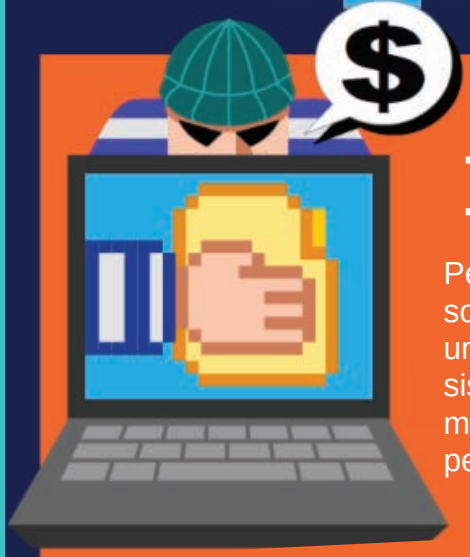
BULETIN ICT MOT

www.mot.gov.my

Bil. 2/2017

SIDANG REDAKSI BULETIN ICT MOT

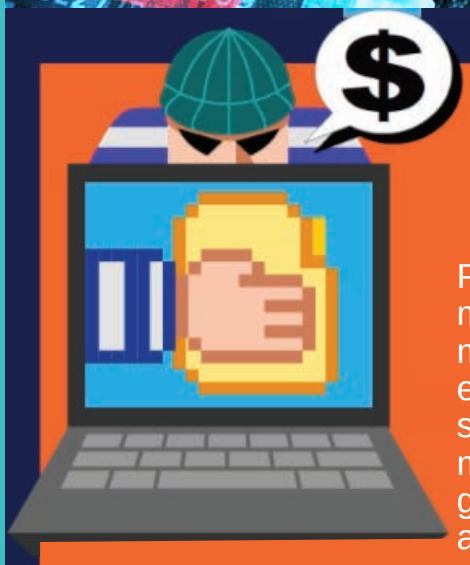
Diterbitkan Oleh:
Bahagian Pengurusan Maklumat,
Aras 7, No. 26, Jalan Tun Hussein,
Presint 4, Pusat Pentadbiran Kerajaan
Persekutuan, 62100 Putrajaya
Tel: : 603-8000 8000
Faks : 603-8888 1999
Website : www.mot.gov.my



Apa itu RANSOMWARE??

Perisian jahat atau malicious software (malware) direka khas untuk menjangkiti sebuah sistem komputer atau peranti mudah alih tanpa pengetahuan pengguna.

Melaksanakan fungsi tertentu bergantung kepada matlamat penciptanya, antara fungsi perisian jahat termasuk mengintip dan mencuri data (cyber espionage), memeras ugut (ransomware), memadam data (angkara cecacing) dan menjejaskan sistem komputer.



Bagaimana serangan RANSOMWARE berlaku??

Penjenayah siber mengunci maklumat atau fail penting milik mangsa sebelum memeras ugut mangsa dengan sejumlah wang tebusan bagi membolehkan mangsa mengakses semula maklumat atau fail mereka

Apabila mangsa memetik (klik) pautan tersebut, malware akan menyelinap masuk dan menjangkiti sistem computer. Ia akan mengunci komputer dan juga menyulitkan (encrypt) fail yang terdapat di dalam komputer berkenaan menyebabkan akses kepada komputer serta fail-fail didalamnya tidak dapat dicapai.

Melalui kaedah muat turun sesuatu program atau aplikasi dari sumber yang diragui.

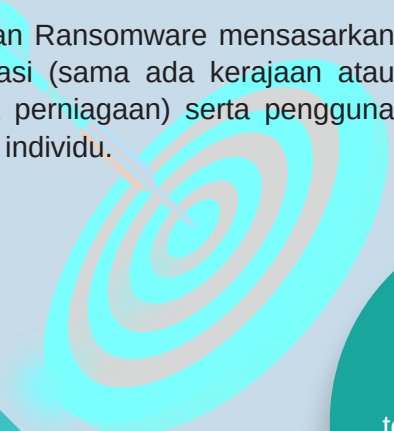
Cecacing ini akan menular di dalam rangkaian sistem komputer dengan sendiri berlainan kaedahnya dengan jenis Ransomware lain yang hanya akan bertindak setelah mendapat arahan dari penjenayah siber yang dibuat secara 'remote'.

