RM™ Education

Support Newsletter

Issue 18

Included in this issue...

Network security
Security best practice checklist
Summer activities checklist
Supported technologies newly added to your support contract
Webinars – RM Cloud Backup, GDPR and Microsoft Teams
Trend Micro updates
Support hot topics

Srijith Ravindran Nair
Project Lead, RM India

supportnewsletter@rm.com

Support Newsletter

Issue 18 / July 2017

Welcome to issue eighteen of the support newsletter. This is the last edition before the summer holidays so as well as including the normal security news, updates and development news, there is also advice on work to carry out during the break. We'll be in touch again in autumn and please do feed back suggestions for content you'd like to see us cover – email us at supportnewsletter@rm.com. Please note you may be the only person within your establishment to receive this newsletter so please pass on to your colleagues.

Network Security

We know how important securing your network is so we have highlighted a number of security issues that we believe are relevant to you and your networks.

RM advice following the WannaCry and Petya Ransomware outbreaks

As has been reported on many news organisations, Petya, a dangerous ransomware variant has been released that impacts Windows client and server operating systems by targeting the same vulnerability (EternalBlue) as WannaCry. It spreads by infecting machines open to this vulnerability. The good news is that most major anti-virus providers, including our partners Trend Micro and Symantec, block this malware. However, the following guidance will help mitigate the potential impact.

Ensure you:

- Have up to date virus definitions for your clients and servers.
- Install the latest patches using your update method for your Microsoft client and servers.
- Have regular cyber security awareness for your colleagues to mitigate against threats that target people.

Read our guidance following the WannaCry and Petya outbreak here.
RM advice on SMB (v1): support.rm.com/TechnicalArticle.asp?cref=TEC5705399
We also recommend that you review the 'Security Best Practice' checklist included in this newsletter.

CC4, Windows 10 and WSUS updates

We are now releasing W10 (v1511 and v1607) and Server 2016 cumulative security updates via WSUS. The June Windows 10 Microsoft Cumulative Security updates - KB4022715 for v1607 and KB4022714 for v1511 have been approved via RM WSUS (as will subsequent monthly security updates) - so these should supersede the packages that we released in NWS5696059 above (this article has also been updated with this information).

If you have W10 v1511 computers on your network then we strongly recommend that you consider rebuilding these to W10 v1607 (please also see advice about CC4UPD203 below), as there is no granular control within the WSUS client on these computers (v1607 computers do have the concept of 'active hours' to stop these updates disrupting lessons).

In the CC4 W10 v1607 Client Pack we set the defaults for the Active Hours of 5am to 6pm. This means that computers will not reboot following a Windows Update during these hours. So, v1511 and v1607 computers will both install any new Windows Updates in the background – but the difference is that v1511 will reboot if no-one is logged on, whereas v1607 computers will wait until a time outside of the Active Hours.

This message is also covered within the CC4 Windows 10 strategy article (NWS5448877).
W10 v1607 is available in your My Account area if you are eligible.

Backup and Disaster Recovery in Schools white paper

With the rise in malware, viruses and ransomware attacks the need to ensure that your data is safely backed up becomes even more paramount. Should your school be attacked by ransomware, it will affect all your onsite systems and you will need to rebuild your network from scratch using uninfected data from a backup. As such a true test of backup success is the restore.

Our white paper proposes backup strategies that could be employed by schools, the hardware and software that can be used and the agreements within schools around data protection.

Raspberry Pi vulnerability

There have been reports in the media of a new exploit/malware/Trojan that targets Raspberry PI devices and turns them into a cryptocurrency miner. The malware itself uses the fact that default credentials are left on these devices – and so the device is 'owned', has the password changed and then the mining software installed. It's not a particularly advanced piece of malware on the surface – simply using default credentials and some Linux commands to install software – researchers looking at the malware are complimenting its encryption, its methods of hiding from honeypots and other security measures.

It attempts to mine the newer cryptocurrencies, since the Pi doesn't have enough power to mine something rarer like bitcoin, fairly innocuous – the Pi is out of commission but it could have been a lot worse. Ideally this type of device should be on a separate VLAN that cannot access the rest of the network.

