



**PANDUAN PENANGANAN INSIDEN
WEB DEFACEMENT JUDI ONLINE**

**DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN BARITO SELATAN**

CSIRT-BARSEL



DAFTAR ISI

PENDAHULUAN	3
1. PENGERTIAN.....	4
2. DAMPAK.....	5
3. ALUR SERANGAN	6
4. PENANGANAN INSIDEN	9
5. MITIGASI	19
REKOMENDASI	20

PENDAHULUAN

Insiden serangan siber semakin marak di Indonesia sejalan dengan pesatnya perkembangan teknologi informasi serta pemanfaatannya diberbagai sektor. Demikian pada sektor pemerintahan, dimana digalakkannya penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE). Pemerintah Kabupaten Barito Selatan yang juga menerapkan SPBE juga tidak luput dari insiden serangan siber. Salah satu bentuk insiden serangan siber yang marak adalah Web Defacement Slot Gacor atau Judi Online yang mengubah tampilan halaman-halaman website.

Dokumen ini dibuat berdasarkan seringnya insiden tersebut terjadi. Dokumen berisikan tentang alur serangan web defacement, cara penanggulangan dan pemulihan atas insiden web defacement serta langkah mitigasi untuk meminimalisir kemungkinan terkena serangan web defacement pada sebuah situs website.

Buntok, Februari 2024

**KEPALA BIDANG
INFORMATIKA, PERSANDIAN DAN STATISTIK
DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN BARITO SELATAN,**



PAHMI MINTARAGA, S.Hut
Pembina (IV/a)
NIP. 19750423 200701 1 013

1. PENGERTIAN

Web defacement merupakan suatu serangan pada website yang mengubah tampilan asli atau konten dari sebuah website. Pelaku serangan web defacement disebut sebagai defacer. Web defacement seringkali dimanfaatkan untuk menguji kemampuan defacer dan sebagai tindakan vandalisme elektronik. Web defacement dapat juga dimanfaatkan untuk kepentingan agenda politik, karena dapat menurunkan reputasi atau kredibilitas dari pihak tertentu.

Serangan web defacement dapat dilakukan dengan memanfaatkan sebuah kelemahan dari sistem sehingga memungkinkan pelaku memiliki akses masuk hingga ke server dan memiliki kewenangan untuk mengganti atau menghapus konten suatu website. Terdapat berbagai metode untuk melakukan web defacement, cara yang sering dijumpai yaitu eksploitasi pada kerentanan plugins framework dan SQL Injection yang memungkinkan akses administratif.

Web defacement belakangan ini marak terjadi pada situs milik pemerintah dan pendidikan, terutama web defacement judi online. Insiden ini terdeteksi cukup masif hingga menyebabkan puluhan bahkan ratusan situs terdampak. Dampak nyata dari web defacement judi online yaitu situs menampilkan halaman judi online. Salah satu alasan hal tersebut banyak menyasar situs milik pemerintah dan pendidikan diindikasikan sebagai cara untuk menghindari situs di-block oleh pihak berwenang.

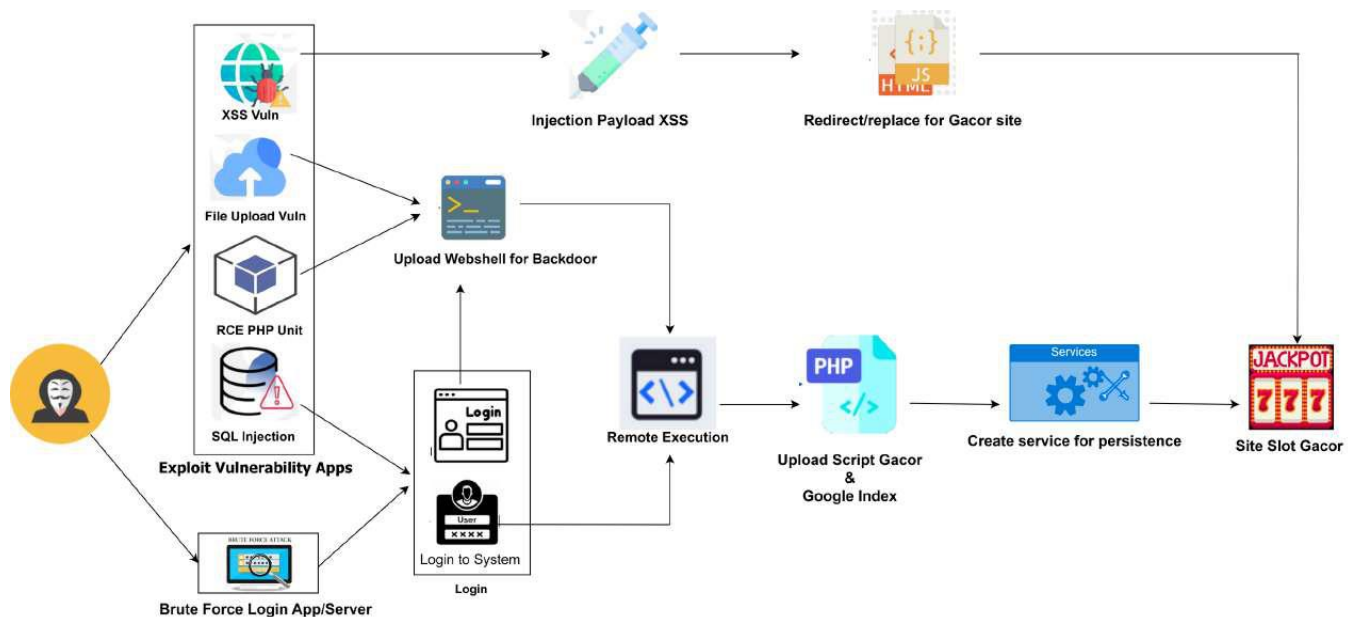
2. DAMPAK

Dampak dari insiden serangan web defacement judi online ini adalah:

