OpenFlow gives malware a caning

SDN comes down to earth – taming a 1400 pupil BYOD beast, enhancing security and increasing student and faculty productivity at a go-ahead school

When Dan Pitt became Executive Director of the newly formed Open Networking Foundation (ONF) he knew he would have to address the pre-conception that software-defined networking (SDN) was just an academic exercise, a revolutionary concept of what networks might have been like if evolution had taken a different path. Indeed at least one major vendor reacted to SDN's potential commoditization threat by playing to that pre-conception.

What the world wanted was a demonstration that SDN, or OpenFlow in particular, could deliver a solution to an existing real world problem – and deliver it at less cost and complexity than non-SDN solutions and in a way that provided measurable benefits. Was that too much to ask?

SDN – an uncertain roadmap to a very clear future

Answering that question, and explaining the problem, is easier if we resort to the old road network analogy. Existing networks distributed intelligence across the network in relatively sophisticated switches and routers – as if one had a city street grid with an individual police officer at every junction directing traffic and using their wits to decide how best to direct it. (OK, add SNMP to the network and you have given the police officer a mobile phone so they could receive some advice from traffic police HQ.) SDN, however adds a separate "control plane" that allows central control of traffic at all those junctions: instead of a police officer you now have at each junction a centrally managed traffic control gantry that allows individual lanes to be controlled and directed while CCTV cameras report traffic conditions back to HQ.

It does not take much imagination to see how such a road network could be intelligently controlled to not only ensure optimal traffic flows but also adapt to special conditions, such as a VIP autocade or bypassing accidents. But what is also obvious from this analogy is that the transition between these two scenarios involves a lot of work, a lot of rethinking, and maybe more investment than anyone thinks they can justify.

The road traffic analogy is so tangible that the benefits can be clearly seen – and everywhere it is being applied. Nowadays we very seldom see police officers directing traffic at road junctions, instead we have traffic lights and a growing investment in CCTV cameras and more sophisticated electronic traffic signs. Yes, it is a massive upgrade, a major on-going investment and a lot of re-thinking, but it has been happening slowly ever since 1920 when the first 4-way traffic light was installed in Detroit.

But when it comes to a less-tangible data network, we can all see the culmination – a fully programmable virtual network and how great that would be – but it is much harder to visualize the steps along the way to achieving that. So one of the first messages put out by the ONF was that you can start installing OpenFlow-enabled switches straight away without any network disruption – they work perfectly well as ordinary switches but will pave the way towards an SDN future when the time comes.

But is there any current benefit to be gained from this? Or is it just a costly act of faith in some future networking heaven?

SDN in action now

In answer to such questions, Dan Pitt has pointed to real-life examples of OpenFlow enabled systems:

- Google's 100% OpenFlow global inter-data center WAN with centralized routing, traffic engineering and bandwidth allocation. It had already realized 95% network utilization with simpler, faster configuration, management and provisioning
- NTT Communications' Enterprise Cloud IaaS service, offering network virtualization within & between data centers plus precise control of compute, network; virtual firewall and load balancer functions.
- AT&T and IBM's secure SDN cloud services, enabling fast and highly secure shared cloud storage and cloud services

These are impressive examples, but way beyond the scope of an average IT department in a medium sized enterprise. Two years on and a lot is happening on the SDN and NFV front, but its practical application is still mostly in the hands of giants who do not want to give away too much detail about their projects.

Dan Pitt is still talking about the future when he says: "Over the next few years, enterprises can look forward to a growing choice of SDN-enabled capabilities – from new hybrid cloud services to orchestration tools that enable full-blown network virtualization. But there's no need to wait for tomorrow's shrink-wrapped solutions: go-ahead enterprises can begin exploiting the benefits of SDN right now".

So when Gregory Bell, Head of Technical Services at Ballarat Grammar, Victoria, Australia, gave a keynote presentation at NetEvents 2013 APAC Cloud Summit, it caused quite a stir. Here was an on-going investment in OpenFlow-enabled switches being put to practical use, delivering a real solution and immediate benefits, without any disruption or significant re-configuration to the network.

Could SDN really deliver ROI along the migration path, and not only when completed? Ballarat Grammar has the answer.

Ballarat Grammar – from OpenFlow investment to SDN deliverables
Ballarat Grammar in Victoria, Australia has an extensive campus hosting a flourishing community of 250 faculty and 1,400 students – with over 200 in boarding houses. While senior students and faculty members are provided with a laptop, staff and students living on campus also have network access via their own devices.

