Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security®
By
Chris Bester

On February 1, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to open-source reports of ransomware targeting K-12 schools.
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

03 February 2023

In The News This Week

Hackers Abused Microsoft's "Verified Publisher" OAuth Apps to Breach Corporate Email Accounts

Microsoft on Tuesday said it took steps to disable fake Microsoft Partner Network (MPN) accounts that were used for creating malicious OAuth applications as part of a phishing campaign designed to breach organizations' cloud environments and steal email. "The applications created by these fraudulent actors were then used in a consent phishing campaign, which tricked users into granting permissions to the fraudulent apps," the tech giant said. "This phishing campaign targeted a subset of customers primarily based in the U.K. and Ireland.“ Consent phishing is a social engineering attack wherein users are tricked into granting permissions to malicious cloud applications, which can then be weaponized to gain access to legitimate cloud services and sensitive user data. The Windows maker said it became aware of the campaign on December 15, 2022. It has since alerted affected customers via email, with the company noting that the threat actors abused the consent to exfiltrate mailboxes. Read the full story by Ravie Lakshmanan here: The Hacker News

JD Sports says 10 million customers hit by cyber-attack

Sportswear chain JD Sports has said stored data relating to 10 million customers might be at risk after it was hit by a cyber-attack. - The company said information that "may have been accessed" by hackers included names, addresses, email accounts, phone numbers, order details and the final four digits of bank cards. The data related to online orders between November 2018 and October 2020. JD Sports said it was contacting affected customers. The group said the affected data was "limited". It added it did not hold full payment card details and did not believe that account passwords were accessed by the hackers. "We want to apologise to those customers who may have been affected by this incident," said Neil Greenhalgh, chief financial officer of JD Sports. "Protecting the data of our customers is an absolute priority for JD."
Read the full article by Michael Race here: BBC News

Russia's Sandworm APT Launches Swarm of Wiper Attacks in Ukraine

The incidents are the latest indication of the growing popularity of dangerous disk wipers, created to disrupt and degrade critical infrastructure and other organizations. - Sandworm, an advanced persistent threat (APT) group linked to Russia's foreign military intelligence agency GRU, has deployed a medley of five different wipers on systems belonging to Ukraine's national news agency Ukrinform. The attack was one of two recent wiper offensives from Sandworm in the country. The efforts are the latest indications that the use of destructive wiper malware is on the rise, as a popular weapon among Russian cyber-threat actors. The goal is to cause irrevocable damage to the operations of targeted organizations in Ukraine, as part of Russia's broader military objectives in the country. Read the full article by Jai Vijayan here: Dark Reading

Experts Warn of 'Ice Breaker' Cyberattacks Targeting Gaming and Gambling Industry

A new attack campaign has been targeting the gaming and gambling sectors since at least September 2022, just as the ICE London 2023 gaming industry trade fair event is scheduled to kick off next week. Israeli cybersecurity company Security Joes is tracking the activity cluster under the name Ice Breaker, stating the intrusions employ clever social engineering tactics to deploy a JavaScript backdoor. The attack sequence proceeds as follows: The threat actor poses as a customer while initiating a conversation with a support agent of a gaming company under the pretext of having account registration issues. The adversary then urges the individual on the other end to open a screenshot image hosted on Dropbox...
Read the story by Ravie Lakshmanan here: The Hacker News

Rising ‘Firebrick Ostrich’ BEC Group Launches Industrial-Scale Cyberattacks

The group's wanton attacks demonstrate that business email compromise is everything a hacker can want in one package: low risk, high reward, quick, easy, and low effort. - Business email compromise (BEC) has become one of the most popular methods of financially motivated hacking. And over the past year, one group in particular has demonstrated just how quick, easy, and lucrative it really is. In a Feb. 1 blog post, Crane Hassold, director of threat intelligence at Abnormal Security, profiled "Firebrick Ostrich" a threat actor that's been performing BEC at a near-industrial scale. Since April 2021, the group has carried out more than 350 BEC campaigns, impersonating 151 organizations and utilizing 212 malicious domains in the process. This volume of attacks is made possible by the group's wholesale gunslinging approach. Firebrick Ostrich doesn't discriminate much when it comes to targets or gather exceptional intelligence in order to craft the perfect phishing bait. It throws darts at a wall because, evidently, when it comes to BEC at scale, that's enough. Read the full story by Nate Nelson here: Dark Reading

