ASEAN-Japan Online Cyber Exercise By Gov-CSIRT Indonesia

Auditorium Roebiono Kertopati
Badan Siber dan Sandi Negara
20 Juni 2019

Cek Kelengkapan

1. Koneksi Internet
   - SSID : WIFI PUBLIC BSSN - 4 / 5 / 10
   - Password : bssnwifi2019
2. Email

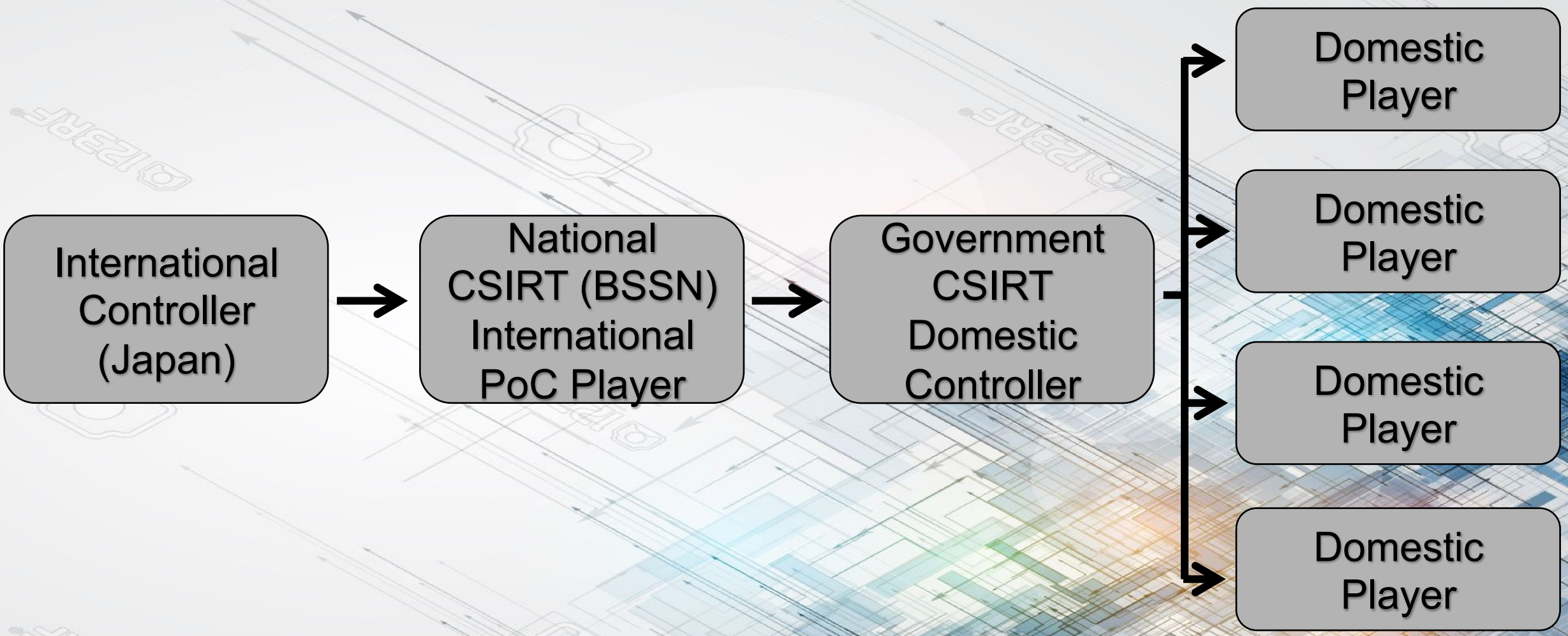
   TO : gulih.pemerintah@bssn.go.id

   CC : cyber.exercise@bssn.go.id

Aset

- Website Pemerintahan
- CMS : Drupal versi 8.5.10
- Keterangan tambahan :
  - Log Website
  - Daftar koneksi outbound server
  - File evil.php

Alur Komunikasi



Tes Komunikasi [GovCSIRT -> Konstituen]

To : **[Nama Instansi]**

From : gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject : COM_CHECK

[Latihan Latihan Latihan]

