Tren Malware dan Teknologi Deteksi

ANGGI ELANDA

ServerHack Organization

NCSD (National Cyber Security Defence) Indonesia

Cyber Techno Media

Indonesia Malware Summit

Selasa, 5 Mei 2015

Bandung

Profile

Nama : Anggi Elanda
TTL : Karawang, 25 Maret 1992

Riwayat Pendidikan :

- 2010, S1 Teknik Informatika, STMIK Rosma Karawang

Pekerjaan :

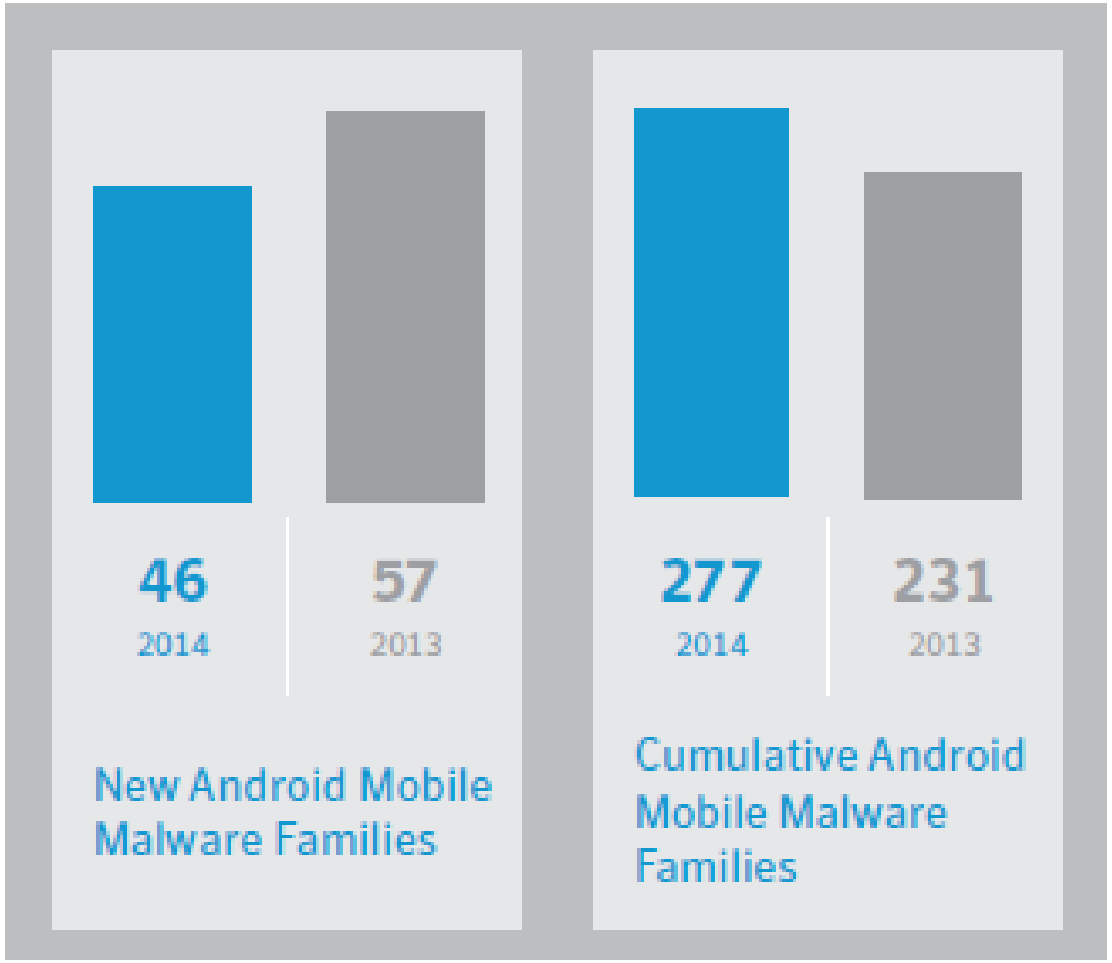
- Staff IT, STMIK Rosma Karawang, 2013 – Sekarang
- Konsultan IT, Pemda Karawang, 2011 – Sekarang

