

Indonesian Journal of Multidisciplinary on Social and Technology

Homepage: https://journal.ilmudata.co.id/index.php/ijmst

Vol. 1 No. 2 (2023) pp: 176-183

P-ISSN: 2986-6790, e-ISSN: 2986-6782

Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang

Saputra Dio Azmi¹, Stiawan Deris², Sutabri Tata³

¹Magister Informatika, Magister Teknik Informatika, Universitas Bina Darma

²Sistem Komputer, Sistem Komputer, Universitas Sriwijaya

³Magister Informatika, Magister Teknik Informatika, Universitas Bina Darma

¹dioazmisaputra@gmail.com, ²stiawanderis @unsri.ac.id ²tata.sutabril@gmail.com*

Abstrak

Sistem deteksi adalah salah satu teknik untuk mendeteksi dan memberikan alarm bahwa adanya ancaman *Malware* bagi setiap perusahaan di indonesia. Sistem deteksi serangan *Malware* bertujuan untuk mendeteksi dan memberikan alarm agar sistem berfungsi secara optimal. Serangan *Ransomware* dapat menghentikan proses transaksi serta fungsi website SMK Negeri 1 Palembang dan memberikan dampak negatif bagi nasabah SMK Negeri 1 Palembang. *Deep Packet Inspection* (DPI) adalah sebuah metode untuk mendeteksi anomali berupa serangan *Ransomware* yang terjadi pada jaringan enterprise SMK Negeri 1 Palembang. Serangan yang dideteksi oleh DPI berupa serangan *Ransomware WannaCry* yang dilakukan oleh *attacker* untuk mendapatkan akses ke file yang ada di client maupun server. Pola serangan paket *Ransomware Wannacry* pada SMK Negeri 1 Palembang dapat dikenali dengan beberapa parameter seperti, *Protocol, Source Port, Destination Port, TLSv,* serta *JA3* yang digunakan.

Kata kunci: Deep Packet Inspection, Intrusion Detection System, Ransomware, WannaCry

1. Pendahuluan

Keamanan jaringan menjadi pelindung data pengguna terhadap serangan *Malware*. Dalam meningkatkan keamanan, di setiap jaringan diperlukan Sistem Pendeteksi untuk melindungi data dari tindak pencurian. Sistem Pendeteksi keamanan jaringan dapat mendeteksi berbagai jenis serangan, serta bersifat otomatis dan dapat mendeteksi semua ancaman. IDS atau bisa disebut juga *Intrusion Dectection System* sebagai perangkat dengan tujuan untuk mendeteksi anomali pada jaringan enterprise(Rodrigues et al., 2017).

Malicous Software atau yang lebih dikenal sebagai Malware merupakan perangkat lunak yang secara eksplisit didesain, untuk melakukan aktifitas berbahaya atau perusak perangkat lunak lainnya seperti Trojan, Virus, Spyware dan Exploit (Ferdiansyah, 2018). Malware diciptakan dengan maksud tertentu, yaitu melakukan aktifitas berbahaya yang berdampak sangat merugikan bagi para korbannya (Kolodenker et al., 2017). Ransomware merupakan salah satu malicious software yang dapat meng-encryption file, serta dapat menyebarkan diri ke komputer lain dalam jaringan yang sama. Jenis paket ransomware yang dapat diidentifikasikan sebagai ancaman adalah Crypto dan Locker, serta mempunyai beberapa jenis family

diantaranya, *Petya, WannaCry, Bad Rabbit, Cerber, CryptoWall* dan *CryptoLocker* (O.Imaji, 2019).

Intrusion Detection System merupakan sistem yang sangat penting dalam melakukan keamanan jaringan serta dapat mendeteksi kemungkinan adanya serangan oleh WannaCry. Teknik yang umum digunakan untuk mendeteksi pada Intrusion Detection System adalah sistem Rule base seperti attack signature dan attack anomaly. Akan tetapi teknik ini masih memiliki kelemahan seperti ketidakmampuan untuk men-denied paket lalu lintas yang masuk dalam jaringan enterprise. Intrusion Detection System dengan teknik deteksi attack signatures tidak bisa mendeteksi tipe serangan baru yang tidak ada pada database serangan. Sedangkan Intrusion Detection System menggunakan mekanisme attack anomaly mendeteksi beberapa variasi serangan baru, tetapi sering menghasilkan false alarms yang cukup besar (Rodrigues et al., 2017).

Deep Packet Inspection (DPI) merupakan Intrusion Detection System dengan pemanfaatan penyaringan paket data dengan memonitor lalu lintas aliran paket, yang berisikan informasi penting yang ada di header maupun payload. DPI dapat membedakan asal paket tersebut melalui header paket, bahkan dapat mengetahui aktifitas-aktifitas paket tersebut (Rodrigues

Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection pada Layanan SMK Negeri 1 Palembang et al., 2017). Identifikasian yang dilakukan memberikan informasi paket berdasarkan 7 Open System Interconnection (OSI) Layers, mulai dari Physical Layer sampai Application Layer. Pendeteksian paket akan diperiksa mulai dari header, 7 OSI Layer, dan payload, serta memungkinkan deteksi paket yang mengandung malicious signature dan anomali pada jaringan enterprise(Saad Hafeez B.Eng. & A, 2017). Dengan enkripsi lalu lintas paket yang dibuat oleh ransomware, DPI dapat melakukan klasifikasi trafik yang ter-enkripsi dengan Pattern Matching dengan, validasi TLSv yang mempunyai Field yang terdapat pada Record Content Type, Protocol Version, Handshake Type dan Service (Salim et al., 2016). Dengan menemukan lalu lintas yang berbahaya dan tak dikenal, DPI akan mengelompokkan fitur berupa atribut-atribut yang dimiliki paket ransomware. Seperti port vang diakses, url vang dibuka, serta aktifitasaktifitas yang ada di dalam paket tersebut (Grant & Parkinson, 2018).

Penelitian (Cheng & Watson, 2018), membahas permasalahan pengidentifikasian *Malware* menggunakan DPI dengan arsitektur *Deep Learning*, untuk memproses *payload* dari perilaku *malware* dengan tanda paket *benign*. Dengan menggunakan *Deep Learning*, penelitian ini dapat memprediksi *traffic* pada *host* dan *client*, serta membangun fungsi seperti *Intrusion Detection System* (IDS).

Pada penelitian yang dilakukan (Velea & Margarit, 2017), membahas tentang visualisasi menggunakan pararel *k-means* pada lalu lintas jaringan, dengan *Shallow Packet Inspection* (SPI). Visualisasi *k-means* hanya yang menghasilkan *average packet interval, data transfered, duration,* dan *packet count*, dengan dibagi beberapa *centroids*.

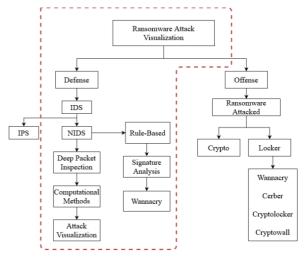
Dari beberapa ulasan diatas, Intrusion Detection System dengan metode Deep Packet Inspection dapat menggunakan open-source tools yang dikenal dengan Snort dengan mengaplikasikan rule based dari Deep Packet Inspection. **OpenDPI** merupakan pengembangan dari Snort, yang mengadaptasi pada pengidentifikasian serta pendeteksian protokol komunikasi yang berfokuskan pada lalu lintas internet. Dari hasil yang didapat dalam proses deteksi Snort akan divisualisasikan dalam bentuk diagram dan data hasil benign pada paket behavior dan signature ransomware.

2. Metode Penelitian

Pada tahap pertama penelitian ini adalah perancangan sistem yang akan digunakan seperti penginstallan perangkat lunak dan perangkat keras yang akan digunakan untuk membantu sistem deteksi yang dilakukan oleh DPI.

- Sistem deteksi yang digunakan untuk mendeteksi serangan *Ransomware WannaCry* akan menerapkan sistem *Defense* untuk mengetahui seberapa banyak dan berbahayanya *Ransomware WannaCry*
- Intrusion Detection System (IDS) akan melakukan tindakan dalam mendeteksi serangan melalui Network-based Intrusion Detection System (NIDS) yang telah menerapkan rule based signature dari Ransomware WannaCry
- Kemudian Sistem Deep Packet Inspectio (DPI) melakukan tindakan pengecekan dan screening informasi paket yang melewati jaringan enterprise tersebut.
- Sistem DPI akan melakukan computational method yang dimiliki oleh sistem rule-based signature dalam paket Ransomware WannaCry dalam status "active"
- Setelah paket Ransomware WannaCry terdeteksi melewati jaringan enterprise, Deep Packet Inspection (DPI) akan melakukan Attack Visualization berupa informasi packet header dan objek gambar yang mengetahui seberapa banyak objek Ransomware WannaCry menyamar.