Kepada Yth Player,

Mohon meresepon email berikut ini. Diinformasikan bahwa pelaksanaan kegiatan ASEAN-Japan Cyber Exercise akan dilaksanakan pada pukul 14.00 WIB

Best Regards,

Direktorat Penanggulangan dan Pemulihan Pemerintah, BSSN

[Latihan Latihan Latihan]

Format Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: COM-CHECK_RESPON

[Latihan Latihan Latihan]

Yth Gov-CSIRT BSSN,

[Isi pesan]

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Stage 0 Simulation

[Phase 0]

Cek Email

To: **[Nama Instansi]**

From: gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject: Inject0_Simulation

[Latihan Latihan Latihan]

Selamat Siang,

Kami mendapat informasi dari ASEAN-Japan bahwa website anda melakukan serangan (fraud) pada salah satu website pemerintahan Japan. Berdasarkan hal tersebut, dimohon agar dapat melakukan investigasi terhadap website anda. Google dork : < 激安 -site:.jp inurl:go.id >

Best Regards,

Gov-CSIRT BSSN

[Latihan Latihan Latihan]

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject0_Simulation_Response

[Latihan Latihan Latihan]

Selamat Siang,

Terima kasih atas laporan yang diberikan, kami sebagai pemilik aset akan melakukan investigasi terhadap aset kami.

Best Regards,

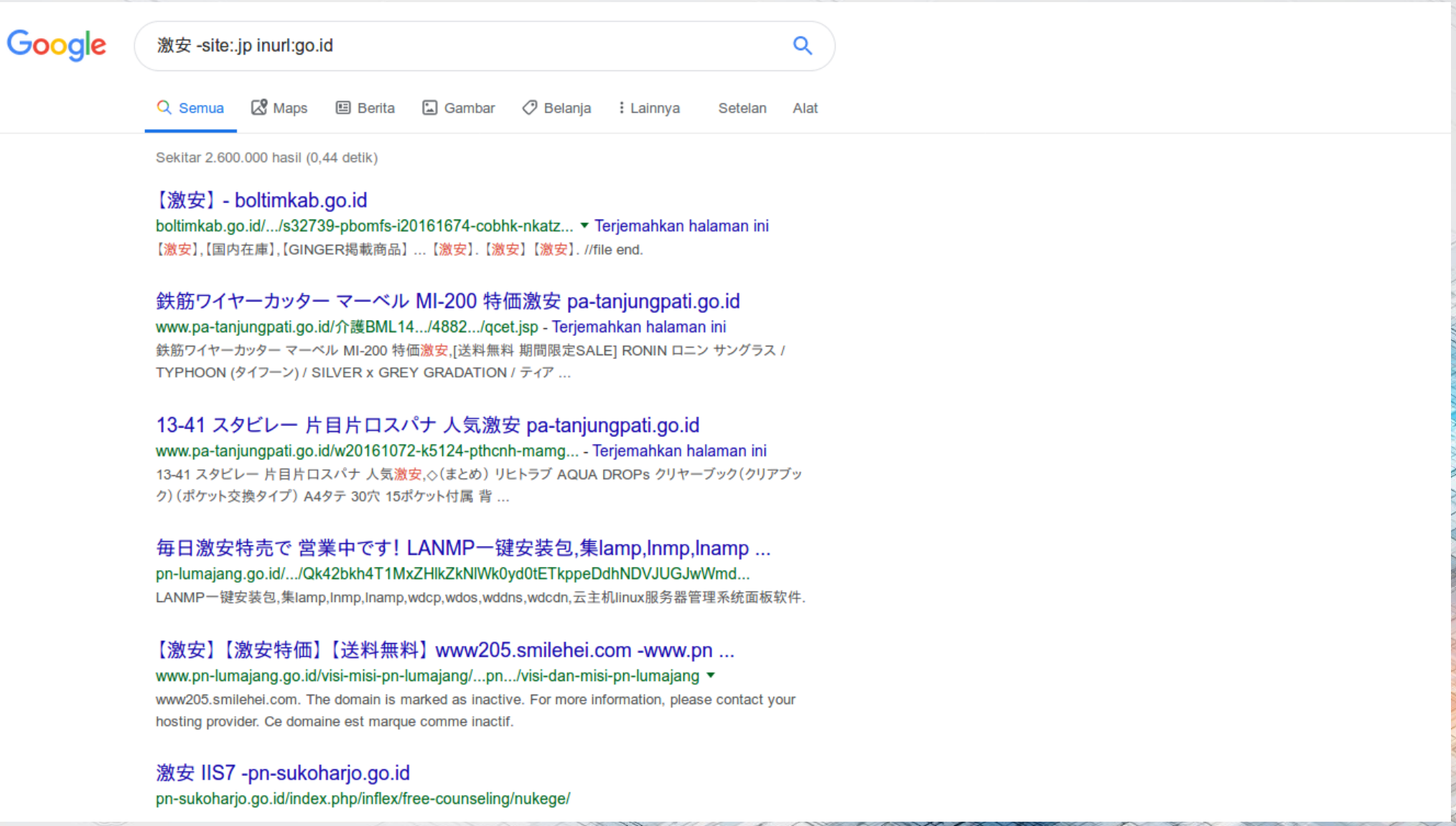
[Nama Instansi]