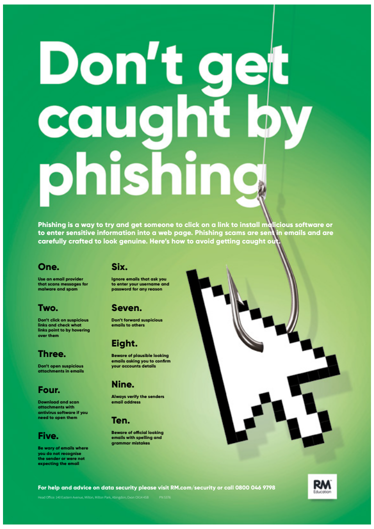
http://opensourceforu.com/2017/06/linux-muldrop-14-trojan-hits-raspberry-pi/
https://www.theregister.co.uk/2017/06/13/linuxmuldrop14_malware_for_raspberry_pi/

Security best practice checklist

Below is some guidance for ensuring your network and users are secure:

- □ Ensure that your servers and computers are properly patched.
- □ Ensure that your AV solution is working and up to date (RM recommends Trend Micro).
- □ Ensure that you have verified, working backups (including the system-state) – see this white paper for more info.
- □ Limit the number of privileged users (if CC4) or users with local-admin rights on their computers.
- □ Avoid using Internet browsers when logged on as a domain-admin account (particularly at servers) – you should use a restricted account on a computer.
- □ Be wary (and educate your staff and pupils) about opening links or attachments in emails (the spring 2017 'Network Infections' RM Seminar PDF is available here).
- □ Limit the use of USB sticks and external hard drives.
- □ Consider an RM External Vulnerability scan.

Data security posters for use in your school



Don't get caught by phishing

Phishing is a way to try and get someone to click on a link to install malicious software or to enter sensitive information into a web page. Phishing scams are sent in emails and are carefully crafted to look genuine. Here's how to avoid getting caught out.

One. Use an email provider that scans messages for malware and spam

Two. Don't click on suspicious links and check what links point to by hovering over them

Three. Don't open suspicious attachments in emails

Four. Download and scan attachments with antivirus software if you need to open them

Five. Be wary of emails where you do not recognise the sender or were not expecting the email

Six. Ignore emails that ask you to enter your username and password for any reason

Seven. Don't forward suspicious emails to others

Eight. Beware of plausible looking emails asking you to confirm your accounts details

Nine. Always verify the senders email address

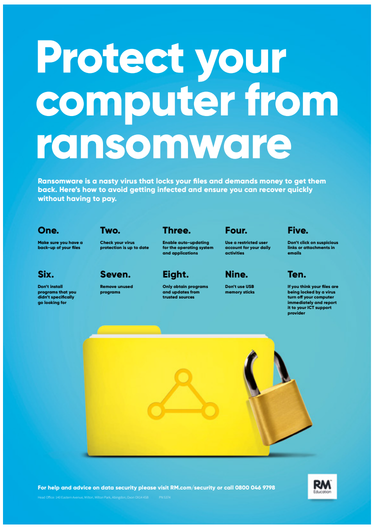
Ten. Beware of official looking emails with spelling and grammar mistakes

For help and advice on data security please visit RM.com/security or call 0800 046 9798

Head Office: 140 Eastern Avenue, Milton, Milton Park, Abingdon, Oxon OX14 4SB PN 5376

RM Education

Download



Protect your computer from ransomware

Ransomware is a nasty virus that locks your files and demands money to get them back. Here's how to avoid getting infected and ensure you can recover quickly without having to pay.