Berikut ini adalah diagram metode penelitian yang dilakukan oleh Snort dan *Deep Packet Inspection* dalam melakukan tindakan pendeteksian *Ransomware WannaCry*.

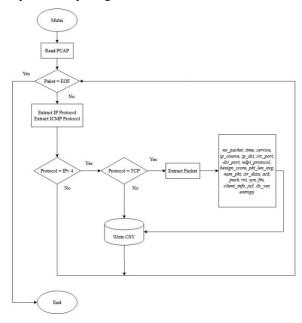


Gambar 2.1. Metode Diagram Penelitian

Kemudian setelah berhasil mendeteksi adanya ancaman *Ransomware WannaCry*, *Deep Packet Inspection* akan melakukan *Collecting* data. Informasi data serangan yang dilakukan *Ransomware WannaCry* akan menghasilkan data format *.pcap*. Format tersebut tidak dapat digunakan untuk mendapatkan informasi yang akurat, akan tetapi harus melakukan proses

ekstraksi agar dapat mendapatkan informasi yang diinginkan. Tahapan selanjutnya adalah melakukan *Feature Extraction*.

Proses *Feature Extraction* adalah proses ekstraksi akan mendapatkan hasil berupa data *xls* yang dapat dibaca dan dipahami, serta dapat diproses lebih lanjut dalam proses visualisasi data menjadi data yang matang dan siap disajikan. Proses alur kerja *Feature Extraction* dapat dilihat pada gambar berikut ini.



Pada tahapan selanjutnya adalah mengoreksi hasil dari deteksi DPI, dengan mengelompokkan atributatribut dari serangan *ransomware* sebagai pola serangan. Setelah mendapatkan atribut-atribut jenis serangan paket *ransomware*, akan diklasifikasi dengan paket normal. Algoritma visualisasi yang telah disediakan akan digunakan untuk menguji total paket yang menjadi *alert*. Pada tahap akhir, akan dilakukan visualisasi data paket dalam bentuk diagram

3. Hasil dan Pembahasan

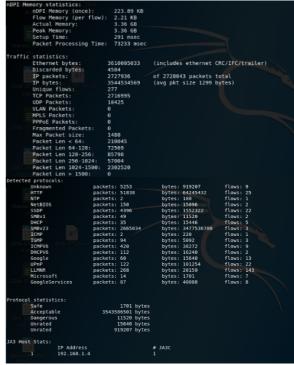
1. Hasil Pendeteksian Deep Packet Inspection

Hasil dari pendeteksian yang dilakukan Deep Packet Inspection dapat digunakan untuk mengenali sebuah paket serangan, salah satunya adalah dengan pola. Pola paket serangan dapat berupa atribut-atribut unik yang dimiliki sebuah paket misalnya protokol yang digunakan, port source, port destination, TLSv, serta benign score. Pada penelitian ini pola paket serangan akan digunakan sebagai pengklasifikasian awal. Untuk mendapatkan pola serangan ada beberapa langkahlangkah pada penelitian tugas akhir yaitu sebagai berikut:

 Mendeteksi serangan Ransomware untuk dibaca oleh sistem DPI sehingga

- mendapatkan *alert* yang berisi informasi serangan.
- Hasil pendeteksi yang dilakukan DPI awal berupa informasi protokol yang digunakan pada headers paket, kemudian dapat dibandingkan dengan raw data dan apakah ada paket lain pada hasil deteksi serangan.
- Mencari atribut-atribut unik seperti TLSv dan JA3 dan Fingerprint maka dapat dicari dari hasil feature extraction, untuk memastikan bahwa paket tersebut adalah benar serangan.

Kemudian atribut yang dihasilkan pada proses deteksi akan divalidasi dengan hasil ekstraksi, dengan memvalidasi waktu yang didapatkan dengan memanfaatkan atribut *time*. Berikut gambar 3.4 adalah proses validasi serangan dengan data ekstraksi.



Gambar 3.1. Hasil Dari Pendeteksian DPI

2. Data Hasil Ekstraksi

Hasil dan Pada proses ekstraksi dataset SMK Negeri 1 Palembang berisi berbagai macam protokol, diantaranya adalah HTTP, HTTPS, NTP, NetBIOS, SSDP, SMBv1, ICMP, IGMP, Google, UPnP, dan LLMNR. Dan atribut yang terdapat pada saat ekstraksi dilakukan antaranya, flow_ID, src_IP, src_port, dst_IP, dst_port, protocol, dan lainnya. Pada gambar 4.3 berikut ini merupakan salah satu hasil dari Pendeteksian yang dilakukan nDPI terhadap SMK Negeri 1 Palembang Beberapa paket yang telah di ekstraksi antara lain, protokol yang digunakan, ip_source, port_destination, ip_destination, port_destination,

DOI: https://doi.org/10.31004/ijmst.v1i2.142 Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0) benign_score, total packet, TLSv dan JA3. Pada gambar berikut adalah hasil Feature Extraction dari pendeteksian DPI. Gambar berikut merupakan hasil dari ekstraksi data yang mengindikasikan adanya serangan Ransomware pada jaringan SMK Negeri 1 Palembang.

1	protocol src_ip	src_port.dst_ip	dst_port	ndpi_proto	benign_scc_t	to_s_pkts	s_to_c_pkts	tls_version	ja3c	tls_client	ja3s	tls_server	entropy
2	6 192.168.1.4	49170 192.168.1.5	445	NetBIOS.SMBv23	0	817459	1238158)	0		0	0
3	6 192.168.1.4	49186 192.168.1.5	445	NetBIOS.SMBv23	0	241956)	0		0	1.8
4	6 192.168.1.4	49181 130.205.193	. 80	HTTP	0	8752	41545	()	0		0	0
5	6 192.168.1.4	49175 130.206.193	. 80	HTTP	0	255	914)	0		0	0
6	17 192.168.1.4	1900 239,255,255	. 1900	SSDP	0	144	0)	0		0	4.73
7	17 192.168.1.5	1900 239.255.255	. 1900	SSDP	0	144	0)	0		0	4.78
8	6 192.168.1.5	49179 192.168.1.4	5357	HTTP	1.1	10	15)	0		0	0
9	6 192.168.1.5	49157 192.168.1.4	5357	HTTP	1.1	9	15)	0		0	0
10	6 192.168.1.5	49169 192.168.1.4	5357	HTTP	1.1	9	15)	0		0	0
11	6 192.168.1.5	49178 192.168.1.4	5357	HTTP	1.1	9	15)	0		0	0
12	6 192.168.1.5	49180 192.168.1.4	5357	HTTP	1.1	9	15)	0		0	0
13	6 192.168.1.5	49184 192.168.1.4	5357	HTTP	1.1	9	15)	0		0	0
14	6 192.168.1.4	49199 192.168.1.5	5357	HTTP	1.1	8	12)	0		0	0
15	17 192.168.1.4	56321 239.255.255	3702	UPnP	0	18	0)	0		0	3.57
16	17 192.168.1.5	61232 239.255.255	. 3702	UPnP	0	10	0)	0		0	2.638
17	6 192.168.1.4	49173 172.217.17.	443	TLS.GoogleServices	1.1	10	8	TLSv1.2	4d7a28d6	OK	f9a66afd	ld OK	2.234
18	17 192.168.1.4	60549 239.255.255	1900	SSDP	0	56	0)	0		0	5.175
19	17 192.168.1.5	137 192.168.1.25	137	NetBIOS	0	90	0)	0		0	3.052
20	6 192.168.1.4	49179 172.217.17.	443	TLS.GoogleServices	1.1	10	8	TLSv1.2	4d7a28d6	OK	f9a66afd	ld OK	2.244
21	17 192.168.1.3	67 255.255.255	. 68	DHCP	0	14	0)	0		0	1
22	17 192.168.1.5	61062 239.255.255	. 3702	UPnP	0	8	0)	0		0	0
23	17 192.168.1.5	65497 239.255.255	1900	SSDP	0	43	0)	0		0	5.175
24	6 192.168.1.4	49176 172.217.17.	443	TLS.GoogleServices	1.1	9	7	TLSv1.2	4d7a28d6	OK	f9a66afd	ld OK	1.844
25	6 192 169 1 4	49192 172 217 17 :	442	TIS GoodleSequires	1.1	9		TI Sut 2	Ad7+2946	or	f9a66afd	HOY	1.846

Gambar 3.2. Data hasil ekstraksi

3. Pengenalan pola serangan *Ransomware* WannaCry

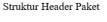
Pada tahap selanjutnya berupa pengenalan pola serangan Ransomware yang dilakukan pada Bank Syariah Indoensia. Serangan yang dilakukan Ransomware ini merupakan serangan WannaCry yang melalui protokol TCP. Alert yang dapat dideteksi nDPI berupa protokol TCP, ip source, port source, ip destination, port destination, dan TLSv1.2. DPI telah mendeteksi beberapa content yang digunakan payload paket, seperti *.google.com, *.android.com, dan lainnya. nDPI juga telah mendeteksi adanya JA3 yang digunakan pada Client Hello dan Server Hello dalam melakukan komunikasi. Pada gambar 3.3. adalah salah satu serangan Ransomware WannaCry dengan tabel informasi payloadnya yang diperoleh dari deteksi DPI.

