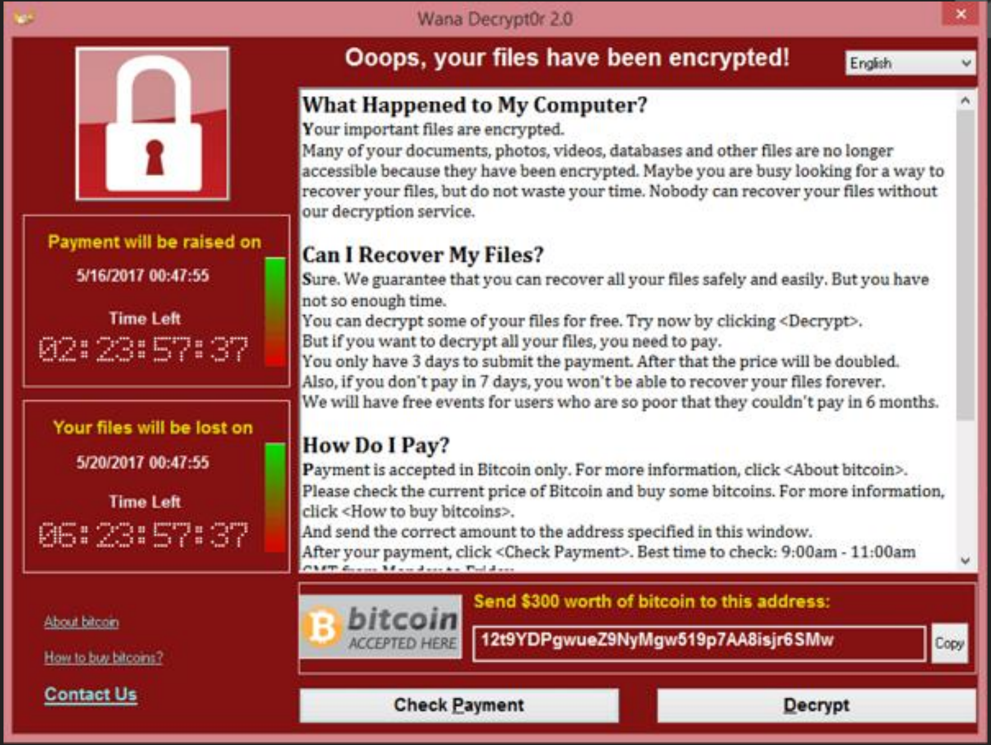
Ransomware 0
Admins 1

Kieran Jacobsen
Readify

Kieran Jacobsen

- Head of Information Technology at Readify
- Microsoft MVP, Cloud and Datacenter Management
- PoshSecurity.com
- PlanetPowerShell.com

NHS



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

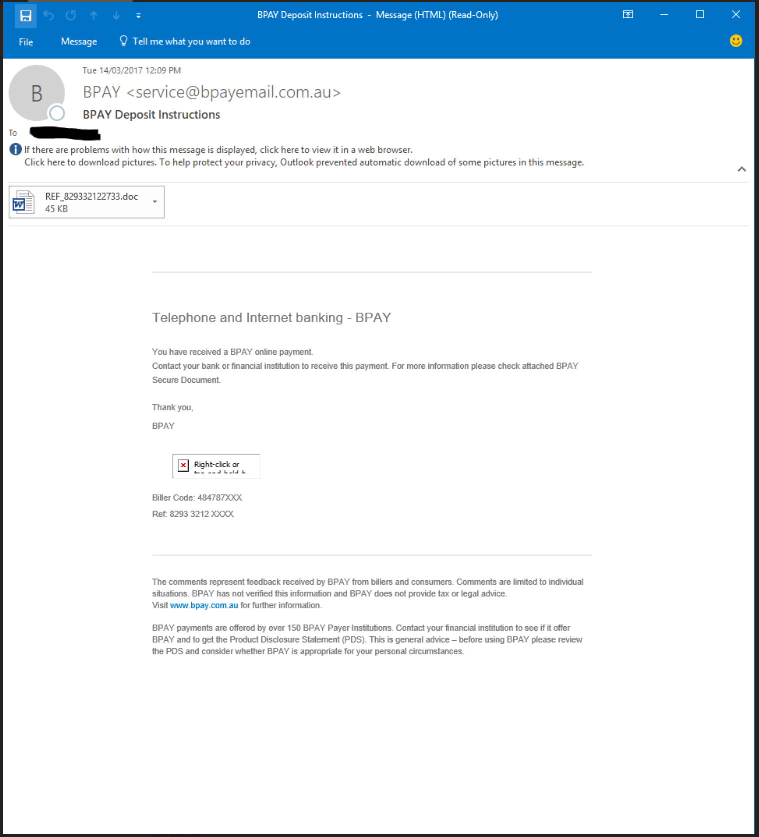
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

