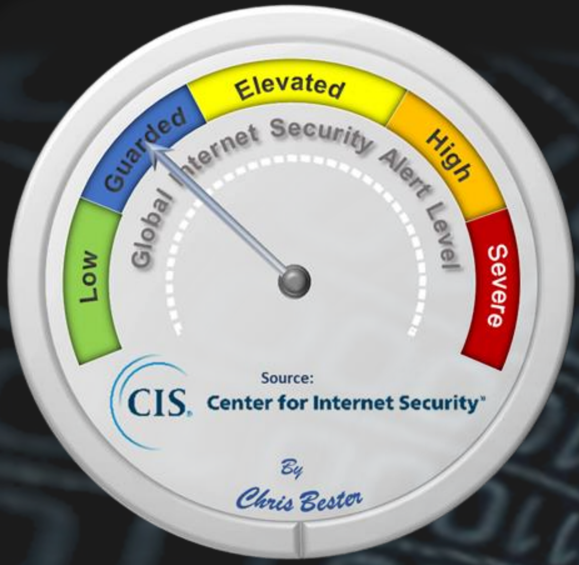

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On October 3, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in LibreOffice, Apple, vBulletin, PHP, Exim, and Google products.

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

04 October 2019

In The News This Week

US, UK and Australia urge Facebook to create backdoor access to encrypted messages

Facebook says it opposes calls for backdoors that would 'undermine the privacy and security of people everywhere' - The United States, United Kingdom and Australia plan to pressure Facebook to create a backdoor into its encrypted messaging apps that would allow governments to access the content of private communications, according to an open letter from top government officials to Mark Zuckerberg obtained by the Guardian. The open letter, dated 4 October, is jointly signed by the UK home secretary, Priti Patel; the US attorney general, William Barr; the US acting secretary of homeland security, Kevin McAleenan; and the Australian minister for home affairs, Peter Dutton, and is expected to be released Friday. It will call on Facebook not to "proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens".

(Remember what I said about Signal last week) Read the full article by Julia Carrie Wong here: The Guardian

Update now: WhatsApp bug allows malicious GIF to steal user data

A newly discovered vulnerability in popular Facebook Inc.-owned messaging service WhatsApp allows an attacker to obtain access and steal data by doing nothing more than sending a malicious GIF to a user. The vulnerability was discovered and publicized Wednesday by a security researcher who goes by the name of Awakened on GitHub. Described as a "double-free bug," it causes the same memory address on a device to be called twice, causing the memory allocation within the app to open the vulnerability. The technical specifications behind the exploit are complicated, but exploiting it is not. A malicious GIF file is initially sent to a user. When the user opens the WhatsApp gallery to send an image with any other message, the malicious GIF triggers the bug. It then opens a remote shell in the app, making the device and its contents open to exploitation. Users are naturally being encouraged to make sure they are running the latest version of WhatsApp to avoid exposing themselves to the vulnerability.

Adapted from an articled by Duncan Riley which you can find here: siliconAngle

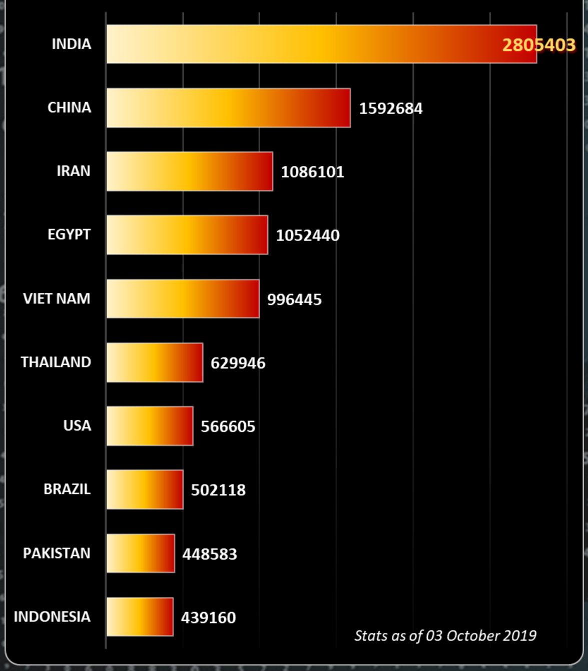
Microsoft bans another 38 file extensions in Outlook for the Web