Dalam isu serangan Ransomware 'WannaCry', ia dikatakan merebak dengan cepat kerana jangkitan tersebut berlaku melalui cecaing (worm) yang dihantar melalui spam emel yang mempunyai pautan berbahaya (malicious links) dan juga melalui dokumen Words, PDF atau fail lain yang disebarkan melalui e-mel.

Pengguna memetik (klik) pautan yang dihantar bersama e-mel menerusi kaedah yang dipanggil phishing iaitu suatu kaedah di mana penjenayah siber melakukan penipuan untuk mendapatkan maklumat sulit/sensitif seperti nama pengguna, katalaluan dan butiran kewangan dengan menyamar sebagai entiti yang boleh dipercayai pengguna.

Siapakah Sasaran Ransomware ?

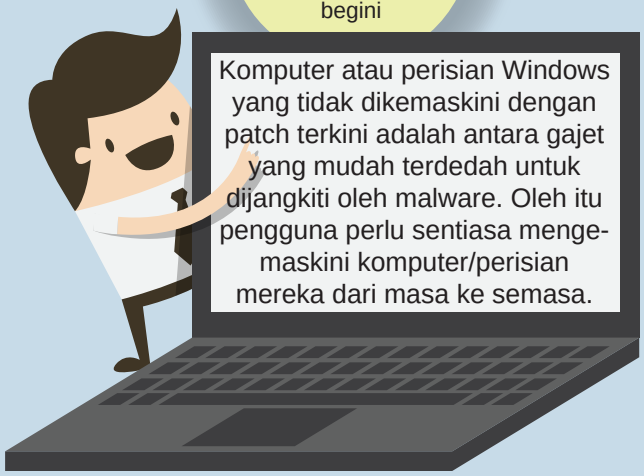
Ancaman Ransomware mensasarkan organisasi (sama ada kerajaan atau syarikat perniagaan) serta pengguna internet individu.



Nasihat kepada pengguna internet (individu) dan juga pentadbir rangkaian sistem komputer untuk menghindar dari menjadi mangsa ransomware

- Sentiasa kemaskini perisian anti-virus yang terkini
- Pastikan sistem operasi komputer dan perisian dikemaskini dengan patch terkini
- Jangan ikuti pautan web dalam emel yang tidak diminta
- Berhati-hati apabila membuka lampiran pada emel
- Ikut amalan terbaik dan selamat semasa menyemak imbas web

Jenis komputer/ perisian yang senang dicerobohi oleh malware begini



Komputer atau perisian Windows yang tidak dikemaskini dengan patch terkini adalah antara gajet yang mudah terdedah untuk dijangkiti oleh malware. Oleh itu pengguna perlu sentiasa mengemaskini komputer/perisian mereka dari masa ke semasa.

UPDATE ANTI-VIRUS

① Klik ikon 'e' di Task Bar

② Klik Menu UPDATE

UPDATE

Klik UPDATE NOW

Update now

SCAN PC

① Klik ikon 'e' di Task Bar

② Klik Menu COMPUTER SCAN

COMPUTER SCAN

③ Klik butang Smart scan

Smart scan
Local disk scan

CUSTOM SCAN

① Klik ikon 'e' di Task Bar

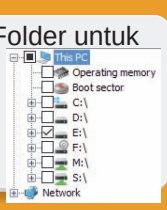
② Klik Menu COMPUTER SCAN

COMPUTER SCAN

③ Klik butang Custom scan

Custom scan
Selection of scan profile and targets to scan

④ Pilih Folder untuk scan

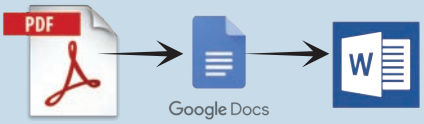


⑤ Tunggu sehingga selesai

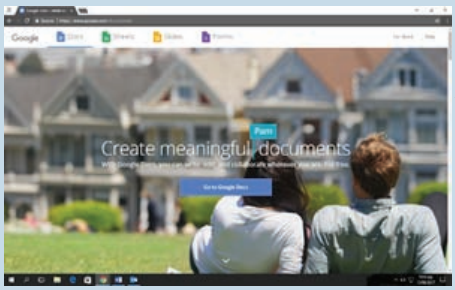
Custom scan - Scan completed

Threats found: 0
Virus signature database used: 15928 (20170817)

