On June 8, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Mozilla, Atlassian, and Google products. (No further update this week)
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
17 JUN 22	543,207,124	6,338,298

Deaths this week: 9,765

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
17 June 2022

In The News This Week

A Ragtag Band of Hackers Is Waging Cyberwar on Putin's Supply Lines

In Belarus, forces opposed to President Alexander Lukashenko have been derailing Russia's war against Ukraine. – Russia's military began sending large numbers of weapons and troops into Belarus in late January. The official purpose of the movement was a joint military exercise, but Belarus, which has a 650-mile border with Ukraine and a government closely aligned with Moscow, was also a logical staging point for Russian President Vladimir Putin to carry out an invasion. Several days after the troops arrived weird things started happening to the computer systems that ran the Belarus national railway system, which the Russian military was using as part of its mobilization. Passengers gathered on train platforms near Minsk, the capital, watched as information screens flickered and normal messaging was replaced by garbled text and an error message. Malfunctioning ticket systems led to long lines and delays as damaged software systems caused trains to grind to a halt in several cities, according to railway employees and posts that circulated on Belarusian social media. Read the rest of the story by Ryan Gallagher here: Bloomberg

Russia Warns Growing Cyber Conflict With U.S. Could Spark War in Real World

Russia's top cyber diplomat has warned that a worsening conflict with the U.S. in cyberspace could lead to a real-world escalation between the two powers as both sides vowed to strike back against any virtual provocations. Washington and Moscow have long denied conducting malicious cyber activities against one another, but U.S. Cyber Command Director General Paul Nakasone confirmed last week in an interview with Sky News that the Pentagon's cyber branch was involved in "a series of operations across the full spectrum," including those both "offensive" and "defensive" in nature, as well as "information operations," in support of Ukraine as it struggles to fend off a Russian incursion launched in February. Days after the senior U.S. military official's comments, Russian special presidential representative for cooperation in the field of information security Andrey Krutskikh accused the U.S. of having "unleashed cyber aggression against Russia and its allies" in an interview Monday with the newspaper Kommersant.... Read the rest by Tom O'Connor here: Newsweek

Anonymous Hits Russia With Devastating Drone Hack That Could Speed Up End Of War

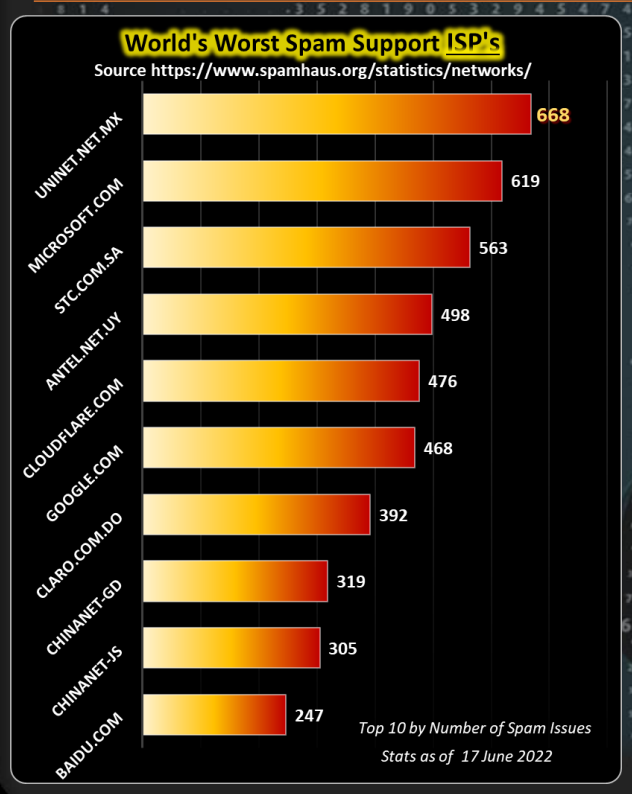
The ongoing war between Russia and Ukraine has seen drones play a more central role in combat, which could even influence outcome of the bloody conflict. Anonymous, the decentralized hacktivist collective and movement, which swore to fight Russia on the cyber front to punish the Kremlin for what it calls a "special military operation," has now hacked into a weapons company, which handles the Russian Unmanned Aerial Vehicles (UAV), getting its hands on tactics and plans. It was initially widely believed the Russian military would steamroll over Ukraine in a matter of days, but things didn't exactly go that way for President Vladimir Putin. While heavy western arms support and fierce Ukrainian resistance have played a visible role in derailing the Kremlin's plans, the cyber warfare carried out by Anonymous behind the scenes has played no less an important part. Following relentless attacks on Russia's government websites, businesses believed to be supporting the Kremlin, oligarchs and sycophants, Anonymous has now hit Russia's military force itself with the drone hack. The hack, announced on Twitter, allowed the Anonymous operative with the Twitter handle @Youanonspider, to obtain classified documents bearing information about Russia's drone plans and tactics, which the hacktivist collective hoped would "help the war to end as soon as possible." Read the rest of the article by Nica Osorio here: IBTimes