Microsoft plans to expand the list of file extensions that are banned in Outlook for the web (previously known as Outlook Web Access (OWA)). The list, which previously included 104 file extensions, will be expanded "soon" with 38 new entries. These new entries are file types that are regularly used to deliver malware to Outlook inboxes. Once added to the list of blocked file extensions, users won't be able to download any of these types of files from their inboxes -- unless the Outlook/Exchange administrator has whitelisted a particular file extension on purpose, using a special config. "The newly blocked file types are rarely used, so most organizations will not be affected by the change," the Microsoft Exchange team said in an announcement on Thursday 3 Oct 2019. The 38 new file extensions that will soon be banned in Outlook for the web include: (1) Java files: ".jar", ".jnlp" - (2) Python files: ".py", ".pyc", ".pyo", ".pyw", ".pyz", ".pyzw" - (3) PowerShell files: ".ps1", ".ps1xml", ".ps2", ".ps2xml", ".psc1", ".psc2", ".psd1", ".psdm1", ".psd1", ".psdm1" – (4) Digital certificates: ".cer", ".crt", ".der" – (5) Files used to exploit vulnerabilities in third-party software: ".appcontent-ms", ".settingcontent-ms", ".cnt", ".hpj", ".website", ".webpnp", ".mcf", ".printerexport", ".pl", ".theme", ".vbp", ".xbap", ".xll", ".xnk", ".msu", ".diagcab", ".grp". The list of 104 file types that Microsoft is currently blocking in Outlook for the web is available here.

Read the full article by Julia Catalin Cimpanu here: ZDNet Article

Worst Botnet Countries by number of Bots

Source: https://www.spamhaus.org/statistics/botnet-cc/



Stats as of 03 October 2019

For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

According to Cyber Defence Magazine, 43% of cyber-attacks are targeted at small businesses, 91% of attacks launch with a phishing email and 38% of malicious attachments are masked as one Microsoft Office type of file or another

Protection and Security in Excel

As many of us are using Excel on a daily basis for various work and personal reasons, the question of security often cross my desk and I therefore decided to give some pointers to our readers. Below is an adaption from a Microsoft article I found published here that explains it nicely.

"Excel gives you the ability to protect your work, whether it's to prevent someone from opening a workbook without a password, granting Read-Only access to a workbook, or even just protecting a worksheet so you don't inadvertently delete any formulas. In this topic we'll discuss the various ways you can utilize the primary options to protect and distribute your Excel files.

A word of caution before we start: **(1) If you forget or lose your password, Microsoft can't retrieve it for you. (2) You should not assume that just because you protect a workbook or worksheet with a password that it is secure - you should always think twice before distributing Excel workbooks that could contain sensitive personal information like credit card numbers, Social Security Number, employee identification, to name a few. (3) Worksheet level protection is not intended as a security feature. It simply prevents users from modifying locked cells within the worksheet.**

Following are the different options available for protecting your Excel data:

- File-level: This refers to the ability to lock down your Excel file by specifying a password so that users can't open or modify it. You have two choices here:
  - ≈ File encryption: When you choose this option, you specify a password and lock the Excel file. This prevents other users from opening the file. For more information, see Protect an Excel file.
  - ≈ Setting a password to open or modify a file: You specify a password to open or modify a file. Use this option when you need to give Read-only or edit access to different users. For more information, see Protect an Excel file.
  - ≈ Mark as Final: Use this option if you want to mark your Excel file as the final version and want to prevent any further changes by other users. For more information, see Add or remove protection in your document, workbook, or presentation.
  - ≈ Restrict Access: If your organization has permissions set up using Information Rights Management (IRM), you can apply any of the available IRM permissions to your document. For more information, see Add or remove protection in your document, workbook, or presentation.
  - ≈ Digital signature: You can add digital signatures to your Excel file. For more information, see Add or remove a digital signature in Office files.

