MAY 2017

blackfoot

BLACKFOOT NEWSFLASH

What can we do about WannaCry?

There has been extensive news coverage over the weekend about the WannaCry malware infection which has impacted computer systems at the NHS, FedEx (USA), Telefonica (Spain), in addition to literally hundreds of thousands of computers in over 150 countries worldwide.

The most likely initial infection vector is either email-borne malware, or users being tricked into clicking on a poison link. At the point of infection, two main programme elements are installed. First, WannaCry itself which sets about encrypting files locally and on any available file shares. And a second which attempts to spread by exploiting the MS17-010 (SMB CVE-2017-0145) vulnerability on any computer systems it can find. The spread is via the SMB v1 protocol, and therefore uses TCP ports 139 and 445.

The main types of systems which are vulnerable to WannyCry are un-patched ones running Windows 7, Windows Server 2008 or earlier. Microsoft released a critical security patch on 14th March for supported operating systems. And, on 13th May Microsoft took the unusual step of releasing a patch for the unsupported Windows XP, Windows Server 2003 and Windows 8 systems in order to protect them against vulnerability MS17-010.

Back in Blackfoot's Winter 2016/17 newsletter, we published ten recommendations on how to counter the threat posed by ransomware. A revised list is published below incorporating some WannaCry specific recommendations:

Supported operating systems and patching:

Only run supported operating systems, those which continue to receive critical patches from their vendor.

If you cannot comply with our first recommendation due to relying on legacy application or embedded systems, take extra security measures to protect them. Ensure that those systems have a hardened configuration, strictly control access to them, implement network segmentation with restricted traffic between them and the rest of the network, and actively monitor and manage the risk represented by these out-of-date systems.

Ensure you have a strong patching policy and update regime, and that devices reflect this. Where security patches cannot be applied for genuine business reasons, take appropriate steps to mitigate the risk of not applying the patch.

Backup, restore, and disaster recovery planning:

Ensure that your data and systems are recoverable in their entirety, so that if you suffer a ransomware infection, you never have to pay the ransom.

This recoverability recommendation implies multiple backups in different locations and on different media, with some of them off-line so that they cannot be compromised by an infected system.

This recoverability recommendation also implies the ability to restore from many moments in time going back days, weeks, months and even years (depending on the frequency of data changes), in order to ensure that if an infection were to go un-noticed for some time, you would still be able to recover data from before the infection.

Data Replication and ShadowCopy offer useful functionality, but do not meet the recoverability recommendations above.

Develop and test your Incident Response and Disaster Recovery Plan in such a way as to ensure that it specifically addresses with the risks posed by ransomware.

Secure builds:

Build all servers, desktops and laptops from a hardened image.

Periodically review builds to satisfy yourself they are secure in the light of changing security threats.

Run anti-virus/anti-malware software, keep it updated and scan systems regularly (even though AV software has a poor record in protecting against ransomware).

Where feasible, disable SMB v1.

Seek out vendor-specific guidance for combatting WannaCry from your OS, AV, firewall, mail server, mail gateway, web gateway, and IDS/IPS vendors, and so on, and implement them.

Securing the perimeter:

Block unnecessary ports at the perimeter, in the case of WannaCry, block ports 139 and 445 which generally do not need to be accessible from outside a network.

Restrict web browsing to whitelisted categories to reduce the chance of staff visiting sites that could contain malware payloads.

Screen e-mail attachments automatically and quarantine dangerous attachments (i.e. not just anti-virus fails but also executables, macro-enabled Office files, and so on).

Consider blocking egress to all UDP destinations at the firewall and restricting access to all IP destinations outside of ports (80, 43) unless there is a business requirement. This can prevent malware infection, but more importantly malware activation and communication with command and control servers on the internet.

Block TOR traffic and traffic to known TOR nodes.

Perform internal and external infrastructure penetration tests annually, and upon network changes.

Conduct firewall and switch ruleset reviews at least annually.

Safe users:

Restrict access to data on a business need to know basis.

Provide all users with regular security awareness training on safe email and web use, including the risks posed by phishing.

Consider periodic phishing vulnerability assessments to test users and reinforce awareness.

Only use privileged accounts for internal administrative activity, not for web browsing, social media applications or any activities that do not require privilege.

Ordinary users should not have local administrative accounts or be able to install software.

Do not permit family members or other non-employees to use the company's laptops.

In the case of BYOD, do not allow employee computers to access company servers, other than indirectly via session virtualisation or application virtualisation.

Next steps

Contact your Blackfoot account manager to discuss early detection and assessment services, call 0845 805 2409 or email info@blackfootuk.com

Further reading

US Cert guidance, including Indicators of Compromise (IOCs) here: https://www us-cert.gov/ncas/alerts/TA17-132A

Microsoft blog: https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

Talos Intelligence: http://blog.talosintelligence.com/2017/05/wannacry.html

MS Security Bulletin MS17-010: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

Blackfoot's Winter 2016/17 newsletter (see pages 4 & 5): http://www.blackfootuk.com/common/pdfs/Blackfoot_New_Issue_12_Winter_2016-17.pdf

John Elliott's thought provoking blog on the subject: https://medium.com/@withoutfire/vulnerabilities-and-ransomware-the-policy-debate-5122507be2a

blackfoot

Blackfoot UK Limited
Tel: 0845 805 2409
E-mail: info@blackfootuk.com
Web: www.blackfootuk.com

ADVISE >
ASSESS >
ASSURE >