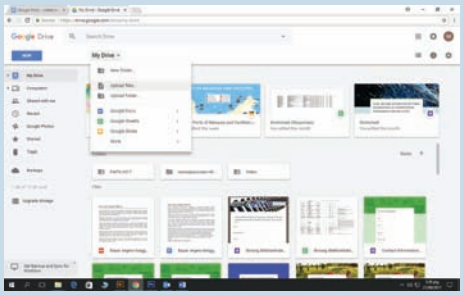
Tukar Format Fail PDF ke Ms Word menggunakan Google docs



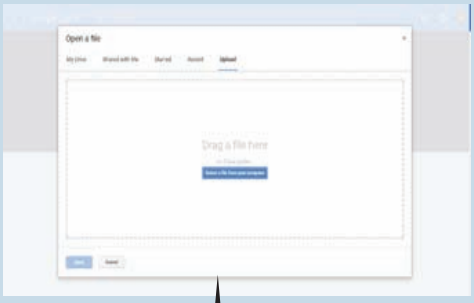
1. Log Masuk Akaun Google (https://www.google.com/docs



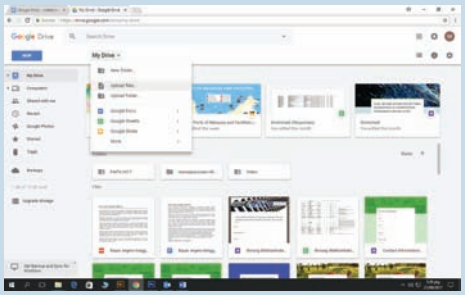
2. Klik MyDrive untuk Muat Naik Fail PDF



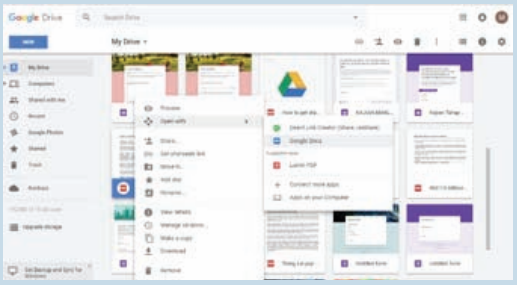
3. Muatnaik File PDF ke dalam MyDrive



4. Klik 'Download as' dan pilih 'Microsoft Word'.



3. Klik kanan pada fail yang telah dimuat naik pada Google Drive berkenaan dan anda pilih pada 'Open with' dan pergi ke 'Google Docs'.



