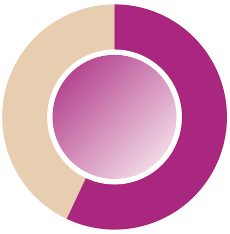
2022 | Q3 Report

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

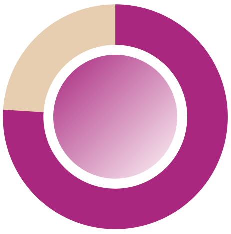
cyberplural.com

hello@cyberplural.com

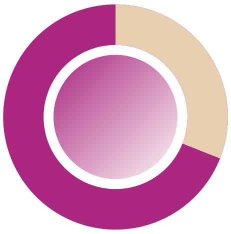
2022 | Q3 at a glance



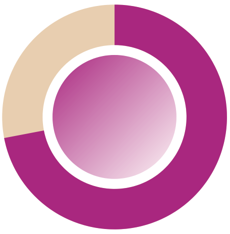
Several unreported incidents hit Nigerian businesses, as many continue to treat cybersecurity incidents as IT-related problems. This has resulted in huge downtime of services and financial loss for affected businesses.



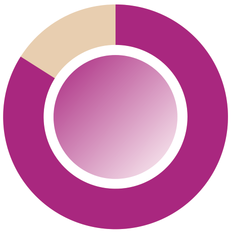
CVEs from Q4 of 2021 and Q1, Q2 of 2022 are still been exploited. CNIs of countries and businesses are the target of multiple breaches and ransomware attacks in Q3. Government-wide network attacks and breaches become prevalent.



Our Dark web HUMINT engagement reported the proliferation of new tools and upgrades to existing and new variants of ransomware from Ransomware groups. Invitation-only forums focused on initial access are also been leverage by cyber criminals.