MAERSK LINE
MADRID MÆRSK


BPAY Deposit Instructions - Message (HTML) (Read-Only)
File
Message
Tell me what you want to do

Tue 14/03/2017 12:09 PM

BPAY <service@bpayemail.com.au>

BPAY Deposit Instructions

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

REF_829332122733.doc
45 KB

Telephone and Internet banking - BPAY

You have received a BPAY online payment.
Contact your bank or financial institution to receive this payment. For more information please check attached BPAY Secure Document.

Thank you,

BPAY

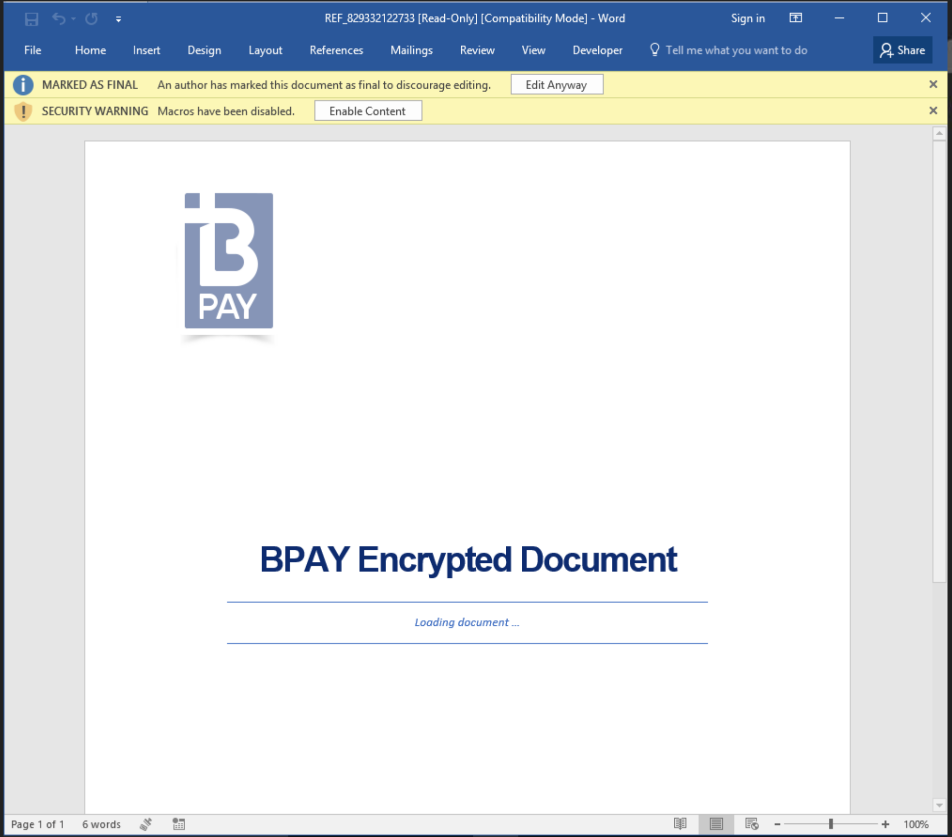
Right-click or

Biller Code: 484787XXX

Ref: 8293 3212 XXXX

The comments represent feedback received by BPAY from billers and consumers. Comments are limited to individual situations. BPAY has not verified this information and BPAY does not provide tax or legal advice.
Visit www.bpay.com.au for further information.

