**Kasus Cybercrime di Indonesia**

**#1 Surabaya Black Hat Pernah Retas 6 Situs Pemerintahan di Jawa Timur**

Tiga mahasiswa salah satu universitas di Surabaya yang tergabung dalam kelompok peretas atau hacker Surabaya, Black Hat, mengaku pernah membobol enam situs pemerintahan di Jawa Timur pada tahun 2017. Aksi mereka tercium polisi setelah melakukan pembobolan sejumlah situs baik dalam dan luar negeri serta melakukan pemerasan.  
"Mereka mendeklair bertanggung jawab atas peretasan enam situs pemerintahan di Jawa Timur," kata Kepala Subdit Cyber Crime Ditreskrimsus Polda Metro Jaya AKBP Roberto Pasaribu, Kamis (15/3/2018).   
Meski begitu, ia mengaku tak bisa membeberkan apa saja situs yang dimaksud. Ia hanya menyebut yang diretas adalah situs milik beberapa kabupaten di Jatim. "Website, ada pemerintah kabupaten apa gitu," ucap dia.

Tim Subdit IV Cyber Crime Ditreskrimsus Polda Metro Jaya membekuk dua orang peretas atau hacker berinisial KPS dan NA di daerah Surabaya, Jawa Timur. Penangkapan peretas yang menamakan diri kelompok SBH itu dilakukan Minggu, 11 Maret 2018.   
Kelompok ini sudah membobol ratusan website dalam dan luar negeri. "Mereka menjebol sistem pengamanan dari sistem elektronik milik orang lain. Kemudian mengancam atau menakut-nakuti dengan meminta sejumlah uang," ujar Kabid Humas Polda Metro Jaya, Komisaris Besar Polisi Argo Yuwono

# #2 63 penjahat Cyber Crime ditangkap Polri

Sebanyak 63 warga negara asing (WNA) berasal dari China dan Taiwan ditangkap petugas Mabes Polri di Medan dan Denpasar, Bali.  
Sebanyak 63 itu merupakan penjahat di dunia maya atau Cyber Crime tiba di Bandara Soekarno- Hatta, Tangerang, Kamis 20 Desember 2012 malam.  
Berdasarkan pengamatan di lokasi, setelah tiba, seluruh WNA tersebut kemudian digelandang menuju Mabes Polri untuk pemeriksaan lebih lanjut. Penjagaan ke-63 penjahat tersebut mendapat pengawalan ketat dari petugas polisi.

Seluruh WNA tersebut, dijemput oleh petugas Reskrim Mabes Polri langsung di landasan pacu (runway) Bandara tersebut dengan menggunakan dua unit bus.   
Para WNA itu, merupakan sindikat Cyber Crime yang telah beroperasi di Indonesia cukup lama dan diduga kuat terkait dengan jaringan kejahatan Internasional di China.

# #3 Tiga Hacker Mahasiswa juga Retas Sistem IT Lembaga Negara

Tim cyber crime Direktorat Reserse Kriminal Khusus (Ditreskrimsus) Polda Metro Jaya meringkus tiga orang peretas atau hacker di daerah Surabaya, Jawa Timur. Ketiga pelaku adalah KPS (21), NA (21), dan ATP (21), mahasiswa aktif di salah satu universitas di Surabaya.   
Berdasarkan pengakuan tersangka kepada polisi, apa yang mereka lakukan merupakan hal yang lumrah di dunia cyber. Dari pemeriksaan sementara, sedikitnya 600 website di 44 negara sudah diretas oleh ketiga pelaku.   
Namun secara keseluruhan, kejahatan cyber ketiganya bukan hanya meretas 600 website, tapi sekitar 3.000 sistem informasi dan teknologi (IT), termasuk sistem lembaga negara, baik di dalam maupun luar negeri. "Ada lembaga negara di luar negeri, tapi tidak bisa kami sebutkan," ujar Kabid Humas Polda Metro Jaya, Kombes Pol Raden Prabowo Argo Yuwono, kepada wartawa, Selasa (13/3/2018).

