doi: 10.47002/metik.v7i2.636

METIK JURNAL VOLUME. 7 NOMOR.2 2023 ISSN-P 2442-9562 ISSN-E 2580-1503

Analisis Cara Kerja Sistem Deteksi Infeksi Worm Pada Komputer

Sumarno[1*]

[1] *Sistem Informasi, Universitas Islam Negeri Sultan Aji Muhammad Idris Samarinda, Indonesia*

[*]*sumarnodharmo@gmail.com*

Abstract

Worms are a type of malware that has the ability to develop and spread automatically to other computers on a network without human interaction. This fast and undetectable infection capability makes worms a serious threat in the world of computer security. This research aims to explore the mechanisms and behavior of worm infection systems on computers. This study involves an in-depth analysis of the functions and methods used by worms to enter, infect, and exploit target computers. This researchalso explain how worms can cause damage to computer systems, steal confidential information, or even create botnet networks to carry out large-scale attacks. Research methods include collecting data from existing worm detection systems, analyzing system logs that occur, as well as simulations to understand how worms work in various scenarios. In addition, this research also consider protection and prevention techniques that can be used to protect computers and networks from worm attacks. Based on observations and experiments, the results of this research can be concluded that the worm infection system spreads through computers connected to the network or through other media on the network and does not require a certain moment to be a trigger to infect the target. It is hoped that the results of this research provide an in-depth understanding of worm infection systems on computers, allowing researchers and computer security practitioners to develop more effective protection strategies. Prevention and early detection efforts will be key in dealing with the growing threat from worms and similar types ofmalware.

Keywords: worm, virus, vandalism

Abstrak

Worm adalah salah satu jenis malware yang memiliki kemampuan untuk berkembang dan menyebar secara otomatis ke komputer-komputer lain dalam jaringan tanpa interaksi manusia. Kemampuan infeksi yang cepat dan tanpa deteksi ini membuat worm menjadi ancaman serius dalam dunia keamanan komputer. Penelitian ini bertujuan untuk mendalami mekanisme dan perilaku sistem infeksi worm pada komputer. Studi ini melibatkan analisis dalam kedalaman fungsi dan metode yang digunakan oleh worm untuk memasuki, menginfeksi, dan mengekploitasi komputer target. Penelitian ini juga menjelaskan bagaimana worm dapat menyebabkan kerusakan pada sistem komputer, mencuri informasi rahasia, atau bahkan menciptakan jaringan botnet untuk melakukan serangan berskala besar. Metode penelitian mencakup pengumpulan data dari sistem deteksi worm yang ada, analisis log sistem yang terjadi, serta simulasi untuk memahami cara kerja worm dalam berbagai skenario. Selain itu penelitian ini juga mempertimbangkan teknik perlindungan dan pencegahan yang dapat digunakan untuk melindungi komputer dan jaringan dari serangan worm. Berdasarkan pengamatan dan percobaan maka hasil penelitian ini dapat disimpulkan bahwa sistem infeksi worm menyebar melalui komputer yang tersambung dengan jaringan atau melalui media lain dalam jaringan dan tidak memerlukan momen tertentu yang menjadi pemicu untuk menginfeksi target. Hasil penelitian ini diharapkan memberikan pemahaman mendalam tentang sistem infeksi worm pada komputer, memungkinkan para peneliti dan praktisi keamanan komputer untuk mengembangkan strategi perlindungan yang lebih efektif. Upaya pencegahan dan deteksi dini akan menjadi kunci dalam menghadapi ancaman yang terus berkembang dari worm dan jenis malware serupa.

Kata kunci: worm, virus, vandalism

1. Pendahuluan

Dalam kontek global yang semakin berkembang pada teknologi informasi, keamanan komputer dan jaringan menjadi sangat penting. Salah satu ancaman utama dalam dunia keamanan siber adalah serangan worm. Menurut *Seth Fogie dan Cyrus Peikari* (2002)[1], WORM *(Write-Once Read-Many)* adalah jenis malware yang dapat menyebar dan menginfeksi sistem komputer tanpa interaksi manusia, dengan memanfaatkan