Tahukah anda Had Nilai & Kelulusan Projek ICT

bagi Kementerian

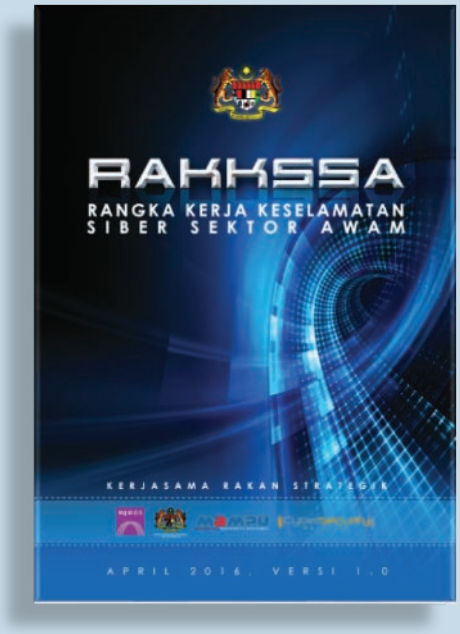
BIL	PROJEK			PERINGKAT KELULUSAN		
	KATEGORI PEROLEHAN PROJEK	SKOP PROJEK	NILAI PROJEK(RM) JUTA (J) RIBU (K)	KETUA SETIAUSAHA	JPICT KEMENTERIAN	JTISA
A	Projek Baharu	1. Pembangunan, naik taraf sistem aplikasi dan/atau integrasi.	< 50K	✓	-	-
			≥ 50K hingga < 1J	-	✓	-
			≥ 1J	-	✓	✓
		2. Perolehan perkakasan dan/atau perisian dan/atau rangkaian dan/atau perkhidmatan ICT.	< 500K	✓	-	-
			≥ 500K hingga <5J	-	✓	-
			≥ 5J	-	✓	✓
B	Peningkatan Sistem	1. Naik taraf sistem aplikasi dan/atau integrasi.	< 1J	-	✓	-
			≥ 1J	-	✓	✓
		2. Naik taraf perkakasan dan/atau perisian dan/atau rangkaian dan/atau perkhidmatan ICT.	< 500K	✓	-	-
			≥ 500K hingga <5J	-	✓	-
			≥ 5J	-	✓	✓
C	Pertambahan Peralatan	Perolehan perkakasan dan/atau perisian dan/atau rangkaian dan/atau perkhidmatan ICT.	< 500K	✓	-	-
			≥ 500K hingga <5J	-	✓	-
			≥ 5J	-	✓	✓
D	Peluasan Projek	1. Peluasan penggunaan sistem aplikasi.	< 1J	-	✓	-
			≥ 1J	-	✓	✓
		2. Perolehan perkakasan dan/atau perisian, dan/atau rangkaian dan/atau perkhidmatan ICT.	< 500K	✓	-	-
			≥ 500K hingga <5J	-	✓	-
			≥ 5J	-	✓	✓

Tahukah anda Had Nilai & Kelulusan Projek ICT

bagi Agensi dibawah MOT

BIL	PROJEK			PERINGKAT KELULUSAN		
	KATEGORI PEROLEHAN PROJEK	SKOP PROJEK	NILAI PROJEK(RM) JUTA (J) RIBU (K)	JPICT AGENSI	JPICT KEMENTERIAN/PEJABAT SUK NEGERI	JTISA
A	Projek Baharu	1. Pembangunan, naik taraf sistem aplikasi dan/atau integrasi.	< 50K	✓	-	-
			≥ 50K hingga < 1J	✓	✓	-
			≥ 1J	✓	✓	✓
		2. Perolehan perkakasan (pembelian dan sewaan), dan/atau perisian, dan/atau rangkaian dan/atau perkhidmatan ICT.	< 500K	✓	-	-
			≥ 500K hingga <5J	✓	✓	-
			≥ 5J	✓	✓	✓
B	Peningkatan Sistem	1. Naik taraf sistem aplikasi dan/atau integrasi.	< 1J	✓	✓	-
			≥ 1J	✓	✓	✓
		2. Naik taraf perkakasan (pembelian dan sewaan), dan/atau perisian, dan/atau rangkaian dan/atau perkhidmatan ICT.	< 500K	✓	-	-
			≥ 500K hingga <5J	✓	✓	-
			≥ 5J	✓	✓	✓
C	Pertambahan Peralatan	Perolehan perkakasan (pembelian dan sewaan), dan/atau perisian, dan/atau rangkaian dan/atau perkhidmatan ICT.	< 500K	✓	-	-
			≥ 500K hingga <5J	✓	✓	-
			≥ 5J	✓	✓	✓
D	Peluasan Projek	1. Peluasan penggunaan sistem aplikasi.	< 1J	✓	✓	-
			≥ 1J	✓	✓	✓
		2. Perolehan perkakasan (pembelian dan sewaan), dan/atau perisian, dan/atau rangkaian dan/atau perkhidmatan ICT.	< 500K	✓	-	-
			≥ 500K hingga <5J	✓	✓	-
			≥ 5J	✓	✓	✓

Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)



"**RAKKSSA** merangkumi kesemua komponen keselamatan yang perlu diambil kira untuk melindungi maklumat dalam ruang siber (sistem-sistem teknologi maklumat dan komunikasi, maklumat yang disimpan dalam sistem-sistem tersebut, manuasia yang berinteraksi dengan sistem-sistem ini secara fizikal atau maya, serta persekitaran fizikal sistem-sistem tersebut disimpan) di Kementerian/agensi."

