1. **Peretasan 1 milyar akun Yahoo. (Muhammad Rayyan Abhad - 155150200111222)**

Sebanyak 500 juta pengguna layanan internet Yahoo dikabarkan telah diretas pada September 2017 lalu. Lantas pada 15 Desember 2017, Yahoo merevisi kabar tersebut dengan mengatakan 1 miliar akun penggunanya telah dibobol oleh oknum tak bertanggung jawab. Hingga kini Yahoo belum bisa mengidentifikasi pelaku yang memanfaatkan celah pada sistem perusahaannya. Dengan ini, Yahoo sudah tiga kali mengalami peretasan selama empat tahun belakangan. Hal ini mau tak mau berpengaruh pada posisi bisnis Yahoo. Verizon yang sudah sepakat mengakuisisi Yahoo pada Juli 2017 lalu mengatakan akan bernegosiasi ulang dengan perusahaan yang jaya pada awal 2000-an itu. Mengutip Reuters, aksi peretasan kali ini bahkan lebih buruk dibanding sebelumnya karena Yahoo berasumsi peretas berhasil mengakses data terkait nama, alamat email, nomor telepon, kata sandi, pertanyaan keamanan lengkap dengan jawab alternatif baik yang terenkripsi maupun tidak.

1. **Kasus Carding Terhadap Beberapa Bank Oleh Sebuah Sindikat (Muhammad Hakiem - 155150201111298)**

Direktorat Kriminal Khusus Polda Metro Jaya berhasil mngunkap sindikat penggandaan kartu kredit atau yang disebut dengan Carding. Kejahatan Carding tersebut telah dilakukan sejak tahun 2000 terhadap beberapa bank yang ada di Indonesia. Pelakunya bernama Andre Christian Brail (28) dan Khayrunnisa (44) yang merupakan eksekutor dari kejahatan tersebut. Cara kerja dari kejahatan Carding ini adalah dengan memanfaatkan pin dan nomor kartu kredit nasabah yang masih bisa digunakan untuk otorisasi secara ilegal. Kemudian dengan menggunakan kartu kredit kosong dicetak melalui perangkat komputer dan mesin cetak canggih. Setelah itu kartu tersebut dapat digunakan untuk transaksi seperti belanja, menginap di hotel serta melakukan tarik tunai. Didapatkan berbagai barang bukti dari kedua tersangka tersebut berupa 27 lembar kartu kredit palsu, delapan buah handphone, sebuah mesin cetak embosser, sebuah skimmer merk MSR 2006, dua buah laptop, sebuah alat pemabaca (umron), sebuah harddisk, sebuah tas merk samhose, dua buah tas merek Charles and Keith hasil transaksi, dan catatan nomor kartu yang diperoleh dari internet. Masih ada satu orang yang dikejar oleh pihak polisi dengan inisial KR yang diduga bertugas memberi data nasabah dari berbagai bank kepada kedua tersangka tersebut. Kedua tersangka tersebut dijerat UU pasal 263 KUHP dan 378 KUHP soal pemalsuan kartu kredit.

Sumber: [www.kompas.com](http://www.kompas.com)

1. **Smiling Hacker Asal Palestina (Akmal Subakti – 155150201111320)**

Awal Januari 2013, pihak kepolisian Thailand menangkap salah satu hacker paling dicari di dunia, Hamza Bendelladj. Bendellaj merupakan pria asal aljazair yang merupakan pemasok virus bernama SpyEye yang dimanfaatkan untuk mencuri uang dari sistem jaringan bank, lembaga keuangan lain, hingga akun pribadi.

Periode 2009-2011 adalah masa-masa kejayaan Bandelledj dalam menjajakan SpyEye. Bersama rekannya asal Rusia, Aleksandr Andreevich Panin, program SpyEye laku keras di pasar gelap internet. Korban dari pencurian data itu mencakup lebih dari 1,4 juta komputer di Amerika Serikat saja, belum termasuk negara-negara lain.

Bendelladj dan Panin menggerakkan imperium kejahatan sibernya dari Rusia sejak 2009. Dari sana mereka menjual SpyEye secara online mulai US$1.000 hingga US$10.000. Berdasarkan keterangan pihak keamanan Amerika Serikat, SpyEye laku keras di pasar gelap dengan klien mencapai 150 lebih. Salah satu dari klien tersebut diperkirakan telah menilap US$3,2 juta atau sekitar Rp42 miliar dalam kurun waktu 6 bulan dengan malware SpyEye.