Students and faculty have administrator access on their school devices, letting them install their own software. This, combined with BYOD devices in the dormitories, has led to a network security nightmare. Although every precaution was taken to cleanse the network and protect users while on the campus, their devices would be taken home overnight or during weekends and holidays and could come back infected with any amount of malware. Naturally the school-owned devices had up to date anti-virus software and intrusion prevention had been installed on the firewall, but the school's IT team was still bogged down with hours of manually identifying and eliminating network threats such as botnets, spyware, and malware— issues that were also impacting student and faculty productivity.

With so many, and such a shifting population of unmanaged devices on the network, Ballarat Grammar needed a solution that could accurately and reliably prevent and report threats to the network – no matter who the user or what the device.

SDN might not have been the obvious choice, except that Ballarat Grammar – as an HP reference site with a keen eye on keeping ahead of IT advances – had one big advantage. Having already invested extensively in OpenFlow-ready switches, all that was needed was to download a free software upgrade to make their switches OpenFlow-enabled and so able to support HP's Sentinel Security app, specifically designed to deliver automated network posture assessment and real-time security features.

Would this not require a major revision: re-programming the whole system to define types of devices, levels of service and all the additional parameters and features that can be catered for in a programmable network? It would if Ballarat Grammar was upgrading to full SDN, but that was not necessary.

This is a very important lesson (see fig.1) you can leave the network running as before with the switches in "hybrid mode" just acting on the additional instruction set needed for the Sentinel application.

What happens now is that as soon as any device is switched on, the DNS traffic is directed straight to the central controller to be security vetted against the TippingPoint reputation database – see diagram which also shows how the wireless access points are linked in. As a cloud service, this reputation database is automatically updated every 30 minutes with the very latest

malware and threats, while Sentinel allows the school to decide and adjust its own acceptability thresholds to fine-tune the system and get the right balance between security and utility.

Unacceptable traffic is not only blocked, it is logged with details on the threat and its source – so that owners of infected devices can be notified and remedial action taken if needed.

OpenFlow lifts the burden

With OpenFlow-ready switches already in place, it proved very quick and easy to install this security solution. It was done over a school break and the very day the pupils returned the results were seen, with thousands of threats automatically identified and blocked with no notable delay in the system response.

According to Gregory Bell, Ballarat Grammar's Head of Technical Services: "There was one device in particular that got our attention, because it alone was responsible for hundreds of these threats. It gave us the power to inform the student, offer to purge and re-image their device and so get them back to the classroom".

The SDN solution saves a lot manual labour, he adds: "We now know exactly where the infections are and how many there are – we can detect threats and respond in a proactive manner. That saves us hours of work every week."

But the benefits don't stop there: without the constant threat of malware students can safely bring their own devices and enjoy the full experience offered by today's rich media educational applications. At the same time, it enables limits to be set on the many distractions that the Internet can provide, as Gregory Bell explains: "With the DNS Blacklist feature, we can restrict access to websites like Facebook, and that encourages the staff and students to engage more with one another during class."

Threat visibility is educating the IT department, and it can be passed on to the pupils. Young people grow tired of grown ups forever issuing warnings, but when staff can back their advice by showing up-to-date statistics about actual threats the network is averting, then pupils take note and respond.

An example to the enterprise

Yes, the SDN future looks bright, with Gartner predicting a $2bn SDN market by 2016 and IDC claiming that" "the SDN Market could represent 35% of datacentre switching" by the same year. But it will remain just a future unless more IT departments follow Ballarat Grammar's pioneering example and start implementing similar, relatively accessible hybrid solutions to address real issues and gain tangible benefits.

Encouraging more teams to give it a try, Dan Pitt added: “IT shops that already tweak their networks by writing scripts to vendors’ APIs will find it easy to program OpenFlow-enabled switches. Using open-source controllers and as little as 500 lines of code, implementers have already automated configuration tasks across products from multiple vendors and gained more control and visibility over their network traffic.”

There are two reasons why companies still hesitate to explore SDN functionality. The first is the doubts about the roadmap expressed earlier: they should be encouraged by the ease and speed of the Ballarat Grammar deployment of a hybrid solution that left the existing network intact but created a control layer to address a specific problem with a surprisingly simple solution.

The second reason is that they are not too clear about the benefits. For Ballarat these went beyond expectations: they got the security and performance they were looking for, but so much more too. As Nathan Burgess, Ballarat Grammar’s Director of Information and Communications Technology puts it:

“There’s no doubt that the OpenFlow solution gives us the power to help staff and students be more productive in the classroom. At the end of the day, that is what we’re all about.”

fig.1