Homeland Security, cyber security experts explain the threat of sextortion

Watch this video if you are concerned about what your kids are exposed to on the internet. It talks about social chat platforms like OMEGLE, TikTok, and other platforms where lurking sextortionists are targeting children.
Watch the 3-minute Video here: YouTube

The Untold Story of a Crippling Ransomware Attack (Case Study)

In this day and age in our modern societies, it is almost uncommon for a day to go by without some news of a ransomware attack somewhere. In fact, according to SonicWall, ransomware attacks peaked at an astonishing 188.9 million attacks measured in the second quarter of 2021, that is more than 2 million attacks a day! But how devastating can it be, and how is the surrounding society of a victim organisation impacted? – Matt Burgess of Wired published an article this week that gives us a little insight into the aftermath of a ransomware attack and the affects it had on the local community. Below then is an extract from the article.

The Untold Story of a Crippling Ransomware Attack

More than two years ago, criminals crippled the systems of London’s Hackney Council. It's still fighting to recover.
IT WAS A Sunday morning in mid-October 2020 when Rob Miller first heard there was a problem. The databases and IT systems at Hackney Council, in East London, were suffering from outages. At the time, the UK was heading into its second deadly wave of the coronavirus pandemic, with millions living under lockdown restrictions and normal life severely disrupted. But for Miller, a strategic director at the public authority, things were about to get much worse. “By lunchtime, it was apparent that it was more than technical stuff,” Miller says.

Two days later, the leaders of Hackney Council—which is one of London’s 32 local authorities and responsible for the lives of more than 250,000 people—revealed it had been hit by a cyberattack. Criminal hackers had deployed ransomware that severely crippled its systems, limiting the council’s ability to look after the people who depend on it. The Pysa ransomware gang later claimed responsibility for the attack and, weeks later, claimed to be publishing data it stole from the council.

Today, more than two years later, Hackney Council is still dealing with the colossal aftermath of the ransomware attack. For around a year, many council services weren’t available. Crucial council systems—including housing benefit payments and social care services—weren’t functioning properly. While its services are now back up and running, parts of the council are still not operating as they were prior to the attack.

A WIRED analysis of dozens of council meetings, minutes, and documents reveals the scale of disruption the ransomware caused to the council and, crucially, the thousands of people it serves. People’s health, housing situations, and finances suffered as a result of the insidious criminal group’s attack. The attack against Hackney stands out not just because of its severity, but also the amount of time it has taken for the organization to recover and help people in need.

Ransom Demands - You can think of local governments as complex machines. They’re made up of thousands of people running hundreds of services that touch almost every part of a person’s life. Most of this work goes unnoticed until something goes wrong. For Hackney, the ransomware attack ground the machine to a halt.

Among the hundreds of services Hackney Council provides are social and children’s care, waste collection, benefits payments to people in need of financial support, and public housing. Many of these services are run using in-house technical systems and services. In many ways, these can be considered critical infrastructure, making the Hackney Council not dissimilar to hospitals or energy providers.

“The attacks against public sector organizations, like local councils, schools, or universities, are quite powerful,” says Jamie MacColl, a cybersecurity and threat researcher at the RUSI think tank who is researching the societal impact of ransomware. “It’s not like the energy grids going down or like a water supply being disrupted … but it’s things that are crucial to the day-to-day existence.”

All the systems hosted on Hackney’s servers were impacted, Miller told councilors at one public meeting assessing the ransomware attack in 2022. Social care, housing benefits, council tax, business rates, and housing services were some of the most impacted. Databases and records weren’t accessible—the council has not paid any ransom demand. “Most of our data and our IT systems that were creating that data were not available, which really had a devastating impact on the services we were able to provide, but the work that we do as well,” Lisa Stidle, the data and insight manager at Hackney Council, said in a talk about the council’s recovery last year.

