LAPORAN TAHUNAN KOMINFO-CSIRT 2023

csirt.komdigi.go.id

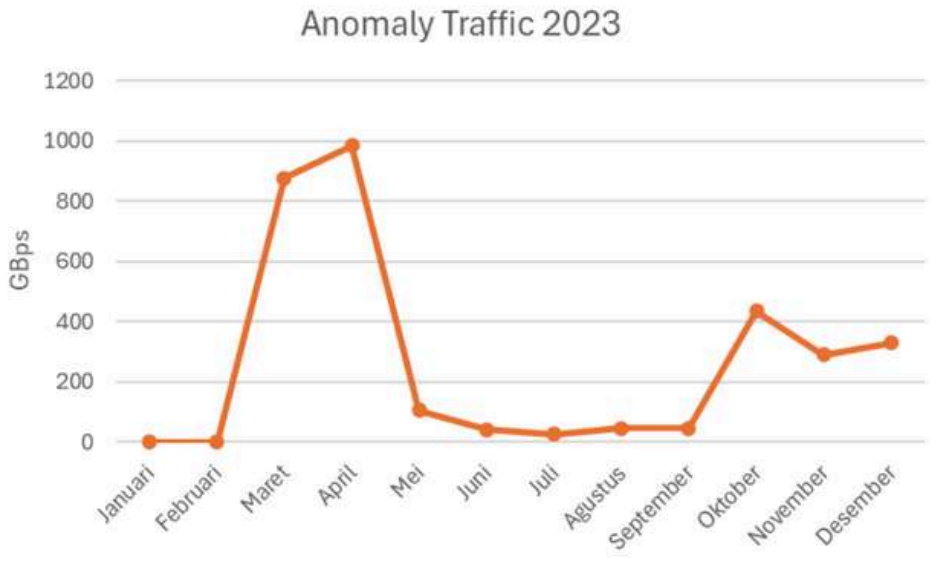
Ringkasan

Laporan Tahunan KOMINFO-CSIRT untuk tahun 2023 menyoroti berbagai peristiwa dan tren keamanan siber yang terjadi di Kementerian Komunikasi dan Informatika. Data menunjukkan bahwa **total trafik anomali** selama tahun **2023** mencapai **3.181 GBps**, dengan puncak **tertinggi** terjadi pada bulan **April (983,8 GB)** dan puncak **terendah** pada bulan **Juni (41,5 GB)**. Sebanyak **18 insiden siber** dilaporkan sepanjang tahun tersebut, dengan jumlah **tertinggi** terjadi pada bulan **Mei (5 insiden)**. Jenis insiden siber yang paling dominan adalah **injeksi berkas berbahaya**, tercatat sebanyak **14 kali**. Selain itu, permintaan *Vulnerability Assessment/Penetration Testing* (VA/PT) tertinggi tercatat pada bulan Januari dan Desember, dengan total 179 permintaan. Data ini memberikan gambaran tentang kompleksitas dan eskalasi ancaman keamanan siber yang dihadapi oleh Kementerian Komunikasi dan Informatika selama tahun 2023, dan menjadi landasan untuk strategi keamanan yang lebih efektif di masa depan.

3.181 GBps

Total Trafik Anomali di lingkungan Kominfo

Total trafik anomali di Kementerian Komunikasi dan Informatika selama tahun 2023 adalah **3.181 GBps anomali**. Anomali trafik **tertinggi** terjadi pada bulan **April** dengan jumlah **983,8 GB anomali trafik**, sedangkan anomali **terendah** terjadi pada bulan **Juni** dengan jumlah **41,5 GB anomali**. Aktivitas anomali trafik ini dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan terhadap suatu organisasi. Berikut merupakan grafik trafik anomali periode Januari - Desember 2023:



Top 5 Trafik Anomali

Key	Category	Blocked
	DDoS Reputation	**61.6 GB**
	Mobile	**1.3 GB**
	Command and Control	**865.7 MB**
	Location Based Threats	**703.5 MB**
	Malware	**27.3 MB**

TLP CLEAR

Top 5 Negara Sumber dan Tujuan

Top Inbound Countries

Nation	Graph	Passed	Blocked	Percent
Indonesia		12.2 Mbps 10.7 kpps	179.7 kbps 105.0 pps	65 %
United States of America		4.6 Mbps 1.8 kpps	165.7 kbps 98.4 pps	25 %
Singapore		1.0 Mbps 339.2 pps	109.1 kbps 26.1 pps	6 %
Hong Kong		530.5 kbps 65.7 pps	10.1 kbps 4.0 pps	3 %
United Kingdom		200.6 kbps 115.4 pps	8.3 kbps 18.0 pps	1 %

