On May 12, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). Multiple Vulnerabilities in Wi-Fi Enabled Devices Could Allow for Data Exfiltration MS-ISAC ADVISORY NUMBER: 2021-068

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
14-May	161,824,992	3,358,520

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

14 May 2021

In The News This Week

HSE shuts down IT systems amid significant cyber attack

There has been "a significant ransomware attack" on the Health Service Executive's (HSE) IT systems. The HSE said it has taken the "precaution" of shutting down all its IT systems in order to "protect them from this attack and to allow us fully assess the situation with our own security partners". As a result there are expected to be cancellations and disruption to some services at a number of hospitals with further clarification expected in the coming hours. Read the full story by Vivienne Clarke here: The Irish Times

Nearly All Wi-Fi Devices Are Vulnerable to New FragAttacks

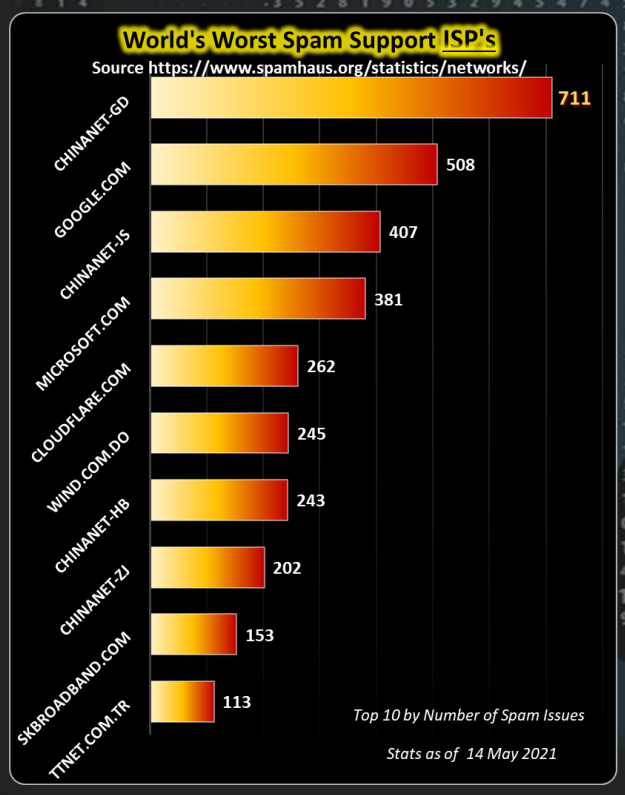
Three design and multiple implementation flaws have been disclosed in IEEE 802.11 technical standard that undergirds Wi-Fi, potentially enabling an adversary to take control over a system and plunder confidential data. Called FragAttacks (short for FRagmentation and AGgregation attacks), the weaknesses impact all Wi-Fi security protocols, from Wired Equivalent Privacy (WEP) all the way to Wi-Fi Protected Access 3 (WPA3), thus virtually putting almost every wireless-enabled device at risk of attack. "An adversary that is within radio range of a victim can abuse these vulnerabilities to steal user information or attack devices," Mathy Vanhoef, a security academic at New York University Abu Dhabi, said. "Experiments indicate that every Wi-Fi product is affected by at least one vulnerability and that most products are affected by several vulnerabilities. IEEE 802.11 provides the basis for all modern devices using the Wi-Fi family of network protocols, allowing laptops, tablets, printers, smartphones, smart speakers, and other devices to communicate with each other and access the Internet via a wireless router. Read the full story by Ravie Lakshmanan here: The Hacker News

80% of Net Neutrality Comments to FCC Were Fudged

NY's AG: Millions of fake comments – in favor and against – came from a secret broadband-funded campaign or from a 19-year-old's fake identities - Broadband providers and a 19-year-old college student were among those who successfully hijacked public comments during a crucial decision-making process in 2017 to overturn net neutrality by flooding the Federal Communications Commission (FCC) with fraudulent comments indicating their position on the move, according to a new report. A secret campaign by the broadband industry to offer support to roll back net neutrality resulted in fake comments comprising more than 40 percent of those sent to the FCC during the public comments phase of its decision, according to the report by the New York State Office of the Attorney General. The industry also sent more than half a million fake letters to Congress to "create the appearance of widespread grassroots opposition to existing net neutrality rules, which as described in an internal campaign planning document would help provide 'cover' for the FCC's proposed repeal," according to the report "Fake Comments: How U.S. Companies and Partisans Hack Democracy to Undermine Your Voice", published online Thursday the 6th of May.. Read the rest of the story by Elizabeth Montalbano here: ThreatPost