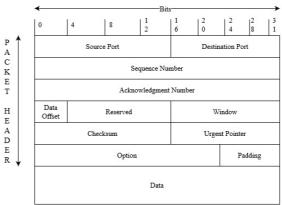


Gambar 3.3. Serangan Ransomware Terhadap SMK Negeri 1 Palembang

4. Struktur Packet Header

Banyak serangan jaringan tidak dapat dideteksi dengan pencocokan string, karena dasarnya tidak menampilkan tanda atau pola dalam payload. Ini berarti, untuk setiap serangan, muatan yang berbeda dapat digunakan sehingga proses pencocokan tanda tangan gagal. Dalam kasus seperti itu, untuk mendeteksi serangan ini, pendekatan lain harus diambil. Salah satunya adalah untuk menganalisis konten *header* paket yang dapat menyajikan anomali, memberikan bukti serangan atau penyelidikan sedang berlangsung.





Gambar 3.3. Struktur Header Paket.

Tabel 1. Informasi Packet Header

A 4	Packet Header						
Atribut	Serangan						
Port Source	mempunyai size 2 byte atau (16 bit) yang berperan untuk mengindikasi asal muasal protocol pada lapisan application yang akan mengirimkan bagian dari TCP yang berhubungan. Perpaduan antara field IP						
Address Source	pada header IP dan field port source pada field header TCP dapat disebut sebagai sumber soket, artinya pada sebuah alamat global dari seluruh jaringan dapat dikirim hanya dengan bagian dari port source.						
Port Destinatio n	mempunyai size 2 byte atau (16 bit) yang berperan untuk mengindikasi tujuan dari protocol pada lapisan application yang memberikan bagian dari TCP berhubungan, artinya pada alamat global akan mengirimkan bagian dari port destination.						
Sequence num	mempunyai <i>size</i> 4 byte atau (32 bit) yang mengindikasi urutan nomor dari octet pertama pada paket data di dalam sebuah bagian TCP yang akan dikirimkan.						
Acknowle- dgment num	mempunyai size 4 byte atau (32 bit). Acknowledgment number atau ACK yang mengindikasi urutan nomor dari octet kemudian dalam aliran byte dapat diterima oleh pengirim dari sisi client untuk pengiriman selanjutnya. ACK sangatlah penting untuk bagian-bagian TCP dengan flag ACK yang diatur ke angka 1.						
Offset Data	mempunyai <i>size</i> 1 byte atau (4 bit), yang dapat mengindikasi data dari setiap bagian TCP pada saat dimuat.						
Reserved	mempunyai <i>size</i> (6 bit), pada saat pengiriman bagian TCP akan di atur kedalam bit pada angka 0.						
Flags	mempunyai <i>size</i> (6 bit), yang dapat mengindikasi flag-flag dari TCP						

	Packet Header					
Atribut	Serangan					
	sebagai Ack, Push, Reset, Urgent, Syn, dan Fin.					
Window	mempunyai size 2 byte atau (16 bit), yang dapat mengindikasi jumlah dari byte yang sebenarnya dimiliki oleh buffer dari host penerima bagian yang bersangkutan. Tujuannya adalah untuk menyusun data dan mengatur lalu lintas data atau control flow					
Checksum	mempunyai size 2 byte atau (16 bit), yang dapat melakukan pemeriksaan integritas dari bagian TCP (payload dan header). Angka dari field checksum akan diset ke angka 0, selama proses perhitungan pada checksum.					
Urgent Pointer	mempunyai size 4 byte atau (16 bit), yang melambangkan lokasi paket data yang dianggap penting atau "urgent" dalam bagiannya					
Padding and Option	mempunyai <i>size</i> 4 byte (32 bit), yang berperan seperti tempat penampung data dari beberapa opsi tambahan dalam bagian TCP					

5. Pola serangan Ransomware WannaCry

Pola serangan berupa Fingerprint Ransomware WannaCry pada dataset SMK Negeri 1 Palembang menggunakan Payload dan Header. Pada header paket terdapat beberapa informasi penting mengenai IP dan Port yang dituju. Sedangkan pada payload mempunyai konten variabel dan TLSv yang digunakan saat handshake antara Client dan Server. Dari TLSv dan Cipher yang digunakan akan membentuk string MD5 kemudian di hash untuk mendapatkan JA3 Fingerprint. Berikut informasi pada client dan JA3C pada serangan paket ransomware wannacry. Berikut kecocok dari hasil pada struktur data dari Packet Header yang dimiliki Ransomware Wannacry.

