cyber

Ransomware and Vulnerable Software

Cyber Briefing – May 2017

Prepared by Rob Gordon

ABOUT YOU and CYBER:

Hello. We are Cyber: Creative technology engineers for desktop, web and mobile. We understand you and continuously have your objectives in mind.

We're a design-led digital services agency: That's not a phrase we like to use too often but it's perhaps the best description you might use for us.

You benefit from a combination of our years of knowledge and experience listening to clients in various industries and sectors, with software development, system design, marketing, web development, eCommerce and with web and mobile apps to create amazing ideas and experiences which help you improve efficiency, communicate better, achieve more and make more…

You can rely on our process always starting with a 'Why', because if we know 'why', we can show you 'how' and then deliver the 'what'.

You could call this the "Cyber way". It's the only way we succeed. It'll change your world, but won't cost the earth.

Your fellow Cyber customers range from SMEs to large corporates: Local businesses to some of the world's largest brands and we are equally proud of the care we take and the work we do for each of you.

By listening carefully and constantly improving, we have a built up a track record of developing, delivering, managing and supporting all types and sizes of digital and web strategies. All of that makes us fun and reliable to work with as we help you achieve your digital goals.

RANSOMWARE AND OUTDATED SOFTWARE

The recent outbreak of the Ransomware affecting businesses across the world is an important warning for those running out of date or un-patched software.

We had a busy weekend checking every machine we support and every system we've ever built. Not to be complacent, we're delighted to have been ahead of the game this time with zero breaches.

Ransomware is showing worrying trends: Malwarebytes show an increase from 17% in 2015 to 259% in 2016. WannaCry spreads by infected machines joining a network, rather than the traditional ransomware attack vectors, which previously required each machine to be infected separately through malicious attachments. It is approaching 200,000 global infections with the worst areas affected being Russia and Europe. The USA is starting to also heat up.

It uses a known Windows exploit called EternalBlue, created by the NSA, and released to the public in April 2017 by a hacking group known as the ShadowBrokers. Microsoft did fix the problem in April but it seems that many system administrators have not updated their systems with the latest Windows patches. It's frightening that organisations like the NHS are still running 15-year-old operating systems such as Windows XP. These haven't been supported for three years: Microsoft had to take the unprecedented step of releasing patch fixes for Windows XP on this occasion, but it'll likely be a one-off.

The powerful feature of this malware is its ability to perform network scans over TCP port 445 (SMB) and compromise other machines. The result is encryption of files and the demand of a ransom payment in the form of Bitcoin. It also installs a persistent backdoor to access and execute code on previously compromised systems allowing for the installation and activation of additional software, such as malware.

The spread of the attack was brought to a sudden halt when one UK-based cybersecurity researcher found, and inadvertently activated, a “kill switch” in the malicious software: It turns out that the virus was coded to check to see if an obscure website address was registered and live and to halt if this was the case. This could easily be overcome in a modified release, which is what has already happened. Yes, this has indeed slowed the initial attack but this is only the first wave of such wormable ransomware attacks.

The warnings that cyber security experts have been sounding for years has finally come to the attention of the public. To remain secure, more money needs to be spent on cybersecurity and organisations need to ensure they use only modern patched operating systems. They also need to educate their staff in safe computing and, of course, to simply back up. Either regular off premises, or non-network attached, backups would have limited the damage of this modern nightmare.

Similar risks apply to software and services running older unpatched versions of PHP, MySQL, .NET, Perl. All manners of services and applications that businesses rely upon are all at risk if they are not maintained and secure.

At Cyber, we remain concerned. We too have some longstanding clients who have yet commit to up-grading from some of oldest versions of Microsoft .NET, SQL and PHP. We are working with many of them to address these issues now.

Cyber always recommends monthly checks of frequent security updates and complete annual reviews of software in use within a business to ensure it is up to date and any major version changes are assessed and implemented accordingly. With the risk at it's highest, these frequencies should be dramatically shortened

Get in touch if you would like to know more about what software you are running in your business, discover if you are at risk and find out how we can help. For further information, please contact us on 01284 330188 or hello@cyb.co.uk