Zero-day recovery: the key to mitigating the ransomware threat

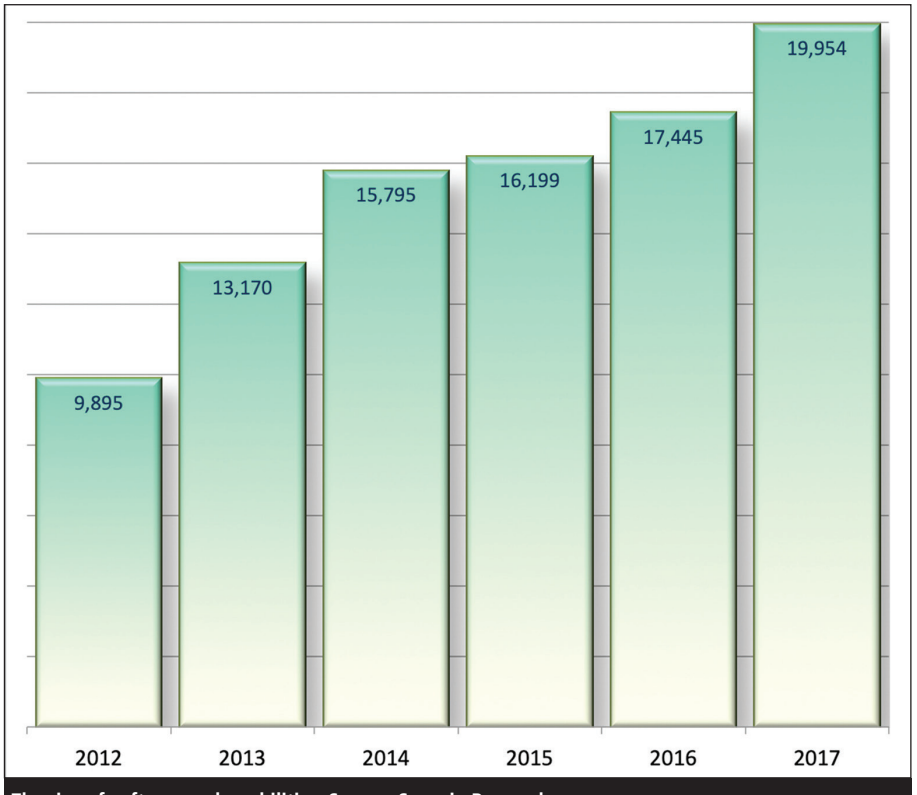

Alex Fagioli

Alex Fagioli, Tectrade

Combine zero-day exploits with ransomware and you have a cyberthreat that few organisations are equipped to handle. If all the focus is placed on cyber defence, what happens when those defences are breached? Financial harm, reputational damage and operational chaos commonly follow. But by bringing IT support and cyber security teams together, organisations can chart another way forward – a zero-day recovery architecture to transform ransomware from a critical business challenge to a mere irritant.

Best practice security dictates that an effective patch management strategy helps mitigate a large percentage of today's cyberthreats. Yet a single research firm discovered more than 20,000 new software flaws last year – an all-time-high and a figure rising with every passing year.[1] Modern organisations are built on software, and as digital transformation takes hold, DevOps and agile development methodologies create new risk as the time-to-market imperative trumps security.

Zero-day vulnerabilities are relatively uncommon, but their impact can be devastating. From the time an exploit is used in the wild to the moment a patch is released, there's a window of vulnerability – or opportunity, depending on your viewpoint – during which most organisations are wide open to attack. Advanced tools including application whitelisting, behavioural analysis and sandboxing are growing in popularity – and offer some protection from unknown threats – but are by no means the norm.



The rise of software vulnerabilities. Source: Secunia Research.

