CyberPlural MSSP

2022 CYBERPLURAL ANNUAL REPORT

consist of findings from each quarter of 2022 with insight into major incidents as observed by our team during incident response, and threat intel Ops as well as outline of cyber outlook for 2023

www.cyberplural.com

hello@cyberplural.com

Executive summary

At CyberPlural where we facilitate practices and teams that are devoted to preventing, detecting, assessing, monitoring, and responding to cybersecurity threats and incidents. We are proud and excited to present to you the first edition of our annual report detailing security incidents, and trends, alongside the impact and changes of Nigeria's cyberspace

We started into the year by providing quarterly reports of what was happening with the cyber threat landscape based on what we are seeing across the globe, and those happening within Nigeria's cyberspace as observed based on threat intelligence, incident response, and proactive monitoring activities carried out by our team from environments leveraging our MSSP services.

We never relent as we move up into the year, and now we are ending it with a big report that brings together these findings and how they can be leveraged going into the new year of 2023.

Stepping into 2022, was with the announcement of the Log4J and several other Microsoft Exchange-related vulnerabilities that are still being exploited up until now which is the Q4. This report contains an instance of massive scans and exploitations of the Log4J on Internet-facing servers of organizations in Nigeria, which lasted for 3 weeks. One interesting thing is that we continued to have new vulnerabilities uncovered as well as instances of patches for the new and old ones made available.

We touched on how legacy systems; crack software and applications were aiding the activities of cyber criminals and how such systems have aided the successful execution of dangerous cyber-attacks. The likes of ransomware as experienced at the individual and organizational level, usage of command and control (C2) such as Cobalt Strike were also identified as a part of the campaign that leverage such vulnerable systems that are internet-facing.

New techniques were also observed and captured around how social engineering attacks like phishing are being delivered today. Where IPFS were used to host credential harvesting scripts targeting organizations and the use of info stealer malware/trojan like redline, and snake oil attached to phishing emails were identified as part of investigated incidents on several occasions.

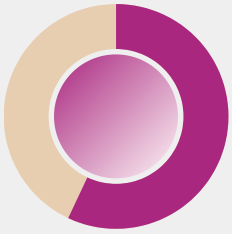
Leveraging our Cyber Threat Intelligence Platform (CyberTIP), we came across campaigns; one targeting Nigerian financial institutions and startups playing within the Nigerian FinTech space. The server was found hosting a large chunk of active reconnaissance info of over 30 organizations within the fintech and traditional banking space. Our HUMINT engagement also found several leakages of data consisting majorly of Personally Identifiable Information (PII) across schools and microfinance banks in Nigeria.

Ransomware and cryptocurrency stealer malware are in the big league in 2022. This report detailed how ransomware groups are not only encrypting victims' data for money but now targeting credentials stored in browsers, files and other sensitive places using info stealer malware. We also observed a wide range of cyberattacks involving cryptocurrency exchange, wallet and bridge that have been used just this year to steal millions of dollars in crypto.

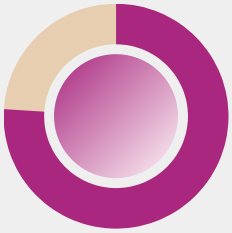
We hope you do enjoy the rest of our findings by going through the report.

Let us start with the last quarter of 2022

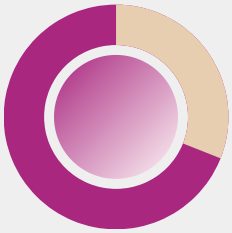
2022 | Q4 at a glance



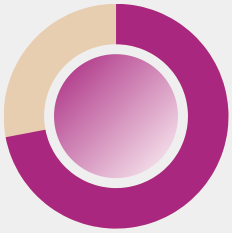
CVEs from Q4 of 2021 and Q1, Q2 and Q3 of 2022 are still been exploited. Critical National Infrastructure (CNI) of countries and businesses continue to be the target of multiple breaches and ransomware attacks in Q4.



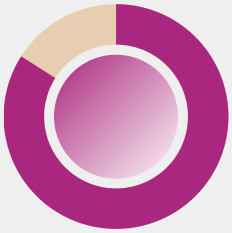
Certain threat actors or groups are now going around with phishing campaigns targeted at businesses /organizations in Nigeria. Hosted their novel script that will harvest unsuspecting users' credentials on IPFS.



From phishing scams to backdoor breaches, a wide range of cyberattacks have been used just this year to steal millions of dollars in crypto. Interesting was the use of crypto stealer malware targeting crypto platform extensions in browsers.



TA was observed to be scanning for and attempting exploitation for initial access vulnerabilities such as Log4j, and Exchange vuln; across organizations in Nigeria with combined pressure by leveraging social engineering through phishing emails containing info stealer malware.

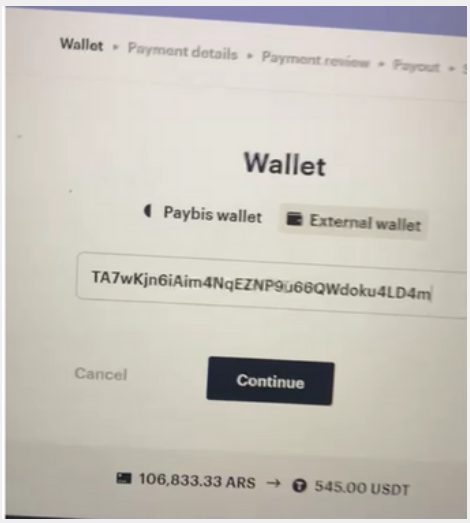


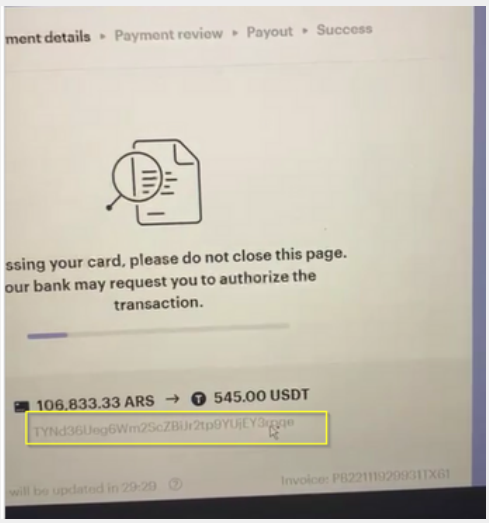
Several unreported incidents involving misconfiguration of cloud infrastructure and insecure applications design have led to breaches of confidentiality, availability and integrity within the startup space.

Crypto Stealer Campaign – Targeting Crypto Platforms Extension in Browsers

What an unbelievable event for this user, who became a victim of a crypto stealer campaign when a sum of $900 worth of USDT meant to be sent to a friend ended up stolen by changing the wallet for which it was destined.

Yes, you heard us right. This user copied the right wallet detail and pasted it on the crypto platform for payment, but since the campaign had this system compromised, they were able to change the wallet to theirs in the process and it became the final destination for the payment.





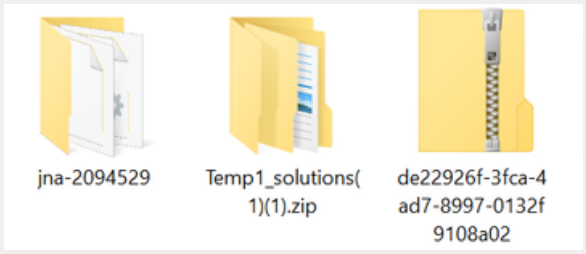
How were they able to pull this off?

And what are the possible MOs of this campaign has understudied by our team in the process of responding to this incident?

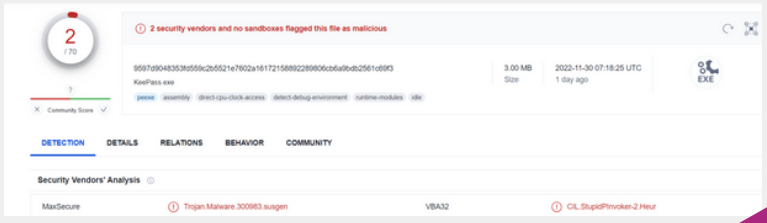
Digging down into the victim's computer to understand how that happened; we found some interesting conversations PowerShell was having as shown below.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
powershell.exe	42780	TCP	Close Wait	10.128.30.54	64283	199.59.243.222	80	11/30/2022 1:54:05 PM	powershell.exe
powershell.exe	36672	TCP	Close Wait	10.128.30.54	64284	199.59.243.222	80	11/30/2022 1:54:05 PM	powershell.exe
powershell.exe	42780	TCP	Close Wait	10.128.30.54	64313	85.94.194.169	80	11/30/2022 1:54:08 PM	powershell.exe
powershell.exe	36672	TCP	Close Wait	10.128.30.54	64314	85.94.194.169	80	11/30/2022 1:54:08 PM	powershell.exe
powershell.exe	31892	TCP	Close Wait	10.128.30.54	64323	199.59.243.222	80	11/30/2022 1:54:26 PM	powershell.exe
powershell.exe	31892	TCP	Close Wait	10.128.30.54	64338	85.94.194.169	80	11/30/2022 1:54:29 PM	powershell.exe
powershell.exe	42780	TCP	Close Wait	10.128.30.54	64343	192.64.119.130	80	11/30/2022 1:54:36 PM	powershell.exe
powershell.exe	36672	TCP	Close Wait	10.128.30.54	64344	192.64.119.130	80	11/30/2022 1:54:36 PM	powershell.exe
powershell.exe	31892	TCP	Established	10.128.30.54	64358	192.64.119.130	80	11/30/2022 1:54:57 PM	powershell.exe

Other interesting executable and JavaScript files were located in temp folders in the User\AppData\Local\Temp and program folder as related to the incident.

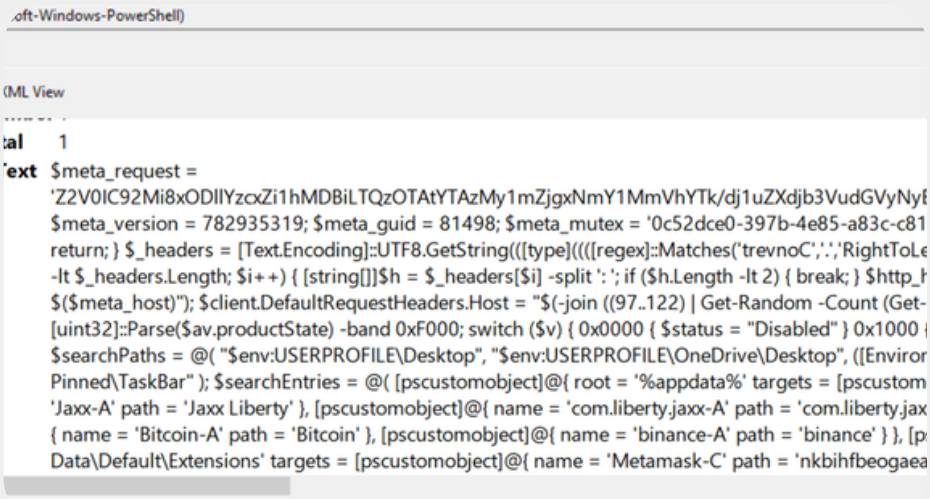


The folder **de22926f-3fca-4ad7-8997-0132f9108a02** was found to contain the **KeePass executable** as shown below and the file is currently being flagged by a few engines on VT



Analysis of what we have in the other folder which is various **.dll** files observed to be stealer malware from behaviour and not currently being flagged by any engine on VT as shown below.

To better understand how they all fit into the puzzle of the stunt that made the destination wallet during the payment to change to another thing entirely, we started by checking the PowerShell logs to see what we can find.



Over 118 events relating to Event 4104 were filters in the logs meaning the PowerShell has been executing remote commands and other errors related to failed resolutions of some random **.xyz** domain the PowerShell was trying to resolve.

We were able to collect the ScriptBlockText from the log indicating what the PowerShell was doing every time such remote calls were made.