[Latihan Latihan Latihan]

Permasalahan

- Adanya aduan insiden siber dari publik bahwa aset anda diindikasikan telah melakukan serangan (fraud) pada website pemerintahan Japan
- Prosedur apa saja yang akan dilakukan oleh anda sebagai pemilik aset terhadap aduan tersebut?

Action


Google
激安 -site:.jp inurl:go.id
Semua
Maps
Berita
Gambar
Belanja
Lainnya
Setelan
Alat
Sekitar 2.600.000 hasil (0,44 detik)
【激安】- boltimkab.go.id
boltimkab.go.id/.../s32739-pbomfs-i20161674-cobhk-nkatz... Terjemahkan halaman ini
【激安】,【国内在庫】,【GINGER掲載商品】...【激安】.【激安】【激安】. //file end.
鉄筋ワイヤーカッター マーベル MI-200 特価激安 pa-tanjungpati.go.id
www.pa-tanjungpati.go.id/介護BML14.../4882.../qcet.jsp - Terjemahkan halaman ini
鉄筋ワイヤーカッター マーベル MI-200 特価激安,[送料無料 期間限定SALE] RONIN ロニン サングラス / TYPHOON (タイフーン) / SILVER x GREY GRADATION / ティア ...
13-41 スタビレー 片目片口スパナ 人気激安 pa-tanjungpati.go.id
www.pa-tanjungpati.go.id/w20161072-k5124-pthcnh-mamg... - Terjemahkan halaman ini
13-41 スタビレー 片目片口スパナ 人気激安,◇(まとめ) リヒトラブ AQUA DROPs クリヤーブック(クリアブック)(ポケット交換タイプ) A4タテ 30穴 15ポケット付属 背 ...
毎日激安特売で 営業中です! LANMP一键安装包,集lamp,lnmp,lnamp ...
pn-lumajang.go.id/.../Qk42bkh4T1MxZHlkZkNlWk0yd0tETkppeDdhNDVJUGJwWmd...
LANMP一键安装包,集lamp,lnmp,lnamp,wdcp,wdos,wddns,wdcdn,云主机linux服务器管理系统面板软件.
【激安】【激安特価】【送料無料】www205.smilehei.com -www.pn ...
www.pn-lumajang.go.id/visi-misi-pn-lumajang/...pn.../visi-dan-misi-pn-lumajang
www205.smilehei.com. The domain is marked as inactive. For more information, please contact your hosting provider. Ce domaine est marque comme inactif.
激安 IIS7 -pn-sukoharjo.go.id
pn-sukoharjo.go.id/index.php/inflex/free-counseling/nukege/

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject0_Preparation_Action

[Latihan Latihan Latihan]

Selamat Siang,

Kami selaku pemilik aset telah melakukan hal-hal sebagai berikut :

