Lab Malware Report

Setia Juli Irzal Ismail

www.cert.or.id

Lab Malware

- 2014
- Relawan

. Aries Syamsuddin - Pemda Blitar
. Abdul Rahim - Pemkot Cirebon
. Arya Dhanang - ITB
. Anggi Elanda - STMIK Rosma Karawang
. Samuel Cahyawijaya - ITB
. Hadi Rasyid Rono - ITB
. Lastono - ITB
. David Setiadi - STMIK Sumedang

Aktivitas

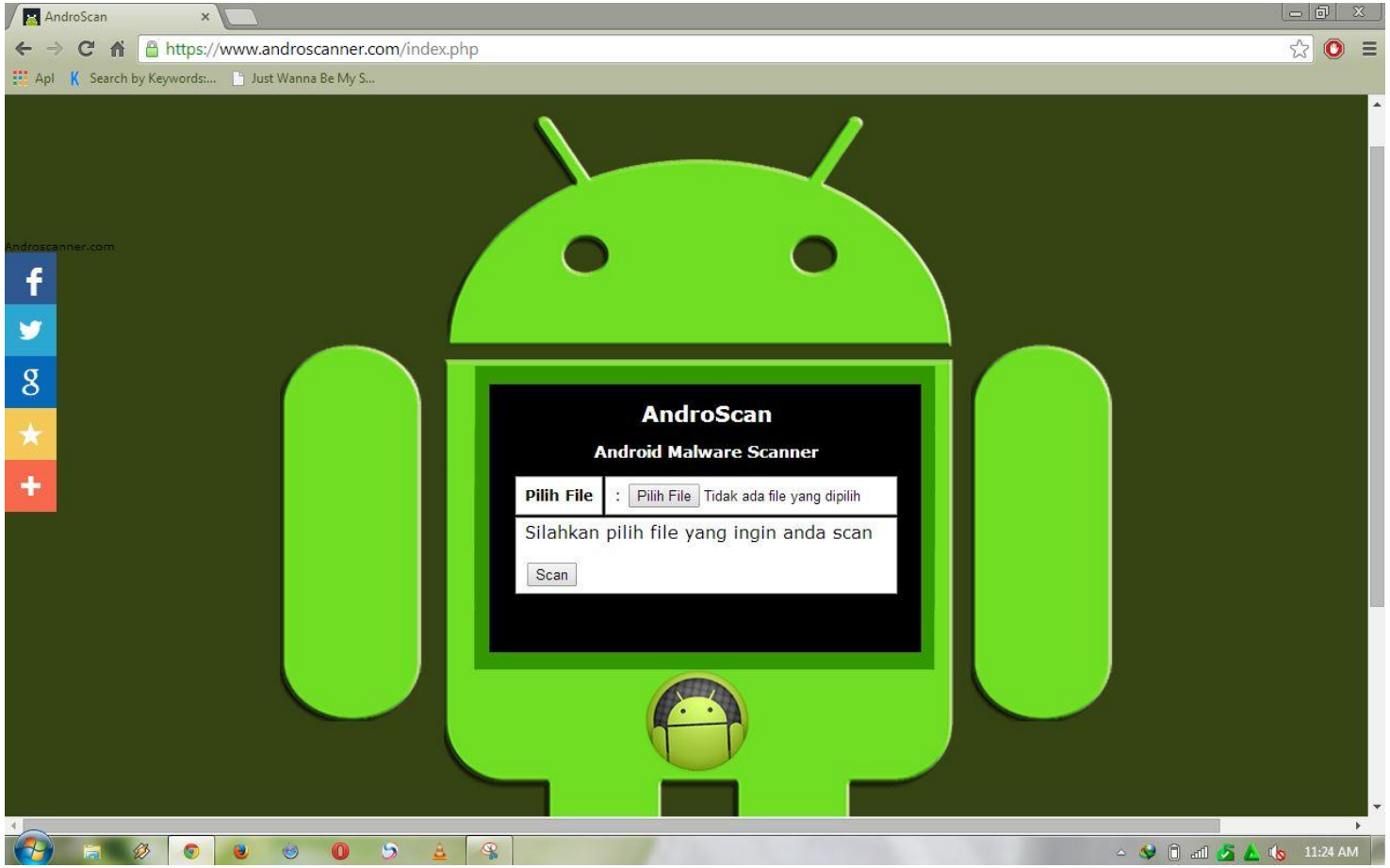
- Survey Malware
- Androscanner
- Malware Wiki
- Malware Advisory
- Malware Summit
- AP-CERT drill
- Training & Sosialisasi