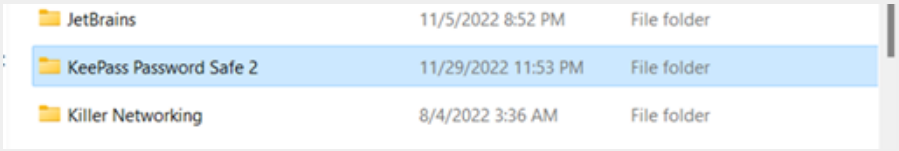
This script was found to contain different functions such as **WMI, Test-Unicode, GetAvStatus, Get-InstallStatus, Get-Apps, Get-UserInfo, Get-UserID, Get-Updates, Set-Updates, f6.**

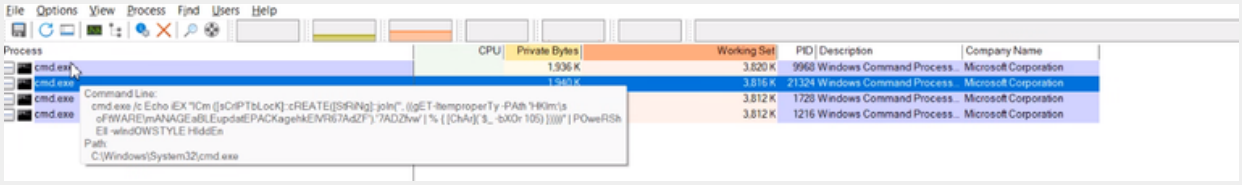
Looking through each of these functions made obvious what they will be doing and the information they will be collecting and looking out for on the infected system such as system information, user information, cryptocurrency-related extensions installed on browsers, a certain type of browsers (such as Chrome, MSEdge, Brave and Opera) and antivirus status.

On the side is the colouration of the script pointing to some of the above-mentioned functions and some interesting directories where searches and installation were done, cryptocurrency platforms (Binance, MetaMask, Coinbase, Coin98, MEWcx, Coinomi) whose users were being targeted.

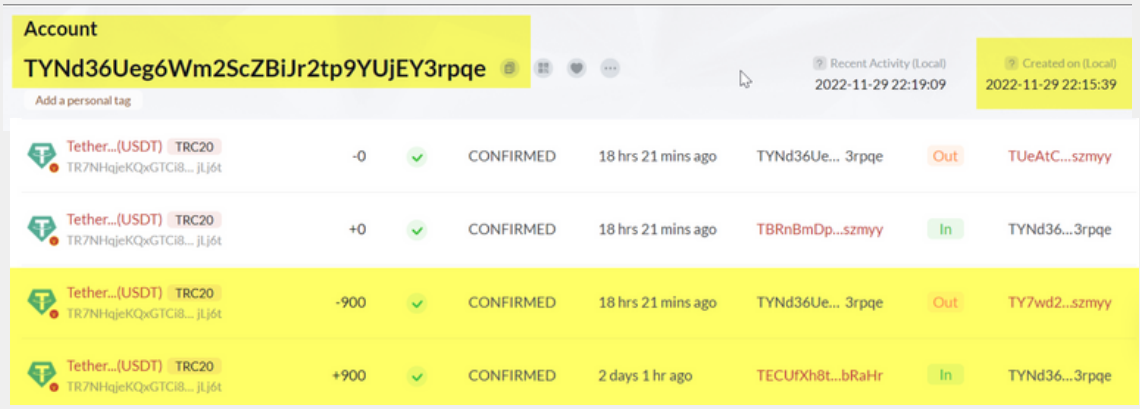
The MetaMask extension was found to be present in the Google Browser of this specific case during the response. A pointer to why the attacker might have succeeded with their stunt with this victim.

Identification and analysis of the script pointed us in the direction of finding other possible changes that might have been made on the compromised system; such as those in various system directories and registries to ensure complete removal to bring the system to its clean state and prevent further reoccurrence.





The specific campaign wallet was found to be a Tether (USDT) wallet and tracked to understand what happened to the sent token as shown below.



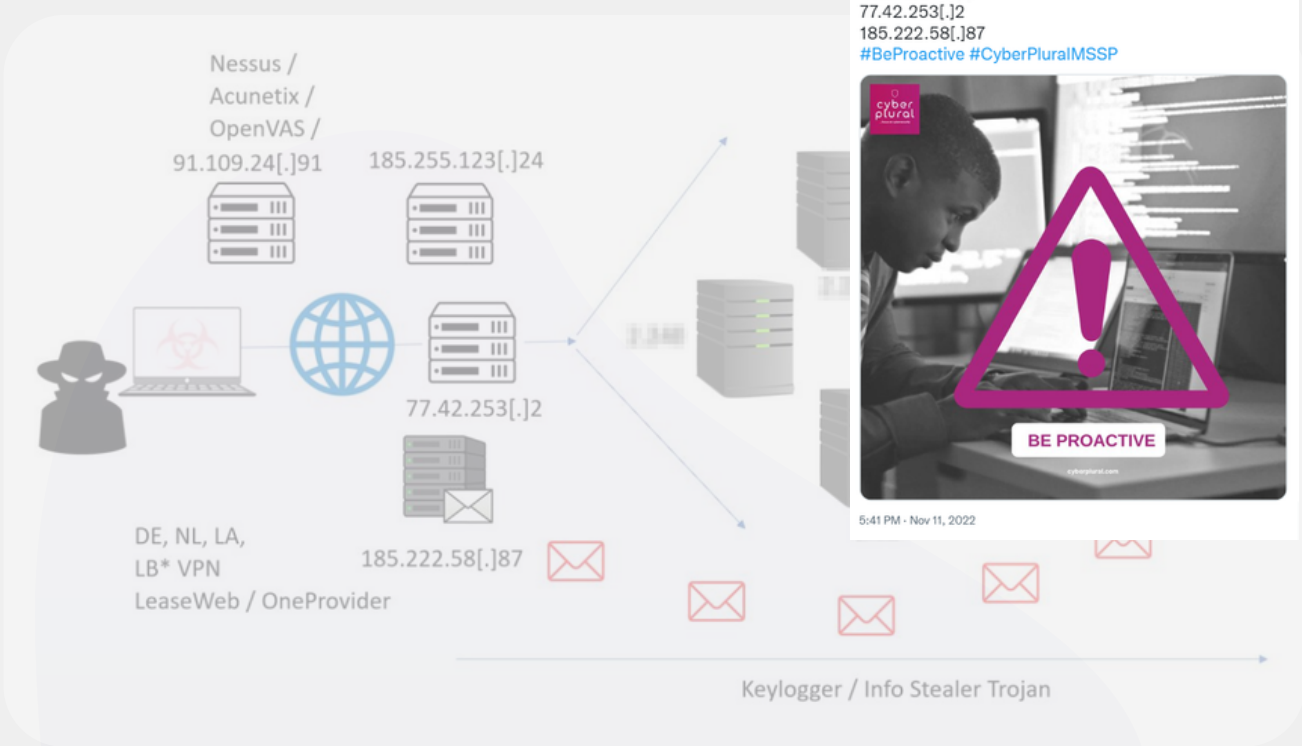
After initial compromise, the campaign was able to maintain persistence and evade detection by leveraging Living off the Land (LOL) TTPs by hiding behind PowerShell, WMI, CMD (wscript, cscript) and Browser, Browser Extensions (which are legitimate applications).

Our conclusion is that the affected user might have downloaded stuff relating to crack software in recent times that allowed the campaign to compromise the system and end up attaining their action on objectives of stealing crypto tokens, related information to the user, credentials and the system in general.

Indicator of Compromise (IOCs)

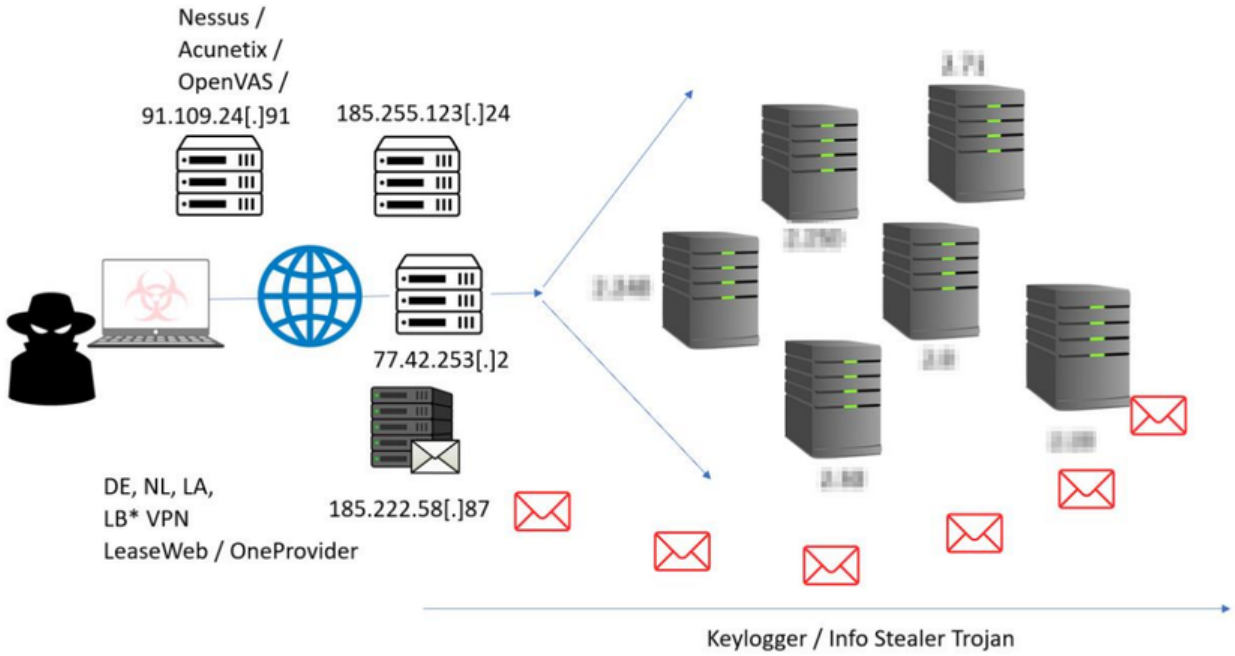
199.59.243[.]222, 85.94.194[.]169, 192.64.119[.]130
HKLM\SOftware\ManageableUpdatePackagehkEIVR67AdZF
HKLM\SOftware\ManageableUpdatePackageHKEivr6
HKLM\SOftware\cvsMXPStjtw
HKLM\SOftware\WinRAR8TEZMIuUj
User\AppData\Local\Temp\de22926f-3fca-4ad7-8997-0132f9108a02
Program Files (x86)\KeePass Password Safe 2
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b8 (SHA256)

The Tale of A Persistent Threat Actor – OPs



It is the case with the activities of the threat actor (TA) / group that our team observed for almost 3 weeks in the month of November. During this period (starting from the second week of November), our observations revealed the interest of the threat actor/group which was to gain initial access leveraging possible vulnerabilities on the Internet-facing assets.

The Tale of A Persistent Threat Actor – Monitoring OPs



The benefit that comes with having visibility (proactive monitoring) in and around your organization's network perimeter cannot be underestimated in cyber defense and understanding the concept of normal and abnormal activities within your visibility context will always put the defense team a step ahead of the bad guys.

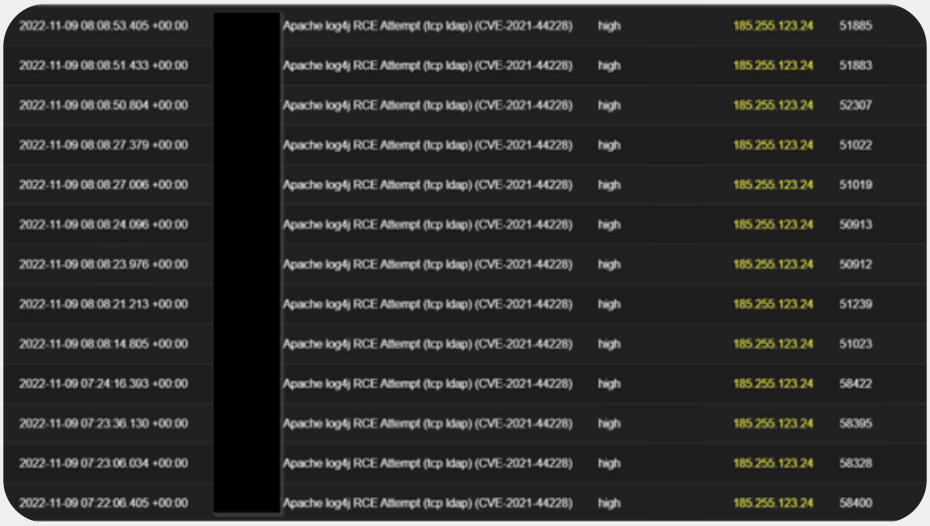
It is the case with the activities of the threat actor (TA) / group that our team observed for almost 3 weeks in the month of November. During this period (starting from the second week of November), our observations revealed the interest of the threat actor/group which was to gain initial access leveraging possible vulnerabilities on the Internet-facing assets.

Other than just looking for vulnerabilities that could be leveraged, the threat actor/group was also pushing through social engineering. By sending phishing emails to some list of curated users within the target users' space, which were found to contain info stealers malware (malware designed to steal user credentials on browsers, in files and generally all that could be found on the infected system) when analyzed.

