Analisis Penggunaan Sertifikat Digital SSL Pada Situs Palsu Untuk Melakukan Serangan Phising

Eko Yon Handri
Puskaji Palsan, Lemsaneg
Jakarta, Indonesia
yon.handri@lemsaneg.go.id

Ayu Pustikasari
Puskaji Palsan, Lemsaneg
Jakarta, Indonesia
ayu.pustikasari@lemsaneg.go.id

Abstraksi—**Pertukaran dokumen pada sistem elektronik banyak menggunakan file PDF karena memiliki fitur yang cukup lengkap. Namun fitur tersebut dimanfaatkan oleh para hacker untuk menyisipkan malware di dalam file PDF. Malware aktif dan mulai menyerang saat file PDF dibuka oleh pengguna. Pencegahan penyisipan malware dapat dilakukan dengan menerapkan tanda tangan digital sebelum file PDF dipublikasikan. Namun apa yang terjadi apabila file PDF yang ditandatangani secara digital telah terinfeksi malware sebelumnya. Paper ini menjelaskan analisis terhadap penerapan tanda tangan digital terhadap file PDF baik yang tidak maupun yang sudah terinfeksi dengan malware.**

Kata kunci—tanda tangan digital, malware, PDF

I. LATAR BELAKANG

File PDF (*Portable Document Format*) merupakan format dokumen elektronik yang sangat populer digunakan dalam komunikasi di sistem elektronik. Penggunaan file PDF banyak ditemui dalam publikasi dokumen publik seperti pengumuman, press release dan bahkan untuk dokumen negara semisal Undang-Undang atau Peraturan Pemerintah. Semakin banyaknya penggunaan file PDF ini memotivasi para pembuat malware untuk menyebarkan malwarenya melalui file PDF tersebut [1]. Malware yang disebarkan dapat berupa virus, *worm*, *trojan horse* dan *spyware* yang memanfaatkan *backdoor*, *rootkit*, *keylogger* serta *cookies tracker* [2]. Malware yang ditanam ke dalam file PDF digunakan dalam kegiatan *Spear Phishing* yaitu mengirimkan file yang dilampirkan (*attachment*) pada email yang seolah-olah berasal dari individu atau organisasi yang dikenal si penerima email [3]. Selain file PDF, format file lain yang biasa digunakan adalah Office Word dan Excel. Tujuan dari serangan ini adalah untuk mendapatkan informasi yang diinginkan oleh seorang hacker dimana tidak hanya untuk mengambil password, kartu kredit, informasi keuangan tetapi juga untuk melancarkan serangan yang lebih besar.

Terdapat beberapa contoh kasus serangan malware dengan spear phishing yaitu tahun 2011 dimana RSA Security berhasil diretas melalui file Excel (.xls) yang berisi *zero-day exploit* dan dilampirkan pada email dan dibuka oleh pegawai sehingga menjalankan *backdoor* di sistem. Pada Juni 2015, serangan yang sama juga mengakibatkan kerugian sebesar 46,7 juta US Dolar pada perusahaan *Ubiquiti Networks Inc* [4]. Kondisi yang saat ini terjadi adalah banyak file PDF yang dipublikasikan di berbagai situs instansi pemerintahan tanpa ada pengamanan yang cukup baik. Hacker dapat memanfaatkan kerawanan ini untuk menyusupkan malware ke dalam file PDF dan mempublikasikan kembali sehingga setiap orang yang mengunduh dan membuka file PDF secara tidak sadar akan menjalankan malware. Malware ini dapat masuk ke dalam sistem jaringan komputer yang lebih luas di tempat mereka bekerja misalkan dengan mengaktifkan *keylogger*. Dan pada saat itulah, hacker dapat dengan mudah melakukan serangan berikutnya.

Pada paper ini lebih khusus membahas penerapan tanda tangan digital pada dokumen PDF. Adanya tanda tangan digital dapat mencegah terhadap pemasukan malware ke dalam dokumen PDF. Dan berdasarkan informasi tanda tangan digital tersebut dapat diketahui keaslian dan keutuhan dokumen serta mendeteksi ketika dokumen PDF mengalami modifikasi khususnya adanya keberadaan malware.

