FEDERAL
TECH
PODCAST

Ep. 34 Weaponized Files and Federal Cybersecurity

My name is John Gilroy and I'll be your moderator. Today we have Darren Curtis, Vice President public sector at Menlo security. And we're gonna talk about cybersecurity and browser isolation and many different aspects of securing the federal government. But Darren, before we begin, maybe give us a thumbnail sketch of Menlo and how you fit in this whole discussion, please.

00:41
Sure, Menlo security, about 910 years old company. We focus on security a different way. It's probably the easiest way to do it. We're using isolation technology to help prevent attacks instead of responding to attacks.

00:58
An ounce of prevention pound of cure. We know that one, don't we? We do. So Menlo Park, California, I shouldn't say Silicon Valley company been around for over 10 years. Is that right?

01:09
I've been around 10 years not far from Menlo Park. We're in Mountain View. California is headquarters.

01:14
Good, good. I go to LA all the time. I don't get that far north in California at all. So I went to your website, and I see this big fancy acronym called heat. And I remember those gangster movies from the 1930s. You're packing heat, you know? So So what is heat all about? I thought this is ice browser for isolated browser. So what does he need? Anyway?

01:34
That's a good question. Then we need another acronym for the government. So we decided to add heat for but highly evasive adaptive threats, which is another reason why it's an acronym, because that's a mouthful to speak to. It's more about what we're trying to draw attention to, which is, actors, bad actors are getting away with doing a lot of things very creatively. And they're working much faster than what our security technology can keep up with. So what we're trying to do is say, you've got potentially legitimate looking threats, getting through your existing security stack. And we believe you need isolation to go from responding to preventing, and the only way you can do that is preventing code and other forms of the threats where they're getting in getting through to the device or to the Agency Network.

02:36
I've been doing this for many years. Darren back when you're in high school, I was on NPR answering questions. And I'd answer questions about PDFs, you know, and for PDFs, PDFs for decades had this like this

sacrosanct, impenetrable, never get in no problem at all. And all of a sudden, the last few years, something as most people think is secure as a PDF can be compromised, and other graphic images can be compromised. And, and so people can let down the garden and bring in a PDF and all of a sudden, that is highly evasive, adaptive technique doing something everyone trust, isn't it?

03:09
That's exactly right. And I mean, the the phrase zero trust really needs to adhere to zero, as in never trust is something that is we're all hearing about in the government, particularly with a mandate from the executive order. But it's critical that you focus on how do you never trust and never trust includes never trusting even that PDF, which could be trustworthy.

03:36
So I set your website reading the blogs this morning, and I read a phrase, I haven't heard this phrase before dynamically generating logos. I mean, now this is awful creative, isn't it? I mean, and if I saw a logo from sports organization, and oh, yeah, here's my tickets have to click on and so what malicious actors are doing is now is they're dynamically creating logos that are very similar to a standard logo. And, and people are clicking on them on phishing email, aren't they?

04:01
Yeah, they sure are. It's a great example of what an evasive adaptive threat really is. You can also think of an HTML smuggling campaign, which is using legitimate looking encoded, you know, malware that is getting through because it looks like common HTML, what you need to do is prevent that from ever getting through directly to the user or the Agency Network.

04:25
I interviewed a person from a rather large company, and this person said that they never answer email, because they're on Slack. Slack is great. And so we got Darren Curtis saying, oh, boy, I would take and exploit the Slack channel. And so you know, I'm gonna avoid all that fishing by going to Slack but this is another tech channel

04:46
isn't. It is SMS text. It's a very common phishing angle. And if you look at the octopus campaign, the phishing campaign from octopus, you know, they're trying to gather people's credential multifactor authentication data and be able to steal log in legitimately log in was stolen credentials and access company. You know, Crown Jewels, shall we say?

05:12
You always think of teacher for years, so I have to spell things out. So this is okay, tap U S, and the big word play is a company called Octo, which handles identification, and so they penetrate some Octa code or what happened with this octopus?

05:27
Well, it's a good question. And we're big fans of Octa multifactor authentication is critical piece to good security. But what they're doing is not penetrating Octo. What they're doing is using a phishing campaign for a user to gather their credentials unknowingly, and showing a fake Octa website. And then that what they're using is those credentials that they've stolen, to actually access the company from there.