"The number of zero-days will increase from one per week in 2015 to one per day in 2021, with the application attack surface growing by 111 billion new lines of code every year"

The bad news is, zero-day threats are also on the rise. Cybersecurity Ventures believes the number of zero-days will increase from one per week in 2015 to one per day in 2021, with the application attack surface growing by 111 billion new lines of code every year.[2]

Tackling ransomware

Of course, zero-day exploits are used in a variety of attacks with a multitude of end goals. But when combined with ransomware they can be particularly damaging for unprepared organisations. Ransomware was the most popular malware type in data breaches analysed by Verizon in 2017: twice as likely to be seen as any other form.[3] One vendor blocked an astonishing 631 million ransomware-related threats in 2017 alone and saw the number of newly discovered variants increase from 247 in 2016 to 347.[4]

The impact of a successful attack is well understood by now: a major productivity hit for employees and

large-scale service outages. This in turn could result in serious financial loss, reputational damage and regulatory fines. The General Data Protection Regulation (GDPR) and NIS Directive both demand best practice security to mitigate the risk of such attacks and arm regulators with the power to levy multi-million-pound fines if they're not satisfied.

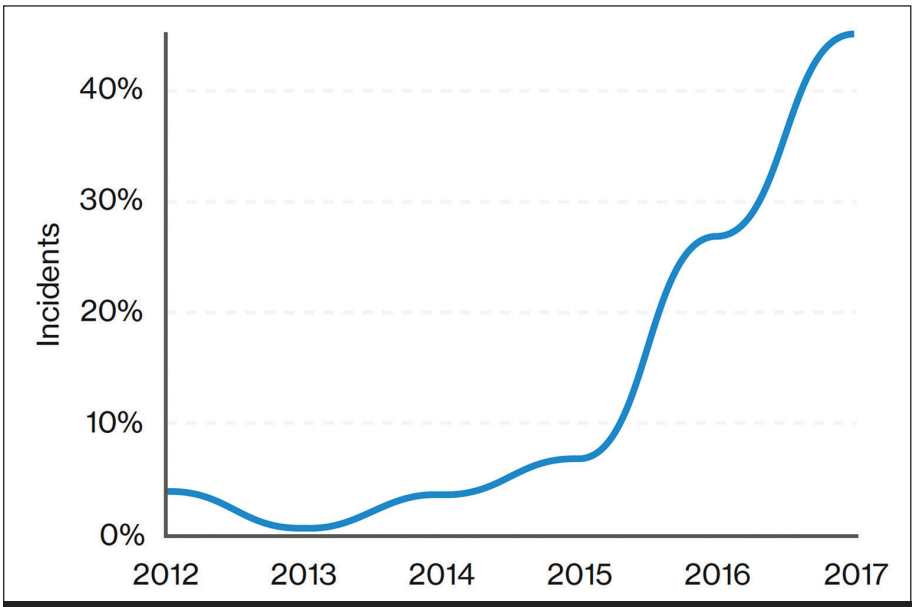
Organisations caught out by ransomware in 2017 suffered huge estimated losses. They included Danish shipper Maersk ($300m) and pharmaceutical giant Merck ($300m-plus).[5,6] The NHS, meanwhile, was forced to cancel an estimated 19,000 operations and appointments as a result of WannaCry.[7]

For many organisations, the binary choice is whether to pay the ransom, even though research suggests only half who do so get their data back.[8] But what if the motivation for the attack wasn't money at all? Nation states are increasingly looking at ransomware as a way to disrupt geopolitical rivals – think NotPetya – or even as a way to hide evidence of the original zero-day exploit.

Think about it: zero-days are expensive and time-consuming things to research and develop. If you've just used one to infiltrate an organisation, you ideally want to increase the ROI by being able to use it again and again. What better way to protect this valuable piece of IP than by encrypting the file system of the victim organisation in order to cover your tracks and distract the IT team?