1) Mengumpulkan informasi terkait aduan tersebut
   - Periksa pada kolom search terkait Google dork : < 激安 -site:.jp inurl:go.id >

2) Melakukan investigasi pada aset kami, dst

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Stage 1 Injeksi 1

[Phase 1-1]

Cek Email

To: **[Nama Instansi]**

From: gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject: Inject1_Situation_Awareness

[Latihan Latihan Latihan]

Selamat Siang,

Kami mendapat informasi dari ASEAN-Japan bahwa website anda masuk ke dalam salah satu *Top Search Result* dalam hal pencarian *Shopping Websites* yang dioperasikan oleh Grup Hacker “FGP-01”. Berdasarkan hal tersebut, dimohon agar dapat melakukan investigasi terhadap website anda.

Best Regards,

Gov-CSIRT BSSN

[Latihan Latihan Latihan]

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject1_Situation_Awareness_Response

[Latihan Latihan Latihan]

Selamat Siang,

Terima kasih atas laporan yang diberikan, kami sebagai pemilik aset akan melakukan investigasi terhadap aset kami.

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Permasalahan

- Adanya aduan insiden siber dari publik bahwa aset anda diindikasikan telah melakukan redirection oleh kelompok hacker ke *Shopping Websites*
- Prosedur apa saja yang akan dilakukan oleh anda sebagai pemilik aset terhadap aduan tersebut?

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject1_Situation_Awareness_Action

[Latihan Latihan Latihan]

Selamat Siang,

Kami selaku pemilik aset telah melakukan hal-hal sebagai berikut :

1) ...

2) ... , dst **[Isi sesuai dengan prosedur masing-masing tim]**

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Expected Action

- Mengimplementasikan SOP terkait penanganan jika terdapat aduan
- Melakukan koordinasi dengan tim CSIRT terkait aduan ini
- Mengumpulkan informasi terkait aduan tersebut
  - Periksa pada kolom search terkait Shopping Websites
  - Melakukan hal sama dengan pelapor, untuk memastikan bahwa aduan sesuai dengan apa yang dilaporkan
- Mengumpulkan informasi terkait Grup Hacker “FGP-01”
  - Media sosial
  - Teknik Serangan
  - Source : IP address, malicious file (backdoor, webshell)

Stage 1 Injeksi 2

[Phase 1-2]

Cek Email

To: **[Nama Instansi]**

From: gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject: Inject2_Identification_and_Measurement_Deployment

[Latihan Latihan Latihan]

Selamat Siang,

Kami mendapat informasi dari Thailand bahwa terdapat vulnerability pada CMS **Drupal versi 8.5.x < 8.5.11** dan **Drupal versi 8.6.x < 8.6.10**. Silakan dilakukan pemeriksaan terhadap versi CMS yang digunakan pada aset anda.

Best Regards,

Gov-CSIRT BSSN

[Latihan Latihan Latihan]

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject2_Identification_and_Measurement_Deployment_Response

[Latihan Latihan Latihan]

Selamat Siang,

Terima kasih atas informasi yang diberikan, akan kami lakukan pemeriksaan versi aplikasi kami.

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Permasalahan

- Adanya Informasi bahwa terdapat kerawanan pada aplikasi CMS versi tersebut
- Prosedur apa saja yang akan dilakukan oleh anda sebagai pemilik aset terhadap informasi tersebut?

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject2_Identification_and_Measurement_Deployment_Action

[Latihan Latihan Latihan]

Selamat Siang,

Kami selaku pemilik aset telah melakukan hal-hal sebagai berikut :

1) ...

2) ... , dst

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Expected Action

- Memeriksa semua aset yang menggunakan CMS Drupal
- Memeriksa versi CMS Drupal, apakah sudah lampau atau sudah dilakukan update/upgrade
  - Jika ada versi yang out-of-date, tindak lanjut : dilakukan analisis lanjutan (indikasi adanya insiden)

Stage 1 Injeksi 3 & 4

[Phase 1-3 & 1-4]

Cek Email

To: **[Nama Instansi]**

From: gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject: Inject3&4_Information_Sharing (3 Attachment)

[Latihan Latihan Latihan]

Selamat Siang,

Kami mendapat informasi dari ASEAN-Japan bahwa telah banyak aduan terkait penipuan pada Fake Shopping Websites dan telah melaporkan insiden ini kepada agen Kepolisian setempat.