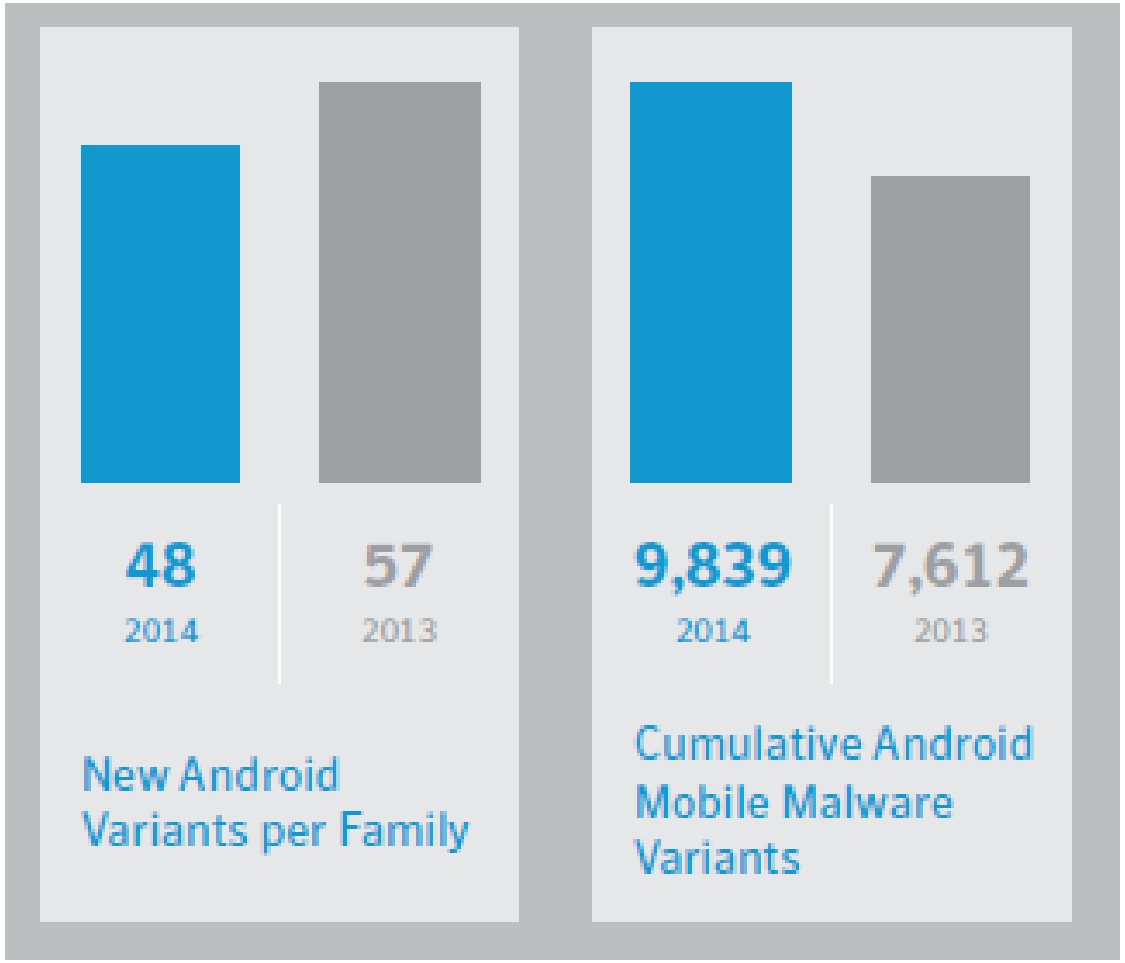
Organisasi :

- ServerHack Organization, 2010 – Sekarang
- NCSD (National Cyber Security Defence) Indonesia, 2014 – Sekarang.
- Cyber Techno Media, 2014 – Sekarang.
- Voluntir Malware, ID-CERT, 2014 – Sekarang.