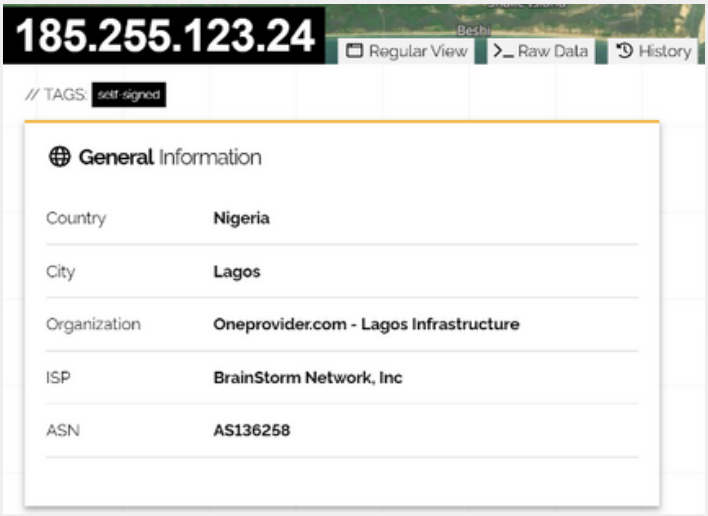
The monitoring OPs took a careful look at all activities in the first week and they started drafting what the attacker infrastructure might look like by trying to connect all related activities, alongside a possible tempo that might give out a trend to watch out for going forward.

Week One

At first, we observed the following foreign IPs; 185.255.123[.]24 and 77.42.253[.]2 to be scanning and attempting exploitation of initial access vulnerabilities like Apache Log4j on some internet-facing servers, where it majorly focused on one server for persistent scan and attempts; where we noticed the TA to have been consistent with his attempt all through the week.

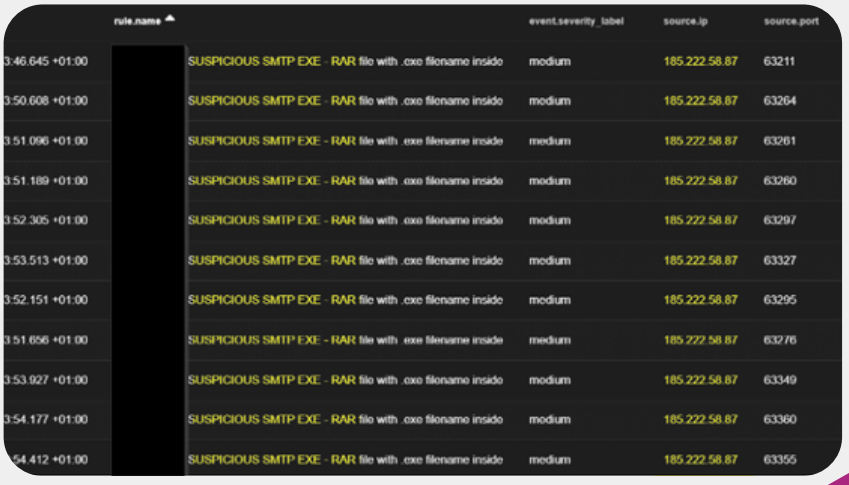


2022-11-09 08:08:53.405 +00:00	[redacted]	Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	51885
2022-11-09 08:08:51.433 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	51883
2022-11-09 08:08:50.804 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	52307
2022-11-09 08:08:27.379 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	51022
2022-11-09 08:08:27.006 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	51019
2022-11-09 08:08:24.096 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	50913
2022-11-09 08:08:23.976 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	50912
2022-11-09 08:08:21.213 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	51239
2022-11-09 08:08:14.805 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	51023
2022-11-09 07:24:16.393 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	58422
2022-11-09 07:23:36.130 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	58395
2022-11-09 07:23:06.034 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	58328
2022-11-09 07:22:06.405 +00:00		Apache log4j RCE Attempt (tcp ldap) (CVE-2021-44228)	high	185.255.123.24	58400



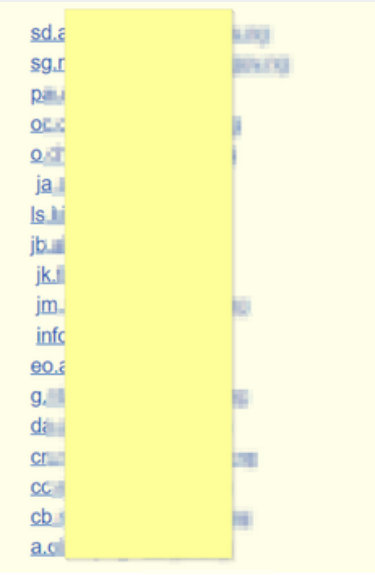
The most interesting thing with one of these foreign IPs is that it was indicating Nigeria as its origin when we decided to have a look into it, but we will tell you what the attacker was trying to do with that. We observed attacker brought part of its infrastructure closer to the target to remain undetected by leveraging cloud infrastructure with assets in Nigeria.

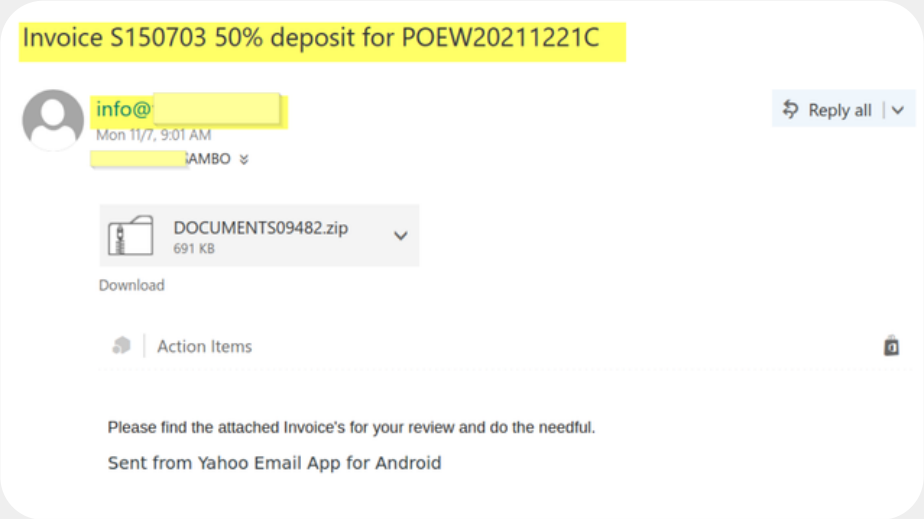
The first series of emails were received on the Monday 7th November 2022 the first week, where we observed this foreign IP 185.222.58[.]87 as captured in the image below to have sent suspicious attachments in a phishing email from info@target-org-domain to various users' inbox (18 different users email received this email) as listed below.

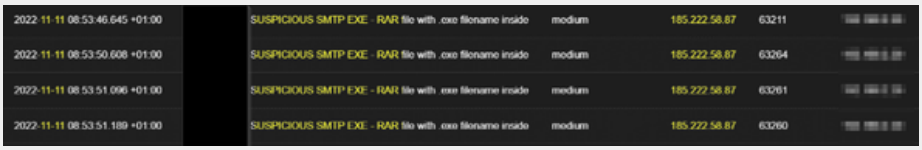


	rule.name	event.severity_label	source.ip	source.port
3:46.645 +01:00	[redacted] SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63211
3:50.608 +01:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63264
3:51.096 +01:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63261
3:51.189 +01:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63260
3:52.305 +01:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63297
3:53.513 +01:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63327
3:52.151 +01:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63295
3:51.656 +01:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63276
3:53.927 +01:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63349
3:54.177 +01:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63360
54.412 +01:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	63355

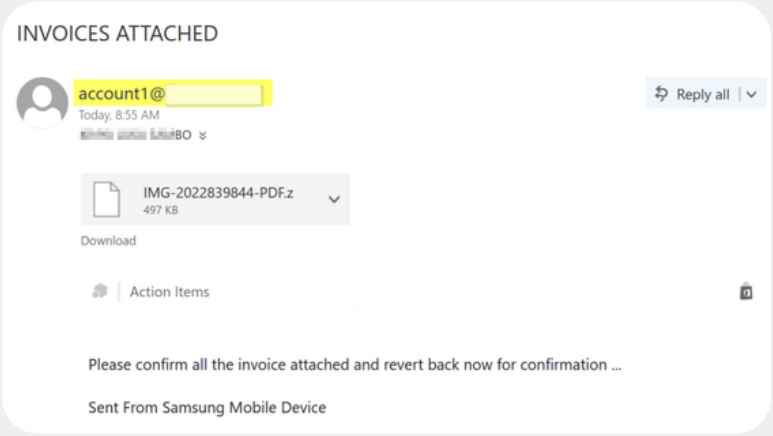
Here is what the first email looks like below.



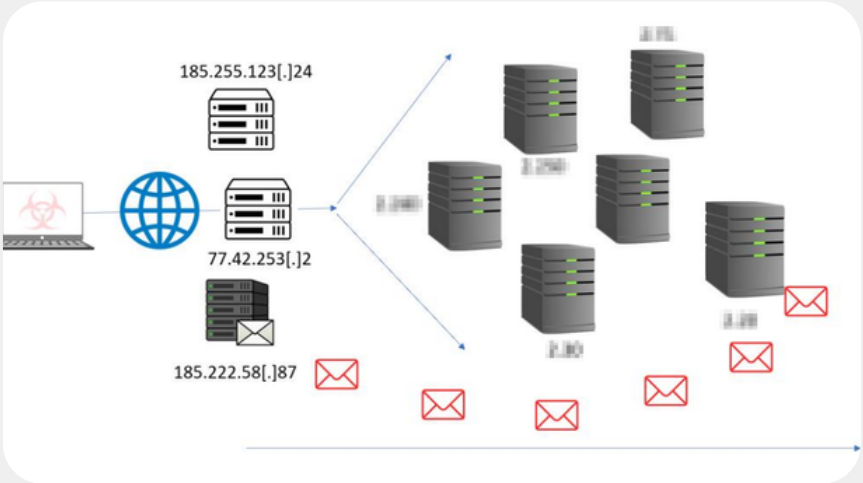




In the continuous effort to break in through social engineering, the TA also sent another series of emails on Friday 11th, November 2022 to the same set of users with different attachments this time coming from account1@target-org-domain, and from the same IP 185.222.58[.]87 as the one received on Monday.



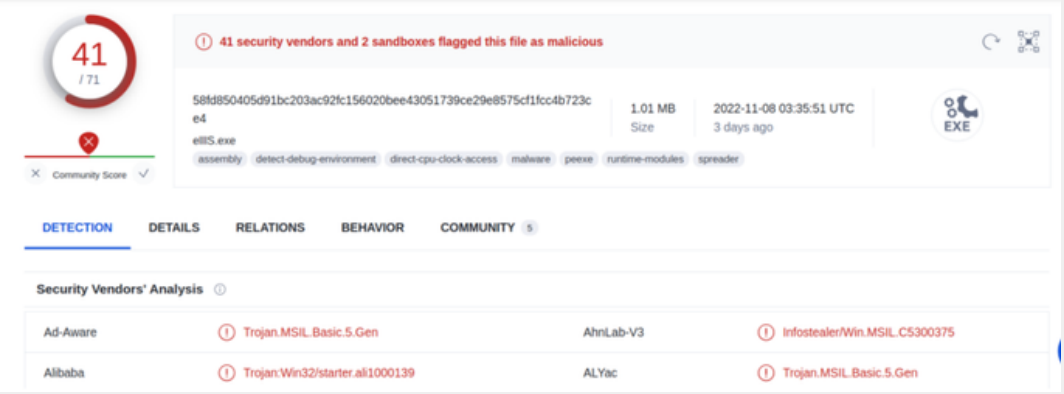
By the end of the first week, the Monitoring OPs have been able to perfectly come up with the draft of the threat group/attacker's infrastructure using observation from close monitoring of the targeted environment as shown below;

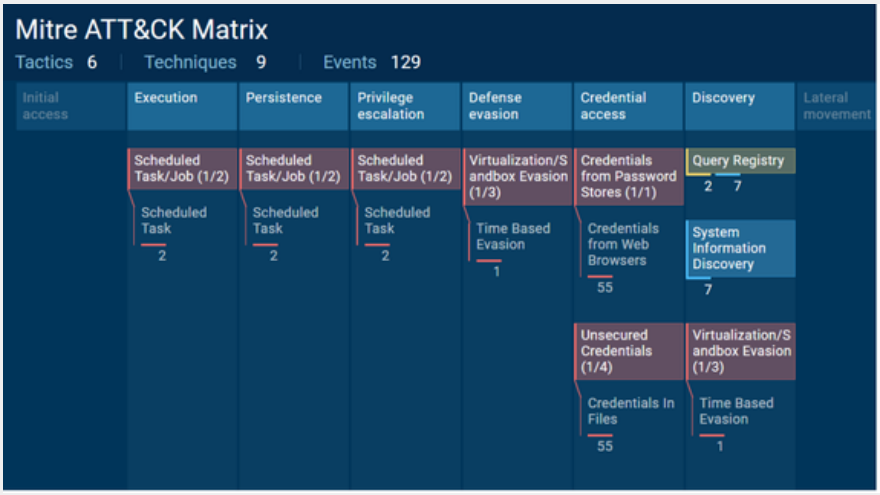


And the following hypotheses were also reached and the potential tempo drafted

- TA send email Monday and Friday (within the week)
- Scans and attempt exploitation throughout the week focusing on two servers majorly; scanning others as well.
- No scan on days emails were sent
- Brought part of its infrastructure closer to the target to remain undetected by leveraging cloud infrastructure with assets in Nigeria.
- A big infrastructure like this and the persistence might imply a bigger motivation and action on objectives on the part of the TA.
- Attachments in emails received were analyzed to understand the intent which was to steal credentials from any compromised users. Attachment comes in two extensions .RAR and .ZIP but both were found to be containing the same info stealer malware.
- The possible root cause of the invitation of TA towards the target already identified
- A necessary course of action (CoA) has been taken relating to the curated list of users the TAs was trying to get to through social engineering.