doi: 10.47002/metik.v7i2.636

sumber daya yang ada disekitarnya, proses penggandaan diri yang dilakukan oleh worm terjadi karena ada celah kemanan yang memang terbuka dalam sistem komputer tersebut atau dikenal dengan sebutan *vulnerability.* Worm merupakan salah satu hasil dari evolusi virus komputer dengan metode seperti ini maka disamakan dengan kerja cacing yang ada dalam tanah yaitu untuk memenuhi kebutuhan dan bertahan hidup dengan memanfaatkan sumberdaya yang ada dialam sekitarnya. Sebuah worm dapat menggandakan dirinya dengan memanfaatkan jaringan komputer yang saling terhubung seperti pada *LAN (Local Area Network), WAN (Wide Area Network)*[2] atau pada jaringan global seperti Internat tanpa campur tangan atau ada pemicu dari user itu sendiri. Karena worm merupakan pengembangan evolusi dari virus komputer maka worm juga dapat menyalin dirinya sendiri dan menginfeksi berkas dalam sistem komputer dengan lebih baik bahkan melalui jaringan komputer yang terhubung dengan sistem yang telah terinfeksi sehingga penularan atau infeksinya menjadi lintas komputer karena dapat menyebarkan melalui jaringan komputer, pada beberapa kasus terbaru terjadinya pada perang rusia dan ukraina saat ini dimana worm menyebabkan kekacauan korporasi[3] diantaranya adalah yang terjadi disejumlah perusahaan internasional yang beroperasi di ukraina, perusahaan raksasa perkapalan A.P. Moeller-Maersk, perusahaan Saint Gobain asal Perancis

dan Mondelez International Inc, Pemilik Coklat Cadbury, Perusahaan BNP Paribas Real Estate, bagian dari Bank asal Perancis yang memberikan layanan properti dan manajemen investasi, bahkan produksi pabrik Cadbury bagian Australia yaitu di Pulau Tasmania juga dipaksa berhenti beroperasi setelah sistem komputernya dilumpuhkan. Sedemikian ganasnya penyebaran worm sehingga hal ini mengharuskan pengguna komputer harus menerapkan sistem keamanan yang baik dalam rangka mengindari serangan tersebut.

Beberapa penelitian internasional sebelumnya telah memberikan wawasan yang berharga mengenai mekanisme dan perilaku worm. Sebagai contoh penelitian oleh *Michael Miller*[4]. mengkaji cara worm mengidentifikasi target, mengeksploitasi kerentanan dalam sistem komputer, dan menyebar ke target lain. Demikian pula penelitian yang dilakukan oleh *Peter Mell*[5], memfokuskan pada analisis lebih mendalam tentang cara kerja virus termasuk worm dan dampaknya terhadap sistem komputer.

Namun, dalam konteks Indonesia, penelitian tentang analisis cara kerja sistem infeksi worm pada komputer masih terbatas. Studi-studi ini sangat penting untuk mengidentifikasi ancaman yang lebih spesifik dalam lingkungan komputasi Indonesia. Oleh karena itu penelitian ini akan berupaya untuk mengisi celah ini dengan mendalami mekanisme sistem infeksi worm pada komputer dalam konteks Indonesia.

Referensi penelitian sebelumnya dari peneliti Indonesia dengan tema yang sama sangat penting dalam upaya ini. Misalnya, penelitian oleh Yudi Ari Adi

[6] menggali cara worm menyebar dan berkembang pada komputer, serta dampak yang ditimbulkannya. Demikian pula, penelitian yang dilakukan oleh Ilhamdi, Yusriansyah dkk [7] memfokuskan pada cara kerja virus termasuk worm dalam ekosistem jaringan Indonesia, yang bisa sangat berbeda dari lingkungan global .

Melalui penelitian ini, bertujuan untuk menyumbangkan pengetahuan dan pemahaman tambahan tentang cara kerja sistem infeksi worm pada komputer, memanfaatkan temuan penelitian sebelumnya sebagai landasan, dengan pemahaman yang lebih mendalam tentang ancaman ini, penting untuk mengetahui atau deteksi sistem infeksi worm dan mengembangkan strategi keamanan yang lebih efektif dan terfokus, guna melindungi komputer dan jaringan dari serangan worm yang semakin canggih.