Oleh karenanya kepada seluruh instansi pemerintahan yang terkena dampak agar dapat melakukan investigasi lebih lanjut untuk menemukan Malicious Activity.

Best Regards,

Gov-CSIRT BSSN

[Latihan Latihan Latihan]

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject3&4_Information_Sharing_Response

[Latihan Latihan Latihan]

Selamat Siang,

Terima kasih atas informasi yang diberikan, akan kami lakukan pelaporan hasil investigasi kami.

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Permasalahan

- Pihak ASEAN-Japan telah melaporkan insiden ini kepada agen Kepolisian setempat
- Setiap instansi dihimbau untuk dapat melaporkan hasil investigasinya
  - [Hints!!]Gunakan file pendukung untuk investigasi
    - File Log
    - File Connection_List
    - File evil.php

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject3&4_Information_Sharing_Action

[Latihan Latihan Latihan]

Selamat Siang,

Kami selaku pemilik aset telah melakukan investigasi dengan hasil sebagai berikut :

1) ..

2) .., dst

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Expected Action

- Melakukan analisis log website
  - Malicious file : evil.php
  - Malicious link : sites/default/files/config_JennQV6qHdZDOOT1IRNyqEiKI6BiFPo6VRfggrOuKfacLW7xp2zTH_-NeVqWhpRGgmZxOdm9Fg
- Melakukan pemeriksaan pada daftar koneksi outbound
  - Malicious Connectivity : 203.0.78.156:5634
  - PID : 1162/apache2

Cont'd

- Memberikan hasil investigasi malicious file (base64decode online):
  1) Malicious File Name : evil.php
  2) MD5 : f508f33ffc0649a599a55e754e4cff5c
  3) File size : 3,0 kB (2987 bytes)
  4) Suspicious IP : 203.0.78.156
  5) Suspicious Port : 5634
  6) Time of Incident : 17/Jun/2019 08:48:15

Stage 2 Injeksi 5

[Phase 2-1]

Cek Email

To: **[Nama Instansi]**

From: gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject: Inject5_Information_Sharing (1 attachment)

[Latihan Latihan Latihan]

Selamat Siang,

Kami mendapat informasi dari ASEAN-Japan bahwa adanya serangan DDoS pada jaringan berskala besar di Singapura. Saat ini pihak Singapura telah melakukan restore jaringan dan melakukan investigasi terkait serangan ini. Dihimbau kepada konstituen Gov-CSIRT agar dapat memonitor jaringan pada masing-masing instansi.

Berdasarkan statistik Id-SIRTII/CC pada tahun 2018, Indonesia menjadi salah satu negara yang paling banyak menjadi sumber serangan. Terkait dengan hal tersebut maka kami menghimbau kepada instansi anda untuk melakukan pemantauan pada koneksi jaringan untuk memastikan bahwa tidak ada aktivitas anomali ke block IP Singapura. Berikut kami lampirkan list block IP Singapura.

Terima kasih.

Best Regards,

Gov-CSIRT BSSN

[Latihan Latihan Latihan]

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject5_Information_Sharing_Response

[Latihan Latihan Latihan]

Selamat Siang,

Terima kasih atas informasi yang diberikan, akan kami lakukan pelaporan hasil monitoring kami.

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Permasalahan

- Adanya kegagalan jaringan berskala besar akibat serangan DDoS di Singapura. Jaringan sudah dipulihkan tetapi penyebab dan penyerang belum diidentifikasi.
- Prosedur apa saja yang akan dilakukan oleh anda sebagai pemilik aset terhadap aduan tersebut?

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject5_Information_Sharing_Action

[Latihan Latihan Latihan]

Selamat Siang,

Kami selaku pemilik aset telah melakukan hal-hal sebagai berikut :

1) ..

