PwC Weekly
Security Report

This is a weekly digest of security news and events from around the world. Excerpts from news items are presented and web links are provided for further information.

pwc

Microsoft zero-day attacks see hackers target Word users with new bug

A new zero-day vulnerability that affects all supported versions of Microsoft Word has been uncovered and security researchers claim that hackers have already launched attacks in the wild, leveraging the bug. A patch is yet to be issued out for this particular vulnerability, which security experts believe, allows attackers to secretly infect systems with different kinds of malware.

The zero-day bug was disclosed by both McAfee and FireEye, who claimed to have notified Microsoft. However, the tech giant is slated to issue out a patch this week to coincide with Patch Tuesday, a Microsoft spokesperson confirmed, ZDNet reported.

According to McAfee researchers, the "earliest attack" detected dates back to January. "The samples we have detected are organized as Word files (more specially, RTF files with '.doc' extension name). The exploit works on all Microsoft Office versions, including the latest Office 2016 running on Windows 10," McAfee researchers said.

The bug is triggered when users open a tricked Word document, which then downloads a malicious HTML file. The file runs a script that hackers can use to install malware. FireEye researchers said, "The Microsoft HTA application loads and executes the malicious script. In both observed documents the malicious script terminated the winword.exe process, downloaded additional payload(s), and loaded a decoy document for the user to see. The original winword.exe process is terminated in order to hide a user prompt generated by the OLE2link."

In other words, hackers can attack affected systems, all the while bypassing security detecting mechanisms designed to prevent such attacks. "This is a logical bug, and gives the attackers the power to bypass any memory-based mitigations developed by Microsoft," McAfee researchers said.

The most alarming aspect of this bug is that it does not rely on enabling macros to infect systems. This means that potential victims may likely not receive Office's alert to users when opening macro-enabled files. In other words, any Word file may potentially contain malicious content.

It is still uncertain as to how many have already been targeted by hackers leveraging this zero-day. Security researchers are yet to disclose further details surrounding the vulnerability, including the identity of the attackers leveraging the bug.

Source:
http://www.ibtimes.co.uk/microsoft-zero-day-attacks-see-hackers-target-word-users-new-bug-that-affects-every-version-1616239

Our perspective

A critical zero-day attack on Microsoft Word is in the wild. Given the broad user base, this attack is a matter of high concern. The bug exploits the OLE functionality to terminate a bait Word document in order to hide a user prompt generated by the OLE2Link. As Microsoft has not released any patch yet, we strongly recommend that Microsoft Office administrators assess the risk of the threat within their environment and apply patches as soon as they become available.
Until Microsoft issues an official patch for this vulnerability, we recommend that Office users protect themselves or mitigate the threat of this zero-day attack by following the guidelines below:
1. Refrain from opening any Office files obtained from untrusted locations.
2. Ensure Office Protected View is enabled as the bug cannot bypass the protected view.
3. Implement the solution provided here: https://arstechnica.com/security/2017/04/booby-trapped-word-documents-in-the-wild-exploit-critical-microsoft-0day/

Hard-coded passwords put industrial systems at risk

We've been dabbling with commercial computing for well over half a century, but we're still making the same mistakes. One of the biggest howlers is hard-coding passwords directly into our computer and networking systems for hackers to find. Just this month, it happened again.

Schneider Electric, which makes supervisory control and data acquisition (SCADA) equipment, has been shipping products with passwords embedded in the firmware, revealed researchers from German firm OpenSource Security. They found that not only was the password for the Schneider ModiconTM221CE16R logic controller hard-coded into the firmware, but that it could not be changed.

The password in question is a decryption key used to open a project file on the system. The hard-coded encryption key is "SoMachineBasicSoMachineBasicSoMa", and cannot be changed. By decrypting the XML file with the key, the user password can be found in the decrypted data, which then allows attackers to modify the system.

The researchers finally went public with the information on April 4, after trying to contact Schneider Electric about it. In response, the vendor sent a mea culpa statement to SC Magazine UK, admitting that they messed up, and promising to do better.

