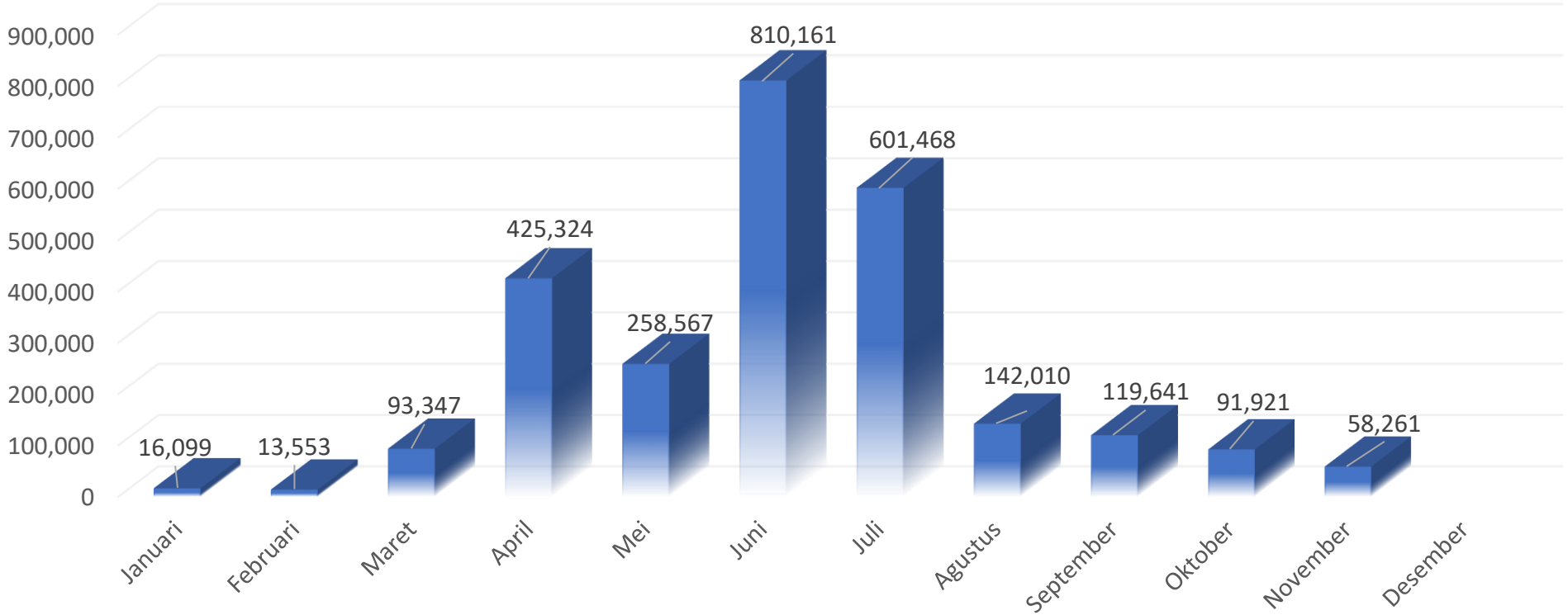
TREND ANCAMAN SERANGAN SIBER

terhadap Infrastruktur
Jaringan K/L Pemerintah

Oleh:

DIREKTUR ANALISA DAN FORENSIK
DEPUTI-VI BIDANG INTELIJEN SIBER BIN

TREND SERANGAN SIBER MENUJU K/L 2020



2.630.352 Cyber Threats

MALWARE
3,5%

BOT SCANNER
1,6%

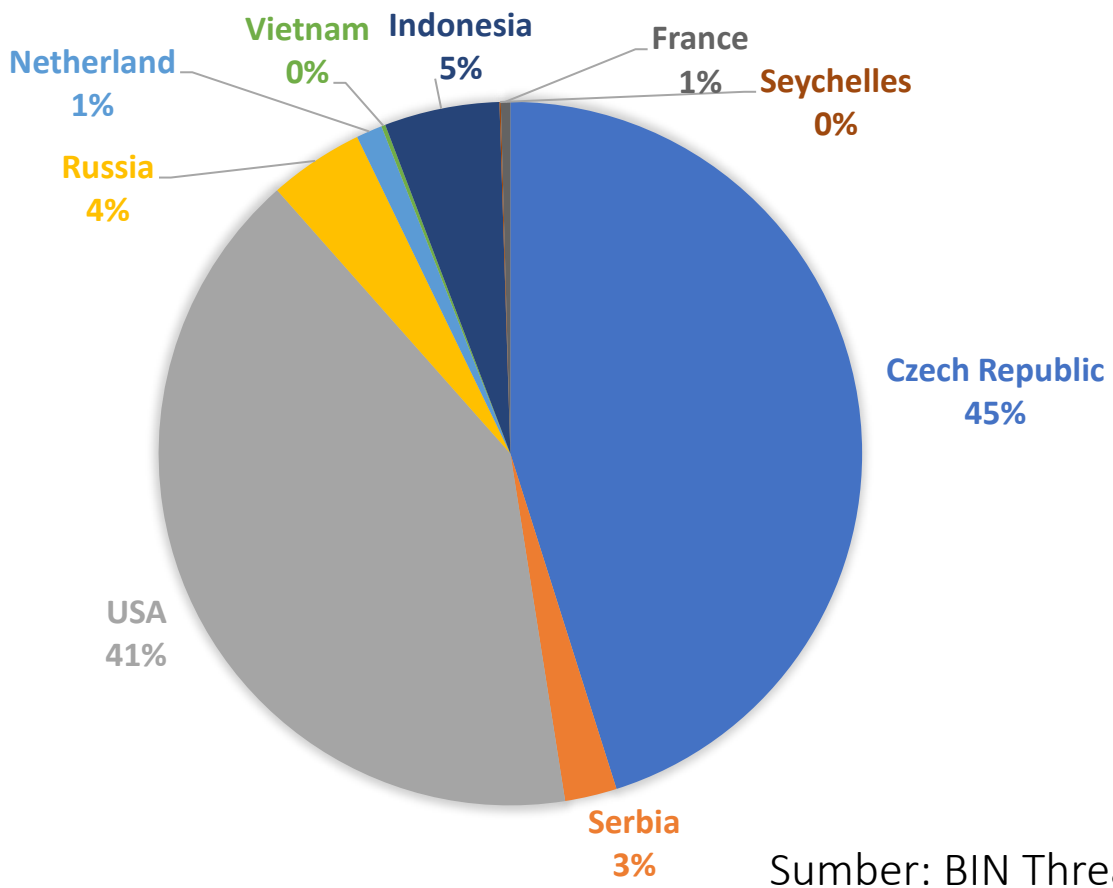
EXPLOIT
4,9%

BRUTE FORCE
62,64%

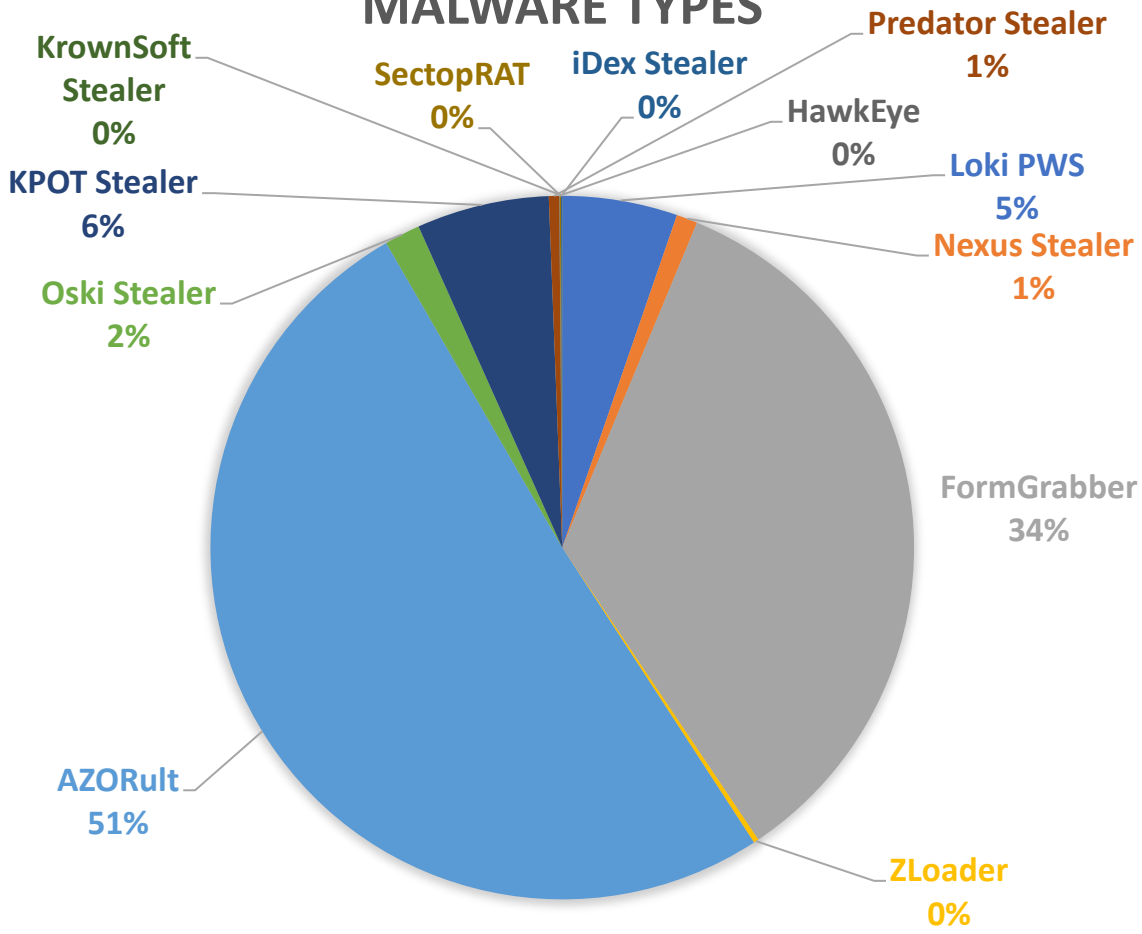
DDOS
27,17%

INFEKSI MALWARE STEALER DI INDONESIA

THREAT ACTOR'S ORIGIN

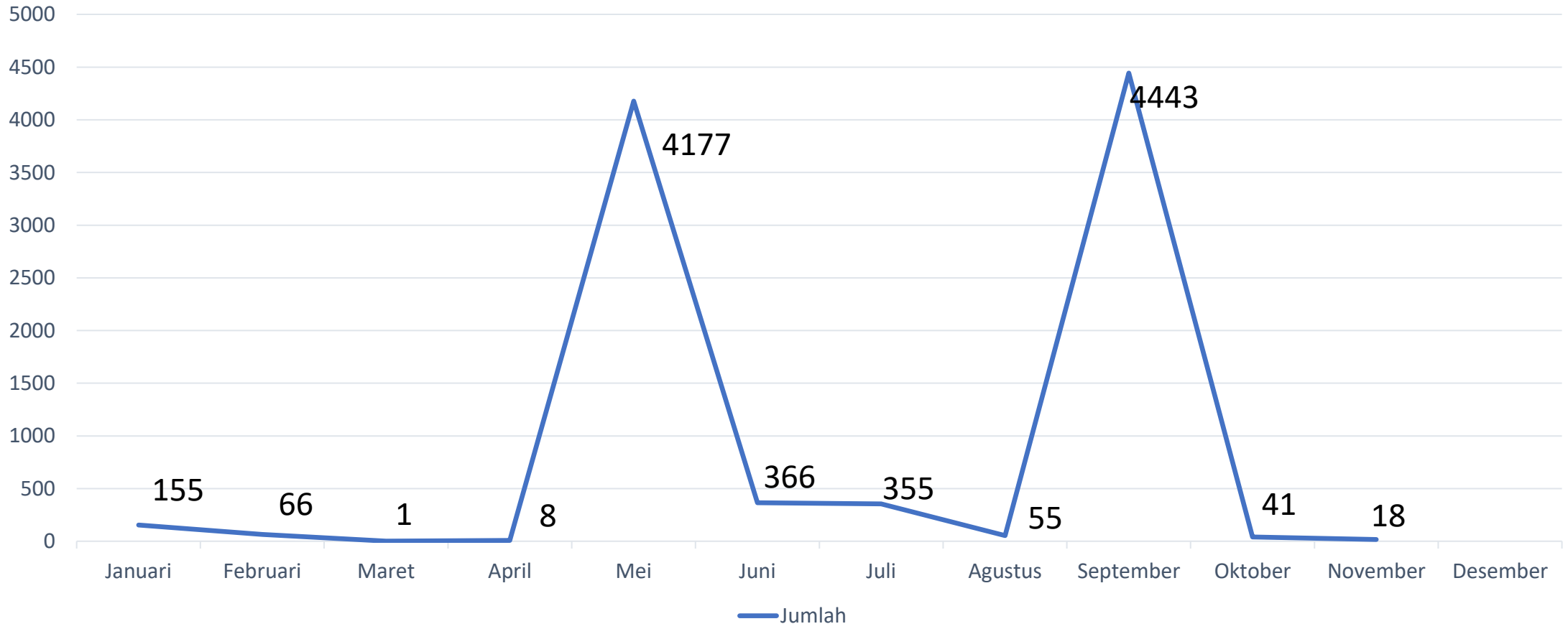


MALWARE TYPES



Sumber: BIN Threat Intelligence dan Dark Web

JUMLAH DATA KREDENSIAL YANG MENGALAMI KEBOCORAN PADA TAHUN 2020



Sumber: BIN Threat Intelligence dan Dark Web

MALWARE AZORULT

AZORult merupakan salah satu jenis *malware* Trojan yang memiliki kemampuan untuk mendapatkan *log keystrokes*. AZORult