Sementara itu, Kasubdit Cyber Crime Polda Metro Jaya AKBP Roberto Pasaribum mengatakan, tidak tertutup kemungkinan jumlah website yang diteras ketiganya lebih dari 44 negara. "Total ada 44 negara dan tidak menutup akan bertambah. Ini masih dalam lidik," ujar Roberto.  
Roberto menjelaskan, ketiga pelaku hacker beraksi dengan menggunakan metode SQL Injection untuk merusak database. Aksi mereka kemudian terungkap setelah Polda Metro Jaya menerima informasi dari Federal Bureau of Investigation (FBI).  
"Kami kerja sama dan mendapat informasi itu. Kami analisa sampai dua bulan berdasarkan informasi dari FBI itu," pungkasnya.

#4 **Situs dan Akun Twitter Kelompok Hacker Lizard Squad Dibredel**

Serangkaian aksi serangan cyber yang dilakukan kelompok hacker [Lizard Squad](http://tekno.liputan6.com/read/2167640/siapa-sebenarnya-kelompok-hacker-lizard-squad) beberapa waktu belakangan membuat geram banyak pihak. Namun kini mereka mulai kena batunya.

Menurut yang dilansir laman Mirror, Jumat (30/1/2015), situs resmi [Lizard Squad](http://tekno.liputan6.com/read/2167462/akun-twitter-taylor-swift-diretas-lizard-squad) yang beralamatkan di [lizardpatrol.com](http://lizardpatrol.com/) sudah tidak dapat diakses. Situs tersebut telah dalam kondisi non-aktif alias offline. Sejauh ini kelompok hacker Anonymous mengklaim bahwa offline-nya situs milik Lizard Squad adalah hasil kerja mereka. “Situs Lizard Squad telah dibersihkan dan dalam keadaan offline: Lizardpatrol.com. Kami menang,” kicau akun Twitter @AnonymousUK2015.

Selain situs resmi, akun Twitter Lizard Squad ([@LizardMafia](https://twitter.com/account/suspended)) juga sudah diblokir. Pihak Twitter mengkonfirmasi perihal pemblokiran tersebut dan menyatakan bahwa akun @LizardMafia diadukan oleh banyak pengguna lain karena dianggap sangat meresahkan. Maka dari itu, Twitter bertindak tegas dengan memblokir akun @LizardMafia. Nama kelompok hakcer Lizard Squad sendiri dalam tempo beberapa bulan terakhir ini memang telah menjadi momok yang menakutkan di dunia maya.

Reputasi mereka sebagai kelompok peretas jempolan dimulai ketika pada akhir tahun 2014 kemarin, tepatnya pada malam perayaan Natal. Saat itu Lizard Squad mengklaim bahwa merekalah pihak yang bertanggung jawab atas tumbangnya dua layanan berbasis internet di ranah industri game, yakni [PlayStation Network](http://tekno.liputan6.com/read/2144844/situs-sony-playstation-di-hack) (PSN) dan Xbox Live.

Tak selang berapa lama, mereka pun meretas situs resmi maskapai penerbangan [Malaysian Airlanes](http://news.liputan6.com/read/2166426/bergambar-kadal-situs-malaysia-airlines-dibajak-lizard-squad) dengan men-deface (mengubah tampilan) laman situs. Lalu yang paling membuat heboh, enam (6) jejaring sosial kenamaan dibuat luluh lantak oleh oleh [Lizard Squad](http://tekno.liputan6.com/read/2167099/ini-penyebab-tumbangnya-facebook-dan-instagram). Keenamnya adalah Facebook, Instagram, MySpace, AOL Instant Messenger, Tinder dan Hipchat.

Mereka juga sempat meretas akun Twitter milik penyanyi populer Taylor Swift dan mengancam akan menyebarkan foto bugilnya di dunia maya.

#5 **Jutaan Password Pengguna Dropbox Dicuri Hacker**

Jutaan username dan password akun pengguna layanan Dropbox dikabarkan telah dibajak [hacker](http://tekno.liputan6.com/read/2118123/ratusan-ribu-foto-bugil-pengguna-snapchat-tersebar). Kebocoran sistem keamanan ini kabarnya berasal dari aplikasi pihak ketiga rekanan [Dropbox](http://tekno.liputan6.com/read/2099403/foto-bugil-artis-dicuri-hacker-amankah-simpan-data-di-cloud) yang berhasil diakses oleh para hacker.