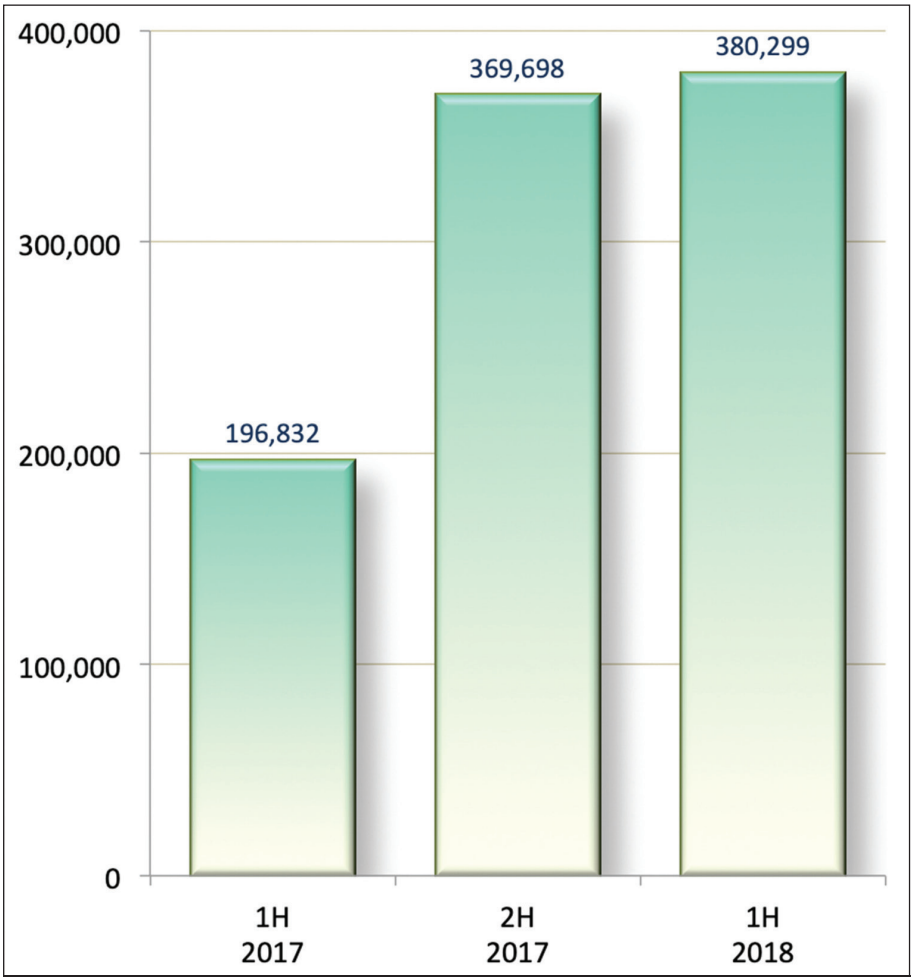
Focus on recovery

A robust underground economy and growing nation state activity will continue to fuel the market for zero-day and ransomware threats. The case for improved resilience is well made – incorporating network segmentation, application control, advanced AV, user education to spot phishing attempts and more. But as discussed, no defences are 100% watertight, especially when faced with sophisticated zero-day malware.

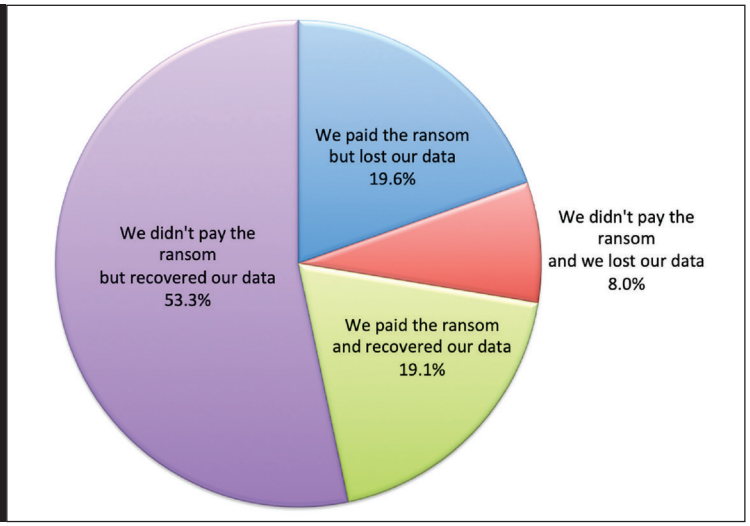


The growing use of ransomware within malware incidents. Source: Verizon.