Berdasarkan gambaran umum di atas dapat diidentifikasi masalah yang terjadi, a) Deteksi dan pencegahan worm, Bagaimana sistem keamanan komputer dapat mendeteksi dan mencegah serangan, b) Dampak serangan worm, Serangan worm dapat memiliki dampak yang merusak terhadap sistem komputer, termasuk pencurian data, penghancuran data, atau gangguan layanan,

doi: 10.47002/metik.v7i2.636

dan c) Perlindungan terhadap data preventif, sebelum worm menyerang komputer sehingga bisa meminimalisir kerugian yang mungkin terjadi.ehingga tujuan analisis yang dicapai dari penelitian ini adalah 1) Untuk mengetahui dan memahami tahap-tahap infeksi worm dilihat dari log sistem, 2) Menganalisis dampak yang dihasilkan oleh worm pada sistem komputer dan jaringan, dan 3) Bagaimana cara mengatasinya sehingga tidak menimbulkan ketakutan yang berlebihan dikalangan pengguna komputer.

Hal ini dilakukan karena melihat perkembangan teknologi informasi terutama terutama teknologi komputer yang terus dan semakin berkembang dikaitkan dengan perkembangan program yang merusak *(Electronic Vandalism)*[8].

2. Metode Penelitian

2.1. Tahap Penelitian

Penelitian ini adalah penelitian yang menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus[9], didukung pula dengan *analytical observation* dan percobaan *(eksperimen)* sederhana berupa ujicoba mandiri, berikut tahapan dalam penelitianini:

Tabel 1. Tahapan Penelitian [10]

No	Uraian	Keterangan
1	Pemilihan Kasus	Identifikasi pemilihan kasus
2	Penentuan Tujuan	Menentukan tujuan kasus
3	Desain Penelitian	Kerangka kerja-desain penelitian
4	Pengumpulan data	Pengumpulan data yang relevan
5	Analisis Data	Analisis data
6	Interpretasi Hasil	Interpretasi hasil/temuan penelitian
7	Kesimpulan	Pembahasan dan kesimpulan

2.2. Instrumen Penelitian

Instrumen penelitian dapat digambarkan dengan langkah-langkah sebagai Berikut :

Tabel 2. Langkah Penelitian

No	Uraian	Keterangan
1	Peralatan Komputer	Penelitian ini menggunakan 1 Pc dan 3 laptop
2	Prosedur Observasi	Penelitian ini dilakukan dengan pengamatan log jaringan deteksi worm pada jaringan
3	Log Jaringan	Gambar dan photo log jaringan yang terdeteksi
4	Analisis Data	Melakukan analisis data disertakan sumber acuan dan hasil percobaan
5	Kesimpulan	simpulan hasil penelitian & sumber referensi yang ada

3. Hasil Penelitian

3.1. Metode Infeksi Worm

Setelah melaksanakan observasi terhadap objek penelitian pada komputer yang telah disiapkan maka dapat ditarik kesimpulan bahwa metode infeksi worm dapat dikategorikan ke dalam beberapa hal sebagai berikut :

Tabel 3. Metode Infeksi Worm

No	Uraian	Keterangan
1	Ekploitasi Kerentanan	Menggunakan kerentanan yang belum diperbaiki
2	Penyebaran melalui jaringan	Menyebar melalui jaringan komputer dengan memanfaatkan protocol jaringan yang tidak aman
3	Pemanfaatan perangkat portable	Menyebar melalui perangkat penyimpanan portable, spt USB drive dll
4	Penciptaan pintu belakang	Menciptakan pintu belakang atau backdoor pada sistem yang terinfeksi
5	Penyebaran melalui e- mail	Menggunakan e-mail sebagai sarana penyebaran dengan mengirim diri sebagai lampiran atau tautan email
6	Penyebaran melalui media sosial	Menyebar melalui platform media sosial dengan memanfaatkan tautan berbahaya atau malware terkait dengan konten yang menarik

doi: 10.47002/metik.v7i2.636

3.2. Tanda Keberadaan Worm

Pada umumnya keberadaan worm akan sulit untuk di deteksi, namun ada beberapa cara untuk mendeteksi keberadaan worm dalam computer [11], antara lain:

Tabel 4. Tanda Deteksi Keberadaan Worm

No	Uraian
1	Sering muncul pesan error
2	Berubah volume disk
3	File hilang secara misterius
4	Ukuran/Data file berubah tanpa sebab
5	Penurunan space memori komputer
6	Aktifitas sistem berjalan lambat secara keseluruhan