Awal dari akhir petualangan Bendelladj dimulai ketika penegak hukum berhasil mengindentifikasi keberadaannya ketika ia ketahuan menjual salinan virus SpyEye senilai US$8.500 atau setara dengan Rp111 juta dengan aparat yang melakukan penyamaran. Semenjak itu, Bendelladj resmi menjadi buronan biro investigasi federal (FBI) AS. Dengan nilai kerugian yang ditanggung perbankan AS mencapai US$20 juta, FBI mengerahkan tenaganya untuk menemukan jejak Bendelladj di seluruh dunia. Dua tahun kemudian, tepatnya pada 6 Januari 2013, Bendelladj akhirnya ditangkap oleh kepolisian Thailand di Bandara Suvarnabhumi saat transit menuju Mesir dari Malaysia

Sumber : [www.cnnindonesia.com](http://www.cnnindonesia.com)

1. **Facebook memata-matai aktivitas data pengguna melalui jaringan internet (Hugo Ghally Imanaka – 155150200111225)**

Pada aplikasi facebook sering kali melihat tawaran untuk mengetahui "Siapa yang melihat profil Anda" dan para pengguna facebook dengan rasa penasaran akan mengklik tautan yang disuguhkan. padahal sesungguhnya tautan tersebut adalah malware atau program jahat terbaru yang tengah beredar di facebook.  Saat mengkliknya para pengguna facebook akan diarahkan ke suatu aplikasi yang memiliki akses ke profil.

Facebook telah yang memanfaatkan jaringan Internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran. Kejahatan ini biasanya ditujukan terhadap saingan bisnis yang dokumen ataupun data pentingnya (data base) tersimpan dalam suatu sistem yang computerized (tersambung dalam jaringan komputer).

Sumber: <https://inet.detik.com/security/d-1505695/waspadai-aplikasi-siapa-yang-melihat-profil-anda-di-facebook--?fbclid=IwAR0cjur8tbsq1lM-2o_QV_AthHcwHZyKARmW2B2ijFhqz1YqPF4wqaNQ76M>

1. **Typosquatting (Masayu Vidya R – 155150201111292)**

Pada tahun 2001, internet banking diributkan oleh kasus pembobolan internet banking milik Bank BCA. Kasus tersebut dilakukan oleh seorang mantan mahasiswa ITB Bandung yang bernama Steven Haryanto. Steven membeli domain-domain internet dengan harga sekitar US$20 yang menggunakan nama dengan kemungkinan orang-orang salah mengetikkan dan tampilan yang sama persis dengan situs internet banking resmi milik Bank BCA yaitu, http://www.klikbca.com, misalnya klikbac.com

Steven Haryanto dapat disebut sebagai hacker, karena dia telah mengganggu suatu sistem milik orang lain, yang dilindungi privasinya. Steven dapat digolongkan dalam tipe hacker sebagai gabungan white-hat hacker dan black-hat hacker, dimana Steven hanya mencoba mengetahui seberapa besar tingkat keamanan yang dimiliki oleh situs internet banking Bank BCA. Steven disebut white-hat hacker karena dia tidak mencuri dana nasabah, tetapi hanya mendapatkan User ID dan password milik nasabah yang masuk dalam situs internet banking palsu. Namun tindakan yang dilakukan oleh Steven, juga termasuk black-hat hacker karena membuat situs palsu dengan diam-diam mengambil data milik pihak lain. Hal-hal yang dilakukan Steven antara lain scans, sniffer, dan password crackers. Maka perkara ini bisa dikategorikan sebagai perkara perdata.

Sumber : <http://appletechnos.com/>

1. **Peretasan Situs SBY (Ajeng Ardhia Arya Kusuma Putri – 155150201111294)**

Dilansir dari nasional.kompas.com, saya menyoroti kasus peretasan situs resmi mantan Presiden Republik Indonesia, Bapak Susilo Bambang Yudhoyono (SBY) yaitu http://www.presidensby.info. Situs yang biasanya memuat kegiatan presiden ini, hanya menampilkan layar hitam dan tidak bisa membuka konten-konten di dalamnya.

