On February 16, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in SAP, Apple, and Google products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
18 Feb 22	420,761,622	5,883,766

Deaths this week: 74,296

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
18 February 2022

In The News This Week

Ukraine accuses Russia of cyber-attack on two banks and its defence ministry

Ukraine accused Russia on Wednesday of being behind a cyber-attack that targeted two banks and its defence ministry, which the country's deputy prime minister said was the largest of its type ever seen. The Kremlin denied it was behind the denial of service attacks – attempts to overwhelm a website by flooding it with millions of requests – but the disruption reignited wider concerns of ongoing cyberconflict. Ilya Vityuk, cybersecurity chief of Ukraine's SBU intelligence agency, said it was too early to definitively identify specific perpetrators, as is typically the case with cyber-attacks, where perpetrators make efforts to cover their tracks. But the official added: "The only country that is interested in such … attacks on our state, especially against the backdrop of massive panic about a possible military invasion, the only country that is interested is the Russian Federation."
Read the rest of the story by Dan Sabbagh here: The Guardian

Red Cross cyber attack the work of nation-state actors

A cyber attack on the systems of the International Committee of the Red Cross (ICRC), which resulted in the data of more than 515,000 vulnerable people being compromised, appears to have been the work of an undisclosed nation-state actor, the organisation has revealed. The attack came to light on 18 January 2022, when the ICRC disclosed that it had been compromised. The compromised data relates to the organisation's Restoring Family Links programme, which assists people separated from their families due to conflict, migration or disaster, reunites missing persons with their families, and helps people in detention. In a new update published on 16 February, the ICRC said its attackers made use of "considerable resources" to access its systems using tactics, techniques and procedures that most detection tools could not have picked up. Among them were advanced hacking tools designed for offensive security that are known to be primarily used by advanced persistent threat (APT) groups with nation-state links, as well as sophisticated obfuscation techniques.
Read the rest of the story by Alex Scroxton here: Computer Weekly

Google Paid Record $8.7 Million to Bug Hunters in 2021

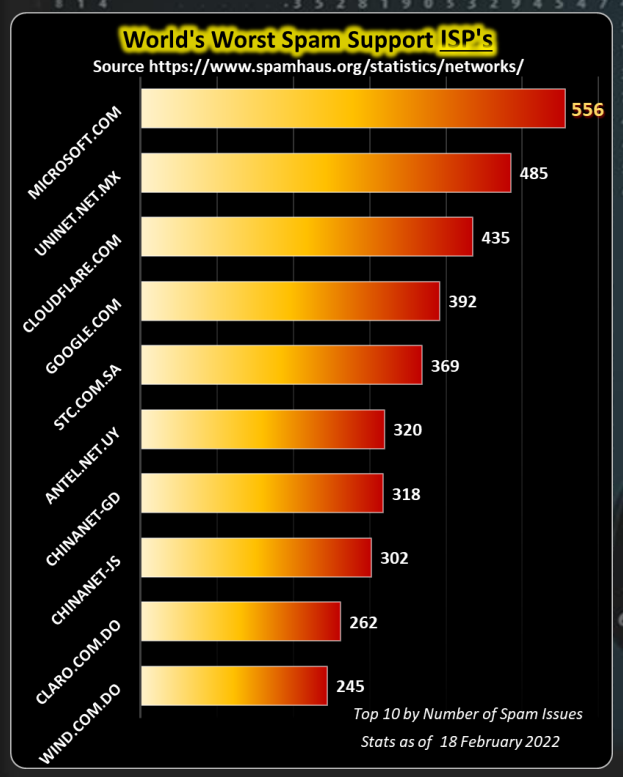
Bug-bounty programs can sometimes say as much about an organization's willingness to work with external security researchers to identify and fix security vulnerabilities in their products as it does about their potential exposure to potential attacks targeting their technologies. By that measure, Google's Android, Chrome, and Play platforms continue to be vulnerability-rich environments for bad actors to target. Last year, Google paid a record $8.7 million in rewards to 696 third-party bug hunters from 62 countries who discovered and reported thousands of vulnerabilities in the company's technologies. That amount represented a near 30% increase from the $6.7 million in rewards that Google paid bug hunters in 2020. Some of the increase had to do with higher pay-outs for certain kinds of bug discoveries. But a lot also had to do with the relatively high number of flaws that researchers are continuing to unearth in some of Google's core technologies. Read the story by Jai Vijayan here: DarkReading