3.3. Analisis Cara Kerja Sistem Infeksi Worm.

Berdasarkan studi kasus yg dilaksanakan ditunjang dengan literatur yang diperoleh, maka cara kerja infeksi worm dalam komputer melibatkan serangkaian langkah yang memungkinkan worm untuk dapat menyebar[6] dan menjalankan aksinya dalam sistem komputer target, sebagai berikut :

Tabel 5. Hasil Analisis Cara Kerja Sistem Infeksi Worm

No	Uraian		Keterangan
	Tahap Infeksi	Metode Penyebaran	
1	Penyusupan awal	Eksploitasi kerentanan	Penyusupan awal melalui eksploitasi kerentanan sistem
2	Replikasi	Penyebaran melalui jaringan	Menggandakan diri dan menyebar dalam jaringan jaringan yang tidak aman.
3	Aksi berbahaya	Eksekusi kode berbahaya	menjalankan kode berbahaya yang merusak memungkinkan untuk
4	Pengendalian jaringan	Penciptaan pintu belakang	mengakses sistem secara jarak jauh.
5	Penyebaran lanjutan	Penyebaran melalui USB dan perangkat portabel	Menyebar melalui perangkat USB/Portable ketika dihubungkan

3.4. Log Keamanan Sistem

Berikut contoh bagaimana kita dapat membuat catatan log ketika permintaan datang dari alamat IP tertentu :

3.4.1. Log KehadiranWorm

Dalam contoh ini, kita harus menggantikan"IP_Worm yang di deteksi" dengan alamat IP yang ingin dideteksi. Jika permintaan datang dari alamat IP tersebut, kode akan mencatat informasi dalam sebuah file log. Ini adalah contoh sederhana dan jangan dianggap sebagai metode deteksi worm yang kuat.

```asp
<%
Dim ip_address
ip_address = Request.ServerVariables("REMOTE_ADDR")

' Ganti "IP_WORM_YANG_DIDETEKSI" dengan alamat IP yang ingin Anda deteksi
If ip_address = "IP_WORM_YANG_DIDETEKSI" Then
    ' Jika permintaan datang dari alamat IP yang Anda deteksi, catat ke dala
    Dim logFile, logText
    logFile = Server.MapPath("deteksi_worm.log")
    logText = "Deteksi worm dari alamat IP: " & ip_address & " pada " & Now
    Set objFSO = Server.CreateObject("Scripting.FileSystemObject")
    Set objFile = objFSO.OpenTextFile(logFile, 8, True)
    objFile.WriteLine logText
    objFile.Close
    Set objFile = Nothing
    Set objFSO = Nothing
End If
%>
```

Gambar 1. Log Keamanan Sistem

Atau dapat menggunakan perintah “Netstat-ano” pada CMD.

```
<%
Dim ip_address
ip_address =
Request.ServerVariables("REMOTE_AD
DR")
' Ganti "IP_WORM_YANG_DIDETEKSI"
dengan alamat IP yang ingin Anda
deteksi
If ip_address =
"IP_WORM_YANG_DIDETEKSI" Then
    ' Jika permintaan datang dari
alamat IP yang Anda deteksi, catat
ke dalam log
    Dim logFile, logText
    logFile =
Server.MapPath("deteksi_worm.log")
    logText = "Deteksi worm dari
alamat IP: " & ip_address & " pada
" & Now
    Set objFSO =
Server.CreateObject("Scripting.Fil
eSystemObject")
    Set objFile =
objFSO.OpenTextFile(logFile, 8,
True)
    objFile.WriteLine logText
    objFile.Close
```

doi: 10.47002/metik.v7i2.636


```
    Set objFile = Nothing
    Set objFSO = Nothing
End If
%>
```

```
Active Connections

Proto  Local Address          Foreign Address        State           PID
TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1028
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
TCP    192.168.1.100:49342    91.198.174.192:80      ESTABLISHED     1234
```

Gambar 2. Log Hasil “Netstat-ano”

Perintah ini akan menampilkan semua koneksi jaringan aktif di komputer,

1. Kolom *"Local Address"* (Alamat Lokal) dan *"Foreign Address"* (Alamat Luar)**:** Periksa kolom ini untuk mencari tanda-tanda alamat IP atau port yang mencurigakan atau tidak dikenal. Jika melihat koneksi ke alamat IP yang tidak dikenal atau port yang tidak biasa, ini bisa menjadi indikasi aktivitas mencurigakan.
2. Kolom *"State"* (Status)**:** Perhatikan kolom ini untuk melihat status koneksi. Koneksi dalam status yang mencurigakan, seperti "ESTABLISHED" (telah terhubung) ke alamat IP yang tidak dikenal, bisa menjadi tanda-tanda aktivitas yang mencurigakan.
3. Kolom *"PID" (Process ID):* Nomor PID adalah proses yang terkait dengan setiap koneksi. Jika melihat nomor PID yang mencurigakan, maka perlu memeriksa proses tersebut dalam Task Manager atau melalui perangkat lunak keamanan untuk menentukan apa yang sedang berjalan.