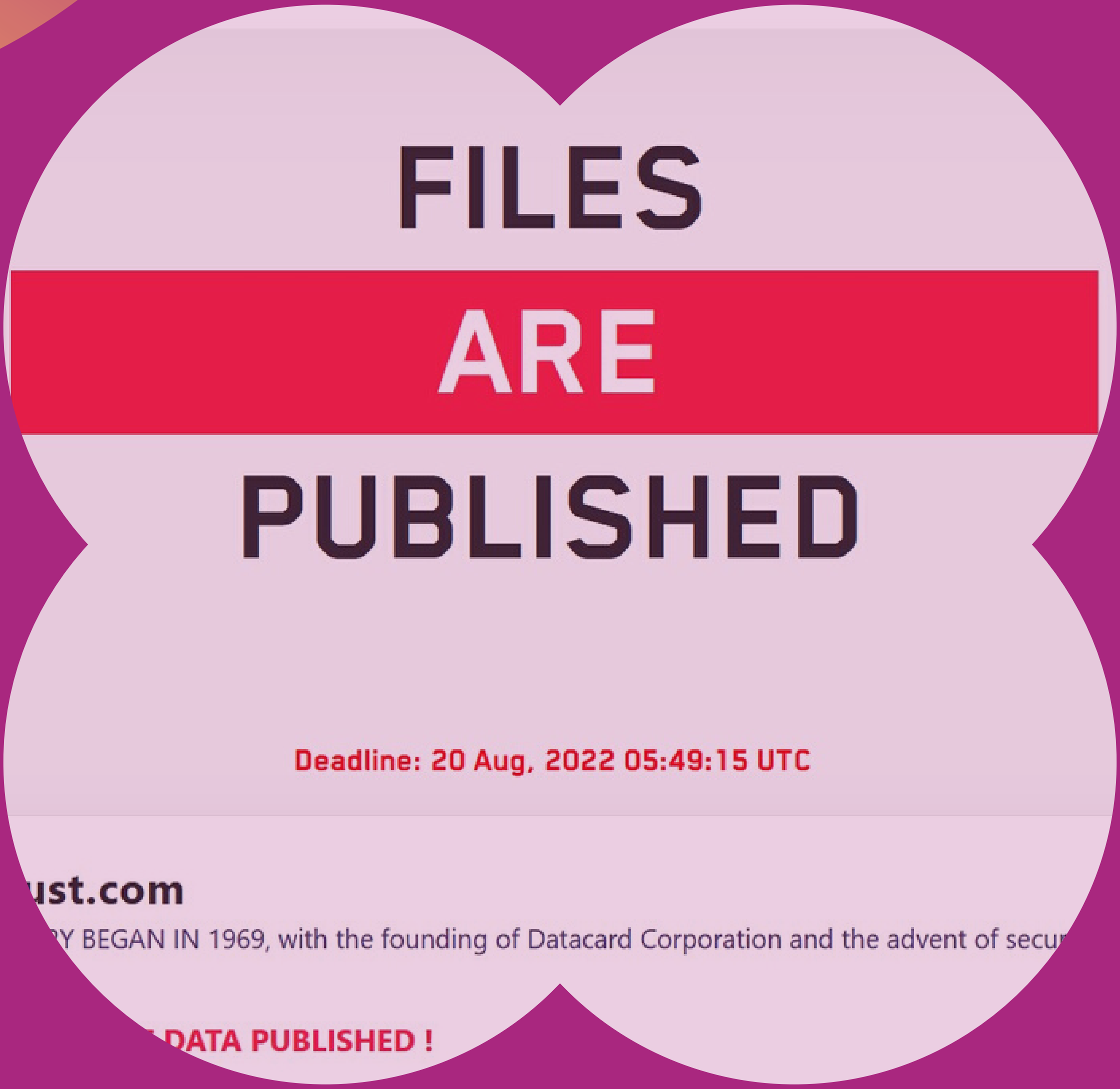


Our Threat Intelligence Team came across a server on the Internet serving critical information identified to be related to businesses and organizations that are more focused on finance / FinTech in Nigeria.



A relatively new social engineering technique known as "MFA Fatigue" has been successfully used to compromise employee accounts at large corporations like Uber, Microsoft, and Cisco.

Digital security giant Entrust breached by Lockbit.



FILES

ARE

PUBLISHED

Deadline: 20 Aug, 2022 05:49:15 UTC

ust.com

Y BEGAN IN 1969, with the founding of Datacard Corporation and the advent of secu

DATA PUBLISHED !

July 2022

Organizations Breached / Experienced Ransomware Attack

- Finland-based company Wartsila
- Federal Electricity Commission (CFE) of Mexico
- US chipmaker giant AMD
- Iranian steel manufacturing plants
- Entrust

Critical CVEs Reported

- Zoho ManageEngine ADAudit Plus
- Atlassian, Gitlab
- SonicWall, Mozilla
- Django, Jenkin
- older AMD and Intel microprocessors

Interesting Highlight

- LockBit added several new companies to their victims' list, including Madco Energi, Clestra, COIC Fiber, Columbia Grain, FarmaOffice, Christiana Spine Center, Rogagnati, and Redox Brands
- Windows 11 is getting new security setting to block connections and lock machines attacked by RDP password brute-force, a method often used by ransomware operators
- Researchers published a report covering the activity of several nation-state hacking groups routinely targeting, and masquerading as, journalists and media organizations
- RaaS group Lockbit released version 3.0 of their ransomware. Among its new features is a bug bounty program, promising monetary rewards to those who can find security flaws in the group's ransomware.

cyber plural
...focus on cybersecurity

Cisco breached, attackers leveraged MFA Fatigue.

cyber plural
...focus on cybersecurity

August 2022

Organizations Breached / Experienced Ransomware Attack

- Italy's tax agency, the Internal Revenue Service (IRS)
- Taiwanese government websites
- Semikron, a German manufacturer of power modules and systems
- Cisco, LastPass confirms breached
- 7-Eleven Denmark
- South Staffordshire Water, UK's largest water company
- Plex streaming service

Critical CVEs Reported

- VMware, Apple, Amazon
- General Bytes Bitcoin ATM servers
- Atlassian
- Gitlab, Mozilla