Survey Malware

- Data trend malware di Indonesia
- Flash disk
- Engine Parser
- 24 kota 9 propinsi
- 379 jenis malware

- www.cert.or.id/media/files/survey_malware_report.pdf

Androscanner



- Malware Scanner
- Android
- APK

id.cert

Malware Wiki

Malware Advisory

- Peringatan kerentanan
- Malware
- Berkala
- Analisa malware

Malware Summit I

- Indonesia Darurat Malware - 5 Mei 2015
- AV Lokal; Smadav, PcMedia AV, Indosky, Infaltech, Spensav, vaksin,
- Komunitas: Serverhack, ACAD-CSIRT, Datacomm
- Gov: Kominfo
- Industri: TrendMicro


INDONESIA MALWARE SUMMIT 2015


MALWARE DAN
GAN AV LOKAL

Rangkuman Hasil Diskusi ID-Malware Summit I

1. Saat ini di Indonesia telah terdapat beberapa perusahaan antivirus lokal, diantaranya SmadAV, PCMAV, SpensAV, Indosky, InpagAV, RRAV dll.
2. Bagi pengguna Antivirus lokal saat ini hanya menjadi second-layer protection, sebagai pendamping anti virus dari luar.
3. Permasalahan utama adalah keterbatasan Resource baik SDM maupun perangkat.
4. Seringkali Antivirus lokal tidak kompatibel dengan beberapa antivirus luar

Usulan Malware Summit I

- Perlu adanya forum dan pertemuan rutin para developer antivirus lokal.
- Terkait kurangnya SDM di bidang analisa malware, perlu adanya kerjasama dengan lembaga pendidikan.
- Tentang kendala perangkat diharapkan ada pihak yang bisa membantu perkembangan anti virus lokal.
- Adanya usulan pembuatan sebuah layanan malware scanner seperti virustotal dimana pengguna dapat melakukan scanning sampel malware dengan semua antivirus lokal.
- Adanya usulan fitur whitelist pada antivirus

Malware Summit II

- 13 April 2017
- Research Sharing
- Dracos - **Automatic Malware analysis** dan repository
- Honeynet - DGA Malware
- M. Ali Syarief - Smartphone Malware
- ID-CERT : Fileless Malware

To-do list

- Virus Total Indonesia masih menjadi tugas berikutnya
  - Infrastruktur untuk keperluan Malware Sharing
- Mendukung keberadaan AV lokal
- Peneliti: mengumpulkan dan mencarikan topik riset dibidang Malware.
- Wadah untuk Peneliti Malware dalam bentuk Telegram grup

Kontak

- jul@tass.telkomuniversity.ac.id
- Tw: @jul_ismail
- FB: jul.ismail
- julismail.staff.telkomuniversity.ac.id/

Malware Outlook 2018

Tren Malware 2017

- Ransomware
- Teknik Pengelabuan
- Mac & Android
- Botnet Malware

Ransomware

- 2017 tahunnya Ransomware
- 400 varian
- Wannacry - Mei
- ExPetr - Juli
- BadRabbit - Oktober

Wannacry

- Eternal Blue exploit → SMB
- Double Pulsar Backdoor
- Rumah sakit
- Hampir 1 juta korban
- Lazarus?
- Mei
- Maret : microsoft patch

ExPetr

- Ukraina, Russia
- 5000 korban
- Eternal Blue exploit
- DoublePulsar backdoor
- MeDoc – Update
- Website Berita di Ukraina
- 2 level enkripsi : file korban dan MFT
- BlackEnergy's KillDisk?
- Juli

Ransomware 2018?