			ndpi_ndpi_proto							in client_in				als
6 192.168.1.4	49181 130.206.193.1	80	7 HTTP	r1sn-gxqpg		50256 1		1	2	0	-			
6 192.168.1.4	49175 130.206.193.1	80	7 HTTP	r2sn-griqpg	0	1168	333	1	2	0	-			
6 192.168.1.5	49179 192.168.1.4	5357	7 HTTP	192.168.1.4	1.1	24	3	0	2	2				
6 192.168.1.5	49157 192.168.1.4	5357	7 HTTP	192.168.1.4	1.1	23	3	0	2	2				
6 192.168.1.5	49169 192.168.1.4	5357	7 HTTP	192.168.1.4	1.1	23	3		2	2	1			
6 192.168.1.5	49178 192.168.1.4	5357	7 HTTP	192.168.1.4	1.1	23	3	0	2	2	1			
6 192.168.1.5	49180 192.168.1.4	5357	7 HTTP	192,168,1,4	1.1	23	3	0	2	2				
6 192.168.1.5	49184 192.168.1.4	5357	7 HTTP	192,168,1,4	1.1	23		0	2	2				
6 192.168.1.4	49199 192.168.1.5	5357	7 HTTP	192,168,1.5	1.1	19	3	0	2	2)		
6 192.168.1.4	49173 172.217.17.3	443	91.2 TLS.Google	Services	1.1	17	9	1	2	0 update.g	CTLSv1.2	4d7a28d6f2263	ed61de68ca66eb011e3	19a66afdd11499d415ca470974ec00
6 192.168.1.4	49179 172-217-17-3	443	91.2 TLS.Google	Services	1.1	17	8	1	2	0 update.g	oTLSv1.2	4078280672263	ed61de68ca66eb011e3	f3a66afdd1f439d415ca470974ec00
6 192.168.1.4	49176 172.217.17.3	443	91.2 TLS.Google	Services	1.1	15	7	1	2	0 update.p	cTLSv1.2	4d7x29d6f2263	ed\$1de88ca66eb011e3	f9a66afdd1f499d415ca470974ec00
6 192,168,1.4	49192 172,217,17,3	443	91.2 TLS.Google	Services	1.1	34	7	1	2	0 update.s	cTL5v1.2	4d7x28d6f2263	ed51de5Sca55eb011e1	f3e56efdd15939d415ce470974ec00
6 192,168,1.4	49167 192,168,1.5	2569	7 HTTP	192,166,1.5		12	3	0	2	2	-	2		
6 192,168,1,5	49162 192,168,1,4	2869	7 HTTP	192,168,1,4	1.1	12	3	0	2	2)		
6 192.168.1.5	49167 192.168.1.4	2869	7 HTTP	192,168,1,4	1.1	12	3		2	2				
6 192.168.1.5	49163 192.168.1.4	2869	7 HTTP	192,168,1,4	1.1	12	3	1	2	0		1		
6 192 168 1.4	49168 192,168,1.5	2869	7 HTTP	192,168,1,5	1.1	11		i	2	0				
6 192.168.1.5	49168 192,168,1.4	2869	7 HTTP	192,168,1.4	1.1	11			2	0				
6 192.168.1.4	49177 172.217.17.3		91.2 TLS.Google		1.1	13		i	2				-457-4-550-550-6777-7	f9a56afdd15499d415ca470974ec00
6 192.168.1.4	49172 216.58.201.14		91.1 TLS.Google	261 77.01	1.1	14	7	i	2					f3a66afdd1f439d413ca470974ec0
6 192.168.1.4	49178 216.58.201.14		91.1 TLS.Google		1.1	12	7		2					19a66afdd15499d415ca470974ec00
					1.1	6	2		2	0 cilents2.	O ILSVI.Z		#G01D400C400HDOTT#2	194004100114990413044709744000
6 192.168.1.4	49180 172.217.168.1		7.13 HTTP.Googl		1.1	6	2		2	0				
1988_ 692,1201 1988_ 692,1286	19 192,168,1,4	13	10.206.193.188	TCP 1CP	54	49181	- 30	[ACK	1 56	p+15814 Ack	35326168	q=1581_ 49181 Nin=1_ 49181	00 88	
1988. 602.1286 1988. 602.1290 1988. 602.1295	19 192.168.1.4 13 192.168.1.4 13 192.168.1.4	13 13 13	10.286.193.188 10.286.193.186 10.286.193.180	1CP 1CP 1CP	94 94 94	49181 49181 49181	- 80 - 50 - 00	[ACK [ACK [ACK	56 50 50	9=15814 Ack p=15814 Ack p=15814 Ack	35326168 35327628 35374346	Hin-1 49181 Hin-6 49181 Hin-1 49181	50 50	
1988 602.1206 1988 602.1200 1988 602.1205 1988 602.1209	19 192.168.1.4 53 192.168.1.4 13 192.168.1.4 18 192.168.1.4	13 12 13	10.286.193.188 10.286.193.188 10.286.193.180 10.286.193.188	TCP TCP TCP	54 54 54	49181 49181 49181 [TCP N	- 88 - 88 - 88 - 88 Endow	[ACX [ACX [ACX Upd	56 50 50 16	9=15814 Ack 9=15814 Ack 9=15814 Ack 49181 = 88	35326168 35327628 35374340 [ACK] Se	Hin=1 49181 Hin=6 49181 Hin=1 49181 q=1581 49181	69 00 00 88	
1988. 602.1206 1988. 602.1200 1988. 602.1205 1988. 602.1209 1988. 602.1301	19 192.168.1.4 33 192.168.1.4 33 192.168.1.4 33 192.168.1.4 38 192.168.1.4 47 192.168.1.4	13 12 13 13	10.286.193.188 10.286.193.188 10.286.193.188 10.286.193.188 10.286.193.188	1CP 1CP 1CP 1CP	54 54 54 54	49181 49181 49181 [TCP N 49181	- 88 - 88 - 88 - 88 Endow - 88	[ACX [ACX [ACX Upd [ACX	56 50 50 16 16 50	p=15814 Ack p=15814 Ack p=15814 Ack 49181 + 88 p=15814 Ack	35326168 35327628 35374346 [ACK] Se 35394788	Nin=1 49181 Nin=6 49181 Nin=1 49181 q=1581 49181 Nin=5 49181	50 50	
1988 602.1206 1988 602.1200 1988 602.1205 1988 602.1209	19 192.168.1.4 55 192.168.1.4 55 192.168.1.4 56 192.168.1.4 57 192.168.1.4 59 192.168.1.4	13 13 13 13 13	10.286.193.188 10.286.193.188 10.286.193.180 10.286.193.188	TCP TCP TCP	94 94 94 94	49181 49181 49181 [TCP N 49181 [TCP N	- 88 - 88 - 88 Endow - 88 Endow	[ACK [ACK Upd [ACK Upd	56 50 50 16 16 50 10	\$15814 Ack \$15814 Ack \$15814 Ack \$15814 Ack \$15814 Ack \$15814 Ack \$15814 Ack	35326168 35327628 35374346 [ACK] Se 35394768 [ACK] Se	Nin-1. 49181 Nin-6. 49181 Nin-1. 49181 Nin-1. 49181 Nin-5. 49181 Nin-5. 49181 q-1581. 49181	50 50 50 50 50	
1988. 602.1290 1988. 602.1290 1988. 602.1295 1988. 602.1299 1988. 602.1301 1988. 602.1301 1988. 602.1305	19 192.168.1.4 33 192.168.1.4 33 192.168.1.4 38 192.168.1.4 38 192.168.1.4 39 192.168.1.4 30 192.168.1.4 30 192.168.1.4	13 13 13 13 13 13 13 13	10,206,193,186 10,206,193,186 10,206,193,186 10,206,193,186 10,206,193,186 10,206,193,186 10,206,193,186	TCP TCP TCP TCP TCP TCP TCP	54 54 54 54 54 54	49181 49181 49181 [TCP N 49181 [TCP N	- 88 - 50 - 90 Endow - 50 Endow Endow	[ACK [ACK [ACK Upd [ACK Upd Upd	50 50 50 50 50 10 10 10	9-15814 Ack 9-15814 Ack 9-15814 Ack 49181 - 80 9-15814 Ack 49181 - 80 49181 - 80	-35326168 -35327628 -35374346 [ACK] Se -35394788 [ACK] Se [ACK] Se [ACK] Se	Nin=1 49181 Nin=6 49181 Nin=6 49181 Nin=5 49181 Nin=5 49181 Nin=5 49181 S318 A 49181 S318 A 49181	50 50 50 50 50 50 50	
1988. 602.1205 1988. 602.1205 1988. 602.1205 1988. 602.1209 1988. 602.1305 1988. 602.1305 1988. 602.1305 1988. 602.1305	19 192.168.1.4 33 192.168.1.4 33 192.168.1.4 33 192.168.1.4 38 192.168.1.4 47 192.168.1.4 59 192.168.1.4 50 192.168.1.4 50 192.168.1.4 50 192.168.1.4	13 13 13 13 13 13 13 13 13 13 13 13 13 1	10,286,193,185 10,286,193,185 10,286,193,186 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185	10P 10P 10P 10P 10P 10P 10P 10P	54 54 54 54 54 54 54	49181 49181 49181 [TCP N 49181 [TCP N [TCP N	- 88 - 52 - 92 Endow - 59 Endow Endow Endow	[ACK [ACK Upd Upd Upd Upd Upd	50 50 50 50 50 10 10 10 10	9-15814 Ack 9-15814 Ack 9-15814 Ack 9-15814 Ack 99181 - 80 9-15814 Ack 49181 - 80 49181 - 80 49181 - 80	35328168 35327628 35374346 [ACK] Se 35394780 [ACK] Se [ACK] Se [ACK] Se [ACK] Se	Hin=1 49181 Hin=6 49181 Hin=1 49181 Hin=1 49181 Hin=5 49181 Hin=5 49181 Q=1561 49181 Q=1561 49181 Q=1561 49181 Q=1561 49181	50 50 50 50 50 50 50	
198E. 602.1296 198E. 602.1290 198E. 602.1295 198E. 602.1295 198E. 602.1305 198E. 602.1305 198E. 602.1305 198E. 602.1305 198E. 602.1400	19 192.168.1.4 133 192.168.1.4 134 192.168.1.4 188 192.168.1.4 17 192.168.1.4 19 192.168.1.4 19 192.168.1.4 19 192.168.1.4 19 192.168.1.4 19 192.168.1.4 10 192.168.1.4	13 13 13 13 13 13 13 13 13 13 13 13 13 1	18, 286, 193, 188 19, 286, 193, 188	109 109 109 109 109 109 109 109 109	9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	49181 49181 (FCP N 49181 (FCP N (FCP N (FCP N 49181	- 88 - 80 - 80 - 80 Lindow Lindow Lindow Lindow - 80	[ACX [ACX Upd [ACX Upd Upd Upd Upd [ACX	Sec Sec	p=15814 Ack p=15814 Ack p=15814 Ack 09181 = 80 p=15814 Ack 49181 = 80 49181 = 80 49181 = 80 49181 = 80 q=15814 Ack	35328168 35327628 -35374346 [ACK] Se -35394760 [ACK] Se [ACK] Se [ACK] Se [ACK] Se	kin=1 49181 kin=6 49181 kin=6 49181 kin=1 49181 kin=5 49181 kin=5 49181 q=1561 49181 q=1561 49181 q=1561 49181 kin=1 49181 kin=1 49181	50 50 50 50 50 50 50	
