



<http://www.runasradio.com>



Richard
Campbell

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.



Greg
Hughes

Text Transcript of Show #121
(Transcription services provided by [PWOP Productions](#))



Andrew Hayter Battles Malcode!
August 12, 2009



[Music]

Brandon Wenn: From runasradio.com, you're listening to RunAs Radio, the Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Brandon Wenn, announcing show #121, with guest Andrew Hayter, recorded Monday, July 13, 2009. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com. You can follow the boys on Twitter at twitter.com/runasradio.

Richard Campbell: Thank you, Brandon. You're listening to RunAs Radio. I am your host, Richard Campbell. With me as always my co-host, Greg Hughes.

Greg Hughes: Hey Richard.

Richard Campbell: And this is a show that you organized, buddy.

Greg Hughes: Yeah. We've got to throw a little security related thing in every now and then.

Richard Campbell: We've got to get enough security in there; no two ways about it and that's your thing.

Greg Hughes: Yeah. I mean, you know the IT world more and more and more is taking on different security. You can think of it as tasks, but really it's becoming much more of a strategic approach, not so much of a tactical dotting i's and crossing t's but a real responsibility that you really have to think about all the time.

Richard Campbell: Absolutely and it's becoming more and more significant as we go along. All right, Greg, let's introduce our guest. Andrew Hayter is the Anti-Malcode program manager for ICSA Labs.

Andrew Hayter: Good morning, Rich and Greg. How are you doing today?

Richard Campbell: Nice to meet you. I'm not familiar with ICSA Labs so why don't we start there. Who are you guys?

Andrew Hayter: Who are we? ICSA Labs is an independent third party organization that does testing and validation of security products for most of the security industry around the world. We have been in business for over 20 years and have taken many adjustments along the way and growth adjustments both from our name which some may recognize early on as NCSA Labs, to a change of our name to International Computer Security Association, and then finally to ICSA Labs. I'll just mention for the record

that ICSA Labs today is an independent division of Verizon Business and the key word there is independent. We work independently of our parent company and can demonstrate that to anybody who's looking at our test results or like to work with us. Again, we work with all the major and all of security vendors -- the major security vendors, all of security vendors around the world in many different areas. My focus is on anti-Malcode products, but in addition to the anti-Malcode products we also provide validation and testing for everything from firewalls, web app firewalls, PC firewalls, network IPS solutions, SSL VPN, VPNs, IPsec VPN, you name it, we do the validation for it including FIPS 140-2 testing and a few other types of security types of testing. All information can be found pretty easily at www.icsalabs.com. That's the quick 30-second approach to ICSA Labs.

Greg Hughes: You're the independent neutral third party that sort of can let people like us know what is the actual current state of affairs when it comes to Anti-Malware software or firewalls or what have you.

Andrew Hayter: Correct and the way we go about that is this is -- and this the model we use with all the different testing programs at ICSA Labs, it's we have been based on consortium models since the very beginning in 1989. A consortium model means we work with vendors, we create a consortium of vendors in the particular technology area and we meet with those vendors, today we meet three to four times a year depending on the consortium, and we talk about the industry, the programs, the products, and the problems and how best to test the products to validate and demonstrate to the consumer, the end-user consumer in the corporate environment, the corporate procurement department, CIL, CISL, or in a lot of the Anti-Malware case the home computer user. What are the right criteria to select, to demonstrate that the product performs its function and does the basic function that it's designed to do. So we meet with the consortium, we develop criteria and those criteria have been developed in over many years so they greatly expand and evolve as time goes on. So the Anti-Malware criteria or anti-virus criteria started way back, our first consortium meeting together was in 1991 when we did the first testing. We set the criteria and then eventually made the criteria working with the vendors a little bit more challenging and brace the bar higher and higher through each iteration of our criteria. The anti-virus is very much a sure area right now but some of the other areas that are new such as SSL VPN or network IPS or the anti-spam, they're relatively new programs and the criteria is under development and in going through that growth stage where working with the vendors will determine the bar to set and where we're going to start raising that bar overtime. In the anti-virus community, what we do is we measure multiple criteria for each one of