2) .., dst

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Expected Action

- Mengimplementasikan SOP terkait penanganan jika terdapat aduan
- Melakukan koordinasi dengan tim CSIRT terkait informasi ini
- Mengumpulkan informasi terkait aduan tersebut

  a. Memeriksa apakah ada koneksi menuju block IP Singapura

Stage 2 Injeksi 6

[Phase 2-1]

Cek Email

To: **[Nama Instansi]**

From: gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject: Inject6_Situation_Awareness

[Latihan Latihan Latihan]

Selamat Siang,

Kami mendapatkan informasi dari Singapura bahwa terjadi serangan siber dari sekelompok hacker. Kelompok hacker bernama Anti-AJ Society mengumumkan melalui Twitter bahwa mereka tengah merancang serangan DDoS ke Singapura. Kelompok hacker ini juga mendeklarasikan bahwa mereka akan melakukan serangan siber skala besar pada lembaga pemerintah di negara ASEAN lainnya segera setelahnya. Peringatan hari ini pukul 13:00 akan menjadi awal dari insiden untuk lembaga pemerintah.

Mohon untuk memeriksa aliran trafik paket, serta akses kepada aset masing-masing. Harap konfirmasikan dan laporkan situasi Anda

Best Regards,

Gov-CSIRT BSSN

[Latihan Latihan Latihan]

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject6_Situation_Awareness_Response

[Latihan Latihan Latihan]

Selamat Siang,

Terima kasih atas informasi yang diberikan, akan kami lakukan pelaporan hasil monitoring kami.

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Permasalahan

- Adanya pengumuman tentang serangan siber dari kelompok hacker Anti-AJ Society melalui Twitter, dimana mereka akan melakukan serangan DDoS ke Singapura. Sebagai tambahan, kelompok hacker ini juga mendeklarasikan untuk melakukan serangan siber skala besar pada lembaga pemerintahan di negara ASEAN lainnya.
- Prosedur apa saja yang akan dilakukan oleh anda sebagai pemilik aset terhadap aduan tersebut?

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject6_Situation_Awareness_Action

[Latihan Latihan Latihan]

Selamat Siang,

Kami selaku pemilik aset telah melakukan hal-hal sebagai berikut :

1) ..

2) .., dst

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Expected Action

- Melakukan koordinasi dengan tim CSIRT terkait aduan ini
- Mengumpulkan informasi terkait aduan tersebut
  - Periksa aliran trafik, apakah ada aktivitas anomali atau tidak
  - Melakukan akses pada port, dan melihat penggunaan bandwith ketika mengakses
  - Memeriksa performa Memory dan CPU
- Mengumpulkan informasi terkait Grup Hacker “Anti-AJ Society”
  - Media sosial
  - Teknik Serangan
  - Source : IP address, malicious file (backdoor, webshell)

Stage 2 Injeksi 7

[Phase 2-2]

Cek Email

To: **[Nama Instansi]**

From: gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject: Inject7_Situation_Awareness

[Latihan Latihan Latihan]

Selamat Siang,

Nat-CSIRT melakukan *teleconference* dengan seluruh negara ASEAN dan juga NISC, sebagai bentuk pengumpulan informasi terkait dengan serangan dari Anti-AJ Society yang tengah terjadi.

Singapura membagikan informasi terkait situasi dari serangan dan balasan terhadap serangan DDoS yang tengah terjadi. Nat-CSIRT Indonesia melaporkan bahwa Indonesia terindikasi mengalami serangan serupa. Sehingga koneksi jaringan pada beberapa ISP dimungkinkan beresiko mengalami gangguan yang dapat mengakibatkan sebagian besar masyarakat Indonesia tidak dapat mengakses jaringan internet.

Best Regards,

Gov-CSIRT BSSN

[Latihan Latihan Latihan]

Permasalahan

- Indonesia merupakan salah satu negara AMS yang terindikasi terkena serangan DDoS, akibatnya adalah adanya kelumpuhan jaringan. Sehingga dilakukan teleconference antara Gov-CSIRT dan Konstituen untuk mengatasi masalah ini.
- Prosedur apa saja yang akan dilakukan oleh anda sebagai pemilik aset jika mengalami insiden tersebut?