Situs SBY yang dimaksud tampak bertuliskan jemberhacker.web.id dan layar hitam, serta tulisan “! Hacked by MJL 007 ! This is a PayBack From Jember Hacker Team”. Pelaku yang bernama Wildan Yani Ashari melakukan aksi tersebut dengan cara masuk menggunakan teknik SQL Injection atau Injeksi SQL ke laman http://www.jatirejanetwork.com dimana situs presidensby.info mendaftarkan hostingnya.

Sebelumnya, pada 8 Januari 2013 Wildan mengakses laman http://www.enom.com, sebuah laman yang merupakan domain registrar www. techscape.co.id, hingga berhasil melakukan log in ke akun techscape di domain registrar eNom. Inc yang bermarkas di Amerika Serikat. Dari situlah Wildan mendapatkan informasi tentang Domain Name Server (DNS) laman www.presidensby.info. Wildan menggunakan akun melalui jatirejanetwork, dan menempatkan sebuah file HTML Jember Hacker Team. Sehingga pengakses ketika membuka www.presidensby.info yang sebenarnya yang terakses adalah tampilan file HTML Jember Hacker Team.

Dari contoh kasus “Meretas Situs SBY” di atas, saya mengidentifikasinya sebagai jenis Cybercrime “Unauthorized Access to Computer System and Service” dimana Wildan melakukan aksi dengan menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Dengan maksud sabotase atau melakukannya hanya karena untuk mencoba keahliannya.

1. **Kasus Penipuan Melalui Email oleh Jaringan Nigeria (Maulidiya Qurrota A’yun – 155150201111295)**

Kasus penipuan dengan modus melalui email jaringan negara Nigeria yang beroperasi di Indonesia. Diketahui pelaku menggunakan email dengan identitas hijacking /419 Nigerian Scam/ Bussiness Email Compromise (BEC). Dalam kasus ini terdapat 3 orang yang terlibat yaitu : Ndubuike Gilber Ukpogu (30) warga negara Nigeria, Dina Febriyanti (31) warga asal Indonesia, Puput Bambang (35) warga asal Indonesia.

Modus dan motif para pelaku Ndubuike Gilber Ukpogu mendapatkan perintah melalui Email dari seorang Hacker bernama Mr. Bright di Nigeria untuk membuka rekening bank penampung. Kemudian Mr. Bright meminta bantuan kepada tersangka Dina Febrianti dan Puput Bambang untuk membuka rekening bank menggunakan KTP palsu di berbagai bank di Jakarta.

Orang-orang ini telah menipu salah satu korban atas nama Louisa Poh sebanyak Rp271 juta di rekening penampung BANK NOBU. Setelah dilakukan penyidikan, dari hasil analisis transaksi keuangan rekening bank milik tersangka ternyata banyak korban lain dari berbagai negara yang merugi hungga jutaan rupiah.

Atas perbuatannya, pelaku dijerat Pasal 263, Pasal 378 Kuhp, Pasal 30 Ayat (1), Ayat (2) Ayat (3), Pasal 35, Pasal 36 Undang-Undang ITE Nomor 19 Tahun 2016, Jp Pasal 82, Pasal 85 Undang-Undang No. 3 Tahun 2011 Tentang Transfer Dana. Sedangkan untuk Mr.Bright sudah dimasukkan dalam Daftar Pencarian Orang (DPO).

Dari kasus diatas masih banyaknya cyber crime yang menyerang bank bank di indonesia, menurut saya bank indonesia harus lebih berhati hati oleh cyber crime sepeeti ini.

Sumber : <https://news.okezone.com/read/2018/11/16/337/1978804/polri-ungkap-kasus-penipuan-melalui-email-oleh-jaringan-nigeria>

1. **Cyberterrorisme Domain Situs** [**www.anshar.net**](http://www.anshar.net) **(Siti Utami Fhylayli – 155150201111296)**

Contoh Kasus Cyberterrorisme domain situs www.anshar.net yang ditengarai sebagai situs yang digunakan oleh kelompok jaringan teroris di Indonesia untuk melakukan propaganda terorisme melalui internet. Domain tersebut dibeli dari kartu kredit curian (hasil carding). Situs tersebut dibeli atas nama Max fiderman yang tentunya bukan nama asli.