Top Inbound Destinations

Destination	Graph	Total Traffic	Traffic Rate
202.89.117.16		21.4 TB 22.7 G packets	5.4 Mbps 717.7 pps
202.89.117.165		7.9 TB 15.4 G packets	2.0 Mbps 485.8 pps
202.89.117.7		6.8 TB 6.5 G packets	1.7 Mbps 205.6 pps
202.89.117.162		6.5 TB 78.8 G packets	1.6 Mbps 2.5 kpps
202.89.116.55		6.1 TB 142.9 G packets	1.5 Mbps 4.5 kpps

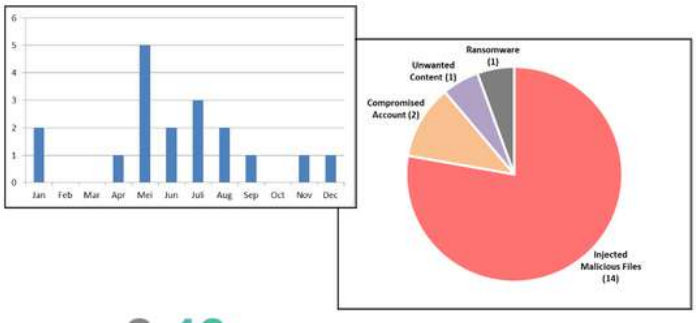
Rekapitulasi Insiden Siber

Incident response merupakan penindaklanjutan insiden siber dengan melibatkan Kominfo-CSIRT selaku CSIRT organisasi dan penanggung jawab sistem yang terdampak itu sendiri. Incident response dilakukan secepat mungkin dalam kurun waktu paling lambat 24 jam untuk mencegah insiden mengakibatkan dampak buruk lebih luas seperti masuknya kejadian insiden pada kanal berita yang dapat merusak citra instansi, pencurian data pribadi pengguna sistem, pengambilalihan kontrol penuh terhadap server, dan lain-lain.

Melalui laporan insiden siber yang masuk ke Kominfo-CSIRT, dilakukan verifikasi untuk mengetahui keabsahannya. Jika verifikasi sudah dilakukan dan insiden siber benar terjadi, maka dilakukan pengidentifikasian untuk menentukan tindak lanjut yang tepat seperti perlu atau tidaknya aplikasi web ditutup dari jaringan publik, penggunaan backup atau VPS (*virtual private server*) baru untuk menunjang pemulihan.

Sepanjang tahun **2023**, telah terjadi **18 kali insiden siber** di aplikasi web. Jumlah **tertinggi** insiden siber ada pada bulan **Mei** yakni sebanyak **5 kali** dan jumlah jenis insiden siber **tertinggi** berupa **injeksi berkas berbahaya (*injected malicious files*)** yakni sebanyak **14 kali**.

Melalui bantuan forensik dan investigasi penyebab terjadinya insiden siber, rekomendasi dan pendampingan perbaikan serta pemanfaatan XDR sebagai *anti-malware* dari Kominfo-CSIRT, sebanyak **18 kali insiden siber**, **16** insiden siber di antaranya **berhasil dipulihkan** sehingga dikembalikan ke jaringan publik, sementara **2 sisanya ditutup** karena memang **sudah tidak digunakan** lagi.