BPAY payments are offered by over 150 BPAY Payer Institutions. Contact your financial institution to see if it offer BPAY and to get the Product Disclosure Statement (PDS). This is general advice – before using BPAY please review the PDS and consider whether BPAY is appropriate for your personal circumstances.



MARKED AS FINAL An author has marked this document as final to discourage editing.

SECURITY WARNING Macros have been disabled.

BPAY Encrypted Document

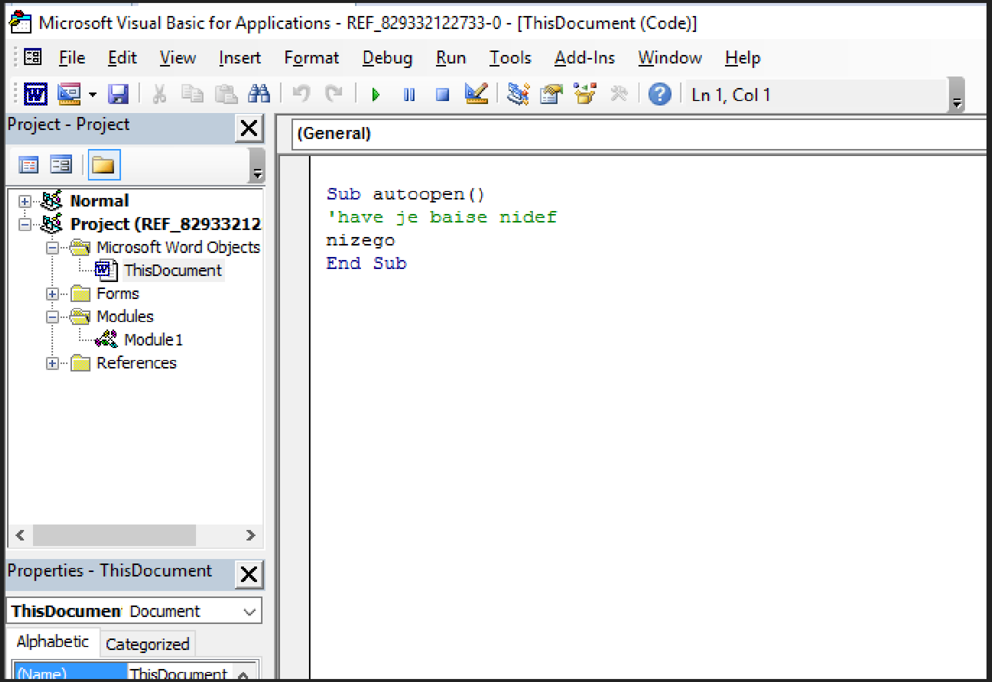
Loading document ...