id.cert

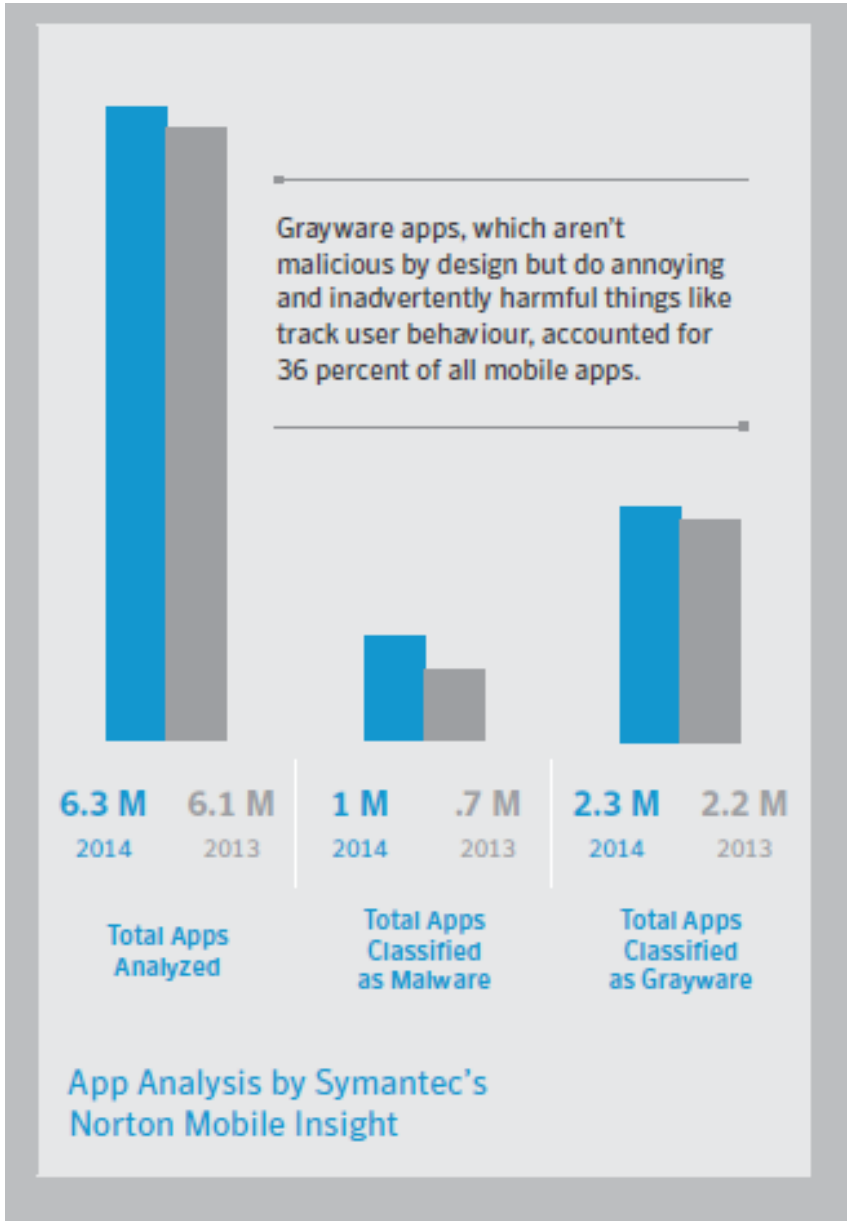
Tren Malware di Dunia

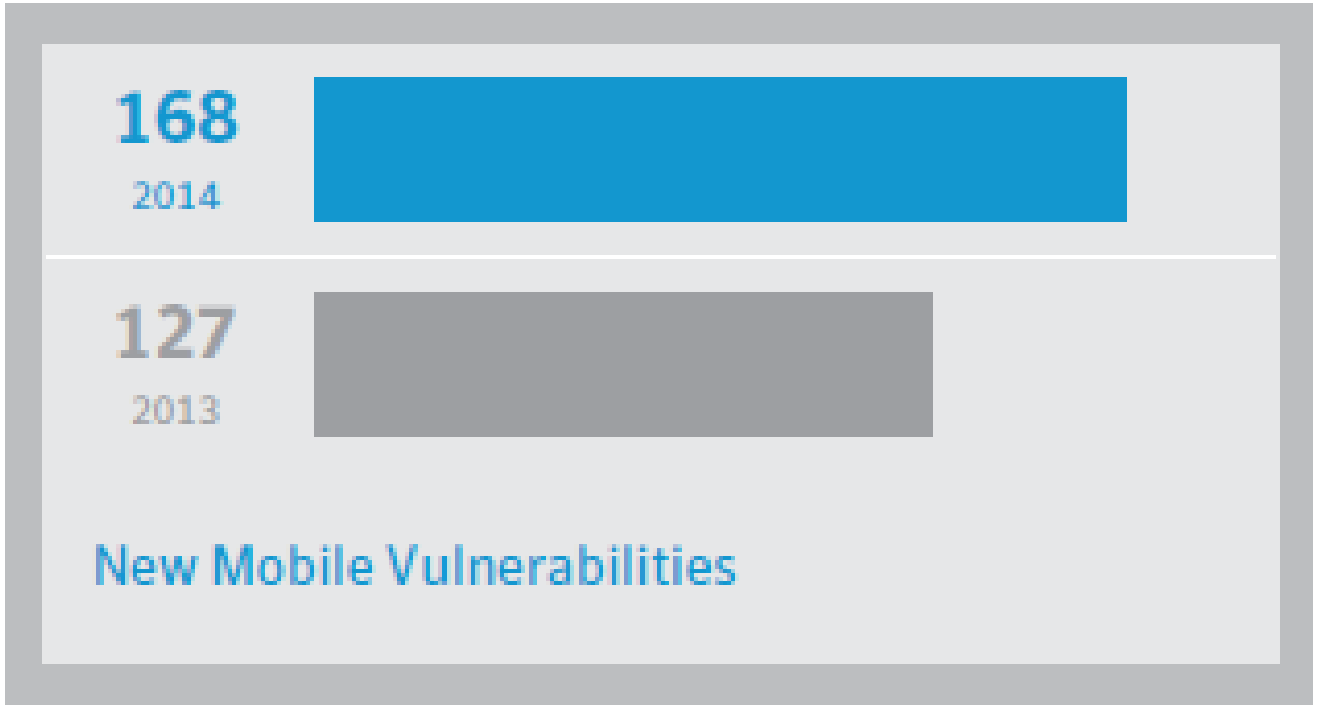




Sumber : http://www.symantec.com/security_response/publications/threatreport.jsp

id.cert





Sumber : http://www.symantec.com/security_response/publications/threatreport.jsp

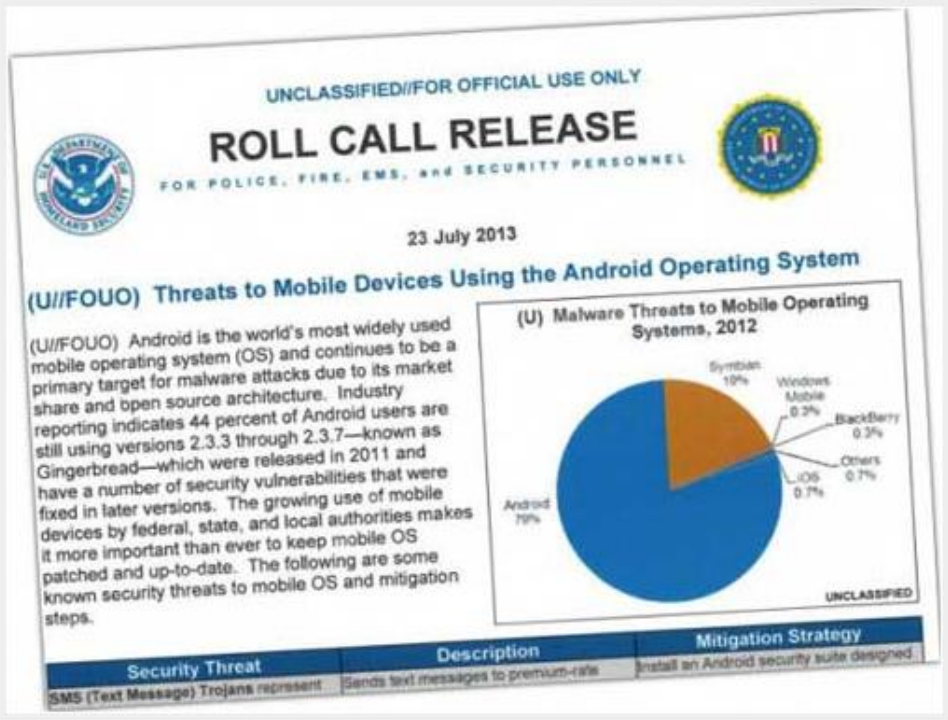
Android menjadi target utama serangan malware dengan total 79%

By Nico

Pemerintah Amerika menyebutkan bahwa Android menjadi mobile OS dengan serangan Malware terbanyak.

