On January 13, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, Mozilla, PHP, Adobe, and Microsoft products.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
15-Jan	93,532,516	2,002,392

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

15 January 2021

In The News This Week

Hackers Steal Mimecast Certificate Used to Securely Connect with Microsoft 365

Mimecast said on Tuesday that "a sophisticated threat actor" had compromised a digital certificate it provided to certain customers to securely connect its products to Microsoft 365 (M365) Exchange. The discovery was made after the breach was notified by Microsoft, the London-based company said in an alert posted on its website, adding it's reached out to the impacted organizations to remediate the issue. The company didn't elaborate on what type of certificate was compromised, but Mimecast offers seven different digital certificates based on the geographical location that must be uploaded to M365 to create a server Connection in Mimecast. "Approximately 10 percent of our customers use this connection," the company said. "Of those that do, there are indications that a low single digit number of our customers' M365 tenants were targeted." Read the full story here: TheHackerNews

Sunspot, the third malware involved in the SolarWinds supply chain attack

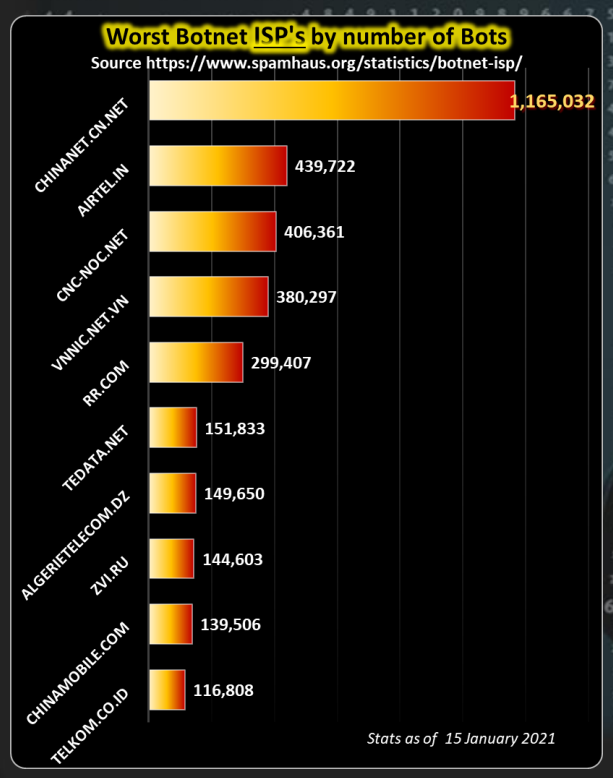
Cybersecurity firm CrowdStrike announced to have discovered a third malware strain, named Sunspot, directly involved in the SolarWinds supply chain attack. According to a new report published by the cybersecurity firm Crowdstrike, a third malware, dubbed SUNSPOT, was involved in the recently disclose SolarWinds supply chain attack. SUNSPOT was discovered after the Sunburst/Soloriqate backdoor and Teardrop malware, but chronologically it may have been the first code to be involved in the attack. At the time of the report, CrowdStrike does not attribute any of the three implants to any known threat actors. CrowdStrike tracks the threat actor behind the SolarWinds attack as StellarParticle, while FireEye and Microsoft identified it as UNC2452, and Volexity as DarkHalo. SUNSPOT is used by the attackers to insert the SUNBURST backdoor into software builds of the SolarWinds Orion IT management product. "SUNSPOT monitors running processes for those involved in compilation of the Orion product and replaces one of the source files to include the SUNBURST backdoor code." states the report published by the security firm. Read the full story here: SecurityAffairs

German police shut down DarkMarket - 'the world's largest darknet marketplace'

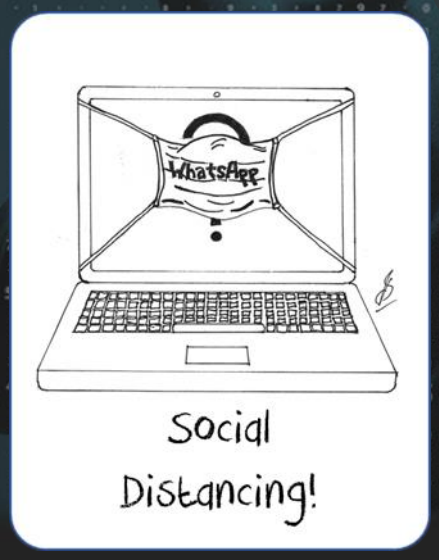
German authorities say they have taken down the 'world's largest' darknet marketplace and arrested an Australian who allegedly used it to sell drugs, stolen credit card data and other illegal goods. Police in Oldenburg shut down the DarkMarket site and turned off its server on Monday after arresting the alleged operator at the weekend, a statement said today. The marketplace offered 'all kinds of drugs' as well as 'counterfeit money, stolen and fake credit card data, anonymous SIM cards, malware and much more,' it is alleged. Calling it 'the suspected world's largest illegal marketplace on the darknet', German prosecutors said the website was brought down by a months-long international investigation involving the FBI and other foreign law enforcement. At the time of its closure, DarkMarket had nearly 500,000 users and more than 2,400 vendors. A total of at least 320,000 transactions were carried out via the marketplace, with more than 4,650 Bitcoin and 12,800 Monero - two of the most common cryptocurrencies - changing hands, prosecutors said. At current exchange rates, that represented turnover valued at €140million (£125million). A 34-year-old Australian national believed to be the DarkMarket operator was arrested near the German-Danish border, just as more than 20 servers it used in Moldova and Ukraine were seized.
Read the full story here: Daily Mail

