
**On June 1, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Microsoft Support Diagnostic Tool.**
**CIS Advisories**

**Covid-19 Global Statistics**

| Date | Confirmed Cases | Total Deaths |
|---|---|---|
| 03 JUN 22 | 534,251,747 | 6,317,751 |

Deaths this week: 9,856

## 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
## 03 June 2022

## In The News This Week

### Hacker tastes own medicine as community gets back stolen NFTs

The dev partner of the Solana-based NFT game raised the royalty to 98% from the usual 5%, resulting in the scammer listing the 25 stolen NFTs for sale, which were then bought back and returned. Tales of traders getting scammed out of their nonfungible tokens were quite common at the peak of the NFT boom. However, in an interesting turn of events, the Solana community came together to "scam" a scammer in order to get back some stolen NFTs.
It all started with the Discord channel hack of cross-chain gaming development studio Uncharted NFT, where scammers managed to drain 109 user wallets. The scammers got away with 150-plus SOL tokens and 25 World of Solana (WOS) NFTs, including three rare and highly valuable digital collectibles. WOS is a collection of 2,222 unique heroines, with the most expensive avatar currently listed for 123 SOL ($5,600). The current floor price of the collection is 2.03 SOL.
In the aftermath of the hack, the community decided to get back the stolen NFTs. The WOS team got in touch with their development partner, who goes by Cyberfrog on Twitter, and raised royalties on the stolen NFTs to 98% from the default 5%. - Read the rest of the story by Prashant Jha here: CoinTelegraph

### Microsoft confirms 'Follina' virus: A 'Zero-Day' vulnerability affecting 32 versions of Windows

Microsoft's advisory, which was issued on its official website, states that the vulnerability is exploited by sending an MS Word document to the targets. - A serious vulnerability has been found in Microsoft Windows, the most-used operating system for computers around the world, which could be exploited by a simple MS Word document. The vulnerability, which affects 32 versions of Windows, was officially acknowledged by Microsoft on Tuesday, while the Indian Computer Emergency Response Team (CERT-In), too, has assigned it a 'high' severity rating. Worryingly, there are also preliminary indications that the vulnerability has already been used to target Indian users. The vulnerability, earlier dubbed 'Follina', was later renamed as CVE-2022-30190. 'CVE' stands for Common Vulnerabilities and Exposures, and every vulnerability that is officially acknowledged is assigned a CVE number for easy reference and further research. Follina falls under the category of 'Zero Day vulnerabilities', meaning vulnerabilities discovered only when malicious hackers exploit them. The term 'Zero Day' is used because there are zero days between their discovery and exploitation.
Read the full article by Gautam Mengle here: FreePressJournal. Additional – ThreatPost, CrowdStrike

### President Cyril Ramaphosa email hack a huge danger to South Africa

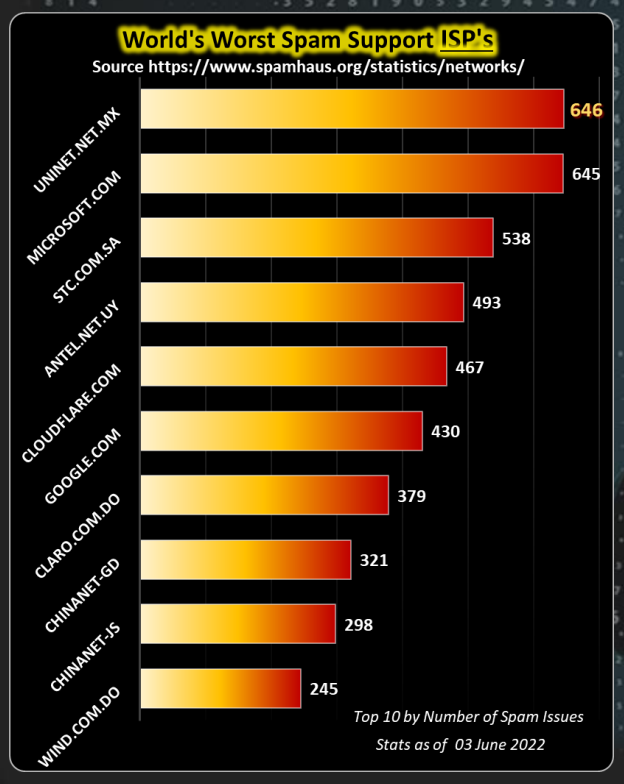
Russian information security firm Kaspersky warns that the alleged compromise of President Cyril Ramaphosa's email account is a significant threat to South Africa. "The impact of such a leak is extraordinary depending on the nature of communication within," said Kaspersky senior security researcher Maher Yamout. He highlighted that South Africa is going through turbulent times politically and economically. "The threat actor could literally destabilise the country if equipped with the right emails," Yamout warned. Kaspersky's comments follow a Sunday Times report about a group calling itself SpiderLog$. According to the report, the group provided screenshots proving they could access sensitive military and intelligence data. In one of the screenshots, SpiderLog$ showed it could get into the defence and state security departments' webmail interface. SpiderLog$ also reportedly obtained details of a loan President Cyril Ramaphosa took out from one of South Africa's top four banks in the 2000s. It said it used data leaked by another group called N4ugtysecTU after it breached credit bureau TransUnion earlier this year..... Read the rest here: Mybroadband