II. SERANGAN MALWARE MELALUI FILE PDF

A. Elemen dan Fitur PDF

PDF memiliki kelebihan untuk menyuguhkan isi dokumen yang cukup kompleks baik melalui elemen statis maupun elemen dinamis dengan adanya interaksi dengan pengguna. Adapun jenis elemen statik dan dinamis dapat dilihat seperti pada tabel 1.

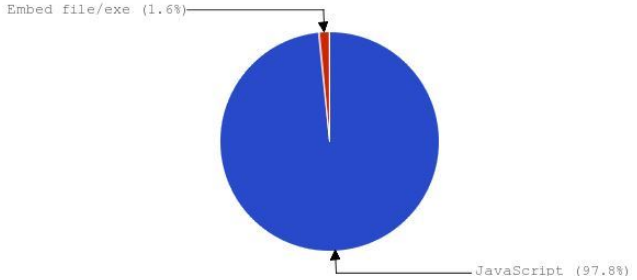
Tabel 1. Elemen PDF
(sumber : Yonts, 2010)

Elemen Statik	Elemen Dinamis
• Teks dan Style-nya • Karakter Encoding dan Font • Multimedia	• Embedded JavaScript dan ActionScript dari Adobe Flash • Dynamic Action Trigger (On Open) • Mengakses data secara online melalui URL

Kombinasi antara kedua elemen yang dimiliki oleh PDF dapat membantu pengguna dalam memanfaatkan isi dokumen secara interaktif dan menarik. Hal ini merupakan kelebihan yang dimiliki oleh PDF sebagai *format file portable* dibanding dengan format file lainnya. Namun kelebihan tersebut dapat dengan mudah dimanfaatkan oleh para hacker untuk memasukkan (*embed*) script malware.

Berdasarkan Malware Tracker, diketahui bahwa serangan yang memanfaatkan malware pada file PDF sebanyak 1,6% memanfaatkan embed file/exe dan 97,8% memanfaatkan

javascript yang dimasukkan ke dalam file PDF [5], seperti terlihat pada gambar di bawah.



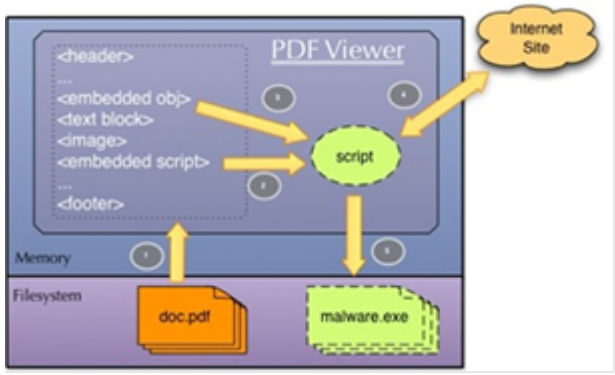
Gambar 1. Prosentase Kode Malware pada PDF
(sumber : Tracker, 2014)

Microsoft Malware Protection Center pada tahun 2013 telah merilis beberapa nama file PDF yang sering digunakan oleh Hacker untuk memasukkan malware yaitu pdf_new[1].pdf,auhtjseubpazbo5[1].pdf,avjudtcobzimxnj2[1].pdf, pricelist[1].pdf, couple_saying_lucky[1].pdf, 5661f[1].pdf 7927, 9fbe0[1].pdf 7065, pdf_old[1].pdf [6]. Menurut Symantec [1], fitur PDF yang kaya juga dimanfaatkan hacker untuk menyembunyikan kode malware yang ditulis dalam bahasa javascript agar tidak terdeteksi oleh anti virus. Adapaun beberapa fitur PDF yang digunakan adalah sebagai berikut :