- **Reputasi:** Tampilan halaman judi online yang tidak pantas atau ilegal pada situs pemerintah akan memberikan kesan negative terhadap integritas.
- **Kepercayaan:** Keamanan dan keandalan situs pemerintah akan diragukan oleh masyarakat dan kemampuan pemerintah dalam melindungi data sensitif dan informasi public jugaikut diragukan.
- **Availability:** Defacement dapat menyebabkan gangguan pada layanan yang disediakan oleh situs pemerintah serta dapat menyebabkan ketidaknyamanan dan ketidakpuasan masyarakat terhadap pemerintah.

3. ALUR SERANGAN

Alur serangan merupakan suatu metode atau jalan yang digunakan oleh penyerang untuk melancarkan serangan. Alur serangan menggambarkan cara penyerang memanfaatkan kelemahan atau celah dalam sistem untuk memperoleh akses tidak sah terhadap sistem.



A. INITIAL ACCES

Initial access melibatkan upaya dalam memanfaatkan kerentanan dan kesalahan pada konfigurasi untuk dapat masuk kedalam sistem. Web defacement judi online diidentifikasi memanfaatkan Exploit Vulnerability Apps dan Brute Force Attack untuk masuk ke dalam sistem.

- Exploit Vulnerability Apps

Penyerang melakukan percobaan eksploitasi kerentanan pada software dan teknologi sistem yang digunakan. Kerentanan dapat berupa bug atau security misconfiguration. Berikut beberapa initial access yang dimanfaatkan penyerang dalam defacement judi online.

- 1) XSS Vulnerability

Penyerang memanfaatkan kerentanan XSS (Cross Site Scripting) untuk melakukan injection payload XSS dengan tujuan untuk menyisipkan script judi online sehingga script akan tertanam pada salah satu halaman legitimate yang secara otomatis ketika diakses akan tereksekusi dan menampilkan halaman judi online.

2) File Upload Vulnerability

Penyerang memanfaatkan kerentanan file upload yang tidak menerapkan filtering dan sanitasi dengan baik sehingga penyerang dapat melakukan upload webshell atau backdoor.

3) PHP Unit Vulnerability

Penyerang sering memanfaatkan kerentanan PHP Unit yang dapat berdampak pada remote code execution. Penyerang akan melakukan instalasi backdoor atau webshell.

4) SQL Injection

Kerentanan SQL Injection juga menjadi salah satu attack vector yang sering dimanfaatkan penyerang dalam melakukan defacement judi online. Kredensial hasil SQL Injection dapat digunakan untuk login aplikasi bahkan ke sistem.

- Brute Force Login

Penyerang sering kali melakukan brute force attack pada aplikasi dan juga pada layanan remote access yang diaktifkan (SSH). Dalam beberapa kasus diketahui bahwa brute force terjadi karena penggunaan password yang tidak kuat sehingga dapat dengan mudah dilakukan brute force attack. Contoh penggunaan password yang dijumpai berhasil dilakukan brute force antara lain 12345, password, admin dan lainnya.

B. EXECUTION

Penyerang akan melakukan aktivitas pada server untuk dapat melakukan penyisipan script judi online, beberapa aktivitas yang dilakukan antara lain:

- Remote Execution

Penyerang memanfaatkan backdoor yang telah tertanam pada server untuk melakukan remote code execution seperti melakukan pembuatan akun dan membuat file-file deface. Beberapa webshell atau backdoor yang sering ditemukan pada defacement judi online yaitu Lzt.zip.gz.txt.php, Mad.php (<https://github.com/MadExploits/Gecko>), dan alfa.php (<https://github.com/backdoorhub/shell-backdoor-list/blob/master/shell/php/alfa.php>).

- Upload script Judi Online dan Google Index

Penyerang akan melakukan modifikasi pada file .htaccess untuk mengizinkan beberapa file webshell untuk dapat dieksekusi pada folder yang telah ditentukan. Kemudian penyerang akan membuat folder SlotGacor yang berisi file index.php dan Google Indexing dengan tujuan supaya akan tampil paling atas pada mesin pencarian Google.

C. PERSISTENCE

Penyerang melakukan mekanisme persistence untuk memastikan akses mereka terhadap server korban tetap tersedia. Berikut beberapa mekanisme persistence yang terjadi pada defacement judi online.