WARNING!
YOU MUST
BE THIS TALL
TO RIDE THIS RIDE

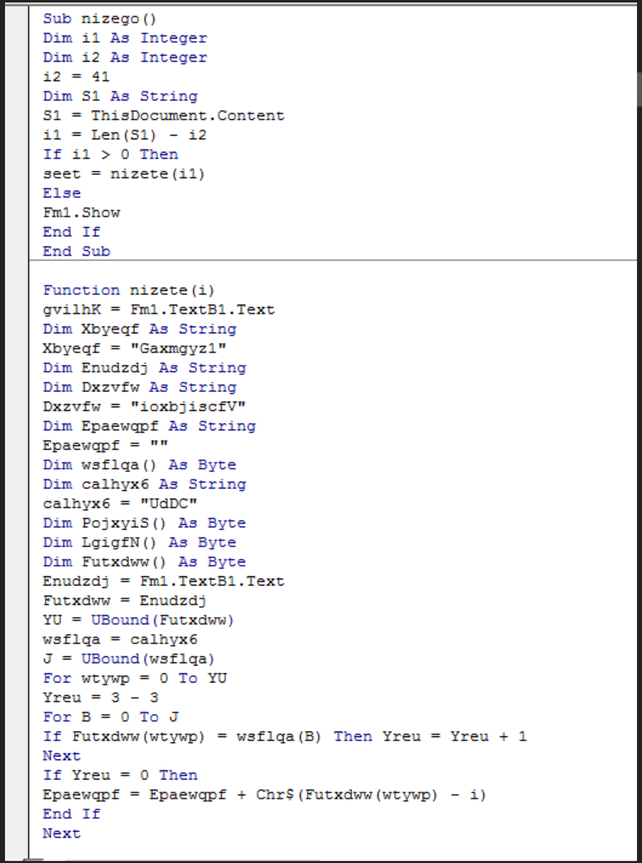
Things you should already know

- Network Segmentation
- Patching

Disable Macros



```
Sub autoopen()
'have je baise nidef
nizego
End Sub
```



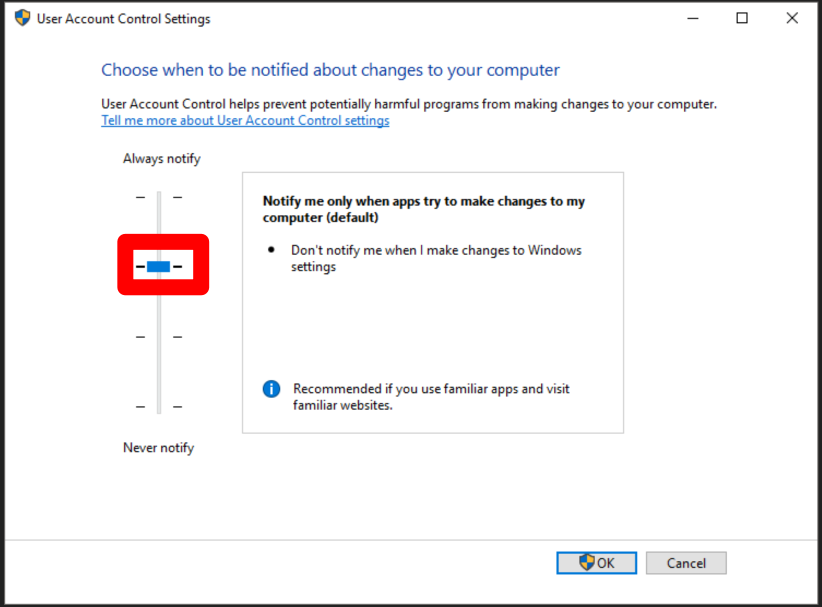
```
Sub nizego()
Dim i1 As Integer
Dim i2 As Integer
i2 = 41
Dim S1 As String
S1 = ThisDocument.Content
i1 = Len(S1) - i2
If i1 > 0 Then
seet = nizete(i1)
Else
Fm1.Show
End If
End Sub

Function nizete(i)
gvilhK = Fm1.TextB1.Text
Dim Xbyeqf As String
Xbyeqf = "Gaxmgyz1"
Dim Enudzdj As String
Dim Dxzvfw As String
Dxzvfw = "ioxbjiscfV"
Dim Epaewqpf As String
Epaewqpf = ""
Dim wsflqa() As Byte
Dim calhyx6 As String
calhyx6 = "UdDC"
Dim PojxyiS() As Byte
Dim LgigfN() As Byte
Dim Futxdww() As Byte
Enudzdj = Fm1.TextB1.Text
Futxdww = Enudzdj
YU = UBound(Futxdww)
wsflqa = calhyx6
J = UBound(wsflqa)
For wtywp = 0 To YU
Yreu = 3 - 3
For B = 0 To J
If Futxdww(wtywp) = wsflqa(B) Then Yreu = Yreu + 1
Next
If Yreu = 0 Then
Epaewqpf = Epaewqpf + Chr$(Futxdww(wtywp) - i)
End If
Next
```

Don’t run as Local Admin

Friends don’t let friends run as local administrators!