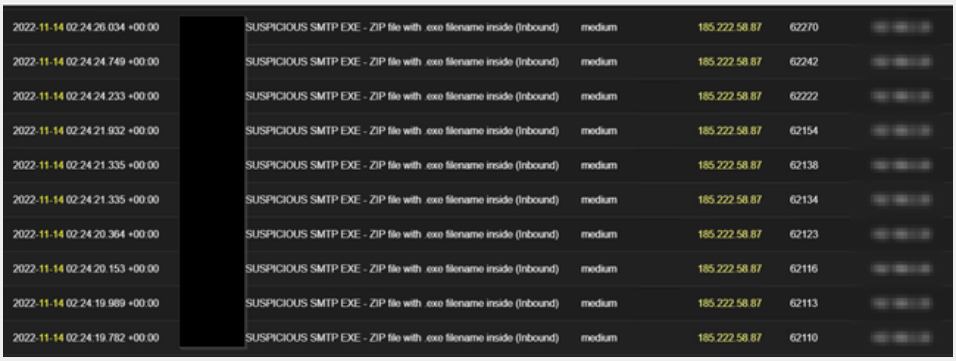
A glance through the dynamic analysis of the attachment using VT engines and attached is the ATT&CK matrix of behaviours





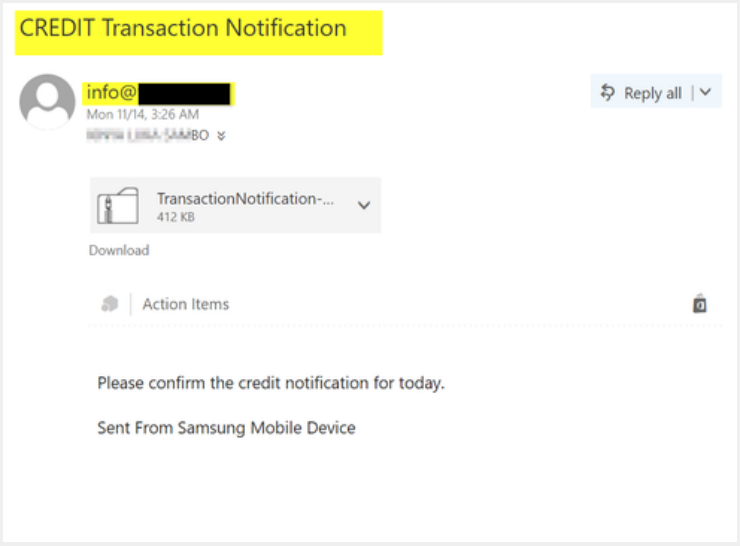
Into the Second Week

Jumping into the second week, we are already expecting to have an email on a Monday and it came in from the same IP responsible for emails from the TA's infrastructure this time around using the info@target-org-domain again as it was from the first series of emails



2022-11-14 02:24:26.034 +00:00	[redacted]	SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)	medium	185.222.58.87	62270
2022-11-14 02:24:24.749 +00:00		SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)	medium	185.222.58.87	62242
2022-11-14 02:24:24.233 +00:00		SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)	medium	185.222.58.87	62222
2022-11-14 02:24:21.932 +00:00		SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)	medium	185.222.58.87	62154
2022-11-14 02:24:21.335 +00:00		SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)	medium	185.222.58.87	62138
2022-11-14 02:24:21.335 +00:00		SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)	medium	185.222.58.87	62134
2022-11-14 02:24:20.364 +00:00		SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)	medium	185.222.58.87	62123
2022-11-14 02:24:20.153 +00:00		SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)	medium	185.222.58.87	62116
2022-11-14 02:24:19.989 +00:00		SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)	medium	185.222.58.87	62113
2022-11-14 02:24:19.782 +00:00		SUSPICIOUS SMTP EXE - ZIP file with .exe filename inside (Inbound)	medium	185.222.58.87	62110

Along with this, the scan continues on Tuesday 15th November, where the TA was able to introduce another server to their infrastructure hosting series of web application scanners, network and host-scanning commercial tools such as Nessus, Acunetix and OpenVAS directed against the internet-facing server on the target org for related vulnerabilities such as Log4J and other web application attacks as shown below



CREDIT Transaction Notification

info@[redacted]
Mon 11/14, 3:26 AM
[redacted]BO

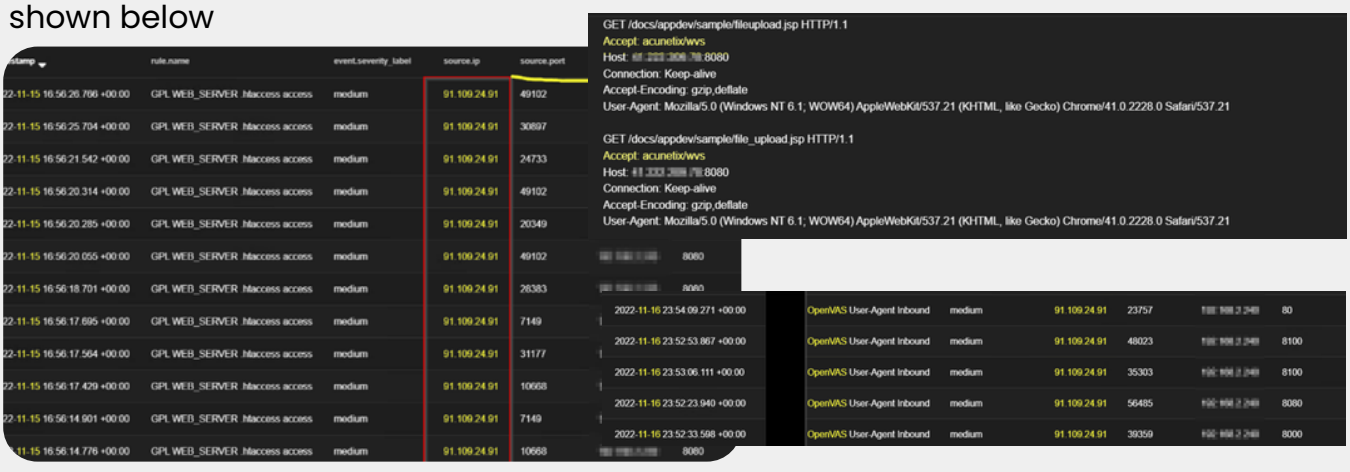
Reply all

TransactionNotification-...
412 KB
Download

Action Items

Please confirm the credit notification for today.

Sent From Samsung Mobile Device



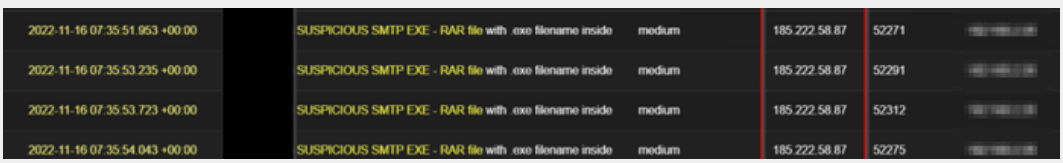
2022-11-15 16:56:26.766 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	49102	
2022-11-15 16:56:25.704 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	30897	
2022-11-15 16:56:21.542 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	24733	
2022-11-15 16:56:20.314 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	49102	
2022-11-15 16:56:20.285 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	26349	
2022-11-15 16:56:20.055 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	49102	
2022-11-15 16:56:18.701 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	26383	
2022-11-15 16:56:17.695 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	7149	
2022-11-15 16:56:17.564 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	31177	
2022-11-15 16:56:17.429 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	10668	
2022-11-15 16:56:14.901 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	7149	
2022-11-15 16:56:14.776 +00:00	GPL WEB_SERVER .htaccess access	medium	91.109.24.91	10668	

```
GET /docs/appdev/sample/fileupload.jsp HTTP/1.1
Accept: acunetix/wvs
Host: [redacted]:8080
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21

GET /docs/appdev/sample/file_upload.jsp HTTP/1.1
Accept: acunetix/wvs
Host: [redacted]:8080
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
```

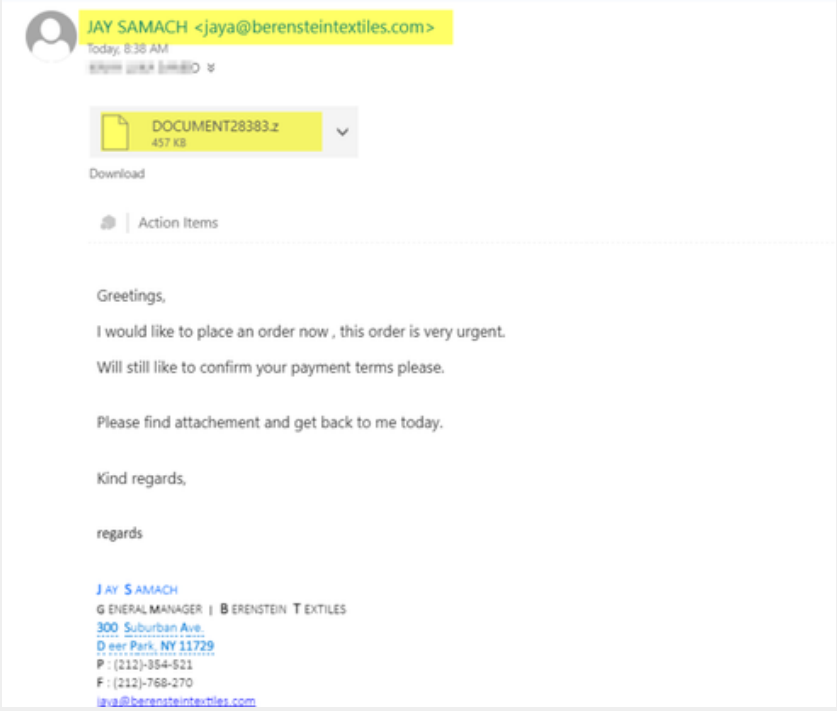
2022-11-16 23:54:09.271 +00:00	OpenVAS User-Agent Inbound	medium	91.109.24.91	23757	80
2022-11-16 23:52:53.867 +00:00	OpenVAS User-Agent Inbound	medium	91.109.24.91	48023	8100
2022-11-16 23:53:06.111 +00:00	OpenVAS User-Agent Inbound	medium	91.109.24.91	35303	8100
2022-11-16 23:52:23.940 +00:00	OpenVAS User-Agent Inbound	medium	91.109.24.91	56485	8080
2022-11-16 23:52:33.598 +00:00	OpenVAS User-Agent Inbound	medium	91.109.24.91	39359	8000

These scans also continue throughout the week and come with more intensity than what we were getting earlier as shown below; the tempo changed to email on interval + scans every day



2022-11-16 07:35:51.953 +00:00	[redacted]	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	52271
2022-11-16 07:35:53.235 +00:00		SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	52291
2022-11-16 07:35:53.723 +00:00		SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	52312
2022-11-16 07:35:54.043 +00:00		SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	52275

This email happened to be the first with a more official body structure and a different source domain other than the target-org-domain; indicating a possible change of mind for the TA with the hope that the previous email might not have been clicked because they look less official. But one thing that was still giving them away was that they were still coming from the server 185.222.58[.]87 responsible for email on their infrastructure and they all contain similar info stealer malware after being analyzed.