- Penyisipan Backdoor/Webshell

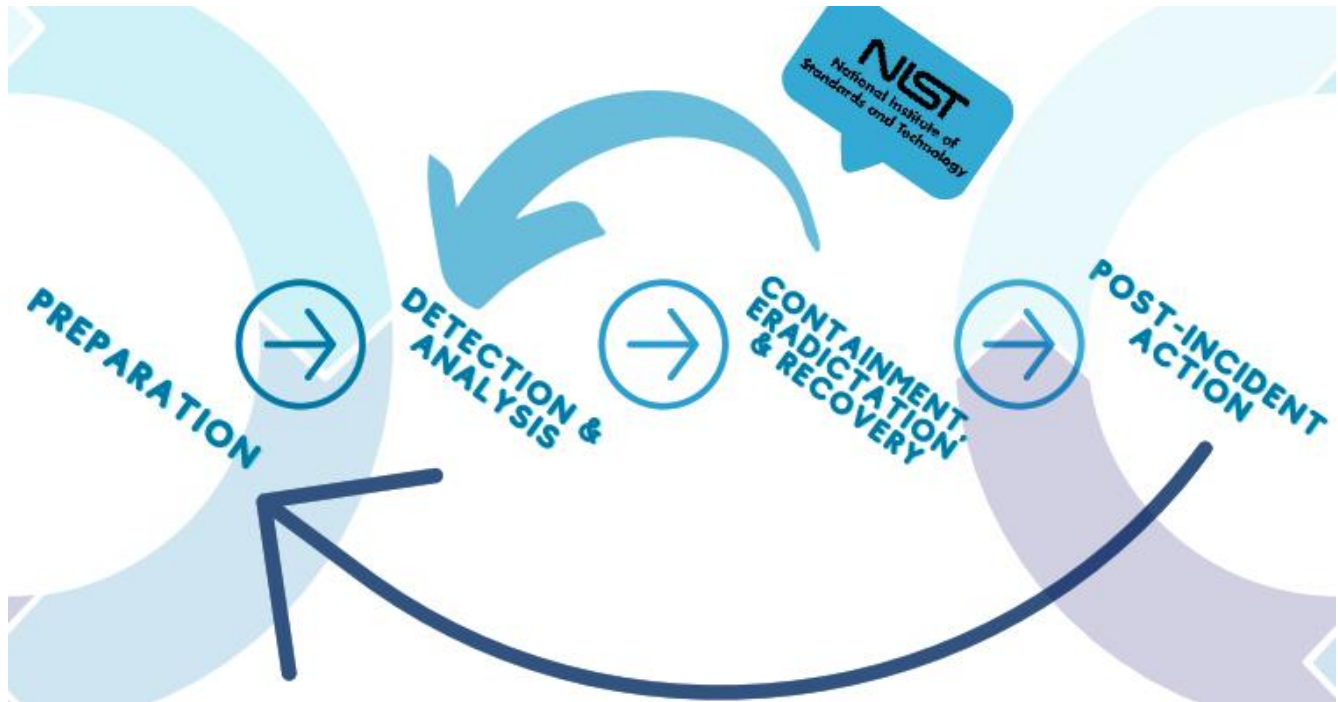
Penyisipan dan upload backdoor atau webshell sering ditemukan pada insiden defacement. Penyerang memanfaatkan webshell sebagai pintu untuk masuk ke server. Beberapa webshell yang sering ditemukan antara lain Lzt.zip.gz.txt.php, Mad.php, b374k.php, dan alfa.php.

- Pembuatan Process dan Service

Beberapa kasus dijumpai bahwa penyerang juga melakukan persistence dengan membuat process dan service yang secara terus-menerus berjalan untuk memastikan bahwa tampilan judi online tidak dapat dihapus. Ketika folder Slot-Gacor dihapus, secara otomatis services dan process akan melakukan generate folder dan isinya kembali. Services yang ditemukan pada insiden defacement judi online antara lain jj.service, ii.srevice, dan cahce-l.service.

4. PENANGANAN INSIDEN

Penanganan insiden web defacement slot gacor atau judi online dapat dilakukan mengikuti prosedur dari Computer Security Incident Handling Guide NIST 800-52 sebagai berikut:



A. PREPARATION

Tahap ini adalah tahap dimana kebijakan, prosedur, teknologi, dan sumber daya manusia harus disiapkan secara matang. Dalam suatu organisasi/institusi, kemampuan melakukan respon yang cepat terhadap suatu insiden merupakan suatu keharusan. Persiapan digunakan untuk mempersiapkan segala sesuatu untuk melakukan penanganan insiden. Beberapa hal yang perlu dipersiapkan dalam tahap preparation antara lain:

- Pembentukan Tim Tanggap Insiden Siber

Pembentukan tim tanggap insiden siber dapat membantu memfokuskan langkah penanganan insiden yang akan dilakukan, sehingga proses penanganan insiden dapat dilakukan dengan cepat dan tepat.

- Penyiapan Dokumen Legal

Dalam melakukan penanganan insiden tentu akan melibatkan dokumen-dokumen terkait dengan sistem berupa spesifikasi sistem. Beberapa dokumen yang perlu disiapkan antara lain:

- 1) Dokumen topologi jaringan
- 2) Dokumen kebijakan atau prosedur penggunaan sistem
- 3) Dokumen informasi aset aset
- 4) Dokumen Chain of Custody (CoC)
- 5) Dokumen Business Continue Plan (BCP), jika terjadi gangguan pada proses bisnis
- 6) Dokumen Incident Response Plan (IRP).