Configure UAC



User Account Control Settings

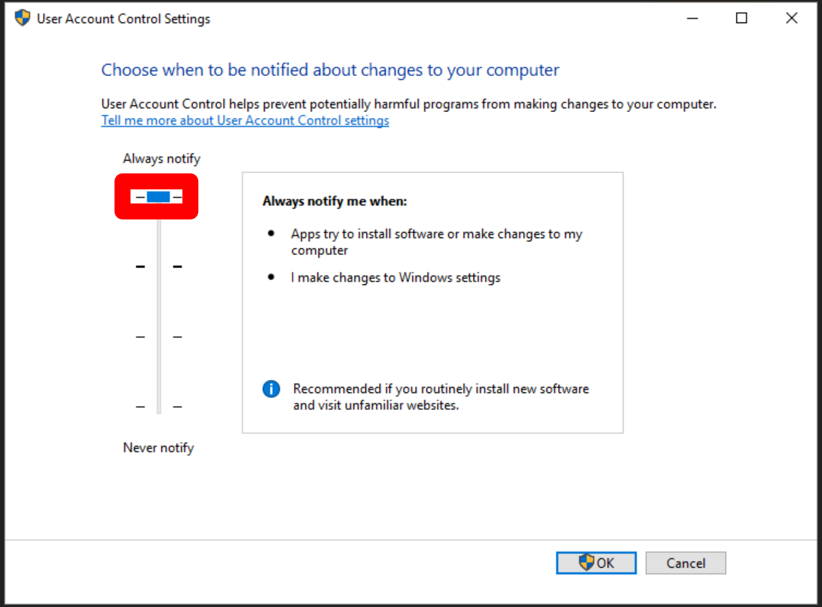
Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Notify me only when apps try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar apps and visit familiar websites.



User Account Control Settings

Choose when to be notified about changes to your computer

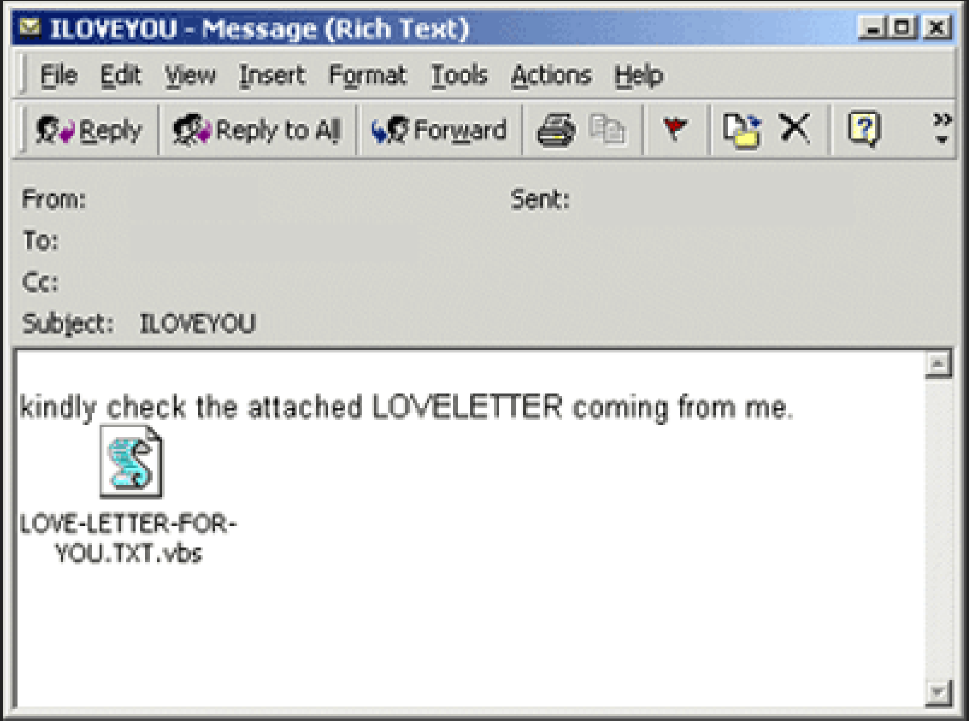
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

Always notify me when:

- Apps try to install software or make changes to my computer
- I make changes to Windows settings

Recommended if you routinely install new software and visit unfamiliar websites.

