**Jurnal Inovasi Artificial Intelligence & Komputasional Nusantara (JIKOMNUS)** DOI: 10.260396/Jikomnus
Vol. 1 No. 1 Juli 2024, hlm 43-47 p-ISSN: 3063-XXXX
SK.ISSN: 30634830/II.7.4/SK.ISSN/09/202 e-ISSN: 3063-4830

# Analisis Keamanan Sistem Operasi Windows Terhadap Serangan Malware Dari Aplikasi Crack Adobe Photoshop

**Khaswa Giovani Simanungkalit[1], M. Inaka Akbar Lubis[2], Dava Ardiansyah Rangkuti[3], Irfan Aprianda[4], Indra Gunawan[5]**

**STIKOM Tunas Bangsa Pematangsiantar**
Email: [1]kaswahsimanungkalit1005@gmail.com , [2]kabot299@gmail.com , [3]davarangkuti10@gmail.com, [4]nandagaming92@gmail.com, [5]indra@amiktunasbangsa.ac.id

(Naskah masuk: 06 Mei 2024, diterima untuk diterbitkan: 30 Juni 2024)

**Abstrak**

Studi ini menyelidiki risiko keamanan yang muncul akibat penggunaan aplikasi crack Adobe Photoshop pada sistem operasi Windows, dengan perhatian khusus pada ancaman malware seperti Trojan dan Ransomware. Penelitian ini dilaksanakan dalam lingkungan virtual untuk mengamati pola serangan, cara penyebaran, serta dampak malware terhadap sistem dan data pengguna.Temuan menunjukkan bahwa aplikasi crack sering digunakan sebagai saluran untuk menyebarkan malware. Trojan menyusup ke dalam sistem secara sembunyi-sembunyi, memberikan akses ilegal kepada penyerang, sedangkan Ransomware mengenkripsi file penting dan meminta tebusan untuk memulihkan data. Dampak serangan ini dapat sangat merugikan, termasuk kehilangan data dan gangguan dalam operasi. Penelitian ini tidak hanya menguraikan cara kerja malware, tetapi juga menawarkan strategi mitigasi. Rekomendasi mencakup peningkatan kesadaran pengguna tentang bahaya perangkat lunak bajakan, penggunaan perangkat lunak keamanan terbaru, serta penerapan praktik pencadangan data secara berkala. Dengan memahami dan mempersiapkan diri terhadap risiko ini, pengguna dapat mengambil langkah proaktif untuk melindungi sistem mereka dari ancaman yang diakibatkan oleh penggunaan aplikasi crack, sehingga menjaga keamanan dan integritas data pribadi mereka.

**Kata kunci**: *Crack Software,Malware,Trojan,Ransomware,Keamanan Windows,Adobe Photoshop*

***Abstract***

This study investigates the security risks that arise from using cracked Adobe Photoshop applications on Windows operating systems, with particular attention to malware threats such as Trojans and Ransomware. This research was carried out in a virtual environment to observe attack patterns, distribution methods, and the impact of malware on systems and user data. Findings show that cracked applications are often used as a channel for spreading malware. Trojans infiltrate systems stealthily, giving attackers illegal access, while Ransomware encrypts important files and demands a ransom to recover the data. The impact of these attacks can be devastating, including loss of data and disruption in operations. This research not only outlines how malware works, but also offers mitigation strategies. Recommendations include increasing user awareness about the dangers of pirated software, using the latest security software, as well as implementing regular data backup practices. By understanding and preparing for these risks, users can take proactive steps to protect their systems from threats posed by the use of cracked applications, thereby maintaining the security and integrity of their personal data.

**Keywords**: *Crack Software, Malware, Trojans, Ransomeware, Windows Security, Adobe Photoshop*

## 1. PENDAHULUAN

Penggunaan perangkat lunak bajakan, khususnya dalam bentuk crack, telah menjadi praktik yang umum di kalangan pengguna komputer yang ingin mengakses perangkat lunak premium tanpa perlu membayar lisensi resmi. Crack ini merupakan perangkat lunak yang telah dimodifikasi oleh pihak ketiga untuk melewati perlindungan keamanan yang diterapkan pengembang, memungkinkan pengguna untuk mengaktifkan perangkat lunak tanpa memerlukan kunci lisensi sah (Gordon & Ford, 2006). Walaupun memberikan akses gratis ke fitur-fitur premium, perangkat lunak crack sering kali membawa risiko keamanan yang serius, termasuk potensi penyebaran malware berbahaya. Aplikasi crack biasanya telah diubah untuk memasukkan kode berbahaya yang dapat menginfeksi sistem operasi, mencuri data pribadi, atau memberikan kontrol jarak jauh kepada penyerang tanpa sepengetahuan pengguna (Sinha et al., 2017). Akibatnya, pengguna yang tidak waspada terhadap ancaman ini berisiko menjadi korban.