Institusi pemerintah Amerika Serikat yaitu Departemen keamanan dalam negeri dan Departemen Kehakiman diketahui telah merilis sebuah memo bersama yang isinya mengingatkan para institusi pemerintah Amerika mengenai ancaman bahaya Malware di ranah mobile.

Memo tersebut menyebutkan bahwa ancaman malware paling besar selama tahun 2012 ditargetkan untuk device ber-OS Android yaitu sebesar 79% dan Symbian OS sebesar 19%, sementara platform mobile lain seperti BlackBerry, iOS, Windows Phone hanya kurang dari 1%.



UNCLASSIFIED//FOR OFFICIAL USE ONLY

ROLL CALL RELEASE

FOR POLICE, FIRE, EMS, and SECURITY PERSONNEL

23 July 2013

(U//FOUO) Threats to Mobile Devices Using the Android Operating System

(U//FOUO) Android is the world's most widely used mobile operating system (OS) and continues to be a primary target for malware attacks due to its market share and open source architecture. Industry reporting indicates 44 percent of Android users are still using versions 2.3.3 through 2.3.7—known as Gingerbread—which were released in 2011 and have a number of security vulnerabilities that were fixed in later versions. The growing use of mobile devices by federal, state, and local authorities makes it more important than ever to keep mobile OS patched and up-to-date. The following are some known security threats to mobile OS and mitigation steps.

(U) Malware Threats to Mobile Operating Systems, 2012

UNCLASSIFIED

Security Threat	Description	Mitigation Strategy
SMS (Text Message) Trojans represent	Sends text messages to premium-rate	Install an Android security suite designed

Disebutkan 3 resiko serangan malware paling umum ke Android yaitu trojan SMS yang mengirimkan pesan teks ke nomor premium, rootkits, dan pemalsuan domain Google Play. Memo tersebut juga menyarankan agar lembaga pemerintah yang menggunakan Android untuk menginstall applikasi software pengamanan, menginstall applikasi *Carrier IQ test* dan melakukan update OS.

Sebenarnya banyaknya jumlah serangan Malware ke Android adalah hal yang wajar dikarenakan OS Android memang paling banyak dipakai didunia. Selain itu, sifatnya yang *opensource* memudahkan setiap orang menganalisa kelemahan yang ada. Dimana hal ini makin diperparah dengan banyaknya device Android yang masih menggunakan OS versi lama.

Sumber : http://www.infoteknologi.com/berita/android-target-utama-serangan-malware/

id.cert

Tren Malware di Indonesia

KOMPAS.com Register Login

Internet >

"Malware" Pencuri Uang Beredar di Indonesia, Bagaimana Menangkalnya?

Penulis: Fabian Januarius Kuwado | Selasa, 14 April 2015 | 13.25 WIB

Share: A+ A-

Ilustrasi malware

TERBARU

Gadget

Senin, 27 April 2015 15.01 WIB

Oppo R7 Meluncur 20 Mei?

Software

Senin, 27 April 2015 14.29 WIB

Google dan Facebook Lacak Korban Gempa Nepal

Gadget

Senin, 27 April 2015 13.51 WIB

Alasan Acer Tidak Latah Bikin Jam Tangan Pintar

Internet

Senin, 27 April 2015 13.08 WIB

Video Terjangan Longsor Everest Beredar di YouTube

e-Business

Senin, 27 April 2015 12.26 WIB

Petinggi Google Jadi Korban Gempa Nepal

Sumber : http://tekno.kompas.com/read/2015/04/14/13250037/.Malware.Pencuri.Uang.Beredar.di.Indonesia.Bagaimana.Menangkalnya.

id.cert

26 Maret 2015

Mendeteksi dan Membasmi Superfish

Malware Superfish yang terinstal dari pabrik pada produk Lenovo membuka celah keamanan berbahaya bagi penggunanya dan malware ini juga ditemukan pada produk Lenovo yang dipasarkan di Indonesia, khususnya produk konsumer yang mendapatkan software preinstal. Sebagai catatan, jika anda membeli produk Lenovo yang tidak mengandung preinstal Windows, artinya anda tidak mendapatkan preinstal Superfish tersebut dan tidak perlu khawatir atas Superfish. Namun jika komputer konsumer Lenovo yang anda beli mengandung OS original preinstal Windows dengan tipe seperti di bawah ini, kemungkinan besar komputer anda mengandung Superfish.