Change Default Extension Actions


ILOVEYOU - Message (Rich Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

From:

Sent:

To:

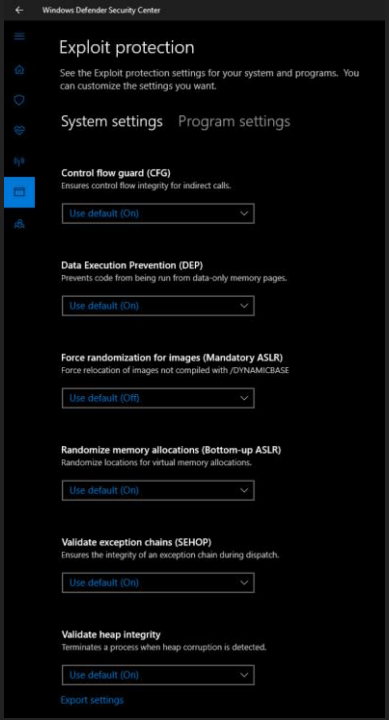
Cc:

Subject: ILOVEYOU

kindly check the attached LOVELETTER coming from me.

LOVE-LETTER-FOR-YOU.TXT.vbs

Windows Defender Exploit Guard



Exploit protection

See the Exploit protection settings for your system and programs. You can customize the settings you want.

Control flow guard (CFG)
Ensures control flow integrity for indirect calls.
Use default (On)

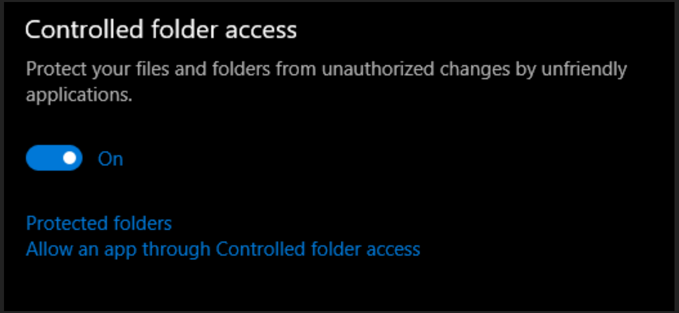
Data Execution Prevention (DEP)
Prevents code from being run from data-only memory pages.
Use default (On)

Force randomization for images (Mandatory ASLR)
Force relocation of images not compiled with /DYNAMICBASE
Use default (Off)

Randomize memory allocations (Bottom-up ASLR)
Randomize locations for virtual memory allocations.
Use default (On)

Validate exception chains (SEHOP)
Ensures the integrity of an exception chain during dispatch.
Use default (On)

Validate heap integrity
Terminates a process when heap corruption is detected.
Use default (On)