- Melakukan Koordinasi Dengan Pihak - Pihak Terkait

Koordinasi menjadi hal yang penting dalam melakukan penanganan insiden. Dengan telah terbentuknya Tim Tanggap Insiden Siber atau CSIRT maka dapat melakukan koordinasi dengan CSIRT Sektorial serta CSIRT Organisasi lainnya sehingga dapat dilakukan sharing informasi dalam mempercepat proses penanganan insiden. Koordinasi dapat dilakukan dengan antara lain:

- 1) CSIRT Sektorial
- 2) CSIRT Organisasi
- 3) Aparat Penegak Hukum
- 4) Nat-CSIRT (BSSN)

- Menyiapkan Jump Kit Penanganan Insiden

Jump Kit merupakan peralatan atau tools yang digunakan untuk melakukan penanganan insiden, dalam hal ini insiden web defacement judi online. Berikut merupakan beberapa tools yang dapat digunakan untuk proses penanganan dan analisis insiden web defacemen judi online.

Evidence Collection	Computer Forensics	IoC Scanner
dd	FTK Imager	ThorLite
FTK imager	Autopsy	Yara Rules
KAPE	Volatility	Redline

- Melakukan Identifikasi Aset Terdampak

Ketika telah terjadi insiden, maka perlu dengan segera dilakukan proses identifikasi aset terdampak. Identifikasi aset terdampak bertujuan untuk melakukan isolasi dan mengganti sistem atau layanan terdampak menggunakan sistem backup.

B. DETECTION & ANALYSIS

Merupakan tahap yang dilakukan secara berulang dengan tujuan untuk dapat mendeteksi adanya malicious file, backdoor, atau webshell pada sistem dan melakukan analisis untuk menemukan root cause insiden yang terjadi. Langkah-langkah yang dapat dilakukan dalam melakukan penanganan insiden web defacement judi online antara lain:

- Melakukan Akuisisi & Pengumpulan Barang Bukti Digital

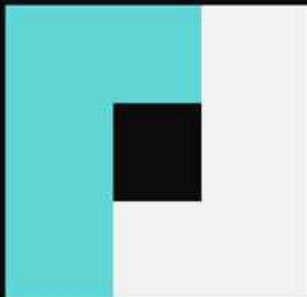
Setelah dilakukan identifikasi aset dan dilakukan isolasi, maka selanjutnya dilakukan pengumpulan barang bukti digital untuk proses analisis. Pengumpulan barang bukti digital dapat dilakukan secara full acquisition atau dengan pengumpulan artefak-artefak.

- 1) Pengambilan artefak pada Windows dapat menggunakan tools KAPE GUI.
- 2) Pengambilan artefak pada Linux dapat dilakukan pada Log akses (/var/log/), bash history (/root dan /home)
- 3) Full Acquisition pada Windows dapat menggunakan tools FTK Imager.
- 4) Full Acquisition pada Linux dapat menggunakan tools dd dengan perintah:

dd if=/dev/sdb of=USB_image.dd bs=4k conv=noerror,sync status=progress

```

awang@CLOUD: /mnt/c/Users/Awan/Downloads/thor18.7lite-linux-pack
$ ./thor-lite-linux --intense --norescontrol --cross-platform --alldrives -p /mnt/c/Users/Awan/Documents/Hunting/
Notice Some modules and features are not available in Lite version and will be disabled
Notice This THOR Lite license permits non-commercial use only. It is strictly prohibited to sell THOR Lite or sell servi
ces that include the use of THOR Lite. For details, see the EULA in the ./docs folder. For a special license that covers
these cases and suppresses this message, please contact our sales via https://www.nextron-systems.com/get-started/


THOR Lite
APT Scanner

Version 18.7.3 (2022-07-27 02:57:26)
(c) Nextron Systems GmbH

Lite Version

> Scan Information
Info Thor Version: 18.7.3
Info Thor Build: 11e67272966 (2022-07-27 02:57:26)
Info Run on system: CLOUD
Info Running as user: awan

```

- Melakukan Scanning Pada Server Terdampak

Scanning dapat dilakukan secara langsung pada server terdampak atau pada file hasil akuisisi (full akuisisi/image). Scanning dapat dilakukan dengan menggunakan tools opensource, seperti **Thor Lite Scanner** yang dapat digunakan untuk mendeteksi kemungkinan malicious file/backdoor/webshell (<https://www.nextron-systems.com/thor-lite/>). Setelah dilakukan scanning maka dapat dilakukan validasi hasil scanning untuk menghindari false positif. Berikut merupakan perintah untuk melakukan scanning spesifik folder menggunakan Thor Lite Scanner:

```
sudo ThorLinux -a Filescan --intense --norescontrol --cross-platform --alldrives -p [path]
```

- Melakukan Pengecekan Koneksi Command and Center (Cnc)

Command and Center (CnC) merupakan infrastruktur yang digunakan oleh penyerang untuk melakukan kontrol terhadap server yang telah terinfeksi. Untuk melakukan pengecekan terhadap kemungkinan CnC maka dapat dilakukan pengecekan port-port terbuka yang memiliki keterangan LISTENING dan ESTABLISHED. Pengecekan port suspicious dapat dilakukan dengan cara dibawah dan selanjutnya dilakukan validasi terhadap beberapa port yang diindikasikan sebagai suspicious.