That should make recovery a vital component of every organisation's cyber security strategy. Yet current approaches are manual, cumbersome and inefficient – or else costly and time-consuming to build. Recovery is just not thought of as a solid last line of defence. That needs to change – and it can, with a zero-day recovery methodology that allows IT to quickly and



Ransomware detections. The volume of attacks has slowed but the malware continues to evolve. Source: Trend Micro



Responses to ransomware and the results. Source: Cyberedge Group.

confidently roll back to an uncompromised version of mission-critical data.

Zero-day recovery

Today it's not a case of if but when your organisation comes under attack. But by putting in some time now you can create a genuinely effective last line of defence to complement those more traditional security tools. This is what a zero-day recovery architecture offers.

"The sheer pace at which businesses operate today, coupled with a crippling industry skills shortage, means these teams are typically under huge pressure to drive digital transformation. But that inevitably creates security gaps"

It starts with traditionally siloed IT support and security teams coming together to work out a set of policies that will define the architecture relevant to the organisation. The sheer pace at which businesses operate today, coupled with a crippling industry skills shortage, means these teams are typically under huge pressure to drive digital transformation. But that inevitably creates security gaps. Organisations need to start viewing security as more intrinsic to the way they operate, with teams collaborating to discuss up front what steps they'll need to take when something goes wrong.

The policies they develop might dictate that when an attack hits, a particular workload needs to be brought back into the server within 20 minutes. Perhaps for a different workload there's less urgency and a timeframe of days rather than hours for recovery. The IT staff also work out at this stage what they do with each workload: do they completely wipe it and rebuild? Do they try to disinfect it? Or do they try to replace it with a private copy?

To develop effective policy here, IT teams need to have a good understanding of the criticality of their workloads and data, and the dependencies that exist within the enterprise architecture. To use an analogy, a pilot and co-pilot will have a checklist to complete if they have to restart an engine: beginning with turning off the fuel pumps, filling up the auxiliary, all the way through to firing up the engine. This is down to the complex set of inter-dependencies linking each system – each step has to be completed in order.

A lot of organisations have not gone through this same process for their IT infrastructure – but it's a vital discipline. They may need to lift out every single one of the workloads they have running in their virtual environment and assign a business priority to each – performance, survivability etc. They'll then end up with a zero-day recovery catalogue containing bronze, silver and gold-type tiering, which will define whether the workload is duplicated, flagged for fast-paced 10-15 minute recovery, and so on.

Planning and categorising in this way enables IT to go back to the workload owner and tell them exactly how much it costs to run their workload and how much it will cost for high survivability per month, for example. It could even help to save money on storage, ultimately meaning the process pays for itself.

Build and test

Next, it's time to build the back-up and recovery architecture. Organisations have historically undervalued their back-up environments. It's not uncommon to see almost a quarter of nightly back-up jobs fail if not properly managed: but often IT has no idea what data it has lost, or what is unavailable. It can mean the difference between going back 12 hours or 48 hours, depending on when the back-up failed. That's not acceptable for a large bank or e-commerce provider.

Organisations therefore need a technology platform to automate failover, or back-up and recovery activity, including snapshot technology to create instant recovery points for immediate redeployment. Also consider an air-gapped data recovery vault and a 'clean room' for those most important gold images.

"Recovery can be a key differentiator for organisations. Zero-day recovery provides the methodology to plug in a solid last line of defence to complement traditional security"

It's not just a case of building the right architecture: organisations must also check that it works. It's surprising how many firms still fail to do disaster recovery testing. If there are faults, they need to be found at this stage rather than after a major cyber attack. Conduct regular restore testing – automated, ideally – and be sure to test the integrity of recovery data.

