On December 26, 2018, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). Due to a vulnerability in Microsoft Internet Explorer, which could allow for arbitrary code execution.

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
28 December 2018

2018 CYBER BREACHES IN REVIEW

BIGGEST INTERNATIONAL CYBER SECURITY BREACHES 2018

Facebook: Facebook admitted that around 50 million users were compromised by the security breach. As per Facebook CEO, the company has not seen the accounts getting compromised nor found any inappropriate activity. Later, Zuckerberg confirmed that the attackers used Facebook developer APIs for getting information. The information was comprised of names, genders, localities which were linked with any user's profile page.

FIFA: Football Leaks organisation leaked around 3.4 terabytes of data and 70 million documents which possessed a good number of corruption allegations. They got leaked to a newspaper in German magazine Der Spiegel. These 3.4 terabytes breach managed to overshadow the 2.6 terabyte Panama Papers, which is known as "the biggest whistle-blower leak in history" and the biggest mystery revealed and ever reported by investigative journalists.

Google+ : At the beginning of 2018, Google identified a vulnerability in an API. It noticed an API for Google's social networking effort Google+ gave third-party app developers the access to data from the friends of the app users.

Uber: Even though, Uber had already faced allegations and was infamous for compromising user data back in 2016. They even paid £133m to settle the legal penalisation owing to the cyber-attack which happened to expose 57 million customers and driver data. Uber, the ride-hailing company, also tried to keep it concealed, however, following the numerous allegations from the public, they did make that public in a smart manner though. In November 2017, they released the information saying that Uber paid $100,000 (£761, 71) to hackers for deleting the acquired data from their systems.

British Airways: This year, British Airways also had to face the cybersecurity breach which affected around 380,000 transactions. This catered the stolen personal and financial data, nevertheless, the passport and flight details were safe. The data remained unsafe and insecure for 2 weeks during the period of 21st August to 5th September when the company's website and apps were under a "sophisticated" attack.

T-Mobile: Around 2 million T-Mobile customers who were based in the US had their account details breached in which their names, email IDs, account numbers, billing details and encrypted passwords. Their UK based acquired remained unaffected though, as per their statement to The Registrar.

And many more.....

Main Source: https://www.itproportal.com/

Know your Malware – Bedep.Botnet

Bedep is a trojan that opens a backdoor on a compromised system and can provide a malicious actor with full control over the system, as well as download additional malware. Once executed, Bedep can facilitate the theft of information or be used to perform click fraud to visit specific websites for financial gain. According to TrendMicro, the Bedep trojan is also used to turn infected systems into **botnets** for other malicious activities. Users are typically infected with Bedep through exposure to malvertising or exploit kits on compromised websites. According to F-Secure, Bedep creates a hidden virtual desktop on the victim's computer, with an instance of Internet Explorer which is used to view unsolicited websites.
First reported in February 2015

Warning Signs that Your Computer is Malware-Infected

Here's one of the scenarios you may not like, but it could happen every day because it's always virus season for computers. You're working on an important project and suddenly you start seeing annoying pop-ups displayed on your computer. Also, it takes too long for your files or computer apps to load. You wait and wait until you start asking yourself: **"Does my computer have a virus?"**
Unfortunately, the answer might be "yes" and your PC could be already compromised with viruses or next-gen malware that are slowing down its activity and performance.
This is one of the many warning signs that show your PC might suffer from a malware infection. There are more of them you need to be aware of and understand, so you can quickly take action.
In this article, we'll show you the most frequent warning signs of malware infection and what can you do about it.

Use these quick links to easily navigate and see some of the most common warning signs displayed on a computer:

1. **Your computer is slowing down** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario1)
2. **Annoying adds are displayed** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario2)
3. **Crashes** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario3)
4. **Pop-up messages** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario4)
5. **Internet traffic suspiciously increases** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario5)
6. **Your browser homepage changed without your input** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario6)
7. **Unusual messages show unexpectedly.** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario7)
8. **Your security solution is disabled** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario8)
9. **Your friends say they receive strange messages from you** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario9)
10. **Unfamiliar icons are displayed on your desktop** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario10)
11. **Unusual error messages** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario11)
12. **You can't access the Control Panel** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario12)
13. **Everything seems to work perfectly on your PC** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario13)
14. **You get the error on the browser** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario14)
15. **You get suspicious shortcut files** (https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/#scenario15)

(Adapted from a Blog by Ioana Rijnetu published by Heimdal Security) - Find the BLOG here: https://heimdalsecurity.com/blog/warning-signs-operating-system-infected-malware/

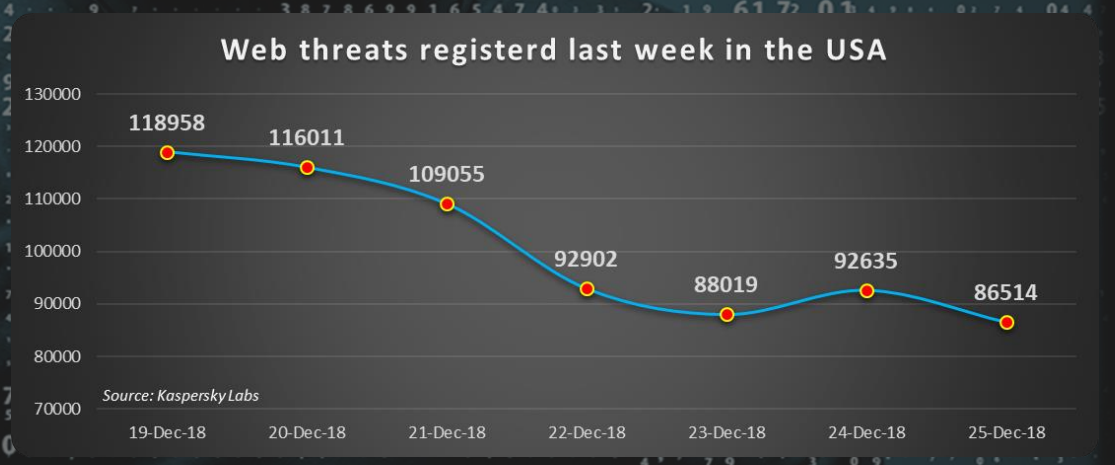
TOP Web threats registered for last week in the USA

#	KNOWN AS	(%)
1	Trojan.Script.Generic	36.92%
2	Trojan.Script.Miner.gen	22.27%
3	Trojan.PDF.Badur.gen	10.06%
4	Trojan.Script.Agent.gen	5.90%
5	Hoax.HTML.FraudLoad.m	3.45%
6	Trojan-Downloader.JS.Inor.a	3.41%
7	Trojan.Win32.Staser.awvm	2.93%
8	DangerousObject.Multi.Generic	2.48%
9	Trojan-Clicker.HTML.Iframe.dg	2.40%
10	HackTool.Win32.Patcher.adn	1.01%

Source: Kaspersky Labs

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

CPO Magazine reported that by
2021
Damage related to Cybercrime is projected to hit
$6 Trillion



Author: Chris Bester