- G Series: G410, G510, G710, G40-70, G50-70, G40-30, G50-30, G40-45, G50-45
- U Series: U330P, U430P, U330Touch, U430Touch, U530Touch
- Y Series: Y430P, Y40-70, Y50-70
- Z Series: Z40-75, Z50-75, Z40-70, Z50-70
- S Series: S310, S410, S40-70, S415, S415Touch, S20-30, S20-30Touch
- Flex Series: Flex2 14D, Flex2 15D, Flex2 14, Flex2 15, Flex2 14(BTM), Flex2 15(BTM), Flex 10
- MIIX Series: MIIX2-8, MIIX2-10, MIIX2-11
- YOGA Series: YOGA2Pro-13, YOGA2-13, YOGA2-11BTM, YOGA2-11HSW
- E Series: E10-30

Salah satu bahaya yang ditimbulkan oleh Supersifh adalah aksinya menggantikan sertifikat pengamanan enkripsi komputer dengan sertifikat tunggal, ibaratnya tadinya setiap komputer mengakses HTTPS pada situs yang berbeda-beda akan secara otomatis menggunakan kredensial yang berbeda, Superfish menggantikan kredensial yang berbeda-beda itu dengan hanya satu kredensial. Hal ini sama saja dengan menciptakan “master key” yang bisa digunakan untuk memecahkan enkripsi yang tadinya aman menjadi tidak aman. Sebagai gambaran, jika anda memiliki master key, anda bisa membuka semua kunci pada pintu di rumah anda hanya menggunakan satu kunci master. Jika tidak percaya dan ingin mengetahui caranya, silahkan ditanyakan caranya pada Kenari Jaya karena begitulah kata iklannya :p.

Mendeteksi Superfish

Jika anda ragu-ragu atau kesulitan menentukan tipe Lenovo yang anda beli, ada satu tools yang bisa membantu untuk mendeteksi Superfish. Kabar baiknya, bukan hanya Superfish yang bisa di deteksi tetapi termasuk Komodia dan Privdog.
Sebagai catatan, **Komodia** bisa dikatakan sebagai Mbahnya Superfish karena komponen Komodia inilah yang digunakan oleh Superfish dan ada lebih dari 100 pengembang software dan adware sejenis dengan kemampuan mirip seperti Superfish mengancam pengguna komputer. Komodia menjual jasa untuk intersep jaringan, pengalih dan pemecah pengamanan SSL dan banyak digunakan oleh SDK pembuat Adware. Salah satu produsen yang menggunakan Komodia dalam produknya adalah Lavasoft.