Situs The Next Web menjadi pihak pertama yang melaporkan masalah ini. Mereka mengklaim telah menemukan penyebaran username dan password sekitar 400 akun Dropbox di laman forum Pastebin. Kelompok [hacker](http://tekno.liputan6.com/read/2117573/hacker-ancam-sebar-ribuan-foto-bugil-pengguna-snapchat) tersebut juga meninggalkan pesan bahwa mereka akan membocorkan lebih banyak lagi jika ada pihak yang berani membayar dengan mata uang digital Bitcoin.

Lebih lanjut dijelaskan, hacker mengaku memiliki sekitar 6,9 juta detail username danpassword pengguna layanan Dropbox. Menanggapi hal ini, pihak Dropbox sendiri telah merilis pernyataan resmi sebagai berikut:

“Dropbox tidak diretas. Username dan password yang sayangnya berhasil dicuri oleh hacker didapat dari layanan lain (aplikasi pihak ketiga) yang digunakan para pengguna untuk dapat masuk ke dalam akun Dropbox. Kondisi ini sama dengan yang terjadi pada Snapchat belum lama ini, ketika hacker berhasil mencuri sekitar 100 ribu foto dari aplikasi pihak ketiga. Sama seperti kami, server Snapchat juga tidak diretas, melainkan server layanan pihak ketigalah yang telah diretas.”

Dropbox sendiri mengaku telah mengirimkan email kepada para penggunanya untuk sesegera mungkin melakukan reset password. Tindakan ini diharapkan mampu meminimalisir korban pencurian detail login.

Kedua kasus yang menimpa Dropbox dan Snapchat memperlihatkan tren peretasan baru yang dilakukan oleh para hacker. Mereka kini tidak lagi menyasar server utama milik penyelenggara layanan, melainkan menyasar server milik aplikasi pihak ketiga.

Kondisinya menjadi sedikit pelik. Pihak penyelenggara layanan dapat dengan mudah mengatakan bahwa mereka tidak diretas, karena memang tidak.  Namun mereka memungkinkan pihak ketiga untuk membuat aplikasi yang terintegrasi dengan para pengguna. Pengguna lalu akan memanfaatkannya, padahal sistem keamanan aplikasi pihak ketiga ini tidak terjamin, dan penggunaannya di luar tanggung jawab penyelenggara layanan.

KASUS CYBERCRIME DI LUAR NEGERI

**#1 cybercrime pornografi John Zuccarini**

Zuccarini tercatat sebagai pelaku tindak pornografi di dunia maya yang pertama kali dimejahijaukan. Lelaki usia 53 tahun tersebut memiliki sebuah situs porno. Ia dengan sengaja memikat anak-anak di bawah umur untuk mengakses situs tersebut. Situs milik Zuccarini cukup banyak. Situs-situs yang diberi nama Joescartoon.com, joecartoon.com, joecartoons.com serta cartoonjoe.com dan beragam variasi domain yang mirip itu didaftarkan pada November 1999.

Cara John Zuccarini menarik perhatian dari remaja dan anak-anak agar bisa masuk ke situs pornonya adalah dengan menggunakan nama-nama domain yang populer di kalangan remaja dan anak-anak, seperti Bob the Builder, Britney Spears, Nsync, Disneyland, dan Teletubbies. Kurang lebih ada 3000 domain yang dipalsukannya atau dibuat mirip. Contohnya, ia mendaftarkan nama domain www.dinseyland.com, jadi bila seorang anak mengakses situs-situs palsu tersebut, mereka akan menuju situs yang menayangkan gambar-gambar porno, dan iklan-iklan pop up porno pun segera bermunculan. Zuccarini berdagang The Country Walk, JZDesign, RaveClub Berlin, dan lebih dari 22 nama yang menggunakan kata “Cupcake”, termasuk Cupcake Party, Cupcake-Party, Cupcake Parties, Cupcake Patrol, Cupcake Incident, dan Cupcake Messenger.

Tentu saja banyak anak di bawah umur yang terjebak oleh ulah Paman John ini. Akhirnya ia ditangkap pihak berwajib Amerika Serikat pada hari Rabu tanggal 3 September 2002 di sebuah hotel di Florida, dan sudah berada di penjara kepolisian Manhattan.