One. Make sure you have a back-up of your files

Two. Check your virus protection is up to date

Three. Enable auto-updating for the operating system and applications

Four. Use a restricted user account for your daily activities

Five. Don't click on suspicious links or attachments in emails

Six. Don't install programs that you didn't specifically go looking for

Seven. Remove unused programs

Eight. Only obtain programs and updates from trusted sources

Nine. Don't use USB memory sticks

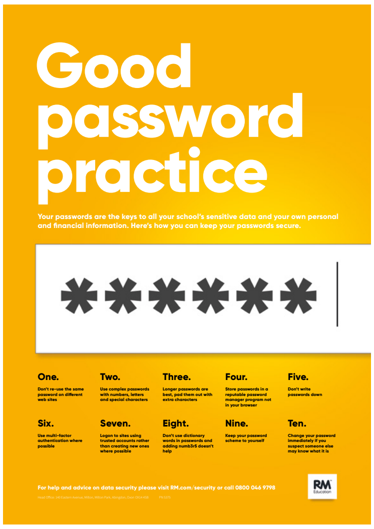
Ten. If you think your files are being locked by a virus turn off your computer immediately and report it to your ICT support provider

For help and advice on data security please visit RM.com/security or call 0800 046 9798

Head Office: 140 Eastern Avenue, Milton, Milton Park, Abingdon, Oxon OX14 4SB PN 5374

RM Education

Download



Good password practice

Your passwords are the keys to all your school's sensitive data and your own personal and financial information. Here's how you can keep your passwords secure.

******

One. Don't re-use the same password on different web sites

Two. Use complex passwords with numbers, letters and special characters

Three. Longer passwords are best, pad them out with extra characters

Four. Store passwords in a reputable password manager program not in your browser

Five. Don't write passwords down

Six. Use multi-factor authentication where possible

Seven. Logon to sites using trusted accounts rather than creating new ones where possible

Eight. Don't use dictionary words in passwords and adding numb3r5 doesn't help

Nine. Keep your password scheme to yourself

Ten. Change your password immediately if you suspect someone else may know what it is

For help and advice on data security please visit RM.com/security or call 0800 046 9798

Head Office: 140 Eastern Avenue, Milton, Milton Park, Abingdon, Oxon OX14 4SB PN 5375

RM Education

Download

Some recent, relevant articles on security

Article reference	Description
TEC5686453	Unsupported Windows 10 builds.
TEC5550285	Security Vulnerability - Exposing RDP (Remote Desktop Protocol).
TEC5557020	Security Vulnerabilities - Risks, external and internal vulnerabilities.

Trend Micro – replacing RM Virus Protect/Symantec Endpoint Protection

Please note that from the 1st September, RM will no longer sell RM Virus Protect (RMVP) and Symantec Endpoint Protection. This means that RMVP and Symantec customers' antivirus contracts will automatically renew to Trend Micro (at the same price as RMVP, £3.21 per device).

Join a webinar to find out more

We'd like to invite you to join a webinar, where you can find out more about why we have partnered with Trend Micro and the antivirus options available to you – on premise, cloud and platform security. Trend Micro are recognised by Gartner (2017) as the leading antivirus/security company and as such we believe their solutions provide a greater level of endpoint protection against ransomware, malware, viruses and new variants as they come about.

The cloud hosted version of Trend Micro has been very popular with RMVP customers who have migrated across already, and so if you would rather your RMVP or SEP contract is upgraded to the cloud version (£4.31 per device) as opposed to the on premise version (£3.21 per device) then please get in touch. For more information about the two products please see below.

Webinars	
Wednesday 12th July	3:30 - 4:30 pm
Thursday 3rd August	10:00 - 11:00 am
Thursday 14th September	10:00 - 11:00 am

To join or receive a recording please email networks@rm.com.

Options available

Trend Micro Cloud (£4.32 per device)

This is hosted and maintained by Trend Micro meaning schools will receive automatic updates and can be server/maintenance free. The solution includes complete device protection with centralised control on Windows, Mac and mobile devices. It protects against common and unknown threats including ransomware, malware and spearfishing. It includes a cloud based antispam filter that can be used with any mail server, as well as Office 365 and G Suite and gives enhanced Office 365 mail security by leveraging sandbox malware analysis for ransomware and other threats.

Cloud App Security (£3.51 per user)

Cloud App Security allows schools to use cloud services while maintaining security. It protects incoming and internal Office 365 mail and cloud file-sharing services such as OneDrive, SharePoint and Google Drive from advanced malware, phishing and other threats by investigating the behaviour of suspicious files. If the content is malicious, it's dealt with in a virtual sandbox. Schools can still use Cloud App Security alongside their current antivirus solution, regardless of the provider. It integrates directly with Office 365/G Suite and other services using APIs, maintaining user functionality.