05:59
So some people call us technology, an RBI technology, remote browser isolation. I keep thinking the World Series, so I'm gonna get RBIs now and Bryce Harper RBIs and Bryce Harper, and what's going on in Philadelphia here? So what? What is the biggest challenge in deploying something like this? I mean, what's the biggest challenge that mental has in working with federal agencies to deploy this RBI? Well, I think that,

06:24
from a challenge perspective, it's one understanding what isolation can technology can do for you. And it's not necessarily a written replace technology, it's an enhancement to what they already have, where you're increasing the security posture by adding isolation to perhaps an existing secure web gateway, or next gen firewall or a WAF. What we're trying to do is never allow code to be directly downloaded to the user's machine or the network.

06:56
I have heard serious debates about wife's web application firewall, application firewall, yeah, I've heard I've heard security guy just throw chairs and yell and scream at each other over this. I mean, really, it's like, get out of the room. This is a big debate, isn't it?

07:11
It isn't a debate. And it's a it's an important piece of technology. But it's not the be all end all. What you're trying to do is secure the application is really what that, you know, gets down to

07:24
last night, I was reading a book called Start With Why by Simon Sinek. And so I always tell my students to start with why. But I want to make a transition to who I want to start with who. So who uses metal security in the federal government now?

07:37
Good question, Department of Energy's client, as well as the Department of Defense, and we are deploying worldwide for the Department of fence right now, for all of their users across the world.

07:49
So it might seamlessly fit into this stack of applications or stack of products.

07:55

That's exactly right. I mean, obviously, the DoD is not ripping out all of their very good security technology. And assuming Menlo is going to be the answer for everything, there's still a whole lot that we need to integrate with. And that's a critical piece to the puzzle.

08:11
And integration is not just a technical term. It's also a I guess it's a solutions term where Menlo Park would would integrate and work with other companies in order to combine on a solution for something as massive as some DoD projects. Is that right?

08:25
Yeah, that's exactly right. I mean, there, there may be companies that do a certain piece of security extremely well. And Menlo is best in class in isolation. So why not combine the two rather than try to get one from everyone or one from one everything from one, excuse me, where it may not be the best of best solution available.

08:50
So well, cup of ice goes kind of cool sit on the deck, and we got out the heater for the duck. We turned it on. And I put my hand up there to see how hot it was. It's pretty comfortable for a nice evening in the fall in the Blue Ridge. And so that's how I check my heat. So how can customers in the federal government check their heat a GA T in your situation?

09:10
Well, we have a we actually just came out with a tool called Heat check. It's a free tool that we're offering. Think of it as a advanced penetration testing tool for the web browser or the browser, where you can actually apply it to your network and see whether a certain piece of will call malware but HTML smuggling we have have pieces that are vanilla, they're not dangerous to the network, but we can show whether they get through or not.

09:50
It's kind of like a penetration test. A browser penetration tester.

09:55
That's exactly right. And it's it's a it's free to use and We want everyone to see what vulnerabilities potentially they have, because it's an important way to secure the federal government.

10:07
Menlo security.com, for that piece of free software. I was there this morning. And there's another great report. And I have to tell my listeners about this. It's called 2022 impacts, ransomware attacks and preparedness. And this applies to the federal government. If you want to learn more, you can go to Resources dot Menlo security.com, and download it. But this is a curveball for me. I always thought phishing attacks are like for, for

Darren donuts in Chicago, or John Lee pizza store in Dallas or something. But But phishing attacks are going after federal agencies like DHS,

10:45
they are they're trying to shut down and grab data and use it for ransom. And what we're suggesting is prevent them from ever getting in by eliminating the weakest link in the security chain, which is the person that will always be the weakest link, they'll click on something either inadvertently or intentionally. And it's going to cause a problem. So if we can eliminate that as a threat vector, and literally eliminate ransomware from the federal government, that's a win.

