Trend dan keterhubungan trend Cybercrime antar tahun

Disusun untuk memenuhi tugas ke VI, MK. Kejahatan Komputer

(Dosen Pengampu : Yudi Prayudi, S.Si, M.Kom)

Fathirma'ruf
13917213

PROGRAM PASCASARJANA TEKNIK INFORMATIKA
FAKULTAS TEKNIK INDUSTRI
UNIVERSITAS ISLAM INDONESIA
YOGYAKARTA
2014

MATERI

Trend dan keterhubungan trend Cybercrime antar tahun

Sumber	2012-2013	2014
RSA	• Trojan (mobile phone) • Malware (pencurian data non-keuangan) • Melumpuhkan layanan dan Penipuan • Security (account) • Hacking system • Security system	• Malware • Phising • Security (Bitcoins) • Security (Botnet) • Security (account)

Sumber : Report RSA 2012-2014

RSA Cybercrime report 2014

RSA, adalah bagian dari Divisi Keamanan EMC, yang merupakan lembaga penyedia utama keamanan intelijen-driven-solusi. RSA membantu organisasi terkemuka di dunia memecahkan masalah mereka yang paling kompleks yang terkait dengan tantangan keamanan sensitive, mengelola risiko organisasi, menjaga akses mobile dan kolaborasi, mencegah penipuan online, dan membela terhadap ancaman canggih, pada tahun 2014 mengeluarkan laporan terkait dengan beberapa perkembangan tekhnologi dan kejahatan pada dunia cyber yang terjadi di dunia yaitu:

Trend # 1: Mobile (Ancaman yang Canggih dan Pervasif pada mobile phone)
Pasar smartphone di seluruh dunia mencapai tonggak sejarah baru pada tahun 2013 dengan penjualan lebih dari satu miliar unit. Dengan meningkatnya penjualan tersebut Pada Juli 2013 Google mengumumkan bahwa lebih dari satu juta aplikasi yang tersedia di Google Play diunduh oleh pengguna smartphone dan Pada Oktober 2013, Apple mengumumkan statistik yang sama untuk App Store.
Sebagai pribadi yang mengikuti dan memanfaatkan teknologi akan membuat meningkatnya data terkait penggunaan smartphone dan aplikasi untuk mobile phone tersebut penjahat cyber akan terus mengembangkan dan memperbaiki skema mereka untuk memanfaatkan tren ini.

Sebagaimana dijelaskan dalam laporan RSA tahun lalu, aplikasi mobile berbahaya dan berisiko tinggi dan telah menjadi vektor ancaman yang signifikan karena

para penjahat cyber meningkatkan upaya mereka untuk menyebarkan malware dan serangan phishing dengan kedok aplikasi yang sah.

Android adalah system operasi paling banyak digunakan oleh platform mobile di dunia yang dikombinasikan dengan sifat open source dari sistem operasinya, hal ini akan berarti juga android adalah platform yang paling diincar oleh ancaman dari tindak cybercrime. Dalam hal terinfeksi jenis serangan malware dan phising Android adalah system operasi yang ada mencapai hampir 1,4 m, dengan catatan terinfeksi satu juta yang terdeteksi pada tahun 2013 saja (hampir tiga kali jumlah yang terdeteksi pada tahun 2012).

penjahat cyber akan menggunakan rekayasa sosial untuk membujuk pengguna untuk menginstal sertifikat atau perangkat lunak keamanan yang palsu di ponsel mereka. Teknik injeksi HTML akan digunakan untuk mengirim pengguna ke link langsung untuk men-download aplikasi berbahaya. Selama instalasi, Aplikasi akan meminta berbagai perizinan dengan tujuan untuk mendapatkan hak super user yang akan memberikan akses penuh ke fitur telepon dan dapat membuat aplikasi yang mustahil (terinfeksi) untuk uninstall pada smartphone.