pada umumnya menyebar melalui email spam berbahaya dan menyamar menyerupai tampilan halaman *login* aplikasi yang sah. Apabila pengguna terkelabui, peretas berpotensi untuk membaca *username* dan *password* pengguna.

Detected	Domain	Login	Source	Threat actor
2020-09-24 18:42:43	[redacted]go.id	[redacted]	AZORult	-/-

Detected 2020-09-24 18:42:43	Login [redacted]	Victim's IP [redacted]	C&C server http://officestore.co.id/linkzer/PL341/panel/admin.php	C&C IP [redacted]
Compromised -/-	Password ?	Country [redacted]	Drop e-mail -/-	Country [redacted]
		City Jakarta		City [redacted]
		Provider [redacted]		Provider [redacted]

INFEKSI MALWARE "AZORULT" YANG BERHASIL MENCURI DATA LOGIN DAN PASSWORD PADA SEKITAR **3.592 AKUN MILIK 115 KEMENTERIAN DAN LEMBAGA**, PEMERINTAH DAERAH PROVINSI SERTA PEMERINTAH DAERAH TINGKAT II MALWARE TERSEBUT MERUPAKAN JENIS TROJAN YANG DAPAT DAPAT MELAKUKAN PENCURIAN KREDENSIAL DARI KORBANNYA DENGAN MENGINFEKSI WEB BROWSER SEPERTI GOOGLE CHROME, FIREFOX MAUPUN OPERA.

KEBOCORAN DATA AKUN TERSEBUT BERDAMPAK PADA SEJUMLAH SUBDOMAIN YANG MEMILIKI PERAN VITAL DALAM SEJUMLAH ASPEK KEGIATAN NEGARA, SIANTARA AKUN YANG BOCOR TERSEBUT JUGA TERDAPAT AKUN PENGELOLA SISTEM PENTING SEPERTI SISTEM PEMBENDAHARAAN NEGARA, SISTEM MANAJEMEN PERSONEL, SISTEM PENGELOLAAN LELANG BARANG DAN JASA SERTA SEJUMLAH SISTEM INFORMASI LAYANAN PUBLIK DAN INTERNAL YANG DIKELOLA OLEH KEMENTERIAN DAN LEMBAGA.