1988. 602.1296 1988. 602.1290 1988. 602.1295 1988. 602.1295 1988. 602.1391 1988. 602.1300 1988. 602.1300 1988. 602.1400 1988. 602.1400 1988. 602.1400	192.168.1.4 153 192.168.1.4 153 192.168.1.4 188 192.168.1.4 188 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 192.168.1.4 193.168.1.4 193.168.1.4 193.168.1.4	13 12 13 13 13 13 14 13 14 13 14 14 15 14 15 14 15 16 16 17 18 18 18 18 18 18 18 18 18 18 18 18 18	10,286,193,185 10,286,193,185 10,286,193,186 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185	10P 10P 10P 10P 10P 10P 10P 10P 10P 10P	94 94 94 94 94 94 94	49181 49181 (FCP N 49181 (FCP N (FCP N (FCP N 49181	- 80 - 80 - 80 Indov - 50 Indov Indov Indov - 80	[ACX [ACX [ACX Upd [ACX Upd Upd Upd Upd Upd	Se Se Se Se Se Se (19) (19)	q=15814 Ack q=15314 Ack q=15314 Ack q=15314 Ack q=15314 Ack 49131 = 30 q=15314 30 q=15314 Ack q=1531 = 30 q=15314 Ack	35328168 -55327628 -35374346 [AOX] Se -55394760 [AOX] Se [AOX] Se [AOX] Se [AOX] Se	Min=1. 49181 Min=6. 49181 Min=6. 49181 Min=1. 49181 Hin=5. 49181 Min=5. 49181 Q=1581. 49181 Q=1581. 49181 Q=1581. 49181 Q=1581. 49181 Min=1. 49181 Min=1. 49181	50 50 50 50 50 50 50	
198E. 602.1296 198E. 602.1290 198E. 602.1295 198E. 602.1295 198E. 602.1305 198E. 602.1305 198E. 602.1305 198E. 602.1305 198E. 602.1400	19 192.168.1.4 33 192.168.1.4 33 192.168.1.4 38 192.168.1.4 39 192.168.1.4 17 192.168.1.4 17 192.168.1.4 18 192.168.1.4 19 192.168.1.4 19 192.168.1.4 10 192.168.1.4 10 192.168.1.4 10 192.168.1.4 10 192.168.1.4 10 192.168.1.4	13 12 13 13 13 13 13 14 13 14 13 14 15 15 16 17 18 18 18 18 18 18 18 18 18 18 18 18 18	10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185 10,286,193,185	109 109 109 109 109 109 109 109 109	94 94 94 94 94 94 94 94 94 94 94 94 94 9	49181 49181 49181 (FICP N 49181 (FICP N (FICP N 49181 (FICP N 49181	- 80 - 80 - 80 Ledow - 50 Ledow Indow Ledow - 90 Endow Ledow - 90 Endow	[ACX [ACX Upd [ACX Upd Upd Upd [ACX Upd	Se Se Se Se Se Se Se ste Se Se Se Se Se Se Se S	9-15814 Ack 9-15814 Ack 9-15814 Ack 49181 - 30 9-15814 Ack 49181 - 30 101 - 30	-35327628 -35327628 -35374346 [AOX] Se -35394760 [AOX] Se [AOX] Se [AOX] Se [AOX] Se -35405300 [AOX] Se	kin=1 49181 kin=6 49181 kin=6 49181 kin=1 49181 kin=5 49181 kin=5 49181 q=1561 49181 q=1561 49181 q=1561 49181 kin=1 49181 kin=1 49181	50 50 50 50 50 50 50 50 50 50 50	
1984 002.1290 1985 002.1290 1986 002.1290 1986 002.1390 1986 002.1390 1986 002.1390 1986 002.1390 1986 002.1400 1986 002.1400 1986 002.1400 1986 002.1400 1986 002.1400 1986 002.1400 1989 002.1400	19 192.188.1.4 33 192.168.1.4 33 192.168.1.4 33 192.168.1.4 38 192.188.1.4 38 192.188.1.4 39 192.188.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4	13 12 13 13 13 13 13 13 13 13 13 13 13 13 13	10, 206, 193, 188 10, 206, 193, 180 10, 206, 193, 180	100 100 100 100 100 100 100 100 100 100	94 94 94 94 94 94 94 94 94 94 94 94 94 9	49181 49181 49181 [FCP N 49181 [TCP N [TCP N 49181 [TCP N 49181 [TCP N 49181	- 88 - 88 - 88 Endow - 88 Endow Endow - 88 Endow - 88 Endow - 88	[ACX [ACX Upd Upd Upd Upd Upd [ACX Upd [ACX	Se Se Se Se Se Se Se Se	\$\text{15814} Ack \(\frac{1}{2}\) \(\frac{1}{2	-95326168 -95327628 -95374346 [AOK] Se -95394768 [AOK] Se [AOK] Se -95465366 [AOK] Se -95465366 [AOK] Se	Min=1, 49181 Min=6, 49181 Min=6, 49181 Min=1, 49181 Min=5, 49181 Min=5, 49181 Min=5, 49181 Min=1, 49181	100 100 100 100 100 100 100 100 100 100	
1984 002.1200 1984 002.1200 1988 002.1200 1988 002.1200 1988 002.1200 1988 002.1301 1988 002.1301 1988 002.1300 1988 002.1300 1988 002.1400 1988 002.1400 1988 002.1400 1988 002.1400	19 192.168.1.4 33 192.168.1.4 33 192.168.1.4 38 194.168.1.4 38 194.168.1.4 39 192.168.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4	11 12 13 13 13 13 13 13 13 13 13 13 13 13 13	10 , 206 , 193 , 188 10 , 206 , 193 , 188	10 10 10 10 10 10 10 10 10 10 10 10 10 1	94 94 94 94 94 94 94 94 94 94 94 94 94 9	49181 49281 49281 [TCP N 49282 [TCP N [TCP N 49281 [TCP N 49281 [TCP N 49281 [TCP N 49281	- 88 - 50 - 50 Indow - 50 Indow Indow - 50 Indow - 90 Indow - 90 Indow - 90 Indow - 90 Indow - 50 Indow - 50 Indow Indow - 50 Indow	[ACX [ACX Upd Upd Upd Upd Upd [ACX Upd Upd Upd Upd Upd	Sec	p=15814 Ack p=15814 Ack p=15814 Ack p=15814 Ack p=15814 Ack 49181 = 80 49181 = 80 49181 = 80 q=15814 Ack 31 = 80 q=15814 Ack 49181 = 80 q=15814 Ack 49181 = 80 q=15814 Ack 49181 = 80 q=15814 Ack	-95326168 -95327628 -95374346 [AOK] Se -953994780 [AOK] Se [AOK] Se [AOK] Se -95465300 [AOK] Se -955465300 [AOK] Se -955465300 [AOK] Se -955465300 [AOK] Se	Min-L 49181 Min-K, 49181 Min-K	100 100 100 100 100 100 100 100 100 100	
1984 002.1200 1985 002.1200 1986 002.1200 1986 002.1200 1986 002.1300 1986 002.1300 1986 002.1300 1986 002.1400 1986 002.1400 1986 002.1400 1986 002.1400 1986 002.1400 1986 002.1400 1986 002.1400 1986 002.1400 1989 002.1420 1989 002.1420	19 192.168.1.4 33 192.168.1.4 33 192.168.1.4 33 192.168.1.4 38 192.168.1.4 38 192.168.1.4 39 192.168.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 30 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4 31 192.168.1.4	13 12 13 13 13 13 13 13 13 13 13 13 13 13 13	10, 296, 193, 188 10, 206, 193, 189 10, 206, 193, 180 10, 206, 193, 180	100 100 100 100 100 100 100 100 100 100	94 94 94 94 94 94 94 94 94 94 94 94 94 9	49181 49281 49281 [FCP N 49281 [TCP N [TCP N 49281 [TCP N 49281 [TCP N 49281 [TCP N 49281	- 80 - 90 - 90 indow - 50 indow indow - 90 erosis indow - 90 erosis e	[ACX [ACX Upd. Upd. Upd. Upd. Upd. Upd. Upd. Upd.	Sec	+15814 Ack +15814 Ack	-35326168 -35327628 -35327636 [AOK] Se -35394760 [AOK] Se [AOK] Se [AOK] Se -35405300 [AOK] Se -35540540 [AOK] Se -35540540 [AOK] Se -35540540	Min-L 49181	100 100 100 100 100 100 100 100 100 100	
1984 602.1200 1988 002.1200 1988 002.1200 1988 602.1200 1988 602.1200 1988 602.1300 1988 602.1300 1988 002.1300 1988 002.1400 1988 002.1400 1988 002.1400 1988 002.1410 1988 002.1410	19 192,166,1,4 33 192,166,1,4 33 192,166,1,4 33 192,166,1,4 33 192,166,1,4 34 192,166,1,4 35 192,166,1,4 36 192,166,1,4 36 192,166,1,4 36 192,166,1,4 36 192,166,1,4 36 192,166,1,4 36 192,166,1,4 37 192,166,1,4 37 192,166,1,4 37 192,166,1,4 37 192,166,1,4 37 192,166,1,4 37 192,166,1,4 37 192,166,1,4 37 192,166,1,4 37 192,166,1,4 37 192,166,1,4 38 192,166,1,4 39 192,166,1,4 30 192,166,1,4	11 12 12 13 13 13 13 13 13 13 13 13 13 13 13 13	10, 296, 193, 188 10, 206, 193, 180 10, 206, 193, 180	100 100 100 100 100 100 100 100 100 100	34 34 34 34 34 34 34 34 34 34 34 34 34 3	49181 49281 49281 (FICP W 49281 (FICP W (FICP W 49281 (FICP W 49281 (FICP W 49281 (FICP W 49281 (FICP W 49281	- 88 - 82 - 82 Indow - 82 Indow - 82 Indow - 82 Indow - 82 Indow - 82 Indow - 82 Indow - 82	[ACK Upd. Upd. Upd. Upd. Upd. Upd. Upd. Upd.	Sec	9-15814 Ack 9-15814 Ack 9-15814 Ack 99181 - 80 9-15814 Ack 49181 - 80 9-15814 Ack 49181 - 80 9-15814 Ack 9-15814 Ack	-35326168 -35327628 -353274346 [AOK] Se -35394763 [AOK] Se [AOK] Se -35465360 [AOK] Se -35540546 (AOK] Se -35540546	kib=L 49181 kib=L 49181 kib=L 49181 kib=L 49181 4918	100 100 100 100 100 100 100 100 100 100	