- Pada Linux: `sudo netstat -tulpn`

```
reed@ubuntu:~$ sudo netstat -tulpn
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 10.0.3.1:53             0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:11211         0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:5432          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
```

- Pada Windows: `netstat -ano`

```
C:\Windows\System32>netstat -ano

Active Connections

Proto Local Address           Foreign Address         State       PID
TCP 0.0.0.0:135              0.0.0.0:0               LISTENING   1912
TCP 0.0.0.0:445              0.0.0.0:0               LISTENING   4
TCP 0.0.0.0:902              0.0.0.0:0               LISTENING   13504
TCP 0.0.0.0:912              0.0.0.0:0               LISTENING   13504
TCP 0.0.0.0:1042             0.0.0.0:0               LISTENING   31380
TCP 0.0.0.0:1043             0.0.0.0:0               LISTENING   31380
TCP 0.0.0.0:1947             0.0.0.0:0               LISTENING   4648
TCP 0.0.0.0:2968             0.0.0.0:0               LISTENING   3740
TCP 0.0.0.0:3655             0.0.0.0:0               LISTENING   4
TCP 0.0.0.0:5040             0.0.0.0:0               LISTENING   15448
TCP 0.0.0.0:5357             0.0.0.0:0               LISTENING   4
TCP 0.0.0.0:7070             0.0.0.0:0               LISTENING   6852
TCP 0.0.0.0:9012             0.0.0.0:0               LISTENING   4112
TCP 0.0.0.0:9013             0.0.0.0:0               LISTENING   4112
```

- Melakukan Pengecekan Mekanisme Presistent

Mekanisme persistent yang digunakan oleh penyerang web defacement judi online salah satunya yaitu membuat Slot-Gacor tidak dapat dihapus, sehingga ketika folder Slot-Gacor dihapus secara otomatis akan muncul kembali. Untuk melakukan pengecekan mekanisme persistent tersebut dapat menggunakan tools auditd pada Linux. Auditd merupakan layanan pada Linux yang berfungsi untuk melakukan pencatatan seluruh aktivitas pada Linux, sehingga ketika terdapat process dan service yang berjalan secara terus-menerus, auditd akan mencatatnya. Berikut merupakan cara melakukan pengecekan mekanisme persistent:

- Pada Linux:

1) Melakukan audit

```
sudo apt install auditd
```

```
sudo nano /etc/audit/rules.d/10-procmon.rules
```

tambahkan rules berikut:

```
-a exit,always -F arch=b64 -S execve -k procmon
```

```
-a exit,always -F arch=b32 -S execve -k procmon
```

```
sudo service auditd restart
```

Selanjutnya dilakukan pemantauan pada file audit.log yang terdapat pada folder /var/log/audit/

Untuk menampilkan isi file audit.log dapat menggunakan perintah

```
sudo tail -f /var/log/audit/audit.log
```

atau

```
sudo cat /var/log/audit/audit.log
```

```
p0=FSUID=33 tty=(name) ses=4294967295 comm=sleep exe=/usr/bin/sleep subj=unconfined key='process' BARCH=x86_64 SYSCALL=execve AUDIT unset UID=www  
p1/www-data% 361D '%vvw-data' FSUID '%vvw-data'  
t(1678347175.849:56580): argc=2 ab='touch' at='/  
678347175.849:56580)' cwd='/dev/shm'  
slot-ganor/.htaccess'  
678347175.849:56580): item=6 name='/usr/bin/touch' inode=19324837 dev=80:02 mode=0100755 uid=6 ogid=6 rdev=00:00 nametype=NORMAL cap_fo=6 cap_i=6 cap fe  
678347175.849:56580): item=1 name='/lib64/lib-linux-s6-64.so.2' inode=19323784 dev=80:02 mode=0100755 uid=6 ogid=6 rdev=00:00 nametype=NORMAL cap_fo=6 ca
```

```
%dit(1678347175.849:56580): proc_title=FAF7553A0802F61707B1365278F7641222F7777Z7E04697364754863617066622620961667961726801622607672E56642F736C6742D067  
t(1678347175.849:56580): arch=c000000 syscall=59 success=yes exit=0 ae=55999da1868 at=55999da245d a2=55999da1230 a3=8 items=2 ppid=201850 ppid=200630  
d=33 fsuid=33 tty=(name) ses=4294967295 comm=sleep exe=/usr/bin/sleep subj=unconfined keys='process' BARCH=x86_64 SYSCALL=execve AUDIT unset UID=www  
p1/www-data% 361D '%vvw-data' FSUID '%vvw-data'  
t(1678347175.849:56580): argc=2 ab='sleep' at='/0,1'
```

2) Menggunakan list services

Untuk mengecek services yang berjalan dapat juga dilakukan dengan menggunakan perintah

```
sudo systemctl list-units --type service | grep running
```

untuk mengetahui detail services yang berjalan dapat menggunakan perintah

```
sudo service name_service status
```

Beberapa nama services yang ditemukan pada kasus defacement judi online antara lain cache-l.service, ii-service, dan jj-service dengan keterangan services “Jendral Maya Still Alive”.

3) Menggunakan list process

Perintah yang dapat digunakan untuk mengetahui proses yang berjalan adalah sebagai berikut:

```
sudo ps aux
```