Kasus di atas merupakan jenis cyber terorism, karena marupakan kejahatan yang bersifat terorisme yaitu memanfaatkan teknologi internet untuk kejahatan terorisme dengan membeli domain yang merupakan situs kelompok jaringan teroris dan melakukan propaganda terorisme.serta kasus tersebut merupakan jenis carding karena menggunakan kartu kredit curian/palsu untuk membeli domain tersebut.

Cara penanggulangan :

Melakukan modernisasi hukum pidana nasional beserta hukum acaranya, yang diselaraskan dengan konvensi internasional yang terkait dengan kejahatan tersebut. Meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime.

Meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut

Meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional.

1. **MORRIS WORM (Rahma Kurnia Sari – 155150201111291)**

Pada tanggal 26 Juli 1989, Cornell mahasiswa pascasarjana Robert Tappan Morris didakwa menyebarkan virus worm pertama Internet, menginfeksi lebih dari 6.000 universitas, pusat penelitian dan komputer militer. Robert Tappan Morris adalah lulusan Harvard dan Cornell mahasiswa pascasarjana ketika ia mengembangkan pertama tersebar luas Internet “cacing.” Dia dirilis pada 2 November 1988, dengan menggunakan sistem MIT untuk menyamarkan kenyataan bahwa ia adalah seorang mahasiswa Cornell.

Robert Morris menjadi orang pertama yang dihukum di bawah 1986 US Computer Fraud and Abuse Act (Undang-undang penyalahgunaan Komputer) karena tindakannya. Setelah insiden inimulai dibentuklah Computer Emergency Response Team Coordination Center, CERT/CC.

ANALISA >

Morris Worm adalah salah satu malware pertama yang menghebohkan dunia. Nama malware ini diambil dari nama pembuatnya Robert Morris, pada saat itu adalah mahasiswa di Cornell University. Malware ini mulai dipublish tanggal 2 november 1988. Malware ini berhasil menginfeksi lebih dari 6000 komputer, padahal saat itu baru sekitar 60000 komputer yang terhubung internet. Jadi malware ini menginfeksi sekitar 10% komputer dunia pada saat itu. Perkiraan kerugian yang diakibatkan adalah sekitar $100.000–10.000.000.

Malware ini mengeksploitasi celah keamanan pada Unix sendmail, finger, rsh/rexec, serta password lemah (yang mudah ditebak). Selain itu beberapa infeksi malware dapat menyebabkan serangan DOS attack. Malware ini dapat berpindah dari satu komputer ke komputer lain yang terhubung pada jaringan. Ketika menemukan sebuah komputer baru, malware mempunyai mekanisme menanyakan apakah sudah terdapat kopi dari worm pada komputer tersebut. Nah disinilah kelemahan worm ini. Kita bisa menjalankan sebuah proses yang akan menjawab “ya” apabila malware menanyakan apakah pada komputer telah terdapat kopi dari morris worm ini. Dengan itu maka worm tidak akan menginfeksi komputer kita. Nah kemudian Michael Rabin mencoba mencari cara untuk mengelabui cara pertahanan ini yaitu dengan mantra, “Randomization.”

PASAL YANG DILANGGAR >

Morris segera diidentifikasi sebagai sumber dari worm, dan pihak berwenang berusaha untuk mendakwa dia di bawah 1986 Penipuan Komputer dan UU Penyalahgunaan , yang dilarang mendapatkan akses tidak sah ke komputer federal.

Butuh jaksa delapan bulan untuk menjatuhkan dakwaan karena ada “perdebatan internal mengenai apakah mungkin mustahil untuk membuktikan tuduhan,” lapor The New York Times. Jaksa harus membuktikan bahwa “Morris dimaksudkan untuk melumpuhkan jaringan komputer.”

Morris dinyatakan bersalah pada tahun 1990 . Dia diberi hukuman ringan: sebesar $ 10.050 denda, 400 jam pelayanan masyarakat, dan masa percobaan tiga tahun.

SARAN >

Keamanan komputer kembangkan lagi menjadi sebuah industri sendiri

Memberi arahan untuk masyarakat rekayasa Internet tentang risiko bug perangkat lunak

Menetapkan panggung untuk keamanan jaringan menjadi daerah yang sah penelitian dan pengembangan.