
**On January 6, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Zyxel, Google and Fortinet products.**

Covid-19 Global Stats

| Date | Confirmed Cases | Deaths |
|---|---|---|
| 07-Jan | 88,499,863 | 1,906,693 |

## 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

## 08 January 2021

## In The News This Week

**Users will be blocked from using WhatsApp unless they agree to Facebook privacy changes** - Messaging service WhatsApp has updated its terms and conditions section to include further Facebook integration – including a requirement that app users share data with the company. In an in-app message sent to users this week, WhatsApp said that the changes will include: Updates to WhatsApp's service and how it processes your data; How businesses can use Facebook hosted services to store and manage their WhatsApp chats; and How WhatsApp will partner with Facebook to offer integrations across Facebook Company products. WhatsApp said that these changes will officially come into effect from **8 February**. After this date, any user which has not agreed to the new terms will no longer be able to use the messaging service. ArsTechnica reports that some of the data that WhatsApp collects includes: User phone numbers; Other people's phone numbers stored in address books; Profile names; Profile pictures; Status message including when a user was last online and Diagnostic data collected from app logs. Under the new terms, Facebook reserves the right to share collected data with its family of companies…. Read the full story here: BusinessTech

**Microsoft Source Code Exposed: What We Know & What It Means**

Microsoft confirmed last week that attackers were able to view some of its source code, which it found during an ongoing investigation of the SolarWinds breach. While its threat-modelling approach mitigates the risk of viewing code, many questions remain that could determine the severity of this attack. In a blog post published on Dec. 31, 2020, officials said Microsoft has not found evidence of access to production services or customer data, nor has it discovered that its systems were used to attack other companies. The company has not found indications of common tactics, techniques, and procedures (TTPs) linked to abuse of forged SAML tokens against its corporate domains. It did find an internal account had been used to view source code in "a number of code repositories," according to the blog post, from the Microsoft Security Response Center (MSRC). This activity was unearthed when investigators noticed unusual activity with a small number of internal accounts, the post explains, and the affected account didn't have permissions to change any code or engineering systems. The accounts were investigated and remediated, officials noted. Read the full story here: DarkReading

**British Court Rejects U.S. Request to Extradite WikiLeaks' Julian Assange**

A British court has rejected the U.S. government's request to extradite Wikileaks founder Julian Assange to the country on charges pertaining to illegally obtaining and sharing classified material related to national security. In a hearing at Westminster Magistrates' Court today, Judge Vanessa Baraitser denied the extradition on the grounds that Assange is a suicide risk and extradition to the U.S. prison system would be oppressive.
"I find that the mental condition of Mr. Assange is such that it would be oppressive to extradite him to the United States of America," judge Baraitser said in a 132-page ruling. The U.S. government is expected to appeal the decision. The case against Assange center on WikiLeaks' publication of hundreds of thousands of leaked documents about the Afghanistan and Iraq wars, as well as diplomatic cables, in 2010 and 2011.
Read the full story here: TheHackerNews

**ElectroRAT Drains Cryptocurrency Wallet Funds of Thousands**

At least 6,500 cryptocurrency users have been infected by new, 'extremely intrusive' malware that's spread via trojanized macOS, Windows and Linux apps. A new remote access tool (RAT) has been discovered being used in an extensive campaign. The attack has targeted cryptocurrency users in an attempt to collect their private keys and ultimately to drain their wallets. The never-before-seen RAT at the center of the campaign, which researchers dub ElectroRAT, is written in the Go programming language and is compiled to target a number of different operating systems, including Windows, Linux and MacOS. The campaign was discovered in December 2020 – but researchers believe it initially began a year ago, and estimate that at least 6,500 victims have been infected, based on the number of unique visitors to the Pastebin pages used to locate command and control (C2) servers.
Read the full article by Lindsey O'Donnell here: ThreatPost

## SolarWinds: The more we learn, the worse it looks

ZDNet Article

While you've been distracted by the holidays, coronavirus, and politics, the more we learn about the SolarWinds security fiasco, the worse it looks.