the products we test and we test a variety of different anti-virus products. Many people think there is this anti-virus and you see it on the store shelf, or you can see it on the flyer on a weekend newspaper, but there's actually a variety of anti-virus products that we test depending on your environment, be it a single user or corporate environment. So we have desktop server anti-virus products which most people are familiar with, but we also can test for things such as a gateway anti-virus product which is on a mail gateway, we can do groupware products so that would be an environment that works with Lotus Domino servers and mail or Microsoft Exchange Mail, we have enterprise content management so that's like in a SharePoint environment, we also can test AV products in managed service such as email or just managed servers or an online product and a few others as well. So there are generally multiple criteria that we use for different types of products with the applied kit of AV coverage.

Richard Campbell: It seems to me like in the past few years, this whole Malware business has gotten way more serious like it's not kids letting worms get out into the wild by accident anymore. It's very much a business of exploiting machines for fun and profit.

Greg Hughes: Crime for profit for sure.

Andrew Hayter: Yeah, Malware for profit. It's still sometimes kids, that's one thing. That's changed. It has been as young as -- I think their recent arrest in a European country-based Malware group was a 15-year-old who is doing all the bad stuff. So it's not just kids, and you're right it's not for fun anymore. If you look back at the origins of computer malware, mainly viruses back in the early days, a lot of it was written because people basically had not a lot to do with their time, a lot of it was written and this is fairly regular research in eastern European countries where the schools are great, the technology in the schools that people were being taught was great, but there wasn't an employment outlet for them and what do I do with my spare time? Well, let me try doing this. It's a proof-of-concept, I'd write something to see if I can do it.

Greg Hughes: Yeah.

Andrew Hayter: Sometimes they do those things and they can't break free; or I write something and let it go just to see what kind of fun it would have, and they weren't too damaging early on. A lot of viruses just had a message inside them or sometimes politically motivated to deliver a message, but as time went on it developed into a more serious business where people found they could make money via writing malware and I think that's the biggest problem we have today, it's what's call a crimeware where it's Malware for profit where there are organizations out

there that are making just as much money. It's organized crime making just as much money in some instances through malware as they would be trafficking drugs or other illegal substances or illegal things, and that could be a very big problem. So you do have a malware for profit and you can do this anywhere, anytime because it's based on working through the internet and you can buy. In the original good old days, you really had to be a very good programmer at the assembly level to be able to write a piece of malware. Today, you can buy a toolkit...

Richard Campbell: Right.

Greg Hughes: Right.

Andrew Hayter: That is just a fourth generation language toolkit. Throw in a couple of things you want to do and it creates a trojan, it creates a piece of malware for you. So it's becoming very easy for anyone to go out there and do bad things.

Greg Hughes: Yes, it is the commoditization of malware.

Andrew Hayter: Correct.

Greg Hughes: Malware has become much, much more complicated overtime too. I mean, what are the things that IT professionals operating in the real world really need to be thinking about now? And you know, another thing, the terms that we sometimes hear that people don't always have a clear definition of are things like Metamorphic or Polymorphic Malware. Maybe you could explain what those things are and try to put some thought around what is the current state of affairs.

Andrew Hayter: Sure. Yeah, yeah. There's a variety of types of -- when you're talking metamorphic and polymorphic, you're usually talking about viruses, but basically a metamorphic is one that can take many different forms and it could change form during its evolution, or today there's another term -- we'll have to repeat this but there's a term -- I just got to think of for a second, I thought of it the other day but we'll come back to it. But anyway, Metamorphic Viruses or Metamorphic Malwares are those that can take many different forms when they are distributed on your system. You don't see as many of what traditionally was known as Metamorphic Viruses anymore, but you do see quite a number of Polymorphic Viruses. Polymorphic Virus is one that can take many forms and when it infects your system it will infect it multiple times and every time it's a different image of the virus, a different piece of virus and it changes its form. As it's polymorphic, it changes its form every time. There's no one signature that can be use to do the detection of that.