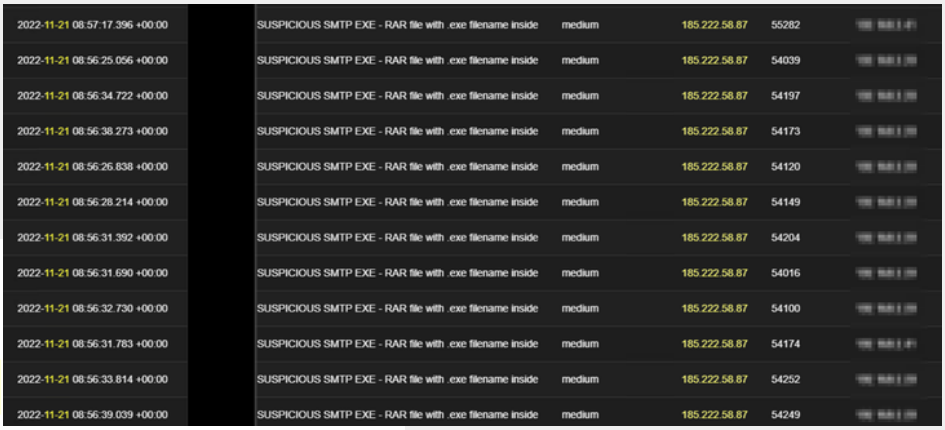
By the end of the second week, the Monitoring OP updated the attacker infrastructure draft they had by including the new server housing the commercial scanner tools and more information on this infrastructure has been identified

And the following hypothesis were also reached and the potential tempo drafted

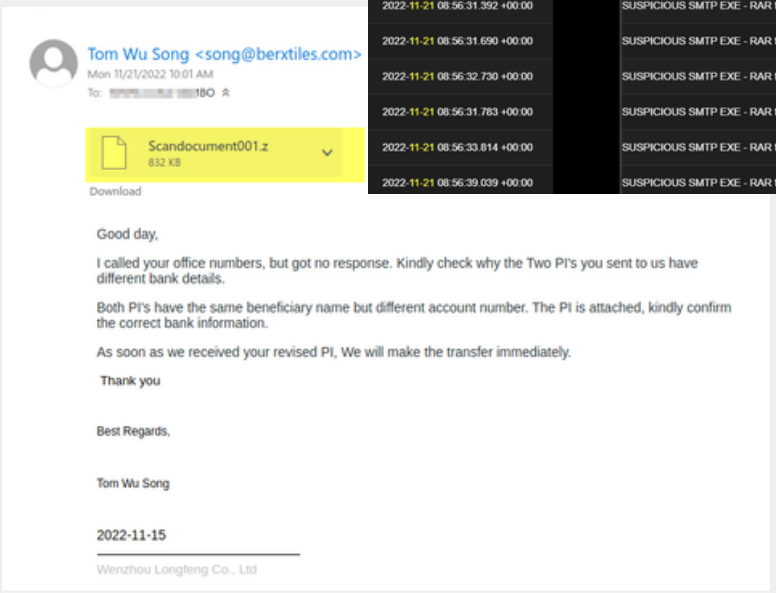
- TA might want to re-strategize going forward as the phishing attempt is not working
- Look like TA is willing and has the budget to expand on infrastructure to get to their goal
- TA is intensifying activities for scan and using commercial tools to aid successful recons.
- Possibly Human-Driven and targeted
- All attachments in all new emails after being analyzed remain to be the info stealer malware just change of name
- Most of what we hypothesised in the first week was validated going forward during analysis and with new observations.

What happened in Week Three

Then we jumped into Week Three where we got our first email, also came in an official body structure as shown below.



2022-11-21 08:57:17.396 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	55282	
2022-11-21 08:56:25.056 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54039	
2022-11-21 08:56:34.722 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54197	
2022-11-21 08:56:38.273 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54173	
2022-11-21 08:56:26.838 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54120	
2022-11-21 08:56:28.214 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54149	
2022-11-21 08:56:31.392 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54204	
2022-11-21 08:56:31.690 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54016	
2022-11-21 08:56:32.730 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54100	
2022-11-21 08:56:31.783 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54174	
2022-11-21 08:56:33.814 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54252	
2022-11-21 08:56:39.039 +00:00	SUSPICIOUS SMTP EXE - RAR file with .exe filename inside	medium	185.222.58.87	54249	



Tom Wu Song <song@berxtiles.com>
Mon 11/21/2022 10:01 AM
To: [redacted]180

Scandocument001.z
832 KB
Download

Good day,

I called your office numbers, but got no response. Kindly check why the Two PI's you sent to us have different bank details.

Both PI's have the same beneficiary name but different account number. The PI is attached, kindly confirm the correct bank information.

As soon as we received your revised PI, We will make the transfer immediately.

Thank you

Best Regards,

Tom Wu Song

2022-11-15

Wenzhou Longfeng Co., Ltd

We watched the scans fade away in the third week as well as the tempo of the email just concentrating now on a single email and eventually the TA stopped sending (possible withdrawal for an easy target or planning a better kill chain that will work). This pushes our team into the watching phase to ensure we are not caught up with any surprises with whatever the re-strategized plans of the TA might be.

In conclusion, we have succeeded in frustrating the threat actor/group after watching them suffer for the past three weeks scanning and sending emails to the mostly retired inboxes as contained in the report.

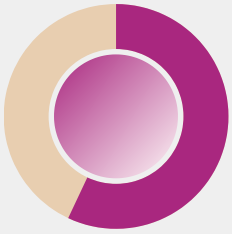
Indicator of Compromise (IOCs)

185.255.123[.]24, 77.42.253[.]2, 185.222.58[.]87, 91.109.24[.]91
58fd850405d91bc203ac92fc156020bee43051739ce29e8575cf1fcc4b723ce4 (SHA256)
3d06cd1430771df1de9948c5f1e0b75eb9f8fe61fe2d7765ddaf916e8d59950c(SHA256)
95f56fb182812795848d78ba412d42c76ee717945a57b0389b24e53e6fbbee04 (SHA256)
132.226.247[.]73:80 , 158.101.44[.]242:80 , 20.99.133[.]109:443 23.216.147[.]76:443
https://www.virustotal.com/gui/file/58fd850405d91bc203ac92fc156020bee43051739ce29e8575cf1fcc4b723ce4/behavior
https://app.any.run/tasks/ba69879f-1493-4c53-8565-49dc38e344a8

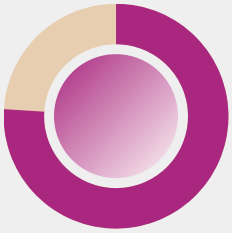
IMG-2022839844-PDF.z | INVOICES ATTACHED, DOCUMENTS09482.zip | Invoice S150703 50% deposit for POEW20211221C, DOCUMENT28383.zip | URGENT ORDER, TransactionNotification-pdf.zip | CREDIT Transaction Notification, Scandocument001.zip | PI,

How interesting was the third quarter of 2022?

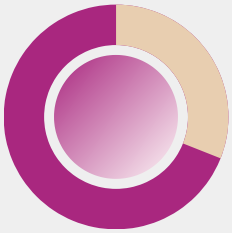
2022 | Q3 at a glance



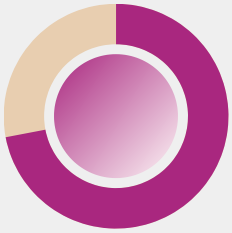
Several unreported incidents hit Nigerian businesses, as many continue to treat cybersecurity incidents as IT-related problems. This has resulted in huge downtime of services and financial loss for affected businesses.



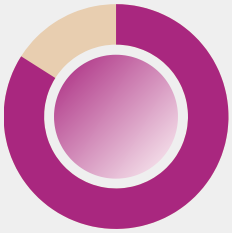
CVEs from Q4 of 2021 and Q1, Q2 of 2022 are still been exploited. CNIs of countries and businesses are the target of multiple breaches and ransomware attacks in Q3. Government-wide network attacks and breaches become prevalent.



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.

Data Protection at Schools and Microfinance banks - Leakage observed

It was during the continuous monitoring ops that we came across certain folders and files we believed to be containing personally identifiable information (PII) of employees, customers and generally that of a microfinance bank. A misconfigured LMS was also found to be leaking sensitive information of students, staff and parents of some schools in Nigeria.

For microfinance banks adopting digitization, requires a proper change management process as old servers are left exposed to leaking customers' data and other related information was the case in most of our findings.

The COVID Lockdown led to several schools trying to adopt digital means of reaching out to their students for educational activities to continue. And for that, many schools have adopted a Learning Management System (LMS) which was the case with many schools today.

But in the process of transitioning, the security of student, parents and staff data was not properly considered which led to the exposure of sensitive information of students, staff and parents through insecure configurations

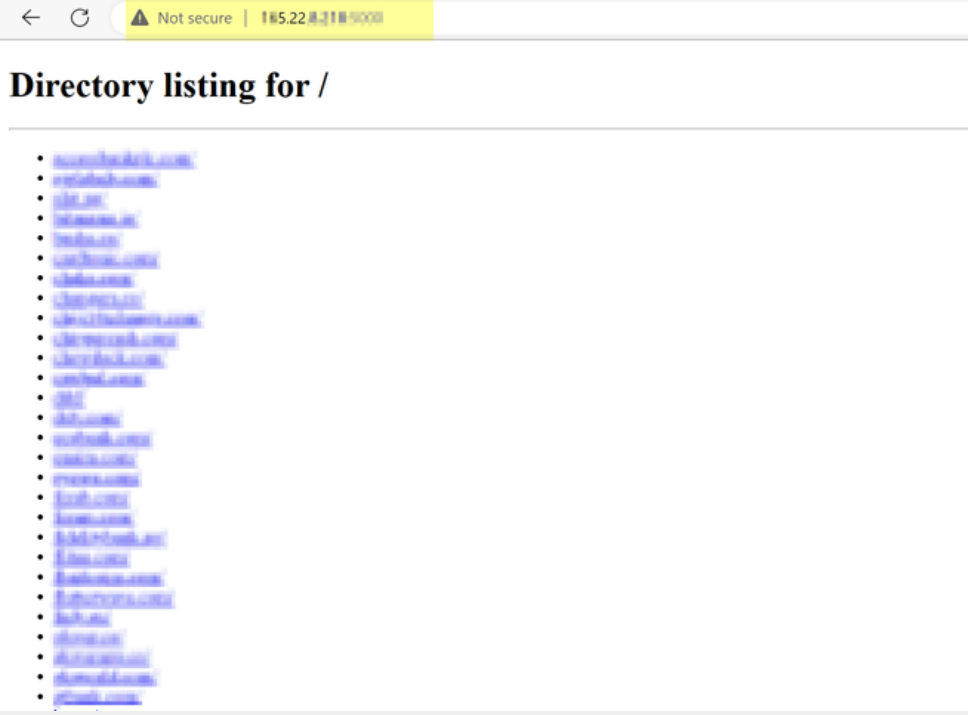
Attention should be given to the protection of related data by parents and school management.

Proper secure coding and development processes in place with continuous vulnerability assessment and penetration testing (VAPT) can provide the needed assurance around data exposure for schools.

Recon data of TA focusing on Nigerian orgs, majorly finance discovered

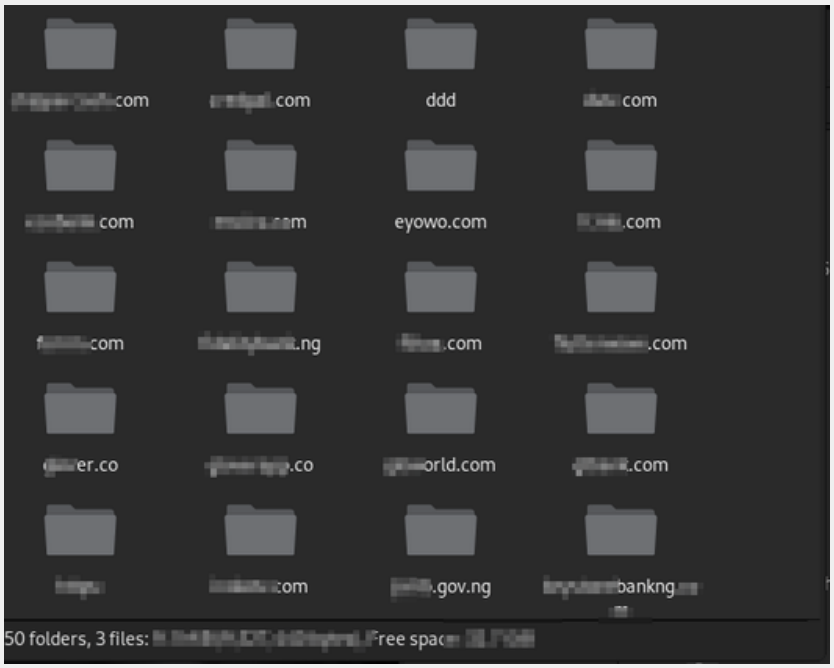
Looking through this trove of data (approximately 16GB, if not more) and how it was organized into different sections for different organizations/businesses make us reach a conclusion that we might be looking at a result of long-term information-gathering activities of a possible threat actor or that of a threat group.

Our Cyber 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.



