Continued from previous page

"There are questions to be answered around Yahoo's claim that this was a state-sponsored hacker," he said. "State-sponsored adversaries don't typically publicly share stolen data or sell it."

Grossman went on to confide that the hacker "Peace of Mind", who has been offering exfiltrated Yahoo data for sale on the dark market, is unlikely to have been state-sponsored. "This means it's possible we're looking at two different Yahoo breaches with two different hacking groups in their system," Grossman concluded. Or, just as likely methinks, that the whole state-sponsored accusation is just smoke and mirrors to deflect from the conclusion that one of the biggest hacks in history could have been perpetrated by an ordinary hacker using commonplace attack methodologies.

The fat lady sings, in private

Opera used to be the big alternative browser contender, then Firefox and, ultimately, Chrome pretty much pushed it to the sidelines. Sure, it has a deserved place on the mobile browser landscape, but beyond that most people probably haven't heard of it now. Which is a shame, since it continues to push the boundaries in the right places. Places such as privacy.

As I write this, Opera has just made a new client available that comes with a commercial-grade VPN built in, and it's free of charge for users (you may have read *PC Pro*'s review of the beta back in issue 263). Last year, Opera bought SurfEasy – which operates the VPN service – so maybe this was to be expected. That it's free, and is speedy in operation, is to be applauded.

You get all the usual refinements of a commercial VPN, such as location configuration and decent server speeds across the board. You also get a 256-bit AES encrypted connection and a "no-log service", with neither Opera or SurfEasy storing your usage data. I've not had time to dig into the privacy policies yet, but will let you know if I discover anything different.

davey@happygeek.com

STEVE CASSIDY

"There's no case for believing that an ignored, uncommunicative antivirus is actually working, or appropriate"

A tour of Silicon Valley emphasises how the world of network security is being turned on its head. It's not just what's going in, but what's going out...

How do you determine whether you're dealing with a freak event, or whether this state of affairs is the new normal? Not an easy question to answer, and not one that comes up often in the IT business. We're a bit weird, if truth be known: talking a lot about innovation and leading-edge technologies, but often dealing with issues that play out over long periods of time.

Although based on the people I find myself listening to these days, it isn't "talking". It's more agonising, confessing, or worrying. What used to be a pretty dry business now has emotions, and that's a far better measure of importance than any number of charts in PowerPoint.

My musing about the dilemma of emergency action versus planned activity has been driven by a week spent in Silicon Valley, touring various tech companies that had clubbed together to bring in some journalists to reveal what said companies were up to. You can discard any ideas of red carpets or five-star treatment: I can exclusively reveal that Silicon Valley is both large enough and yet crowded enough that we were averaging three hours a day in a coach, just to get around. This was a nitty-gritty business.

You can read about the strangest encounter in *Fibre Fight Club*, p122: that wasn't so much driven by a current crisis, as it was by a steady story of background success. The most noticeable group was a whole posse of startup businesses, focusing on malware and ransomware mitigation. My observations from the visit with F-Secure in Helsinki earlier this year have now been underlined in half-inch Sharpie and scribbled over with actinically bright highlighter dye: these guys all acknowledge my version of the state of play, with such intensity that some have bet their careers on it.

To recap: security threats come and go, and tend therefore to be handled on a crisis-management basis. New virus? Set the clock running to see which antivirus firm gets there first, and then decide whether you need to change software or you can wait for your incumbent LAN resident utility to receive an update. New site exploit? Consider flipping your www subdomain pointers to target your spare online backup copy (you do have such a thing, right?), until the hole in the hosting platform OS has been patched.

Steve is a consultant who specialises in networks, cloud, HR and upsetting the corporate apple cart
@stardotpro

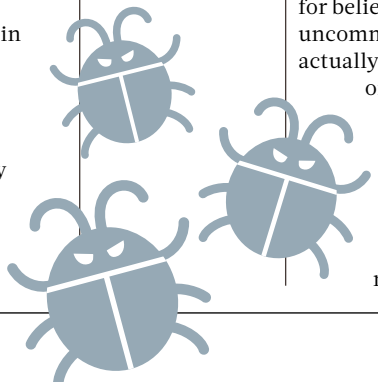
"What used to be a dry business now has emotions, and that's a far better measure of importance than any number of charts in PowerPoint"

The industry has even enshrined this outlook in a whole raft of best practices, because it seems that this is a "normal situation". I've put that in quotes because, to me, it never did seem normal at all. Certainly, the statistics now coming from the more radical thinkers in the enterprise network security business suggest that there are long periods of time (months, not weeks) when work PCs are both infected and showing a little thumbs-up icon from their alleged protection software.

But many businesses think this is fine. Once a practice is entrenched in custom and procedure, it can start to be ignored. Annual invoices for antivirus software updates can be signed, and auditors can be kept happy simply by looking at a piece of paper.