Richard Campbell: This is really exploiting a weakness in any virus software that depends on these signatures to identify the...

Andrew Hayter: Well, Polymorphic Viruses have been around since the dawn of men in the AV industry. It's not something that's going to be -- it's not terribly difficult for the highly qualified anti-virus developer to work on and the anti-virus engines are very good now at looking at a polymorphic sample and then being able to iterate out 2,000 varieties of it to be able to find it on a computer. So the better anti-virus developers out there don't have much trouble at all with the polymorphic samples at all. They can handle it fairly well and that's something we do tests for in our environment as to test to make sure that the vendors' product cannot just detect the original sample of the polymorphic but will replicate it out numerous times to make sure they can detect the replicates and that can demonstrate the strength of an AV vendor research community where they can detect the multiple iterations of a polymorphic sample.

Greg Hughes: I'm an IT guy and I do security stuff. What are the things that I need to be doing, or what are the things that I need to be thinking about today that are maybe different than what I had to be concern with two or three years ago when it comes to Anti-Malware or combating malware and protecting maybe a business?

Andrew Hayter: I think from the professional perspective if you're an information security professional and you're building your environment for your corporation, you have to just keep in mind everything old is new again in some respects and you cannot get rid of the older technologies or older types of implementations that you've had. You still need to put in a desktop Anti-Malware product on your computer and you need to keep that product up to date. I mean, we can start at the desktop working backwards. Part of that deployment of a desktop anti-virus product also requires end-user education, end-user education not only on the fact that I had this Anti-Malware product on my computer, it may at some point in time tell me something bad is going on but also educating your end-users on what not to do, where not to do, what not to click on. A lot of the problems that you have, in every type of environment is people, end-users clicking on attachments or clicking on links within whatever mail, email, or web page they go to and getting infected and that could be a big problem. So there has to be a lot of education on the end-user side and that goes in the corporate environment and the non-corporate environment on what behaviors to not do or to avoid when working with anything in technology these days. Working your way back from that, you have to protect your servers. Your servers could be your mail gateway servers,

whatever it might be that is connecting everybody together, they also need a layer of Anti-Malware protection. Step back further, the gateway coming into the company should have Anti-Malware protection. Of course, you're going to have some other types of protection on these things as well. You're going to have intrusion protection and there's going to be all sorts of other security protocols built-in but we have to work with all these protocols simultaneously. You just can't turn on one hoping it's going to catch everything.

Greg Hughes: Right.

Andrew Hayter: So as you go back through your corporation, you go up the food chain, everything can be protected and these days we use the advocacy called Defense in Depth. You still need to implement Defense in Depth from a malware perspective...

Greg Hughes: Sure.

Andrew Hayter: Because some malware can make it through certain levels of your defenses and it will kick one on the desktop, or it may get caught at the gateway and never make it to the desktop. So you really have to be very cautious about it, really have to have an educated community within your user-base to be able to protect that. I kind of go back and you can cut this later, but I always talk about -- there's a clothing firm that's in the northeast, I don't know how far across the country they go, called SYMS, and one of their big commercials is "With SYMS, an educated consumer is our best customer." And I firmly believe an educated user, when it comes to security, is your best user out there. They know what to do, when to do it, and what not to do and I think that's the right approach, is you can put all the implementation, all the products in place that you want, but you have to educate the users on what to use, when to use, and how to use, and when to call someone up and say, "Hey, I have a problem." There are a lot of configurability and administrative interfaces these days with most of the larger products that does send messages through to the help desk, your knock wherever it might be, to let people know there's a problem and you have to implement all those level of security. You can't just get around it these days.

Greg Hughes: Yeah. There's a school of thought that there are no technology problems. There are really only people problems and technology is just a way, a set of tools that you can use in a process of solving your people problems.