1984 002.1200 1985 002.1200 1986 002.1200 1986 002.1200 1986 002.1200 1986 002.1300 1986 002.1300 1986 002.1300 1986 002.1300 1986 002.1400 1986 002.1400 1986 002.1400 1986 002.1400 1986 002.1400 1989 002.1400 1989 002.1400 1989 002.1400 1989 002.1400 1989 002.1400 1989 002.1400 1989 002.1400 1989 002.1400 1989 002.1400	19 19: 195.185.1.4 33 190.165.1.4 33 190.165.1.4 33 190.165.1.4 33 190.165.1.4 34 190.165.1.4 17 190.165.1.4 18 190.165.1.4 18 190.165.1.4 18 190.165.1.4 190.190.165.1.4 190.190.165.1.4 190.190.165.1.4 190.190.105.1.4 190.190.105.1.4 190.190.105.1.4 190.190.105.1.4 190.190.105.1.4 190.190.105.1.4 190.190.105.1.4 190.190.105.1.4 190.190.105.1.4 190.190.105.1.4 190.190.105.1.4	13 12 13 13 13 13 13 13 13 13 13 13 13 13 13	10 , 206 , 193 , 126 10 , 206 , 193 , 126 10 , 206 , 193 , 126 10 , 206 , 193 , 186 10 , 206 , 193 , 186	100 100 100 100 100 100 100 100 100 100	94 94 94 94 94 94 94 94 94 94 94 94 94 9	49181 49281 49281 (FCP W 49281 (FCP W (FCP W 49281 (FCP W 49281 (FCP W 49281 (FCP W 49281 (FCP W 49281	- 88 - 82 - 82 Indow - 82 Indow Indow - 82 Indow In	[ACK Upd. Upd. Upd. Upd. Upd. Upd. Upd. Upd.	Sec	\$15314 Ack	-35326166 -35327626 -353274346 [AOK] 56 -35394760 [AOK] 56 -35405300 [AOK] 56 -35405300 [AOK] 56 -35505340 [AOK] 56 -35505340 [Min-6. 49181 Min-6. 49181 Min-6. 49181 Min-1. 40181 Min-1. 40181 Min-1. 40181 Min-6. 49181 Min-	200 000 000 000 000 000 000 000 000 000	
1984 602.1200 1988 002.1200 1988 002.1200 1988 602.1200 1988 602.1200 1988 602.1300 1988 602.1300 1988 002.1300 1988 002.1400 1988 002.1400 1988 002.1400 1988 002.1410 1988 002.1410	19 192,186,1.4 33 192,186,1.4 33 192,186,1.4 33 192,186,1.4 34 192,186,1.4 35 192,186,1.4 36 192,186,1.4 36 192,186,1.4 36 192,186,1.4 36 192,186,1.4 36 192,186,1.4 36 192,186,1.4 36 192,186,1.4 36 192,186,1.4 37 192,186,1.4 37 192,186,1.4 37 192,186,1.4 37 192,186,1.4 37 192,186,1.4 37 192,186,1.4 37 192,186,1.4	13 13 13 13 13 13 13 13 13 13 13 13 13 1	10, 296, 193, 188 10, 206, 193, 180 10, 206, 193, 180	100 100 100 100 100 100 100 100 100 100	94 94 94 94 94 94 94 94 94 94 94 94 94 9	49181 49282 49282 (FCP N 49282 (FCP N (FCP N 49282 (FCP N 49281 (FCP N 49281	- 88 - 82 - 82 Ledow - 82 Ledow Ledow - 82 Ledow - 82 Ledow	[ACK Upd	Sec	\$15814 Ack \$15814 Ack \$15814 Ack \$15814 Ack \$49181 - 30 \$15814 Ack \$15814	-35326166 -35327622 -35374346 [AOK] 56 -35394763 [AOK] 56 [AOK] 56 -35495363 [AOK] 56 -3549546 -355496 -35549 -3	kib=L 49181 kib=L 49181 kib=L 49181 kib=L 49181 4918	100 100 100 100 100 100 100 100 100 100	
1988. 692, 1296 1988. 692, 1295 1988. 692, 1295 1988. 692, 1295 1988. 692, 1295 1988. 692, 1395 1988. 692, 1395 1988. 692, 1495 1988. 692, 1495 1988. 692, 1495 1989. 692, 1415 1989. 692, 1425 1989.	19 197, 1861,14 30 190, 1861,14 30 190, 1861,14 30 190, 1861,14 31 190, 1861,14 417 190, 1861,14 417 190, 1861,14 417 190, 1861,14 419 190, 1861,14	13 12 13 13 13 13 13 13 13 13 13 13 13 13 13	10, 296, 193, 286 10, 206, 195, 286 10, 206, 195, 180 10, 206, 180 10, 206, 195, 180 10, 206, 180 10, 206, 180 10, 206, 180 10, 206, 180 1	100 100 100 100 100 100 100 100 100 100	\$60 544 545 545 545 545 545 545 545 545 54	49181 49181 49181 (FICP N 49181	- 89 - 50 - 50	[ACK Upd	See	-15314 Ack -15314 Ack	-39326168 -39327622 -39374346 [AOK] Se -39394763 [AOK] Se -3946346 [AOK] Se -39549546 [AOK] Se -395496 [AOK] Se -39	Min-L 49181 Min-L 4918	TO T	
1985. 002,1200 2985. 002,1200 2985. 002,1200 1985. 002,1200 1985. 002,1300 1985. 002,1300 1985. 002,1300 1985. 002,1300 1985. 002,1400 1985. 002,1400 1985. 002,1400 1985. 002,1400 1985. 002,1400 1989. 002,1400	19 197, 1861,14	13 12 13 13 13 13 13 13 13 13 13 13 13 13 13	10, 286, 193, 286 100, 286, 193, 286 100, 286, 193, 180	100 100 100 100 100 100 100 100 100 100	544 545 545 545 545 545 545 545 545 545	49181 49181 49181 49181 (100 h 49181	- 89 - 50 - 50 - 50 Ladow - 50 Ladow - 50 Ladow - 50 Ladow - 90 Ladow - 90 - 90 Ladow - 90 - 90 Ladow - 90 - 90 Ladow - 90 - 90	[ACK Upd	See	-1514 Ack -1514 Ack -1524 Ack -1524 Ack -1524 Ack -1514 Ack -1515 - 20 -1524 Ack -1524 Ack	-39326168 -95327628 -95327628 -95327628 -95327628 -95327628 -95425366 -954266 -954	Min-L 49181 Min-L 4918	100 100 100 100 100 100 100 100 100 100	
1985. 002.1299 1981. 002.1299 1981. 002.1299 1981. 002.1299 1981. 002.1299 1981. 002.1299 1982. 002.1390 1982. 002.1390 1982. 002.1390 1982. 002.1390 1982. 002.1490 1982. 002.1510 1982. 002.1510	19 192, 1861,14 33 190,1661,14 33 190,1661,14 33 190,1661,14 33 190,1661,14 31 190,1661,14	13 12 13 13 13 13 13 13 13 13 13 13 13 13 13	109, 209, 139, 200, 109, 209, 209, 209, 209, 209, 209, 209, 2	10 10 10 10 10 10 10 10 10 10 10 10 10 1	544 545 545 545 545 545 545 545 545 545	49181 49281 49281 [TCP N 49281	- 89 - 50 - 50 - 50 Lindow - 50 Lindow	[ACK Upd	See	-15314 Ack -1531	-39326168 -39327622 -39327436 [AOK] Se -3939476 [AOK] Se -3939476 [AOK] Se -3946336 [AOK] Se -3946336 [AOK] Se -3956376 [AOK] Se -3956376 [AOK] Se -39576226 [AOK] Se -39576226		100 100 100 100 100 100 100 100 100 100	
1985. 602,1209 1986. 602,1209 1986. 602,1209 1986. 602,1209 1986. 602,1209 1986. 602,1209 1986. 602,1209 1986. 602,1209 1986. 602,1209 1986. 602,1209 1986. 602,1400 1986. 602,1500 1986. 602,1500 1986. 602,1500	19 199, 1861,14 30 190,1661,14 30 190,1661,14 30 190,1661,14 417 190,1661,14 417 190,1661,14 418 190,1661,14 419 190,1661,14	13 12 13 13 13 13 13 13 13 13 13 13 13 13 13	189, 286, 139, 188 189, 286, 139, 188	10 10 10 10 10 10 10 10 10 10 10 10 10 1	\$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40	49181 49281 49281 49281 1 [TCP N 49281	- 89 - 50 - 50 - 50 Indow Indow Indow - 50 Indow - 50 Indow Indow Indow Indow Indow Indow - 50 Indow	[ACK Upd	See	-15514 Ack -15614 Ack -1561	39326168 39327628 39327628 [AOK] 56 39394768 [AOK] 56 [AOK] 56 39394768 [AOK] 56 3939476 [AOK]	Hilms. 4933 Hilms. 4938 Hilms. 493	100	
1985. 002.1299 1981. 002.1299 1981. 002.1299 1981. 002.1299 1981. 002.1299 1981. 002.1299 1982. 002.1390 1982. 002.1390 1982. 002.1390 1982. 002.1390 1982. 002.1490 1982. 002.1510 1982. 002.1510	19 197, 1861, 1.4	13 12 13 13 13 13 13 13 13 13 13 13 13 13 13	109, 209, 139, 200, 109, 209, 209, 209, 209, 209, 209, 209, 2	10 10 10 10 10 10 10 10 10 10 10 10 10 1	\$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40	49181 49181 49181 (FCP N 49181 (FCP N 100	- 88 - 52 - 52 - 52 - 52 - 52 - 52 - 52 - 53 - 53 - 53 - 53 - 53 - 53 - 53 - 53	[ACK Upd. Upd. Upd. [ACK Upd. Upd. Upd. Upd. Upd. Upd. Upd. Upd.	See	-15514 Ack -15514 Ack -15614 Ack -1561	-39326169 -39327629 -39327	Hilms. 49181 49181 Hilms. 4918	100 100 100 100 100 100 100 100 100 100	
1984. 007.120 1982. 007.120 1982. 007.120 1982. 007.120 1982. 007.120 1983. 007.120 1984. 007.120 1989.	18 197, 186, 1,4	13 12 13 13 13 13 13 13 13 13 13 13 13 13 13	18-28-19-3-38 18	100 100 100 100 100 100 100 100 100 100	\$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40	49181 (FCP W 49181) (FCP W 491	- 89 - 50 - 50 - 50 - 50 - 50 - 50 - 50 - 50	[ACK Upd Upd Upd [ACK Upd	See	-1551A Ack -1551	39320160 393327620 393327620 [AOK] 56 373394760 [AOK] 56 373394760 [AOK] 56 373394760 [AOK] 56 373394760 [AOK] 56 37349260 [AOK] 56 37349260 [AOK] 56 373749260 [AOK] 56 3737490 [AOK] 56 3737490 [AOK] 56 3737490 [AOK] 56 3737490 [AOK] 56 3737490 [AOK] 56 3737490 [AOK] 56 3737490	Hints. 49131 Hint	100	
1988 - 602 . 1000 1988 - 602 .	18 197, 186, 1,4	13 12 13 13 13 13 13 13 13 13 13 13 13 13 13	18, 286, 195, 186 18, 286, 195	10* 10* 10* 10* 10* 10* 10* 10* 10* 10*	\$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40 \$40	49181 (FCP W 49181) (FCP W 491	- 89 - 50 - 50 - 50 - 50 - 50 - 50 - 50 - 50	[ACK Upd Upd Upd [ACK Upd	See	-1551A Ack -1551	39320160 393327620 393327620 [AOK] 56 373394760 [AOK] 56 373394760 [AOK] 56 373394760 [AOK] 56 373394760 [AOK] 56 37349260 [AOK] 56 37349260 [AOK] 56 373749260 [AOK] 56 3737490 [AOK] 56 3737490 [AOK] 56 3737490 [AOK] 56 3737490 [AOK] 56 3737490 [AOK] 56 3737490 [AOK] 56 3737490	Hidrac, 4933	100 100 100 100 100 100 100 100 100 100	