Expected Action

- Konstituten mengkonfirmasi situasi setelah melakukan monitoring pada aset yang dimiliki. Sharing informasi yang diperlukan meliputi:

✓Waktu dan tanggal insiden

✓Tingkat keparahan (*Severity*)

✓Asal dan Target IP address

✓Penyebab

✓Situasi insiden

✓Dampak yang disebabkan dari serangan

✓Tindakan yang telah dilakukan

✓*Log incident*

Stage 2 Injeksi 8

[Phase 2-3]

Cek Email

To: **[Nama Instansi]**

From: gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject: Inject8_Identification_and_Measurement_Deployment

[Latihan Latihan Latihan]

Selamat Siang,

Kami mendapat informasi dari ASEAN-Japan terkait hasil investigasi dari lembaga keamanan dan ISP di Thailand bahwa serangan DDoS terjadi akibat DNS Reflection ke Singapura berasal dari alamat IP domain Thailand.

Lembaga keamanan di Thailand menginvestigasi bahwa terdapat PC yang memiliki alamat IP tersebut dan mengkonfirmasi bahwa di dalamnya terinstall Remote Access Trojan (RAT) bernama JBiFrost.

Best Regards,

Gov-CSIRT BSSN

[Latihan Latihan Latihan]

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject8_Identification_and_Measurement_Deployment_Response

[Latihan Latihan Latihan]

Selamat Siang,

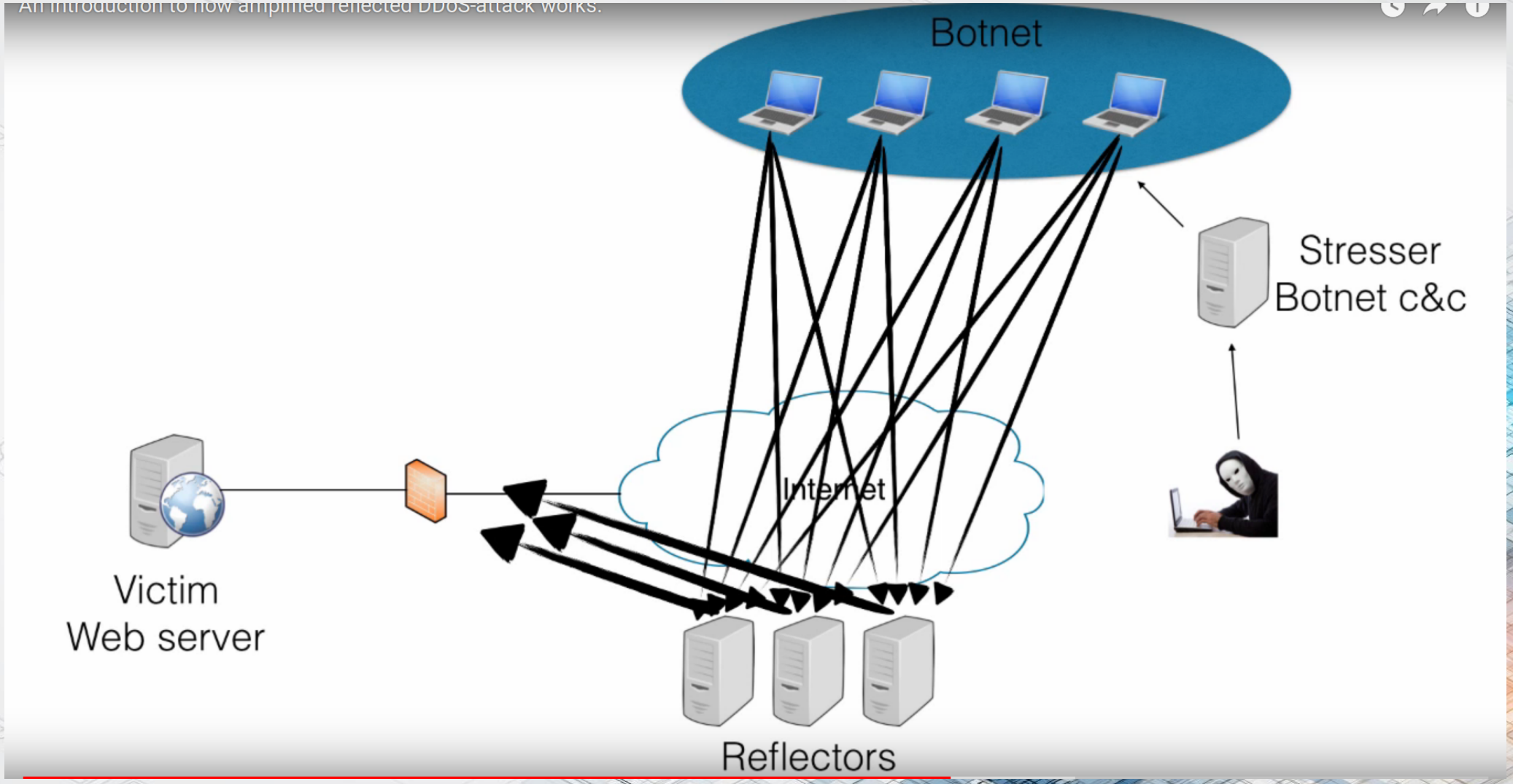
Terima kasih atas informasi yang diberikan.