Andrew Hayter: In most cases with malware, I'd say quite a number of them can be solved because they're people problems; however, you do have other



types of exploits that generate malware such as cross-site scripting exploits that have been all over the news pages recently where it's not necessarily something that you can control but you can control linking, clicking on links that you're not sure of; and then you have drive by malware and that's another type of problem where you're just not going to know, but usually on sites that in a business environment you as a user in a business environment are not typically should be or can be visiting during the day.

Greg Hughes: Sure.

Andrew Hayter: So that can eliminate a lot of the issues in businesses. It all depends on your protocols and controls. We've had to work on some businesses at a completely lock-down tight and you can't go anywhere from within the business to the internet.

Greg Hughes: Right.

Andrew Hayter: Just very specific internet sites are very, very limited and highly controlled. So there are a lot of things you can do upfront to take advantage of this.

Greg Hughes: So once again, it's really about the balance, balance your people, your people controls and process controls and your technology controls and leverage them together, build that Defense in Depth for that layer security model. It's really the same story whether it's malware or software development or infrastructure or what have you.

Andrew Hayter: Yeah and I think you have to take a balanced approach. You don't have to be so restrictive that the PC basically doesn't do anything all day but looking for viruses. That can be a terribly non-productive environment at all so it might push the end-user, those that want to do it, the kids and go in and disable some of the Anti-Malware protection too so you have to fast rate that balance between performance and protection. Letting everybody and educating everybody to know that that performance hit that maybe taken on your machine in some instances is the protection and it needs to be there to safeguard what you're doing and then all the other standard business practices are backing up information, backing up your desktop, backing up your servers, backing up all your information so that as soon as you get attack by anything you do have and retained a clean copy of your work. Again, nothing has changed when it comes to normal security and standards like that, but being a little bit more diligent about how you do it and when you educate people and keep them in the loop is of prime importance.

Richard Campbell: So we find that most of the infection vectors these days are social engineering

vectors, that let's say leaving USB keys in the parking lot kind of stuff or click on this, rather than the direct infection vectors that we call hacking.

Andrew Hayter: I would say that you break it up on a couple of things. There's hacking, there's targeted attacks, and then there's social engineering. Hacking is something that the typical end-user can't control, but those who have oversight over systems and development and websites and applications certainly can set their programs up for better standards and do security in mind when they're doing applications so that they couldn't be hacked. Certainly those putting up web servers, corporate web servers and corporate web pages, they have plenty of information on how to develop a web page/websites so that it can't be hacked and I think a lot of those considerations have to be considered and there's nothing to do there, they're stacked with plenty of documentations to help you from that. So hacking is going to happen, you've got the web pages that you need to just set things up properly. The social engineering part, well, that again is a learned behavior.

Richard Campbell: Right.

Andrew Hayter: You have leaving the USB key in the drive, a very, very easy thing to fix and that's turn off auto run. That's been going on for a long time, you could turn off auto run. If you think way, way back in the days when they have these things called diskettes, let alone floppy drives, one of the features and it's still in some of the anti-virus products you see today, is to scan of the removable media on shutdown and that was very important for diskette drives because you could boot from a diskette drive. So one of the vectors you use to have was you'd have a diskette in your machine that was infected but it hadn't executed yet so you shut down your machine and the next time that you turn it on of course it would try to boot from the diskette drive first because the diskette drive was bootable, it would have an infection on it and that infection would spread so the thought was to do a shutdown scanner and you'd look at the diskette drive as you shutdown; therefore, you'd know right away if you left something on the drive. You can disable auto run and that's well documented on how to do that and it's a little bit more complex than just going in and tweaking a setting, to turn off auto run. There are lots of components to auto run that are very well documented. I believe in the case of Microsoft Operating Systems, they have very, very well documented all the different iterations of auto run and how to work within the registry to turn those things off and that's a corporate policy, you could set that policy and push that out to all your end-users to set up the way you would like it to be set-up. So you have those things. Let's look at one more aspect to social engineering. Clicking on things that



you shouldn't be clicking on, responding to emails and blind links that they don't know what they are, working with Twitter. One of the issues that you find with the vulnerabilities are the problems that Twitter had recently, are the use of URL shortening tools. I think the first one that happened around Easter was it was a Bitly, a Bitly URL, and Bitly basically takes a great big long URL that's hard to remember and it takes a lot of space written by Twitter members with 140 characters and shrinks it down to this little thing that you can click on it but you don't inherently, by looking at the Bitly URL know where you're going. So people click on this Bitly URL from people they thought they can trust and voila, they were infected with a cross-site scripting vulnerability which downloaded a malware.

Richard Campbell: Right.

Andrew Hayter: It's a learning process. We go back and you mentioned auto run, you look at **Conficker**. Now, one of the things that's very, very important for everybody to know, and this is the IT professionals, is update, update, update. Automatic updates should be turned on. You should be applying the updates. Whenever Patch Tuesday comes around, you should really, really evaluate the updates that come out on Patch Tuesday and apply them as soon as it's physically possible to all your end-users. If you look at the Conficker worm, the vulnerability that **Conficker** took advantage of, which was patch by Microsoft more than a month prior to the first outbreak or the first views of **Conficker**, had everybody applied the patch in a timely fashion **Conficker** should not have done anything because the hole was fixed. Yet we see that there are hundreds of thousands if not millions of machines infected outside the normal world by **Conficker** and when you look at the statistics of **Conficker** a lot of that were copies of Microsoft Operating Systems that were bootleg, they were not legal copies therefore they didn't have automatic updates going on them all the time. A lot of this is preventable. **Conficker** pretty much, from my opinion, was preventable had you performed all your updates. Had you had a legal copy of the Windows Operating System, it would have prevented **Conficker**. So just do everything right and you should pretty much stay clean most of the time. That's not a hard thing to do, but we've talked to several companies who have old servers and they're just running old operating systems that they haven't updated in quite a long time and they want to know how can they -- you know, they've got a problem, what is this problem, what do they do about it. We'll say if you update your servers this would have been protected. It's not always easy to go back to something that should be updated a year ago and get it into the process and then meet that on this server that needed updating. So be honest with yourself, auto fit your company and say I've got to

update everything or else we're going to have big problems.

Richard Campbell: Yeah, no kidding and of course people are hesitant on patching because patching has its own consequences. It's almost as if we should have a separate stream for this but this brings up a sort of core conversation which is this whole zero infection day battle. When this thing first comes out and you're sort of in a race to get the signatures in place and battle things back versus these are know viruses, they're spreading by slower vectors and we have time to do the updates. How are we doing here? I'm just trying to get a sense from your perspective of where those battles lie.

Andrew Hayter: The zero day threats, from my perspective, even though they can be serious threats, they're generally not a threat that has a large target base initially and I think there's been enough in the press, the typically there's a fast enough reaction from the operating system vendors or browser vendors and a very rapid reaction from the anti-virus malware developers, Anti-Malware developers, to update their products and with the changes in the nature of the Anti-Malware products going from a signature-based to a heuristic-based type of environment, with dynamic-based type of environment, a lot of these threats can be caught fairly immediately. Now that could be hours or days but this is not something that I think is your all day threats, you're going to hurt too many people anymore because it's typically taking advantage of more of the really obscure vulnerabilities that exist and not everybody is going to be attacking the more obscure ones because the more obvious ones have been patched-up and covered already.

Richard Campbell: Right.

Andrew Hayter: There's a whole lot more due diligence going on right now in preventing those any kind of vulnerability upfront; however, that condition still exists so you need to think about that at the same time, but again keep it up, keep the passion. You should be fairly, fairly good with this.

Richard Campbell: It seems to me we have a good engine around that, that the thing that we need to pay attention to is the social engineering side in getting our users aware of the things that they're doing routinely that are creating infections.