Gambar 3.4. Pola *Packet Header* dari *Ransomware* WannaCry

Pada tabel 2. Pola Serangan *Ransomware Wannacry* menjelaskan pola-pola serangan paket *Ransomware WannaCry* yang terdeteksi di dalam jaringan SMK Negeri 1 Palembang yang akan digunakan pada proses pendeteksian menggunakan DPI.

Tabel 2. Pola Serangan Ransomware WannaCry

Ransom		Pola Ransomware					
Flow	TLSv	Payload					
Ransom 1	1.2	.google.com, .android.com, .appengine.com					
Ransom 2	1.2	.bdn.com, .cloud.google.com, crowdsource.google.com,					
Ransom 3	1.2	.g.co, gcp.gvt2.com, .gcpcpdn.gvt1.com, ggpht.cn, gkecnapps.cn					
Ransom 4	1.2	.google-analitics.com, .google.ca, .google.cl, .google.co.in					
Ransom 5	1.2	.google.co.jp, .youtube.com, .gstatic.cn,					
		.youtube-nocookie.com .google.de, .googlevideo.com,					
Ransom 6	1.2	.gstatic.com, .google.com.mx, .google.com.tr					
Ransom 7	1.2	.google.cocnapps.cn, .google.commerce.com, .yt.be, .ytimg.com.					

6. Pengidentifikasian TLSv pada Client Hello

Proses Identifikasian JA3C yang berupa observasi lanjutan dari pola serangan dari *Ransomware WannaCry*. Dengan memvalidasi protokol yang digunakan dalam dataset, yang berisikan konten serangan berupa protokol TCP, IP, Port dan TLSv pada Client. *Handshake* yang disetujui oleh Client terhadap server dengan memverifikasi Cipher yang digunakan. Pada Gambar 3.5 adalah protokol, TLSv dan *Cipher* yang digunakan dalam serangan *Ransowmware WannaCry* saat melakukan *handshake* terhadap *Server Hello*.



Gambar 3.5. Validasi TLSv dan *Cipher* pada *Client Hello*

7. Pengidentifikasian TLSv pada Server Hello

Proses Identifikasi informasi yang akan diberikan dari Server ke Client, yang dimana TLSv yang telah disepakati antara Server dan Client dengan *Cipher* yang sama. Proses validasi yang dilakukan adalah untuk mencari JA3S *Fingerprint* dengan kecocokan *raw data* dan hasil dari deteksi. JA3S adalah *Fingerprint* yang dibuat oleh Server dengan *Cipher* yang akan digunakan dalam serangan *Ransomware WannaCry*. Pada gambar 3.6 adalah validasi TLSv yang digunakan dalam *Server Hello* dan informasi berupa *cipher* yang digunakan *Ransomware WannaCry*.