Ongoing monitoring is also required to ensure that recovery point objectives (RPOs) are met and to detect any unexpected behaviour in the environment.

Restore with confidence

With this set-up in place, you'll be able to restore applications quickly and easily from the recovery vault in line with policy – within minutes if necessary. That's peace of mind for any data-centric organisation worried about the threat posed by ransomware: from healthcare and finance to the retail and manufacturing sectors. Those thought by attackers to have the most to lose will be first in line, although the bottom line is that everyone's a potential target today.

Security breaches are inevitable, whether they stem from a zero-day exploit or even an unpatched vulnerability. That means recovery can be a key differentiator for organisations. Zero-day recovery provides the methodology to plug in a solid last line of defence to complement traditional security.

About the author

Alex Fagioli joined Tectrade in 1999 as a specialist technical consultant, drawing on his background as an engineer to assist clients with data protection, back-ups and recovery. Over the next 18 years, he worked his way up through roles in sales and technical departments – including head of pre-sales and CTO – before taking the helm as CEO in 2012.

References

1. 'Vulnerability Review 2018: Global Trends'. Flexera Software. Accessed Dec 2018. https://resources.flexera.com/web/pdf/Research-SVM-Vulnerability-Review-2018.pdf.
2. 'Zero Day Report 2017'. Cybersecurity Ventures, 3 Jan 2017. Accessed Dec 2018. https://cyber securityventures.com/zero-day-vulnerabilities-attacks-exploits-report-2017/.
3. 'Data Breach Investigations Report 2018'. Verizon. Accessed Dec 2018. www.verizonenterprise.com/verizon-insights-lab/dbir/.
4. 'Unseen Threats, Imminent Losses'. Trend Micro, 28 Aug 2018. Accessed Dec 2018. www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/.
5. 'Interim Report Q2 2017'. Maersk, 16 Aug 2017. Accessed Dec 2018. http://investor.maersk.com/news-releases/news-release-details/interim-report-q2-2017.
6. 'Merck & Co (MRK) Q3 2017 Results – Earnings Call Transcript'. Seeking Alpha, 27 Oct 2017. Accessed Dec 2018. https://seekingalpha.com/article/4117318-merck-and-co-mrk-q3-2017-results-earnings-call-transcript?page=1.
7. 'Investigation: WannaCry cyber attack and the NHS'. National Audit Office, 27 Oct 2017. Accessed Dec 2018. www.nao.org.uk/report/investigation-wannacry-cyber attack-and-the-nhs/.
8. '2018 Cyberthreat Defense Report'. Cyberedge Group. Accessed Dec 2018. https://cyber-edge.com/wp-content/uploads/2018/03/CyberEdge-2018-CDR.pdf.

GDPR – project or permanent reality?

Rob Perry, ASG Technologies

Rob Perry

With the General Data Protection Regulation (GDPR) deadline now months in the past, you'd be forgiven for thinking that your work on compliance – at least with this regulation – is done. However, even though the May 2018 date for the beginning of enforcement of this regulation is behind us, being GDPR compliant is not a one-time event, but a long-term ongoing commitment. Making the mistake that you don't have to think about it anymore could be costly.

For the vast majority of businesses, meeting the 25 May 2018 deadline required a significant amount of time, money and resources. And with so much information to digest in order to get to this stage, the idea that there is still work to do may seem daunting. In the run-up to the deadline, it was suggested that as many as 60% of businesses would miss it.[1]

Some of the biggest obstacles companies encountered to becoming GDPR compliant included a lack of knowledge and understanding of the regulation; shortage of time, skilled resources and budget; and an insufficient understanding of the data inventory within the organisation. At 99 articles, the GDPR is lengthy and confusing. It is important to recognise any shortfalls in your initial approach and understanding of the GDPR in order to prevent these from undermining your compliance efforts further down the line.

Given the level of resources involved with the initial push for compliance, trying to maintain the same pace with