atau

```
sudo ps aux | www-data
```

Beberapa kasus defacement judi online menggunakan mekanisme persistent dengan menjalankan proses dengan bash script yang terencode base64.

```

22078 0.0 0.0 239604 7228 ? Ssl Feb10 0:01 /usr/libexec/upoword
23029 0.0 0.0 394756 12094 ? Ssl Feb10 0:06 /usr/libexec/padlock2/udiskd
15375 0.0 0.0 294376 18960 ? Ssl Feb11 0:14 /usr/libexec/packageltd
73667 0.0 0.0 7368 3296 ? Ss Feb11 17:41 /bin/bash -c while sleep 2; do echo cGF0PS9hcHBzZXJ2L3ZhcjE93cmlmIFAgISAtIzAkcGF0F0gJlYgWYAhIClKQoZGlybmFrTZAkcGF0KSBDQDyOBoAGVUClAgICBta2RpciAtcCAkKRgpcmShbWUgJHBBhdCkgJlYgY3VybnByeSBhbHJlYWRSIGV4XHNocykzMkkaKAWYgYAiJChndZGF0ICllICclLVScGhBgogICAgICBtZWV2dGhJGVzZXI160JH.
99855 0.0 0.0 5768 1028 ? S 10:09 0:00 sleep 2
161933 0.0 0.0 9288 4720 ? Ss Feb12 23:29 /bin/bash -c while sleep 2; do echo cGF0PS9hcHBzZXJ2L3ZhcjE93cmlmIFAgISAtIzAkcGF0F0gJlYgWYAhIClKQoZGlybmFrTZAkcGF0KSBDQDyOBoAGVUClAgICBta2RpciAtcCAkKRgpcmShbWUgJHBBhdCkgJlYgY3VybnByeSBhbHJlYWRSIGV4XHNocykzMkkaKAWYgYAiJChndZGF0ICllICclLVScGhBgogICAgICBtZWV2dGhJGVzZXI160JH.
99864 0.0 0.0 5768 1028 ? S 10:09 0:00 sleep 2
22534 0.0 0.0 17464 8844 ? Ss Feb13 0:00 /lib/systemd/systemd --user
22535 0.0 0.0 171480 5972 ? Ss Feb13 0:00 - {sd-pam}
22541 0.0 0.0 38740 5812 ? Ssl Feb13 0:00 - /usr/bin/pipewire
22542 0.0 0.0 22912 5832 ? Ssl Feb13 0:16 - /usr/bin/pipewire-media-session
22543 0.0 0.0 293032 62768 ? Ssl Feb13 0:01 - /usr/bin/pulseaudio --daemonize=no --log-target=journal
22545 0.0 0.0 10236 4964 ? Ss Feb13 0:00 - /usr/bin/dbus-daemon-om --session --address=systemd: --no-f
60252 0.0 0.0 9288 4704 ? Ss Feb13 23:27 /bin/bash -c while sleep 2; do echo cGF0PS92YXlvd3d3L3NpbWVwITcGF0YQppZABbICcgLWYgJHBBhdCBdCIYmlFsgISAtIzAkcKGpcmShbWUgJHBBhdCkgXTsgdGhlgogICAgBtKaXIgLUAqJChkaXJuYWI1ICRrYXOpICYmlIGBkeXJlY3RvcnkvIWxyZWFeSBlleGlmdDHIImZmpCmlmIFsgJlQoc3RhdkCAtYyApJVUuICRrYXOpIlAhPSAIJHVvZXI1IF07IHROZW4KICAgIGNob3duICF89865 0.0 0.0 5768 1024 ? S 10:09 0:00 sleep 2
42657 0.0 0.0 2888 576 ? S Feb15 0:00 sh /home/[REDACTED] bin/441438abdlac652551dd
ver --host=127.0.0.1 --accept-server-license-terms --enable-remote-auto-shutdown --port=0 --telemetry-level all --con
ec8a499b8bf.token
42667 0.0 2.7 3966892 181368 ? Sl Feb15 1:49 /home/[REDACTED] bin/441438abdlac652551dd
[REDACTED] bin/441438abdlac652551ddbe4d08dfcec8a499b8bf/out/server-main.js --start-server --host=127.0.0.1 --m
etry-level all --connection-token-file /home/[REDACTED].441438abdlac652551ddbe4d08dfcec8a499b8bf.t
48250 0.0 0.0 9824 2536 ? Ss Feb15 0:00 /usr/sbin/xinetd -pidfile /run/xinetd.pid -stayalive -inet_c
49050 0.0 0.0 41328 3820 ? Ss Feb15 0:29 /usr/lib/cosatfix/sbin/master -w

```

➤ Pada Windows:

Untuk melakukan pengecekan suspicious services pada Windows dapat menggunakan GUI yaitu dengan mengetikkan Windows + R lalu ketik services.msc. selanjutnya dapat dilakukan pengecekan daftar services yang berjalan apakah terdapat services mencurigakan. Untuk melakukan pengecekan process, pada Windows dapat menggunakan tools command line tasklist. Ketikkan tasklist pada command-line sehingga akan muncul daftar process yang berjalan.

```
C:\Windows\System32>tasklist
```

Image Name	PID	Session Name	Session#	Mem Usage
System Idle Process	0	Services	0	8 K
System	4	Services	0	11.248 K
Secure System	140	Services	0	74.672 K
Registry	192	Services	0	55.084 K
smss.exe	868	Services	0	1.100 K
csrss.exe	1412	Services	0	6.524 K
wininit.exe	1544	Services	0	6.292 K
services.exe	1616	Services	0	13.616 K
LsaIso.exe	1624	Services	0	3.612 K
lsass.exe	1652	Services	0	31.652 K
svchost.exe	1772	Services	0	41.660 K
fontdrvhost.exe	1800	Services	0	3.092 K

