ANALISIS FORENSIK *MALWARE* PADA PLATFORM WHATSAPP PERANGKAT MOBILE ANDROID MENGGUNAKAN FRAMEWORK D4I

SKRIPSI

Disusun Oleh:
M. KHOTIBUL UMAM
09020620031

PROGRAM STUDI SISTEM INFORMASI
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL
SURABAYA
2023

PERNYATAAN KEASLIAN

JUDUL	:	ANALISIS FORENSIK MALWARE PADA PLATFORM WHATSAPP PERANGKAT MOBILE ANDROID MENGGUNAKAN FRAMEWORK D4I
NAMA	:	M.KHOTIBUL UMAM
NIM	:	09020620031
ANGKATAN	:	2020

Menyatakan bahwa saya tidak melakukan plagiat dalam penulisan skripsi saya yang berjudul: "ANALISIS FORENSIK MALWARE PADA PLATFORM WHATSAPP PERANGKAT MOBILE ANDROID MENGGUNAKAN FRAMEWORK D4I". Apabila suatu saat nanti terbukti saya melakukan tindakan plagiat, maka saya bersedia menerima sanksi yang telah diterapkan.

Demikian pernyataan keaslian ini saya buat dengan sebenar-benarnya.

Surabaya, 04 Januari 2024

Yang menyatakan,

(M. KHOTIBUL UMAM)

NIM. 09020620031

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi oleh:

Nama : M. KHOTIBUL UMAM

Nim : 09020620031

Judul : ANALISIS FORENSIK MALWARE PADA PLATFORM WHATSAPP PERANGKAT MOBILE ANDROID MENGGUNAKAN FRAMEWORK D4I

Ini telah diperiksa dan disetujui untuk diujikan.

Surabaya, 21 Desember 2023

Menyetujui,

Dosen Pembimbing 1	Dosen Pembimbing 2
(Muhammad Andik Izzuddin, M.T)	(Subhan Nooriansyah, M.Kom.)
NIP. 198403072014031001	NIP. 199012282020121010

LEMBAR PENGESAHAN TIM PENGUJI SKRIPSI

Skripsi M.Khotibul Umam ini telah dipertahankan
didepan tim penguji skripsi
di Surabaya, 03 Januari 2024

Mengesahkan,
Dewan Penguji

Penguji I	Penguji II
Dr. Achmad Teguh Wibowo, M.T., MTCNA	Ahmad Yusuf, M.Kom
NIP. 198810262014031003	NIP. 199001202014031003

Penguji III	Penguji IV
Muhammad Andik Izzuddin, M.T	Subhan Nooriansyah, M.Kom.
NIP. 198403072014031001	NIP. 199012282020121010

Mengetahui,
Dekan Fakultas Sains dan Teknologi
UIN Sunan Ampel Surabaya

Dr. A. Saepul Hamdani, M.Pd
NIP. 196507312000031002

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN AMPEL SURABAYA
PERPUSTAKAAN
Jl. Jend. A. Yani 117 Surabaya 60237 Telp. 031-8431972 Fax.031-8413300
E-Mail: perpus@uinsby.ac.id

LEMBAR PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademika UIN Sunan Ampel Surabaya, yang bertanda tangan di bawah ini, saya:

Nama : M.KHOTIBUL UMAM
NIM : 09020620031
Fakultas/Jurusan : SAINS DAN TEKNOLOGI / SISTEM INFORMASI
E-mail address : khotib.bul@gmail.com

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Perpustakaan UIN Sunan Ampel Surabaya, Hak Bebas Royalti Non-Eksklusif atas karya ilmiah :
■ Sekripsi ☐ Tesis ☐ Desertasi ☐ Lain-lain (.....)
yang berjudul :
ANALISIS FORENSIK MALWARE PADA PLATFORM WHATSAPP PERANGKAT *MOBILE ANDROID MENGGUNAKAN FRAMEWORK D4I*

beserta perangkat yang diperlukan (bila ada). Dengan Hak Bebas Royalti Non-Ekslusif ini Perpustakaan UIN Sunan Ampel Surabaya berhak menyimpan, mengalih-media/format-kan, mengelolanya dalam bentuk pangkalan data (database), mendistribusikannya, dan menampilkan/mempublikasikannya di Internet atau media lain secara ***fulltext*** untuk kepentingan akademis tanpa perlu meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan atau penerbit yang bersangkutan.