### US confirms military hackers have conducted cyber operations in support of Ukraine

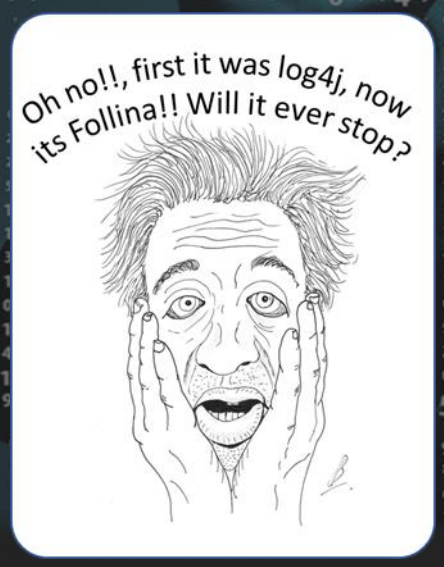
Cyber Command, the US military's hacking unit, has conducted offensive cyber operations in support of Ukraine as it defends itself against Russia's invasion, the head of the command has confirmed. The disclosure underscores how important projecting power in cyberspace -- in support of Ukraine's defenses and to potentially deter Russia from conducting cyberattacks against US infrastructure -- has been to the Biden administration as it continues to avoid directly engaging Russia in a shooting war. "We've conducted a series of operations across the full spectrum; offensive, defensive, [and] information operations," General Paul Nakasone said in an interview with Sky News.
Read the rest of the article by Sean Lyngaas here: CNN

### Russian Killnet cyber attacks begin on Italian-linked businesses

An alert has been issued by Italy's Computer Security Incident Response Team (CSIRT) warning public and private sector organisations of a heightened risk of cyber attacks from pro-Russian hackers. National public entities like governmental departments, Italian utility companies, and any public sector organisation with a brand image tied to the country of Italy are thought to be at risk, CSIRT Italy said. The security authority did not specify the identity of the hackers of particular concern, but linked cyber attacks that took place between 11-21 May 2022 against Italian organisations to the hackers in question. The information provided would suggest that the hackers believed to be targeting the country are the pro-Russian Killnet group. Read the rest of the story by Connor Jones here: ITPro




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




## ZTNA vs. VPN

The new buzzword going around is ZTNA (Zero Trust Network Access), and there was much talk about it at this year's IT Web Security Summit which I was fortunate enough to attend. The Covid pandemic has changed the working environment significantly as we see more and more employers adopting a hybrid approach of physical and remote working environments in the aftermath of lockdowns. This brought about its own challenges and associated risks. The question now remains, how do companies adequately control their remote workers? The traditional VPN (Virtual Private Network) seems to work well but it has its limitations if it comes to more granular control. Although still in its infancy stages, ZTNA could be the answer to many control issues in this hybrid environment.
Richard Sutherland of TechRadar wrote a good explanatory piece comparing the two technologies and below is an extract of the main points.

### ZTNA vs VPN: What are the Differences

With remote working here to stay, companies must have secure ways for remote workers to access internal network resources like applications, databases, and servers. Traditionally, this is done with a virtual private network (VPN)(opens in new tab), but zero trust network access (ZTNA) solutions are becoming more common. In this ZTNA vs VPN comparison, we look at the main differences between the two approaches, including their features, performance, and customer support, so you can decide which is best for your business.
VPNs enable workers to remotely access resources on the company network as if they were on a device physically connected to the network. However, offering remote users complete access to all resources on a company network is a security risk.
ZTNA solutions also provide remote access to resources, but they have more restrictive and customizable user authentication. The best ZTNA solutions make the remote use of company resources more secure and make it easier for employees to access them.

