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

On March 7, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe and Google products. On the 20th of March an advisory came out for vulnerabilities in Mozilla Firefox

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

22 March 2019

In The News This Week

Norsk Hydro Cyber Attack

Norwegian aluminium producer Norsk Hydro ASA was hit by ransomware-wielding attackers early this week. The company lost no time in reacting and responding to the attack – they notified the authorities, called in experts to help, and (very laudably) committed to keeping the public informed. In the latest official update on the situation, the company shared that: (1) With the help of experts from Microsoft and other IT security partners, they are working on reverting virus infected systems back to a pre-infected state and on systematically restoring business critical IT-based functions. (2) There have been no reported safety incidents as a result of the cyber-attack, and most operations are running either as normal or close to it, with the exception of Extruded Solutions, which is currently running at approximately 50 percent of normal capacity. "Progress has been made, with restart of some plants as well as utilizing stock to keep delivering to customers," they reassured. (3) The Norway's National Investigation Service (Kripos) has opened an investigation. (4) They still don't know how long it might take to restore stable IT operations.

The company has yet to name the ransomware that hit them, but the Norwegian National Security Authority says it's LockerGoga. It's ultimate destructiveness depends on the version. "All available information at present suggests the Norsk Hydro event used a type of malware incapable of spreading on its own. Instead, similar to the Ryuk events in 2018, the adversary needed to penetrate the network and establish an alternate means of seeding it with ransomware to deliver an impact," Joe Slowik, Principal Adversary Hunter at Dragos, told Help Net Security.

"As best we can tell now, it appears the adversary likely compromised Active Directory at Norsk to use legitimate means to spread the ransomware widely and quickly. As a result, this event requires more adversary interaction and dedication than self-propagating worms such as WannaCry and NotPetya, and appears more targeted in nature. Finally, no samples of the ransomware indicate use or exploitation of vulnerabilities, so precise Windows versions and patching appears irrelevant in this case."

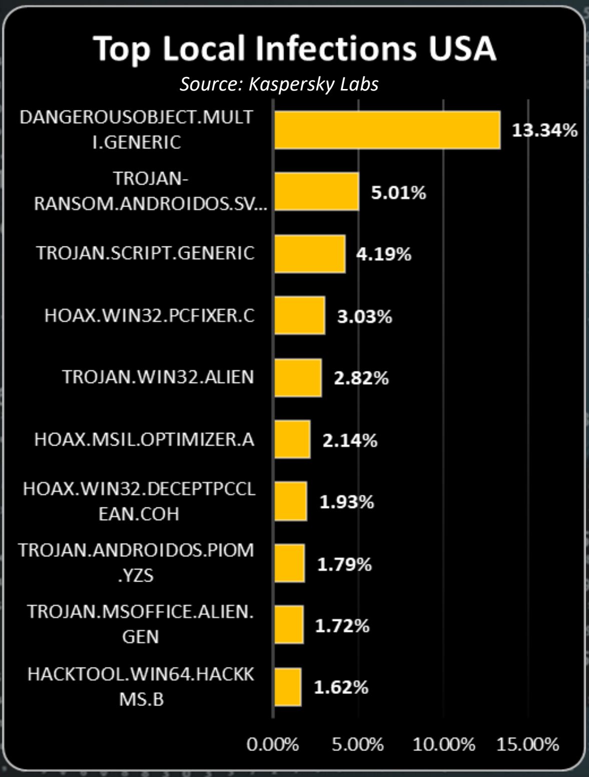
The company confirmed that no ransom has been paid to the attackers and that they have cyber insurance. Read the full story by Zeljka Zorz here: https://www.helpnetsecurity.com/

The privacy risks of pre-installed software on Android devices

Many pre-installed apps facilitate access to privileged data and resources, without the average user being aware of their presence or being able to uninstall them. Many pre-installed apps facilitate access to privileged data and resources, without the average user being aware of their presence or being able to uninstall them. On the one hand, the permission model on the Android operating system and its apps allow a large number of actors to track and obtain personal user information. At the same time, it reveals that the end user is not aware of these actors in the Android terminals or of the implications that this practice could have on their privacy. Furthermore, the presence of this privileged software in the system makes it difficult to eliminate it if one is not an expert user. These are the results of a study carried out by Universidad Carlos III de Madrid (UC3M) and the IMDEA Networks Institute, in collaboration with the International Computer Science Institute (ICSI) at Berkeley (USA) and Stony Brook University of New York (USA). The study encompasses 82,000 pre-installed apps in more than 1,700 devices manufactured by 214 brands, revealing the existence of a complex ecosystem of manufacturers, mobile operators, app developers and providers, with a wide network of relationships between them. This includes specialized organizations in user monitoring and tracking and in providing Internet advertising. - These results are detailed out in an article that will be made public on the 1st of April 2019. Get more details here: https://www.helpnetsecurity.com/

Top Local Infections USA

Source: Kaspersky Labs



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

Cybersecurity Ventures Reports:

The World Wide Web was invented in 1989.

The first-ever website went live in 1991.

Today there are more than **1.9 billion** websites.