Saya bersedia untuk menanggung secara pribadi, tanpa melibatkan pihak Perpustakaan UIN Sunan Ampel Surabaya, segala bentuk tuntutan hukum yang timbul atas pelanggaran Hak Cipta dalam karya ilmiah saya ini.

Demikian pernyataan ini yang saya buat dengan sebenarnya.

Surabaya, 07 Januari 2024

Penulis

(M.KHOTIBUL UMAM)

ABSTRAK

Sistem operasi Android, sebagai salah satu sistem operasi smartphone paling populer di dunia, memiliki pangsa pasar yang signifikan. Namun, popularitasnya juga menciptakan peluang bagi pengembang aplikasi yang tidak bermaksud baik untuk memanfaatkan celah keamanan. Penelitian ini memfokuskan analisis forensik terhadap *malware* dengan format .apk yang disebarkan melalui *platform* WhatsApp pada perangkat *mobile* Android. Menggunakan framework D4I, penelitian ini mengidentifikasi serangkaian tindakan berbahaya dari fase instalasi hingga aksi pada objek dalam *Cyber Kill Chain* (CKC). Hasil analisis menunjukkan kompleksitas modus operandi *malware* dan efektivitas Framework D4I dalam memahami dan mengidentifikasi ancaman keamanan. Penelitian ini memberikan wawasan yang mendalam terhadap risiko dan mekanisme serangan serta menyajikan rekomendasi untuk memperkuat keamanan perangkat Android dari ancaman siber yang semakin kompleks.

Kata Kunci : Android, Malware, Analisis Forensik, framework D4I, Cyber Kill Chain (CKC), Keamanan Android

ABSTRACT

The Android operating system stands as one of the most popular smartphone platforms globally, holding a significant market share. However, its widespread usage also presents opportunities for malicious developers to exploit security vulnerabilities. This research centers on the forensic analysis of malware in the .apk format distributed via the WhatsApp platform on Android mobile devices. Employing D4I framework, the study identifies a series of malicious actions from the installation phase to actions on objects within the Cyber Kill Chain (CKC). The analysis reveals the intricacies of the malware's modus operandi and highlights the effectiveness of the D4I framework in comprehending and identifying security threats. This research provides in-depth insights into the risks and mechanisms of attacks, presenting recommendations to enhance Android device security against evolving cyber threats.

Keywords : Android, Malware, Forensic Analysis, D4I Framework, Cyber Kill Chain (CKC), Android Security.

DAFTAR ISI

LEMBAR PERSETUJUAN PEMBIMBING ..... **III**
LEMBAR PENGESAHAN TIM PENGUJI SKRIPSI ..... **IV**
PERNYATAAN KEASLIAN ..... **V**
LEMBAR PERSETUJUAN PUBLIKASI KARYA ILMIAH ..... **VI**
MOTTO ..... **VII**
UCAPAN TERIMAKASIH ..... **VIII**
KATA PENGANTAR ..... **IX**
ABSTRAK ..... **X**
ABSTRACT ..... **XI**
DAFTAR ISI ..... **XII**
DAFTAR GAMBAR ..... **XV**
DAFTAR TABEL ..... **XVI**
DAFTAR LAMPIRAN ..... **XVII**
BAB I **1**
PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Perumusan Masalah 4
1.3 Batasan Masalah 4
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 5
1.6 Sistematika Penulisan Skripsi 5
BAB II **7**
TINJAUAN PUSTAKA **7**
2.1 Penelitian Terdahulu 7
2.2 Dasar Teori 10
2.2.1 Integrasi Manajemen IT 10
2.2.2 Android 11
2.2.3 Malware 11
2.2.4 Malware Android 12
2.2.5 Phising 15
2.2.6 Malware Analysis 15
2.2.7 Android Debug Bridge (ADB) 16