In March of 2020, Americans began to realize that the coronavirus was deadly and going to be a real problem. What no Americans knew then was that at about the same time, the Russian government's hack of SolarWinds's proprietary software Orion network monitoring program was destroying the security of top American government agencies and tech companies. There were no explosions, no deaths, but it was the Pearl Harbor of American IT.

Russia, we now know, used SolarWinds' hacked program to infiltrate at least 18,000 government and private networks. The data within these networks, user IDs, passwords, financial records, source code, you name it, can be presumed now to be in the hands of Russian intelligence agents. The Russians may even have the crown-jewels of Microsoft software stack: Windows and Office. In a twist, which would be hilarious if it weren't so serious, Microsoft claims it's no big deal.

That's because Microsoft has "an inner-source approach – the use of open-source software development best practices and an open-source-like culture – to make source code viewable within Microsoft." It's nice that Microsoft is admitting that the open-source approach is the right one for security -- something I and other open-source advocates have been saying for decades. But, inner source isn't the same thing as open source.

When hackers, not Microsoft developers, have access to proprietary code, the door's open for attacks. True, Microsoft's "threat models assume that attackers have knowledge of source code. So viewing source code isn't tied to elevation of risk." But, making that assumption is one thing. Dealing with reality is something else.

For decades, one of proprietary software's stupid assumptions is that "security by obscurity" works. While it can help -- no, really it can if used intelligently -- that's not the case with proprietary code. Even with the best will in the world, I doubt that Microsoft has really undertaken the hard security code review needed to lock down its proprietary code. The almost weekly revelations of new Microsoft security holes and mishaps doesn't make me feel warm and fuzzy about the security of its software.

While President Donald Trump has completely ignored the actions of Russian President Vladimir Putin's government, America's Cybersecurity Infrastructure and Security Agency (CISA) said the hacks posed a "grave risk" to US governments at all levels.

Worse was revealed. Over the Christmas season holidays, the CISA said that all US government agencies must update to Orion's 2020.2.1HF2 version by the end of the year. If they can't, they must take these systems offline. Why? Because yet another SolarWinds' Orion vulnerability was being used to install the Supernova and CosmicGale malware. This security hole, CVE-2020-10148, is an authentication bypass in the Orion API that allows attackers to execute remote code on Orion installations.

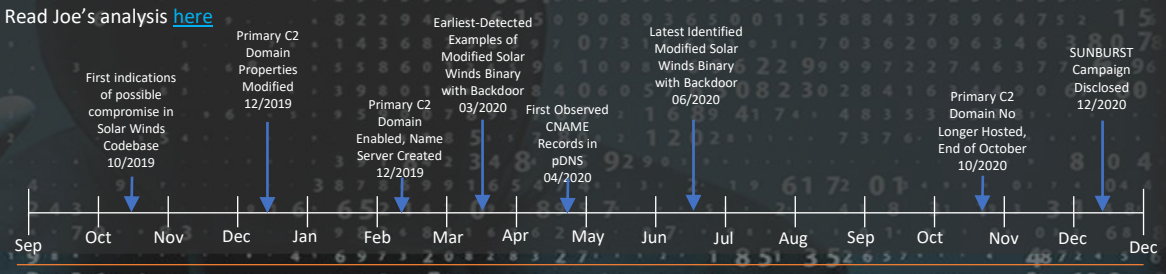
I have an even better idea than updating Orion. Dump Orion. Dump it now. And start an investigation of the SolarWinds' mediocre security record.