Berdasarkan undang-undang Truth in Domain Names Act, tindakan Zuccarini digolongkan sebagai kejahatan karena memikat anak-anak ke dalam pornografi internet. Zuccarini bisa dijatuhi hukuman penjara hingga empat tahun dan denda sebesar 250.000 dolar AS.

**#2 menyusup ke dalam sistem jaringan komputer Alta Vista Chavet**

Peristiwanya sudah cukup lama berselang, Juni 2002. Namun aksi yang dilakukan oleh Laurent Chavet ini baru diputuskan oleh Pengadilan Negeri California pada 2005 kemarin. Chavet didakwa bersalah karena menyusup ke dalam sistem jaringan komputer Alta Vista dan menimbulkan kerusakan di dalamnya. Lelaki berusia 30 tahun asal Kirkland ini telah menggunakan password dan username karyawan Alta Vista untuk mengakses jaringan komputer tempat ia pernah bekerja itu dari rumahnya di Mateo, California. Sejumlah data penting Alta Vista telah dihapus dan dirusak oleh Chavet tanpa sepengetahuan karyawan lain.

Chavet resmi didakwa bersalah pada 2 Juli 2004. Ia dikenai pasal yang mengatur ikhwal pelarangan mengakses tanpa izin ke sistem komputer yang dilindungi, yakni pasal 18 U.S.C. ayat 1030(a)(4). Jerat lain adalah pada pasal yang sama ayat 1030(a)(5) tentang mengakibatkan kerusakan pada sistem komputer yang dilindungi.

Putusan hukuman dilakukan pada 19 Agustus 2005 oleh Hakim Susan Illston dari San Fransisco. Chavet dikenai hukuman penjara lima tahun dan denda sebesar 250.000 dolar Amerika.

Tertangkapnya Chavet adalah hasil investigasi bersama antara pihak Computer Hacking and Intellectual Property (CHIP) Unit of the United States Attorney’s Office dan Federal Bureau of Investigation (FBI).

**#3  pembuat program worm Anthony Scott Clark.**

Kasus paling gres yang baru saja diputus hakim Amerika Serikat adalah pembuat program worm Anthony Scott Clark. Pemuda asal Oregon ini masih berumur 21 tahun waktu didakwa oleh penuntut umum Kevin V. Ryan pada Desember 2005 lalu. Penyebabnya terkesan simpel, tetapi fatal akibatnya. Clark sepertinya iseng menyerang situs belanja online eBay dengan worm buatannya. Akibat ulahnya itu Clark berhasil menginfeksi begitu banyak komputer yang mengunjungi eBay pada bulan Juli dan Agustus 2003.

Selama periode itu Clark menyebarkan kerusakan berupa Distributed Denial of Services (DDOS) pada situs eBay. Serangan DdoS merupakan salah satu jenis serangan yang menyebabkan terjadinya penolakan terhadap perintah user. Target dari aksi ini adalah sistemnya.

Selama kurun waktu itu pula Clark telah menghasilkan sekitar 20.000 bots yang dihasilkan program worm-nya. Bots ini masuk melalui celah kelemahan yang terdapat pada Windows Operating System – “Remote Procedure Call for Distributed Component Object Model,” alias RPC-DCOM. Bot ini beraksi melalui server Internet Relay Chat (IRC). Begitu user terkoneksi, melakukan log, lalu Clark tinggal menginstruksi agar bot melakukan serangan DdoS pada komputer yang terhubung ke internet. Secara personal Clarks memerintahkan agar bot-bot itu merilis serangan DdoS pada server bernama eBay.com. Maka bukan hanya komputer yang terhubung dengan IRC saja yang terinfeksi, melainkan juga situs eBay.

Atas tindakannya ini Clark dijerat dengan tuntutan penjara maksimum 10 tahun dan denda 250.000 dolar Amerika Serikat. Pada 3 April 2006 akan dijadwalkan ketokan palu terakhir oleh Hakim James Ware.

**#4 2.4 milyar poundsterling kerugian akibat kejahatan berteknologi canggih.**

Pada tahun 2004, kegiatan bisnis di Inggris sempat mengalami kerugian sekitar 2.4 milyar poundsterling akibat kejahatan yang dilakukan secara elektronik, demikian menurut pengakuan Unit Nasional Kejahatan Teknologi Tinggi (The National Hi-Tech Crime Unit).