2.2.8 NIST 17
2.2.9 Cyber Kill Chain 17
2.2.10 D4I Framework 18
2.2.11 Qu1cksc0pe - All-in-One malware analysis tool. 20
2.2.12 Smseye 22
2.2.13 VirtualBox 23
2.2.14 Kali Linux 23
2.3 Integrasi Keilmuan 24
BAB III **26**
METODOLOGI PENELITIAN **26**
3.1 Identifikasi Masalah 27
3.2 Persiapan Penelitian 27
3.2.1 Studi Literatur 27
3.2.2 Persiapan Bahan 27
3.2.3 Pembuatan Skenario 29
3.3 Analisis *Malware* 31
3.3.1 Analisis Statik 32
3.3.2 Analisis Dinamik 32
3.4 Analisis Forensik Menggunakan *Framework* D4I 33
3.4.1 Pilih Fase CKC 33
3.4.2 Identifikasi dan kategorisasi artefak 33
3.4.3 Korelasi dan pengelompokan artefak 33
3.4.4 Membangun Chain of corelate Artifact (CoA) 33
3.4.5 Analisis pola dan metode penyerang 33
3.4.6 Eksplorasi lanjutan 34
3.4.7 Pembahasan 34
BAB IV **35**
HASIL DAN PEMBAHASAN **35**
4.1 Hasil Analisis Statik 35
4.1.1 Analisis Statik Awal (analyze) 35
4.1.2 Analisis VirusTotal (vtFile) 39
4.2 Hasil Analisis Dinamik 41
4.2.1 Skenario A 41
4.2.2 Skenario B 43

4.3 Hasil Analisis Forensik Menggunakan Framework D4I 46
4.3.1 Pemilihan Fase CKC 46
4.3.2 Identifikasi Artefak 46
4.3.3 Korelasi Artefak 47
4.3.4 Membangun CoA 49
4.3.5 Analisis CoA 49
4.3.6 Eksplorasi Lanjutan 50
4.3.7 Pembahasan 51
BAB V **53**
PENUTUP **53**
5.1 Kesimpulan 53
5.2 Saran 54
DAFTAR PUSTAKA **55**
LAMPIRAN **65**

DAFTAR GAMBAR

Gambar 2.1 Tahapan Forensik Digital NIST 17
Gambar 2.2 Tahapan Cyber Kill Chain (CKC) 18
Gambar 2.3 Tahapan forensik D4I 19
Gambar 3.1 Alur Penelitian 26
Gambar 4.1 Analisis dinamik Redmi Note 7 (Online) 41
Gambar 4.2 Analisis dinamik Oppo A7 (Online) 42
Gambar 4.3 Analisis dinamik Redmi 6A (Online) 43
Gambar 4.4 Analisis dinamik Redmi Note 7 (Offline) 43
Gambar 4.5 Analisis dinamik Oppo A7 (Offline) 44
Gambar 4.6 Analisis dinamik Redmi 6A (Offline) 45
Gambar 4.7 Chain of Correlate Artifacts 49

DAFTAR TABEL

Tabel 2.1 Penelitian Terdahulu 7
Tabel 2..2 Pemetaan Fase Cyber-Kill-Chain 19
Tabel 3.1 Skenario A 30
Tabel 3.1 Skenario B 30
Tabel 4.1 Permission 36
Tabel 4.2 Activities 37
Tabel 4.3 Receiver 37
Tabel 4.4 Statistics About Categories and Components 37
Tabel 4.5 Extracted URL Values 38
Tabel 4.6 Security 39
Tabel 4.7 Exported Activities 39
Tabel 4.8 Threat Categories 40
Tabel 4.9 Threat Names 40
Tabel 4.10 Deteksi Antivirus 40
Tabel 4.11 Identifikasi Artefak 46
Tabel 4.12 Korelasi Artefak 47

DAFTAR LAMPIRAN

Lampiran 1 Analisi awal (Analyze) **.....63**
Lampiran 2 Analisi Virus Total (vtFile) **.....75**
Lampiran 3 Skenario A Redmi Note 7 **.....76**
Lampiran 4 Skenario A Oppo A7 **.....76**
Lampiran 5 Skenario A Redmi 6A **.....77**
Lampiran 6 Skenario B Redmi Note 7 **.....78**
Lampiran 7 Skenario B Oppo A7 **.....79**
Lampiran 8 Skenario A Redmi 6A **.....80**

DAFTAR PUSTAKA

Acharya, Saket, Umashankar Rawat, And Roheet Bhatnagar. 2022. "A Comprehensive Review Of Android Security: Threats, Vulnerabilities, Malware Detection, And Analysis." *Security And Communication Networks*. Https://Doi.Org/10.1155/2022/7775917.

Aji, Adnan Bayu. 2017. "Pemanfaatan Keylogger Berbasis Spyware Untuk Memonitoring Aktivitas Penggunaan Keyboard User." *Prosiding SNATIF Ke-4 Tahun 2017*.