**ZTNA vs VPN: Features** - VPNs and ZTNA remote access solutions have much crossover when it comes to features. We can consider ZTNA as evolved VPNs, extending the features of VPNs while fixing some of their inherent security weaknesses.
**Trust Model** - VPNs largely work on the assumption that any user and device connected to the local company network is trusted. These trusted devices can access all the other devices and applications on the network. When you connect remotely through a VPN, your device becomes another one of these trusted devices. ZTNA is based on the Zero Trust security model, which works on a "never trust, always verify" basis. Whether a user is connecting from a local computer or a remote one, this model always authenticates the user and device each time they make a new request. This is fundamentally more secure than the basic VPN model that would enable a compromised remote machine to access the entire internal network.
**Access Model** - VPNs work on the network level and only have visibility of the low-level network traffic being sent back and forth. While you can set up rules for which parts of your network will be accessible and to whom with some VPNs, you can't set up very advanced rules because VPNs don't know much about the applications users are accessing. ZTNA is different in that it works on the application level. Users are not given access to networks—instead, they only have access to the specific applications they are authorized to use. This makes ZTNA much more secure than basic VPNs. Even malicious users would only be able to do a limited amount of damage if they gained access to the network.
**Authentication** - ZTNA has a much more robust authentication system than VPNs. VPNs often just require a username and password to connect, and then the remote user has complete access to the network. In contrast, every request on a ZTNA infrastructure first goes through a trust broker. The trust broker checks that the user is who they say they are, that they have the right to make the request they are making, and that there are no red flags in their security. ZTNA can deny requests if the remote computer doesn't have the latest security updates or malware is detected, for example. This cuts down on the chance of a compromised remote computer being used to access sensitive company data.
**ZTNA vs VPN: Performance**
**Speed** - ZTNA can be significantly faster than VPNs. This is because ZTNA allows authenticated users to connect directly to applications instead of requiring all traffic to be sent through a central point in a corporate data center. The user first validates with the trust broker, then they're able to directly access the resources they need without having to transmit all data through a VPN. Another significant advantage of a ZTNA approach is that the resources users access don't need to be on your local corporate network at all—they can be on the cloud. The trust broker authenticates the user, who is then given access to the cloud-based resource. Having your resources on the cloud allows for massive scalability and improved speeds.
**Ease of Use** - Accessing company resources through a VPN requires the download and setup of a VPN client. The employee must also remember to connect to the VPN each time they want to use these resources, and this is especially annoying if they need to use different VPNs for different aspects of their job. When set up correctly, ZTNA doesn't require a separate program to be run in the background. As long as the user authenticates themselves, they simply run the company application they want to from wherever they are. From the user's point of view, this is much more straightforward and convenient.
**ZTNA vs VPN: Support**
While VPN and ZTNA providers all offer some level of customer support, ZTNA solution companies provide more hands-on support overall. ZTNA is more focused on enterprise-level security for larger companies, whereas VPNs are often used on a smaller scale or for personal use.
**ZTNA vs VPN: Verdict**
A VPN solution is one of the simplest ways to enable remote workers to access resources on your company network. We continue to recommend VPNs for small businesses that have only a few employees because they're relatively easy to put into place. Advertisement
However, ZTNA solutions are the clear winner for larger companies with multiple different resources that need to be shared remotely. ZTNA's application-based access model solves the problem of users getting access to resources they shouldn't have access to.

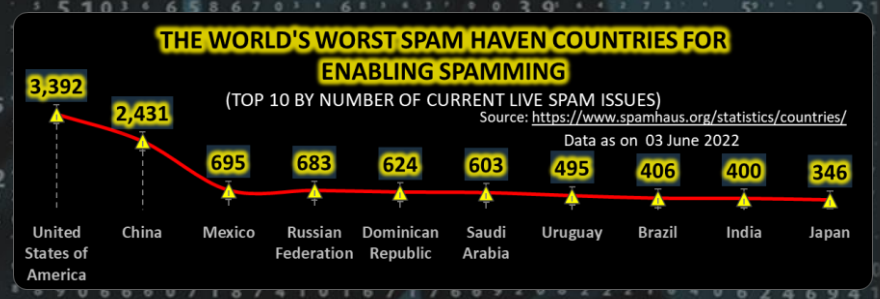
Read this full post here: TechRadar

### Other Interesting News and Cyber Security bits:

- Hydrogen's promise: How fuel cells might power lower-carbon datacentres
- Five Eyes nations warn against impending Russian cyber attacks
- Five Eyes, Nine Eyes and Fourteen Eyes explained: how these alliances affect you?
- SANS Daily Network Security Podcast (Storm cast)

flightradar24
LIVE AIR TRAFFIC
Track any Aeroplane in flight globally

Marine Traffic
Track any Sailing Vessel globally




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