3.4.2. Log Penyusupan Awal

Log sistem penyusunan awal worm pada jaringan adalah sebuah catatan yang mencatat aktivitas awal dari worm yang masuk ke dalam jaringan komputer.

```
[Tanggal & Waktu]: [Contoh: 2023-10-18 13:45:22]
[Sumber IP]: [Contoh: 192.168.1.100]
[Tujuan IP]: [Contoh: 192.168.1.200]
[Tujuan Port]: [Contoh: 445]
[Protokol]: [Contoh: SMB]
[Aktivitas]: [Contoh: Koneksi Gagal]
[Deskripsi]: [Contoh: Upaya koneksi ke port 445 pada sistem tujuan gagal.]
```

Gambar 3. Log. Penyusupan awal

log mencatat percobaan koneksi gagal dari sumber IP 192.168.1.100 ke tujuan IP 192.168.1.200 pada port 445 menggunakan protokol SMB. Ini adalah salah satu tanda awal infeksi worm yang mencoba memanfaatkan kerentanan sistem di port tersebut.

3.4.3. Log. Replikasi upaya penyebaran Replikasi mencatat aktivitas replikasi oleh worm komputer, yang mencakup upaya penyebaran atau infeksi ke sistem lain dalam jaringan

```
[Tanggal & Waktu]: [Contoh: 2023-10-19 09:15:30]
[Sumber IP]: [Contoh: 192.168.1.75]
[Tujuan IP]: [Contoh: 192.168.1.200]
[Tujuan Port]: [Contoh: 445]
[Protokol]: [Contoh: SMB]
[Aktivitas]: [Contoh: Upaya Replikasi]
[Deskripsi]: [Contoh: Sumber IP 192.168.1.75 mencoba mereplikasi diri ke sis
```

Gambar 4. Log. Replikasi Penyebaran

log mencatat upaya replikasi oleh worm dari sumber IP 192.168.1.75 ke sistem dengan alamat IP 192.168.1.200 melalui protokol SMB dan port 445. Ini menunjukkan bahwa worm mencoba untuk menyebar ke sistem target dengan memanfaatkan layananSMB

3.4.4. Log. Eksekusi kode berbahaya Eksekusi kode berbahaya(malicious code execution log) mencatat aktivitas di mana worm atau serangan siber lainnya mencoba mengeksekusi kode berbahaya atau malware pada sistem komputer

```
[Tanggal & Waktu]: [Contoh: 2023-10-20 14:25:12]
[Sumber IP]: [Contoh: 192.168.1.60]
[Tujuan IP]: [Contoh: 192.168.1.300]
[Tujuan Port]: [Contoh: 80]
[Protokol]: [Contoh: HTTP]
[Aktivitas]: [Contoh: Eksekusi Kode Berbahaya]
[Deskripsi]: [Contoh: Sumber IP 192.168.1.60 mengirimkan permintaan HTTP ke
```

Gambar 5. Log. Eksekusi Kode Worm

log mencatat upaya eksekusi kode berbahaya oleh sumber IP 192.168.1.60 pada sistem dengan alamat IP 192.168.1.300 melalui protokol HTTP dan port 80

3.4.5. Log. Melihat hak akses pengguna Untuk mengelola hak akses berkas dan direktori di sistem Windows, maka dapat digunakan perintah “icacls” pada CMD, dengan hasil sebagai berikut :

doi: 10.47002/metik.v7i2.636


```mathematica
C:\ContohFolder NT AUTHORITY\SYSTEM:(F)
                BUILTIN\Administrators:(F)
                DOMAIN\NamaPengguna:(R,W,D,WDAC,WO)

Successfully processed 1 files; Failed processing 0 files
```