France launches 'cyber city' to pool resources for better digital security

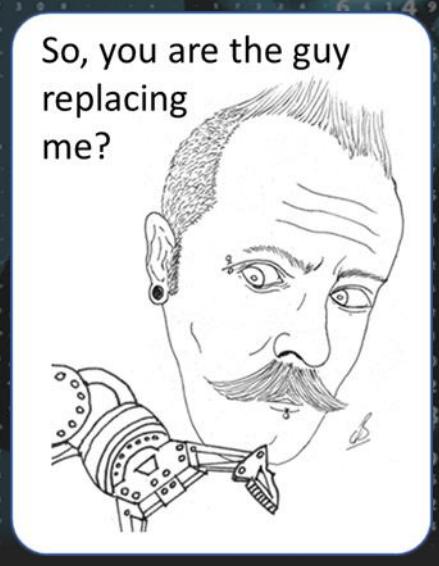
French finance minister Bruno Le Maire has inaugurated a new cyber campus near Paris' La Défense business district. The centre brings together specialists from the public and private sector in an effort to develop new security and to defend France and French business from cyber attacks. Designed by Christian de Portzamparc, the 13-storey 'Campus Cyber' in La Défense will be home to 1,700 people with backgrounds in the military, as well as industry and public administration who will share their expertise in a joint effort to fight cyber crime. The campus is part of President Emmanuel Macron's cyber security initiative that will cost €1 billion, including €720 million of public money. The plan was unveiled 12 months ago. By mixing secret service agents, with police, health workers and engineers from companies such as Orange and Thalès, Macron is hoping the campus will provide a hub for new ideas. Read the rest of the story here: RFI

Snippets from the past – Users affected by security hole

Times Daily - Aug 8, 2000. – Read how the "Security hole" in Netscape's Browser affected people in 2000, and it shows how these vulnerabilities are still with us today - Read the rest archived article here: Google Archives



For Reporting Cyber Crime in the USA go to the Internet Crime Complaint Center (IC3)



What is a Bug Bounty Program?

As we've read in the news this week of substantial pay-outs to bug hunters, one asks the question of how lucrative a career in bug hunting can be. For those not in the know, bug bounty programs allow independent security researchers to report bugs to an organization like Google, AOL, or Apple and receive rewards or compensation. These bugs are mainly aimed at security exploits and vulnerabilities, though they can also include process issues, hardware flaws, and so on. But the question really is, is it worth your while to give up your current day job to go bug hunting? Megan Kaczanowski explored this in an article posted on freecodecamp.org, and I thought I'll share an extract of some of the main points.

Bug Reports

The reports are typically made through a program run by an independent third party (like Bugcrowd or HackerOne). The organization will set up (and run) a program curated to the organization's needs. Programs may be private (invite-only) where reports are kept confidential to the organization or public (where anyone can sign up and join). They can take place over a set time frame or with no end date (though the second option is more common).

Who uses bug bounty programs?

Many major organizations use bug bounties as a part of their security program, including Google, Microsoft, AOL, Android, Apple, Digital Ocean, Goldman Sachs, and more. You can view a list of all the programs offered by major bug bounty providers, Bugcrowd and HackerOne, at these links or links listed in the resources area below. *(I picked up some SSL issues on the HackerOne site, "hackerone.com/bug-bounty-programs" please proceed to this site with caution)*

Why do companies use bug bounty programs?

Bug bounty programs give companies the ability to harness a large group of hackers in order to find bugs in their code. This gives them access to a larger number of hackers or testers than they would be able to access on a one-on-one basis. It can also increase the chances that bugs are found and reported to them before malicious hackers can exploit them.

Why do researchers and hackers participate in bug bounty programs?

