
**On February 8, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in vBulletin and Google products.**
**CIS Security Advisories**

## 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
## 10 February 2023

## In The News This Week

### 20 Million Users Impacted by Data Breach at Instant Checkmate & TruthFinder

PeopleConnect-owned background check services Instant Checkmate and TruthFinder have disclosed data breaches affecting a total of more than 20 million users. In individual data breach notices published on February 3, the organizations informed users that the incident was discovered after cybercriminals started sharing databases stolen from the two companies on underground forums. The databases – or 'lists', as the two companies call them – contain names, email addresses, phone numbers, encrypted passwords, and password reset tokens that are either expired or inactive. "We have confirmed that the list was created several years ago and appears to include all customer accounts created between 2011 and 2019. The published list originated inside our company," the announcements read..
Read the full story by Ionut Arghire here: SecurityWeek

### Cops make arrests and seize drugs after hacking Exclu encrypted messaging app

Police in the Netherlands, Belgium and Poland raided 80 addresses after covertly intercepting messages from the Exclu encrypted messaging app. - European police have shut down an encrypted messaging service used by thousands of people including members of organised crime groups. A joint operation led by Dutch and German police has led to more than 45 arrests following a multi-country probe into the Exclu encrypted messaging service. Police covertly read decrypted communications on the app for five months before launching coordinated raids, according to a series of announcements on Monday 6 February 2023. Exclu claims on its website to offer the "most secure encryption protocols", which it says have been audited by cryptography experts to ensure they contain no backdoor vulnerabilities....
Read the rest of the article by Bill Goodwin here: ComputerWeekly

### Tor Network Under DDoS Pressure for 7 Months

For the past seven months, the Tor anonymity network has been hit with numerous distributed denial-of-service (DDoS) attacks, its maintainers announced this week. - Some of the attacks have been severe enough to prevent users from loading pages or accessing onion services, the Tor Project says. Publicly released in 2003, Tor directs traffic through a global network of more than 7,000 relays, to help users maintain anonymity and protect their privacy while navigating the web. Despite its legitimate purpose, Tor has also been used for illegal activities. Attacks against Tor are not new, with many of them seeking to deanonymize users. In DDoS attacks, the target is flooded with rogue network traffic originating from multiple different sources in an effort to disrupt the target service by depleting resources. According to the Tor Project, despite its efforts to mitigate the impact of the experienced DDoS attacks, continuous shifts in methods are making the task difficult. "The methods and targets of these attacks have changed over time and we are adapting as these attacks continue. It's not possible to determine with certainty who is conducting these attacks or their intentions," Tor says..
Read the full article by Ionut Arghire here: SecurityWeek

### UN experts: North Korean hackers stole record virtual assets

UNITED NATIONS (AP) — North Korean hackers working for the government stole record-breaking virtual assets last year estimated to be worth between $630 million and more than $1 billion, U.N. experts said in a new report. - The panel of experts said in the wide-ranging report seen Tuesday by The Associated Press that the hackers used increasingly sophisticated techniques to gain access to digital networks involved in cyberfinance, and to steal information that could be useful in North Korea's nuclear and ballistic missile programs from governments, individuals and companies. With growing tensions on the Korean Peninsula, the report said North Korea continued to violate U.N. sanctions, producing weapons-grade nuclear material, and improving its ballistic missile program, which "continued to accelerate dramatically."...
Read the rest of the story by Edith M. Lederer here: Associated Press

### NewsPenguin Goes Phishing for Maritime & Military Secrets

A sophisticated cyber-espionage attack against high-value targets attending a maritime technology conference in Pakistan this weekend has been in the works since last year. A novel threat actor that researchers have dubbed "NewsPenguin" has been conducting an espionage campaign against Pakistan's military-industrial complex for months, using an advanced malware tool. In a blog post on Feb. 9, researchers from Blackberry revealed how this group carefully planned out a phishing campaign targeting the Pakistan International Maritime Expo & Conference (PIMEC) ... Read the full story here: Dark Reading