Gambar 6. Log melihat akses pengguna

Hasil menunjukkan daftar pengguna atau grup yang memiliki hak akses ke direktori "C:\Contoh Folder" beserta jenis hak akses yang diberikan (misalnya, "F" untuk Full Control, "R" untuk Read, "W" untuk Write, dll). Jika ada pengguna atau group yang tidak memiliki hak akses maka kita dapat menghapusnya“remove”

3.4.6. Log. Pemindaian Keamanan

Perintah "MpCmdRun"digunakan untuk menjalankan Microsoft Malware Protection Command Line Utility, yang memungkinkan Anda untuk melakukan pemindaian keamanan dan berbagai tugas terkait keamanan menggunakan Command Prompt(CMD).

```mathematica
MpCmdRun -Scan -ScanType 1
```

```scss
Microsoft Antimalware Service has started. The system is using signature-ba
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
Scanning 46545 items (125465 files)
```

Gambar 7. Hasil Pemindaian Keamanan

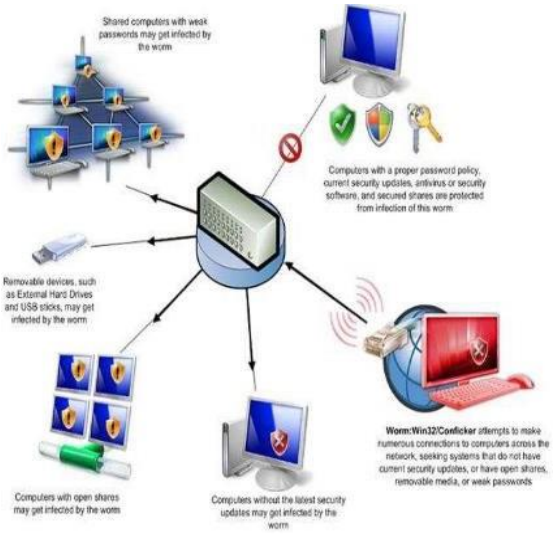
3.5. Dampak worm pada beberapa negara

Pada beberapa negara telah mengumumkan dampak dan kerugian yang diakibatkan oleh serangan worm, diantaranya adalah :

a. Serangan *Stuxnet* (Iran) pemerintah Iran mengumumkan serangan Stuxnet pada tahun 2010 yang menargetkan infrastruktur nuklir negara tersebut[12].
b. Serangan *WannaCry* (Berbegai Negara) Serangan *Ransomware WannaCry* pada tahun 2017 menginfeksi ribuan komputer diseluruh dunia.[13] Dampak yang ditimbulkan antara lain adalah penutupan rumah sakit, gangguan layanan publik dan kerugian finansial
c. Serangan *NotPetya* (Ukraina) pada tahun 2017[3], yang pertama kali menginfeksi system komputer di ukraina dan kemudian menyebar ke seluruh dunia
d. Serangan *SolarWind*s (AS) Terungkap pada tahun 2020, yang mengakibatkan dampak besar pada banyak organisasi di Amerika Serikat[14]

3.6. Pembahasan

Penelitian ini bertujuan untuk mendalami dan menganalisis mekanisme dan perilaku sistem infeksi worm pada komputer. Worm adalah salah satu jenis malware yang dapat menginfeksi komputer dan jaringan dengan cepat tanpa interaksi pengguna. Kemampuan worm untuk menyebar dan menyusup ke dalam sistem komputer tanpa deteksi awal telah membuatnya menjadi ancaman serius terhadap keamanan siber.



Gambar 8. Cara Kerja Worm [15]

Pentingnya penelitian ini terletak pada upaya untuk memahami bagaimana worm bekerja, bagaimana mereka menyebar, dan dampaknya terhadap sistem komputer. Melalui pemahaman yang lebih mendalam tentang mekanisme worm, kita dapat mengembangkan strategi perlindungan yang lebih efektif dan mencegah serangan-serangan yang merusak.