This new Android malware bypasses multi-factor authentication to steal your passwords

A newly discovered form of Android malware steals passwords, bank details and cryptocurrency wallets from users – and it does so by bypassing multi-factor authentication protections. The malware has been detailed by cybersecurity researchers at F5 Labs, who've dubbed it MaliBot. It's the latest in a string of powerful malware targeting Android users. In addition to remotely stealing passwords, bank details and cryptocurrency wallets, MaliBot can access text messages, steal web browser cookies and can take screen captures from infected Android devices. It can also get around multi-factor authentication (MFA) – one of the key cybersecurity defences people can use to protect themselves against cyber criminals. Like many Android malware threats, MaliBot is distributed by sending phishing messages to users' phones via SMS text messages (smishing) or attracting victims to fraudulent websites. In both cases, victims are encouraged to clink on a link, which downloads malware to their phone. After being downloaded, MaliBot covertly asks the victim to grant accessibility and launcher permissions... Read the post by Danny Palmer here: ZDNet

China's Opinion - Operation Black Hand: U.S. is the primary threat to global cyber security

CGTN, The English-language, state-run news channel based in Beijing, posted the following article this week stating an opinion on global cyber security. An interesting read... - It is hardly a secret that the United States has been running the largest, most expensive, highly intrusive, and outrightly unlawful global cyber warfare intelligence operations for decades, which have not even spared Washington's friends and allies. Way back in 2013, Edward Snowden leaked highly classified information revealing a labyrinthine of global surveillance programs, many run by the NSA ... Read the rest here: CGTN



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

BOLA Threat Unwrapped

Almost like the deadly Ebola virus (discovered in 1976 near the Ebola River in the Democratic Republic of Congo) which lead to the death of thousands of people, the BOLA vulnerability can lead to the digital invasion and critical disruption of applications and computer systems. BOLA or "Broken Object Level Authorization" is cited as one of the most critical API vulnerabilities on web applications today. The OWASP foundation listed Broken Access Controls as the number one threat to Web Applications in 2021, and Object Level Authentication is one of these controls that is widely open for abuse if not done correctly. The Open Web Application Security Project® (OWASP) Top 10 Web Application and API Security Risk listings are globally recognised measures for Application Security and are used by most developers as a focal point when it comes to security controls. OWASP is a non-profit foundation that works to improve the security of software through community-led open-source software projects. Now that you have all that information, let's unwrap and look at what the BOLA threat is.

Analogy

Cequence Security offer the following analogy; "Imagine it's a Friday night and you are out with your friends to the club. At the door, the bouncer asks you for your ID and lets all of you in. You go to the bar and order some drinks – it's a busy bar, so the bartender gives you a receipt with the number 30 on it to identify your order. After a while you are called to the bar, and you present your receipt, and the bartender hands you your drinks. You come back for a second round, and your friend decides it's time to have some fun – they change the 0 on the paper to a 6. You go to the bar, present your receipt again, and to your surprise there is an order number 36. The bartender hands you a bunch of free drinks and bam! The party is turned up a notch.

The above story is an apt analogy for two application security concepts: authentication and authorization. Authentication is "Who am I?" and authorization, also referred to as access control is used to determine "What I can do?" The bouncer lets you in after looking at your ID, which is you being authenticated to the system (aka the club). Later, when you manipulate the receipt from the bar, you are modifying the bars' authorization (what drinks you receive based on what you purchased). Security systems operate no differently.

In simple terms Broken Object Level Authentication can be defined as an authentication coding error that allows a rogue user to access objects that they should not have access to through manipulation of the object IDs. Broken Object Level Authorization (BOLA) gives attackers access to data they should not have and as such, ranks as the #1 threat in the OWASP Top 10 lists for both Web Application and API Security.