11:14
I spent 10 minutes this morning trying to build a headline for this interview. And I came up with everything and played this and that and RBIs and baseball and all kinds of fun things. But I came up with a phrase, weaponized files. So that's the PDF used to be the safest thing in the world rock solid. Now, it is a weaponized file, I mean that it's a good title for this interview.

11:39
That is a great title. And it speaks to what I spoke to someone in the DoD awhile ago. And they they coined the phrase that I've continued to use, which is, if the file is weaponized, it detonates in the cloud rather than on our our agency network. And I was thinking, that's brilliant. I liked the DoD angle where it's detonating. And I liked that it's a weaponized file. But it's detonating in the cloud away from the the person's machine or the agency network

12:09
there. And we got to hire a cartoonist to come up with a cartoon for social media to describe with us here. And here's the half hour interview summarizing the cartoon. Well, I guess it speaks to the next quote I'm going to use, and this quote says ransomware is one of the biggest single threats to government networks. Really, I mean, five years ago, it wasn't I mean, it was it was at COVID. And what precipitated all this attack on the government specially with phishing?

12:37
Well, COVID, I think hackers had some more time on their hands to get better at what they're doing. But ransomware and government, it's not just the federal government, you've seen recent attacks on school systems, in banking, in county state agencies as well. They're finding a weak link, and they're exploiting it. And that's really the challenge that you, you need to close that weak link by preventing it from happening in the first place. And that's what we're trying to do. But it's definitely an issue that's growing, and it'll continue to grow.

13:13
So let's say I'm going to a Red Hat event next week, face to face trying to do once every couple of months now. And let's say you're there with me and someone walks up to you and they go, Oh, Menlo, what do people get mostly confused about? What do they do? They classified differently? What I think about mental security?

What do you always have to say? No, no, it's Menlo Park, California. What do you have to say to correct people when they have this assumptions about mental security?

13:36
Why usually, of course, there's the West Coast Silicon Valley angle, that we have to just describe where we are. But we have to describe what we do, you know, isolation Technologies, a new way of thinking for security, detect and remediate or responding after the bad guy is in your network. It's not working. And that's why we're seeing a growing threat and security. And what we need to tell people in this instance is how isolation prevents things from happening in the first place. And you need to start thinking of security as a prevention strategy rather than a detect and response strategy. Sort of like locking the front door rather than letting a bad guy in and then hoping you chase them out.

14:26
So there are other companies that obviously do have this isolation technology. So why is mental better and what's the magic sauce the mental has that the other companies don't?

14:39
Really good question probably better designed for a technical person who could give you the details of that. But in a nutshell, what we do is we don't video stream, the, the web or the Internet back to the user that is a bandwidth hog and it also is not high definition. You have a Hard time scaling that type of technology, what we do is called DOM mirror and document object modeling. And what that is, is literally providing a rendered image of the internet that you can freely interact with. But your if you accidentally click on something that seems good, but isn't good, that malware will detonate in the cloud. And the other great thing is, once you close the tab in that browser, you close the session, we have a disposable container that's holding that session, we throw away that container.

15:37
When I was thinking about these threats, I was thinking about a previous interview I did Episode 28, with a company that you may know of called spycloud. I interviewed Joel Bagnall, he, he worked at very high levels in the federal government, he has access to lot I did a half hour interview, and he couldn't talk about half the things I wanted to talk about. So. So if you want to hear a different perspective on this and hear here, a guy who is really at the top of his game, listen to Joe, nice conversation for episode 28 of federal tech podcast. He's Have you ever met Joe.

16:05
I've never met Joe. I've heard of spycloud. But there's a lot of great technology coming out of some of the areas of the government that we just don't know about until years later.

16:16
Well, the podcasts I want to do with him is like a podcast or a whiskey bar where there's no one recording anything. He says, Okay, this is really what's going on, I think that it wouldn't be good run for the hills after that

conversation. So are there specific target agencies that would deploy this easier than others? Would a civilian agency be able to deploy this quicker than a three letter agency? Or maybe that the military to see? Or are there sweet spots for your technology in the federal government?