Trend Micro On-Prem (£3.21 per device)

For schools that do not want to remove their existing server designated to antivirus/security, but still require protection against ransomware and other threats, on any platform, then Trend Micro On-Prem is the solution needed to meet the school's protection needs. This solution incorporates complete device protection and an antispam filter for any on premise mail server and Office 365 and G Suite.

If you would like any further information please contact your account manager.

Support hot topics/CC4 updates

Recent CC4 updates can be found in the article TEC1255704 as usual (note that we have recently reduced the size of this article and put the archived updates in 'TEC5733502 - Archive of Community Connect 4 (CC4) software updates'). CC4 updates in development can also be reviewed in this link: TEC2625548.
Some recent CC4 updates include:

CC4 update/DWN	Description	More information
CC4 Updates Rollup Tool 2017 **DWN5685718**	Covers updates from CC4UPD174 to 201. Allows a faster install of the updates (see below for additional information).	Applicable to CC4.3, 4.5 and CoP networks.
CC4UPD205	A fix to allow CC4 builds to work if recent .NET security updates have been installed at the CC4 First or Site servers.	We recommend that all CC4 customers install this update. Fixes the issues described in TEC5173330.
CC4UPD202	Fixes for CC4 Access 2016 server and Windows 10 Start menu.	Currently in field trial.
CC4UPD203	A new CC4 build root certificate to ensure that builds continue to work after October 2017.	In field trial, but will be live for the summer. See below for more details on this.
CC4UPD204	This will follow on from 203 and is a change to the RM WSUS approval server certificate for your networks.	All CC4 customers will need this critical update to ensure that after October 2017, RM approved WSUS updates continue to be approved within your local WSUS for your servers and computers.

Note on the terminology used in the article:
CC4.3 – your CC4 First server is running Windows 2008R2 server.
CC4.5 – your CC4 First server is running Windows 2012R2 server.
CoP – Connect on Prem - your CC4 First server is running Windows 2016 server.

CC4 Rollup 2017

We are pleased to announce that we have recently made available a new CC4 rollup tool to help you get the latest CC4 updates installed on your network in a timely fashion. CC4 Rollup 2017 includes updates from the range C4UPD174 to CC4UPD201 (note that there are some omissions due to size etc. - these are documented in DWN5685718).

CC4 build certificates & CC4UPD203

In October 2017, the current root certificate used during the CC4 build process (to set up a secure connection between the computer and CC4 server) will expire. We are releasing CC4UPD203 before the summer which contains a replacement certificate for this task. We recommend that all CC4 customers install this to ensure that builds continue to be successful into the new school term.

CC4 OneDrive Mapper – v2 (re-release)

If you use the CC4 OneDriver Mapper, then we recommend that you check the My Account area on rm.com for the re-release of this update. This contains fixes for the following:

- Logon issues if users have an apostrophe in their username.
- A fix for TEC5712760 - RM OneDrive Mapper fails to connect after users have changed their Office 365 password.
- Logon issues from home.

Connect on Prem (CoP) and CC4 Access on 2016 released

We have now released the latest versions of CC4 and CC4 Access on Windows 2016 server. For more information:

- Please click here for more details from Microsoft on Server 2016.
- Please click here for the RM Spring 2017 Seminar session on Server 2016.

Summer activities

CC4 customers may be thinking of activities to perform over the coming summer break. If you are planning a network refresh/rebuild of your computers, then please use the following as a checklist.

☐ Ensure that you have followed the recent security advice and that your WSUS server is functioning correctly (see NWS5696059).

☐ Ensure you have the latest CC4 updates installed (you may wish to start with CC4 Rollup 2017) and then add any additional updates (see DWN5685718).

☐ We recommend that W10 eligible customers install the v1607 (Anniversary Edition) release that is available on rm.com (My Account) before building or rebuilding.

☐ Install CC4UPD203 to add the new CC4 Build Root Certificate.