What were they thinking?

Insecurities in SCADA systems are bad enough, because they are industrial control systems that keep serious pieces of critical national infrastructure running, ranging from water treatment plants to agricultural systems. These aren't the kind of things that you want to be vulnerable, and yet hard-coded passwords are a common problem in that world. Siemens has been caught putting hardwired passwords into its own controllers more than once.

Hard-coded passwords also crop up in other products.

Routers are common targets for attack because vendors won't learn from each others' mistakes. US-CERT warned that droves of them were discovered to have hard-coded passwords in 2015,

This month, Cisco found that its Mobility Express Software, which ships with some of its Aironet wireless access points, has an admin-level FSH password hard-coded.

Lenovo included the password 12345678 into the Android and Windows versions of its SHAREit file sharing app, and in a clear entry into the "what were they thinking" category, researchers found hard-coded passwords in around 300 medical devices across approximately 40 vendors. This stuff is rampant.

Why do people hard-code passwords in the first place? One reason is that manufacturers just aren't very good at customizing equipment rolling off the production line. Burning the same thing into every device makes them easier to manage.

Another is that it makes the development process easier. Developers will often need shared access to certain system resources such as internal databases when developing a product, and they'll frequently embed the access passwords directly in their code to make authentication easier. They always mean to change it later, of course, but it's often not a priority.

Unfortunately, while all these things make it easier for the vendor, it also makes them easier to hack.

So what's the answer? One potential solution, according to OWASP, is to use a "first login" mode that requires the user to enter a unique strong password.

This would be a great example of security by design – the concept of designing systems from the ground up with security in mind, rather than bolting it on later as an afterthought. It carries its own challenges, though: what if the user forgets their password? In that case, a factory reset would get them back to first-login mode, presumably.

Hard-coded passwords put industrial systems at risk

Hard-coded passwords won't always be visible to users. They're buried in the source code, but can still be found by a malicious actor with motivation and the appropriate tools. So what can companies do to try and protect themselves?

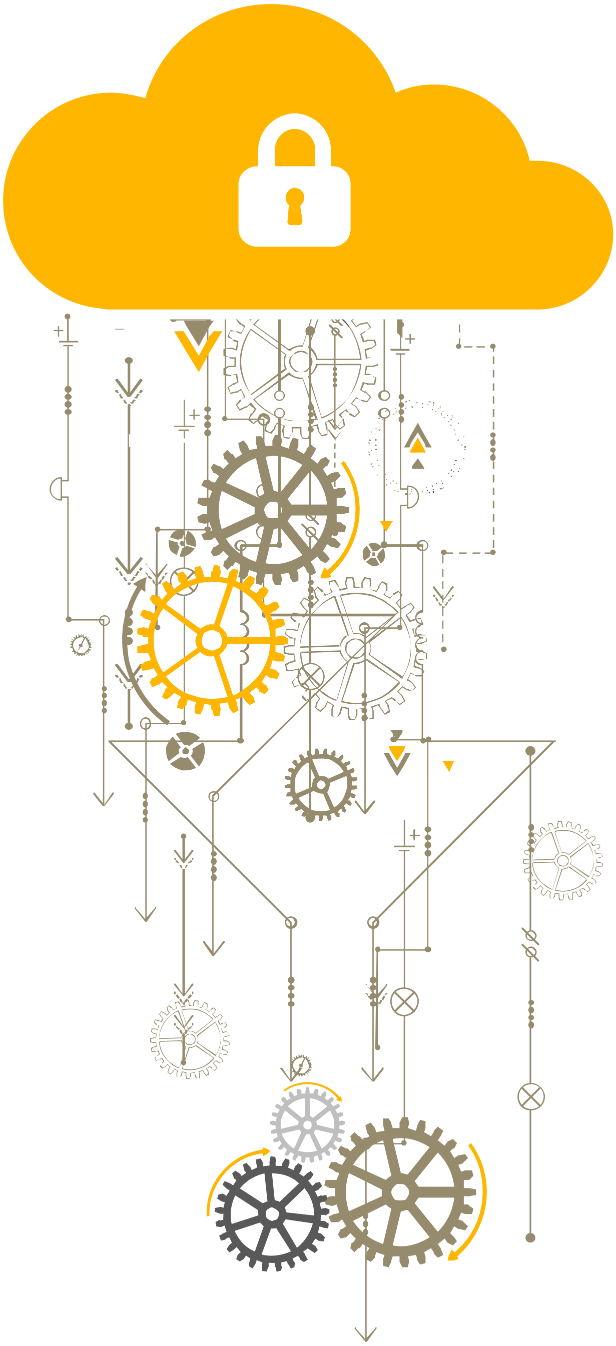
Having a word with the vendor is a good place to start. Asking them how easy it would be for the company to recover the device for you in the event of a lost password can reveal whether hard-coded passwords are a known feature. Simply asking the company straight out to confirm that it doesn't use these things is also a strategy.