- Ransomware as a Service
- Malware kits : utk membuat ransomware sendiri
- Darkweb
- Cerber, Satan, Philadelphia
- Ransomware Android, Mac, Linux
- Bitcoin → Monero (Kirk)
- Target: Sektor Kesehatan, Pemerintahan, Infrastruktur Penting, Pendidikan, SME

Pengelabuan

- Anti security : AV, Firewall
- Anti sandbox : sandbox
- Anti analyst : packer, obfuscation, RE
- Machine learning evasion
- Hardware based evasion

Timeline

- 1980: Encryption: cascade virus
- 1990: Polymorphic: Chameleon (encrypt,junk)
- 1998: Metamorphism (instruction diacak)
- 1999: Packer
- 1999: Rootkit:
- 2008: DGA: conficker worm
- 2011: Darknet Market: Silkroad
- 2015: Firmware : Equation Group, Hacking Team: IoT
- 2015: Dridex: obfuscation: powershell, sandbox evasion
- 2016: Fileless Malware
- 2017: Machine learning detection: Cerber

Darknet Market

- Cryptservice: $53 - FUD
- Lazercrypter: free packer
- Macro Exploit Crypt Service: Macro utk nyebarin malware $53
- Crypter Source Code: $1,99
- Arctic Miner:cryptocurrency Miner: $3,2
- Betacrypt: Code mutation: $239
- BHGroup: crypter ASM & C: $35
- Tutorial FUD backdoor: $0,94

Stegano Malware

- Steganography?
- 2011 Duqu: mengumpulkan informasi dr korban
- Enkrip data-> Embed File-> server CnC
- 2014: ZeusVM (Varian): image stegano, menyembunyikan command
- 2016: Lurk: Encryped Url->BMP file->unduh payload
- 2016: Stegoloader

Sundown Exploit Kit-case

1. User browsing: website yg dihack atau malware ads
2. Redirected ke exploit server
3. Unduh gambar (PNG) -> Gambar kosong
4. Encoded exploit → URL utk unduh payload
5. Exploit celah keamanan pada IE

Stegano Malware - 2

- Cerber: Macro pada word→drop .vbs → unduh jpg
- Vawtrak: unduh favicon.ico
- Magento case: malware mengirim info payment card dg image stegano
- Network stegano: menyembunyikan trafik ke CnC server pada trafik DNS atau Http Request → teslacrypt

Android

- 2017: 10 juta sampel malware android
- Rootnik
- Dloadr-ECZ
- Axent-ED

King of Glory

- Game di Cina
- Palsu – Ransomware
- Lock screen & Crypto ransom
- Lock Screen
- Judy: 36 juta korban
- Xavir: 800 android apps
- WireX botnet: 140000 korban: Ddos

Ghostclicker

- 300 aplikasi
- Nyamar jadi google play service library
- Facebook ads library
- adware

Mac Malware

- PUA
- Optimizer: MacKeeper, Advanced Mac Cleaner , TuneUpMyMac, dll
- MacRansom
- MacSpy.

Microsoft - Malware

- Office
- Powershell
- Zero Day Vulnerability

Botnet

- Botnet?
- IoT : Ip camera
- Mirai Botnet → Tsunami Ddos

Trend Lainnya

- Distribusi Software: CC-Cleaner, ExPetr
- UEFI & BIOS attacks: hacking team
- Wiper: Shamoon → aramco

- Sosmed: fake akun & bot → hoax
- Router & Modem hack

thank you
рахмат
danke
謝謝
ngiyabonga
teşekkür ederim
Баярлалаа
mersi
kia ora
barka
welalin
tack
spas
mahalo
tapadh leat
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
gracias
kiitos
dankie
nanni
nandri
dhanyavad
mauruuru
köszönöm
akun
dankon
aciu
хвала
asante
manana
obrigada
tenki
bedankt
bayarlalaa
gràcie
hvala
enkosi
dziękuję
djiere dieuf
tau
mochchakkeram
murakoze
дякую
mamnun
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
chokrane
sobodi
dėkuji
sagolun
sukriya
kop khun krap
taiku
arigatô
takk
dakujem
trugarez
obrigado
mèsi
didi madloba
ありがとう
najis tuke
tanemirt
grazie
terima kasih
rahmet
ευχαριστώ
diolch
dhanyavadagalu
shukriya
mercê
мерси
kam sah hamnida
rahmat
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci