NETEVENTS

GLOBAL PRESS & ANALYST SUMMIT

Debate I:
Ransomware, Spearphising, and Worse

Chaired by: Andrew Braunberg

Managing Director, Research NSS Labs

Panel:

Bryan Gale, VP Product Marketing, Cylance

Greg Fitzgerald, Chief Operating Officer & Chief Marketing Officer, Javelin Networks

Greg Maudsley, Senior Director, Product Marketing, Menlo Security

Greg Enriquez, CEO, TrapX Security

Frank Wiener, VP Marketing, Wedge Networks

Andrew Braunberg, NSS Labs

While they are assembling up here, we can just get moving. I've just got a couple of slides that we can think of these very much. It's kind of ransomware 101 just for folks who aren't quite security people in the room. I'll do a quick kind of definition and then we'll get these guys talking about some of their different techniques they have for solving some of these problems.

So the big session was supposed to have been about ransomware, spearphishing and other attacks. Ransomware is just such a huge topic of conversation right now, it seemed like the one we should focus on, so that's my goal here. So, again, just a couple of quick slides.

Definition, what exactly is ransomware? Well, it's nothing new, but it is getting much more sophisticated. Basically what it is, is malware makes it on to your device. In current iterations it will encrypt files on that device and they can be eliminated or could actually be more recently it could be a full disc encryption, lock everything down and then make you pay to get your data back. How you would get that data back is you would pay the hackers and

they would send you the private key and you would unlock your data. So it's relatively simple.

As I say, it's not particularly a new idea and ransomware has kind of evolved from what we were talking this morning at breakfast. What was really more kind of a scammy kind of approach to having fake performance assessment applications that they would deliver on your device or fake AB software they would put on your device and claim you needed some level of remediation, of course, which you would have to pay for.

They kind of migrated into just locking your device down but not actually encrypting your files or your data, just making it difficult to actually access the device and again pay some ransom to get that removed.

Now we've moved to very sophisticated encryption methods to completely make your data unavailable to you. It's clever, but it's really frustrating to say the least.

One thing I want to point out, and this will come out with the group up here, there's nothing particularly innovative or unique about the way this malware is delivered, so keep that in mind. It's the same techniques that people have been using. It's phishing campaigns, it's spearphishing, it's drive-by downloads, malvertising. These are things we're familiar with. The issue here is that once the malware gets on your device, it's particularly pernicious.

Another think I would just point out is that if your data does in fact become unrecoverable and the FBI, by the way, for the United States folks is currently telling victims not to pay the ransom and just kind of grin and bear it, but by the way, please send us a little note and tell us how much you pay, all the details about your attack. If you actually did pay to get it back, they would be curious how much you paid them. But they would prefer you don't at this point.

So that kind of gets us the quick and dirty overview.

Now we've got a really interesting panel up here who approaches this problem from a lot of different ways, which I like. I might hop here I think to take a few notes, but why don't we just run down the list.

We've got most a Greg panel here, by the way, but I'll let them go. Greg, do you want to go first and we'll go down and then we'll open it up.

Greg Enriquez, TrapX Security

Good morning. I'm Greg Enriquez with TrapX Security. We're an advanced cyber defence company. We use deception technology in the way we implement protection for corporations and governments.

Frank Weiner, Wedge Networks

My name is Frank Weiner. I'm with Wedge Networks and Wedge provides security both for the cloud layer to provide security as a service and endpoints. As Stuart alluded to this morning, our game is really about prevention, blocking threats from entering the network.

Greg Maudsley. Menlo Security

Yes, I'm Greg Maudsley. I'm the Senior Director of Product Marketing for Menlo Security. We're also in the game of prevention. We're focusing on a new technology called Isolation which basically provides 100 per cent insulation from web and email threats.

Greg Fitzgerald, Javelin Networks

I'm Greg Fitzgerald. I'm representing Javelin Networks here. We are focused on attackers post-compromise. Our esteemed colleagues here who are preventing, as Stuart McClure stated, it's kind of hard to keep attacks off. We focus on what the attacker does next, the subsequent attacks on the compromised machine and keep them contained. That's what Javelin Networks does.

Bryan Gale, Cylance

My name is Bryan Gale and I work for Stuart. I run product marketing for Cylance. I think you all got a pretty good introduction just a few minutes ago in terms of what Cylance does. But we use AI and machine learning on the endpoint to predictively block cyberattacks on the endpoint.

Andrew Braunberg

Yes, great. Okay, thank you all. I appreciate you being up here. I know we don't try to make these really tell me exactly what your product is up to when we do these, but you approach this in really different and I think interesting ways. We've got definitely five different approaches up here and again let's think some of them might be very targeted at ransomware specifically. Some of them are just addressing some of these other points in the kill chain, if you will, on how that malware is getting to the device, or what we do afterwards. So, again, some different approaches here.

Bryan, why don't we do it in reverse order? Do you want to drill in a little bit without making it too much of a complete product pitch but just give us a little bit more colour on how you guys are approaching it and at which point in the chain?

Bryan Gale

Sure. So, if we focus on ransomware specifically and the point of the chain at which we block that, we are purely an endpoint technology. We're not at the network layer or any other perimeter device at all whatsoever.

From a ransomware standpoint specifically, one of the things Stu alluded to earlier was there is not really new techniques or things being done. A lot of it is just repackaging of the old capabilities. The way that we're unique from the rest of the incumbents, traditional blacklisting players is we don't rely on a signature for a file. One of the things we see with ransomware is the rise of ransomware as a service platforms where anyone can effectively go out and within 10 minutes get a custom crafted binary and payload from a malicious attack at an organisation that they choose. Now, that attack is guaranteed to evade defences from traditional signature-based ABs because the ransomware platforms are actually testing these packages on a daily basis multiple times a day against those signatures that are created by the AB industry at large. So we need a new approach, a different approach, than signatures to try and block those.

So by analysing or extracting the common features within those ransomware variants and being able to predict that something is malicious or not has proven to be very, very successful for us and that's why we're seeing a tremendous amount of growth and traction in the market.

Greg Fitzgerald

Great. Now, what Javelin Networks does is once the computer is compromised and actually locks up the computer, the ransomware actually has gotten very mature today. It's using doing something else in the sense that it is not just saying this computer is locked up, send me a bit coin to unlock it. It's usually siphoning data off that machine and trying to gather further information to penetrate because if you can think about what the attacker actually wants is not just to get one machine, he's trying to get to many, hundreds, maybe thousands and usually lock down that particular organisation so that it's actually a serious problem and they need to pay that ransom.

So Javelin actually automatically and autonomously is picking up that movement, or those activities on the host of what it is looking for - new credentials, or other machines that it needs to try to get to. It's alerting silently to those IT managers and then it's actually locking down that particular machine from the attacker so that that data can't leave, or that they can't penetration further into the organisation.

Greg Maudsley

Great, thanks. So Menlo Security has a cloud-based isolation platform. It doesn't require any endpoint software, nor an appliance. Our approach is that we don't make any sort of good versus bad determination. Our assumption is

that all websites are bad, all emails are bad and the only way to effectively prevent any end user from getting infected is to isolate them 100 per cent from those threats.

So we spawn virtual browsers in our isolation platform in which we fetch and execute all active content and then safely rewrite and transcode only the safe visual elements down to the endpoint. We effectively, by that way, by not passing any active content down to the endpoint, insulate the users from ever contracting malware, including ransomware.

Frank Weiner

For Wedge Networks, our approach is to scan the data and remove threats before it's delivered to the end user. Our systems, we've got two different sets of solutions. One, operating at the cloud layer to inspect all data flowing to and from all users at all locations. We're about to introduce a new family of products focused on the enterprise which provides the same types of capabilities. So it's detecting spam and malware and viruses, those types of things that are introducing ransomware.

What we're going to be announcing tomorrow is a new initiative to bring some of the artificial intelligence that was discussed earlier this morning into the network layer so that we can use this to protect not just the endpoints that are running artificial intelligence locally, but the Internet of Things and other devices that are introduced into the enterprise that might not yet have that artificial intelligence. By taking the traditional multi-layered approach into the artificial intelligence realm, we expect to really up the game and raise the barriers and make it more and more difficult for those threats to enter.

Greg Enriquez

I'd like to drift a little bit into the history of ransomware since I had personal experience. In 2012 I worked for a company that was actually cited in ransomware that was attacking individuals' computers and that's where it started. The attackers thought I can encrypt a C drive and collect $300 through a credit card from an end user. They got smart. They evolved and they changed and they figured out I can get $300 from an end user. If I encrypt a share drive and I encrypt a network drive, I can get $17,000 from a hospital or from a corporation.

So in the early days we had TeslaCrypt that started and it went through and it encrypted first the A drive, then the B drive, then the C drive, then the F drive, then the Z drive. That evolved and it started going backwards, working from the middle both ways.

We then saw from TeslaCrypt additional ransomware like Locky which was recently out and then we moved into Seven, which is the most recent strain of ransomware.

What they're doing is they're going after corporations where the real money is and they're going after the network share drive and they're trying to encrypt the real data. They don't care about the C drive or the end user anymore.

So what we do at TrapEx Security is we shift the cost to the attacker. We put fake networks out there and fake assets, so as soon as they hit the end user they get directed to a fake share drive or a fake server. Then they start to encrypt our fake system. We immediately alert the system that the encryption has begun. You may lose the endpoint, but you won't lose the corporate data or the government database that you're most interested in.

So what we've been able to do is shift the cost to the attacker, evolve our approach to stopping ransomware so that they can't get what they're after and then we can do what Stuart said, they'll go work at Kentucky Fried Chicken or other places.

Andrew Braunberg

Thank you. All right, I should probably ask which approach is best, but I think that would probably take too long. I should have asked though, and I'm glad you brought it, has anyone in the room been a victim of ransomware that they want to admit to? No shame in it obviously, but just kind of curious. No, no one in the room, that's probably surprising.

Greg Enriquez

Our phone lines lit up because they cited our company in the end user ransomware and so they call us and say I didn't go there. You encrypted my computer and said I was going at bad sites.

Andrew Braunberg

Okay, that was good. There was a lot of good points brought up there and that will segue nicely I think into where we want to go which are some of these drivers. But the distinctions between prevention and lateral movement I mean there is a lot of bits here that can help limit exposure. This shift to which I should have probably brought in on the frontend when I was talking about moving from mostly being consumer victims to a lot more corporate victims right now and the hospitals that got mentioned. When you think about it, who the heck would lock up healthcare records in a hospital? It's just crazy. But it gets to the point of motivation, or how far down the stack are we going. I

think Stuart called them ankle biters, which I like as a term. Script kiddies is another one you can use.

The tools here are getting easier to use, so maybe we can run back through. This morning we were talking about a lot of them are about approaches, the dollars being major drivers, the ability to have these things available as a service, the sophistication of attacks is getting a lot heavier, just some inherent weakness in web platforms. These all came up and I know you all have opinions on them. Can we just bounce back through from you Greg and just whatever one you want to point out and maybe elaborate a little bit on some of the issues that are driving this.

Greg Enriquez

I will touch on healthcare a little bit. We all have the adage if they want to get in they will get in. We certainly must protect the perimeter. It's the first level of defence and you have to do it, but they will get in, so then what. We want to watch the lateral movement and where they're going.

What we've seen in hospitals is they will get in. They will get in through an administrator or through some spearphishing approach. Once they do get in, they will find the most unmanaged and the simplest devices and those could be the medical devices, the blood gas analysers, the PAC systems, the radiology equipment that's running back levels of Windows that isn't running current advanced cybersecurity defences because they're protected by the manufacturers and the FDA. So those are places for the attackers to hide out or dwell with ransomware and other areas.

So now you think about the motivation. If I can encrypt your drive and get money, what if I encrypt your blood gas analyser and stop the operating room, or stop surgery from taking place, or the PACs device so you can't share radiology information across which should be an open hospital network for doctors, clinics and providers to use?

So I touched on your point of what could be a motivation. Ransomware could be an approach to blocking the use of industrial control systems, hospital systems, and other things that we need to run our daily lives.

Frank Weiner

What's interesting is ransomware is basically easy money, but it's not just easy money for the cybercriminal that is extorting the money from you. They're beginning to commercialise the technology and make it available in the form of ransomware as a service on the dark web. What that is doing is it's lowering the bar for the skillset for cybercriminals to be able to go in and execute with very advanced technologies in terms of breaking in and delivering ransomware. So there is a whole commercialisation and, if you will,

industrialisation that's beginning to happen that's just going to increase the amount of activity on this front. So the value and the effort being lower, that's an interesting set of drivers.

Greg Maudsley

Ransomware attackers are taking advantage of the inherent and increasing vulnerability of today's web. So, you and I as users of the web demand a rich experience. We want scrolling videos. We want all kinds of interactive content. In order to do that, today's most popular websites have to pull from dozens of different other domains all over the world. They have no control over the OS that those other domains are running and in many cases, they're running very, very old operating systems with known CBEs, or vulnerabilities.

So it's not enough to just compromise or install a drive-by on a site. You can go to a background domain which is much easier to compromise and that's what they're taking advantage of in many parts, in many ransomware attacks today.

Greg Fitzgerald

I think overall, cybersecurity is interesting. I've been in it for over 20 years when it was just encryption and a user name and password. It's always this cat and mouse game. I think with all the technologies you've got we're finally trying to give power back to the cat because the mouse has been winning for a while.

In that sense, the idea is let the mouse get the cheese, but don't let him get the entire block. Let them get a little crumb because trying to prevent the entire cheese block from getting eaten is much easier than it is to allow them to have a little bit because they're going to get in right, some way, shape, or form, whether it's through malware, or whether it's through credential stealing, whether it's because you've actually got a rogue employee who is completely legit, right. It's now about the activity that the attackers are doing.

So I think frankly the security guys and what Stuart has said around the new models that are coming today using artificial intelligence and mathematics that are advanced is making it much more effective in the way the security industry is helping organisations and it's making it much more efficient. Because, if you think about it, there is not enough security personnel in the world, there is not enough money in the money and there is just frankly not enough time to prevent these attackers from getting in. There are more bad guys than there are good guys.

So I think as we see hopefully in the next year or two here we're seeing a change of the good guys winning a bit more before the bad guys stop. Next year when we're all together here in America hopefully we're not talking about

ransomware. It's probably going to be another problem that we're all talking about that the bad guys have figured out how to penetrate the organisations.

Andrew Braunberg

Bryan, if you could keep it relatively. I think I ran over. I'm not trying to cut you off.

Bryan Gale

I'd turn it back on kind of the motivation. The motivation is very much financial. To give you guys a sense of the scope of the problem, there was a report that came out I think a little bit earlier this week. Since we're in Silicon Valley right now, a good metric of success, think of any start-up that reaches that plateau, or not a plateau but that milestone of $100 million in revenue, well that would by all measures would be astounding success.

A report earlier this week highlighted just one single ransomware platform, syndicate, whatever you want to call it, that brought in $121 million only in the first half of this year alone. So they're close to a $300 million run rate as a ransomware platform. They build an admin console, they provide support, they guarantee the binaries get by detection. It is entirely financially motivated and way too easy for anyone to go create a custom package and attack an organisation today. So it's all financially backed right now.

Andrew Braunberg

Excellent. Do we have time for some questions? Great.

Michael Howard, HIS Markits

Michael Howard. I used to market formerly Infonetics. Every time I think about security I think about the complexity of networks and they keep getting more complex. There is the cloud and everything involved. How does an IT director, or whoever is responsible for an enterprise, choose a security vendor, or do they have to choose 25 security vendors? It seems to me that's not ransomware, but to me it's always the same problem. Who do you buy from and how many do you have to buy from and which parts of your network have you covered and which parts of your network have you not covered?

Andrew Braunberg

It's a great question. Greg, go ahead.

Greg Maudsley

I would like to start. I won't talk long because I will let the other guys. We were talking this morning about that and it's really security still continues to be like an insurance game. It's a risk game. How much money do I have to spend for how much defence can I have?

In answering your question, each organisation is very different. What we as vendors have been working on are hopefully more efficient, effective models, or approaches that make that decision more flexible to the buyer. So, if you're a cloud company and you're like hey we want to centralise everything and send everything through a cloud, that's the better opportunity. If you've got a lot of distributed individuals that are not connected to the cloud, I mean through your corporate cloud, then you probably need more of a malware prevention because they've got to be disconnected and protected.

So I see what's nice about today's world, while yes, it's very complex and I'm a part of that problem - all of us are creating this marketing that says the same thing do we stop attackers. The beautiful piece is that the flexibility for the buyer is now available because if you think about five years ago pretty much we all did the exact same dog gone thing and you had to take it as it came. But thank you to the cloud, thank you to this powerful computing that allows us to do so much more effectively and efficiently. You guys can comment more, but that was more of a generic approach.

Greg Enriquez

I'll just add to that by saying a security buyer has to stand back and look at what their risk is, who the attacker is, who they think their adversary will be and then build a layered strategy around that. You have to think about the problem you're trying to solve, not the solutions that are out in the market. There is 700 security start-ups every quarter I think. I'm not sure.

Andrew Braunberg

There are 1500 vendors out there that we are keeping an eye on. I think the insurance comment is really important. I think cyber risk management is not nearly as sophisticated as many other branches of risk management and this idea of cyber insurance and using insurance as a vehicle to transfer risk is a really interesting one. It's one that's been gestating for a decade or more, but it's getting more sophisticated.

It gets back to the actuarial data comment that was made in the keynote that part of the problem is there isn't that actuarial database to be able to really create the right premiums for the coverage that you're getting, but that's getting more sophisticated.

Eventually I think we will get to the point where insurance companies are driving risk and best practice decisions much as they are in many other areas of our lives. But it's really not the case in cyber today.

Did anyone else want to jump in on that one?

Frank Weiner

I can chime in on that one as well. To your point, it's all about risk and to echo something that Stuart said earlier, if you look at the four elements of risk that CISOs are looking to mitigate today, it's basically application and server security, it's access security, it's web, and it's email. As you're looking at how to allocate your budget across those, CISOs that we talk to indicate that web and email account for about 85 per cent of the risk that they're trying to mitigate today. So that certainly factors into who should I buy, how much should I spend, and how I keep my budget.

Andrew Braunberg

Anybody else? Do we have time for another one? No. We're told we're done. I'm sorry about that. I take complete blame for that. Thank you, gentlemen.

Greg Enriquez

Thank you.

Frank Weiner

Thank you.

[End]