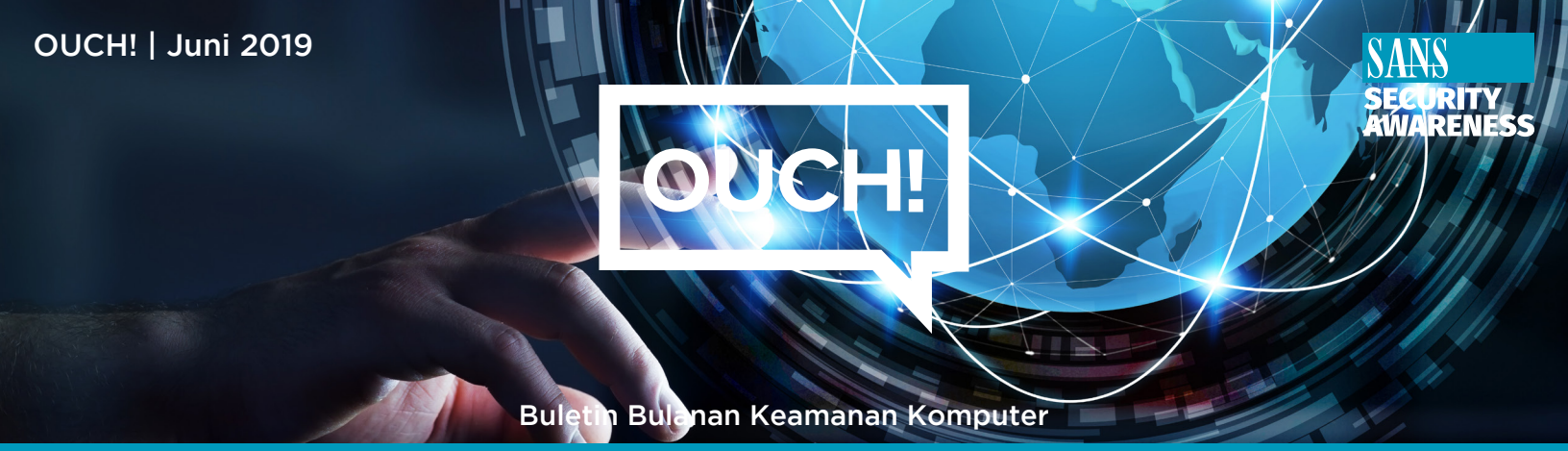


Buletin Bulanan Keamanan Komputer

# Dark Web

## Sekilas

Anda mungkin pernah mendengar istilah “Dark Web” di media dan bertanya-tanya “apa itu Dark Web?” atau “perlukah melakukan sesuatu?”. Di sini akan diulas sekilas apa itu Dark Web dan manfaatnya bagi Anda.

## Mengenal Dark Web

Dark Web tersusun dari berbagai sistem di internet, dirancang sebagai sarana komunikasi dan berbagi informasi secara aman dan anonim (tanpa nama). Ada banyak “Dark Web” beroperasi, tidak seperti Facebook yang dikelola oleh satu organisasi. Dark Web merupakan gabungan beragam sistem dan jaringan dikelola oleh banyak pihak untuk aneka keperluan. Sistem Dark Web tersambung dan merupakan bagian dari sistem internet, namun tidak mudah ditemukan dengan menggunakan sistem browser biasa. Diperlukan perangkat lunak khusus untuk menemukan dan mengaksesnya. Misalnya Tor Project. Untuk mengakses Dark Web ini perlu unduh dan pasang perangkat lunak browser Tor.Pada saat menggunakan browser Tor, pertukaran data antar komputer sesama pengguna Tor akan dienkripsi. Dalam perjalanannya, alamat IP yang digunakan akan berubah, artinya pada saat sebuah situs diakses, aktifitas online Anda bersifat anonim. Contoh lain Dark Web adalah Zeronet, Freenet dan I2P.

## Siapa Penggunanya?

Kriminalis Siber adalah pengguna terbesar Dark Web. Mereka memiliki situs web dan forum disksusi di dalam Dark Web dengan tujuan untuk menunjang aktifitas kriminal seperti jual beli obat terlarang atau jual beli data curian secara anonim dan aman. Contoh: saat terjadi pembobolan bank atau toko daring, informasi dicuri bakal dijual ke pihak lain melalui situs yang ada di Dark Web.

Dark Web bisa juga bermanfaat. Misal, disebuah negara dimana sensor informasi ada dimana-mana, jaringan Dark Web bisa digunakan untuk berbagi informasi sekaligus menyimak perkembangan dunia secara aman dan anonim. Jurnalis, pengungkap informasi penting dan pihak-pihak yang sadar akan pentingnya privasi bisa menggunakan Dark Web guna meningkatkan tingkat anonimnya sekaligus menerabas sistem sensor informasi. Selain itu, orang-orang seperti itu tidak hanya bisa menggunakan teknologi Browser Tor guna mengakses Dark Web tapi juga internet biasa.

## Apa Yang Harus Dilakukan

Bila tidak ada alasan kuat untuk memakai Dark Web, hindari penggunaannya. Beberapa situs Dark Web dikaryakan untuk melakukan tindakan ilegal, banyak situs itu akan menggunakan komputer Anda sebagai jalan pintas dalam mencapai tujuannya, dibeberapa kejadian malahan bisa merambah dan menyerang komputer Anda. Berbagai perusahaan menawarkan jasa pemantauan dan akan mengirimkan pesan bila nama atau informasi lainnya dicuri oleh kriminalis siber dan ditemukan di Dark Web. Apakah notifikasi seperti itu berguna? Masih belum bisa dipastikan manfaatnya. Cara perlindungan terbaik adalah berasumsi bahwa data pribadi Anda telah terpapar di Dark Web dan digunakan oleh kriminalis siber. Jadi simak hal-hal berikut ini:

- **Waspada terhadap telepon atau surel seakan-akan berasal dari organisasi resmi dan mendesak Anda melakukan sebuah tindakan seperti membayar denda. Pelaku kriminal malahan bisa menggunakan informasi tentang Anda guna merancang serangan khusus untuk Anda.**
- **Awasi penggunaan kartu kredit dan laporan bank. Kalau perlu atur notifikasi otomatis saat terjadi transaksi. Dengan cara ini Anda bisa memantau kemungkinan terjadinya penyalah gunaan. Bila hal itu terjadi, segera laporkan ke perusahaan kartu kredit atau bank.**
- **Awasi "Credit Score" (khususnya di Amerika) Anda. Itu tidak berdampak pada penggunaan kartu kredit Anda dan merupakan cara paling ampuh untuk melindungi diri dari pencurian data pribadi.**

## Versi Bahasa Indonesia

BIPIMax memberikan Pelatihan Optimasi Proses Bisnis (LSS) dan Pengenalan Keamanan & Proteksi Informasi. Informasi lengkap: http://www.bipimax.net

## Editor Tamu

***Micah Hoffman*** *(@WebBreacher) is investigator utama di Spotlight Infosec LLC, instruktur bersertifikat SANS Institute dan perancang pelatihan SANS OSINT. Micah memadukan seluk beluk bidang inteligensia siber dan open source dalam proyeknya, bahan pelatihan dan gaya pengajaran.*

## Sumber Pustaka


| | |
|---|---|
| Penipuan Terfokus: | https://www.sans.org/u/RfW |
| Rekayasa Sosial: | https://www.sans.org/u/Rg1 |
| Identity Theft: | https://www.identitytheft.gov |
| Credit Freeze: | https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/ |
| Tor Browser: | https://www.torproject.org/ |
| SANS OSINT Course: | https://sans.org/sec487 |