Anggraini, Indra, Yesi Novaria Kunang, And Firdaus. 2020. "Penerapan Naive Bayes Pada Detection Malware Dengan Diskritisasi Variabel." *Telematika* 13 (1): 11–21. Https://Doi.Org/10.35671/Telematika.V13i1.886.

Anwar, Nuril, Son Ali Akbar, Ahmad Azhari, And Imam Suryanto. 2020. "Ekstraksi Logis Forensik Mobile Pada Aplikasi E-Commerce Android." *Mobile And Forensics* 2 (1): 1–10. Https://Doi.Org/10.12928/Mf.V2i1.1791.

Aprilliansyah, Deco, Imam Riadi, And Sunardi. 2022. "Analysis Of Remote Access Trojan Attack Using Android Debug Bridge." *IJID (International Journal On Informatics For Development)* 10 (2). Https://Doi.Org/10.14421/Ijid.2021.2839.

Apriyandi, D, And T M EL6115. 2016. "Penanganan Insiden Pada Malware Android." *Budi.Rahardjo.Id*.

Ariyianingsih, Sindy, Ari A. Andrianto, Surya Adri Kusuma, And Rezi. 2023. "Korelasi Kejahatan Siber Dengan Percepatandigitalisasi Di Indonesia." *Jurnal Ilmu Hukum*, May.

Ashawa, Moses, And Sarah Morris. 2019. "Analysis Of Android Malware Detection Techniques: A Systematic Review." Http://Sdiwc.Net/Digital-Library/Analysis-Of-Android-Malware-Detection-Techniques-A-Systematic-Review.

Benufinit, Yonly Adrianus, And Jhon Enstein. 2021. "Analisa Sikap Responsif Mahasiswa Terhadap Simulasi Oracle Virtualbox Pada Matakuliah Sistem Operasi." *Jurnal Pendidikan Teknologi Informasi (JUKANTI)* 4 (2): 11–18.

BSSN. 2022. "Keamanan Siber Indonesia 2022."

Cahyanto, Triawan Adi, Victor Wahanggara, And Darmawan Ramadana. 2017. "Analisis Dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis Dan Malware Analisis Statis." *Jurnal Sistem & Teknologi Informasi Indonesia* 2 (1).

Cannarile, Angelo, Vincenzo Dentamaro, Stefano Galantucci, Andrea Iannacone, Donato Impedovo, And Giuseppe Pirlo. 2022. "Comparing Deep Learning And Shallow Learning Techniques For API Calls Malware Prediction: A Study." *Applied Sciences (Switzerland)* 12 (3). Https://Doi.Org/10.3390/App12031645.

Catak, Ferhat Ozgur, Ahmet Faruk Yazi, Ogerta Elezaj, And Javed Ahmed. 2020. "Deep Learning Based Sequential Model For Malware Analysis Using Windows Exe API Calls." *Peerj Computer Science* 6. Https://Doi.Org/10.7717/PEERJ-CS.285.

Caturiyanto, Totok Wahyu, Arief Setyanto, And Eko Pramono. 2020. "Analisa Dan Perbandingan Performa Hypervisor Esxi, XEN, VMWARE Workstation Pro, Dan Virtualbox." *Jurnal Informa : Jurnal Penelitian Dan Pengabdian Masyarakat* 6 (2). Https://Doi.Org/10.46808/Informa.V6i2.182.

Chandrasena, Sampath. 2022. "Data Preservation And Risk Management In Management Information Systems." *South Florida Journal Of Development* 3 (1): 1459–79. Https://Doi.Org/10.46932/Sfjdv3n1-112.

Dandotiya, Monika. 2022. "A Secure Detection Framework For ARP, DHCP, And Dos Attacks On Kali Linux." *International Journal For Research In Applied Science And Engineering Technology* 10 (7). Https://Doi.Org/10.22214/Ijraset.2022.42176.

Army, A. (2023). Sms Eye. [online] GitHub. Available at: https://github.com/AbyssalArmy/SmsEye [Accessed 28 Dec. 2023].

Danilo Jaramillo, H., S. Armando Cabrera, E. Marco Abad, V. Alfredo Torres, And José Carrillo Verdúm. 2015. "Definition Of Cybersecurity Businness Framework Based On ADM-TOGAF." In *2015 10th Iberian Conference On Information Systems And Technologies, CISTI 2015*. Https://Doi.Org/10.1109/CISTI.2015.7170391.