Unit ini telah mengklaim bahwa pada kongres kejahatan internet (E-Crime Congress) yang dilaksanakan di London pada 5 April 2005, yang menurut sebuah survei yang dilakukan oleh NOP, sekitar 89% dari sampel contoh yang terdiri dari 200 perusahaan mengatakan bahwa mereka sempat mengalami berbagai bentuk serangan kejahatan berteknologi tinggi sejak tahun 2004.

Menurut survei tersebut, dapat dilaporkan bahwa:

- 90% dari 200 perusahaan di Inggris pernah mengalami serangan penetrasi yang ilegal yang berusaha masuk ke sistem komputer perusahaan mereka.

- 89% merasa pernah dirugikan akibat data-data informasi penting mereka telah dicuri dan lolos keluar melalui jaringan internet

- 97% dari responden pernah mengalami serangan virus komputer yang telah merugikan mereka sekitar 71 poundsterling

- Sementara kerugian akibat penipuan/pemalsuan data finansial (financial fraud) telah merugikan mereka sekitar 9% yaitu sebesar 68 juta poundsterling.

Survei ini juga menemukan bahwa lebih dari seperempat jumlah perusahaan yang menjadi responden telah gagal dalam mengamankan jaringan data mereka saat dilakukan proses audit keamanan jaringan data.

Trevor Pearce, direktur jendral Pasukan Nasional Pencegah Kejahatan (National Crime Squad), pernah mengungkapkan pada para delegasi yang menghadiri kongres ini bahwa "tiga puluh lima persen dari perusahaan-perusahaan yang disurvei di Inggris tidak mempunyai masalah dalam hal prosedur manajemen krisis, dimana dalam hal ini, kami tahu bahwa dari pengalaman panjang menangani jaringan offline dunia, sangat esensial untuk mengenali situasi dan gejala-gejala tindak pemerasan."

Dia mengkonfirmasi bahwa agen rahasia yang menangani masalah kejahatan serius dan terorganisir (SOCA \_ Serious and Organised Crime Agency), telah merencanakan untuk bekerja sama dengan para pegawai pemerintah dalam hal pertanggungjawaban mereka untukmenangani masalah kejahatan berteknologi tinggi yang terorganisir baik lokal maupun internasional melalui unit ini, bila unit ini sudah benar-benar bekerja dengan baik.

Kasus kejahatan penipuan/pemalsuan (fraud) yang pernah terjadi di India, mengungkap adanya indikasi kebocoran data finansial akibat adanya sistem outsourcing di BPO, katanya lagi, dan keluhan ini disampaikan pada Nasscom maupun pada pemerintah India untuk bertindak lebih serius dalam menangani pengamanan serta perlindungan data, maupun memberlakukan screen test bagi para calon karyawan yang akan bekerja di sektor industri perbankan (baik yang langsung maupun yang melalui outsourcing).

**#5 pencuri digital situs perbankan**

Pada bulan April 2005, polisi Estonia telah berhasil menangkap seorang pemuda berusia 24 tahun yang didakwa telah mencuri dan membobol dana sebesar jutaan dollar dari rekening-rekening online bank-bank di seluruh Eropa dengan menggunakan virus yang dapat menghapus dirinya sendiri setelah pekerjaan haram itu dilakukan.

Modus operandi di pencuri adalah dengan menuliskan semacam pengumuman yang mengatasnamakan lembaga-lembaga pemerintah, bank-bank dan perusahaan-perusahaan investasi, yang dalam pengumuman yang dikirim online tersebut dicantumkan pula sebuah link yang secara sembunyi-sembunyi akan mengirimkan (mengupload) virus. Virus ini kemudian mentransmisikan setiap data pribadi, termasuk data rekening dan password internet banking yang dikirimkan kepada si pencuri yang menciptakan virus ini. Setelah pekerjaan mengirimkan informasi finansial ini selesai dilakukan, maka virus itu akan menghapus dirinya sendiri setelah sebelumnya mengosongkan isi seluruh rekening yang ada di rekening yang dibobolnya. Sang pencuri digital itu pun diganjar lima tahun penjara akibat ulahnya.