When the state of security makes you WannaCry

SCOTT CRAWFORD, PATRICK DALY

15 MAY 2017

Hundreds of thousands of systems in countries across the globe were compromised last week by WannaCry, a ransomware attack moving with unprecedented speed and scale, crippling critical systems including the UK's National Health Service, FedEx, Nissan and Telefonica. Will this incident bring about unprecedented change in the way security is understood and managed?

451 Research®

On May 12, 2017, a ransomware attack known as WannaCry (also known as WannaCrypt, WanaCrypt0r, wcrypt and a handful of other names) spread rapidly around the world within a day, infecting more than 200,000 computers in 99 countries – numbers that continue to vary as the incident unfolds. The attack capitalized on a number of factors that combined to make this not only the largest incident of its kind to date, but also one of the most alarming.

THE 451 TAKE

There are many troubling aspects about WannaCry, beyond the handling and disclosure of nation-state cyber weapons and tactics. The attack itself suggests that the perpetrators had a clear idea of just how quickly and widely it would spread: the ransoms demanded were trivial ($300-600 in many cases), while the demand itself was written in 28 languages, suggesting the attackers' expectation of a return based on volume. The attackers further seemed to recognize that the worm functionality WannaCry entailed would be highly effective, capitalizing as it did on the Shadow Brokers dump in April of cyber-attack tools and tactics believed attributable to the NSA. The perpetrators appear to have estimated their targets well. Healthcare organizations were among those most dramatically affected. WannaCry targeted older versions of Microsoft Windows, which particularly bedeviled entities such as the National Health Service in the UK, where the continued use of software no longer vendor-supported, such as Windows XP, was widely publicized in late 2016. XP is a 16-year-old operating system no longer maintained by Microsoft except under custom support (but for which Microsoft quickly issued an emergency fix in the wake of this incident) – and healthcare organizations are a frequent ransomware target since systems may be critical to life and safety. The callousness to issues of health and death on a global scale these observations suggest is chilling.

Just as troubling is the widespread lack of awareness of the realities of security management the attack revealed. For many organizations and in some industries, keeping systems updated to resist such threats is not a trivial task, for a host of reasons. At the same time, however, the extent of WannaCry's impact revealed just how many of those responsible for securing critical systems still do not seem to recognize how serious and immediate such a threat can be. In the UK healthcare system, for example, providers have had as much as seven years to retire, upgrade or at least better defend out-of-date Windows systems, but these systems remain in place and exposed regardless. Is there really nothing that could have been done to better protect these vital resources? Will this incident result in a new sensitivity to just how critical information security has become to virtually every aspect of life? Will this mark a watershed of shift to making security a priority on a par with IT's 'business objectives'? We explore these questions that demand an answer – and soon, since time is not on our side, with billions of 'smart' things becoming increasingly integral to everyday life.

THE ATTACK

The ransomware attack that began on May 12 was a perfect storm of forces that converged to produce one of the most significant security incidents to date. It capitalized on tactics attributed to a group known as 'Equation Group,' believed to be linked to the NSA, that were made public in April by a group known as Shadow Brokers. The tools disclosed in the Shadow Brokers incident included an exploit known as EternalBlue, which targets Windows vulnerabilities in the Server Message Block v1.0 (SMBv1) system not publicly known until March, a month before the ShadowBrokers disclosure, when Microsoft issued Security Bulletin MS17-010. (Curiously, researchers noted the absence of any acknowledgement by Microsoft of anyone who may have worked with the company on the MS17-010 issues, even though MS17-010 was directly relevant to a number of tools disclosed by the Shadow Brokers a month later). Microsoft itself has decried the ways that governments accumulate and manage stockpiles of cyber weapons, calling for a 'Digital Geneva Convention' on the matter in February.

WannaCry also probed potential victim hosts for another tool in the kit leaked by Shadow Brokers, a 'backdoor' called DoublePulsar, which, if found installed, could also be used to load a malicious payload. According to some researchers, DoublePulsar had been found on tens of thousands of systems around the world within days of the Shadow Brokers disclosure – outcomes that beg the question of how far government agencies should go to arm the public with information when their wares escape their control.

The attack marked the return – with a vengeance – of the worm, a type of attack not widely seen since the late 1990s to early 2000s. (Remember CodeRed?) Most ransomware attacks to date have relied primarily on tactics such as phishing to spread. While some victims reported that phishing may have been an initial vector for WannaCry, it was its worm functionality seeking out hosts susceptible to EternalBlue that was stunningly effective, circling much of the world within a few hours. Had it not been for the early discovery by a researcher known publicly only as MalwareTech of a 'kill switch' in the attack that caused the attack to cease functioning when it contacted a specific domain – a domain that MalwareTech quickly registered in the course of his investigation – which quashed WannaCry before the role of this domain in the attack was understood – the impact of WannaCry could have been even more dire.

WannaCry has affected (so far) 99 countries and a variety of industries. Schools and universities in China, energy and telecommunications firms in Spain, FedEx in the US, railway ticket machines in Germany, car factories in Europe, and several Russian targets all fell victim. Among those most vividly publicized was the UK National Health Service, where 48 trusts were affected. At least 16 NHS hospitals suffered compromised access to essential information that forced the diversion of patients, deferral of less-critical procedures and other consequences. Many of these organizations recovered many of their capabilities within the ensuing weekend, but the impact will be felt for some time as officials and the public wrestle with questions of accountability and demands to improve resilience.