Diana, Diana, Richardus Eko Indrajit, And Erick Dazki. 2022. "Komparasi Algoritma Naïve Bayes, Logistic Regression Dan Support Vector Machine Pada Klasifikasi File Application Package Kit Android Malware." *Jutisi : Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi* 11 (1). Https://Doi.Org/10.35889/Jutisi.V11i1.815.

Dimitriadis, Athanasios, Nenad Ivezic, Boonserm Kulvatunyou, And Ioannis Mavridis. 2020. "D4I - Digital Forensics Framework For Reviewing And Investigating Cyber Attacks." *Array* 5 (March): 100015. Https://Doi.Org/10.1016/J.Array.2019.100015.

Fachri, Fahmi, Abdul Fadlil, Imam Riadi, Ahmad Dahlan, Yogyakarta Jln Soepomo, And Informasi Artikel. 2021. "Analisis Keamanan Webserver Menggunakan Penetration Test." *JURNAL INFORMATIKA* 8 (2). Http://Ejournal.Bsi.Ac.Id/Ejurnal/Index.Php/Ji.

Fairuz, Fairuzabietamam. 2021. "Model Model Penyebaran Malware Pada Jaringan Komputer." *Jurnal Ilmiah Betrik* 12 (1). Https://Doi.Org/10.36050/Betrik.V12i1.259.

Farhan Febrianto, Achmad, Avon Budiono, And Ahmad Almaarif. 2019. "Analisis Malware Pada Sistem Operasi Android Menggunakan Metode Network Traffic Analysis Malware Analysis In Android Operating System Using Network Traffic Analysis Method."

Zulkifli, S.E., M.M, Arief Budi Pratomo, S.Kom., M.MSI, Ibrahim, A., Adhani, I., Dr. Hj. Umalihayati, S.ST., S.KM., M.Pd, Faridatun Nadziroh, S.ST., M.T, Subhan, Hatta, R., Okki Navarone Wibisono, S.E., M.Si., M.M and Ady, A.

(2023). TEKNOLOGI INFORMASI & MANAJEMEN. Cendikia Mulia Mandiri.

Putri Ramadhani (2019). Pengaruh Sistem Informasi Manajemen Dalam Meningkatkan Efektivitas Dan Efisiensi Pengelolaan Sekolah. Ina-Rxiv (OSF Preprints). doi:https://doi.org/10.31227/osf.io/58c3q.

Ficco, Massimo. 2022. "Malware Analysis By Combining Multiple Detectors And Observation Windows." *IEEE Transactions On Computers* 71 (6). Https://Doi.Org/10.1109/TC.2021.3082002.

Hasmin, Erfan. 2019. "Implementasi Algoritma Twofish Pada Keamanan Data Berbasis Aplikasi Android." *Seminar Nasional Sistem Informasi Dan Teknik Informatika Sensitif*.

Herlambang, Sendi, Setio Basuki, Denar Regata Akbi, Zamah Sari, And Kontak Person. 2018. "Seminar Nasional Teknologi Dan Rekayasa (SENTRA) 2018 ISSN (Cetak) 2527-6042 EISSN (Online)." Www.Virusshare.Com,.

Hutchins, Eric M, Michael J Cloppert, And Rohan M Amin. 2011. "Intelligence-Driven Computer Network Defense Informed By Analysis Of Adversary Campaigns And Intrusion Kill Chains."

Hutchinson, Shinelle, And Umit Karabiyik. 2019. "Forensic Analysis Of Spy In Android Devices." Https://Commons.Erau.Edu/Adfsl/2019/Paper-Presentation/3.

Indana Zulfa, Mulki, Silvester Tena, And Sampurna Dadi Rizkiono. 2023. "Aktivitas Sniffing Pada Malware Pencuri Uang Di Smartphone Android." *RENATA Jurnal Pengabdian Masyarakat Kita Semua*. Vol. 1. Https://Doi.Org/10.Xx/Paperid.

Ismail, Najiahtul Syafiqah, Halizah Saad, Robiah Yusof, And Mohd Faizal Abdollah. 2017. "General Android Malware Behaviour Taxonomy." *Defence S And T Technical Bulletin* 10 (2).