    Note: To add a digital signature, you need a valid certificate from a certificate authority (CA).
- Workbook-level: You can lock the structure of your workbook by specifying a password. Locking the workbook structure prevents other users from adding, moving, deleting, hiding, and renaming worksheets. For more information on protecting workbooks, see Protect a workbook.
- Worksheet-level: With sheet protection, you can control how a user can work within worksheets. You can specify what exactly a user can do within a sheet, thereby making sure that none of the important data in your worksheet are affected. For example, you might want a user to only add rows and columns, or only sort and use AutoFilter. Once sheet protection is enabled, you can protect other elements such as cells, ranges, formulas, and ActiveX or Form controls. For more information on protecting worksheets, see Protect a worksheet.

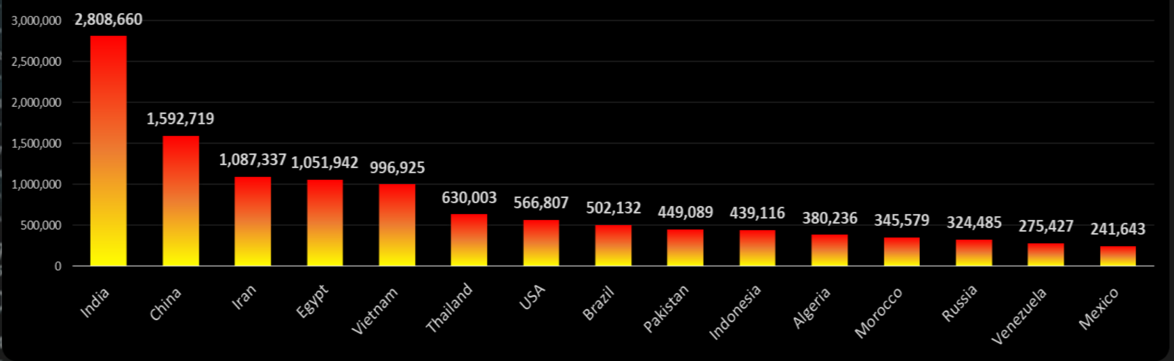
Which level of protection should I use?

- To control the level of access users should have to an Excel file, use file-level protection. Let's say you have a weekly status report of your team members in an Excel file. You don't want anyone outside your team to be even able to open the file. There are two options available:
  - ≈ If you don't want others to open your file: You can encrypt the Excel file, which is the most common technique used. This basically means you lock it with a password and nobody except you can open it.
  - ≈ If you want to enable Read-only or editing access to different users: Maybe, you want the managers in your team to be able to edit the weekly status report, but team members should only have Read-only access. You can protect the Excel file by specifying two passwords: one to open, and the other to modify. You can later share the appropriate passwords with the team depending on the access they should be given.
- To control how users should work with worksheets inside your workbook's structure, use workbook-level protection. Let's say your status report workbook has multiple worksheets, and each worksheet is named after a team member. You want to make sure each team member can add data to their own worksheet, but not be able to modify any of the worksheets in the workbook, whether it be adding a new worksheet, or moving worksheets around within the workbook.
- To control how users should work within an individual worksheet, use worksheet-level protection. Let's say each worksheet in your status report workbook contains data that is common to all worksheets, like header rows or a specific report layout, and you really don't want anyone to change it. By protecting your worksheet, you can specify that users can only perform specific functions in a sheet. For example, you can give users the ability to enter data, but keep them from deleting rows or columns, or only insert hyperlinks or sort data.

You can use one or more levels of protection for your Excel data depending on your/your organization's needs. You can choose to use all of the available options or a combination of options—it's completely up to the level of security you want for your Excel data. For example, you may choose to encrypt a shared Excel file, as well as enable workbook and worksheet protection, while only using worksheet protection on a personal workbook just so you don't accidentally delete any formulas."

Composite Blocking List (CBL) - Number of Infections - Top 15 Countries

(Last 10 Days) Source: https://www.abuseat.org/public/countryinfections.html



Author: Chris Bester
chris.bester@yahoo.com