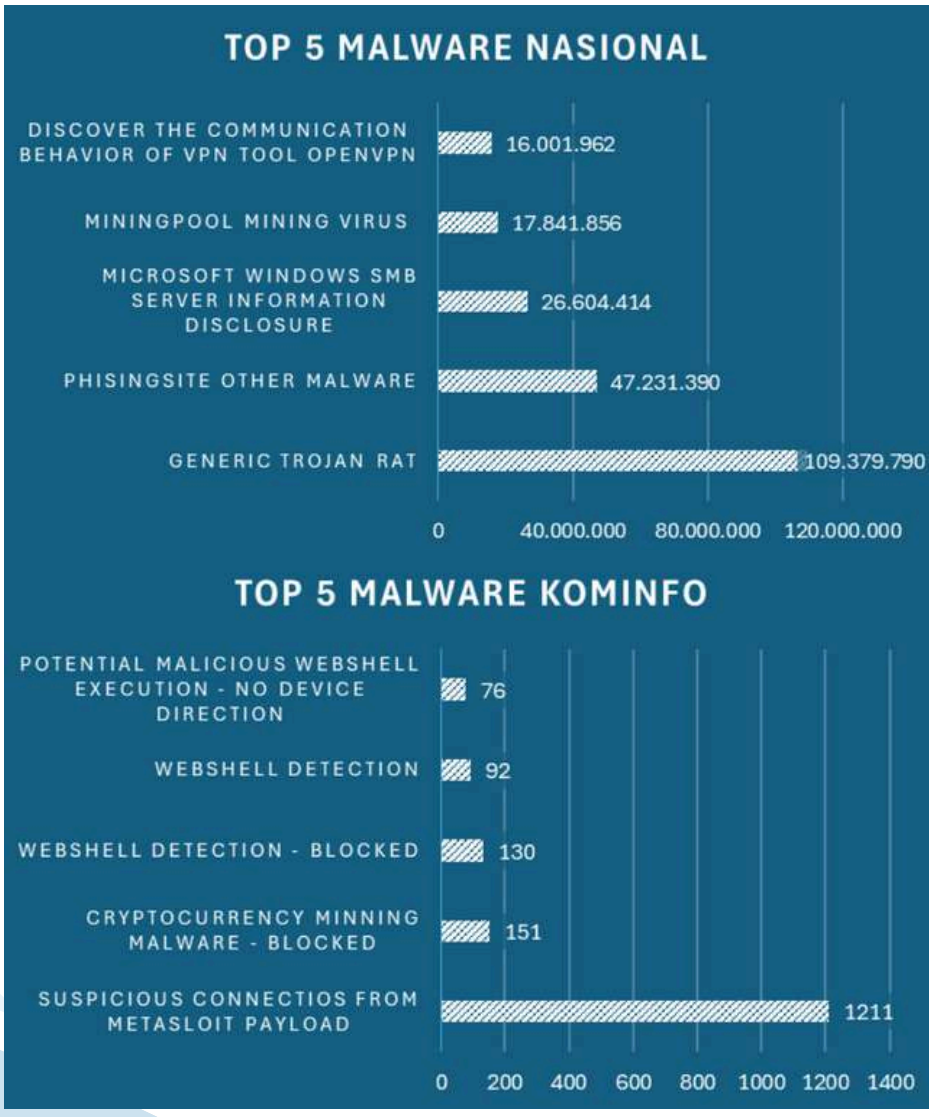


2 TAKEN DOWN

16 RECOVERED

Top 5 Common Malware Activity

Malware (*Malicious Software*) dapat menjadi ancaman serius bagi organisasi dimana *malware* dapat merusak sistem, melakukan pencurian data, mengancam reputasi organisasi bahkan sampai mengakibatkan kerugian materiil . Kominfo-CSIRT telah mampu mencegah dan mengatasi beberapa *malware* yang saat ini sering menjadi penyebab terjadinya insiden dengan menggunakan tools *XDR* (*Extended Detections and Responses*). Berikut data 5 teratas *malware* yang sering dideteksi secara nasional dan *malware* yang berhasil diatasi oleh tim Kominfo-CSIRT.