The classes of information (the result of active reconnaissance) we saw depict what an attacker needs to kickstart its journey along the cyber kill chain to have their hands-on objective.

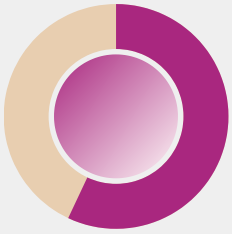
Just recently our CTI team came across this trove of data on a server on the Internet containing active reconnaissance information about all digital assets of the bank. Related data are **domain info, emails and passwords, cloud providers, fuzz data for endpoints, zone transfer, dorks, waf checks** and some other interesting pointers to where **lfi, ssrf, rce** could be leveraged on all web apps.



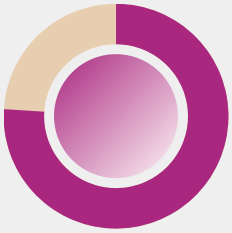
As an MSSP, we understand how affected organizations can leverage this information to bolster their defense to be able to stay ahead of all possible game plans from the threat actor or group which is on the mission to leverage them as well.

What happened in the second quarter of 2022?

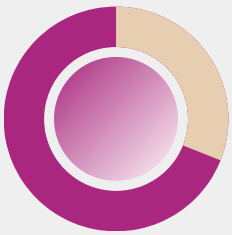
2022 | Q2 at a glance



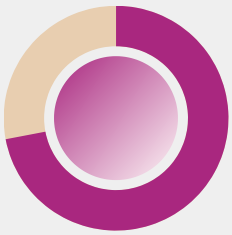
High / Critical CVEs such as Spring4Shell and Follina were reported in Q2 of 2022 with patches available for core technology products that organizations leverage in everyday business.



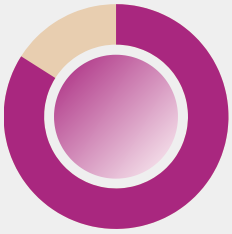
CNI of countries and businesses are the target of multiple breaches and ransomware attacks in Q2. CVEs from Q4 of 2021 and Q1 of 2022 are still been exploited. More African targets make it to the news such as Bet9ja and Shoprite Holdings.



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



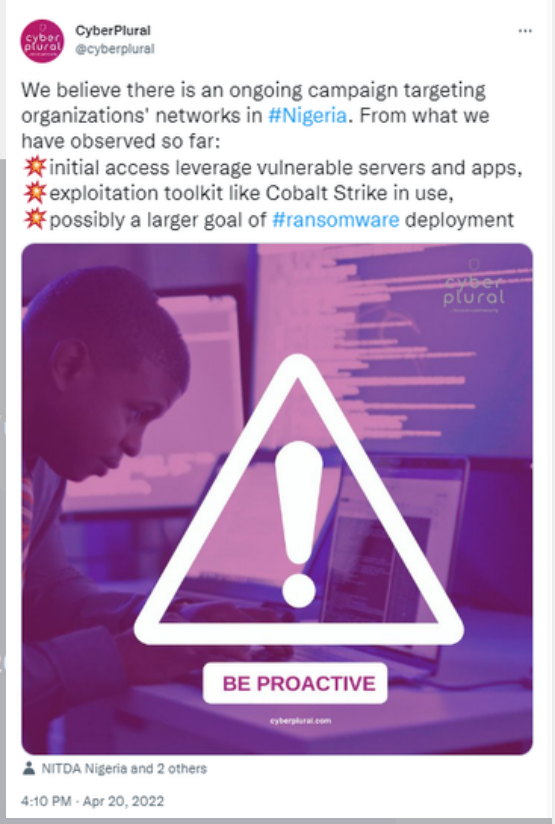
Our CTI Team revealed threat actors leveraging the Cobalt Strike Framework and other popular RAT within public institutions' networks in Nigeria.



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

When they come with Cobalt Strike, just know it is serious!

```
beacon_type: HTTP
dns-beacon.dns_idle: 134743044
dns-beacon.maxdns: 235
http-get.client:
  Accept: */*
  Host: download.windowsupdate.com
  .cab
http-get.uri: 116.204.211.180,/c/msdownload/
http-get.verb: GET
http-post.client:
  Accept: */*
  download.windowsupdate.com/c/
  Host
  .cab
http-post.uri: /c/msdownload/update/others/2
http-post.verb: GET
http_post_chunk: 96
jitter: 20
maxgetsize: 1048576
port: 80
post-ex.spawnto_x64: %windir%\sysnative\rundll32.exe
```



The campaign was found to be focused on open targets that presented themselves (opportunistic hacking) and activities observed so far have been more targeted toward government organizations, telecommunication, and finance.

When they come with Cobalt Strike, just know it is serious!

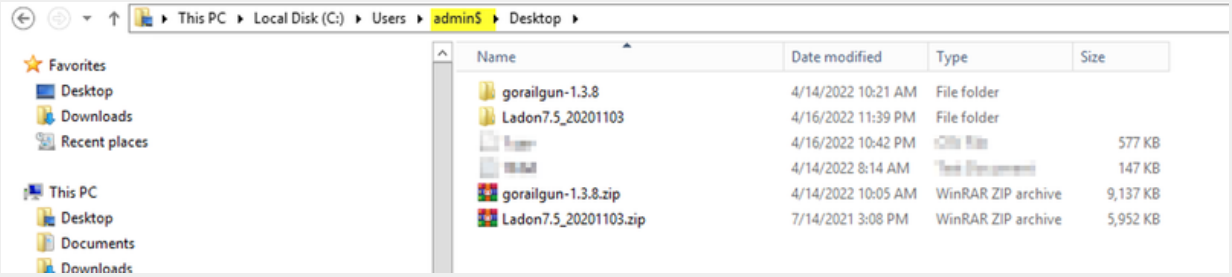
```
beacon_type: HTTP
dns-beacon.dns_idle: 134743044
dns-beacon.maxdns: 235
http-get.client:
  Accept: */*
  Host: download.windowsupdate.com
  .cab
http-get.uri: 116.204.211.180,/c/msdownload/update/others/2016/12/29136388_
http-get.verb: GET
http-post.client:
  Accept: */*
  download.windowsupdate.com/c/
  Host
  .cab
http-post.uri: /c/msdownload/update/others/2016/12/3215234_
http-post.verb: GET
http_post_chunk: 96
jitter: 20
maxgetsize: 1048576
port: 80
post-ex.spawnto_x64: %windir%\sysnative\rundll32.exe
```

Following this campaign, the initial point of entry leverage misconfigurations in internet-facing assets which could be applications, web servers and mail services. In one of the referenced cases, the attacker leveraged a misconfigured server on the target network which was found to be the beachhead as captured below in the security platform.

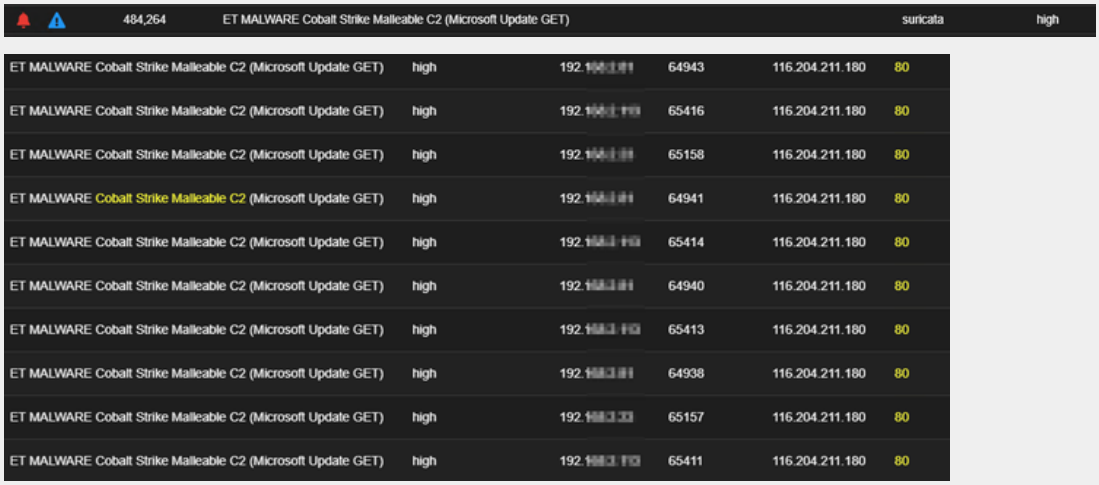
⚠	2022-04-14 08:32:10.008 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:10.013 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:10.355 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:10.713 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:11.004 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:11.016 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:11.018 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:11.027 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:11.027 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:11.074 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:11.356 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:11.382 +01:00	192	116.204.211.180
⚠	2022-04-14 08:32:11.392 +01:00	192	116.204.211.180

Drilling down on this compromise server we found a hidden account where the attacker dropped some other malicious file that was captured during the investigation. These files were identified to be used for internal recon of the environment; scanning network blocks for resources that may be of interest to the attacker;

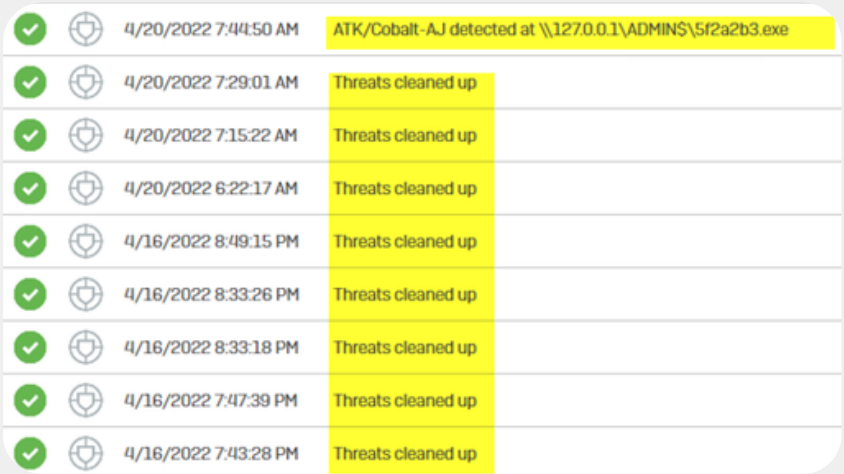
SMB shares, web services, workgroups, open ports and services and possible credential dumping (one of them is a plugin for Cobalt Strike). The result of this internal recon was found in some text files on the server eventually.



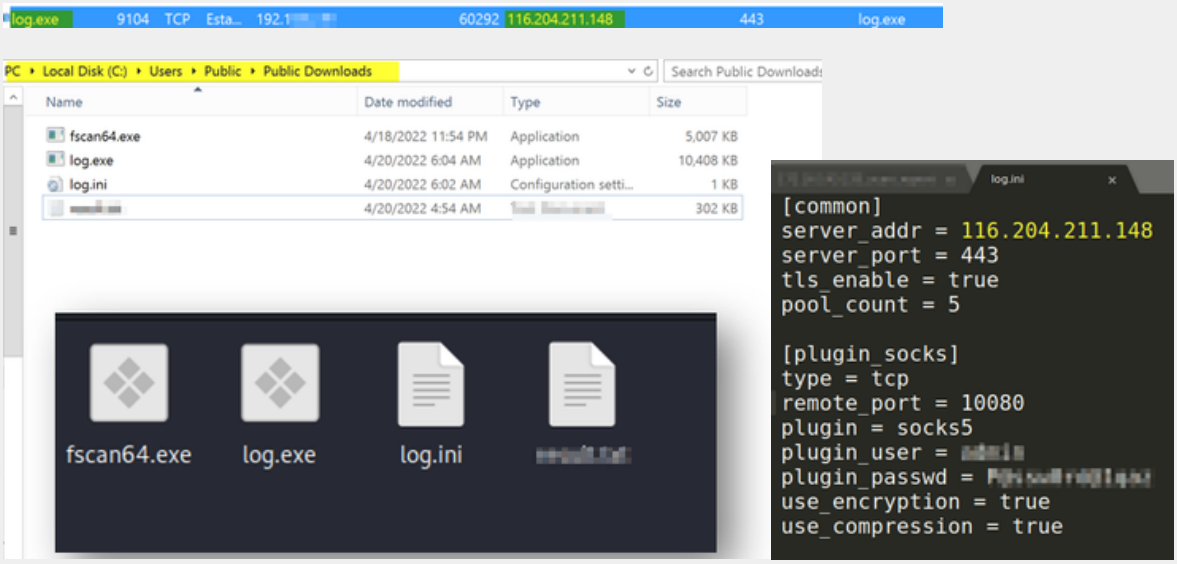
Leveraging some of the information captured on the beachhead and the alerts from the SIEM platform, we were able to understand more systems were already talking with the C2 server on port 80 following the IoCs which is an indication that the possibility of credential dumping, internal enumeration, lateral movement and possible infiltration and exfiltration might have taken place during this period.