Gambar 3.6. Validasi *Cipher* dan TLSv pada Server Hello

8. Korelasi serangan *Ransomware Wannacry* dengan data hasil ekstraksi

Korelasi serangan antara *alert* yang dihasilkan *Deep Packet Inspection* dan hasil *Feature Extraction*, yang dimana terdapat beberapa informasi diantaranya pada client didapati pola *fingerprint Ransomware Wannacry* yang menggunakan JA3C yang sama dan pada client berbeda. Berikut adalah korelasi tabel 2. Dan gambar 3.7.

Tabel 2. Fingerprint Ransomware

Client	Pola Ransomware					
Client	JA3C					
update.googleapis.	4d7a28d6f2263ed61de88ca					
com	66eb011e3					
clients2.google.co	4d7a28d6f2263ed61de88ca					
m	66eb011e3					



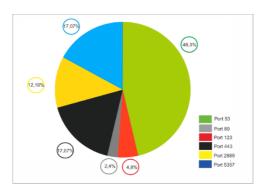
Gambar 3.7. Informasi yang diperoleh dari pendeteksian DPI

- Pada nomor 1 menjelaskan protokol yang digunakan yaitu TCP.
- Pada nomor 2 menunjukkan IP Source Address yang digunakan Client.
- Pada nomor 3 menunjukkan Port Source yang digunakan Client untuk Request informasi dengan mengirim beberapa Cipher yang akan disetujui.
- Pada nomor 4 menunjukkan *IP Destination Address* yang digunakan pada Server.
- Pada nomor 5 menunjukkan Port Destination yang digunakan Server untuk mengirim informasi yang telah disetujui oleh Cipher yang digunakan.
- Pada nomor 6 adalah protokol yang digunakan pada nDPI.
- Pada nomor 7 adalah nama protokol *Deep Packet Inspection*.
- Pada nomor 8 adalah TLSv 1.2 yang digunakan untuk *handshake* antara *Client Hello* dan *Server Hello*.
- Pada nomor 9 adalah JA3C yang berupa Fingerprint dengan memvalidasi keamanan dari TLSv dan Cipher yang digunakan.
- Pada nomor 10 adalah JA3S yang dibuat server dari TLSv dan Cipher yang disepakati dengan client

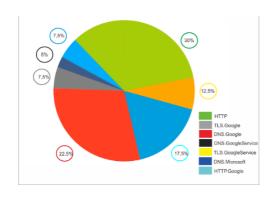
9. Hasil Diagram yang memvisualisasikan serangan *Ransomware Wannacry*

Hasil diagram visual dari proses klasifikasi atribut yang terdapat pada jaringan SMK Negeri 1 Palembang. Atribut yang didapat saat proses klasifikasi berupa destionation port dan protocol name pada dataset RansomX. Pada data yang telah didapat, ada beberapa serangan yang tidak menggunakan TLS dan hanya menggunakan port tujuan berupa alert. Alert inilah yang diambil

sebagai sampel data untuk menghitung berapa banyak serangan yang terjadi. Ini dapat membuktikan adanya paket serangan dengan nilai benign pada paket tersebut. Dengan data ini, maka dapat diklasifikasi menjadi bentuk diagram dengan menggunakan open-source tool, yang merujuk pada metode clustering yang akan mendapatkan hasil visual yang lebih konsisten.



Gambar 3.8. Klasifikasi *Destination Port* terhadap *benign score*



Gambar 3.9. Klasifikasi nama server yang diakses terhadap *benign score*.

4. Kesimpulan

Deep Packet Inspection adalah cara pendeteksian serangan Ransomware dengan menerapkan pada sistem keamanan SMK Negeri 1 Palembang. Snort dapat membantu dalam sistem pendeteksian dengan bantuan Deep Packet Inspection untuk mendeteksi serangan WannaCry, dengan memvalidasi Ransomware keamanan TLSv dan penggantian kunci Cipher. Dalam mendapatkan Fingerprint Deep Packet Inspection menggunakan metode String Matching pada sistem Snort dan dapat memvalidasikan TLSv yang digunakan Ransomware WannaCry, pada saat proses handshake yang dilakukan Client Hello dan Server Hello. Saat proses Handshake berlangsung Deep Packet Inspection menghasilkan JA3 sebagai bukti Fingerprint. Hasil deteksi yang diperoleh dari Deep Packet Inspection akan mendapatkan pola Fingerprint dari hasil validasi keamanan TLSv dan Cipher yang digunakan. Penelitian selanjutnya, dapat menerapkan pendeteksian secara real-time menggunakan plot yang lainnya. Menerapkan algoritma clustering lain dalam menentukan titik puncak serangan paket Ransomware WannaCry. Penelitian tahap selanjutnya dapat berupa Intrusion Detection System dengan bantuan snort dalam penerapan String Matching dan dapat memblokir serangan yang terdeteksi.

Reference

Al-Hisnawi, M., & Ahmadi, M. (2017). Deep packet inspection using Cuckoo filter. 2017 Annual Conference on New Trends in Information and Communications Technology Applications, NTICT 2017, October 2019, 197–202.

https://doi.org/10.1109/NTICT.2017.7976111

Cheng, R., & Watson, G. (2018). D 2 PI: Identifying Malware through Deep Packet Inspection with Deep Learning.

Ferdiansyah. (2018). Analisis Aktivitas Dan Pola Jaringan Terhadap Eternal Blue Dan Wannacry Ransomware. JUSIFO (Jurnal Sistem Informasi), 2(1), 44–59. http://eprints.binadarma.ac.id/3873/1/Ferdiansyah-Analisis Aktivitas dan Pola Jaringan Terhadap Eternal Blue dan Wannacry Ransomware.pdf

Grant, L., & Parkinson, S. (2018). *Identifying File Interaction Patterns in Ransomware Behaviour*. *September*, 317–335. https://doi.org/10.1007/978-3-319-92624-7_14

Jatti, S. A. V., & Kishor Sontif, V. J. K. (2019). Intrusion detection systems. *International Journal of Recent Technology and Engineering*, 8(2 Special Issue 11), 3976–3983. https://doi.org/10.35940/ijrte.B1540.0982S1119

Kiru, M. U., & Jantan, A. (2020). Ransomware Evolution: Solving Ransomware Attack Challenges. *The Evolution of Business in the Cyber Age, January*, 193–229. https://doi.org/10.1201/9780429276484-9

Kolodenker, E., Koch, W., Stringhini, G., & Egele, M. (2017).

PayBreak: Defense against cryptographic ransomware. ASIA CCS 2017 - Proceedings of the 2017 ACM Asia Conference on Computer and Communications Security, 599–611. https://doi.org/10.1145/3052973.3053035

O.lmaji, A. (2019). Ransomware Attacks: Critical Analysis, Threats, and Prevention methods. March, 1–32.

Rodrigues, G. A. P., de Oliveira Albuquerque, R., de Deus, F. E. G., de Sousa, R. T., de Oliveira Júnior, G. A., Villalba, L. J. G., & Kim, T. H. (2017). Cybersecurity and network forensics: Analysis of malicious traffic towards a honeynet with deep packet inspection. *Applied Sciences (Switzerland)*, 7(10), 1–29. https://doi.org/10.3390/app7101082

DOI: https://doi.org/10.31004/ijmst.v1i2.142 Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

- Saad Hafeez B.Eng., T. I. U. of B., & A. (2017). Deep Packet Inspection using Snort. *Deep Packet Inspection Using Snort*, 24. http://ondemand.gputechconf.com/gtc/2017/presentation/s746 8-wenji-wu-network-traffic-analysis-using-gpus.pdf
- Salim, T., Valianta, S. A., & Stiawan, D. (2016). Klasifikasi Trafik Terenkripsi Menggunakan Metode Deep Packet Inspection (Dpi). 2(1), 424–429. http://ars.ilkom.unsri.ac.id
- Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International:* Digital Investigation, 32, 200892. https://doi.org/10.1016/j.fsidi.2019.200892
- Velea, R., & Margarit, L. (2017). Network Traffic Anomaly Detection Using Shallow Packet Inspection and Parallel K-means Data Clustering. December.

- https://doi.org/10.24846/v26i4y201702
- Winanto, E. A., Heryanto, A., & Stiawan, D. (2016). Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means. *Annual Research Seminar 2016*, 2(1), 359–362.
- Xu, C., Chen, S., Su, J., Yiu, S. M., & Hui, L. C. K. (2016). A Survey on Regular Expression Matching for Deep Packet Inspection: Applications, Algorithms, and Hardware Platforms. *IEEE Communications Surveys* and Tutorials, 18(4), 2991–3029. https://doi.org/10.1109/COMST.2016.2566669