Trend # 2: Popularitas Bitcoin

Popularitas Bitcoin Membuatnya menjadi Target untuk Pencurian dan kasus penipuan Mata Uang. Penggunaan bicoints rentan dengan aktivitas phishing klasik dan serangan dengan rekayasa sosial, sejumlah bursa Bitcoin secara online telah melaporkan serangan oleh hacker yang diduga menciptakan transaksi penipuan dengan memanfaatkan cacat dalam protocol. untuk menutup pada bulan Februari 2014 beberapa bursa bitcoints Mt Gox salah satunya melaporkan kebangkrutan dalam menghadapi kerugian besar. 850.000 Bitcoins dilaporkan telah hilang, yang mewakili sekitar 7% dari semua Bitcoins yang ada pada saat itu - meskipun Mt Gox tidak kemudian menemukan 200.000

Trend # 3: Malware Gets Canggih, Serangan APT (Botnet)

Serangan Malware Menjadi trend Umum dalam beberapa kasus Penipu dan sebagai motif penjahat dunia maya dalam mencari cara-cara baru yang canggih dalam tindak kejahatan cybercrime termasuk dengan memanfaatkan botnet, mereka juga menghasilkan keuntungan yang signifikan dari aktivitas serangan malware.

Botnet digunakan oleh penipu, penjahat cyber dan hacktivists untuk menjadi tuan rumah infrastruktur untuk meluncurkan serangan seperti DDoS untuk menurunkan situs bank, pemerintah lembaga dan organisasi profil tinggi lainnya. Banyaknya komputer zombie dalam botnet berarti serangan akan bergerak, sehingga sulit untuk menemukan sumber yang melakukan control (pusat control botnet yang bertugas mengendalikannya) terhadap botnet yang telah menyebar pada beberapa infrastruktur

Trend # 4: User Authentication Will be Redefined by Mobile

Dengan keberadaan dunia online atau internet keberadaan sandi telah lama menjadi masalah bagi sebuah organisasi, terutama dengan keberadaan portal konsumen yang mereka hadapi, di mana jumlah identitas digital dari konsumen yang mencapai jutaan membutuhkan perlindungan mencapai ke dalam jutaan. Beberapa Konsumen mengharuskan mereka untuk membuat password yang dapat mudah untuk di ingat. Hal ini dapat menyebabkan pengguna untuk membuat password yang lemah, dan menuliskannya di atas kertas, atau kembali menggunakan password yang sama di beberapa situs. Bahkan, salah satu dari lima pengguna secara online mendaur ulang password yang sama untuk setiap account online mereka.

Hal tersebut dimanfaatkan oleh penjahat yang berada di dunia cyber, untuk melakukan peretasan terhadap account pengguna dengan memanfaatkan teknik tertentu, dan tentunnya dari sebab penggunaan password yang sama untuk semua layanan akan dapat dengan mudah para pelaku untuk menembus semua akun dari pengguna tersebut.

RSA Cybercrime report 2012 -2013

Trend # 1: Perang Trojan (Zeus) dan Malware (pencurian Keuangan)

RSA telah mengamati lanskap Trojan sepanjang 2011, dan Zeus 2.0 terus Mendominasi sebagai Trojan keuangan terkemuka sepanjang tahun. Disangkal paling luas menyebarkan malware keuangan di dunia, Zeus bertanggung jawab untuk sekitar 80% dari semua serangan terhadap lembaga keuangan saat ini dan diperkirakan telah menyebabkan lebih dari $ 1000000000 kerugian global dalam lima tahun terakhir.