Pada penelitian sebelumnya yang sejenis membahas perilaku analisis cara kerja sistem infeksi virus yang dilakukan oleh Petrus Dwi Ananto Pamungkas [16], membahas program yang merusah salah

doi: 10.47002/metik.v7i2.636

satunya adalah worm dan sistem keamanannya, termasuk kemampuan worm dalam menggandakan diri tanpa ada file pemicu, selanjutnya menurut penelitian yang dilakukan oleh Febriyanti Panjaitan dkk [17], analisis malware dengan surface dan runtime analisis, mengemukakan perihal cara program yang merusak termasuk worm dalam penyusupan ke dalam sistem komputer, selanjutnya penelitian yang dilakukan oleh Sugeng Murdowo [8] membahas mengenai virus komputer dan perilakunya, temasuk didalamnya adalah perilaku worm dalam sistem komputer, berdasarkan semua referensi yang termuat maka dapat di tarik suatu kesamaan bahwa worm komputer dalam sistem infeksinya menyebar melalui komputer yang tersambung dengan jaringan atau melalui media lain yang berhubungan dengan file yang terinfeksi terlebih dahulu dengan worm, berbeda halnya dengan virus komputer yang menyebar ketika rutin pemicunya diaktifkan atau di-klik dan seterusnya, maka worm tetap dapat menginfeksi file yang terhubung dengan jaringan dan tidak memerlukan momen tertentu yang menjadi pemicu untuk menginfeksi target, jika dilihat dari efek yang ditimbulkan maka virus dengan worm sama-sama mempunyai efek merusak yaitu, menginfeksi target dan menggandakan diri sehingga memori menjadi penuh, menyembunyikan diri sehingga tidak mudah dideteksi oleh antivirus, dan manupulasi termasuk merusak file/sistem yang terinfeksi.[18]

3.7. Keamanan Sistem

Langkah – langkah umum perlindungan dari serangan worm[6] dapat di implementasi kan sebagai Berikut :

Tabel 6. Langkah Perlindungan Siber Secara Umum[19] Dan Dalam Bahasa Pemrograman

No	Uraian	Keterangan
1	a. Pembaruan system	a. Validasi input
2	b. Firewall	*b.* Penggunaan *Filter dan Whitelist*
3	c. Perangkat lunak keamanan	c. Pengkodean yang aman
4	d. Tautan, lampiran dan email	d. Manajemen akses
5	e. Perangkat lunak anti malware	e. Pembaruan Rutin
6	f. Pemindaian berkala	*f.* Penggunaan perlindungan *Cross-Site Scripting(XSS)*
7	g. Backup data	g. Perlindungan terhadap serangan CSRF
8	h. Pemantauan keamanan	h. Pemantauan keamanan berkelanjutan
9	i. Penggunaan sandi	
10	j. Pembaruan aplikasi	
11	k. Keamanan siber berkelanjutan	

4. Kesimpulan

Dari penelitian diatas dapat disimpulkan bahwa :

a. Worm adalah ancaman siber yang dapat menyusup dan menyebar dengan cepat melalui jaringan komputer tanpa memerlukan campur tangan manusia serta dapat menyebabkan kerusakan serius pada sistem dan merusak keamanan informasi.
b. Sistem infeksi worm pada komputer melibatkan serangkaian tahap, termasuk penyusupan awal, replikasi, penyebaran, eksploitasi kerentanan, instalasi dan penyisipan, aksi berbahaya, pembuatan pintu belakang, pengendalian jaringan dan penyebaran lanjutan.
c. Penting untuk memahami bahwa upaya pencegahan dan deteksi worm adalah bagian penting dari keamanan siber yang efektif, dan kerjasama yang kuat antara pengguna dan profesional keamanan siber sangat diperlukan untuk melindungi sistem komputer dan jaringan dari ancaman worm.

5. Saran

Dari hasil penelitian yang diperoleh, maka dapat disarankan antara lain :

a. Diperlukan adanya penelitian lebih lanjut mengenai analisis cara kerja sistem infeksi worm pada komputer, sehingga akan didapatkan hasil lebih akurat.
b. Melakukan dengan benar tahap-tahap pengamanan terhadap serangan siber khususnya worm pada sistem komputer.
c. Sehubungan dengan pintu masuk penyebaran worm adalah memanfaatkan

doi: 10.47002/metik.v7i2.636

kelemahan sistem keamanan jaringan, maka sangat perlu sekali memperkuat sistem keamanan jaringan komputer dan senantiasa memeriksa hak akses pengguna komputer yang terhubung dengan jaringan.

6. Daftar Pustaka

[1] C. P. Seth Fogie, "Windows Internet Security:Protecting Your Critical Data," *Prentice Hall PTR, Up. Saddle River, New Jersey*, vol. 222,2002.