- Menggunakan algoritma enkripsi standar dari Adobe (RC4 dan AES) untuk melindungi isi kode malware agar tidak terdeteksi oleh antivirus
- Menggunakan kompresi multi-level untuk menghindari deteksi antivirus karena tidak semua antivirus mendukung semua jenis kompresi
- Memanfaatkan celah keamanan flash yang disimpan ke dalam file PDF

B. Pola Serangan Malware pada PDF

Pada paper ini dijelaskan pola serangan malware yang ditulis dalam bahasa pemrograman yang populer yaitu JavaScript. Kode malware direkayasa sedemikian rupa kemudian disisipkan ke dalam file PDF. Malware mulai diaktifkan ketika file PDF dibuka oleh pengguna. Gambar 2 di bawah menjelaskan bagaimana malware pada PDF bekerja.



Gambar 2. Pola Serangan Malware Melalui PDF
(sumber : Yonts, 2010)

Dari gambar di atas, langkah-langkah serangan malware dapat dijelaskan sebagai berikut :

1) Pengguna membuka PDF (doc.pdf) yang telah disisipi kode malware dalam struktur embedded script.
2) Embedded script diatur untuk dijalankan dengan fitur On Open yang dimiliki oleh PDF.
3) Embedded Script diekstraksi dan mengkonstruksi ulang menjadi script malware.
4) 4Script malware akan mengunduh aplikasi malware dari alamat situs internet yang tersimpan tersembunyi dari script tersebut ke dalam sistem pengguna.
5) Aplikasi malware (malware.exe) diinstal ke dalam sistem pengguna.

III. PENERAPAN TANDA TANGAN DIGITAL PADA PDF

A. Tanda Tangan Digital

Tanda tangan digital merupakan representasi suatu dokumen dalam bentuk nilai hash (*message digest*) yang dienkripsi dengan kunci privat menggunakan algoritma asimetrik [13]. Tanda tangan digital menyediakan 3 (tiga) aspek keamanan data yaitu autentikasi, integritas dan nir-sangkal [14]. Adapun proses penerapan tanda tangan digital ada 2(dua) yaitu :

1) Proses Penandatanganan (*Signing*)
   Proses penandatanganan adalah proses penggunaan kunci privat dengan algoritma asimetrik untuk mengenkripsi dokumen.

2) Proses Verifikasi (*Verifying*)
   Proses Verifikasi adalah proses penggunaan kunci publik dengan algoritma asimetrik untuk mendekripsi hasil enkripsi dokumen dengan kunci privat yang berpasangan.

Gambar 3. Proses Tanda Tangan Digital
(Sumber : Forouzan, 2007)

B. Mekanisme Penandatanganan File PDF

Ada 2 (dua) cara mekanisme penandatanganan secara digital terhadap file PDF yaitu penandatananan eksternal dan internal. Pendantanganan eksternal dilakukan dengan menggunakan aplikasi PDF Signer. Aplikasi PDF Signer tidak perlu membuka file PDF terlebih dahulu untuk melakukan penandatanganan agar malware tidak bekerja saat pembukaan file PDF tersebut. Sedangkan penanatanganan internal dilakukan dengan menggunakan aplikasi aplikasi PDF Reader dimana file PDF harus dibuka dulu kemudian diberikan tanda tangan digital. Kedua mekanisme penandatanganan tersebut membutuhkan sertifikat digital berekstensi p12 atau pfx yang menyimpan kunci privat di dalamnya.

IV. STUDI KASUS

Terdapat beberapa tools baik offline maupun online yang dapat digunakan untuk melakukan analisis terhadap file PDF yang terindikasi malware di dalamnya. Sebagian besar tools analisis malware di PDF disediakan oleh Sistem Operasi Kalilinux atau REMnux seperti PeePDF dan Pdfid. Tools lain adalah JsunPack yang dapat diunduh dari jsunpack.jeek.org, PDF Stream Dumper dan Origami dari Ruby Framework. Tools online yang bisa digunakan adalah PDF Examiner yang dapat diakses dari malwaretracker.com dan juga Wepawet yang dapat diakases di http://wepawet.iseclab.org. [8].