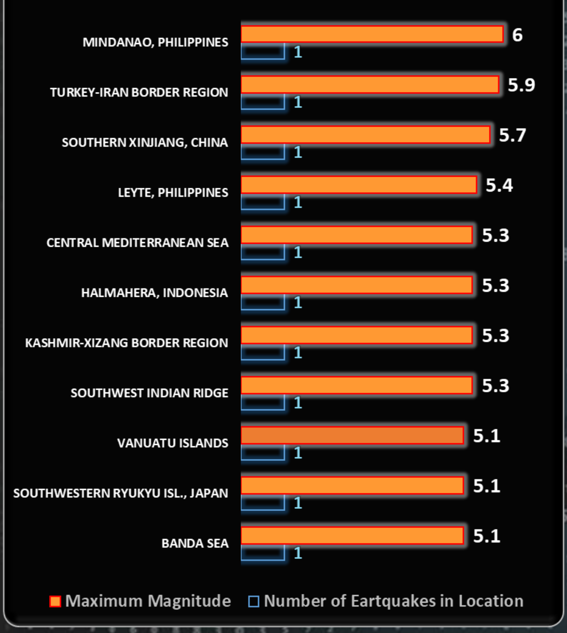
One person living with disabilities in Hackney, who asked not to be named for privacy reasons, says they applied for social care at the end of June 2021—eight months after the cyberattack first hit—but didn’t end up with a care plan or visits from carers until February 2022. “I could not wash myself. I couldn’t wash my own hair,” they say. “And the reason for that delay, they repeatedly told me, was the hack.” The person recalls that when they first heard back from the council, months after initially getting in touch, the worker they spoke with was relieved they were still alive, as their situation hadn’t been clear and there had been a delay in the case.

Since the ransomware attack, Hackney residents have told independent complaints boards how they suffered. At one point during the aftermath of the cyberattack and the ongoing pandemic, Hackney had a backlog of around 7,000 home repairs. A Housing Ombudsman report from May 2022 said Hackney was responsible for “severe maladministration” leading to “substantial delays” in dealing with “damp, mold, and leaks” at one person’s home. While Hackney had lost its records in the cyberattack, the Ombudsman said the council didn’t make enough efforts to check emails (which were still available) or interview staff about the case. (The attack “impacted on our ability to retrieve our housing management and repairs data, as well as historic records, and sadly impeded our ability to investigate the resident’s complaint,” the council said.)

The council was also criticized because its system for reporting noise complaints wasn’t working. There was a backlog of council tax payments. It was also unable to investigate people’s complaints properly, as records weren’t available. The loss of housing records and people’s correspondence led to “large numbers” of complaints to the council in the first months after the attacks, according to council reports. In one instance, a resident hadn’t been able to use their kitchen for over a year, and work was partially delayed because the cyberattack made the building plans inaccessible. And in July 2022, ITV News reported a family of seven living in Hackney was forced to leave their home because the council wasn’t able to update their housing benefit payments.....   Unfortunately, that is all I have space for in this post, to read the rest, please click and visit the Wired site.

Resources: Wired, SonicWall, Techjury, AntivirusGuide, Riskrecon

Earthquakes with a maximum magnitude of more than 5 in the last 7 days



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

OH NO!! That’s appalling!!... How can I prevent my kids from being exposed to that?

Parents, educate yourself on the dangers of the Internet and the measures you can take to protect your kids

Other Interesting News and Cyber Security bits:

- Is President Biden’s National Cybersecurity Strategy a good idea? (5 min Video)
- AI - Humanity May Reach Singularity Within Just 7 Years, Trend Shows
- 98% of Firms Have a Supply Chain Relationship That Has Been Breached: Analysis
- Cyber Security Tutorial: A Step-by-Step Guide
- SANS Daily Network Security Podcast (Storm cast)

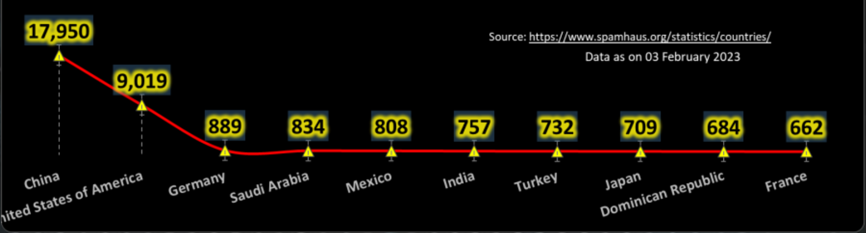
flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally

www.iris.edu IRIS Interactive Earthquake Map

Marine Traffic

SatelliteXplorer Track satellites in orbit

THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING
(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)



Source: https://www.spamhaus.org/statistics/countries/
Data as on 03 February 2023

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