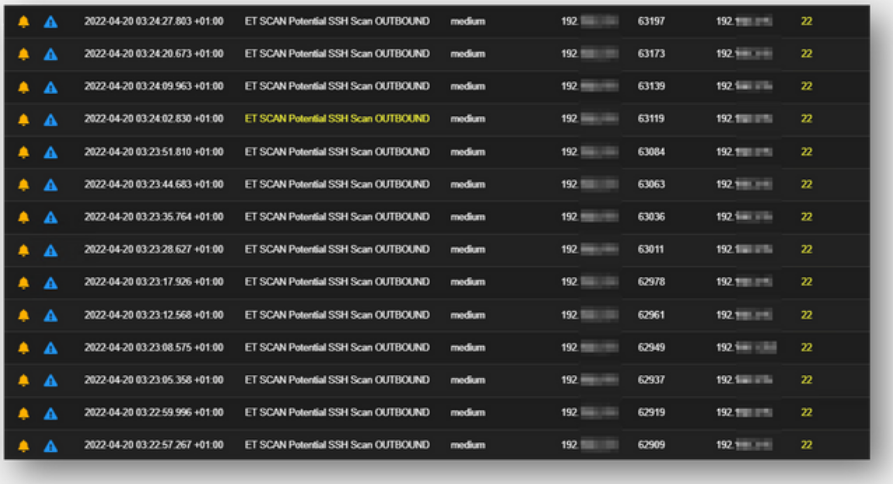
With the **Cobalt Strike C2** infrastructure in place, the attacker was using this to laterally move around the network and of which the stager was found on another server and the Endpoint Detection and Response agent blocked the connection initiated by continuous removal of the stager.



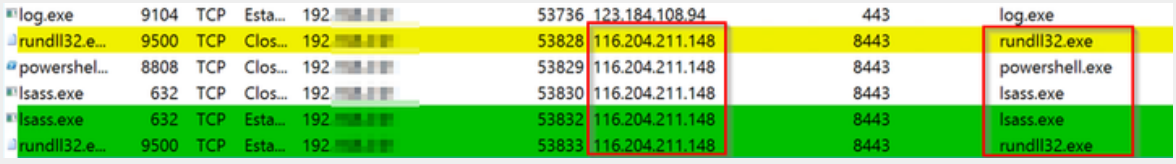
In one of the servers, we found some other series of internal recon tools that are connecting to the redirect IP of the C2 infrastructure as shown below. These files reside in the Public Downloads in the Public User folder, and the **log.ini** is found to contain the configuration file through which it is used to communicate to the C2.



log.exe found to be running on one of the compromised servers was observed to have generated the following events on the SIEM platform, an internal recon in search of devices with port SSH (22) services running within the internal network. Other searches targeting other standard ports were also found and captured.



Legitimate processes like rundll32.exe, lsass.exe, and powershell.exe were seen to have taken over by the malicious Cobalt Strike stager communicating with the redirect IP of the C2 server 116.204[.]211.148



From the above investigation, it is obvious the attacker pushing this campaign meant business considering the type of tools that were captured during the incident response engagement. Such attackers willing to leverage a C2 infrastructure hosting Cobalt Strike, with some other interesting tools as captured above will be willing to go to any length to meet their financial objectives.

which can come in two ways; either credential stealing or data exfiltration which will allow them to put up the data for sale on the dark web. Probably to a competitor or some ransomware operators who will come back to deploy their ransomware on the already existing compromised network. This time around the double extortion scheme might be useful for the attacker.

Organizations are advised to embark on patch management, system hardening for legacy systems that cannot be patched, close unused ports and services, and use secure ports on other internet-facing assets that are regularly open for public access. They can also adopt the service of CyberPlural MSSP which will provide a combination of advanced cyber technology that can protect their users, endpoint and networks through a 24/7 proactive monitoring and incident response capability.

Indicator of Compromise (IOCs)

Contained below is the list of Indicator of Compromise (IoCs) observed on the compromised server investigated. Hashes and possible file locations for all dropped files by the attackers. This information might change from operator to operator but the campaign approach remains the same.

SHA256	IoC
aa305ad62d70cec54fdafa685ec8ab9d67bc486891c848fe0e9b2ffdc745b802	gorailgun-1.3.8.zip
7953c193e332830909d86ab35d50793cb157f03cc0e43bbc28afb09b00dbd48e	Ladon7.5_20201103.zip
c92c158d7c37fea795114fa6491fe5f145ad2f8c08776b18ae79db811e8e36a3	AdFind.exe
d26437cc6ff9d094d42947d214c80a313e064ca403e9dd33a8110d7e859dd10e	fscan64.exe
60c2f395a7af8433b6a71601168ed96dad412375db9622d7b50344a6f3d297c1	log.exe
b81d6956938efae1c077869b084a834a54982db36e845b524a5a0896aa2c3c94	gorailgun-1.3.8.exe
b6a17063e36522ea5e0778110e6de92f3f50af63818ffee6e4652d4403d3b714	LadonGUI40.exe

116.204[.]211.180, 116.204[.]211.148

123.184[.]108.93 , download.windowsupdate.com.cab

log.ini, \\127.0.0.1\ADMIN$\5f2a2b3.exe, C:\Users\admin$\Desktop

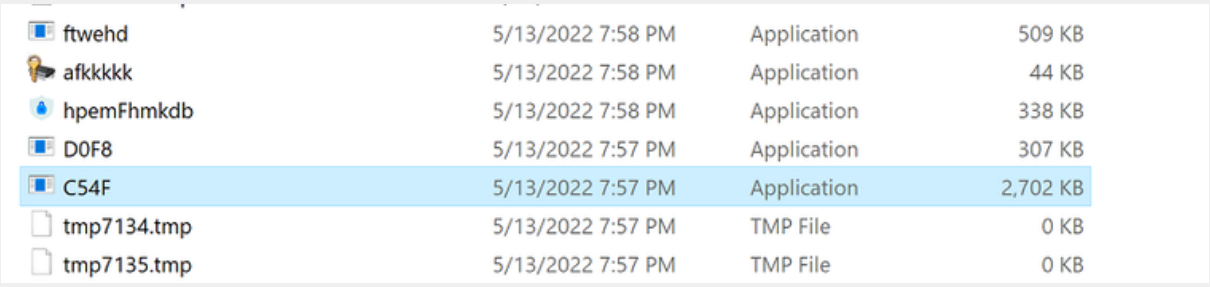
C:\Users\Public\Downloads, %windir%\sysnative\rundll32.exe

/c/msdownload/update/others/2016/12/29136388_

server.publickey_md5: defb5d95ce99e1ebbf421a1a38d9cb64

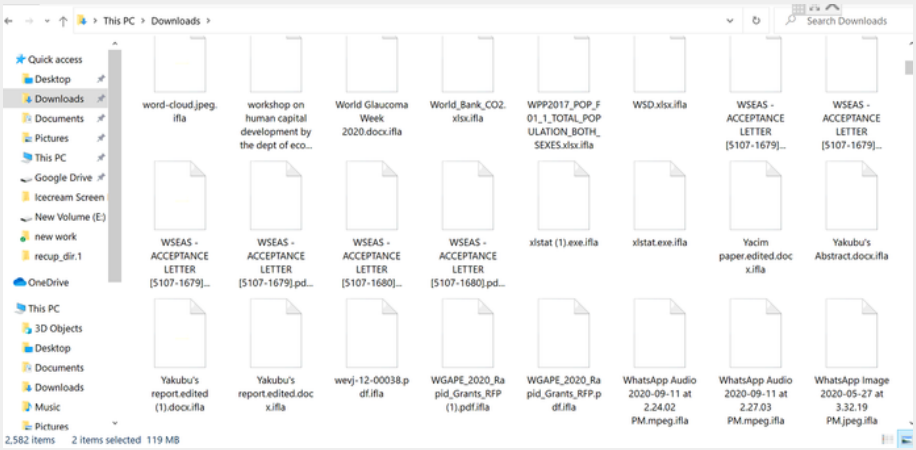
Ransomware: corporate-wide and individual incidents observed

During this period of the year, several individual incidents of ransomware were reported to our SOC and investigated by our team; variants such as EKING of Phobo Ransomware, IFLA and .FATP of DJVU ransomware were found to have infected their systems and asked users to pay around $450-$950 as ransom. The corporate-wide incident was also reported by Bet9ja.



ftwehd	5/13/2022 7:58 PM	Application	509 KB
afkkkkk	5/13/2022 7:58 PM	Application	44 KB
hpemFhmkdb	5/13/2022 7:58 PM	Application	338 KB
D0F8	5/13/2022 7:57 PM	Application	307 KB
C54F	5/13/2022 7:57 PM	Application	2,702 KB
tmp7134.tmp	5/13/2022 7:57 PM	TMP File	0 KB
tmp7135.tmp	5/13/2022 7:57 PM	TMP File	0 KB

In one of these incidents investigated, we observed the ransomware package to have come alongside some info stealer malware that dumped user's cookies, credentials in browsers and files prior to the encryption and those stolen credentials in the process were used to access users related accounts when users refused to make the ransom payment within the stipulated amount of time. This was the case with the **.FTAP** variant of **DJVU** ransomware.



In another incident, where the **IFLA** ransomware was found to have encrypted all of the user's system under investigation and several other info stealer malware like **REDLINE** were found on the system; REDLINE is a notorious info stealer trojan capable of talking to a C2 and capable of stealing credentials from Password Stores, Web Browsers, Unsecure credentials, Credential in Files.

CEO STATEMENT: WE HAVE CONTROL, ALL ACCOUNTS, DATA, AND FUNDS ARE SECURE

The past few days have been challenging for us as a business. In the early hours of Wednesday, 6th April, 2022 we suffered an unprovoked and unjustified sophisticated criminal cyber-attack on our platform.

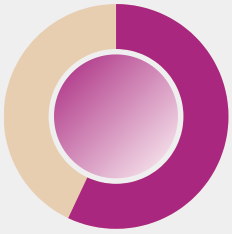
Many of our customers and stakeholders have had to deal with the inconvenience of not being able to access their accounts or place bets on the bet9ja.com platform. On behalf of the management and every member of the team, I would like to apologize for this and express that we deeply regret this situation.

We can confirm that the ransomware attack came from the Blackcat Group. You can find information about the cyber criminal organisation online.

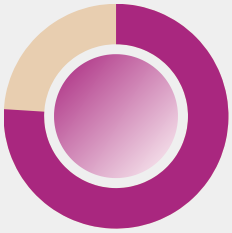
In April, Nigerian betting platform Bet9ja suffered a ransomware attack perpetrated by the BlackCat ransomware group. The attack disrupted Bet9ja's regular operations, and many users cannot use their platform for several hours. Several ransomware-related incidents might have occurred in other organizations that were not reported as captured in the third quarter.

Back to the first quarter of 2022!

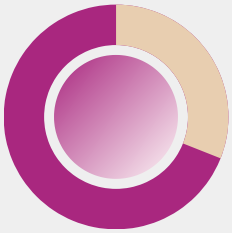
2022 | Q1 at a glance



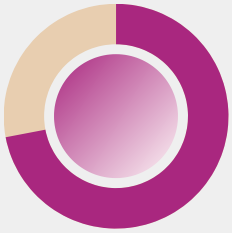
High / Critical CVEs were reported in Q1 of 2022 with patches available for core technology products that organizations leverage in everyday business.