AKTIVITAS APT DI INDONESIA

- DarkHotel
- RedDelta (China)
- OceanLotus
- Naikon APT (China State Actor)
- Dark Caracal (Kazakhstan/Lebanon)

DarkHotel

- Pada Maret 2020, APT ini terdeteksi menargetkan menyerang beberapa agensi pemerintahan China, termasuk agensi pemerintahan yang berlokasi di Afghanistan, Armenia, Ethiopia, India, **Indonesia**, Iran, Israel, Italy, Kyrgyzstan, Malaysia, North Korea, Pakistan, Saudi Arabia, Tajikistan, Thailand, Turkey, UAE, United Kingdom dan Vietnam
- Serangan siber yang dilakukan oleh APT DarkHotel memanfaatkan aplikasi VPN SangFor.

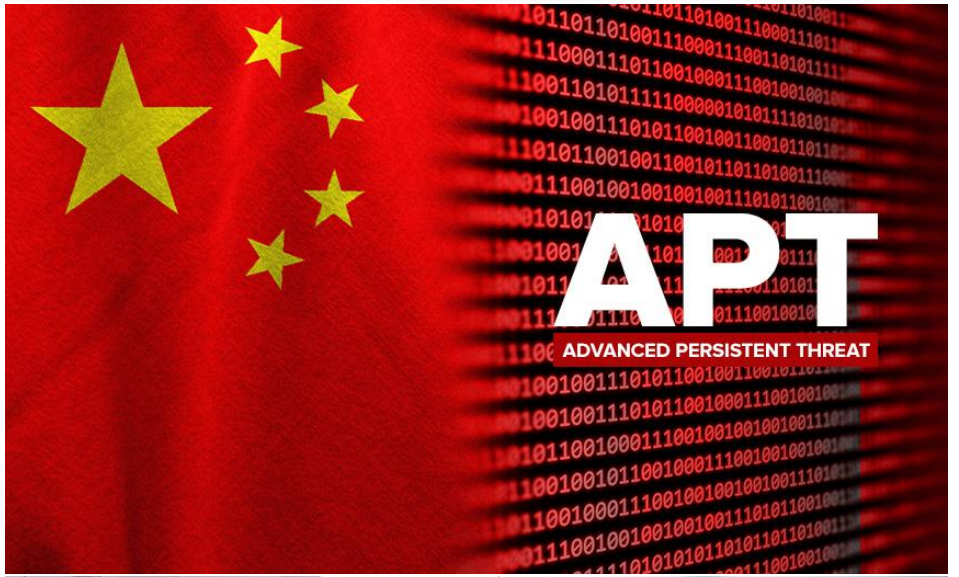
AKTIVITAS APT DI INDONESIA

- DarkHotel
- RedDelta (China)
- OceanLotus
- Naikon APT (China State Actor)
- Dark Caracal (Kazakhstan/Lebanon)

RedDelta (China)

- Pada Juli 2020, kelompok APT China RedDelta terdeteksi melakukan serangan siber dengan menggunakan teknik phising memanfaatkan beberapa jenis malware seperti PlugX, Poison Ivy, dan Coblat Strike

- Pada Mei s.d. Juli 2020, diduga kuat kelompok APT ini menargetkan salah satu Kementerian di Indonesia



AKTIVITAS APT DI INDONESIA

- DarkHotel
- RedDelta (China)
- OceanLotus
- Naikon APT (China State Actor)
- Dark Caracal (Kazakhstan/Lebanon)

OceanLotus

- Pada April 2020, kelompok APT OceanLotus terdeteksi melakukan serangan siber dengan menargetkan pengguna Android di beberapa negara. Sejak tahun 2016, kurang lebih sebanyak 300 kasus serangan siber terdeteksi terjadi di India, Vietnam, Bangladesh, **Indonesia**, Nepal, Myanmar and Malaysia.
- Serangan siber yang dilakukan oleh kelompok APT OceanLotus ini bertujuan untuk mengumpulkan data pribadi atau penting milik korban. Informasi yang dapat diperoleh antara lain lokasi (geolocation), Riwayat panggilan (call logs), daftar kontak, dan SMS.