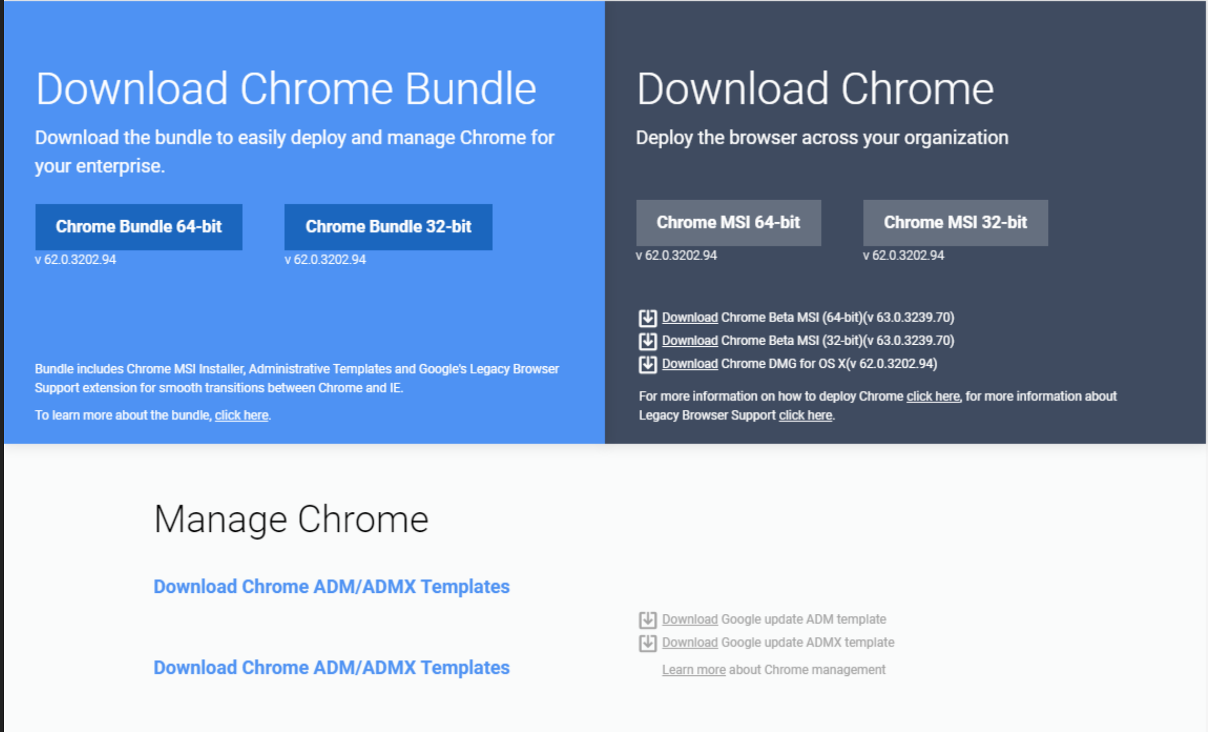


Controlled folder access

Protect your files and folders from unauthorized changes by unfriendly applications.

On

Deploy Chrome and Firefox



Download Chrome Bundle

Download the bundle to easily deploy and manage Chrome for your enterprise.

v 62.0.3202.94

v 62.0.3202.94

Bundle includes Chrome MSI Installer, Administrative Templates and Google's Legacy Browser Support extension for smooth transitions between Chrome and IE.

To learn more about the bundle, click here.

Download Chrome

Deploy the browser across your organization

v 62.0.3202.94

v 62.0.3202.94

Download Chrome Beta MSI (64-bit)(v 63.0.3239.70)
Download Chrome Beta MSI (32-bit)(v 63.0.3239.70)
Download Chrome DMG for OS X(v 62.0.3202.94)

For more information on how to deploy Chrome click here, for more information about Legacy Browser Support click here.

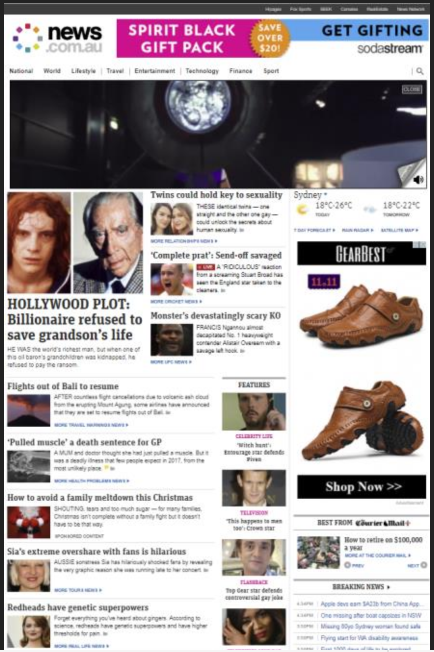
Manage Chrome

Download Chrome ADM/ADMX Templates

Download Chrome ADM/ADMX Templates

Download Google update ADM template
Download Google update ADMX template
Learn more about Chrome management