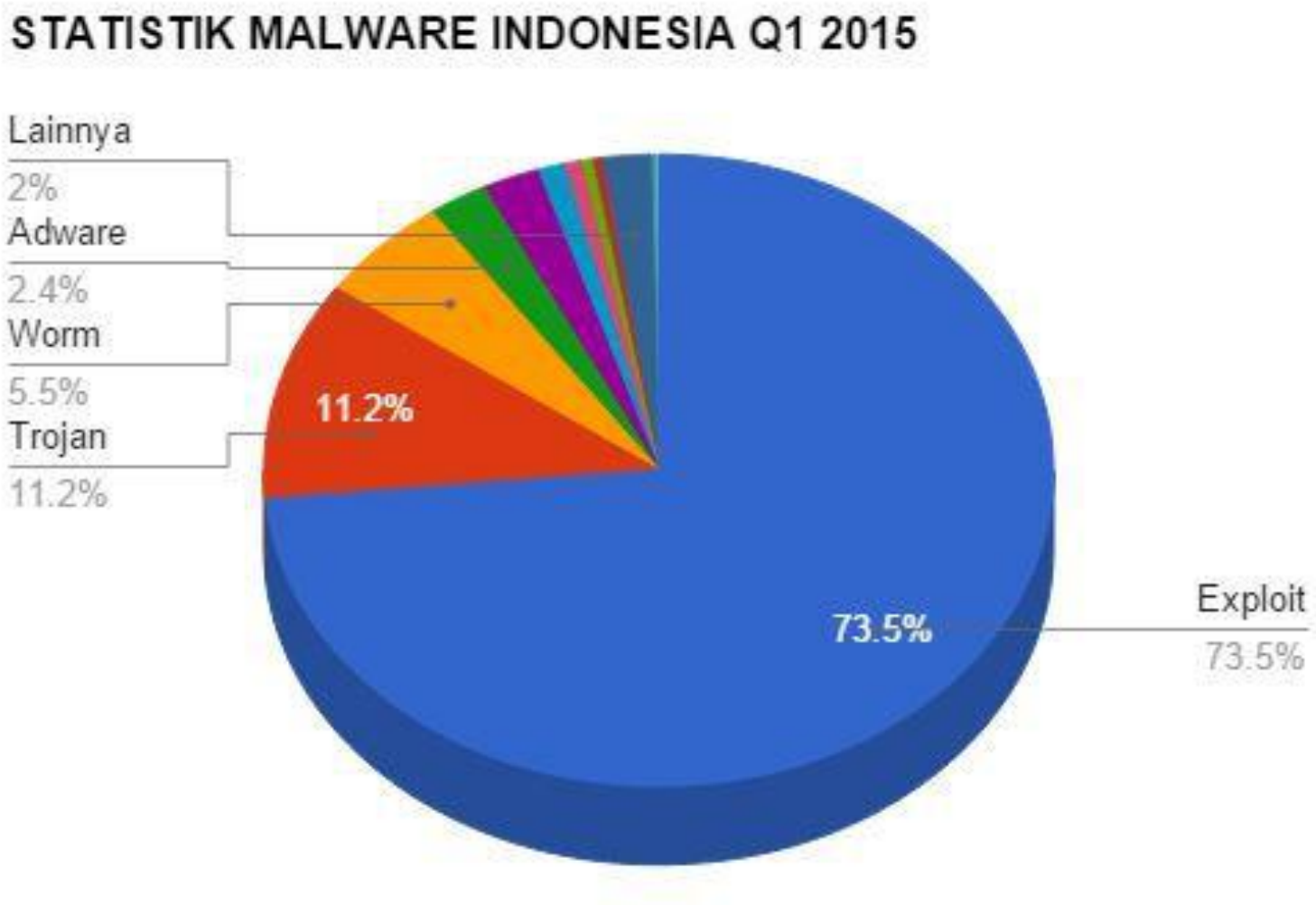
Privdog adalah produk yang dikeluarkan oleh vendor sekuriti Comodo pembuat Comodo Antivirus yang memberikan antivirus secara gratis.
Sebagai catatan, mayoritas vendor antivirus yang memberikan produknya secara gratis hampir dapat dipastikan memiliki metode untuk mendapatkan keuntungan dari para pengguna antivirusnya seperti menginstalkan toolbar atau addons yang bertujuan untuk monetisasi

Sumber : http://www.vaksin.com/0315-detect-superfish

Cek Malware Superfish

- https://filippo.io/Badfish/
- Microsoft Windows Malicious Software Removal Tools
- http://support.lenovo.com/us/en/product_security/superfish_uninstall

Statistik Malware di Indonesia



Sumber : http://www.vaksin.com/0415-statistik-malwareq1

id.cert

Statistik Malware Indonesia Q1 2015

Kuartal pertama 2015, penyebaran malware di Indonesia di dominasi oleh malware yang melakukan eksploitasi atas celah keamanan sebanyak 73,5 % , diikuti oleh trojan 11,2 % dimana salah satunya adalah trojan yang melakukan penyerangan atas situs internet banking. Peringkat 3 dan 4 masing-masing ditempati oleh jagoan lama worm sebanyak 5,5 % dan Adware sebanyak 2,44 %. Dari insiden malware di kuartal pertama 2015 beberapa hal penting yang perlu menjadi perhatian para pengguna internet Indonesia adalah kesadaran untuk melakukan patching atau penambalan atas celah keamanan dari piranti lunak yang digunakan, salah satunya dengna cara memproteksi komputernya dengan pengamanan bank guard dan anti exploit serta menghindari situs freeware yang banyak mengandung adware / PUP seperti Softonic, Brothersoft dan Cnet.

