Pertemuan Tahunan IX ID-CERT

dan

ID-Malware Summit II

2017

PROPOSAL

Bandung, 13 April 2017

1. LATAR BELAKANG

Setiap tahun ID-CERT mengadakan Pertemuan Tahunan (Annual Gathering) untuk melaporkan kegiatan ID-CERT selama satu tahun sebelumnya, memaparkan rencana kerja tahun berjalan, melaporkan Incident Monitoring Report (IMR) tahun sebelumnya dan diskusi seputar tren IT. Untuk tahun 2017 ini tema Pertemuan Tahunan IX ID-CERT tahun 2017 adalah ***Securing Mobile Phone and Identity Theft,*** mengamankan perangkat seluler anda dan pencurian identitas. Karena maraknya kasus mengenai penyadapan pada *mobile phone* dan pencurian identitas di beberapa media sosial, maka diskusi pada Pertemuan Tahunan IX ini memfokuskan diri pada topik pengamanan *mobile phone* (penyadapan, non malware) dan pencurian identitas pada Twitter dan Google.

Bersamaan dengan Pertemuan Tahunan IX ini, ID-CERT juga menyelenggarakan ID-Malware Summit II dengan tema ***Smartphone Malware and Fileless Malware*** karena mengambil pokok bahasan mengenai *malware* pada *smartphone* dan *fileless malware*. *Smartphone* telah menjadi salah satu barang wajib bawa bagi sebagian besar orang. Pada tahun 2018, menurut TechInAsia dan emarketer.com, pengguna *smartphone* di Indonesia diperkirakan akan melampaui jumlah 100 juta. Dengan jumlah penduduk Indonesia sekitar 255 juta orang, jumlah pengguna *smartphone* tersebut sangatlah besar, hampir mencapai 2/3 dari jumlah total penduduk. Seiring dengan kegunaan dan kecanggihan perangkat tersebut, kesadaran untuk bersih dari virus atau *malware* masih sangat kurang.

Smartphone Malware

Menurut penelitian dari Ericcsson pada tahun 2020 akan ada 6 Milliar perangkat *smartphone*. Semakin banyak pengguna yang menggunakan *smartphone* tidak hanya untuk membaca berita tapi juga untuk melakukan transaksi *ecommerce* dan *online banking*. Sementara itu jumlah *smartphone malware* juga mengalami peningkatan. Pada tahun 2015 saja, Kaspersky menemukan 884.774 sampel *mobile malware* baru dan 7.030 sampel trojan *mobile banking* baru. Selain itu terjadi juga peningkatan kasus *mobile Ransomware*. Menurut International Data Group, 74% kasus keamanan yang dilaporkan perusahaan pada tahun 2015 adalah kasus Ransomware. Kemudian ada juga ancaman *mobile spyware*, *MMS malware*, *Mobile Adware*, dan SMS Trojan. Untuk itu pada pertemuan ini ID-CERT mengundang para pakar keamanan

untuk memaparkan bagaimana sebenarnya perkembangan terkini ancaman *malware* pada *smartphone* ini.

Fileless Malware

Fileless malware adalah *coding* berbahaya yang hanya ada di memori dan tidak terinstal pada harddisk komputer target. *Fileless malware* ditulis langsung ke RAM. *Code*-nya diinjeksikan ke beberapa proses yang sedang berjalan, seperti iexplore.exe atau javaw.exe, yang kemudian digunakan untuk mengeksploitasi perangkat tersebut. Pengguna biasanya terkena *fileless malware* karena mengunjungi situs web yang berbahaya, yang sengaja diarahkan setelah mengklik iklan penyerang (*malvertisement*). Karena *malware* tersebut bukan berupa file, sehingga seringkali dapat menghindari sistem pencegahan intrusi dan program antivirus.

Februari 2017, Kaspersky melaporkan 140 perusahaan di 40 negara mengalami serangan *Fileless Malware*. Serangan ini menyerang sektor perbankan, pemerintahan dan industri Telekomunikasi di Amerika Serikat, Prancis, Ekuador, Kenya, Inggris, dan Russia. Serangan *Fileless Malware* ini sangat sulit dideteksi karena tidak meninggalkan sampel *malware* di harddisk korban. Semua aktivitas *malware* dijalankan dalam memori (RAM). Pada pertemuan ini akan dibahas tentang ancaman *fileless malware* ini, bagaimana serangan *fileless malware* ini dijalankan dan bagaimana cara pencegahan yang dapat dilakukan.