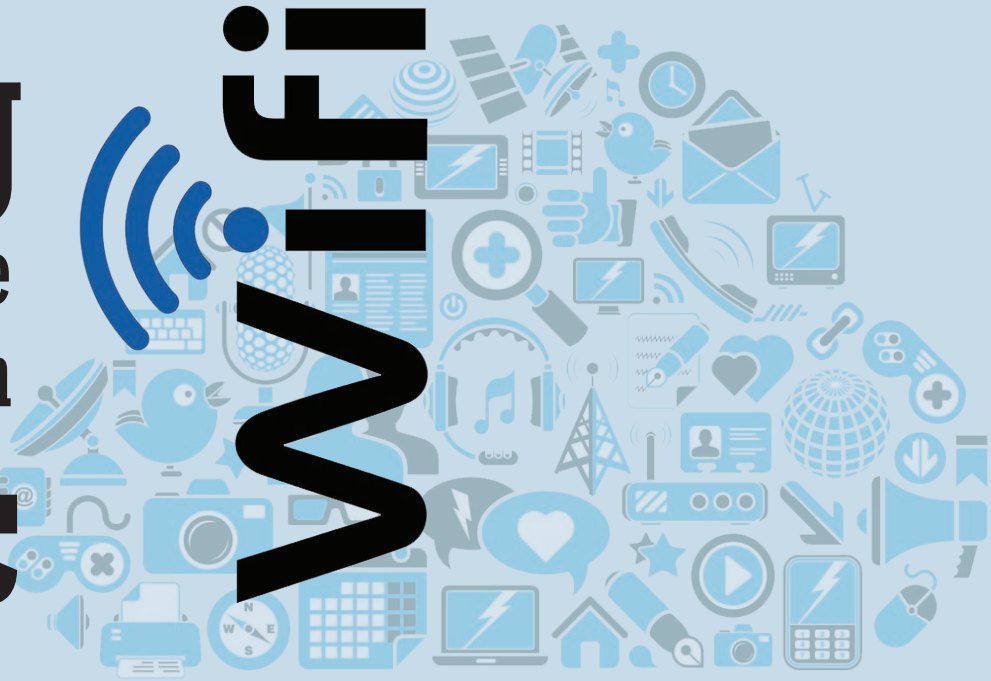
1. Memastikan hanya satu rangka kerja keselamatan siber yang menyeluruh
2. Menangani serangan dan pencerobohan siber semakin meningkat dan menggugat kestabilan dan kemakmuran negara.
3. Memastikan perlindungan yang bersesuaian dengan nilai dan sensitiviti aset
4. Menggantikan pekeliling dan arahan berkenaan keselamatan siber telah dikeluarkan sejak tahun 2000 dan secara berasingan serta mengandungi perincian yang menyukarkan perubahan untuk mengikut perkembangan teknologi.

Objektif RAKKSSA

Objektif RAKKSSA adalah untuk memberi panduan asas kepada agensi dalam merancang perlindungan yang diperlukan bagi ruang siber masing-masing dan memastikan keselamatan penyampaian perkhidmatan Sektor Awam serta meningkatkan tahap keyakinan pemegang taruh.

8 Komponen Utama RAKKSSA

Nothing is private when done in Public



Before Connecting

- Set Strong Passwords
- Enable Password Protected Screen Saver
- Encrypt File and Folders
- Secure Operating System (OS)
- Secure Browser
- Disable Network Discovery
- Turn Off File Sharing
- Install Security Software

When Connected

- Set Strong Passwords
- Use HTTPS
- Avoid Sensitive Transactions
- Avoid Leaving Device Unattended
- Get Paranoid. Practice healthy paranoia. Be alert of your surroundings in public areas as sensitive or private information on the screen of your device is exposed and vulnerable.

Before Disconnected

- Clear Cache
- Disconnect from public Wi-Fi
- Manage Wireless Network

Tip Online Shopping

- Secure your pc with firewall & antivirus software
- Shop only from reputable sites. Checks that it begins with https
- Monitor your credit & banking state-ments regulary
- Beware of " too good to be true" offers from social networks, emails and text message
- Never shop or bank on public wifi unless using vpn
- Make purchases with a credit card instead of a debit
- Use strong password to secure all your online accounts
- Think twice before you click