Paper ini melakukan 2 (dua) kasus PDF yang akan dianalisis. Kasus pertama adalah melakukan analisis terhadap kode JavaScript secara umum pada PDF dan kasus kedua adalah melakukan analisis terhadap kode JavaScript malware pada PDF. File PDF tersebut dikondisikan sebelum dan setelah diberikan tanda tangan digital. Tools yang digunakan adalah PDF Examiner Online.

A. Analisis Indikasi Malware Pada Kode JavaScript Umum

Nama file yang digunakan pada analisis ini adalah malcode.pdf yang telah disisipi kode JavaScript umum. Proses penandatangan yang digunakan pada analisis ini adalah internal. Dengan menggunakan fitur aplikasi Adobe PDF yang ada, file malcode.pdf diberikan tanda tangan elektronik yaitu dengan hanya menambahkan gambar tanda tangan dan juga diberikan tanda tanga digital dengan menggunakan sertifikat digital. Hasil analisis awal dapat dilihat seperti tabel di bawah ini.

Tabel 2. Analisis Penerapan Tanda Tangan

No.	Nama File	Kondisi	Penyisipan Javascript Normal	Penyisipan Javascript Paksa
1	Malcode.pdf	Normal	Bisa	Bisa
2	Malcode-1.pdf	Tanda tangan elektronik	Bisa	Bisa
3.	Malcode-2.pdf	Tanda tangan digital tanpa trusted dynamic dan javascript	Tidak	Signature Invalid
4.	Malcode-2a.pdf	Tanda tangan digital tanpa trusted dynamic dan javascript dan dikunci	Tidak	Signature Invalid
5.	Malcode-3.pdf	Tanda tangan digital dengan trusted dynamic dan javascript	Tidak	Signature invalid
6.	Malcode-3a.pdf	Tanda tangan digital dengan trusted dynamic dan javascript dan dikunci	Tidak	Signature invalid

Berdasarkan tabel di atas, diketahui bahwa PDF yang telah disisipi kode JavaScript ketika diberikan tanda tangan digital tidak dapat disisipi kembali dengan kode JavaScript. Dalam kondisi penyisipan kode JavaScript yang disisipka ke file pDF secara paksa misalkan dengan Hex Editor atau tools lainnya maka dapat dideteksi dengan informasi bahwa nilai tanda tangan digitalnya menjadi invalid. Hal ini dapat mencegah penyalahgunaan file PDF yang sudah tersebar di internet untuk disisipi kode JavaScript jahat seperti malware oleh Hacker. Dan apabila file PDF tersebut berhasil disisipi Malware maka dapat dideteksi dengan melihat validitas tanda tangan digitalnya.

Analisis selanjutnya adalah dengan menggunakan tools PDF Examiner untuk mengetahui keberadaan kode JavaScript yang terindikasi maware file PDF. Dengan nama file dan kondisi yang sama hasil analisis tersebut dapat dilihat seperti tabel di bawah ini.

Tabel 3. Indikasi Malware Pada Kode JavaScript

No.	Nama File	
1	Malcode.pdf	Suspicious containts JavaScript (**Suspicious** [4] Beta OpenIOC) 1.0 @ 15: suspicious.warning: object contains JavaScript 1.0 @ 186568: suspicious.warning: object contains JavaScript 34.0 @ 185394: suspicious.warning: object contains JavaScript 35.0 @ 187169: suspicious.warning: object contains JavaScript
2	Malcode-1.pdf	Analysis: **Suspicious** [2] Beta OpenIOC 1.0 @ 16: suspicious.warning: object contains JavaScript 35.0 @ 189669: suspicious.warning: object contains JavaScript
3	Malcode-2.pdf	Analysis: **Suspicious** [1] Beta OpenIOC 22.0 @ 793: suspicious.warning: object contains JavaScript
4	Malcode-2a.pdf	Analysis: **Suspicious** [1] Beta OpenIOC 22.0 @ 784: suspicious.warning: object contains JavaScript
5	Malcode-3.pdf	Analysis: **Suspicious** [1] Beta OpenIOC 22.0 @ 791: suspicious.warning: object contains JavaScript
6	Malcode-3a.pdf	Analysis: **Suspicious** [1] Beta OpenIOC 22.0 @ 787: suspicious.warning: object contains JavaScript

