push a lot of bandwidth. They have the capability to push video and sometimes multiple streams of video, they're actually really good for DDOS because you can send lots and lots of traffic and you have to remember that most people don't monitor their networks, so the end user that installed this will have no idea this is happening.

The patch that would have prevented this, was out months before the exploitation. If you got hit by WannaCry, did anybody get his by WannaCry here? You should have patched your machine three months before. If you'd been patching your machines, if you'd been practicing good hygiene on your systems, it would have never of attacked you but people don't. People don't update their machines, they don't update their operating system it's human nature. In January the venerability advisory was given out. Microsoft patched it in March. The big WannaCry wasn't until May 12th, the one that hit all the news. It could have been avoided.

This is the thing about having the kill switch in there. We don't know why they did this, there's a lot of suspicion about whether or not they were doing it prevent people putting this into sandboxes, I don't think we'll ever know unless the guy gets arrested and tells. Somebody figured it out. I've not actually talked to the researched who this so I don't know if he figured it out and registered the name or he registered the name and just got lucky but either way, we should be thankful because it killed the exploitation of WannaCry pretty much overnight. People got very lucky. I suspect that people have read this and won't make that mistake again.

UNKNOWN SPEAKER: So, I was involved in the research that actually ended up being -- with that being registered. The researcher who found it, registered it because he noticed it wasn't registered, he hadn't finished reading the code until after the kill switch domain was registered and sent out. After the registration happened, the infection rate dropped dramatically and we tried to figure out why, it was because he found the kill switch. The particular person that found that is -- it's hard to talk to him right now because he's being investigated for another crime.

JOHN CRAIN: Sometimes it's better to lucky than good. Yeah, he or I should say we, got lucky that he registered that name when he put it in the DNS everything went away and I was better again.

Let's talk about abuse in an ICANN context being as we're all here for the wonderful ICANN meeting. That's where you all go YAY. ICANN Discussions regularly touch on abuse issues. You may not always realize that some of the issues they're talking about touch on abuse but regularly they do.

A few things that are going on at the moment, Whois accuracy, is anybody here heard of the term Whois accuracy? It's been an ongoing discussion forever, far back as I can remember and I'm old, I've been here a long time and it's all about access to Whois registration data that is accurate and useful and those discussion happen all over the place. That crosses with discussions about something called GDPR coming out of Europe, has everybody heard of GDPR?

Yup. This is basically, really you shouldn't be publishing all this accurate personally identifiable data about people, so there's two things are nicely in conflict which should give us lots of fun discussions. The issue of public safety, we use the term public safety because not everybody involved in dealing with badness is law enforcement. There's a lot of private security organizations and there's also a lot of government organizations involved in trying to protect the public and public safety that aren't necessarily law enforcement.

There's a lot of discussion going on at the moment about reporting abuse and measuring abuse. I'm giving a presentation later in the week about Our Measurement System and I've already given a few this week. There's a lot of stuff about abuse going on here. They might not necessarily call it abuse but it does affect it.

Whois accuracy GDPR, public safety and reporting abuse are very common topics. Often these discussions are quite heated, they are fun to watch, they're not necessarily fun to be part of all the time but they are interesting to watch. There are many different interests here, all of which are valid but they just happen to compete and then finding what the similarities and the common ground is, is always an interesting thing to watch. We say public safety, now that the government advisory committee -- you can go ahead.

TOSCA BRUNO VAN-VIJFEIJKEN: Thank you. Tosca Bruno-van Vijfeijken on the board of the Public Interest Registry .org. As a relative newcomer, tell me a little bit more about this all valid but competing interests that cause heated debate; that's really interesting to me.

JOHN CRAIN: You have one side that looks at abuse and just says, well is should just be gone and then you have the other side for example, well there's cost to that and then you have people that say names should be cheap and you have people saying that names should be secure. These are competing values, they might not sound like they're competing but they are. You cannot say that ball has to black and the wall has to white, it can be one or the other, it's a lot of those kinds of things.

Pretty much everybody has a lot of the same interests in the end, everybody wants a secure, nobody wants this rubbish in their systems but the way you do it and what the policy will be, will affect businesses and they will affect safety. There's always contention between how far you go one way or the other. It makes for very interesting discussions.

TOSCA BRUNO VAN-VIJFEIJKEN: Understood, thank you.

JOHN CRAIN: Go ahead, Michele.

MICHELE NEYLON: Just for the lady who was up at the mic, if you're interested come along to the RDS PDP Working Group Sessions, you will find a room full of very passionate and very engaged people who cannot agree on anything apart from that they may nor may not like coffee and alcohol. Anything to do with the subject matter of the discussion is probably not going to be a agreed.

There's a lot of different interests and it's an ongoing debacle discussion. There's also a session on Monday afternoon I think, on GDPR, which is a cross community session, I think it's Monday, where you will also hear didn't interests, you'll have intellectual property verses public safety verses those of us who actually try to make a living.

JOHN CRAIN: Passionate, that's a good word, I like that. Lots of passionate discussion. The Government Advisory Committee has something called The Public Safety Working Group, obviously abuse a public safety issue. The Government Advisory Committee gives a lot -- the way they communicate with the rest of the ICANN community is through communiques, they've had various communiques' over the years that have talked about abuse. Some of it defining what they'd thought abuse was, some it talking about what new protections we should when had the new gTLD rounds.

Obviously, governments worry about -- they're public so they worry about public safety so it's a logical place for a lot of the input to come from into the policy discussion. They have this working group and like I said, it's public safety working group and public safety encompasses both law enforcement but also subject matter expects. They have the ability to invite nongovernmental people, if though it said government advisory committee working group. They deliberately set it up so they could bring in subject matter experts, which is very good.