However, there is always the chance that the vendor simply may not know about the vulnerability. Trust no one.

Segmenting equipment inside your organization is important, so that if someone gets access to a system, they won't be able to move laterally without a lot of extra work and other system compromises. Use different subnets, and harden individual systems against attack.

None of this will completely eliminate the risk – in cybersecurity, nothing ever does – but it will at least reduce it.

Source:
https://nakedsecurity.sophos.com/2017/04/10/hard-coded-passwords-put-industrial-systems-at-risk



Forget Mirai – Brickerbot malware will kill your crap IoT devices

A new form of attack code has come to town and it uses techniques similar to Mirai to permanently scramble Internet of Things devices.

On March 20 researchers at security shop Radware spotted the malware, dubbed Brickerbot, cropping up in honeypots it sets up across the web to lure interesting samples. In the space of four days, one honeypot logged 1,895 infection attempts by Brickbot, with the majority of attacks coming from Argentina, and a second logged 333 attempts – untraceable as they came from a Tor node.

"The Bricker Bot attack used Telnet brute force – the same exploit vector used by Mirai – to breach a victim's devices," Radware's advisory states.

"Bricker does not try to download a binary, so Radware does not have a complete list of credentials that were used for the brute force attempt, but were able to record that the first attempted username/password pair was consistently 'root'/'vizxv.'"

The malware targets Linux-based IoT devices running the BusyBox toolkit, and seems to have a particular affinity for Ubiquiti network devices, which have their own security issues. Once inside the operating system, the code starts to scramble the onboard memory using rm -rf /* and disabling TCP timestamps, as well as limiting the max number of kernel threads to one.