Berdasarkan tabel di atas, dapat diketahui bahwa keempat file PDF yang diberikan tanda tangan digital memiliki indikasi adanya malware dari kode JavaScript lebih sedikit dibandingkan kedua file PDF awal tanpa tanda tangan digital. Hal ini berarti penerapan tanda tangan digital pada PDF dapat menghilangkan object yang berupa kode JavaScript yang diindikasi merupakan malware. Hilangnya object kode Javascript tersebut bukan berarti malware di dalam file PDF ikut hilang tetapi dirubah menjadi data stream seperti terlihat pada tabel 4, sehingga malware masih dimungkinkan tetap berjalan walaupun sudah diterapkan tanda tangan digital.

Perubahan jumlah object kode JavaScript dibuktikan dengan melakukan analisis file PDF menggunakan tools PDFStream Dumper. Hasil analisis object pada struktur PDF adalah sebagai berikut :

Tabel 4. Analisis Object Struktur PDF

No.	Nama File	Jumlah Object	JavaScript Object	Data Stream	Launch Action	XML Data
1	Malcode.pdf	43	5	8	3	1
2	Malcode-1.pdf	43	3	11	3	1
3.	Malcode-2.pdf	35	1	28	-	1
4.	Malcode-2a.pdf	35	1	28	-	1
5.	Malcode-3.pdf	35	1	28	-	1
6.	Malcode-3a.pdf	35	1	28	-	1

Berdasarkan tabel di atas, diketahui bahwa bahwa keempat file PDF yang diberikan tanda tangan digital memiliki Javacript Object lebih sedikit dibandingkan dengan file PDF yang asli yaitu berkurang 4 object. Hal ini berarti bahwa penerapan tanda tangan digital dapat menghilangkan JavaScript Object dan merubahnya menjadi data stream yang ditandai dengan jumlah bertambah.

B. Analisis Pada Kode JavaScript Malware

Nama file yang digunakan pada analisis ini adalah ghostnet.pdf yang telah disisipi kode malware backdoor untuk mengakses sistem target secara ilegal. Malware ini akan aktif

dan berjalan saat pengguna membuka file PDF tersebut. Oleh karena itu, proses penandatanganan dilakukan secara eksternal yatu menggunakan aplikasi PDF Signer. File PDF yang telah ditandatangani diberinama ghostnet[signed].pdf. Kedua file ini dilakukan analisi dengan tools online PDF Exminer dengan hasil sebagai berikut :

Tabel 5. Detektsi Malware Pada File PDF

No.	Nama File	
1	Ghostnet.pdf	9.0 @ 9658: suspicious.javascript object 10.0 @ 9701: suspicious.warning: object contains JavaScript 10.0 @ 9701: pdf.exploit util.printf CVE-2008-2992 10.0 @ 9701: suspicious.string -shellcode- 10.0 @ 9701: suspicious.obfuscation using unescape 10.0 @ 9701: suspicious.obfuscation using substring
2	Ghostnet[signed].pdf	Analysis: Malware [52] Beta OpenIOC 14.0 @ 3583: suspicious.warning: object contains JavaScript 14.0 @ 3583: pdf.exploit util.printf CVE-2008-2992 14.0 @ 3583: suspicious.string -shellcode- 14.0 @ 3583: suspicious.obfuscation using substring 14.0 @ 3583: suspicious.obfuscation using unescape

Berdasarkan tabel di atas, dapat diketahui bahwa kedua file PDF tersebut sama-sama terdeteksi adanya malware yaitu pada informasi pdf.exploit util.printf CVE-2008-2992. Hal ini berarti penerapan tanda tangan digital pada file PDF yang terindikasi malware tidak berpengaruh terhadap keberadaan malware di dalamnya. Malware tetap ada di dalam file PDF dan tidak terjadi proses blok terhadap aktivasinya ketika tanda tangan digital diterapkan. Tanda tangan digital tetap menjalankan fungsi keamanan data saja yaitu untuk menjamin autentikasi, integritas dan nir-sangkal.