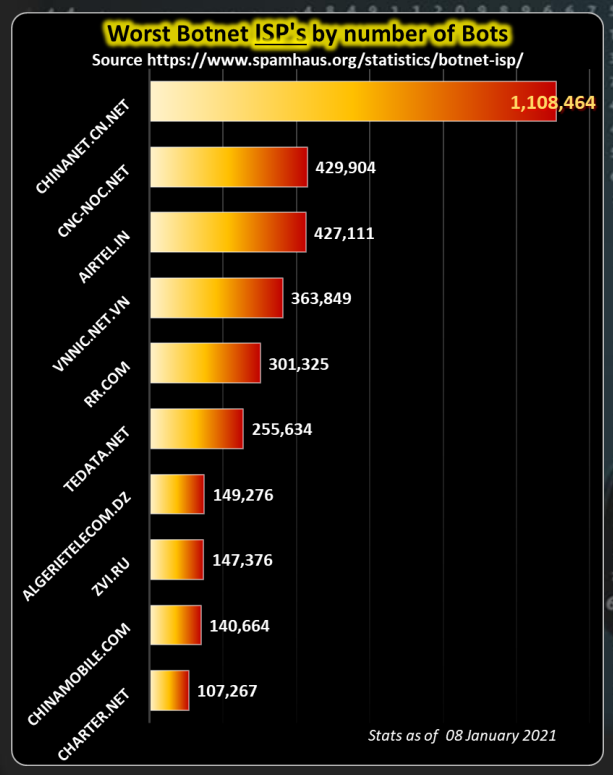
As time goes by more and more government agencies and companies have been shown to have been hacked. This includes the Department of State; Department of Homeland Security; National Institutes of Health; the Pentagon; Department of the Treasury; Department of Commerce; and the Department of Energy, including the National Nuclear Security Administration. Everyone claims that nothing too important has been revealed, but then, they would say that, wouldn't they? Sen. Mark Warner (D-Virginia), ranking member on the Senate Intelligence Committee, told the New York Times the hack looked "much, much worse" than first feared. "The size of it keeps expanding."

How much bigger will it get? We don't know. Personally, I'd assume that if my company had been using SolarWinds Orion software during 2020, I've been hacked.

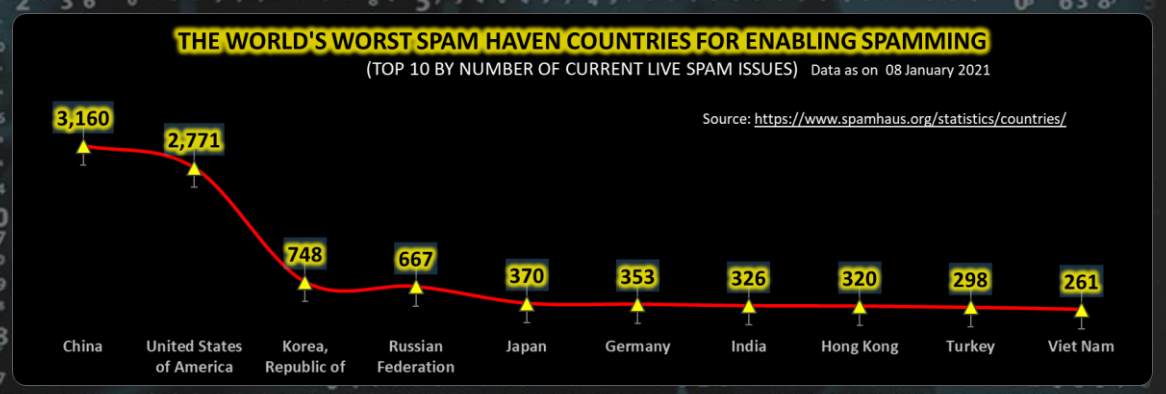
It didn't come with bombs like the attack on Pearl Harbor, but this attack on our national agencies and American Fortune 500 companies may prove to be even more damaging to our national security and our business prosperity. Now, we'll see if American developers, system administrators, and managers can rise to the occasion to rebuild their systems the way their grandparents did the country in the 1940s. Source: ZDNet

Joe Slowik of DOMAINTOOLS created the below timeline depicting the likely period of SUNBURST (aka Solarigate) activity.
Read Joe's analysis here




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


**Author: Chris Bester** (CISA,CISM)
chris.bester@yahoo.com