Finding and reporting bugs via a bug bounty program can result in both cash bonuses and recognition. In some cases, it can be a great way to show real-world experience when you're looking for a job, or can even help introduce you to folks on the security team inside an organization. This can be full-time income for some folks, income to supplement a job, or a way to show off your skills and get a full-time job. It can also be fun! It's a great (legal) chance to test out your skills against massive corporations and government agencies.

What are the disadvantages of a bug bounty program for independent researchers and hackers?

A lot of hackers participate in these types of programs, and it can be difficult to make a significant amount of money on the platform. In order to claim the reward, the hacker needs to be the first person to submit the bug to the program. That means that in practice, you might spend weeks looking for a bug to exploit, only to be the second person to report it and make no money. Roughly 97% of participants on major bug bounty platforms have never sold a bug. In fact, a 2019 report from HackerOne confirmed that out of more than 300,000 registered users, only around 2.5% received a bounty in their time on the platform. Essentially, most hackers aren't making much money on these platforms, and very few are making enough to replace a full-time salary (plus they don't have benefits like vacation days, health insurance, and retirement planning).

What are the disadvantages of bug bounty programs for organizations?

These programs are only beneficial if the program results in the organization finding problems that they weren't able to find themselves (and if they can fix those problems)! Any bug bounty program is likely to attract a large number of submissions, many of which may not be high-quality submissions. An organization needs to be prepared to deal with the increased volume of alerts, and the possibility of a low signal to noise ratio (essentially that it's likely that they'll receive quite a few unhelpful reports for every helpful report).
The vast majority of bug bounty participants concentrate on website vulnerabilities (72%, according to HackerOne), while only a few (3.5%) opt to look for operating system vulnerabilities. This is likely due to the fact that hacking operating systems (like network hardware and memory) requires a significant amount of highly specialized expertise. This means that companies may see significant return on investment for bug bounties on websites, and not for other applications, particularly those which require specialized expertise.
It can be potentially risky to allow independent researchers to attempt to penetrate your network. This may result in public disclosure of bugs, causing reputation damage in the public eye, or disclosure of bugs to more malicious third parties, who could use this information to target the organization.

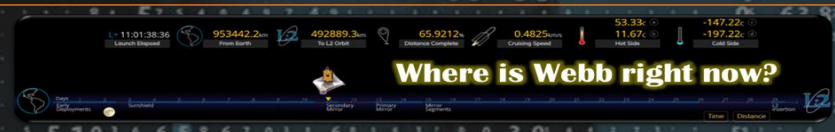
Which is better – bug bounty programs or hired penetration testers?

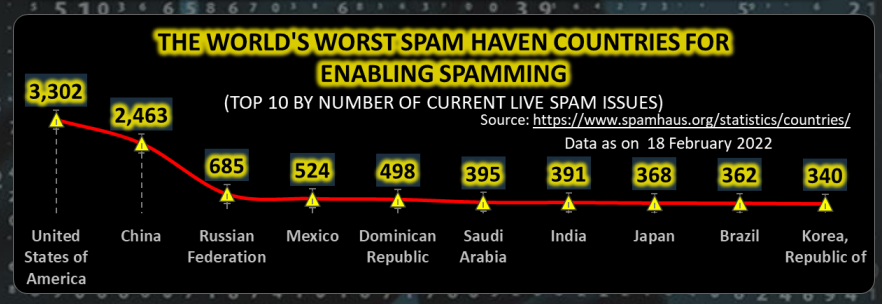
Often these two methods are not directly comparable - each has strengths and weaknesses. If the organization would benefit more from having more people (of varying skill levels) looking at a problem, the application isn't particularly sensitive, and it doesn't require specific expertise, a bug bounty is probably more appropriate. If the application is internal/sensitive, the problem requires specific expertise, or the organization needs a response within a specific time frame, a penetration test is more appropriate.

Resources: FreeCodeCamp, BugHunters.Google, Microsoft, Apple, Facebook, Sony, Dell, HP, Bugcrowd, OpenBugBounty, Amazon

Other Interesting News and Cyber Security bits:

- Here's how Raspberry Pi is creating a new generation of Python developers
- Now You Can Rent a Robot Worker—for Less Than Paying a Human
- SANS Daily Network Security Podcast (Stormcast)





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