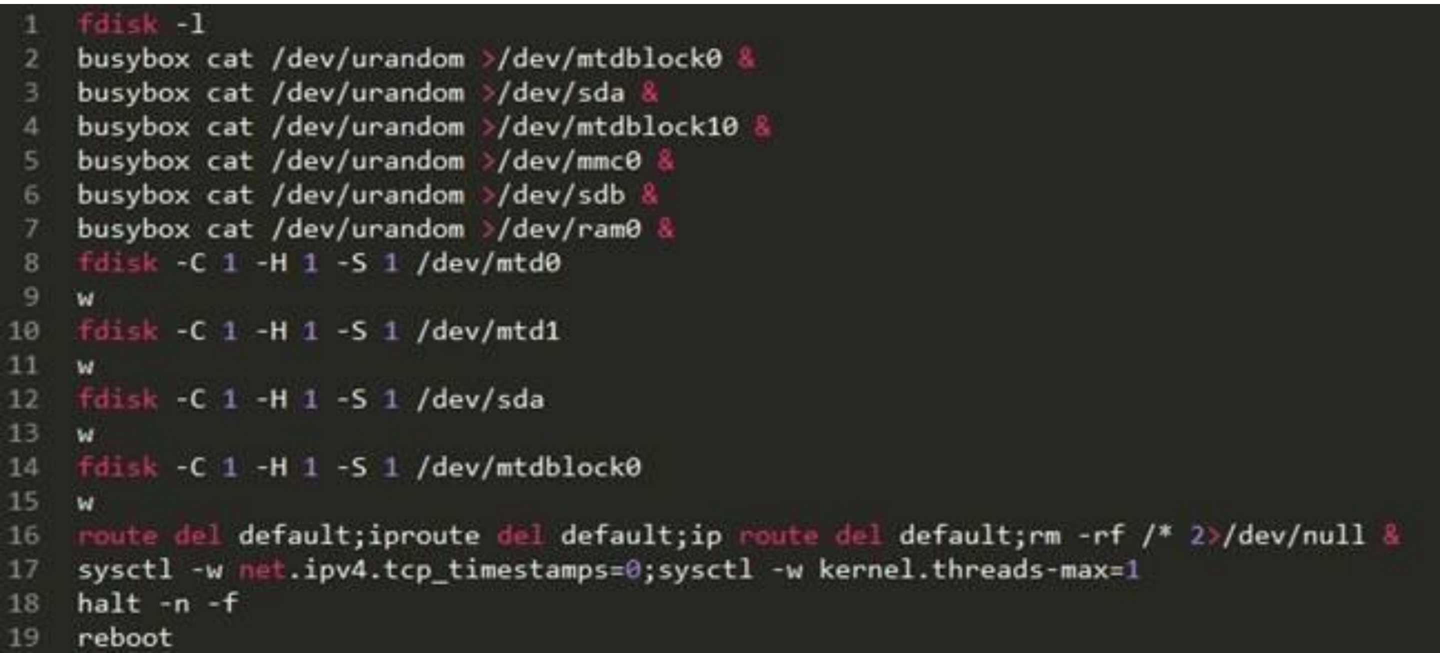
Brickerbot then flushes all iptables firewall and NAT rules and adds a rule to drop all outgoing packets. Finally it tries to wipe all code on the affected devices and render them useless – a permanent denial of service.

To block the attack, the key factor is disabling Telnet and changing the device's factory-set passwords. Radware also recommends using intrusion prevention systems to lock down devices.

Source: ***https://www.theregister.co.uk/2017/04/08/brickerbot_malware_kills_iot_devices/***