### Cryptographers Decode Secret Letters of Mary, Queen of Scots

Nearly a half-millennium after her execution, encrypted letters from the imprisoned royal offer a fascinating look into early cryptography. - A tranche of more than 55 encoded letters written by Mary, Queen of Scots has been uncovered, and decrypted by a team of cryptographic experts. Read more about it here: Dark Reading

## How AI chatbots like ChatGPT and Google's Bard can influence Cybersecurity

ChatGPT has been the talk of the town since it was launched in late November last year, and the gurus out there have been speculating on the potential impact or influence Generative Artificial Intelligence (AI) can have in the Cybersecurity world. But first, for those who are not in the know, let's have a look at what ChatGPT and its Google rival, Bard, are. ChatGPT is essentially a chatbot developed by the Microsoft-funded organisation, OpenAI. It utilizes complex language models to interact with humans in a conversational way to answer questions and even follow-up questions. It can admit its mistakes and learn from them, challenge incorrect premises, and reject inappropriate requests. Google launched its own version called Bard this week with enormous fanfare in the media as an answer to the success of ChatGPT.
But what does that mean for us in the Cybersecurity world? Recently, VentureBeat conducted a Q&A with David Reber, the chief security officer at Nvidia and ex-senior director of cybersecurity at Nutanix. He shared his thoughts on the impact that generative AI and tools like ChatGPT will have on the threat landscape in 2023.

### Q&A session with Nvidia's CSO, David Reber "Generative AI, ChatGPT has made security a 'cat and mouse' game"

**VB: Why does it take AI to stop AI-driven cyberthreats?**

**Reber:** Understanding the limitations of your adversary provides you with insights into where they may or may not go next. One of the traditional limitations of the adversary was tailoring attacks at scale and the knowhow.
With advances in generative AI, finely-tuned and targeted attacks are at the fingertips of the least sophisticated attackers.
Machine scale is the competition. Speed and complexity of attacks outpace human capacity. This is where AI for the defender comes to play. How do we use their tools against them? It is a cat and mouse game that will forever be present. Continuous adaptation on both sides, now adapting at machine scale.

**VB: What challenges do security teams face when using defensive AI against offensive AI?**

**Reber:** A decade ago, the industry pivoted to an "assume breach" strategy. We recognized the dichotomy that the adversary must be right once, while the defense must be right every time.
Our adversaries understand our limitations: human capacity, regulations, competing priorities. As we continue to face increased regulations of commercial cyberpractices, the need to get it right compounds.
The challenge with AI is fundamentally trust. How do we know it works to focus human capacity elsewhere? Fundamentally it is AI until we trust it, then it becomes automation.
We have a self-driving car, but do we trust it to get us to our destination? The offense is in a demolition derby. As long as they make an impact they win. They don't have rules, bounds nor the legal oversight to hinder in the event something goes wrong.

**VB: How can CISOs/security leaders leverage AI in a way to 'outfox' uses of malicious AI?**

**Reber:** It is estimated that there are more than 14 billion devices connected to the internet in 2022. To outfox use of malicious AI, security leaders need to be less interesting than the average target or increase the cost of the attack. While we are in the formative phase of generative AI, we can look at traditional stall tactics.
Create a more interesting target on your network, [a] honeypot, that knows how to interact in return. The goal is to force the adversary to make more noise and waste time on less valuable agents. Masquerade fake data as intellectual property. It is a battle of deception. The game has not changed, the toys are just different.