Sumber : http://www.vaksin.com/0415-statistik-malwareq1

id.cert

Exploit

- **CVE-2010-2568** adalah celah keamanan LNK.Shorcut yang sebenarnya berumur lebih dari 5 tahun namun sampai saat ini masih termasuk ke dalam celah keamanan yang paling banyak di eksploitasi. Celah keamanan ini menjadi favorit karena bisa dieksploitasi untuk menguasai banyak sekali OS Microsoft Windows baik workstation maupun server seperti Windows XP SP3, Server 2003 SP2, Vista SP1 dan SP2, Server 2008 SP2 dan R2, Windows 7 yang memungkinkan penyerang untuk menguasai komputer korban dengan file .LNK atau PIF shorcut file yang telah dipersiapkan sebelumnya. Celah keamanan ini juga diekslpoitasi oleh Stuxnet melalui **CVE-2010-2772** pada Siemens WinCC SCADA sistem.
- **CVE-2011-0979** adalah celah keamanan pada Microsoft Excel 2002 SP3, 2003 SP3, 2007 SP2, 2010. Office 2004, 2008 dan 2011 for Mac, Open XML File Format Converter for Mac dan Excel Viewer SP2. Celah keamanan ini memungkinkan penyerang menjalankan program lain guna menguasai komputer yang memiliki celah keamanan ini.
- **CVE-2013-2729** adalah exploit yang menyerang Adobe Acrobat Reader yang lebih dikenal dengan nama Adobe Reader BMP/RLE heap corruption vulnerability. Celah keamanan ini dimanfaatkan oleh pembuat malware dan mampu menginfeksi komputer sekalipun sudah dilindungi program antivirus yang terupdate namun tidak memiliki exploit protection. Salah satunya digunakan untuk mengirimkan email yang jika dijalankan akan mengunduh dan menjalankan GOZ Game Over Zeus. Eksploitasi yang muncul sejak tahun 2013 ini terdeteksi menguasai usaha exploit yang dihentikan oleh G Data anti exploit.

Sumber : http://www.vaksin.com/0415-statistik-malwareq1

Sality, Zeus, Conficker dan beberapa masih merajai Dunia

- https://map.virustracker.net/

Incident Monitoring Report (IMR)

Incident Monitoring Report (IMR) yang dilakukan oleh ID-CERT pada tahun 2013 -2014 yang masih diurutan pertama yaitu **SPAM.**

2013

NO	Kategori Komplain	Rating (%)
1	SPAM	40,40
2	NETWORK INCIDENT (Deface, DDos Attack, etc)	27,81
3	MALWARE	10,07
4	INTELLECTUAL PROPERTY RIGHTS/HaKI	8,71
5	KOMPLAIN SPAM	2,50
6	SPOOFING/PHISHING	1,65
7	RESPON ADUAN	0,86

2014

NO	Kategori Komplain	Rating (%)
1	SPAM	51,78
2	INTELLECTUAL PROPERTY RIGHTS/HaKI	24,14
3	KOMPLAIN SPAM	6,74
4	NETWORK INCIDENT (Deface, DDos Attack, etc)	6,61
5	SPOOFING/PHISHING	4,67
6	MALWARE	4,57
7	RESPON ADUAN	1,49

Sumber : http://cert.or.id/tentang-kami/id/

id.cert

Teknologi Pendeteksian

- **AndroScanner** – Malware Scanner Android (ID-CERT)
- **AMOS** – Android Malware Operating System (ID-SIRTII/CC)
- **Emsisoft Emergency Kit** (Portable Scanner)
  Download : http://www.cert.or.id/bahan-bacaan/id/konten/24/

Contact

- Twitter : @DemonicCloud9
- Facebook : Gie Cloudnine
- Email : - gie@serverhack.org

  - gie@defence.id

id.cert