Broken Object Level Authorization

Antonia Din of Heimdal Security wrote "Broken Object Level Authorization (BOLA) vulnerability, often also referred to as Insecure Direct Object Reference (IDOR), is the most severe and most common API vulnerability today. Broken Object Level Authorization happens when an application does not correctly confirm that the user performing the request has the required privileges to access a resource of another user. Almost every company has APIs that are vulnerable to BOLA".

Impact of Broken Object Level Authorization (BOLA) in Cybersecurity (Heimdal Security)

Object level authorization is an access control mechanism that is usually implemented at the code level to validate that one user can only access objects that they should have access to. An object is any information to which the application has access. When an application includes a BOLA or IDOR vulnerability the application has a strong probability of exposing sensitive information or data to attackers. Once recognized, BOLA vulnerabilities can be exceptionally easy to exploit, frequently using simple scripting. All the attackers need to do is to exchange the ID of their own resource in the API call with an ID of a resource belonging to another user. The absence of proper authorization checks enables hackers to access the specified resource. This attack is also known as IDOR (Insecure Direct Object Reference). This issue is very common in API-based apps as a result of the server component not fully tracking the client's state, and instead, counting more on object IDs, that are sent from the client to determine which object to access.

There are two main types of Broken Object Level Authorization (BOLA): (1) Based on user ID - The API endpoints receive a user ID and access the user object based on this ID. For example: /api/trips/get_all_trips_for_user?user_id=777. It's usually easier to solve this type of BOLA because the authorization mechanism is straightforward — the developers simply fetch the ID of the logged-in user from the session (e.g.: `current_user.id`), and compare it with user_id from the GET parameter. Things get more complicated when one user is supposed to manage other users by design (for example sub-users, regional manager, etc). **(2) Based on object ID** - The API endpoint receives an ID of an object which is not a user object. For example: /api/trips/receipts/download_as_pdf?receipt_id=1111. - The reasons why we end up having Broken Object Level Authorization (BOLA) vulnerabilities in the code are quite simple: the lack of security control and human error. For example, an API that handles both sensitive and non-sensitive data. Some requests should have authorization checks and others shouldn't therefore it's easy to miss a check when writing code.

How to know if an API is vulnerable

It is in fact at risk in the following cases: **(1)** API includes an ID of the resource, either in the URI, the request headers, or the body. /api/restaurant1/financial_info. **(2)** API does not check permissions for the invoker to access the resource. The ID has a clear structure that can be something like /api/123/financial_info. - Current security scanning tools can't detect Broken Object Level Authorization (BOLA) vulnerabilities. They can't determine if a specific API endpoint should be authorizing a given user each time, this is a task for a human. It is crucial that all the APIs designers and developers are conscious of the vulnerability and are able to discover the existence of such vulnerability. Broken Object Level Authorization vulnerabilities must be identified during the code development process, through regular architecture reviews, code reviews, and evaluating API request logs.

Wrapping it up - Broken Object Level Authorization (BOLA) is a severe vulnerability, easy to notice and attack and prospective impacts are enormous. Trusting the information that is moved to the API by the customer is the origin of this vulnerability. Please check out the resources below to learn more and find ways to prevent BOLA exposure.

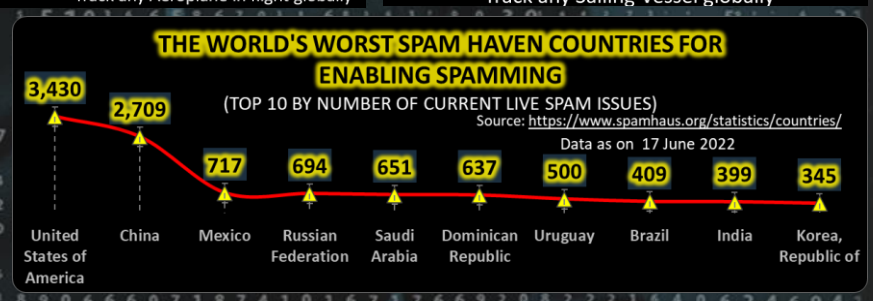
Resources: Heimdal Security, Cequence Security, OWASP, HowToGeek, Inon Shkedy

Other Interesting News and Cyber Security bits:

- Return to the office or else? Why bosses' ultimatums are missing the point
- 10 Most Advanced Military Drones in the World
- Microsoft acquires cyber security firm Miburo to spot foreign threats
- 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