Trend # 2: Cybercriminals akan Cari Cara Baru untuk pencurian Data Non-Keuangan

Penjahat dunia maya terus memahami nilai dari ata non-keuangan yang dapat mereka panen, Trojan dan malware sudah aktif mencari cara untuk menguangkan informasi ini. Tidak hanya informasi yang diperdagangkan, tetapi akses ke korban komputer adalah Sesuatu yang dapat ditawarkan untuk dijual, juga. Beberapa contoh data non-keuangan untuk dijual saat ini adalah sebagai berikut:

1. *Laporan utilitas dari perusahaan terkait data internal maupun data nasabah*
2. *Data rekam medis yang dalam hal inipara pelaku kejahatan cyber mencuri database pasien terkait rekam medis*
3. *Hacked account pengguna internet*
4. *Akses kepada computer yang telah terinfeksi sebelumnya*

Trend # 3: Penipuan terhadap layanan
Trend ini dilakukan oleh para penjahat cyber dengan memanfaatkan beberapa vendor yang memberikan jasa terhadap user di media internet, untuk melakukan aktivitas penipuan dan pencurian yang dapat merugikan pihak vendor penyedia layanan online maupun pengguna layanan, contoh, permainan saham, took online, dll.

Trend #4: Account Takeover and Increasing Use of Manual-Assisted Cyber Attacks
Otentikasi kuat saat login telah menjadi perlu untuk melindungi account keuangan online.Namun, penjahat dunia maya secara konsisten mengembangkan metode serangan baru yang dapat memotong Login otentikasi - dan bahkan sistem otentikasi dua faktor. Beberapa serangan yang berkembang sepanjang 2011 adalah man-in-the-browser yang Trojans dan forwarding SMS.

Perlindungan transaksi telah menjadi bagian penting dari melindungi transaksi keuangan dari pengambilalihan account yang dilakukan dengan motif penipuan keuangan, Amerika Serikat secara khusus mewajibkan bank untuk melaksanakan deteksi penipuan berbasis risiko dan sistem yang memungkinkan otentikasi out-of-band untuk transaksi berisiko tinggi dan dilakukan dengan pemantauan yang tetap.

Trend # 5: The Rise of Hacktivism
Hacktivism selanjutnya dipopulerkan pada tahun 2011 oleh beberapa kelompok-kelompok seperti Anonymous, LulzSec, dan AntiSec dengan tujuan untuk mengambil alih kepemerintahan dan perusahaan global, Tujuan dari hacktivism yang paling sering didorong oleh bermuatan politis.
agenda dengan maksud untuk menimbulkan rasa takut, intimidasi, atau penghinaan publik. Untuk itu ada kalanya untuk mereka memikirkan kembali keamanan informasi, pemahaman musuh, termasuk motivasi mereka, kemampuan, dan tujuan, sangat penting dalam bagaimana organisasi melindungi diri mereka sendiri.

Trend #6: Better Information Sharing will Lead to More Crackdowns on Cyber Gangs and Botnet Operators

Pada tahun 2011, itu adalah tahun yang sangat penting dalam hal berbagi informasi kepada seluruh lembaga penegak hukum internasional, untuk dapat bekerjasama dengan beberapa lembaga yang terkait dalam penanganan kasus cybercrime

Analisa Keterhubungan trend kasus cybercrime

Dari laporan RSA yang merupakan bagian dari Divisi Keamanan EMC, yang merupakan lembaga penyedia utama keamanan intelijen-driven-solusi. Dengan tujuan untuk membantu organisasi terkemuka di dunia memecahkan masalah, menyatakan bahwa Perkembangan kejahatan pada dunia cyber sangatlah terorganisir baik dari manajemen maupun perkembangannya, dapat dilihat bahwa serangan –serangan yang terjadi dari tahun 2012 – 2013 sangatlah pesat mengikuti perkembangan teknologi yang ada, kasus yang ada pun memiliki keterhubungan maupun perkembangan dilihat dari sisi teknik maupun cara melakukannya.

DAFTAR PUSTAKA

http://www.emc.com/collateral/white-paper/rsa-cyber-crime-report-0414.pdf (diakses pada tanggal 22-12-2014 Pukul 09.00 PM)

http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf (diakses pada tanggal 23-12-2014 Pukul 10.33 PM)

http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf (diakses pada tanggal 23-12-2014 Pukul 11.33 PM)