## 2. METODOLOGI

Penelitian ini menggunakan pendekatan forensik digital untuk menganalisis perilaku malware yang terdapat dalam aplikasi crack Adobe Photoshop pada sistem operasi Windows. Proses forensik dilakukan di lingkungan virtual yang terisolasi untuk menghindari penyebaran malware ke jaringan lain dan mencegah risiko kerusakan sistem. Metode ini melibatkan beberapa tahapan utama: pengumpulan sampel, pengujian pada mesin virtual, pemantauan aktivitas malware, analisis dampak, serta penyusunan strategi mitigasi. Masing-masing tahap dijelaskan secara lebih rinci sebagai berikut:

### 1. Pengumpulan Sampel

Tahap ini dimulai dengan pengumpulan sampel crack Adobe Photoshop dari berbagai situs unduhan yang dicurigai menjadi sumber malware. Proses ini dilakukan dengan menelusuri beberapa situs torrent dan situs crack yang sering menyediakan versi bajakan perangkat lunak populer. Untuk memastikan keragaman sampel, berbagai versi crack Adobe Photoshop yang berbeda dikumpulkan. Sebelum dilakukan analisis, setiap file diperiksa menggunakan perangkat lunak VirusTotal untuk mendapatkan indikasi awal terkait ancaman yang mungkin terkandung di dalamnya.

1) Alat yang digunakan: Web VirusTotal, perangkat lunak pemindai malware.
2) Tujuan: Mendapatkan sampel malware dari aplikasi crack Adobe Photoshop untuk dianalisis lebih lanjut.

### 2. Pengujian di Mesin Virtual (Virtual Machine)

Setelah mendapatkan sampel, pengujian dilakukan pada lingkungan virtual yang menggunakan Virtual Machine berbasis Windows 10. Lingkungan virtual ini dipilih agar penelitian dapat dilakukan dengan aman tanpa merusak sistem fisik. Mesin virtual dikonfigurasi dengan jaringan internal tanpa koneksi internet untuk mencegah malware berkomunikasi dengan server command-and-control eksternal.

- Spesifikasi Mesin Virtual:

1) Sistem Operasi: Windows 10 Pro, 64-bit.
2) RAM: 4 GB.
3) Storage: 60 GB.
4) Jaringan: Internal Network (No Internet).

- Tahap Pengujian:

1) Instalasi crack Adobe Photoshop di mesin virtual.
2) Pencatatan perubahan awal sebelum instalasi untuk dijadikan baseline.

### 3. Pemantauan Aktivitas Malware

Selama pengujian, aktivitas malware dipantau secara real-time menggunakan berbagai alat forensik digital untuk mendeteksi perubahan pada file sistem, entri registry, dan lalu lintas jaringan. Pemantauan dilakukan untuk mengidentifikasi perilaku berbahaya yang mungkin muncul selama atau setelah instalasi crack. Alat-alat yang digunakan antara lain:

1) Process Monitor: Mengamati proses yang berjalan, perubahan pada file sistem, dan registry yang diakses oleh malware.
2) Wireshark: Mengumpulkan dan menganalisis paket jaringan untuk mendeteksi komunikasi mencurigakan yang mungkin mengindikasikan koneksi ke server jarak jauh.
3) Registry Editor: Memantau perubahan registry untuk melihat apakah malware mencoba menanamkan dirinya di sistem agar tetap berjalan setelah reboot.

### 4. Analisis Dampak Malware

Tahapan ini fokus pada analisis dampak malware terhadap kinerja dan stabilitas sistem. Peneliti mengamati beberapa indikator utama seperti penggunaan CPU, memori, perubahan file sistem, serta munculnya proses baru yang tidak sah. Aktivitas yang dicurigai sebagai perilaku malware (misalnya enkripsi file, modifikasi file sistem) dicatat dan dibandingkan dengan baseline yang telah diambil sebelumnya.