- Melakukan Pencarian Malicious File atau Suspicious File

Selain menggunakan metode scanning Thor Lite Scanner, untuk menemukan malicious file atau suspicious file dapat dilakukan dengan menggunakan pencarian melalui command-line. Untuk melakukan pencarian diperlukan keyword seperti “Slot-Gacor”, “shell.php”, dan lainnya.

```
sudo apt install locate && update
```

```
sudo locate slot- atau sudo locate gacor
```

```
sudo locate nama_shell.php
```

atau menggunakan command find

```
sudo find / -type f -executable -printf "%T+ %p\n" 2>/dev/null | grep -Ev "000| /site-packages/python/node_modules|.sample|gems" | sort r | head -n 100
```

- Melakukan Analisis Pada Barang Bukti Digital yang Telah Dikumpulkan

- Pada Linux:

Analisis barang bukti dapat dilakukan pada log akses dan log system (auth, wtmp, btmp, auditd). Seluruh log tersebut tersimpan pada folder /var/log/. Log akses terdapat pada /var/log/apache2 atau /var/log/httpd

- Pada Windows:

Log akses server Windows secara default terdapat pada folder engine website. Pada web server XAMPP terdapat pada folder xampp/apache/logs. Selain melakukan analisis pada log akses, terdapat windows event log yang terdapat pada folder

C:\Windows\System32\winevt\logs atau C:\Windows\System32\config.

Untuk melakukan analisis secara otomatis pada Windows Event Log dapat menggunakan tools **Hayabusa** yang dapat diunduh pada laman <https://github.com/Yamato-Security/hayabusa>. Hayabusa akan melakukan scanning Windows Event Log berdasarkan Sigma rules.

C. CONTAINMENT, ERADICATION & RECOVERY

- Melakukan Pengarsipan dan Penghapusan File Malicious dan Suspicious yang Ditemukan

Pengarsipan file malicious dan suspicious termasuk script judi online sebelum dilakukan penghapusan bertujuan untuk analisis lebih lanjut dan dapat memanfaatkan file-file tersebut untuk membuat rules deteksi untuk perangkat keamanan. Setelah file-file tersebut diarsipkan, selanjutnya dapat dilakukan pembersihan atau penghapusan.

- Melakukan Modifikasi File .htaccess

Penyerang melakukan modifikasi file .htaccess untuk mengizinkan malicious file dengan ekstensi tertentu dapat dieksekusi. Oleh karena itu perlu dilakukan modifikasi kembali pada file .htaccess.

- Melakukan Pembatasan Akses Pada Server Terdampak

Pembatasan akses pada server terdampak dilakukan dengan cara melakukan blocking alamat IP yang terindikasi melakukan aktivitas malicious. Selain itu juga dapat dilakukan penutupan port untuk remote access, sehingga akses ke server hanya dapat dilakukan secara local atau menggunakan VPN. Hal ini bertujuan untuk menghindari kemungkinan lateral movement.

- Melakukan Kill Process dan Service Malicious atau Suspicious

Pada beberapa kasus defacement judi online diketahui bahwa terdapat process dan services yang berjalan secara terus-menerus sebagai mekanisme persistent. Oleh karena itu perlu dilakukan pengarsipan file process dan services tersebut untuk analisis lebih lanjut dan selanjutnya dilakukan penghentian atau kill process.

➤ Pada Linux:

- 1) Kill Process

```
sudo kill -9 PID_process
```

- 2) Kill & delete Service

```
sudo service name_service stop
```

```
sudo service name_service disable
```

```
sudo rm /etc/systemd/system/name_service.service
```

- 3) Penghapusan file dan folder malicious/suspicious

```
sudo rm -r folder_slot
```

```
sudo rm name_shell.php
```

➤ Pada Windows:

- 1) Kill Process

```
taskkill /PID pid_process /F
```

- 2) Kill & delete Service

```
sc query state-all | find "name_service"
```

```
sc stop name_service
```

```
sc delete name_service
```

- 3) Penghapusan file dan folder malicious/suspicious

Penghapusan pada Windows dapat dilakukan dengan menggunakan shift+delete

- Melakukan Hardening Sistem Dan Server

Sebelum dilakukan proses pemulihan, pastikan seluruh malicious file dan suspicious telah dilakukan pengarsipan dan penghapusan. Langkah selanjutnya yang dapat dilakukan yaitu:

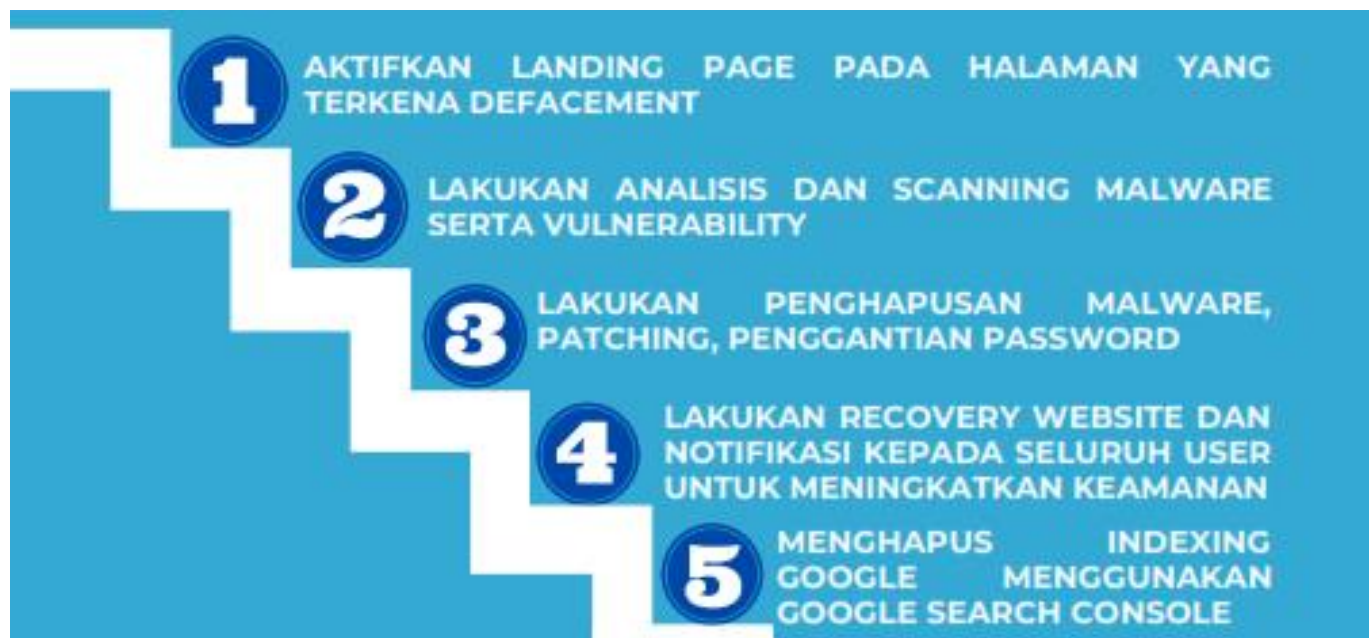


- Melakukan Pemulihan Atau Recovery

Setelah beberapa tahap hardening telah dilakukan, maka selanjutnya proses pemulihan atau recovery dapat dilakukan. Setelah proses pemulihan berhasil hendaknya sistem selalu dilakukan maintenance secara berkala dan pemantauan secara proaktif untuk mendeteksi dan menghindari kejadian serupa terjadi Kembali.

5. MITIGASI

Mitigasi dalam insiden web defacement slot gacor atau judi online dapat dilakukan dengan langkah-langkah berikut ini sebagai penanganan pertama dari serangan web defacement menurut BSSN:



REKOMENDASI

BSSN sebagai Badan Siber dan Sandi Negara merekomendasikan hal yang dapat dilakukan pemilik sistem sebagai upaya penguatan dan pencegahan terhadap serangan Web Defacement sesuai Panduan Keamanan Sistem Informasi (ISO/IEC 27002:2013) yaitu sebagai berikut :

A. PEMBARUAN SISTEM

- Rujukan: ISO/IEC 27002:2013, kontrol A.12.6.1 - Manajemen pembaruan system.
- Pastikan sistem operasi, server web, basis data, dan perangkat lunak lainnya diperbarui secara teratur dengan memasang pembaruan keamanan terbaru. Hal ini akan mengurangi risiko eksploitasi kerentanan yang diketahui oleh penyerang.

B. PENGATURAN KEAMANAN

- Rujukan: ISO/IEC 27002:2013, kontrol A.13.2.1 - Kebijakan keamanan sistem.
- Terapkan kebijakan keamanan yang memadai untuk server web dan sistem terkait. Konfigurasi server web dengan pengaturan keamanan yang sesuai, termasuk pengecualian file yang tidak perlu dan mematikan fitur yang tidak diperlukan.

C. KONTROL AKSES

- Rujukan: ISO/IEC 27002:2013, kontrol A.9.1.2 - Manajemen hak akses pengguna.
- Terapkan manajemen hak akses pengguna yang ketat. Berikan izin akses yang sesuai kepada pengguna berdasarkan prinsip kebutuhan paling sedikit (principle of least privilege).

D. PEMANTAUAN KEAMANAN

- Rujukan: ISO/IEC 27002:2013, kontrol A.12.4.1 - Pemantauan penggunaan system.
- Gunakan alat pemantauan keamanan untuk mengawasi aktivitas situs web. Tinjau log dan deteksi aktivitas yang mencurigakan, seperti upaya login yang tidak sah atau perubahan file yang tidak diinginkan.

E. PERLINDUNGAN PASSWORD

- Rujukan: ISO/IEC 27002:2013, kontrol A.9.2.1 - Penggunaan password yang aman.
- Terapkan kebijakan penggunaan password yang kuat. Pastikan pengguna menggunakan password yang kompleks, dan tetapkan kebijakan penggantian password secara berkala.

F. BACKUP RUTIN

- Rujukan: ISO/IEC 27002:2013, kontrol A.12.3.1 - Manajemen backup.
- Lakukan backup rutin dari situs web dan database. Simpan salinan cadangan di lokasi yang aman dan pastikan proses pemulihan (restore) berfungsi dengan baik jika diperlukan.

G. PELATIHAN KEAMANAN

- Rujukan: ISO/IEC 27002:2013, kontrol A.10.1.1 - Kesadaran, pendidikan, dan pelatihan keamanan.
- Lakukan pelatihan keamanan bagi pengguna dan administrator situs web. Tingkatkan kesadaran mereka tentang praktik keamanan, seperti menghindari mengklik tautan yang mencurigakan atau memperbarui perangkat lunak yang penting.

H. AUDIT KEAMANAN

- Rujukan: ISO/IEC 27002:2013, kontrol A.12.6.2 - Manajemen kerentanan teknis.
- Lakukan audit keamanan secara teratur untuk mengidentifikasi kerentanan dan celah keamanan pada situs web. Tinjau dan perbaiki temuan secara teratur untuk meningkatkan keamanan.