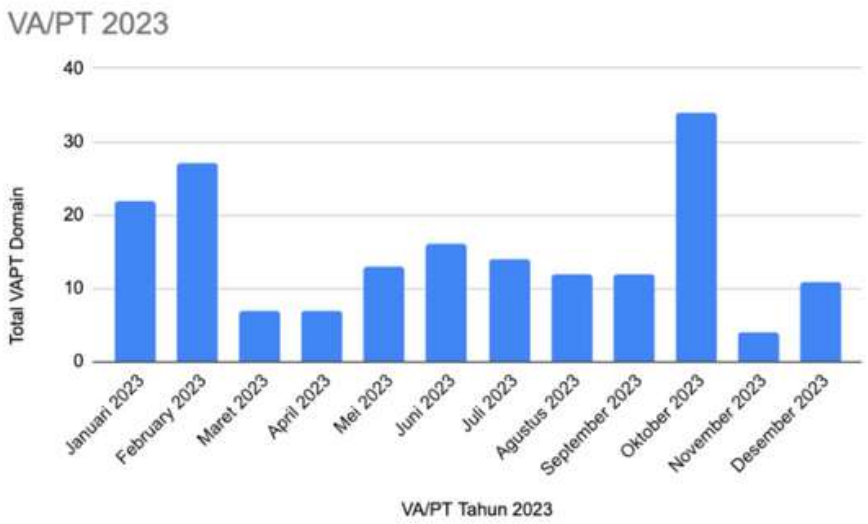


VA/PT pada KOMINFO-CSIRT

VA (*Vulnerability Assessment*)/ PT (*Penetration Testing*) merupakan kegiatan pengujian ketahanan sistem dalam upaya memanajemen potensi risiko siber. Melalui serangkaian pengujian terbarukan dan sistematik baik secara manual maupun menggunakan tools, temuan celah keamanan dikategorikan dan dijadikan dasar prioritas perbaikan. Tujuan utama VA/PT adalah memberikan pemahaman yang mendalam tentang keadaan keamanan siber terbaru dan membantu organisasi untuk fokus menangani kerentanan yang paling kritis.

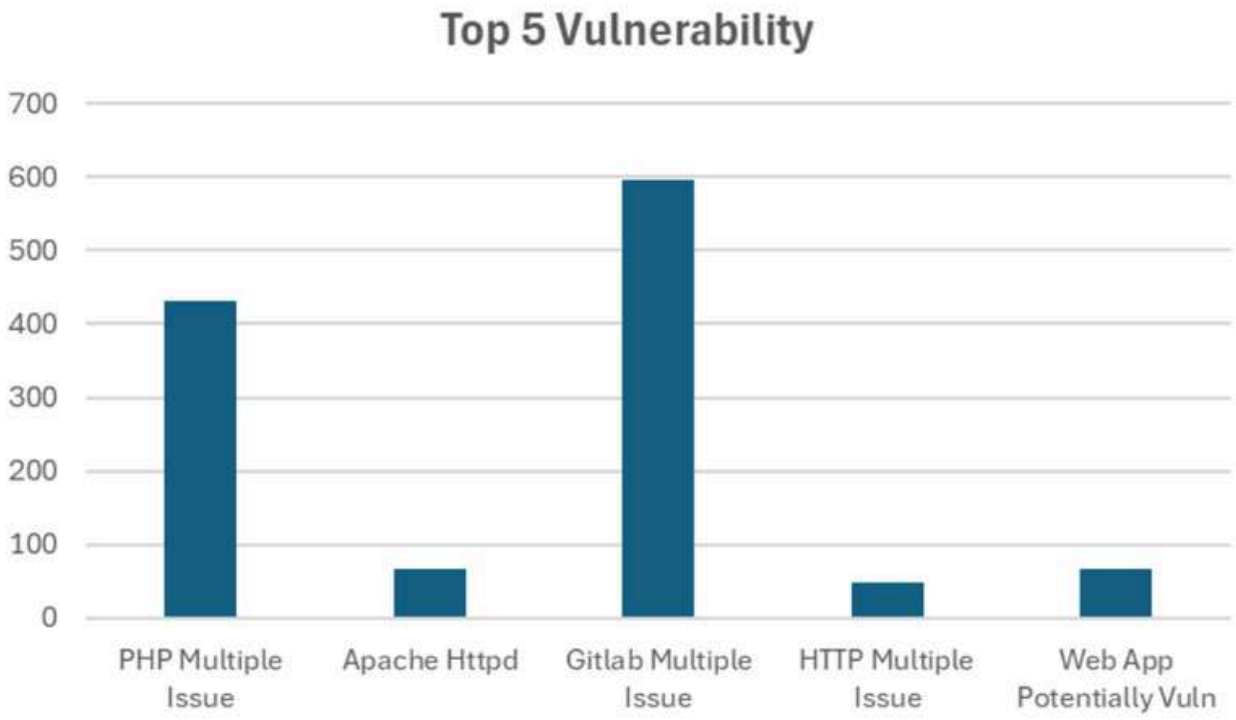
Melalui Helpdesk/aplikasi permintaan terhadap VA/PT dapat dilakukan oleh penanggung jawab aplikasi baik yang belum rilis maupun yang sudah rilis. Sebelum aplikasi diizinkan mendapatkan subdomain dan dapat diakses di jaringan publik/internet, aplikasi harus lolos dari VA/PT dengan kondisi tidak ada kerentanan dengan kategori sedang atau lebih tinggi.

Dari data pada sistem informasi, didapatkan permintaan **VA/PT tertinggi** tahun 2023 terjadi di bulan **Januari** dan **Desember** 2023 memiliki jumlah **179 *Request*** untuk dilakukan VA/PT.



