cyber plural
...focus on cybersecurity

2022 | Q1 Report

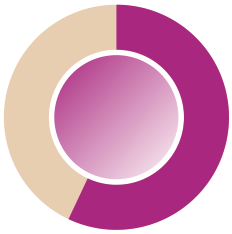
Lessons Learnt - Cyber Incident Reports, Major CVEs & Threat Intel.

cyber plural
...focus on cybersecurity

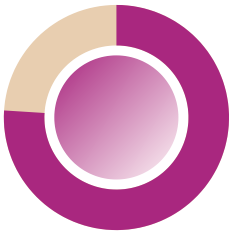
cyberplural.com
hello@cyberplural.com

cyber plural
...focus on cybersecurity

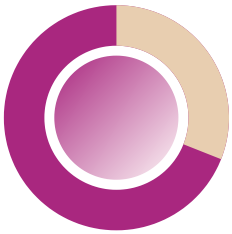
2022 | Q1 at a glance



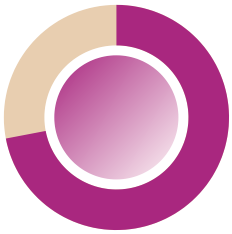
High / Critical CVEs were reported in Q1 of 2022 with patches available for core technology products that organizations leverage in everyday business.



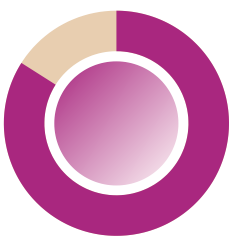
Critical National Infrastructure (CNI) and big businesses are targets of multiple breaches and ransomware attacks in Q1. CVEs from Q4 of 2021 are still been exploited



Dark web HUMINT engagement reported threat actors claim to have data of Nigerian organizations that are put up for sale.



CTI activities revealed several digital infrastructures in Nigeria are susceptible to opportunistic hacking as old CVEs in legacy applications and unpatched vulnerabilities can be leveraged.



Misconfiguration, Insecure Design and Lack of Proper logging and monitoring identified as top flaw of web applications tested in Q1.

cyber plural
...focus on cybersecurity

Members of the REvil ransomware group arrested.

cyber plural
...focus on cybersecurity

January 2022

Organizations Breached / Experienced Ransomware Attack

- Vietnamese trading platform ONUS
- Photography Company Shutterfly
- QNAP network-attached storage (NAS)
- UK Spar wholesaler James Hall & Co
- US Police Department
- Education FinalSite
- German defense contractor Hensoldt
- Central Bank of Indonesia

Critical CVEs Reported

- Apache, Netgear, VMware,
- Apple, Microsoft, Zoho.
- Cisco, McAfee Enterprise.

Interesting Highlight

- FIN7 hackers have been sending malicious USB devices through the US postal services, hoping to infect organizations in the transportation, insurance and defense industries.
- Interpol and the Nigerian Police Force arrested 11 suspects connected to an international business email compromise (BEC) campaign that targeted over 50,000 victims.
- Russia's Federal Security Service (FSB) arrested several members of the REvil ransomware group
- North Korean APT group Lazarus is using the Windows Update client as a living-off-the-land tool, to run malicious code on Windows in an email phishing campaign masquerading as job offers

cyber plural
...focus on cybersecurity

Eastern Europe conflict affecting the dynamics of the Cyberspace.

2022 | Q1 Report

cyberplural.com

February 2022

Organizations Breached / Experienced Ransomware Attack

- A significant ransomware attack disrupted operations of oil port terminals in Belgium, Germany and in the Netherlands. 17 Ports!
- German sportswear company Puma
- British food company KP Snacks
- Email accounts of News Corp journalists were hacked as part of an espionage campaign.

Critical CVEs Reported

- Cisco, Samba software,
- Apple, WordPress, Mozilla,
- Google, Zabbix, Okta Advanced Server Access Client.

Interesting Highlight

- Microsoft announced that the Office VBA macro feature, exploited in numerous cyberattacks, will soon be blocked by default
- Threat actors started a campaign using fake Windows 11 upgrade installers to users of Windows 10, where victims are lured into downloading and executing the password-stealing malware.
- Russia/Ukraine Conflict Buildup - Organizations warn to increase vigilance and resilience due to the high risk of being targeted by foreign influence campaigns, with misinformation, disinformation and malformation (MDM) tactics.
- Russia/Ukraine - Eastern Europe conflict affecting the dynamics of the Cyberspace | Hacktivists, cybercriminals and white hat researchers are picking a clear side.
- US-based Chipmaker NVIDIA was hit by a cyber-attack impacting their developer tools and email systems

cyber plural
...focus on cybersecurity

LAPSUS$ hacking group breached Microsoft, Okta and others.

cyber plural
...focus on cybersecurity

March 2022

Organizations Breached / Experienced Ransomware Attack

- NVIDIA leak by the LAPSUS$ hacking gang
- Swedish camera company Axis
- Conti Ransomware internal chats leaked
- Romanian gas station chain Rompetrol
- UK ferry operator Wightlink breached
- TransUnion South Africa breached
- Russia's largest meat producer Miratorg Agribusiness Holding
- Morgan Stanley customer breached

Critical CVEs Reported

- Schneider and GE Digital's SCADA Software,
- Linux Kernel (Dirty Pipe),
- Azure (AutoWarp), APC UPS,
- ClickHouse DBMS,
- Sophos, VMware, Google

Interesting Highlight

- The Log4Shell flaws are still exploited by threat actors to deploy various malware payloads, but mostly for DDoS botnets and planting crypto miners.
- DDoS attack targeted several Israeli Government websites.
- Large companies including Microsoft, Okta, NVIDIA, Samsung & Ubisoft have been breached by the LAPSUS$ hacking group
- UK Police announced having arrested 7 teenagers, aged 16 to 21 years old, suspected of being behind the LAPSUS$ hacking group.
- Google acquire Mandiant, Siemplify
- Several data wiper malware has been identified to be targeting and used in the ongoing cyber conflict in eastern Europe. They are designed to damage targeted systems by deleting data, programs, and drives.

2022 | Q1 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 Q1.
- 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 Q2 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