This is an error of category: just because your antivirus is a piece of software, downloaded and updated like your word processor, browser or operating system, the temptation is to manage it within the same relationship. Yet there's no case for believing that an ignored, uncommunicative antivirus is actually working, or appropriate, or non-intrusive.

Often if I'm trying to disinfect a machine I'll tear off the existing antivirus and replace it with that of a competitor. This produces a disturbed, somewhat huffy reaction in the incumbent IT



support team: they chose that product and justified their choice to a board that doesn't feel satisfied without a bit of to-and-fro questioning and resulting sense of ownership. Yet, I wouldn't be there, sitting trying to fix the thing, if their choice of product was up to scratch.

Some of this is because there are products out there that simply do a bad job. I was mortified to find that one of the startups I was interviewing was roundly dismissive of Trend Micro's range of products. I've been in the habit of using its web-based visiting machine scanner to clean up after a breach for quite some time, based on meeting folk at the company, talking to them, and understanding where they think they do well. Yet here was a company ready to put Trend Micro at the bottom of its preferred list, based on quite separate experiences from mine. But I don't want you to stick to the old thinking here. Put out of your mind any idea of how many stars there would be beside each competitor in a table of antivirus products. Look, instead, at the story from Cylance.

Visit **cylance.com** and you may well react with some scepticism to the company's attempt to rabble rouse the indifferent public to its highfalutin claims. It offers a radically different way to import the results of incomprehensibly huge runtimes on tens of thousands of AWS server instances, somehow squeezing them down into a humble and lightweight machine-resident activity and file-signature checker.

My point about Cylance, and many of the other brands on display in my tour, is this: they had to start up a whole new brand, away from the businesses where the nature of the problem was becoming clear. The old businesses weren't able to simply tack on a bit more code to their existing products, or add a gold product line to the existing silver and bronze offerings. They were too mentally invested in the idea that malware and ransomware don't require special treatment. Nothing less than a whole new brand – delivering a whole new class of product – would do to get people to understand just how separate this class of problem really is.

Everybody I spoke to on the tour had one cut or another of the best way to attack such vulnerabilities. Menlo Security (**menlosecurity.com**) has just about the best coded, fastest-loading site, with the most superb background videos – but the videos have nothing at all to do with its anti-malware solution, which starts from a rather Brexit-like stat that 12% of the workforce are just too dumb to resist clicking on links in emails (the main malware infection vector these days).

ABOVE A tour of Silicon Valley startups was quite revealing

LEFT Cylance delivers a whole new class of anti-malware product

"Menlo directs your clicks to its servers, which conduct far more diligent anti-malware checking"

Menlo rewrites all your clicks so they're directed to its own servers, which conduct far more diligent anti-malware checking before letting the click through to whatever lies beyond. This looks a lot like the way that web proxies used to work, in the dim and distant past: another old standard for online safety that suppliers such as WebSense moved into the cloud for major corporates, many years ago.

Is this a new take on an old story? I think not. Everyone I spoke to was emphatic that they weren't seeking to sweep away the old order. The fact that ransomware sidesteps services from existing providers didn't, in their view, invalidate the situations where the old stager does manage to beat off the attacker. This is enshrined in the concept of "security chaining".

A security chain is a series of devices or configurations, in which each part of the analysis of the traffic on your LAN is divided up. You have a traditional outward-facing firewall at one end, and then a spam washer, VPN endpoint, or a link scanner, each one configured to pass traffic on to the next in the chain. On the inside of the network is an internal traffic firewall, which is biased to report on new and unusual types or destinations. Not coming in, but going out.

If one part of the security chain turns out to be a bit below par, then you are, in this config, far more able to take it out and replace it with an

improved or competing version, or even switch between on-site VM, hardware appliance or cloud service at will. It's all reduced to an exercise in Software Defined Networking.

I bumped into a client almost as soon as I was back from this trip, who wanted to know if I agreed with his consultants' proposed DMZ-based firewall configuration. As I explained just how far the company network security business has moved from the relatively harmless, easily laid-out architectures that DMZ is based on, his face took on that slightly guarded, wary look of someone who realises he's just turned up at a drag-race in a pedal-car.

It was the look that convinced me to evaluate this outburst of startups and revolutionary uses of cloud and AI, not as just the usual speed of innovation in Silicon Valley, but rather as a clear sign that "normal" isn't what it used to be, that ransomware may well be the killer app of the Dark Web, and that we're all going to have to treat the internet as a much less-friendly place in future.