- Kategori Dampak yang Dianalisis:

1) Perubahan File Sistem: Melihat apakah ada file yang dimodifikasi atau ditambahkan oleh malware.
2) Perubahan Registry: Analisis entri registry yang diubah atau dibuat oleh malware.
3) Dampak Kinerja: Mengukur penggunaan CPU dan RAM sebelum dan sesudah infeksi.

**5. Penyusunan Strategi Mitigasi**

Berdasarkan hasil analisis, strategi mitigasi disusun untuk membantu pengguna dalam mencegah infeksi serupa di masa depan. Rekomendasi ini meliputi langkah-langkah teknis seperti penerapan kebijakan keamanan, penggunaan perangkat lunak anti-malware yang kuat, serta pembatasan akses ke situs-situs berisiko.

- Rincian Mitigasi:

1) Peningkatan Keamanan Sistem: Menggunakan perangkat lunak keamanan yang lebih kuat.
2) Penetapan Kebijakan Penggunaan Perangkat Lunak: Melarang penggunaan perangkat lunak bajakan.
3) Edukasi Pengguna: Meningkatkan kesadaran tentang risiko yang ditimbulkan oleh crack.

## 3. HASIL DAN PEMBAHASAN

**Identifikasi Pola Serangan Malware**

Penelitian ini menemukan dua malware utama yang tersembunyi di dalam crack Adobe Photoshop, yaitu Trojan Emotet dan Ransomware Locky. Keduanya memiliki cara kerja dan teknik penyebaran yang berbeda. Untuk mendeteksi aktivitas malware ini, crack Adobe Photoshop dijalankan pada sistem Windows 10 di lingkungan virtual yang dipantau menggunakan alat pemantauan seperti Process Monitor, Wireshark, dan Registry Editor. Berdasarkan hasil pemantauan, berikut pola serangan dari kedua malware tersebut:

**1. Trojan Emotet**

- Penyebaran: Trojan ini menyamarkan dirinya sebagai installer Adobe Photoshop yang seolah-olah sah. Ketika pengguna mengunduh dan memasang crack tersebut, Emotet secara otomatis aktif tanpa menunjukkan tanda-tanda awal yang mencolok.
- Modus Operandi: Trojan ini memodifikasi entri registry dan mengganti beberapa file sistem utama seperti winlogon.exe dan svchost.exe. Hal ini memungkinkan malware untuk menanamkan dirinya di sistem dan tetap aktif bahkan setelah komputer direstart.
- Dampak: Setelah masuk ke dalam sistem, Emotet mencuri informasi penting seperti kata sandi, data login, dan informasi keuangan pengguna. Selain itu, malware ini membuka backdoor yang memungkinkan penyerang mengakses perangkat secara jarak jauh, sehingga mereka dapat mengunduh dan menjalankan program jahat lainnya di komputer korban.

**2. Ransomware Locky**

- Penyebaran: Locky hanya aktif saat pengguna membuka aplikasi Adobe Photoshop yang telah diinstal. Begitu dijalankan, ransomware ini mengenkripsi semua file di direktori C:\ menggunakan ekstensi .locky.
- Modus Operandi: Menggunakan algoritma enkripsi AES-256, ransomware ini mengunci file yang ada di komputer, membuatnya tidak dapat diakses tanpa kunci dekripsi. Setelah semua file terenkripsi, Locky akan menampilkan pesan yang berisi permintaan tebusan dalam bentuk mata uang kripto (Bitcoin).
- Dampak: File yang telah terenkripsi tidak dapat diakses oleh pengguna. Tanpa kunci dekripsi yang diminta oleh penyerang, pemulihan file hampir tidak mungkin dilakukan

**Dampak Keamanan pada Sistem Operasi Windows**

Infeksi dari Trojan Emotet dan Ransomware Locky memberikan dampak yang serius terhadap keamanan sistem Windows dan berpotensi mengganggu stabilitas serta kerahasiaan data pengguna. Berikut adalah dampak utama yang ditemukan:

- Modifikasi File Sistem Emotet secara diam-diam mengubah file sistem Windows yang penting, seperti winlogon.exe dan svchost.exe. File-file ini biasanya menjalankan fungsi sistem kritis di latar belakang. Modifikasi ini memungkinkan Trojan tetap tersembunyi dan aktif meskipun sistem direstart. Selain itu, perubahan ini dapat menyebabkan malfungsi sistem seperti proses booting

yang gagal atau layanan sistem yang berhenti secara tiba-tiba.