Block Advertising in Browsers



Twins could hold key to sexuality

'Complete prat': Send-off savaged

HOLLYWOOD PLOT: Billionaire refused to save grandson's life

Monster's devastatingly scary KO

Flights out of Bali to resume

'Pulled muscle' a death sentence for GP

How to avoid a family meltdown this Christmas

Sia's extreme overshare with fans is hilarious

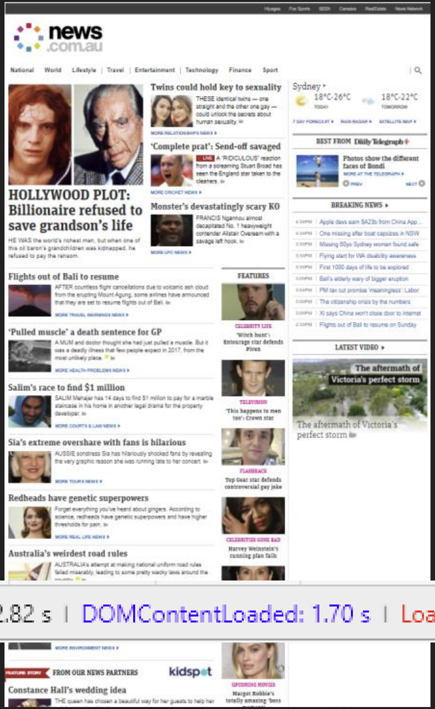
Redheads have genetic superpowers

BEST FROM Courier Mail

How to retire on $100,000 a year

BREAKING NEWS

720 requests | 13.8 MB transferred | Finish: 43.45 s | DOMContentLoaded: 1.46 s | Load: 21.53 s


news.com.au
National World Lifestyle Travel Entertainment Technology Finance Sport
Sydney
18°C-26°C
18°C-22°C
kidspot

Twins could hold key to sexuality

'Complete prat': Send-off savaged

HOLLYWOOD PLOT: Billionaire refused to save grandson's life

Monster's devastatingly scary KO

BEST FROM Daily Telegraph

Photos show the different faces of Bondi

BREAKING NEWS

Flights out of Bali to resume

'Pulled muscle' a death sentence for GP

Salim's race to find $1 million

Sia's extreme overshare with fans is hilarious

Redheads have genetic superpowers

Australia's weirdest road rules

LATEST VIDEO

The aftermath of Victoria's perfect storm

FROM OUR NEWS PARTNERS

Constance Hall's wedding idea

176 requests | 1.0 MB transferred | Finish: 2.82 s | DOMContentLoaded: 1.70 s | Load: 2.09 s

Thank you

Macros

https://decentsecurity.com/enterprise/#/block-office-macros/

UAC

https://www.tenforums.com/tutorials/3577-change-user-account-control-uac-settings-windows-10-a.html

Script Extensions

http://www.dankalia.com/tutor/01002/0100201018.htm

Exploit Guard

https://docs.microsoft.com/en-us/windows/threat-protection/windows-defender-exploit-guard/windows-defender-exploit-guard

Chrome & Firefox

- Chrome: http://goo.gl/2QvOT
- Firefox: https://developer.mozilla.org/en-US/Firefox/Enterprise_deployment

Ad Blocking

- Internet Explorer: https://decentsecurity.com/adblocking-for-internet-explorer-deployment/
- Edge: https://www.microsoft.com/en-us/store/p/adblock/9nblggh4rfhk
- Chrome: https://decentsecurity.com/ublock-for-google-chrome-deployment/
- Firefox: https://decentsecurity.com/ublock-for-firefox-deployment/