Andrew Hayter: Correct. You can't say enough about the social engineering fact. I think I haven't seen statistics in the corporate environment. In the home user environment, it's rampant. I mean, in a corporate environment, you can probably control things a little bit better by not permitting things like Twitter or Facebook from occurring during the business hours or on business equipment. Certainly



policy had a lot to do with that and that's again part of education, corporate policy that says you don't do these things on these machines. In this business it's corporate policy. It's terms of employment. That's another possibility as well. I think one possibility is often overlooked and it depends on the company, the size of the company and things like that. If you know your users are doing a lot of work at home on their own machines by accessing corporate systems remotely and if you're using VPNs and other methodologies, that's great for security but why not offer your home users the same Anti-Malware protection that you have on your desktops so at least you know that they're using something and they're not risking your corporate assets in another way or bringing something in there that might be infected because not everybody at home is going to be using the most up-to-date and latest piece of Anti-Malware products. They may use what was shipped with the PC and not choosing to sign a subscription to get it updated so they're having out of date software. So maybe another policy could be, "For all my home users, here's the copy of what we use at work." Yeah, it may cost me something but how much savings will I have by giving people at work the option to use a product I know is current and updated. That's another opportunity for people to protect their systems further.

Richard Campbell: I'm going to try to stay away from product names but I know that there are vendors out there that have built products so that when you attempt to connect to the business network, it interrogates your machine fairly severely and insists on a certain level of patching and security before you're able to access those business resources in the first place.

Andrew Hayter: Right. There are products out there that, believe it or not, they're not the AV products, the Anti-Malware products themselves all the time. They're other third party utilities that offer that service and that level of configuration of profiles to validate before you connect to the system that you have all the right level for patches and operating systems and latest signature updates. You see that a lot in SSL VPN type of environments as well where you're doing that environment.

Richard Campbell: Yeah.

Andrew Hayter: And there are products out there that work that way.

Richard Campbell: And I do think that the USB key thing is a huge problem that folks are going from infecting their key at home and then taking it to the office.

Andrew Hayter: That's exactly what happened 15 years ago in the anti-virus world. It's when you

didn't have a machine at home but you're allowed to do work at home...

Richard Campbell: Right.

Andrew Hayter: Or you work on a spreadsheet at home and you'd be cranking on this spreadsheet and unknown to you someone had been on the computer ahead of time and brought a game in that their kid got from school and that game was infected and infected the diskette that you saved your spreadsheet to and you put it in your computer at work and you infected your computer at work and all your colleagues and things like that. It's no different. I mean, it's just another form of portable media, it's the flash drive; and again you can prevent it with auto run, you can prevent it with automatic disk scanning when it's put in. There are lots of ways to prevent it, it's just that you've got to do it and sometimes it takes a little extra effort but you've got to evaluate the price of security and go from there. I think one other point that I just remember now that we want to cover too is what we call targeted attacks.

Richard Campbell: Right.

Andrew Hayter: Because we've talked about zero day attacks, we talked about social engineering and everything like that but I think we have to think about targeted attacks too. Targeted attacks are looking to take advantage of one company or one reach in another world and they're a little bit more difficult especially if there is a zero-day of attack to deal with because not everybody is going to be seeing this attack and not everybody is going to have the information about it. But the targeted attack can be going after one company's assets, find a vulnerability in that company and then just going in there in zero-day fashion and they just clobber the company and doing as much damage as it can in one day and usually they're in and out one day, or one or a couple of hours, and they're over with. So you have to be aware of targeted attacks, either targeted to a company or targeted to a region of the world and then they can be a little bit more precarious, a little bit more difficult to weed out. Or in a large company that is operating in different parts of the world might only have this targeted attack in one part of the world and then because you're interconnected on the corporate network, it could spread. Even if it wasn't intended for other geographies, they could spread that way.

Richard Campbell: Absolutely or again if this is an engineered attack, if your company is being attacked that way, they go after a branch office that is sort of the weak link given the control or the permissions there, you now have access to the entire infrastructure.



Andrew Hayter: Right, correct. I think that one of the important things for the IT professionals on the security side to instill in their other organizations is when you start putting a lot of devices out remotely, that you do configure the device and do change the default passwords and user IDs, because frequently I've seen that condition exist where the whole company got infected because the remote side or the branch site had wide open user ID and passwords, they never change it from the default and that's an easy way in, and most people going out there trying to hack that's one of the first things they're going to try.