16:46
Well, it's really available to anyone in the federal government, we have our impact level certification from the DOD, we'll have our FedRAMP authorization in the next week or two, don't quote me on that. It's a dependency, obviously on the FedRAMP PMO, completing their process. But we've completed everything we need to the thing we have, that's a bit of a nuance, but may speak to the three letter agencies and others is we also have software that can provide the same thing, if you're looking at a hybrid cloud environment where you need to go on premises versus giving access to the public Internet.

17:25
Mental security's got a strong presence all over the world, actually. And so I imagine you have meetings where you keep up with threats. So in the last six months, what, what kind of new threat technology have you been informed of at Menlo that maybe our listeners don't know about?

17:44
Well, that's really what the highly invasive adaptive threat acronym heat is trying to bring to light is the ongoing new threats that are being developed using legitimate code or a legitimate pathway to your network or to your device. And it's being encoded, and essentially snuck in to some a user unknowingly. And that's what we're trying to draw attention to is that this is an ongoing thing. Hackers are getting smarter, they're getting more creative, they have to, and they're trying to evade what the current technology can identify,

18:25
or say about these dynamically generated logos. And when I was researching this morning, I found that the number one logo that's used in fishing is DHL. And I have a daughter living in rural Africa. So I can send through DHL so we can get there. So wow, it could be me, it could be I could be getting an email from DHL saying your package didn't arrive in, in Ethiopia or something like that. So. So this DHL, so what happens is, Darrin sends a package to his daughter in Wyoming, and he gets a note back from DHL Only it's not DHL. It's a weaponized file that's doing an unprecedent personating DHL, and you go, Well, I want to get this to my bang, you're gone. Ha, yep. I mean, and, and what you're saying is this is not limited to just to, to you and I and, and our friends here in Northern Virginia. They go after schools and hospitals. This is the most nefarious of it all. They're going after hospitals and locking down hospitals with this phishing attack.

19:23
They are and they're, they're using it as a weapon against, you know, the administration who they think has deep pockets to pay to get their data back.

19:35

And I think that's a glimmer of it as to whether or not they pay the ransom, or not. I think a commercial organization may have some options, but really the federal government, if you're going to comply with some of the zero trust initiatives are out there. You have to come up with a solution, like some kind of isolation browser solution that can be deployed easily and have flexibility because I think if we learned anything, since COVID, is that you have to have flexibility for scaling out tivities and if your isolation technology can't scale, well, then you're going to be stuck. I mean, if somehow, who knows what's gonna happen, you know, birds and cats falling from the sky, and it has to work out of house again. And there may have scaling requirements there that would prevent well actually might allow malicious code to come in because there's so much I couldn't handle.

20:23
Yeah. And it becomes a customer experience at that point, John, and I think why where that starts to break down is to your point, things start to get through usually, because the IT shop is forced to allow exceptions to get through. So they're going to bypass the isolation technology, because they have to in order to keep their customers happy. And what we're doing is a different technology that can scale. And because we are not allowing images or the files to actually be downloaded, they're looking at them. And if you think about it about 70 75% of the time, I know I don't download the file, I look at it, I read the PDF, and then I closed the session, I don't need it. So if you need to, we'll do a scan on those types of files. But most of the time, you don't need to so save the bandwidth, save the time, improve the customer experience, while literally eliminating the phishing and ransomware attacks. Oh, good.

21:31
Well, Darren, unfortunately, here, we're running out of time, this has been a great discussion about weaponize files. And about I think the aspect of scaling is has to be in everyone's plans for the next five years, I was going to ask you about the next five years, but you have to be the next five years because you have to plan for expansion, you have to expand for I don't know what's gonna happen next four years. But if you have a basic system that can scale and grow, then you're going to be in a safe position when the next major attack occurs.

21:59
Yeah. And to your to your point earlier. You know, we are all over the world. And part of that, as you think of the onset of edge computing, you want to be closest to the person using the browser. So we've set up shop all over the world, in order to be closest to the users are FedRAMP, of course, will be east west in the US. But, you know, it's it's critical to be close to the user to improve the latency to improve the customer experience. Great.

22:28
You've been listening to the federal tech podcast with John Gilroy. I like to thank my guest, Darren Curtis, the Vice President public sector at Menlo security. Thank you, Darren.

22:36
John. Thank you really appreciate it. That was fun.