- Pencurian Data Pribadi Trojan ini didesain untuk mengambil informasi sensitif pengguna, termasuk kredensial login, data keuangan, dan informasi pribadi lainnya. Emotet menggunakan metode injeksi pada browser yang mengumpulkan informasi ketika pengguna melakukan login ke situs-situs tertentu. Data yang terkumpul dikirim ke server penyerang, yang kemudian digunakan untuk aktivitas kejahatan siber seperti pencurian identitas dan pengambilalihan akun.
- Penguncian File oleh Ransomware Locky menggunakan enkripsi AES-256 untuk mengunci file pengguna, yang dikenal sebagai salah satu algoritma enkripsi paling kuat dan sulit untuk dipecahkan tanpa kunci dekripsi. Setelah proses enkripsi selesai, ransomware ini menghapus salinan bayangan (shadow copy) yang biasanya digunakan untuk pemulihan data. Hal ini membuat pemulihan file hampir tidak mungkin dilakukan tanpa membayar tebusan yang diminta oleh penyerang.

**Rekomendasi dan Strategi Mitigasi**

Berdasarkan hasil analisis, berikut beberapa rekomendasi untuk mencegah serangan serupa di masa depan:

- Gunakan Software Resmi Hindari penggunaan perangkat lunak bajakan atau crack. Disarankan untuk mengunduh perangkat lunak dari situs resmi serta menggunakan lisensi asli untuk mengurangi risiko infeksi malware.
- Pantau Aktivitas Sistem Gunakan alat monitoring seperti Process Monitor dan Sysmon untuk mendeteksi aktivitas yang mencurigakan. Perubahan penggunaan CPU, proses yang tidak wajar, serta perubahan registry harus diawasi dengan ketat.
- Lakukan Backup Data Secara Berkala Buat cadangan data secara rutin di perangkat terpisah seperti hard drive eksternal atau penyimpanan awan (cloud storage). Ini penting untuk memastikan data masih dapat dipulihkan jika terjadi serangan ransomware.
- Terapkan Keamanan Berlapis Gunakan kombinasi firewall, perangkat lunak anti-malware yang selalu diperbarui, serta pembatasan hak akses pada aplikasi pihak ketiga untuk mencegah penyebaran malware dari aplikasi yang tidak sah.

Dengan menerapkan strategi-strategi ini, risiko serangan malware dapat diminimalkan dan keamanan sistem dapat ditingkatkan secara signifikan, sehingga serangan dari penggunaan aplikasi crack di masa depan dapat dihindari

## 4. KESIMPULAN

Penelitian ini menyimpulkan bahwa penggunaan crack Adobe Photoshop sangat berbahaya bagi keamanan sistem Windows karena berpotensi menyebarkan malware seperti Trojan Emotet dan Ransomware Locky. Trojan Emotet mampu mencuri data penting dan memodifikasi sistem, sedangkan Ransomware Locky dapat mengunci file dan meminta tebusan. Akibatnya, pengguna berisiko kehilangan data dan privasi mereka. Oleh karena itu, penggunaan perangkat lunak asli, pembaruan sistem secara rutin, serta pemantauan aktivitas sistem sangat disarankan untuk mencegah serangan di masa depan.

## 5. DAFTAR PUSTAKA

Budiman, A., & Setiawan, D. (2020). Deteksi dan Pencegahan Malware Ransomware pada Sistem Windows Menggunakan Algoritma Machine Learning. Jurnal Keamanan Siber, 3(1), 30-39.

Yulianto, F., & Pratama, D. (2021). Eksplorasi Malware dalam Perangkat Lunak Bajakan: Studi Kasus Adobe Photoshop. Jurnal Keamanan Sistem Informasi, 13(4), 120-128.

Wahyudi, A., & Subekti, H. (2017). Studi Kasus Ransomware Locky pada Lingkungan Virtual Machine Windows 10. Jurnal Teknologi Informasi dan Keamanan, 9(3), 100-109.

Rahmawati, D., & Saputra, M. (2018). Analisis Kerentanan Sistem Operasi Windows Terhadap Serangan Ransomware. Jurnal Informatika dan Keamanan Siber, 2(1), 17-25.

Setiawan, B., & Nugraha, A. (2017). Implementasi Algoritma Keamanan Berlapis untuk Pencegahan Malware pada

Sistem Windows. Jurnal Keamanan Teknologi Informasi, 7(2), 90-98.

Ramdani, H., & Firmansyah, D. (2020). Pendeteksian Aktivitas Malware Menggunakan Proses Monitor pada Sistem Windows 10. Jurnal Forensik Digital, 6(3), 44-52.