AKTIVITAS APT DI INDONESIA

- DarkHotel
- RedDelta (China)
- OceanLotus
- Naikon APT (China State Actor)
- Dark Caracal (Kazakhstan/Lebanon)

Naikon APT (China State Actor)

- Pada Mei 2020, kelompok APT Naikon terdeteksi telah melakukan serangan siber menargetkan pemerintahan beberapa negara, antara lain Australia, **Indonesia**, Filipina, Thailand, Myanmar, dan Brunei Darusalam.
- Dalam serangan yang dilakukannya, kelompok APT Naikon menggunakan backdoor dengan nama Aria-Body.

AKTIVITAS APT DI INDONESIA

- DarkHotel
- RedDelta (China)
- OceanLotus
- Naikon APT (China State Actor)
- Dark Caracal (Kazakhstan/Lebanon)

Dark Caracal (Kazakhstan/Lebanon)

- Serangan siber yang dilakukan oleh kelompok APT Dark Caracal terdeteksi menargetkan perusahaan dan institusi pemerintahan di beberapa negara, antara lain Cili, Cyprus, Jerman, **Indonesia**, Italia, Singapura, Swis, Turki, dan Amerika Serikat
- Beberapa perusahaan yang menjadi target serangan siber oleh kelompk APT Dark Caracal meliputi perusahaan yang bergerak dalam bidang keuangan, energi, industri makanan, kesehatan, dan IT.

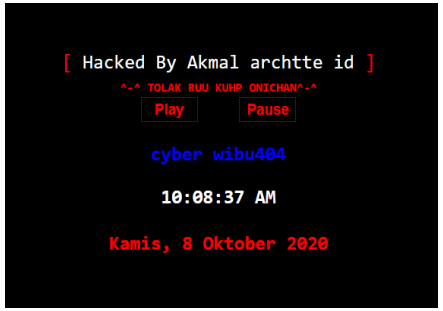
PENGARUH DINAMIKA SOSIAL TERHADAP ANCAMAN SIBER

DINAMIKA SOSIAL → MEMANFAATKAN SERANGAN SIBER SEBAGAI SARANA UNTUK MENGUNGKAPKAN PROTES/ASPIRASI → DARI BEBERAPA JENIS SERANGAN SIBER, SALAH SATU CONTOHNYA YAITU DEFACEMENT → CONTOH: AKSI PROTES UU OMNIBUS LAW MELALUI DEFACEMENT TERHADAP WEBSITE K/L PEMERINTAH

PENGARUH DINAMIKA SOSIAL TERHADAP ANCAMAN SIBER

DINAMIKA SOSIAL → MEMANFAATKAN SERANGAN SIBER SEBAGAI SARANA UNTUK MENGUNGKAPKAN PROTES/ASPIRASI → DARI BEBERAPA JENIS SERANGAN SIBER, SALAH SATU CONTOHNYA YAITU DEFACEMENT → CONTOH: AKSI PROTES UU OMNIBUS LAW MELALUI DEFACEMENT TERHADAP WEBSITE K/L PEMERINTAH

SELAMA OKTOBER 2020, SEDIKITNYA TERDAPAT 27 DOMAIN WEBSITE MILIK PEMERINTAHAN YANG MENJADI TARGET SERANGAN SIBER BERUPA DEFACEMENT, DENGAN MENAMPILKAN GAMBAR DAN PESAN TERKAIT PROTES TERKAIT UU OMNIBUS LAW.



APA YANG PERLU DILAKUKAN?

Meningkatkan Kewaspadaan terkait Keamanan Siber

Melakukan perencanaan pembangunan dan peningkatan infrastruktur keamanan informasi sesuai dengan tingkat ancaman yang memenuhi standar keamanan.

Melakukan pemeriksaan dan pemantauan infrastruktur jaringan secara berkala sebagai upaya mendeteksi adanya potensi serangan siber yang telah berhasil masuk ke dalam jaringan

Melakukan respon insiden serangan siber secara komprehensif, serta berkolaborasi dengan lembaga keamanan siber nasional.

DEMIKIAN
TERIMA KASIH