Analisi selanjutnya adalah menggunakan tools PDFStream Dumper untuk mengetahui keberadaan object pada struktur PDF yang terindikasi Malware. Hasil analisis object pada struktur PDF adalah sebagai berikut :

Tabel 6. Analisis Object Malware Pada PDF

No.	Nama File	Jumlah Object	JavaScript Object	Data Stream	Launch Action	XML Data	Exploit Found
1	ghostnet.pdf	39	1	7	2	1	Stream 10
2	ghostnet [signed].pdf	62	1	10	3	2	Stream 14

Berdasarkan tabel di atas, diketahui bahwa bahwa penerapan tanda tangan digital pada file PDF yang terinfeksi malware menambah jumlah object, datastream, launch action dan XML Data. Dan object malware tetap terdeteksi di kedua file tersebut. Hasil analisis dengan PDF Stream Dumper ini menguatkan analisis sebelumnya dimana keberadaan malware disimpan ke dalam data stream setelah diterapkan tanda tangan digital.

V. PENANGANAN TERHADAP PDF TERINDIKASI MALWARE

Banyak cara yang dapat dilakukan untuk menghindari serangan malware dari file PDF yang dibuka pengguna. Cara penanganannya tidak hany abergantung pada bantuan teknologi seperti Anti Malware atau Firewall security awareness dari pengguna juga sangat penting. Berikut beberapa cara penanganan dari serangan malware dari file PDF yaitu :

- Melakukan kontrol aplikasi PDF Reader dengan cara menonaktifkan Javascript, memonaktfikan pembacaan PDF melalui browser dan memblok PDF Reader untuk mengakses filesystem dan akses jaringan komputer tertentu.
- Cek namafile PDF yang dianggap mencurigakan dan tidak langsung membukanya
- Selalu melakukan pemindaian file PDF yang dilampirkan di email atau file PDF yang diunduh dari website tertentu
- Melakukan update sistem operasi dan anti virus
- Menginstalasi Anti-Malware
- Menerapkan kebijakan ketat pada sistem operasi
- Melakukan filtering terhadap Emai Gateway maupun Web Gateway

Berdasarkan hasil analisis terhadap penerapan tanda tangan digital pada file PDF yang terinfeksi malware, maka cara penanganan tersebut di atas tetap perlu dilakukan meski file PDF sudah ditandatangani secara digital. Pengaruh tanda tangan digital terhadap file PDF baik yang tidak terinfeksi maupun yang sudah terinfeksi dapat dijelaskan sebagai berikut:

1) Tanda tangan digital dapat mencegah penyisipan kode malware pada file PDF karena setalah ditandatangani, fitur penyisipan kode JavaScript otomatis dinonaktifkan.

2) File PDF yang sudah ditandatangani namun tetap berhasil disisipi malware dapat dideteksi sejak dini dengan mengecek validitas tanda tangan digitalnya.

3) Penerapan tanda tangan digital pada file PDF yang sudah terinfeksi malware tidak mempengaruhi keberadaan malware karena kode malware disimpan ke dalam object data stream pada struktur PDF.

4) Peran tanda tangan digital pada file PDF yang sudah terinfeksi malware adalah menginformasikan pihak yang melakukan penandatangan tersebut berdasarkan sertifikat digital yang digunakan, sehingga dapat diketahui sumber penyebaran malware.

VI. KESIMPULAN

File PDF yang banyak digunakan pengguna untuk melakukan pertukaran dokumen sangat rentan disisipi malware khususnya dengan kode JavaScript. Pola serangan yang dilakukan malware di file PDF adalah dengan menyembunyikan kode malware untuk mengunduh aplikasi malware sebenarnya dari alamat url yang tersimpan di dalamnya. Aplikasi malware tersebut akan mulai berjalan saat file PDF dibuka oleh pengguna.