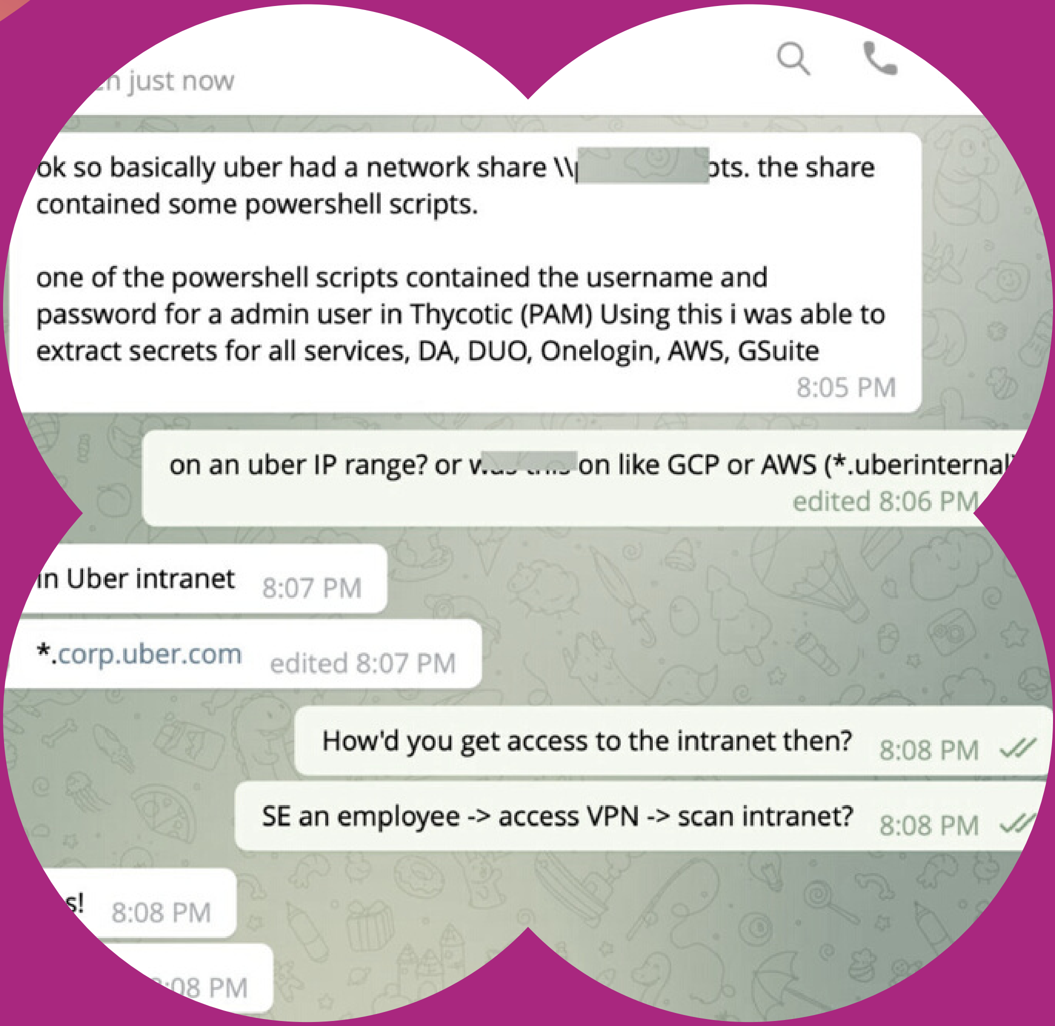
Interesting Highlight

- Montenegro suffered a large-scale cyber attack, affecting multiple government services. According to some sources, it potentially affected critical infrastructure, transportation and telecommunications
- Researchers warn of the increasing popularity of the 'Dark Utilities' platform, which offers C&C-servers-as-a-service for its customers. Threat groups have been observed to be using this service, which is capable of targeting multiple operating systems, to avoid having to create and maintain their own C&C server infrastructure.
- Reports detailing the threat of emerging ransomware variants BlueSky and Black Basta were published. Active since 2022, analysts estimate these threats to gain popularity in the upcoming months.
- Phishing campaign dubbed Oktapus on Cloudflare and Twilio revealed points to 9,000 accounts were affected in over 130 organizations

cyber plural

...focus on cybersecurity

Uber hack announced on the company's own Slack Platform.



h just now

ok so basically uber had a network share \\[redacted]pts. the share contained some powershell scripts.

one of the powershell scripts contained the username and password for a admin user in Thycotic (PAM) Using this i was able to extract secrets for all services, DA, DUO, Onelogin, AWS, GSuite

8:05 PM

on an uber IP range? or [redacted] on like GCP or AWS (*.uberinternal

edited 8:06 PM

in Uber intranet 8:07 PM

*.corp.uber.com edited 8:07 PM

How'd you get access to the intranet then? 8:08 PM

SE an employee -> access VPN -> scan intranet? 8:08 PM

s! 8:08 PM

:08 PM

September 2022

Organizations Breached / Experienced Ransomware Attack

- Damart, a French clothing company
- The Portuguese airline company TAP Air Portugal
- Italy’s energy agency Gestore dei Servizi Energetici SpA (GSE)
- The clothing company The North Face
- Uber suffered a data breach
- The legislature of Argentina’s capital city
- Los Angeles Unified School District (LAUSD)

Critical CVEs Reported

- Apple, Microsoft, Google.
- HP Support Assistant
- WordPress plugin BackupBuddy

Interesting Highlight

- Microsoft announced plans to disable basic authentication in Exchange Online tenants worldwide in order to improve security and make it more difficult for threat actors to steal sensitive information using man-in-the-middle attacks
- Two zero-day vulnerabilities in Microsoft Exchange have been disclosed, with reports of exploitation in the wild. These vulnerabilities allow an authenticated user to gain RCE capability on exchange servers.
- North Korean APT group Lazarus (aka APT28) was found to be targeting energy providers across the globe, in an espionage campaign exploiting the log4shell vulnerability on VMware Horizon as initial access
- A potential LinkedIn social engineering campaign was discovered, in which threat actors created a network of fraudulent profiles of CISO executives in fortune 500 companies.

2022 | Q3 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 Q3.
- 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 .

cyber plural

...focus on cybersecurity

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