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

On September 29, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Nagios, Apple, Google, SonicWall, and Microsoft products. See Latest CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
01 Oct	234,551,205	4,797,146

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

01 October 2021

In The News This Week

Russia arrests top cybersecurity executive in treason case

MOSCOW, Sept 29 (Reuters) - Russian authorities have arrested the chief executive of a leading Russian cybersecurity company on suspicion of state treason, a court said on Wednesday, sending a chill through Russia's IT and business sectors. Ilya Sachkov, 35, who founded Group IB, one of Russia's most prominent cyber security firms, was arrested on Tuesday, the RTVI TV channel reported as law enforcement officers carried out searches at the Moscow offices of the firm. State news agency TASS cited an unnamed security source as saying Sachkov was accused of working with unspecified foreign intelligence services and of treason that hurt Russia's national interests. He denied both allegations, it said. Group IB said in a statement it was sure Sachkov was not guilty of the allegations, but that it was unable to comment further on them. Read the full story here: Reuters

This dangerous mobile Trojan has stolen a fortune from over 10 million victims

An Android Trojan has now achieved a victim count of over 10 million in at least 70 countries. -According to Zimperium zLabs, the new malware has been embedded in at least 200 malicious applications, many of which have managed to circumvent the protections offered by the Google Play Store, the official repository for Android apps. The researchers say that the operators behind the Trojan have managed to infect so many devices that a stable cash flow of illicit funds, "generating millions in recurring revenue each month," has been established. Believed to have been in operation since November 2020, the "GriftHorse" campaign relies on victims being duped into handing over their phone number, which is then used to subscribe them to premium SMS messaging services. Victims first download Android apps that appear innocent and legitimate. These apps vary from puzzle games and utilities to dating software, food and drink, with the most popular malicious app -- a translator -- accounting for at least 500,000 downloads. Read the full story by Charlie Osborne here: ZDNet

Defense contractors required to get cybersecurity defense certification to prevent hacks

HUNTSVILLE, Ala. – The threat of cyber security hacks and information breaches is an ever-present threat with serious consequences. In an effort to protect national security, all Department of Defense contractors will have to have a level of "Cybersecurity Maturity Model" certification to do business. Nationwide, this will impact all of the defense industrial bases which include 300,000 companies in the supply chain and many of those are in north Alabama. The Cybersecurity Maturity Model Certification (CMMC) is a unified standard for implementing cyber security across the defense industry. "There are five levels. Level one through five and at some point in the near future any contractor that does business with the D.O.D in the defense industrial base, they will be required to have a certain level of certification to participate," says Gray Analytics VP and General Council Jay Town. Town says the level of certification required for a company will depend on the type of work the government is asking them to do. "If you're selling tires, it's gonna probably be a much lower level than if you're building lasers for satellites and things like that," says Town. Read the full story here: News19

New Azure AD Bug Lets Hackers Brute-Force Passwords Without Getting Caught

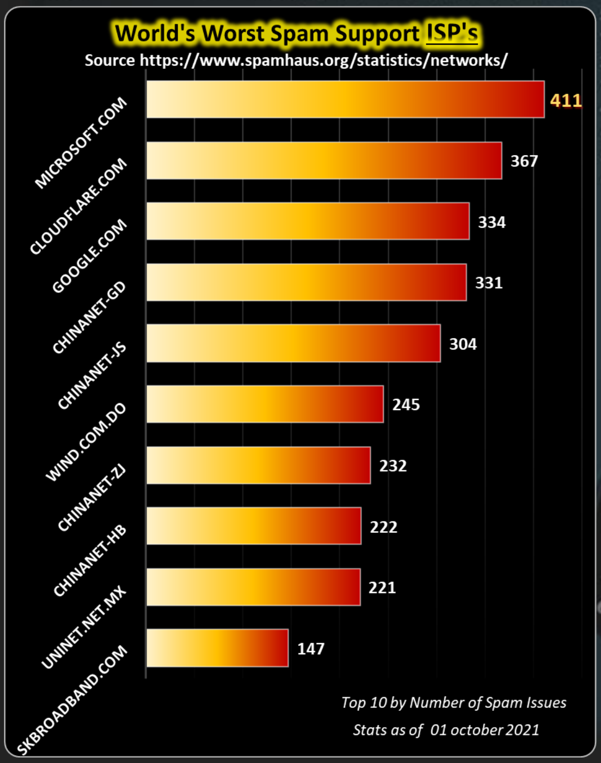
Cybersecurity researchers have disclosed an unpatched security vulnerability in the protocol used by Microsoft Azure Active Directory that potential adversaries could abuse to stage undetected brute-force attacks. "This flaw allows threat actors to perform single-factor brute-force attacks against Azure Active Directory (Azure AD) without generating sign-in events in the targeted organization's tenant," researchers from Secureworks Counter Threat Unit (CTU) said in a report published on Wednesday. Read the story here: The Hacker News

Notorious Spyware Tool Found Hiding Beneath Four Layers of Obfuscation

FinFisher (aka FinSpy) surveillance software now goes to extreme lengths to duck analysis and discovery, researchers found in a months-long investigation. FinFisher/FinSpy, the infamous and highly controversial commercial spyware sold by German firm FinFisher to nation-states and law enforcement for surveillance purposes, now wraps itself in four layers of obfuscation and other detection-evasion methods to elude discovery and analysis. It took researchers at Moscow-based security firm Kaspersky eight months of full-time reverse engineering and analysis to uncover this ultra-stealthy new version of the spyware for Windows, Mac OS, and Linux…. Read the full story here: Darkreading

World's Worst Spam Support ISP's

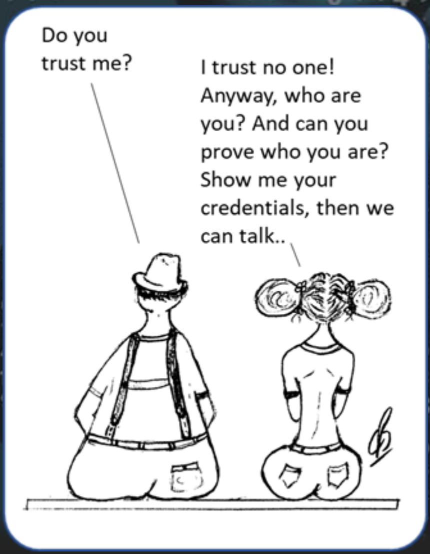
Source https://www.spamhaus.org/statistics/networks/



Top 10 by Number of Spam Issues

Stats as of 01 october 2021

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


Do you trust me?
I trust no one! Anyway, who are you? And can you prove who you are? Show me your credentials, then we can talk..

Zero Trust Model Explained

There has been a lot of talks lately on the subject of Zero Trust and the drive to get there. With President Joe Biden's endorsement and signing of the executive order that specifically states that the "Federal Government have to advance toward Zero Trust Architecture", the rest of the world is quickly following this direction. The threat landscape has changed dramatically over the last few years and with recent state-sponsored attacks focusing on the critical infrastructure of countries, the notion to "trust no one and verifying everything" is quickly becoming the standard response. But, what is the "Zero Trust Model" and how can it be implemented? With years of embedded trust models in current architectures, implementing a Zero Trust model is not as easy as one would think. But according to the experts, Zero Trust does not require that you get rid of all your current security controls. With some tweaking and careful planning, a Zero Trust model can be implemented without a massive rebuild and cost outlay.
The Microsoft paper on the Zero Trust Model explains the concept really well, below then is a short extract of the key points.

Zero Trust overview (Microsoft)

Instead of believing everything behind the corporate firewall is safe, the Zero Trust model assumes breach and verifies each request as though it originates from an uncontrolled network. Regardless of where the request originates or what resource it accesses, Zero Trust teaches us to "never trust, always verify." In a Zero Trust model, every access request is strongly authenticated, authorized within policy constraints and inspected for anomalies before granting access. Everything from the user's identity to the application's hosting environment is used to prevent breach. We apply micro-segmentation and least privileged access principles to minimize lateral movement. Finally, rich intelligence and analytics helps us identify what happened, what was compromised, and how to prevent it from happening again.