From the real Amazon to the virtual

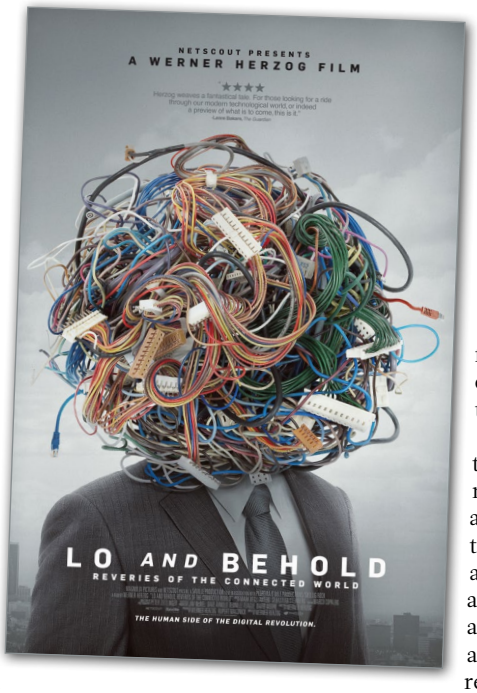
My enduring memory of a film directed by Werner Herzog has always been that of Klaus Kinski, looking deranged in the foreground while a whole region's worth of tribesmen haul a full-size, white and rusty paddle steamer over the dark soil of the Mato Grosso. Therefore, I wasn't expecting to see his name associated with NetScout.

Relationships between the IT sector and the world of visual media have been poor: whether you look at news coverage or fictional movies, sponsorship deal or the supply of special effects' raw horsepower, it's all been pretty uncomfortable, and easily dismissed as lowbrow stuff.

Not so once you deal with Mr Herzog. He was commissioned by NetScout to do some interviews with notable figures associated with the internet and the cloud (I'm guessing my invite was lost in the post). How the initial contact was made, I don't know, but the NetScout team is disarmingly candid about what it got from it: almost immediately after the interview process started, back came Mr Herzog with the statement that the material he was getting wasn't limited to the formulaic, corporate promo category… this was a documentary in the making. To its great credit, NetScout let him do what he wanted to do.

The result of this artistic laissez-faire was presented at the London Film Festival back in September. The title is *Lo and Behold*, and it's a set of interviews of the type you may normally associate with Nick Broomfield or Louis Theroux, but with the intellectual heft and readiness to get surreal that comes with all that Herzog touches. As I write, I haven't seen the full movie, only snippets during NetScout's presentations, but it looks like an 100% bullseye on the strange world of networks, internet businesses, and the people who have decided they have an opinion on the matter.

Who are NetScout, you ask? The firm makes network management and monitoring software, though perhaps the more immediately recognised brand it has just acquired is Fluke, which makes those very beautiful, very expensive, rugged network cable and signal testers. Fluke gear only ever appears in the hands of seasoned, battle-scarred network professionals, who will always be the first to tell you that their business can be extremely odd, whether that's from the spread of characters they meet, or from seeing what those characters get up to on the internet.



ABOVE ***Lo and Behold*** **provides an insight into the strange world of networks and internet businesses**

I'm quite surprised by the vehemence of my own reaction to finding that a tech firm has backed the production of an art-house documentary about connectedness and humanity: it reflects a sense of adulthood, a readiness to examine not just next quarter's results or how many users some service can boast, but the wider issues that the screaming tornado of 21st-century capitalism acts to drown out.

Thinking about it on the long flight home (I never sleep on planes), from what I know of the network packet analysis business, and what it means to unequivocally see every last bit and byte of what people get up to on the internet, maybe that decision isn't so surprising after all.

cassidy@well.com

Fibre Fight Club

Non-disclosure agreements are part and parcel of a writer's life. Often, a new product will be legally secret due to its impact on share prices once it's released, but the writer has to see it in advance so the coverage appears in sync with the launch date. This is accepted. One of my destinations on the Silicon Valley tour had reason, it felt, to take that general proposition and extend it a little.

Not only were we constrained not to reveal any facts about the product until after 21 September, but our agreement not to do so had an automatic and explicit duration of three years, despite the right for either party to withdraw at any time…

The net end effect of such an ambitious and unusual piece of paper was to make everybody's eyes glaze over, and avoid posting anything at all about the business in question. It was impossible to figure out whether some piece of hardware you were looking at was inside or outside the provisions and threats of the NDA, and as soon as a question session came up in among the presentations, hardly anybody was interested by the technology: they wanted to know about the motivation for the secrecy.

The answer was actually very illuminating. This business was under persistent competitive attack by a certain very large far-eastern telecommunications vendor. Keeping its proprietary technologies out of the clutches of this distant but enormous, unscrupulous competitor was clearly vitally important to future revenues: for them, the new normal was to get a legally binding agreement out of everyone who set foot on the premises.

I wish I could say that I thought what I signed really was legally binding – that it would work as the company intended. Unfortunately, I don't think it will help – and that isn't my opinion as a legal-phobic nerd, it's my opinion as a consultant to a top-five UK patent law firm. Switching hats for a third time, it's also my view as a writer, that the company can only do itself harm by such measures. After all, having written about it here I'm now obliged by its terms not to identify the company.