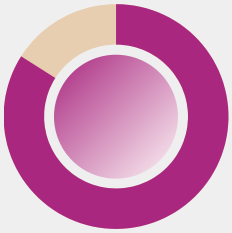
Critical National Infrastructure (CNI) and big businesses are targets of multiple breaches and ransomware attacks in Q1. CVEs from Q4 of 2021 are still been exploited



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

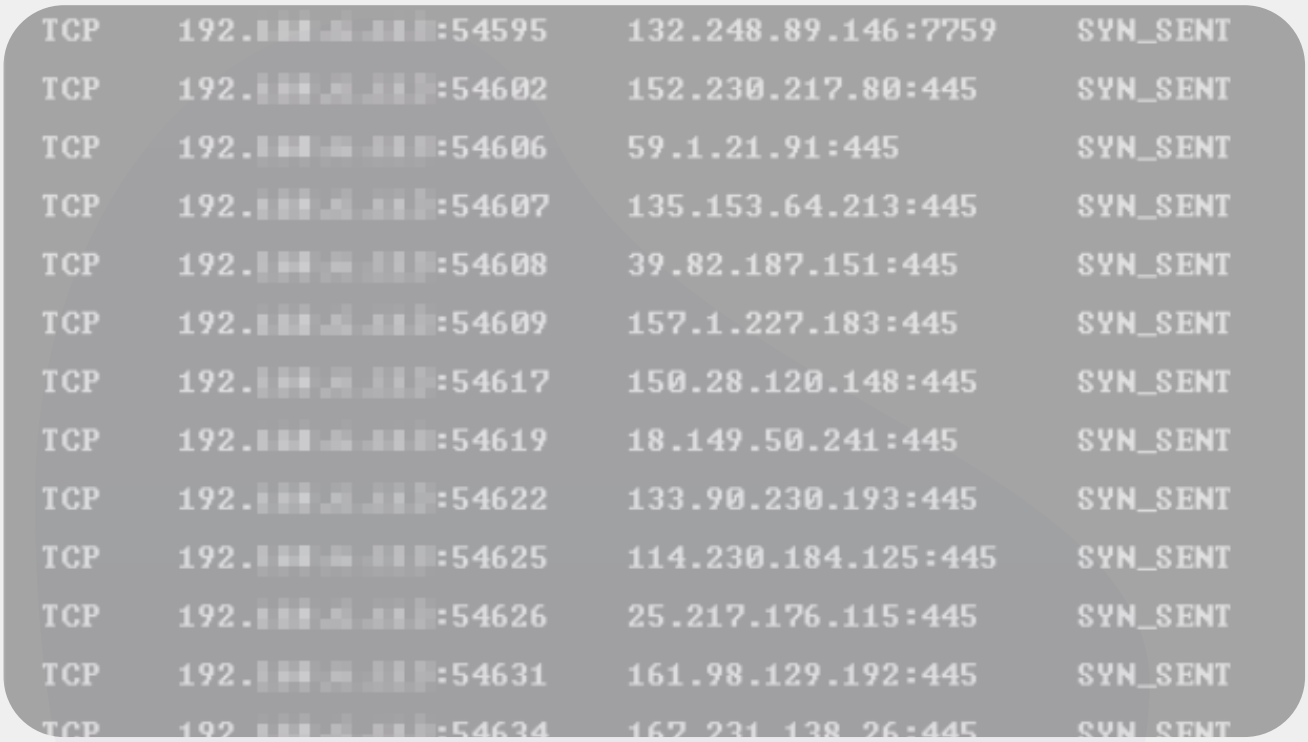


CTI activities revealed several digital infrastructures in Nigeria are susceptible to opportunistic hacking as old CVEs in legacy applications and unpatched vulnerabilities can be leveraged.

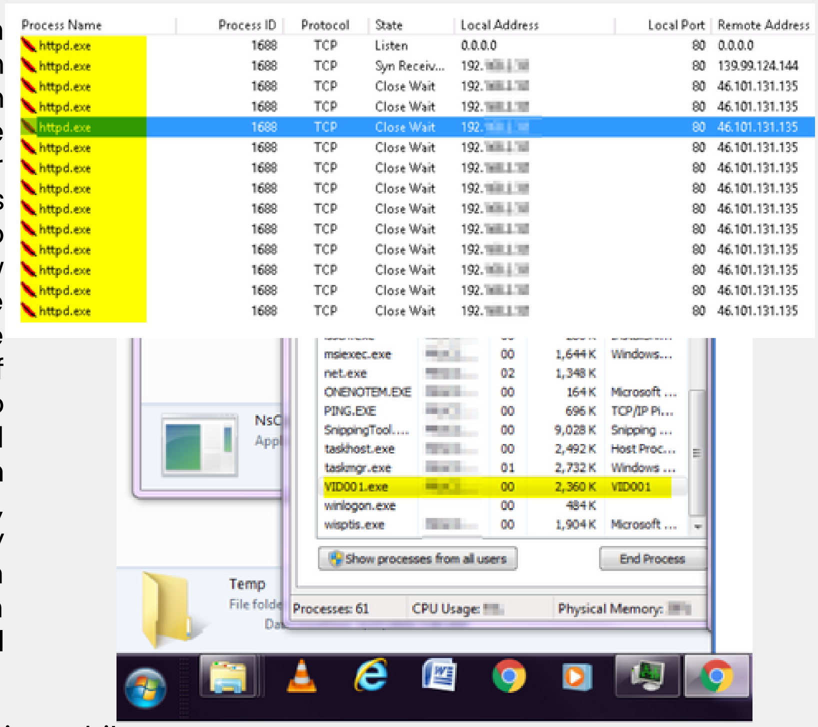


Misconfiguration, Insecure Design and Lack of Proper logging and monitoring were identified as the top flaws of web applications tested in Q1.

how legacy systems can aid cyber threat actors



How are you handling Legacy systems in your organization today? Are they been given the needed priority? or we don't even care about them anymore? Today, every security team need to pay special attention to those devices that are running legacy software and hardware because of their ease of compromise.



How do you advise an organization to move away from Apache services that has been installed for almost a decade without an update or other security routines due to limitations of web applications not built to scale? For many that argued how they cannot just throw off these legacy systems, a use case where special consideration in term of security is not even in place to protect those applications and hardware covered on this list can consider hardening, use of DMZ, continuous monitoring and many other blue techniques that can further help assure the protection of affected systems and applications.

We noticed that the core objective while keeping most of those old applications is to keep ensuring functionality while ruling down on security (the slogan is; it is working and that is how we have been using it). What many managers of these old applications met are documentations on how to keep it running to support organizational needs; hence, they are ignorant of the architecture of the systems and how to scale them up to work in the latest environment.

Below are some compelling reasons organizations may be keeping a legacy system;

- The system works satisfactorily, and the owner sees no reason to change it.
- The costs of redesigning or replacing the system are prohibitive because it is large, or complex.
- Retraining on a new system would be costly in lost time and money, compared to the anticipated appreciable benefits of replacing it (which may be zero).
- The way that the system works is not well understood. Such a situation can occur when the designers of the system have left the organization, and the system has either not been fully documented or documentation has been lost.

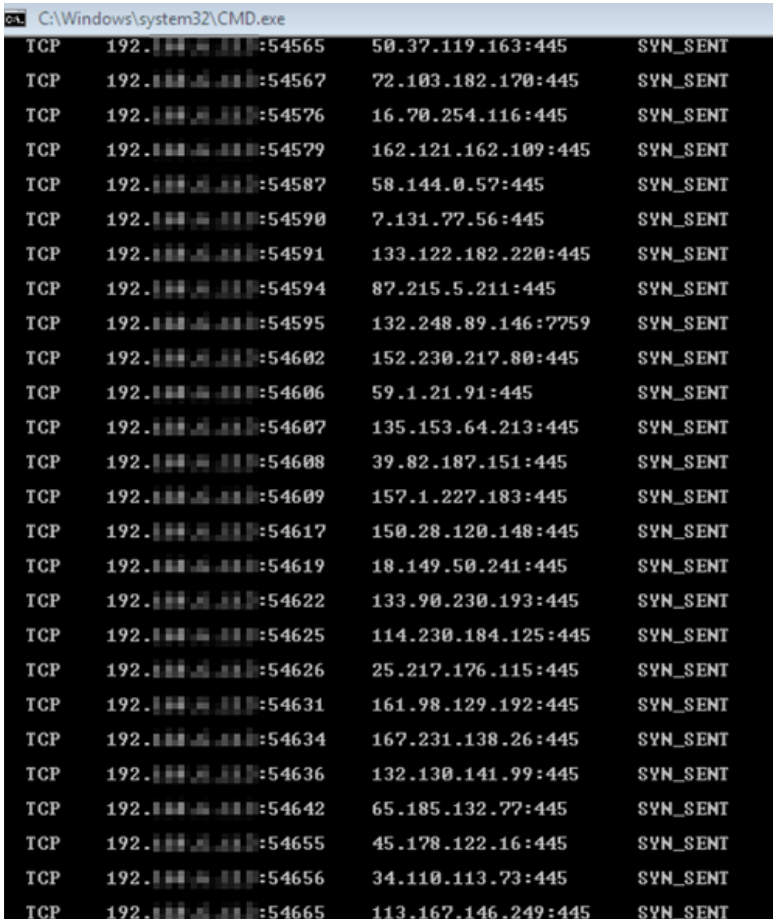
In an engagement, we observed after the deployment of SIEM that the network has been **compromised** with Wannacry involving different workstations in departments within the organization.

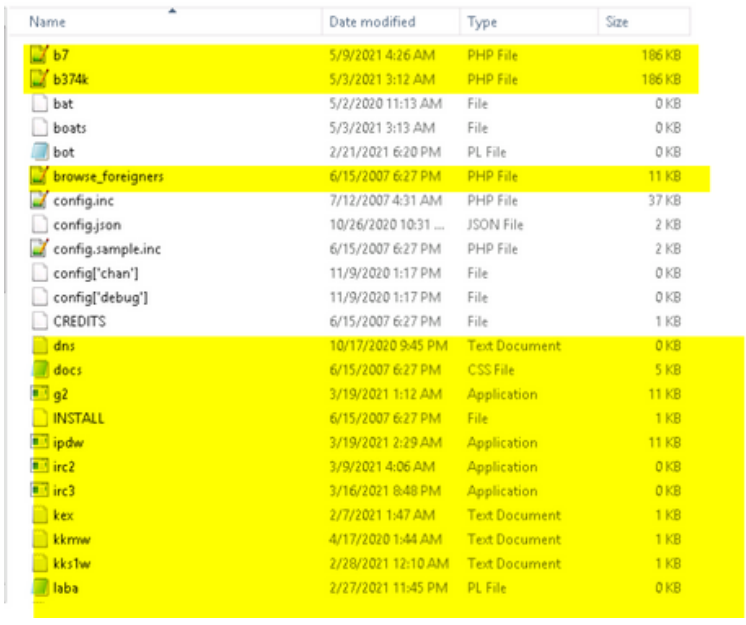
This engagement revealed that mostly Windows 7 and Windows Server 2008 are Operating systems that dominated the network, giving the attacker the leverage to move around on port 445 (SMB) which hosts the known vulnerability for the WannaCry Ransomware. Not only this but enormous crypto miners were also detected on tens of workstations within the organization's network, consuming network bandwidth and system resources. What is surprising is how many of these unsupported versions of the Windows Operating systems (Reached End of Life) from Microsoft dominated a network in recent times.

For IT team and employees, so long they can still use their systems, unknowingly sitting on a time bomb that may tick any time when it involves one of these new variants of Ransomware groups wreaking havoc across the world like Avvadon, Conti, Darkside and others. And in many other cases APT (Advanced Persistent Threat) actors, where the focus is data exfiltration, collection of servers for botnets, crypto-jacking, users credential's compromise, and dark web data leakage.

Some organizations are already on the way out of migrating from these old systems by rebuilding their applications to fit into more recent environments in terms of operating systems and underlying hardware requirements so as to keep out security threats from the organization.

They are also doing it for speed and other users' needs which may not be initially featured in the old applications. We advised that security should be part of what to be considered and should be part of the plan from the onset in this new rework, by subjecting them to application testing, and code review right before deploying into production and afterwards





2023 Cyber Outlook

2023 Outlook -

Network-wide ransomware incidents against government-related entities in Africa. As MSPs that manage government infrastructure, tend to be targeted.

Attack against elections through propaganda, defacement, and cyber activity by interested espionage groups may be observed.

Financial institutions, traditional & fintech will continue to see cyberattacks against their infrastructure as we monitor campaigns gathering information on their digital infrastructure.

Cryptocurrency platforms will continue to be targeted by TAs who seek to steal tokens by infecting and exploiting wallets, bridges and network.

As the growth of cloud adoption continues. Startups and organizations leveraging the cloud will continue to be targeted, as first-timers are prone to insecure configurations that can be leveraged.

More actions will be seen from Data Protection Agencies in Africa in 2023 to ensure regulatory compliance across businesses and organizations operating in their space.

References

https://blog.cyberplural.com/crypto-stealer-campaign-targeting-crypto-platforms-extension-in-browsers/

https://twitter.com/Bet9jaOfficial/status/1512864410796277763?s=20

https://blog.cyberplural.com/2022-q3-report/

https://blog.cyberplural.com/2022-q2-report-lessons-learnt/

https://blog.cyberplural.com/when-they-come-with-cobalt-strike-just-know-it-is-serious/

https://www.vanguardngr.com/2022/04/fg-condemns-hacking-of-bet9ja/

https://blog.cyberplural.com/2022-q1-report-lessons-learnt/

cyber plural
...focus on cybersecurity

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

CyberPlural's MSSP methodology is unique in its approach, providing the opportunity to creatively design a cybersecurity strategy and plans that provide businesses/organizations with the resiliency to scale in the ever-growing world of the Internet at a very affordable cost targeted at driving value for clients.

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

Our strategies and approaches are tightly structured and aim to provide the overall security required for business continuity, as our services are packed into Security Operations, CyberDemia, Threat Intelligence, System Assessment and Audit, with Research & Development.

email

hello@cyberplural.com

web

cyberplural.com

blog

blog.cyberplural.com

cyberdemia

cyberdemia.cyberplural.com

social

cyberplural