[2] Rastri Prathivi and Vensy Vydia, "Analisa Pendeteksian Worm dan Trojan Pada Jaringan Internet Universitas Semarang Menggunakan Metode Kalifikasi Pada Data Mining C45 dan Bayesian Network," *J. Transform.*, vol. 14, no. 2, pp. 77–81,2017.

[3] Voaindonesia, "Virus Komputer Petya Menyebar dari Ukraina untuk hambat bisnis dunia," *Voaindonesia*, 2017. [Online].Available: https://www.voaindonesia.com/a/virus-komputer-petya-menyebar-dari-ukraina-untuk-hambat-bisnis-dunia/3920788.html

[4] M. Miller and NetLibrary Inc., *Absolute PC security and privacy*.2002.

[5] P. Mell, K. Kent, and J. Nusbaum, "Special Publication 800-83 Sponsored by the Department of Homeland Security Guide to Malware Incident Prevention and Handling Recommendations of the National Institute of Standards and Technology," 2015.

[6] Y. A. Adi, "Model Epidemik Pada Penyebaran Virus Komputer," *Semin. Nas. Mat. Dan Pendidik. Mat. 2006*, 2006.

[7] Y.IlhamdiandY.N.Kunang,"Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik," *Bina Darma Conf. Comput. Sci.*, vol. 3, no. 1, pp. 256–264, 2021, [Online]. Available: https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2124

[8] S. Murdowo, "Mengenal Lebih Dalam Tentang Virus-Virus Komputer dan Perilakunya," *J. Ilm. Infokam*, vol. 19, no. 1, pp. 74–84, 2023, doi: 10.53845/infokam.v19i1.344.

[9] M. A. M. Fitrah, M.Pd & Dr. Luthfiyah, *Metodologi Penelitian : Penelitian Kualitatif, Tindakan Kelas & Studi Kasus*. Sukabumi, Jawa Barat: CV. Jejak,2017.

[10] D. Assyakurrohim, D. Ikhram, R. A. Sirodj, and M. W. Afgani, "Metode Studi Kasus dalam Penelitian Kualitatif," *J. Pendidik. Sains dan Komput.*, vol. 3, no. 01, pp. 1–9, 2022, doi: 10.47709/jpsk.v3i01.1951.

[11] Harjono, "Deteksi Malware Dalam Jaringan Menggunakan Dionaea," *Techno, ISSN 1410 - 8607*, vol. 14, no. 2, pp. 64–69,2013.

[12] Kompas.id, "Kisah Perang Siber Iran, Menguak Strategi Teheran Menandingi Serangan Israel-AS," www.Kompas.id. [Online]. Available: https://www.kompas.id/baca/internasional/2021/04/19/kisah-perang-siber-iran-menguak-strategi-teheran-menandingi-serangan-israel-as

[13] Kominfo.go.id, "FAQ Wannacryptor Ransomware,"Kominfo.go.id.

[14] K. P. Dkk, "SolarWinds Hack Adalah Karya 'Setidaknya 1.000 Insinyur', Para Eksekutif Teknologi Memberitahu Senat"," *Guardian*, 2021.

[15] M. Robert and C. Aiba, "Virus atau Worm," vol. 2020, no. 1, pp. 1–7,2020.

[16] P. D. A. Pamungkas, "Analisis Cara Kerja Sistem Infeksi Virus Komputer," *Bina Insa. ICT J.*, vol. 1, no. 1, pp. 15–40, 2018.

[17] F. Panjaitan, H. Yudiastuti, and M. Ulfa, "Analisis Malware dengan metode Surface dan Runtime Analysis," *J. Ilm. Matrik*, vol. 23, no. 1, pp. 1–11, 2021, doi:10.33557/jurnalmatrik.v23i1.1148.

[18] J. Na, A. M. Universitas, P. Indonesia, Y. Padang, and S. Barat, "Metoda Pertahan Diri Program Virus," *J. Ilm. Process.*, vol. 8, no. 2, 2013, [Online]. Available: http://processor.stikom-db.ac.id/index.php/processor/article/view/71

[19] P. P. Pemungkas, S. Sutrisno, and S. Sunarsih, "Pengembangan Model Epidemik Sira Untuk Penyebaran Virus Pada Jaringan Komputer," *J. Fundam. Math. Appl.*, vol. 2, no. 1, p. 13, 2019, doi:10.14710/jfma.v2i1.26.