TLP CLEAR

Top 5 Kerentanan



Lesson Learned Top 5 Insiden Siber

1

Pentingnya Pemantauan dan Deteksi Dini:

- Kemampuan deteksi dini dan respon cepat terhadap ancaman siber menjadi kunci utama dalam meminimalisir dampak kerusakan.
- Perlu dilakukan investasi pada teknologi pemantauan dan analitik keamanan siber yang mumpuni.
- Tim keamanan siber harus selalu siaga dan proaktif dalam mengidentifikasi potensi ancaman.

2

Memperkuat Keamanan Infrastruktur TI:

- Infrastruktur TI yang rentan terhadap serangan siber menjadi celah bagi para pelaku cybercrime.
- Perlu dilakukan penguatan keamanan infrastruktur TI dengan menerapkan langkah-langkah seperti:
  - Patching kerentanan sistem operasi dan aplikasi secara berkala.
  - Menerapkan kontrol akses yang ketat dan autentikasi multi-faktor.
  - Melakukan segmentasi jaringan untuk membatasi penyebaran malware.

TLP CLEAR

Lesson Learned Top 5 Insiden Siber

3

Memperkuat Kerjasama dan Kolaborasi:

- Penanganan insiden siber membutuhkan kerjasama dan kolaborasi antar berbagai pihak.
- Perlu dibangun komunikasi dan koordinasi yang efektif antar unit di Kominfo, serta dengan lembaga terkait seperti BSSN, Polri, dan komunitas keamanan siber.
- Berbagi informasi dan pengetahuan tentang ancaman siber menjadi kunci untuk meningkatkan pertahanan kolektif.

4

Pentingnya Pengelolaan Risiko Siber:

- Pengelolaan risiko siber yang efektif membantu organisasi dalam mengidentifikasi, menilai, dan menanggapi potensi ancaman siber.
- Perlu dilakukan penerapan kerangka kerja manajemen risiko siber yang komprehensif di Kominfo.
- Penilaian risiko siber harus dilakukan secara berkala untuk memastikan keefektifan langkah-langkah mitigasi yang diterapkan.

5

Meningkatkan Kesadaran Keamanan Siber:

- Kurangnya kesadaran dan pengetahuan tentang keamanan siber menjadi faktor utama dalam banyak insiden siber.
- Perlu dilakukan edukasi dan pelatihan secara berkelanjutan kepada seluruh pegawai Kominfo tentang praktik keamanan siber yang baik.
- Penting untuk membangun budaya keamanan siber yang kuat di lingkungan Kominfo.

TLP CLEAR

KTT ASEAN 42

Pada Konferensi Tingkat Tinggi (KTT) ASEAN ke-42 yang diadakan di Labuan Bajo tanggal 10-11 Mei 2023, PDSI juga turut aktif berpartisipasi dalam upaya pengamanan siber. PDSI bertanggung jawab atas keamanan siber di lingkup Media Center, yang meliputi persiapan teknis dan pemastian keamanan koneksi jaringan di area tersebut dari serangan siber, malware, dan ancaman lainnya. Sebagai bagian dari langkah-langkah pengamanan tersebut, dilakukan pemantauan lalu lintas jaringan di Media Center, pemasangan perlindungan endpoint berupa XDR pada 61 PC di Media Center, serta pemasangan WAF pada empat website terkait acara tersebut, yaitu asean2023.id, media-registration.asean2023.id, dan cloud.asean2023.id.

Upaya tersebut telah terbukti berhasil dalam mewujudkan keamanan siber di Media Center pelaksanaan KTT ASEAN ke-42. Selama acara tersebut berlangsung, dari 61 PC yang terpasang, sebanyak 31 PC terdeteksi mengalami infeksi *malware*, namun tindakan pencegahan yang diimplementasikan oleh *agent* XDR telah berhasil memblokir serangan tersebut. Selain itu, segala percobaan serangan yang masuk berhasil dicegah oleh WAF yang dikelola oleh PDSI Kominfo. Setiap alamat IP penyerang juga telah diidentifikasi sebagai bad-IP dan dimasukkan ke dalam daftar blokir IP untuk mencegah serangan potensial di masa mendatang.