Richard Campbell: True.

Andrew Hayter: It's by using the default's password and user ID.

Richard Campbell: In unsecured WiFi node in branch offices.

Andrew Hayter: Yup. It's not that every WiFi node, but yeah, that will work too.

Richard Campbell: Yeah, same sort of thing.

Andrew Hayter: Yeah. I mean, in an open WiFi node, you're going to be doing a little bit more war driving and driving fast and sitting in a parking lot but there have been some very well-known hacks that have cost companies a whole lot of money, billions of dollars, because of someone sitting in a parking lot with the mobile device snooping in and collecting information.

Richard Campbell: Yeah.

Andrew Hayter: So collect your information, or if you're going to be collecting information outside of the anti-virus, you have to do it in a secure fashion and you have to encrypt the information and then you get into the whole thing, if you're dealing with credit cards, with implementing the right PCI 1.2 levels of protections and doing your audits, doing due diligence in your audits to demonstrate that the products you're using your implementation meets the criteria within PCI 1.2 for credit card transactions.

Richard Campbell: I think PCI is a whole show unto itself because it is a great topic, certainly a standard that I have to work with in the past.

Andrew Hayter: Right and if you look at the latest PCI 1.2; section 5 is all about the entire virus. So that's a whole node that you write. It's a whole node of discussion but when you're starting on a corporate environment putting all these pieces of the puzzle together, it seems like a whole lot of work but it's there for protection of your data, your company assets and your customer's assets.

Richard Campbell: We're almost heading to the point where we start to talk about the cyber warfare angles of this when you start talking about targeted attacks in regions and so forth. I'm thinking about the recent incidents around the country of Georgia where there was a concerted effort to disrupt the entire internet for that country and Malware can certainly be a part of that attack.

Andrew Hayter: Yeah, that was two years ago almost now.

Richard Campbell: Last year, yeah.

Andrew Hayter: Last year, the Georgia attack in Georgia and part of that you have Estonia where that was thought to be the first to real cyberwar and then Georgia, and then in the past week you had a series of attacks in South Korea and in the US that have been targeted attacks. What I think you have to consider is there's a whole lot more of this going on than meets the public eye.

Richard Campbell: Yes.

Andrew Hayter: All the time I think this type of environmental attacks have been around longer than the public seems to be aware or things like that, and again they're targeted, they're political in nature and how can you prevent them, it's an awfully tough question. When you look at the attack this week in Korea, South Korea, and in the US, there's still a lot of debate and a lot of evidence to be collected out there to be determine exactly how this got into so many systems in South Korea and what was the mechanism, what was the access mechanism to get in to just so many systems; and that still is a wet Friday when I pulled some recent papers on this. There's no good information on how these DDoS attacks started and how the Malware is a bottleneck, how a bottleneck got so spread out, went undetected, and then triggered itself and did massive DDoS attacks on many, many, many URLs that were out their domains. So these things are going to continue to happen and hopefully the governments, the US government will look in at cyber threats a whole lot more seriously now. Many other governments are looking at it from their own government perspective but I know there's a tremendous amount of international cooperation on cyber threats and sharing intelligence and sharing technical information that should over time be better to manage and understand and see these things coming before they actually occur.

Richard Campbell: Andy, thanks so much for coming on the show.



Andrew Hayter: No problem, Rich and Greg. I greatly appreciate the opportunity to let people know about what the latest in the world of Anti-Malware; and my final thought would be if you're evaluating your Anti-Malware or any other security solutions, it's to take a look at what ICSA Labs offers in the form of lab reports to again get that third party validation and testing information about the security products you're choosing.

Richard Campbell: So that's www.icsalabs.com.

Andrew Hayter: That's correct, that's our website and get there, get the reports, get the latest information on which products are certified.

Richard Campbell: Andy, thanks a lot.

Andrew Hayter: You're welcome.

Richard Campbell: And we'll talk to you next week on RunAs Radio.