Pada paper ini, telah dipelajari bahwa penerapan tanda tangan digital pada file PDF yang terinfeksi malware tidak menghilangkan kode malware di dalamnya karena disimpan pada object data stream. Hal ini memberikan penjelasan bahwa cara penanganan terhadap file PDF tetap dilakukan walaupun sudah ditandatangani secara digital. Sedangkan penerapan tanda tangan digital pada file PDF yang tidak terinfeksi malware dapat memberikan perlindungan terhadap penyisipan kode malware dengan mengecek validitas tanda tangan digitalnya. Tools yang digunakan pada paper ini hanya 2 (dua) jenis yaitu PDF Examiner dan PDFStreamDumper. Oleh karena itu, untuk mengoptimalkan hasil analisis penerapan tanda tangan digital pada file PDF yang terindikasi malware, perlu dilakukan penelitian lebih lanjut dengan menggunakan tools lain yang tersedia.

REFERENCES

[1] K. Selvaraj dan N. F. Gutierrez, “The Rise Of PDF Malware,” Symantec Security Response, California, 2010.

[2] P. Mell, K. Kent dan J. Nusbaum, Guide to Malware Incident Prevention and Handling, Gaitherburg: NIST 800-83, 2005.

[3] D. Stepenson, “Spear Phising : Who's Getting Caught?,” Firmex, 30 May 2013. [Online]. Available: http://www.firmex.com/thedealroom/spear-phishing-whos-getting-caught/. [Diakses 11 May 2016].

[4] D. Brecht, “Spear Phishing: Real Life Examples,” Infosec Institute, 18 Januari 2016. [Online]. Available: http://resources.infosecinstitute.com/spear-phishing-real-life-examples/. [Diakses 11 Mei 2016].

[5] M. Tracker, “PDF Current Threats,” Malware Tracker Limited, 14 Agustus 2014. [Online]. Available: http://www.malwaretracker.com/pdfthreat.php. [Diakses 11 Mei 2016].

[6] msft-mmpc, “The rise in the exploitation of old PDF vulnerabilities,” Microsoft TechNet, 29 April 2013. [Online]. Available: https://blogs.technet.microsoft.com/mmpc/2013/04/29/the-rise-in-the-exploitation-of-old-pdf-vulnerabilities/. [Diakses 11 Mei 2016].

[7] A. Blonce, E. Filiol dan L. Frayssignes, Portable Document Format (PDF) Security Analysis and Malware Threats, Rennes: Army Signals Academy, 2008.

[8] R. Shaw, “Analyzing Malicious PDFs,” Infosec Institute, 20 November 2013. [Online]. Available: http://resources.infosecinstitute.com/analyzing-malicious-pdf/. [Diakses 11 Mei 2016].

[9] W. Knowles, “So Who Hacked EC-Council Three Times This Week?,” Infosec News, 28 Februari 2014. [Online]. Available: http://www.infosecnews.org/so-who-hacked-ec-council-three-times-this-week/#.VzKNIIR96Hs. [Diakses 11 Mei 2016].

[10] R. McCormick, “Ethical hacking organization hacked, website defaced with Edward Snowden's passport,” The Verge, 24 Februari 2014. [Online]. Available: http://www.theverge.com/2014/2/24/5441386/ethical-hacking-organization-website-defaced-with-snowden-passport. [Diakses 11 Mei 2016].

[11] J. Yonts, “PDF Malware Overview,” SANS, 19 Juli 2010. [Online]. Available: http://www.sans.org/security-resources/malwarefaq/pdf-overview.php. [Diakses 11 Mei 2016].

[12] Kristinn, “PDF malware analysis,” SANS Digital Forensics and Incident Response Blog, 14 Desember 2009. [Online]. Available: https://digital-forensics.sans.org/blog/2009/12/14/pdf-malware-analysis. [Diakses 11 Mei 2016].

[13] Burnett, S., & Paine, S. (2004). RSA Security's Official Guide to Cryptography. California: McGraw-Hill.

[14] Forouzan, B. A. (2007). Cryptography And Network Security. New York: McGraw Hil