KTT ASEAN 43

Sama seperti pada kegiatan yang disebutkan sebelumnya, selama pelaksanaan Konferensi Tingkat Tinggi (KTT) ASEAN ke-43 di Jakarta Convention Center (JCC) pada 5 – 7 September 2023, PDSI turut berperan dalam upaya pengamanan siber di Media Center KTT ASEAN ke-43. PDSI menyediakan infrastruktur dan keamanan siber berupa pemasangan perlindungan endpoint XDR pada 204 PC yang ada di Media Center. Selama acara tersebut berlangsung, sebagian besar PC terdeteksi mengalami infeksi malware, namun tindakan pencegahan yang diimplementasikan oleh agent XDR telah berhasil memblokir serangan tersebut.

Upaya lain yang dilakukan oleh PDSI adalah pemasangan WAF pada empat website terkait acara tersebut, yaitu asean2023.id, media-registration.asean2023.id, dan cloud.asean2023.id. Seluruh percobaan serangan yang masuk telah berhasil diblokir oleh WAF PDSI Kominfo dan setiap IP attacker dimasukkan ke dalam kategori bad-IP serta didaftarkan ke dalam blocked IP demi antisipasi serangan berikutnya.

KTT AIS Forum 2023

Dilihat dari kesuksesan PDSI dalam mengawal kegiatan internasional sebelumnya, pada penyelenggaraan KTT AIS Forum tahun 2023 yang dilaksanakan pada tanggal 8 - 12 Oktober 2023 di BNDCC Nusa Dua Bali, PDSI kembali diberikan tanggung jawab untuk menjaga keamanan siber di lingkup Media Center. PDSI menyediakan infrastruktur dan keamanan siber berupa pemasangan WAF untuk tiga aset website yang digunakan pada KTT AIS Forum tahun 2023, yaitu aisforum2023.id, registration.aisforum2023.id dan cloud.aisforum2023.id.

Selain itu, pemasangan XDR untuk server dan endpoint juga dilakukan. Tim Keamanan PDSI melakukan instalasi XDR pada 30 PC yang akan digunakan wartawan sebagai pertukaran media informasi. Pemantauan dan pendeteksian juga dilakukan terhadap serangan yang berpotensi membahayakan aset KTT AIS Forum 2023. Adapun seluruh percobaan serangan yang masuk telah berhasil diblokir oleh WAF yang dipasang oleh PDSI Kominfo.

Perayaan Natal Nasional 2023

Dalam rangka mengantisipasi terjadinya serangan malware yang menyebabkan kerusakan pada sistem komputer, PDSI memberikan dukungan keamanan siber dari PDSI untuk Perayaan Natal Nasional 2023 yang diselenggarakan pada 26 - 28 Desember 2023 di Surabaya. Dukungan yang diberikan yakni instalasi XDR di level endpoint pada 1 laptop server registrasi dan 5 laptop client yang digunakan untuk scan barcode untuk memvalidasi undangan yang hadir.

Panitia menggunakan dua aplikasi web, yaitu website utama dan website registrasi. Kedua website tersebut ditempatkan pada cloud guna menjaga keamanan. Tim Keamanan Informasi PDSI telah mengarahkan keduanya ke WAF agar WAF dapat melakukan pemantauan, penyaringan, dan pemblokiran data yang berasal dari pengguna.

Secara umum, pada pelaksanaan event Natal Nasional 2023 tidak terdapat serangan yang cukup berarti sehingga proses bisnis aplikasi tetap terjaga. Berdasarkan hasil pemantauan, serangan yang terdeteksi antara lain Illegal Resource Access dan Cross-site Scripting yang telah diblok oleh rule WAF. Selain itu, hasil monitoring XDR selama pelaksanaan event Natal Nasional 2023 menunjukkan adanya 2 jenis malware pada 2 endpoint, yaitu SPYWARE dan TROJAN. Kedua malware tersebut telah dikarantina dan dihapus oleh rule XDR.

Kesimpulan dan Penutup

Laporan tahunan ini merupakan laporan dari hasil kegiatan semua program yang dilaksanakan di Kementerian Komunikasi dan Informatika sepanjang tahun 2023. Sepanjang tahun 2023, KOMINFO-CSIRT telah berupaya meningkatkan kesiapsiagaan, respons cepat, dan kapasitas dalam menghadapi berbagai tantangan keamanan siber. Ke depan, KOMINFO-CSIRT akan terus berkomitmen untuk memperkuat strategi keamanan siber melalui pengembangan kapabilitas, peningkatan kesadaran keamanan bagi seluruh pemangku kepentingan, serta implementasi kebijakan yang lebih adaptif terhadap dinamika ancaman siber.