Here's the same list of issues that they're dealing with, GDPR, Whois accuracy, carrier-grade NAT, Network Address Translation is fun thing that they worry about. This is a different type of identifier issue, it's not a DNS issue, it's an IP addressing and associating IP addresses with interfaces or user's interfaces that law enforcement worry about how they find information about identifiers. It's different to DNS but it's another identifier issue.

The issue of fast flex, as I said they're not happy that people can do this and they have the discussion about is there anything we can do in the case there are actually legitimate uses for this. Of course, DNS Abuse in all its forms is something that they're very interested in and they have open groups.

We of course have contracts. ICANN is not a regulator in the sense we're not some kind of regulatory or authority that has dictate and regulations that people have follow. We manage our relationships through contracts. We have policy discussions in the ICANN realm and the outcome of those policies normally get formulated in the contracts. We have contracts with generic top-level domains. We do not have contracts with country code top level domains.

These contracts really just for the registries, for gTLDs. They have some specifications, we're going to share these slides, I'm not going read through them all. I'm not a lawyer, I probably don't understand half of them. We have the registry base agreement, that's with the TLD operators and then we have the registrar accreditation agreement with the registrars and both of those have a elements related to abuse and the handling of abuse...

Let's talk about what we're doing this week. There are a few sessions that I think might be interesting to you. I believe that tomorrow is Sunday. The Government Advisory Group will be giving an update, so you can hear what they're doing. They've given an update to the GAC. It's on the schedule as being open, the links are in here.

On Tuesday, they will have another meeting, actually two meetings, as the Board they will have their own meeting where they discuss their topics that's the first one and then they're going to have quite a long session, I believe it's most of the morning dedicated to GDPR and Whois or whatever is going to replace Whois, registry data. If you're interested go to that one, I think that's going to be really interesting.

Then on Wednesday there is a group the Domain Name Association Health Domain Initiative, which is actually an industry initiative to deal with these issues, not a ICANN policy thing but actually industry getting together and saying how are we affected by this. If you're interested in abuse and how people in the industry are actually taking action on their own, go to this one. So I have one minute less and I'm happy to take questions. Can you use the microphone, please?

UNKNOWN SPEAKER: [Inaudible]. Now my newcomer and fellow hat on. So, our fellowship program leader, Siranush, has just told us there's no stupid questions from a newcomer, so challenge accepted. On the agenda of the meeting there are two or three meetings related to security and stability advisory committee, so basically it sounds this is something which is related to security and stability, so could you please explain in a few words what's going on there in this advisory committee? Thank you.

JOHN CRAIN: ICANN has two sorts of input bodies if you want, there's the supporting organizations, the GNSO, ccNSO and then there are advisory committees. The security and stability advisory committee can advise on any matters relating to security, they do have an interest in abuse and they are working on documents related to abuse. They also have interest in Whois and who Whois data.

Some of the meetings are closed sessions and some of them are open. I'm not sure which are which but it is on the scheduled and I would encourage, especially you seem to be working in the security field, I would absolutely encourage you to go to those meetings and introduce yourself or if you don't want to I'll introduce you to some of the members and have discussions about what they're working on because they do do fascinating work. It's quite an interesting group of individuals with a lot of skills across the security realm. They are touching on abuse issues but they're touching on many other things, DNSSEC protocol changes, the whole gamete of security issues that affect the identifier systems. Farzaneh?

FARZANEH BADIEI: Hello john, Farzaneh Badieis speaking. I had the impression -- thank you, this was really great. I specifically attended this session to see how you defined DNS Abuse because we want to keep it technical so that we don't come up with copy writing and say infringe is DNS Abuse and then put it in there. Thank you very much.

I was wondering if you consider or if the public safety considers the technical definition DNS Abuse, I assume SSAC is defining and working the definition abuse or they have already something. If they take that on, how do they ensure that you are not -- ICANN does not go beyond the technical definition? Also, your presentation was very grim, come on, it's not the end of the world, IoT's actually can be useful.

JOHN CRAIN: Well, they can be if you want to make a cup of coffee from the distance, yes, I actually have hundreds, literally hundreds of IOT devices in my own network and I use them all the time and some of them are fantastically secure but some of them are not. The issue of the definition of DNS Abuse, specifically in my job, being the guy at ICANN that has to look at this kind of stuff, is I don't know if problematic is the word but it's interesting that we don't have very clear definitions or probably even worse that we have multiple clear definitions and SSAC would be a very good place and know there are working on abuse issues.

That would be a very good place to help us as would the PSWG with terminology about what we do consider to be identifier abuse and I use identifier abuse in this case rather than DNS because there other abuse types and if they could give me a nice crisp list and say this is identifier abuse and remit and this is not and is out of remit I would be so extremely happy. I don't see that happening anytime soon because as you indicated, there are people that think certain elements are DNS Abuse and other would say that's content or that's legality or sometimes it's freedom of speech issues, there's a lot of things that conflated.

As I said, there are many opinions of this and I think Michele called it passionate discussion. I ran out of time, which is probably good. I will be around for a little while, so if you have questions you didn't want to ask into the microphone feel free to approach me. Thank you very much everybody.

CATHY PETERSEN: Thank you very much everybody. If you want to hang around, in about 10 minutes we will have our next How It Works on Internet Networking and we will be talking about IPv4, IPv6 Protocols, Internet Addressing and How Routing of Data on the Internet is Done. Thank you.

[END OF TRANSCRIPTION]