South Africa threatens litigation over new WhatsApp privacy policy

South Africa's newly established Information Regulator is consulting lawyers about Facebook-owned WhatsApp's new privacy policy and warned it is considering litigation. Users of the popular instant messaging app have until 15 May to accept WhatsApp's new privacy policy or face the possibility of having their experienced degraded until the app becomes unusable or they accept the new terms. Facebook had planned to introduce the new privacy policy earlier this year but pushed its implementation out to May after a global backlash from users that prompted many to download alternative apps such as Signal and Telegram. The Information Regulator has now stepped in and demanded that Facebook offer South African users the same terms and conditions being offered to users in the European Union. "The Information Regulator has, after correspondence, written to WhatsApp and requested it to revise the privacy policy for South Africa to the standard used in the EU," it said in a statement on Friday. "The regulator has received no agreement from WhatsApp. Under the circumstances, the regulator is briefing attorneys to prepare an opinion on the way forward in terms of litigation."
Read the article by Duncan McLeod here: TechCentral



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

Wi-Fi and FragAttacks Explained

With the breaking news this week on millions of Wi-Fi devices that are vulnerable to attack, I had some questions on how does it really affect the broader populace out there. What does it mean for the layman on the street?
Most of us know about Wi-Fi and we generally need it if we want to connect our phones to the internet without using data from the data bundle on the phone or tablet, or to connect a laptop to the printer, etc. Now, for the not-so-technically minded, let's explore what Wi-Fi is and then how FragAttacks work..

What is Wi-Fi?

Although Wi-Fi is typically used to access the internet on portable devices like smartphones, tablets, or laptops, in actuality, Wi-Fi itself is used to connect to a router or other access point, which in turn provides internet access. Wi-Fi is a wireless connection to that device, not the internet itself. It also provides access to a local network of connected devices, which is why you can print pictures wirelessly or look at a video feed from Wi-Fi connected cameras with no need to be physically connected to them. Instead of using wired connections like Ethernet, Wi-Fi uses radio waves to transmit information at specific frequencies, most typically at 2.4GHz and 5GHz. Each frequency range has several channels that wireless devices can operate on, helping to spread the load so that individual devices don't see their signals crowded or interrupted by other traffic — although that does happen on busy networks.
The typical range of a standard Wi-Fi network can reach up to 100 meters in the open air. Buildings and other materials reflect the signal, however, making most Wi-Fi networks far narrower than that. Typically, ranges of 10-35 meters are more common. The strength of the antenna and the frequency broadcast can also impact the effective range of the network. Higher frequencies like 5GHz and 60GHz have far shorter effective ranges than 2.4GHz. These frequencies are considerably higher than the frequencies used for cell phones, walkie-talkies and televisions. The higher frequency allows the signal to carry more data. To be able to operate at any one of these frequencies however, it needs to transmit and receive using a set of communication rules or standards called protocols. These are industry standards set by the Institute of Electrical and Electronics Engineers (IEEE), and are used by manufacturers to ensure that their devices will be able to communicate with Wi-Fi devices made by someone else.