THE STORY WITHIN THE STORY

In light of these factors, the continued ease with which attackers can still pull off a ransomware attack in many organizations ironically seems the most mundane. Yes, bitcoin helps make ransomware not only profitable but routinely feasible by coupling a readily exchanged cryptocurrency with a system that effectively helps preserve attacker anonymity. But the larger question remains: Why do organizations continue to be so vulnerable, not only to recurring ransomware attacks, but to the resurgence of attacks such as worms that many thought had become a thing of the past?

This is a persistently troubling question, one that seemingly remains astonishingly difficult to answer. Ransomware continues to succeed in part because organizations remain susceptible to many common vectors of attack, from propagation through phishing, that lead to users executing an exploit, to the lack of preventive controls, as well as limited awareness and ability to respond when a compromise is in progress. Many have pointed fingers at the failure of organizations to keep their software maintained against such threats. After all, the MS17-010 patches that would have mitigated the WannaCry vulnerabilities had been released a full month ahead of the Shadow Brokers disclosure of the tools used.

The continued dependency of many victim organizations on software no longer vendor-supported was also widely decried – software for which no patch would have been available had not, in this case, Microsoft made public an exceptional fix for Windows versions out of support. How can agencies critical to life, health and safety be so glaringly dependent on such vulnerable systems? Isn't that just a disaster waiting to happen?

Too many seem to assume that these questions have easy answers. Security professionals with at least some experience with management know otherwise. The funding and support necessary to ensure the necessary processes, tools and expertise are ready and in place often take a back seat to 'business priorities,' whatever those may be. Even among technologists, security is often an afterthought. Critical though security may be, when ensuring security threatens to slow the pace of innovation, development or the business that depends on those capabilities, security may be left by the side of the road. Those who cry 'foul!' in such cases are at risk of being characterized as roadblocks to progress. Soft skills, thus, become just as important to security managers as technical expertise – more so, in fact, if they ever hope to see their objectives implemented. Technologists in other fields can win as innovators; security pros must often be good salespeople first and foremost to succeed in their objectives.

This is not to excuse what may be outright negligence. Microsoft stopped retail sales of Windows XP in 2008 but did not end support until 2014. So why continue to run XP systems? Or for that matter, any known vulnerable yet valuable resource where exposures can be reached sooner or later from publicly accessible networks? Perhaps in some cases, certain types of critical assets – and yes, that includes those that may be vital to life or safety – may be dependent on older hardware or software that cannot be changed or maintained without having an impact on those critical factors. But does that justify not making the investment in supportable technology, particularly when the lead time to change may be years?

Often, decisions are made because there does not seem to be enough evidence of impact to warrant the investment or potential complications. This is an unfortunate fact of life when it comes to risk management generally; substantive changes often come in the wake of a serious incident – not before, when they could have kept such incidents from happening altogether. Such outcomes may emerge from the wake of WannaCry and its variants that seem sure to follow.

Yet even among security pros, there remains a mindset that could itself stand an overhaul. For years, we have assumed that hygiene – patching and maintenance of software and systems – is key to good security. But by definition, there is no patch for the 'zero day' attack, which exploits vulnerabilities not previously known. Systems don't always need the wide range of services they run, which are often unnecessary to their function. Nor do these systems necessarily need the wide network accessibility they often have. (Not only has WannaCry been successful in finding hosts running vulnerable SMBv1, but it finds them on the internet as well.) In addition, people often have more latitude for making damaging changes in IT than they should. Why do systems remain so persistently susceptible?

A NEW MINDSET

The good news is that we do see innovation in security technology that assumes that resources will be (and should be) accessible from any device, application or system, by any consumer (human or otherwise), over any kind of network – and that means in the face of a world full of threats. We also have technologies that can protect against attacks for which no patch is available. When systems cannot be reliably maintained or replaced, we have tools that can harden them and make them more resilient to any type of exploit. We have a new generation of tactics that recognize not only malicious behavior before it has an impact, but also legitimate behavior that can more reliably recognize and authenticate users far more safely than the password, a tactic that seems more ripe for relegation to the dustbin of history than ever before. We see these capabilities on the verge of being extended much more widely.

These techniques are all designed to secure technology once it is placed into operation. We also have a growing range of techniques to secure it in development, from concept to source libraries to release and deployment. And with the advances of cloud technologies predicated on disciplined and highly responsive management that can sharply limit the scope of exposure (microservices, anyone?), we may have even better control than before – and at cloud scale.

These are among the security technologies we find interesting at 451 Research. But it's not just about the tools. We believe that, as an industry, we should assume that the adversary is always present, in any environment – which is, in fact, often the case, despite efforts to segment and secure networks. We should dedicate ourselves to making common threats uncommon, and capitalize on ways to do this that are as transparent to legitimate use as possible. Tools are emerging that can help make this possible, but without changes in mindset – not just from the businesspeople and technologists that make IT, but security pros as well – we will not see them realize their full promise.

It, therefore, remains one of the sadder facts of risk-related fields that it takes a serious incident such as WannaCry to precipitate change. Will we ultimately win? It cannot be denied that security tends more to resemble an arms race, where every advance by the defender is met by new tactics from the adversary. Increasing the adversaries' cost and decreasing their effectiveness may simply move them to new targets – IT handles too much of value for them to ignore the opportunity. The explosion of the Internet of Things may accelerate faster than our ability to secure it. But that's not to say we can't do a better job than we've been doing up to now.