http://www.itwire.com/business-it-news/security/73349-a-quick-glance-menlo-security.html
A quick glance – Menlo Security
16/06/16

**It's simple, really.  If you don't want to have a web page dump malware on your device, don't render it there.**

Such is the essential premise of the Menlo Security Isolation Platform (MSIP) where all Web pages visited by any subscribing device will be rendered on Menlo Security's servers and only the resultant page, devoid of any scripts or other executable content, is delivered to the device.

In this scenario, any form of drive-by hijacking of Web pages via corrupted advertising links (or any other form of Web-sourced intrusion) is neutered by the fact that Menlo's servers are the only computing devices that will actually experience the illicit behaviour – and they're well-equipped to deal with it.

Thus, only a fully rendered "clean feed" Web page is delivered to the user.

Menlo claims that there will be "no noticeable latency" although it might well be that in fact page loading is actually improved since Menlo's servers are certainly going to be more efficient at rendering a page than the typical smartphone and the actual content delivered to the user's device has been stripped of a great deal of scripting and other background code.

After obtaining $US45 million in two rounds of fund raising, Menlo Security is ready to conquer the world with a slew of recruitments of ex-Juniper and FireEye people (amongst others).

iTWire had a chance to sit down with Peter Lunk, Menlo Security's vice-president of marketing, at a conference recently. First we were interested in what made MSIP a significant new product.

**Peter Lunk:** The whole purpose behind Menlo is to prevent malware from reaching the users. It's a different approach entirely. So rather than trying to make a determination of good traffic versus bad traffic at the device, it isolates the browser and removes the need for recovery.

When I load a Website onto my machine here I'm going to see the main site. Maybe it's Forbes or CNN or what have you, but I'm going to see a ton of scripts executing – ad networks, content delivery networks from all over the world. On average, you're going to load 35 different scripts. Some people are bigger offenders than others, that one [Lunk pointed to a specific item on a presentation slide] loaded over 200 scripts — that was probably an entertainment site — they tend to be the noisiest.

And they download a bunch of code, and then, to make it worse, we fingerprinted all those servers that were providing all those scripts. Whereas your main site might be trusted – you might be going to *The Straits Times* or some trusted site, the

scripts are coming from all manner of places. This is why we keep seeing malware infections – not that people are spending a bunch of time on sites they shouldn't be on anyway, but even legitimate sites are delivering malware.

**iTWire:** ...and there are regular reports of reputable sites serving "crap" which is not under their control.

**Lunk:** It happens. Someone compromises one of their network sites, someone forgets to renew the registration and someone else uses it to start serving malware...

The traditional way of handling this problem has been, "well, I'm going to have a whole stack of security devices and they're going to make a decision for me." Originally this started with AV and this grew to IDS systems, to sandboxing. And those guys [the 'stack of security devices' vendors] would say well we're 99 point something percent accurate at stopping things, but they won't say they're 100 percent. It's fundamentally too hard to go to 100%.

So, rather than taking that approach, where it's really bad, we say let's take all of it and run it in isolation.

So today, you're going to go to a Website, fetch the content, you're going to execute it and you're going to present the information; render it on your screen. Rather than doing fetch, execute and render all on your device, the Menlo approach is to say 'let's do the fetch and execute steps out on the MSIP that sits in the cloud'. So this is all happening on virtual machines, and they just provide the safe rendering information to your device. That way we don't have to make a decision on whether it's good or bad.

It's almost like IT giving you a new laptop every time you change sites, but of course there are some things that won't work. Obviously your microphone and webcam ought to be connected to a virtual machine somewhere out in the cloud!

**iTWire:** So, how does the system dealt with Web downloads.

**Lunk:** Say I wanted to download a document. MSIP would say that's probably not a good idea, do you really want to download that? What we'll do is scan it and give you a PDF. So, if you want to pull down a PowerPoint of an Excel spreadsheet, we'll give you the same option to get a PDF, which is probably a good idea – you probably don't want to be downloading spreadsheets from random places of the Internet.

But let's say you're adamant, 'I really want to do that' – we have the settings capability where the security settings can say 'yes, you're allowed to do that' but gives you a warning to say 'are you sure you want to do that?' And if you're adamant, it will let you do it. Or you can have a security setting in there that says, 'you are NOT allowed to download Excel spreadsheets from the Internet'.

**iTWire:** What about image files? Does MSIP deliver the actual picture? I'm thinking about steganographically encoded images that might be embedded on a Web page.

**Lunk:** Yes, it is the actual image that's delivered to the user.

***iTWire attended the conference as a guest of NetEvents.***