☐ Review the security best practice checklist (see above).

☐ Install the tool attached to DWN5423369, which adds a GpNetworkStartTimeoutPolicyValue that helps with a number of scenarios.

☐ Ensure that your CC4 build WIMs (OS images) are up to date. The latest WIMs available are: W7 (CC4UPD187 - DWN5028976/CC4UPD188 - DWN5031376), W8.1 (CC4UPD184 - DWN4936049) and the Windows 10 v1607 should be available in your My Account area (if you are eligible).

☐ If you are rebuilding, then you may need to check your OVS-ES licences for W8.1 or W10 to ensure that you can activate Windows correctly.

☐ Use the ‘RMStalePackageDetector’ tool (DWN3522158) to look at your computer estate and work out which ones to core upgrade or rebuild (e.g. if you have a low number of package updates on computers, then core upgrade, however if the list is long then you may wish to rebuild).

☐ We recommend that you implement the package provided in DWN5128006 to help avoid an issue where computers can boot into an unknown state (add this package to your Default Assignments).

Some recent, relevant articles

Articles

Article reference	Description
TEC5714011	RM WSUS - Updates may remain in an Approval Pending state within the RMMC.
DWN5142756	CC4.5 networks may have computers showing as 'Offline' in the RMMC if the ephemeral ports have been reset to defaults.
TEC5658152	Upcoming webinars - spring and summer 2017. (Any customer can apply for and attend these webinar sessions.)
TEC5730060	Veeam Backup & Replication backup fails with error "Unable to truncate Microsoft SQL Server transaction logs".
TEC1329475	Community Connect 4 Microsoft Updates - Overview Guide.
TEC5666650	Best practice advice on Trend Micro Worry-Free Business Security installation.
TEC5631372	Best practice advice on anti-virus removal.
NWS5448877	CC4 Windows 10 strategy.
TEC5764035	How to alter the "Active Hours" for Windows 10 v1607 and above computers in CC4.
NWS5701113	CC4DRV111 and 114 (and soon to be re-released CC4DRV113) have been re-released to address a security issue with the Conexant HD Audio driver. We recommend you install these new driver packs before any summer rebuilds if you have computers that use these packs.

Also, do visit the CC4 portal on the RM Support website for the latest editor's choice and technical articles. For the full list of CC4 Assured hardware please see TEC1299560.

Updates to RM Cloud Backup

Our installation services have been updated to include MABs update 2. This will be affecting our D2D2C service only. To summarise the key features that you will benefit from by having the updated version installed:

- Can now be installed on Server 2016. This is separate to its ability to back up server 2016 servers, which it has always been able to do.
- Support for backing up SQL 2016, SharePoint 2016 and Exchange 2016.
- New Modern Backup Storage technology that allows for up to three times faster disk backups and up to 50% reduction in on premise storage consumption.
- It leverages Windows Server 2016 native capabilities such as REFS block cloning, deduplication and workload aware storage to optimise overall storage utilisation.
- Support for backing up Hyper-v 2016 host VMs which uses Resilient Change Tracking (RCT) technology for incremental backups.
- This means more reliable backups i.e. no more consistency checks.
- Support for vCenter and ESXi v6.5.

To find out more about RM Cloud Backup watch a webinar now at https://youtu.be/Jq7ByqMFT4s

RM Supported Technologies List

The latest version of the supported technology list now includes support for Server 2016, MABS and Trend Micro. Click here to find out more.

RM Unify – Network provisioning

We are pleased to announce that we will soon be releasing an add-on to allow user provisioning into CC4 networks from RM Unify. If you are interested in finding out more please email rmunify@rm.com.

The RM Unify roadmap is available to view here https://trello.com/b/qpuOCQTg

Webinars

We are running a series of regular webinars to help you stay up to date with the latest technologies, products and services for your school. Delivered by one of our experts, or partners, the webinars are free to join and will last no longer than an hour with a live Q&A built in.