Where does that pesty Phishing/SPAM mail come from?

You open your private mailbox in the morning and you see this mail telling you your account is about to expire or you won this marvellous holiday or there is a new voicemail waiting for you, and so on. And when you open it and you see the sender address is from this weird company or person you never heard of or worse, you recognise the sender address and it is strange because this person will never send you something like this? And if you hover your mouse curser over the "Click Here" link, you see this strange unusually short URL address or an overly complex loooong URL. Well we all had some of these and anyone with two brain cells will recognise it as a Scam, a Phish or a SPAM and wish we can report it somewhere? Corporate emails are usually taken care of by the local IT or security department.

How to analyse Email Header information

Today we will look at how you can analyse the email header and how to trace the originating IP address. But, before you start to delft into this though, make sure your anti-virus solution is up-to-date and active just in case you open a mail that carries a malicious payload that can infect your computer. (If you don't have an anti-virus solution running, there are many solutions you can download that comes with a free licence for home users, such as Windows Defender, AVG, Avast, etc.)

Where do I get the Email Header Information

First, where do you get the header information? If you are using Microsoft Outlook, open the mail in question. Now navigate to the top left of the open window and select "File" then select "Properties" which will be towards the bottom in the column in the right. This will open a pop-up window where you will see "Internet Headers" towards the bottom. Now select and copy the entire contents of the Internet Headers box.

Now to analyse this information, you need to open a message analyser which you will find freely available on the internet. I usually use the Microsoft analyser that you will find here https://testconnectivity.microsoft.com/ . Select "Message Analyser" and paste the content you just copied into the message box and click "Analyse Headers". (Other analysers I sometimes use can be found here: https://mxtoolbox.com/EmailHeaders.aspx or https://www.iptrackeronline.com/email-header-analysis.php)

What information do I get?

The analysis will provide you with a myriad of useful and, for the no-propeller heads, useless information. For the purpose of today's insight, we want to look at the originating IP address. Once the IP address is established you can trace it using various online tools. The one I frequently use is https://www.robtex.com/ which will give you a ton of information. Others, like https://ipinfo.io/ and many more are available if you use your preferred search engine to look for it.

Is the IP address blacklisted or linked to fraudulent activities?

You can also check if the IP address is blacklisted or linked to fraud scams or ransomware sites. Some popular links to use: http://www.ipvoid.com/ , https://ransomwaretracker.abuse.ch/tracker/ , https://www.virustotal.com/

Now that you have a taste of what you can do with the email header information, let's look at places you can report Phishing emails or Scams, etc. If the scam is bank related, most internet banking sites will provide a link where you can report a scam or phishing email that mimics the bank's credentials. Most large businesses will have special divisions set up to deal with reported scams and will have information available on their website. You can also go to the sites to report Cyber Crimes listed elsewhere in this bulletin.

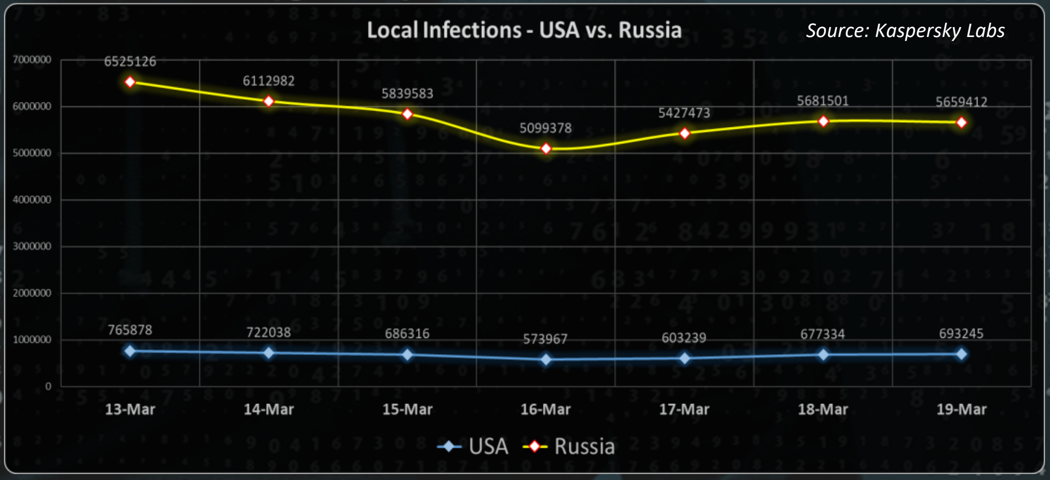
Lastly, you can also blacklist email addresses on your local Outlook account, just right-click on the unopened mail and select "Junk" then "Block Sender" and you won't see any mail from that sender again 😊

Email Header Information in other popular mail apps

How to get header information in other popular mail apps - For G-Mail, select the More option (downward-pointed arrowhead " ▾ ") next to the Reply button in the top right corner, then select "Show original". For Yahoo Mail, select the More option (three dots "…" next to the Spam button in the top banner, then select "View raw message".

Local Infections - USA vs. Russia

Source: Kaspersky Labs



Author: Chris Bester