Guiding principles of Zero Trust:

(1) Verify explicitly. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

(2) Use least privileged access. Limit user access with Just-In-Time and Just-Enough Access (JIT/JEA), risk-based adaptive polices, and data protection to protect both data and productivity.

(3) Assume breach. Minimize blast radius for breaches and prevent lateral movement by segmenting access by network, user, devices, and application awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility, drive threat detection, and improve defences.

Controlling access with policy - Today, organizations need to be able to provide secure access to their resources regardless of user or application environment. Before we allow access, we want to assess a user's location, their role in the organization, the health of their device, the type of service and classification of the data they're requesting access to, and more. To do this effectively, we need to use signal and automated policy enforcement to deliver the right balance between security and optimal user experience.

A Zero Trust security model relies on automated enforcement of security policy to ensure compliant access decisions throughout the digital estate.

Building Zero Trust into your organization - A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy. This is done by implementing Zero Trust controls and technologies across six foundational elements: **identities, devices, applications, data, infrastructure, and networks**. Each of these six foundational elements is a source of signal, a control plane for enforcement, and a critical resource to be defended. This makes each an important area to focus investments.

Identities

Identities – whether they represent people, services, or IOT devices – define the Zero Trust control plane. When an identity attempts to access a resource, we need to verify that identity with strong authentication, ensure access is compliant and typical for that identity, and follows least privilege access principles.

Devices - Once an identity has been granted access to a resource, data can flow to a variety of different devices—from IoT devices to smartphones, BYOD to partner managed devices, and on-premises workloads to cloud hosted servers. This diversity creates a massive attack surface area, requiring we monitor and enforce device health and compliance for secure access.

Applications - Applications and APIs provide the interface by which data is consumed. They may be legacy on-premises, lift-and-shifted to cloud workloads, or modern SaaS applications. Controls and technologies should be applied to discover Shadow IT, ensure appropriate in-app permissions, gate access based on real-time analytics, monitor for abnormal behavior, control of user actions, and validate secure configuration options.

Data - Ultimately, security teams are focused on protecting data. Where possible, data should remain safe even if it leaves the devices, apps, infrastructure, and networks the organization controls. Data should be classified, labelled, and encrypted, and access restricted based on those attributes.

Infrastructure - Infrastructure (whether on-premises servers, cloud-based VMs, containers, or micro-services) represents a critical threat vector. Assess for version, configuration, and JIT access to harden defense, use telemetry to detect attacks and anomalies, and automatically block and flag risky behavior and take protective actions.

Networks - All data is ultimately accessed over network infrastructure. Networking controls can provide critical "in pipe" controls to enhance visibility and help prevent attackers from moving laterally across the network. Networks should be segmented (including deeper in-network micro segmentation) and real-time threat protection, end-to-end encryption, monitoring, and analytics should be employed.

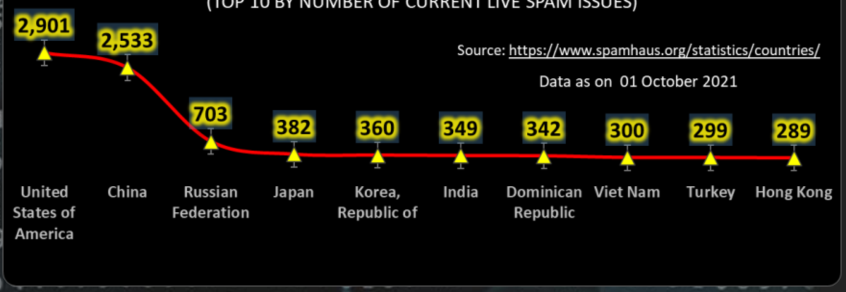
That is all I have space for in this post, please read the rest of the 7 page Microsoft Paper to get a full picture of Zero Trust.

Other Interesting News and Cyber Security bits:

- This Microchip With Wings Is The Smallest Flying Structure Humans Have Ever Built
- Zero Trust: Cybersecurity's next step
- Whitepaper: Effective Techniques for Robust OT Security

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 01 October 2021

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