Upcoming Webinars	
RM Cloud Backup	Tuesday 11th July 9:30 - 10:15am
Countdown to GDPR - what is involved for your school and the steps to take to get GDPR ready	Tuesday 11th July 3:30 - 4:15pm
What's new in Office 365 - Microsoft Teams for Education	Wednesday 12th July 9:30 - 10:15am

Find out more or book your place now.

RM Seminars

Autumn 2017 – Save the date!

We look forward to you joining us at one of the RM Seminars in the autumn. We are working on the CPD content for these events, so please email any suggestions you may have to: networks@rm.com

Thursday 2nd November
Google London (Giles St)

Tuesday 7th November
Microsoft Reading

Friday 10th November
Warrington, Park Royal Hotel

Monday 13th November
Stansted, Radisson Blu

Wednesday 15th November
Exeter, Sandy Park

Wednesday 22nd November
Ashford, Ashford International

Monday 27th November
St Johns Hotel, Birmingham

Date/venue to be confirmed
London

To book your place please visit: www.rm.com/seminars

RM Recommends

RM Recommends – Server and Storage range

We have expanded the RM Recommends range to now include servers and storage, with Dell EMC as our chosen partner. The range includes five years Dell Pro-Support as standard with the option of including RM Disaster Recovery; a unique add on providing full server recovery in the event of hardware failure.

Take a look at the range here and email hardware@rm.com for any enquiries.

RM Recommends – Secondary school wireless

Working with Fortinet as their number one partner within the education market, we are able to offer you wireless technology like no other! Fortinet's single channel technology is perfect for your school's environment for the following reasons:

- Allows ease of roaming for teachers and pupils without the hassle of switching between multiple channels.
- The technology enables speeds of up to 2 x faster than competitor speeds.
- With RM's price promise, you won't be able to find Fortinet wireless cheaper.

Please email fortinet@rm.com for any enquiries.

Other news...

Microsoft Teams in Education

Microsoft have released more information about classroom collaborative tools in Microsoft Teams. Join our 'What's new in Office 365' webinar on the 12th July – 9.30-10.15 am to find out more. Email networks@rm.com for joining instructions.

The Association of Network Managers in Education (ANME)

ANME is a non-profit making organisation founded by two network managers and run voluntarily by Rick Cowell, a network manager, with over fifteen years' experience.

The ANME caters for network managers and IT technicians from all over the country, providing CPD in the form of termly meetings. Although focussing on the larger area of secondary schools, the ANME is open to all network managers in all stages and sectors of education, and in addition welcomes IT support staff who maintain the IT infrastructure and day-to-day running of the network.

Join for free now at www.anme.co.uk

My Account

Software releases and new CC4 features are delivered via your My Account area of rm.com. If you have purchased a product or are otherwise entitled to it, you will be able to download it from your My Account area as soon as it is available. If you are not sure whether you are eligible for a product e.g. whether you have the necessary licences, then please contact your Sales Account Manager. Please see TEC1983855 for further details.

Meet the team

Srijith Ravindran Nair
Project Lead
RM India

Srijith manages the 2nd and 3rd line support teams in India as well as the remote implementations team.

He joined RM in Jan 2005 as a graduate trainee in the TRG team and has worked in a number of roles including the 'Integration Service team" and the managed services' TSG team.

He holds a postgraduate (MSc) in Computer Networking and certificates in CCNA, MCSA 2000, VCP 4.1. Six Sigma Black belt and is also a certified 'ITIL Expert' and is very fond of ITIL practice!

Srijith has won a number of awards in recognition of the improvement processes he has introduced and for the quality of the customer service he provides. Outside work, he loves reading books and travelling around in his car. His favourite book is Wings of Fire by Dr. APJ Abdul Kalam and his favourite car to drive is the Honda City.

Look out for the next issue!

Email any suggestions to
supportnewsletter@rm.com

RM Education

Support Newsletter

Issue Sixteen / March 2017

Included in this issue...

Support hot topics
Connect on Prem – CC4 on Server 2016
Automatic CC4 AD provisioning
Supported technologies newly added to your support contract
Webinars – Cloud backup and Moving Office to the Cloud
RM Cloud

RM Education

Barry Macpherson
Support Engineer, Bellshill, Scotland