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

DNS Reflection



Lesson Learned

- Mitigasi terhadap DNS Reflection Attack
  1. Melakukan pencegahan terhadap infeksi botnet dengan cara : menginstall anti-virus pada komputer client, mem-block koneksi inbound dan outbond yang malicious
  2. Dari jaringan : melakukan rate limit, melakukan verifikasi terhadap pengirim
  3. Dari server DNS : memfilter port 53, melakukan blokir berdasarkan IoC atau Bad Reputation IP.

Stage 2 Injeksi 9

[Phase 2-4]

Cek Email

To: **[Nama Instansi]**

From: gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject: Inject9_Situasional_Awareness_Infomation

[Latihan Latihan Latihan]

Selamat Siang,

Kami mendapat informasi dari ASEAN-Japan bahwa adanya hubungan antara FGP-01 yang mengoperasikan situs belanja palsu dengan kelompok hacker Anti-AJ Society.

Malaysia melakukan pencarian informasi IoC pada RAT yang dilaporkan dari Thailand dan mengkonfirmasi adanya sumber komunikasi yang mencurigakan (203.0.xxx.xxx) yang telah dipantau secara terus menerus. Oleh karena itu, disinyalir bahwa kelompok kriminal penipuan FGP-01 pada Stage 1 merupakan kelompok yang sama dengan kelompok hacker Anti-AJ Society.

Best Regards,

Gov-CSIRT BSSN

[Latihan Latihan Latihan]

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject9_Situasional_Awareness_Infomation

[Latihan Latihan Latihan]

Selamat Siang,

Terima kasih atas update informasi yang diberikan.

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Stage 2 Injeksi 10

[Phase 2-5]

Cek Email

To: **[Nama Instansi]**

From: gulih.pemerintah@bssn.go.id

CC : cyber.exercise@bssn.go.id

Subject: Inject10_Information_Sharing

[Latihan Latihan Latihan]

Selamat Siang,

Kami mendapat informasi dari ASEAN-Japan bahwa anggota dari kelompok kriminal (Anti-AJ Society), pelaku dari penyerangan siber berskala besar di Singapura telah ditangkatp. Akun twitter dari pelaku pun sudah di tangguhkan. Insiden sudah diatasi dan situasi keamanan siber kembali terkendali.

Best Regards,

Gov-CSIRT BSSN

[Latihan Latihan Latihan]

Respon Email

To: gulih.pemerintah@bssn.go.id

From: **[Nama Instansi]**

CC : cyber.exercise@bssn.go.id

Subject: Inject10_Information_Sharing

[Latihan Latihan Latihan]

Selamat Siang,

Terima kasih atas informasi yang diberikan.

Best Regards,

[Nama Instansi]

[Latihan Latihan Latihan]

Selesai