cyber plural
...focus on cybersecurity

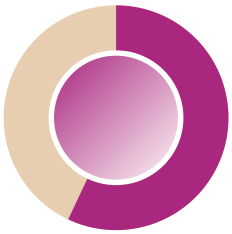
2022 | Q2 Report

Lessons Learnt - Cyber Incident Reports, Major CVEs & Threat Intel.

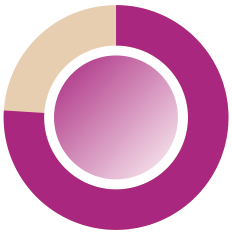
cyber plural
...focus on cybersecurity

cyberplural.com
hello@cyberplural.com

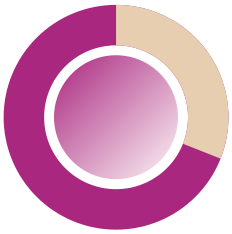
2022 | Q2 at a glance



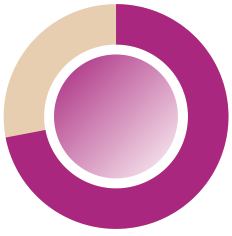
High / Critical CVEs such as Spring4Shell and Follina were reported in Q2 of 2022 with patches available for core technology products that organizations leverage in everyday business.



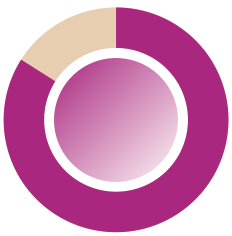
CNI of countries and businesses are the target of multiple breaches and ransomware attacks in Q2. CVEs from Q4 of 2021 and Q1 of 2022 are still been exploited. More African targets make it to the news such as Bet9ja and Shoprite Holdings.



Our Dark web HUMINT engagement reported several disruptions on forums and underground rooms since the inception of the Russian Invasion, many forums got shutdown by law enforcement



Our CTI Team revealed threat actors leveraging the Cobalt Strike Framework and other popular RAT within public institutions' networks in Nigeria.



Misconfiguration, Insecure Design and Lack of Proper logging and monitoring were identified as the top flaws of the security assessment conducted in Q2.

cyber plural
...focus on cybersecurity

Bet9ja Ransomware Incident.

2022 | Q2 Report

cyberplural.com

April 2022

Organizations Breached / Experienced Ransomware Attack

- Snap-on, a US-based automobile tools manufacturer
- German wind turbine company Nordex
- Back and forth Campaign Between Russia and Ukraine (Wipers, DDOS, Defacement)
- Bet9ja, Nigeria popular betting platform.

Critical CVEs Reported

- VMware Spring Core, Microsoft
- Apple, Cisco, Gitlab
- Zyxel, Google,
- Atlassian, Lenovo

Interesting Highlight

- Chinese state-sponsored APT10 group (aka Cicada) is targeting organizations globally with what appears to be a cyber-espionage campaign leveraging the VLC media player. Victims include government, legal, religious and NGO sectors
- The new Spring4shell vulnerability (CVE-2022-22965) has been actively exploited by threat actors since the beginning of April
- Docker servers are actively being targeted by the LemonDuck botnet to mine cryptocurrency on the Linux platform.
- CISA, the FBI and the US Treasury Department alert on the North Korean APT group Lazarus targeting companies in the blockchain and cryptocurrency sectors, using social engineering on employees.
- Several senior European Union officials have been allegedly infected with the Israeli NSO group Pegasus spyware. It is not clear at this time who is at the origin of these attacks nor which information was compromised

cyber plural
...focus on cybersecurity

BlackCat Ransomware with many lives become a prevalent threat.

May 2022

Organizations Breached / Experienced Ransomware Attack

- Costa Rica has declared a state of Emergency
- Lincoln College, a 157-year-old institution in Illinois
- Austrian federal state Carinthia
- The Parker Hannifin Corporation
- Indian airline SpiceJet
- Credential stuffing attack against General Motors

Critical CVEs Reported

- F5 BIG-IP Networking Device,
- Microsoft, Sonicwall, Mozilla,
- Google.

Interesting Highlight

- Threat analysts have revealed a recent campaign that uses the RIG Exploit Kit to deliver RedLine stealer malware – an info-stealing malware popular on the Russian Underground
- CISA and other international cyber authorities have released a joint advisory warning of possible threats aimed at managed service providers (MSP) and their clients.
- FBI warns of BlackCat ransomware after that breached over 60 organizations worldwide.
- Russia/Ukraine - Eastern Europe conflict affecting the dynamics of the Cyberspace | several wiper malwares targeting and destroying information have been reported.
- A new ransomware dubbed “Cheers” targeting VMware ESXi servers has been identified, used for used a double-extortion attacks.

cyber plural
...focus on cybersecurity

Ransomware Attack on Shoprite Holdings.

June 2022

Organizations Breached / Experienced Ransomware Attack

- Costa Rica's public health service was attacked by Hive ransomware
- The Italian municipality of Palermo
- Shoprite Holdings, Africa's largest supermarket chain
- Kaiser Permanente, a US based healthcare provider
- Shields Health Care Group, Massachusetts-based medical services provider

Critical CVEs Reported

- Google, Citrix, Zimbra Email,
- Microsoft, Apple, Android

Interesting Highlight

- Researchers revealed a zero-day vulnerability in Microsoft Office that enable remote code execution on a victim's machine. The vulnerability, dubbed "Follina"
- A global Interpol operation codenamed "First Light 2022" was conducted against crime groups behind telecommunications and social engineering frauds.
- The largest ever-recorded HTTPS DDoS attack has recently been mitigated, with 26 million requests per second.
- The BlackCat ransomware gang now has a website available to let their victims' customers and employees verify if their data was stolen in a ransomware attack.
- Online scamming fraud: 3 Nigerians arrested in INTERPOL Operation Killer Bee
- The Russian ransomware operation Conti has finally shut down its operation, a process that seems to have begun in May 2022.

2022 | Q2 Recommendations

- Using MFA for all user accounts - These days, passwords alone do not provide full protection on our accounts.
- Ensure your Vulnerability Management Program is active to capture all the applicable changes in terms of patches that are available for vulnerabilities identified in Q2.
- Invest in a cybersecurity awareness program that can measure users' behaviour improvement towards empowering them to become an element of defense for the organization.
- Proper network segmentation should be implemented across the enterprise and the necessary hardening of critical servers and other crown jewels.
- A review of all legacy applications, servers, and networks are required going into Q3 to ensure all risks are captured and mitigated around them.
- Proper implementation of a disaster and recovery plan should be implemented, and should from time to time tested to be sure it can serve its purpose when needed.
- Proactive monitoring & an effective incident response plan should be implemented to ensure visibility and effective handling of identified security incidents.
- Breach & Attack simulation activities, Purple teaming engagement, and drills can help identify gaps in security control's effectiveness, people and process ahead of threat actors.
- Continuous review of third party relationships and contracts is mandated for all organizations to ensure gaps that can cost the security of data are all checkmated at all time .

We help startups and enterprises create and manage resilient cybersecurity plans and implementation across board while they focus on profit-making and business growth.

Do you need help with any of the recommendations, feel free to consult and use our services.

Contact US

web

cyberplural.com

email

hello@cyberplural.com

blog

blog.cyberplural.com

social

cyberplural

#BeProactive