2. TUJUAN

Tujuan menyelenggarakan Pertemuan Tahunan IX ini adalah:

- Incident Monitoring Report (IMR) 2016.
- Melaporkan kegiatan ID-CERT selama tahun 2016.
- Memaparkan rencana kerja ID-CERT untuk tahun 2017.
- Penjelasan *membership* di ID-CERT.
- Diskusi dengan topik Membership ID-CERT, *mobile phone security* (penyadapan, non malware), pencurian identitas pada Twitter dan Google.

Tujuan menyelenggarakan ID-Malware Summit II ini adalah:

- Meningkatkan *malware awareness* kepada pengguna *smartphone*
- Membahas smartphone malware
- Membahas fileless malware
- Cara mencegah malware

3. WAKTU DAN TEMPAT PELAKSANAAN

Hari : Kamis

Tanggal : 13 April 2017

Waktu : 08.00 – 17.00

Tempat : Telkom Bandung

4. SASARAN KEGIATAN DAN ESTIMASI PESERTA

Pertemuan Tahunan IX ID-CERT untuk level ***Intermediate*** dan ID-Malware Summit II tahun 2017 ini diselenggarakan untuk level ***Advance***. Adapun sasaran kegiatan ini adalah dari kalangan:

1. Konstituen dan Responden ID-CERT
2. Peneliti dan akademisi Malware
3. Komunitas penggiat malware
4. Industri Anti Virus
5. Komunitas IT
6. Divisi IT dari Pemerintah/POLRI/TNI/Kominfo dan swasta

Estimasi jumlah peserta:

1. Konstituen dan Responden ID-CERT	15 orang
2. Peneliti dan akademisi Malware	10 orang
3. Komunitas penggiat malware	10 orang
4. Industri Anti Virus	10 orang
5. Komunitas IT	15 orang
6. Perusahaan & Perbankan	10 orang
7. Pemerintah/Polri/TNI/Kominfo	10 orang
8. Umum/lainnya	20 orang
Jumlah peserta	**100 orang**

5. DRAFT AGENDA ACARA

DRAFT AGENDA ACARA			
Jam	Durasi (menit)	Acara	Pembicara
08.00 - 08.30	30	Registrasi ulang Gathering	Panitia
08.30		**Pembukaan Gathering**	
08.30 - 08.45	15	Pembukaan Acara dan Sejarah ID-CERT	Budi Rahardjo, PhD.
08.45 - 09.00	15	Sambutan Kominfo	Kominfo
09.00 - 09.30	30	Laporan kegiatan ID-CERT termasuk IMR, Rencana kerja 2017, Membership	Ahmad Alkazimy
09.30 - 09.50	20	Teknologi Anti DdoS	CBN
09.50 - 10.00	10	Diskusi dan tanya jawab	CBN
10.00 - 10.15	**15**	**Morning Coffee Break**	
10.15		*Diskusi Panel Sesi 1:*	
		Identity Theft (Google, Twitter)	
10.15 - 10.45	30	Identity Theft - Google (dalam konfirmasi)	Google
10.45 - 11.15	30	Identity Theft - Twitter (dalam konfirmasi)	Twitter
11.15 - 11.45	30	Diskusi dan tanya jawab	
11.45 - 12.00	15	Penutupan dan Photo bersama	Ahmad Alkazimy, panitia, peserta
11.00 - 12.00	60	Regitrasi ulang ID-Malware Summit	Panitia
12.00 - 13.00	**60**	**ISOMA**	
13.00		**Pembukaan ID-Malware Summit II**	
13.00 - 13.30	30	Pembukaan Acara dan Summary ID-Malware Summit II	Ahmad Alkazimy
13.30 - 13.45	15	Sambutan Kominfo (dalam konfirmasi)	Kominfo
13.45		*Diskusi Panel Sesi 2:*	
		Mobile Phone Security	
13.45 - 14.15	30	Presentasi 1	
14.15 - 14.45	30	Presentasi 2	
14.45 - 15.15	30	Diskusi dan tanya jawab	
15.15 - 15.30	**15**	**Afternoon Coffee Break + Sholat Ashar**	
15.30		*Diskusi Panel Sesi 3:*	
		Fileless Malware	
15.30 - 16.00	30	Presentasi	
16.00 - 16.15	15	Diskusi dan tanya jawab	
16.15 - 16.30	15	Summary ID-Malware Summit II	Ahmad Alkazimy
16.30 - 16.45	15	Penutupan dan Photo bersama	Ahmad Alkazimy
16.45 - 17.00	15	Pembagian Sertifikat ID-Malware Summit II	Panitia

Presentasi berisi penjelasan teknis mengenai *smartphone malware* dan *fileless malware* sesuai topik, dan bukan berisi jualan produk.