Our perspective

Botnets have the potential to wreak havoc. Some like Mirai have done serious damage to many organisations. The presence of the Brickerbot botnet in the wild is a matter of concern, as this botnet is using a default password and exploiting telnet. Administrators are advised to change the default password of routers and limit access to telnet the devices.



```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

PwC collaborates in uncovering new global cyber espionage campaign

The close working collaboration between private sector companies and UK's National Cyber Security Centre led to identifying and disrupting new cyber-attack campaign.

A hacking group has conducted one of the most prolific espionage campaigns since APT1 in 2013, employing new tactics to reach a broad audience.

PwC's cyber security practice has worked closely with BAE Systems and other members of the security community and the UK's National Cyber Security Centre (NCSC), to uncover and disrupt what is thought to be one of the largest ever sustained global cyber espionage campaigns.

Since late 2016, when the scale of the espionage campaign became increasingly apparent, PwC and BAE Systems, through their membership of the Cyber Incident Response (CIR) scheme, shared their research into the campaign with NCSC, which has notified affected communities.

PwC and BAE Systems believe the hacking group widely known as 'APT10' conducted the espionage campaign, by targeting providers of managed outsourced IT services as a way in to their customers' organisations around the world, gaining unprecedented access to intellectual property and sensitive data.

This indirect approach of reaching many through only a few targets demonstrates a new level of maturity in cyber espionage. The sheer scale of the operation was only uncovered through collaboration, and is still only likely to reflect a small portion of APT10's global operations.

Richard Horne, cyber security partner at PwC, commented:

- "The future of cyber defence lies beyond simple intelligence sharing, but in forging true collaboration between organisations in the public and private sector with the deep technical and innovative skills required to combat this type of threat.
- "This operation has demonstrated the importance of the recently established National Cyber Security Centre, set up for moments just like this. Operating alone, none of us would have joined the dots to uncover this new campaign of indirect attacks.
- "Together we've been working to brief the global security community, managed service providers and known end victims to help prevent, detect and respond to these attacks.
- "New forms of attack require new ways of working to defend our society. Close working collaboration is key."

APT10 campaign key findings

We have seen APT10 targeting managed service provider networks from 2016 onwards, and it is likely that this activity had begun as early as 2014.

APT10 has significantly increased its scale and capability since early 2016, adding new developers and intrusion operators to continually enhance their capability.

APT10 focuses on espionage activity, targeting intellectual property and other sensitive data from a wide range of sectors and countries. The group is known to have exfiltrated a high volume of data from multiple victims and used compromised networks to stealthily move this data around the world.

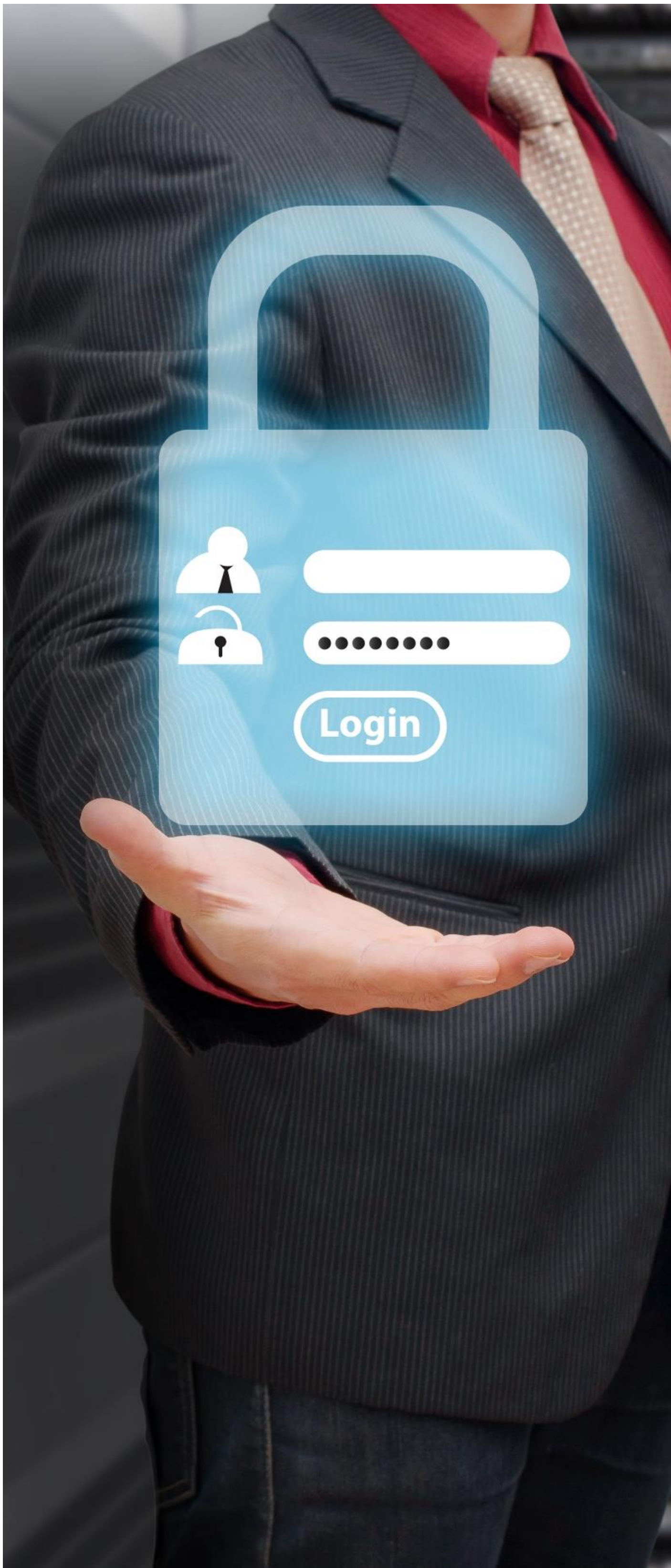
A number of Japanese organisations have also been targeted directly in a separate, simultaneous campaign by the same group, with APT10 masquerading as legitimate Japanese government entities to gain access

Kris McConkey, partner, cyber threat detection and response at PwC, who will present on the findings of this joint research today at the Kaspersky Security Analyst Summit in St. Maarten, added:

PwC collaborates in uncovering new global cyber espionage campaign

- "The indirect approach of this attack highlights the need for organisations to have a comprehensive view of the threats they're exposed to – including those of their supply chain. Alongside our research work, we have also notified the threat intelligence community and worked with the NCSC to notify managed service providers and known victims.