Ismiyushar, Naufal Abrian, M Teguh Kurniawan, And Adityas Widjajarto. 2018. "Analisis Dampak Malware Berdasarkan Api Call Dengan Metode Anomali Malware." *E-Proceeding Of Engineering* 5 (2).

Karayat, Ritik, Manish Jadhav, Lakshmi Sudha Kondaka, And Ashwath Nambiar. 2022. "Web Application Penetration Testing & Patch Development Using Kali Linux." In *8th International Conference On Advanced Computing And Communication Systems, ICACCS 2022*. Https://Doi.Org/10.1109/ICACCS54159.2022.9785232.

Kurnia Hatika, Leidy, Avon Budiyono, And Ahmad Almaarif. 2019. "Analisis Ketepatan Deteksi Malware Pada Software Antivirus Menggunakan Metode Analisis Statis Accuracy Analysis Of Malware Detection In Antivirus Software Using Static Analysis Method."

Leon, Roee S., Michael Kiperberg, Anat Anatey Leon Zabag, And Nezer Jacob Zaidenberg. 2021. "Hypervisor-Assisted Dynamic Malware Analysis." *Cybersecurity* 4 (1). Https://Doi.Org/10.1186/S42400-021-00083-9.

Li, Ping, And Yu Ju Lan. 2022. "Digital Language Learning (DLL): Insights From Behavior, Cognition, And The Brain." *Bilingualism* 25 (3). Https://Doi.Org/10.1017/S1366728921000353.

Malvi, Afif, And Painem Painem. 2020. "Pengamanan File Gambar Pada Media Video Dengan Kriptografi Algoritma RSA Dan Steganografi Algoritma End Of File (EOF)." *Informatik : Jurnal Ilmu Komputer* 16 (2). Https://Doi.Org/10.52958/Iftk.V16i2.1860.

Manalu, Andi Setiadi, And Sahat Sonang Sitanggang. 2019. "Perancangan Dan Implementasi Private Cloud Storage Dengan Owncloud Pada Jaringan Lokal Menggunakan Virtualbox." *Journal Of Computer Networks, Architecture, And High-Performance Computing* 1 (2). Https://Doi.Org/10.47709/Cnahpc.V1i2.244.

Meng, Guozhu, Matthew T Patrick, Yinxing Xue, Yang Liu, And Jie Zhang. 2019a. "Securing Android App Markets Via Modeling And Predicting Malware

Spread Between Markets." *IEEE Transactions On Information Forensics And Security* 14: 1944–59. Https://Api.Semanticscholar.Org/Corpusid:69659978.

Mertens, Xavier. 2023. "The Importance Of Malware Triage." *SANS Internet Storm Center*, 2023.

Mira, Fahad. 2021. "A Systematic Literature Review On Malware Analysis." In *2021 IEEE International IOT, Electronics And Mechatronics Conference, IEMTRONICS 2021 - Proceedings*. Https://Doi.Org/10.1109/IEMTRONICS52119.2021.9422537.

Mitra, Joydeep, Venkatesh-Prasad Ranganath, And Aditya Narkar. 2019. "Benchpress: Analyzing Android App Vulnerability Benchmark Suites," March. Https://Doi.Org/10.1109/ASEW.2019.00020.

National Institute Of Standards And Technolgy. 2020. *NIST Privacy Framework: A Tool For Improving Privacy Through Enterprise Risk Management*. *NIST Special Publication*.

Nugroho, Andre Ahmad. 2016. "Kajian Yuridis Malware Menurut Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Jurnal Mahasiswa Fakultas Hukum*.

Nur Iman, Anandika, Avon Budiyono, And Ahmad Almaarif. 2019. "Analisis Malware Pada Sistem Operasi Android Menggunakan Permission-Based Malware Analysis In Android Operation System Using Permission-Based."

Nurfiansyah, Adi, Yuli Sun Hariyani, And Dadan Nur Ramadan. 2018. "Desain Dan Implementasi Aplikasi Android Utnuk Memantau Status Tumbuh Kembang Balita Desain And Implementation Android Application For Monitoring Child Growth." *E-Proceeding Of Applied Science* 4 (3).

Nurindahsari, Fitri, And Bita Parga Zen. 2021. "Analisis Statik Keamanan Aplikasi Video Streaming Berbasis Android Menggunakan Mobile Security Framework (Mobsf) Security Static Analysis Of Android-Based Video Streaming Application Using Mobile Security Framework (Mobsf)." Vol. 4. Https://Databoks.Katadata.Co.Id.