6. KEPANITIAAN

Panitia pelaksana:

- Ahmad Alkazimy
- Setia Juli Irzal Ismail
- Wayan Achadiana
- Rahmadian L. Arbianita
- Oryzandi + tim

Penasehat:

- Budi Rahardjo, PhD.
- Andika Triwidada

7. ANGGARAN BIAYA

Anggaran biayanya sebagai berikut:

Anggaran Biaya ID-CERT Gathering IX dan ID-Malware Summit II

No.	Rincian	Jumlah	Unit	@	Jumlah Anggaran (Rp)
Paket A					
1	Sewa tempat acara, coffee break pagi-sore, dan makan siang	130	orang	350.000	45.500.000
2	Live streaming (device+bandwidth+operator)	1	Hari	2.000.000	2.000.000
3	Sewa infocus	1	Hari	1.000.000	1.000.000
4	Kaos panitia, pembicara, peserta Summit	100	buah	70.000	7.000.000
5	Tas goodybag Summit	100	buah	5.000	500.000
6	Notes Summit	100	buah	5.000	500.000
7	Bolpen/pensil Summit	100	buah	3.500	350.000
					56.850.000
Sponsor Paket A mendapatkan pemasangan LOGO pada:					
	Spanduk (backdrop), standing banner, kaos, web, video, sertifikat, name tag				
	Logo ukuran **besar** sejajar dengan logo ID-CERT				
Paket B					
8	Honor pembicara	7	orang	1.500.000	10.500.000
9	Akomodasi pembicara	7	orang	400.000	2.800.000
10	Transportasi pembicara	7	orang	500.000	3.500.000
11	Honor penasehat	2	orang	1.000.000	2.000.000
12	Transportasi penasehat	2	orang	200.000	400.000
13	Honor panitia	5	orang	500.000	2.500.000
14	Transportasi panitia luar kota	3	orang	350.000	1.050.000
15	Transportasi panitia dalam kota	2	orang	150.000	300.000
					23.050.000

Sponsor Paket B mendapatkan pemasangan LOGO pada:					
	Spanduk (backdrop), standing banner, kaos, web, video, sertifikat, name tag				
	Logo ukuran **sedang**, posisi di bawah logo ID-CERT dan sponsor paket A				
Paket C					
16	Sertifikat pembicara + peserta Summit	100	buah	5.000	500.000
17	Goodybag untuk pembicara (tas + souvenir)	7	buah	150.000	1.050.000
18	Spanduk (backdrop)	1	buah	300.000	300.000
19	Standing banner	2	buah	150.000	300.000
20	Dokumentasi photo + video	3	orang	750.000	2.250.000
21	Sewa video + tripod	1	hari	300.000	300.000
22	Map untuk sertifikat Summit	100	buah	2.000	200.000
23	Gantungan kunci/pin	100	buah	5.000	500.000
24	Stiker	100	buah	2.000	200.000
25	ATK (sewa printer, tinta, HVS, spidol, dll)	1	set	2.000.000	2.000.000
26	Name tag panitia, pembicara, peserta Summit	100	buah	5.000	500.000
					8.100.000
Sponsor Paket C mendapatkan pemasangan LOGO pada:					
	Spanduk (backdrop), standing banner, kaos, web, video, sertifikat, name tag				
	Logo ukuran **kecil**, posisi di bawah logo ID-CERT dan sponsor paket A + B				

8. HUBUNGI KAMI

Website : www.cert.id

Email : cert@cert.or.id

idcert@cert.or.id

Kontak Utama : +62-889-1400-700 (HelpDesk)

Alamat : Griya Bukit Mas II Blok D3 No. 22

Bojong Koneng, Bandung, Indonesia 40191

9. PENUTUP

Demikian proposal ini kami sampaikan, dengan harapan dapat dijadikan pertimbangan bagi pihak-pihak untuk ikut berpartisipasi dalam kegiatan **Pertemuan Tahunan IX ID-CERT dan ID-Malware Summit II 2017**.

Ketua Panitia,

Ahmad Alkazimy

ID-CERT,

Budi Rahardjo, PhD

Referensi:

https://id.techinasia.com/jumlah-pengguna-smartphone-di-indonesia-2018
https://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694
https://usa.kaspersky.com/internet-security-center/threats/mobile-malware
https://www.sophos.com/en-us/security-news-trends/security-trends/malware-goes-mobile.aspx
http://whatis.techtarget.com/definition/fileless-infection-fileless-malware
http://thehackernews.com/2017/02/fileless-malware-bank.html
https://arstechnica.com/security/2017/02/a-rash-of-invisible-fileless-malware-is-infecting-banks-around-the-globe/
http://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-17-security-predictions-for-2017.html