**VB: Any comments on ChatGPT?**

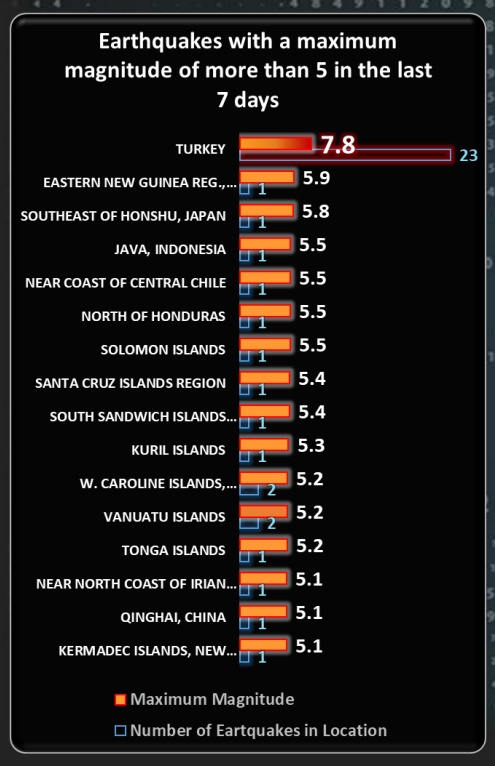
**Reber:** It will democratize offensive security. Previously, the offense was limited by real time tailoring at scale and technical knowhow. ChatGPT has the potential to remove this limiting factor.
It will breed a new generation of script kiddies, more a fleet of prompt kiddies. The adversary's limitations are now removed. It also is an opportunity for the defender to predict what is coming. Look around corners not yet explored in their attack surface.

**VB: Are there any other comments you'd like to add on this topic?**

**Reber:** The market is flooded with niche solutions. Everyone is trying to find their piece of the next generation of computing. With the current economic situation, we all need to find ways to do more with less. This is going to lead to more unification of technology stacks and less point solution tool investments.
History continues to teach us the power of collective defense. As we embark in the new generation of democratized offense, we need to come together as an ecosystem.
Interoperability to transport information exchange is how we stay ahead of the adversary. If you are the one in 14 billion, share your knowledge. Enable the industry to move faster than the adversary.

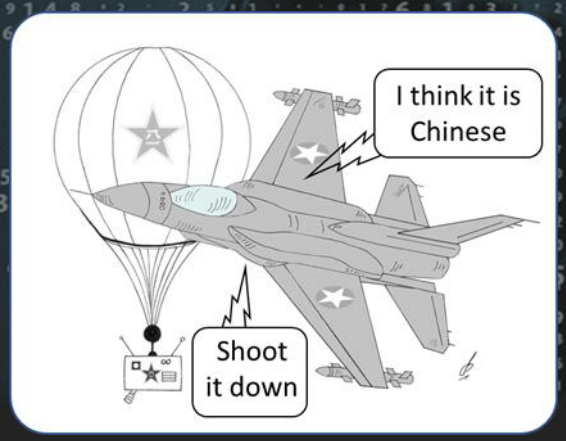
You can watch the video or read the transcript here: VentureBeat

Resources: OpenAI, Google, BBC News, Nature, Technopedia, Economic Times




For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

IRIS Interactive Earthquake Map



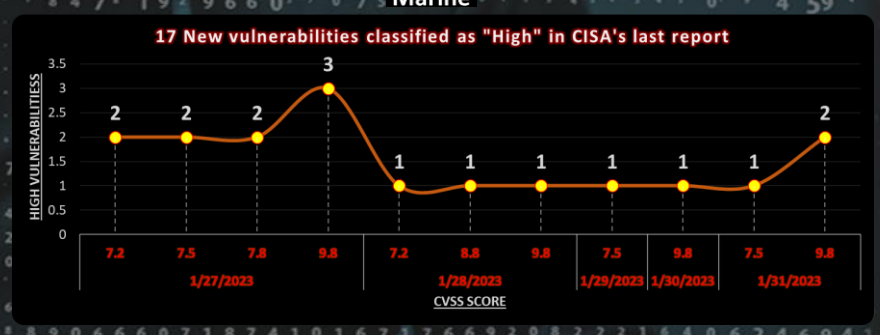

## Other Interesting News and Cyber Security bits:

- US downs Chinese balloon, drawing a threat from China
- NASA's HiRISE Captures a Bear's Face on Mars – What Is It Really?
- The Worldwide Cyber Security Consulting Services to Reach $8.614 Billion in 2027
- Webinar 21 Feb - The War in Ukraine - A Year in Review | Russia's Hybrid Warfare Strategy
- SANS Daily Network Security Podcast (Storm cast)

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally

Marine Traffic

SatelliteXplorer Track satellites in orbit




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