The most common Protocols

802.11a transmits at 5 GHz and can move up to 54 megabits of data per second. It uses a more efficient coding technique (OFDM) that splits the radio signal into several sub-signals before they reach a receiver. This greatly reduces interference.
802.11b is the slowest and least expensive standard. For a while, its cost made it popular, but now it's becoming less common as faster standards become less expensive. 802.11b transmits in the 2.4 GHz frequency band of the radio spectrum and can handle up to 11 megabits of data per second. This is still the most common default setting on most routers today.
802.11g transmits at 2.4 GHz like 802.11b, but it's a lot faster -- it can handle up to 54 megabits of data per second. 802.11g is faster because it uses the same OFDM coding as 802.11a.
802.11n is the most widely available of the standards and is backward compatible with a, b and g above. It significantly improved speed and range over its predecessors. This standard reportedly can achieve speeds as high as 140 megabits per second and can transmit up to four streams of data, each at a maximum of 150 megabits per second. Most routers however only allow for two or three streams.
802.11ac is the newest standard but is not widely adopted yet. 802.11ac is backward compatible with 802.11n and the other older ones, with "n" on the 2.4 GHz band and "ac" on the 5 GHz band. It is less prone to interference and far faster than its predecessors, pushing a maximum of 450 megabits per second on a single stream. It allows for transmission on multiple spatial streams, up to eight, optionally.

Everyone within a network's range and a compatible Wi-Fi device can detect the network and attempt to connect to it. That's what allows it to operate in private and public settings, but it does raise security concerns. That's why security standards/protocols like WPA, WPA2, and WPA3 exist and why it's essential to change your password if you think someone's accessing your network without permission. Another antidote is to set your router to prevent your Wi-Fi network to broadcast its presence, thus making it a hidden network that you can only connect to if you know about it.

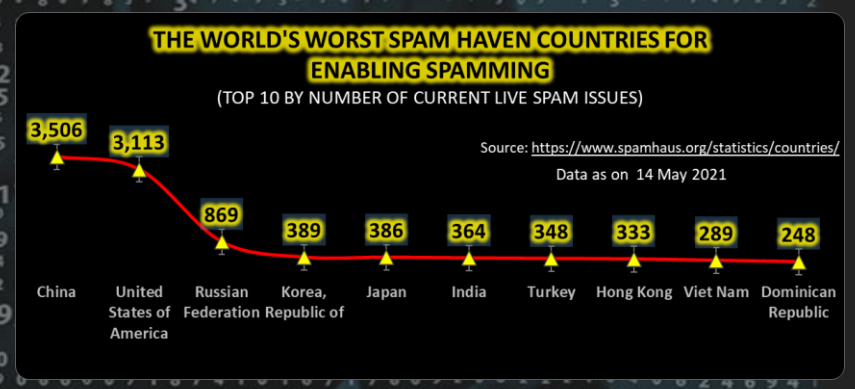
FragAttacks (fragmentation and aggregation attacks)

It was announced in the media this week that most Wi-Fi devices are vulnerable to a flaw discovered by Mathy Vanhoef, a Belgian security researcher. He said that 3 of the vulnerabilities discovered are actual design flaws in the Wi-Fi standard and therefore "affect most devices." The discovered vulnerabilities affect all modern security protocols of Wi-Fi, including the latest WPA3 specification. Even the original security protocol of Wi-Fi, called WEP, is affected. He lists the 3 design flaws as follows: (1) aggregation attack, (2) mixed key attack, (3) fragment cache attack. On top of this, several other vulnerabilities were discovered that are caused by widespread **programming mistakes** in Wi-Fi products. Unfortunately I will not be able to go into the technical details of the attack in this bulletin as I'm running out of space, but please see Vanhoef's website for a detailed explanation.

What we want to know though is how vulnerable are we and how easy is it to exploit these vulnerabilities? The first thing to remember, is that a would be attacker has to be in range to gain access to your Wi-Fi network (less than 100 meters). Secondly, the design flaws are hard to abuse because doing so requires user interaction. The biggest concern according to Vanhoef are the programming mistakes in Wi-Fi products since several of them are trivial to exploit. Most manufacturers have updates available already, so please check in on the manufacturer's websites for update details and instructions and apply these to ensure your Wi-Fi equipment is safe. References: Digitaltrends, HowStuffWorks, FragAttacks, ThreatPost

Other Interesting News and Cyber Security bits:

- Heimdal AI Discovers a Complex Phishing Cryptocurrency Scam Campaign
- DarkSide ransomware explained: How it works and who is behind it
- US fuel pipeline 'paid hackers $5m in ransom'.



Thanks to my friend Graeme Cartwright for his news contributions this week

AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com