Google reveals sophisticated Windows and Android hacking operation

The attackers used a combination of Android, Chrome, and Windows vulnerabilities, including both zero-days and n-days exploits. Google published a six-part report today detailing a sophisticated hacking operation that the company detected in early 2020 and which targeted owners of both Android and Windows devices. The attacks were carried out via two exploit servers delivering different exploit chains via watering hole attacks, Google said. "One server targeted Windows users, the other targeted Android," Project Zero, one of Google's security teams, said in the first of six blog posts. Google said that both exploit servers used Google Chrome vulnerabilities to gain an initial foothold on victim devices.
Read the full article by Catalin Cimpanu here: ZDNet



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



WhatsApp privacy debacle

ZDNet Article

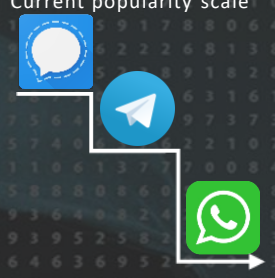
In the wake of the storm that erupted after WhatsApp's new privacy statement ultimatum, I probed the net to see what it really means and what opinions are floating around on the issue. WhatsApp posted an ultimatum that if users do not accept the new privacy policy, they will be booted off the app by 8 February 2021. The ultimatum triggered a huge outcry from the WhatsApp community prompting many to switch to alternative chat platforms. This brought about the question of exactly what data is collected by the various platforms. I found a list, compiled by Jagmeet Singh of Gatget360, that shows the scary picture of what private data WhatsApp and its owner, Facebook, are collecting. You can look at the list below and make up your own mind with what you feel comfortable with. Please read the full article here. (Some news snippets included for context)

WhatsApp Vs Signal, Telegram, Facebook Messenger: What Data Does Each App Collect?

Facebook Messenger	WhatsApp	Telegram	Signal
Purchase History	Device ID	Contact Info	**None.** (The only personal data Signal stores is your phone number, and it makes no attempt to link that to your identity.)
Other Financial Info	User ID	Contacts	
Precise Location	Advertising Data	User ID	
Coarse Location	Purchase History		
Physical Address	Coarse Location		
Email Address	Phone Number		
Name	Email Address		
Phone Number	Contacts		
Other User Contact Info	Product Interaction		
Contacts	Crash Data		
Photos or Videos	Performance Data		
Gameplay Content	Other Diagnostic Data		
Other User Content	Payment Info		
Search History	Customer Support		
Browsing History	Product Interaction		
User ID	Other User Content		
Device ID			
Product Interaction			
Advertising Data			
Other Usage Data			
Crash Data			
Performance Data			
Other Diagnostic Data			
Other Data Types			
Browsing History			
Health			
Fitness			
Payment Info			
Photos or Videos			
Audio Data			
Gameplay Content			
Customer Support			
Other User Content			
Search History			
Sensitive Info			
iMessage			
Email address			
Phone number Search history			
Device ID			

Source: https://gadgets.ndtv.com/apps/news

Current popularity scale



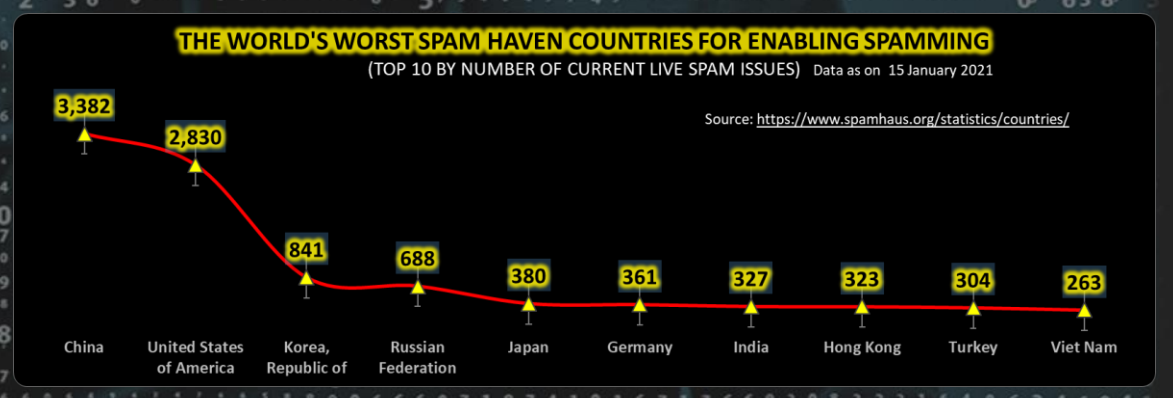
CNBC – 12 Jan 2021, Signal and Telegram downloads surge after WhatsApp says it will share data with Facebook

Signal saw approximately **7.5 million** installs globally through the Apple App Store and Google Play store between Jan. 6 and Jan. 10, according to Sensor Tower. That's 43 times the number from the previous week. It is highest week or even monthly install number for Signal in the app's history.

Meanwhile Telegram saw **5.6 million** downloads globally from Wednesday through Sunday, according to Apptopia.

The Verge - Signal sees surge in new signups after boost from Elon Musk
Encrypted messaging app Signal says it's seeing a swell of new users signing up for the platform, so much so that the company is seeing delays in phone number verifications of new accounts across multiple cell providers.

Business Insider – Signal's downloads skyrocketed 4,200%
Signal saw 7.5 million downloads last week, a 4,200% increase on the previous week. Telegram saw 9 million downloads, a 91% increase. India was the biggest source of downloads for both.



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