- "This is a global campaign with the potential to affect a wide range of countries, so organisations around the world should work with their security teams and providers to check networks for the key warning signs of compromise and ensure they respond and protect themselves accordingly."

Source: http://www.pwc.co.uk/who-we-are/regional-sites/northern-ireland/press-releases/cyber-espionage-campaign.html



Wonga data breach: Almost 270,000 customers could be affected

Payday loan firm Wonga says it is "urgently investigating" a potential data breach that could have affected up to 270,000 customers.

The company says the hack involved "illegal and unauthorised access" to the personal data of current and former customers in both the UK and Poland, with up to 245,000 UK borrowers potentially affected.

It remains unclear where the hack took place, but Wonga is said to have known of the attack for more than a week – though it initially didn't believe data had been stolen.

The lender has began making customers aware of the hack on Saturday, providing details of a dedicated customer services phone line.

Affected borrowers were informed that the data accessed may have included names, email addresses, home addresses, phone numbers, the last four digits of card numbers (but not the whole number) and/or bank account numbers and sort codes.

According to the firm, customers' login details for their online accounts didn't seem to have been stolen at this point.

In a statement, it said: "We do not believe your Wonga account password was compromised and believe your account should be secure, however if you are concerned you should change your account password."

A message sent to those affected read: "We believe there may have been illegal and unauthorised access to some of your personal data on your Wonga.com account."

The company also said in a statement that it was “working closely with authorities" and is "in the process of informing affected customers.”

The police, Information Commissioner’s Office (ICO), and the FCA have all been made aware of the suspected breach. with a spokesperson for the ICO telling The Guardian: “All organisations have a responsibility to keep customers’ personal information secure. Where we find this has not happened, we can investigate and may take enforcement action.”

If you're concerned that you may have been affected, the company advises contacting your bank and asking them to be monitor for suspicious activity.

It also says customers should be more aware of online or telephone scams, and has set up a help page with advice, which can be found here.

Source:
http://www.trustedreviews.com/news/wonga-data-breach-almost-250-000-customers-could-be-affected

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,23,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity. Please see www.pwc.com/structure for further details.

For any queries, please contact:

Sivarama Krishnan
sivarama.krishnan@in.pwc.com

Amol Bhat
amol.bhat@in.pwc.com

This report presents the highlights of security news and events from around the world that have been published on external websites. This publication has been prepared for a general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC, its partners, employees and agents do not accept any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it. PwC is however available for follow-up on any queries you may have regarding information and IT security. The views, opinions and interpretation shared in the newsletter are strictly of the individual's collating this newsletter and is not necessarily a representation of the firm's views. All images, information, references in this presentation are protected by copyright, trademark, patent, trade secret and other intellectual property laws of the respective publisher. Our sharing of this presentation along with such protected images with you does not authorise you to copy, republish, frame, link to, download, transmit, modify, adapt, create derivative works.

MB/April2017-9382