Pangestu, Dwi, And Andrian Syahputra. 2020. “Perancangan Aplikasi Keamanan Cloud Database Menggunakan Operasi Xor Dengan Algoritma Affine Berbasis Android Design Of Cloud Database Safety Applications Using Xor Operation With Affine Algorithm Based On Android.” *54. IT Journal*. Vol. 8.

Pratiwi, Shiela Novelia Dharma, And Brodjol Sutijo Suprih Ulama. 2016. “Klasifikasi Email Spam Dengan Menggunakan Metode Support Vector Machine Dan K-Nearest Neighbor.” *Jurnal Sains Dan Seni ITS* 5 (2).

Priadi, Aidil Yusuf, And Arizal Arizal. 2022. “Impact Analysis Of Crypto Miner Malware Attacks Using Android Debug Bridge (ADB) Vulnerabilities Via TCP/IP On Android-Based Raspberry Pi 4 Iot Device.” In *Proceedings - 4th International Conference On Informatics, Multimedia, Cyber And Information System, ICIMCIS 2022*. Https://Doi.Org/10.1109/ICIMCIS56303.2022.10017625.

Puji Rahayu, Yunike Dwi, And Nanang Trianto. 2021. “Analisis Malware Menggunakan Metode Analisis Statis Dan Dinamis Untuk Pembuatan IOC Berdasarkan STIX Versi 2.1.” *Info Kripto* 15 (3). Https://Doi.Org/10.56706/Ik.V15i3.30.

Ramadhan, Andi, Lindawati Lindawati, And Martinus Mujur Rose. 2023. “Komparasi Algoritma Neural Network Dan K-Nearest Neighbor Dalam Mendeteksi Malware Android.” *Building Of Informatics, Technology And Science (BITS)* 5 (1). Https://Doi.Org/10.47065/Bits.V5i1.3538.

Razzaq, Abdul, Matthew Aditya, Amelia Widya, Octa Kuncoro Putri, Desta Lesmana Musthofa, And Pujo Widodo. 2022. “Serangan Hacking Tools Sebagai Ancaman Siber Dalam Sistem Pertahanan Negara (Studi Kasus: Predator).” *Global Political Studies Journal* 6. Https://Doi.Org/10.34010/Gpsjournal.V6i1.

Rizky, Laksamana Putra. 2019. “Analisis Aktivitas Malware Pada Ram Android Dan Sandbox Environment.”

Rusli, Mulyadi, Teuku Djauhari, Fattachul Huda Aminuddin, Junaidi Surya,) Fakultas, And Ilmu Komputer. 2022. "Sistem Informasi Pengenalan Batik Jambi Berbasis Android Pada Sangar Batik Olak Kemang Kota Jambi" 15 (1).

Sadlek, Lukas, Pavel Celeda, And Daniel Tovarnak. 2022. "Identification Of Attack Paths Using Kill Chain And Attack Graphs." In *Proceedings Of The IEEE/IFIP Network Operations And Management Symposium 2022: Network And Service Management In The Era Of Cloudification, Softwarization And Artificial Intelligence, NOMS 2022*. Https://Doi.Org/10.1109/NOMS54207.2022.9789803.

Sahfitri, Vivi. 2018. "Analisis Forensik Malware Pop-Up Ads Iklan Pada Platform Android." Https://Www.Researchgate.Net/Publication/328489181.

Saputra, Hendra, Setio Basuki, And Mahar Faiqurahman. 2019. "Implementasi Teknik Seleksi Fitur Pada Klasifikasi Malware Android Menggunakan Support Vector Machine (SVM)." *Repositor* 1 (1). Https://Doi.Org/10.22219/Repositor.V1i1.1.

Senanayake, Janaka, Harsha Kalutarage, And Mhd Omar Al-Kadri. 2021. "Android Mobile Malware Detection Using Machine Learning: A Systematic Review." *Electronics (Switzerland)*. MDPI AG. Https://Doi.Org/10.3390/Electronics10131606.

Shi, Chen, Chris Chao, Chun Cheng, And Yong Guan. 2021. "Forensic Analysis On Joker Family Android Malware." Https://Logger-Dyu6ojodva-Uk.A.Run.App.

Siddiq, Ahmad, Helda Yudiastuti, And Febriyanti Panjaitan. 2020. "Analisis Perilaku Malware Dengan Metode Surface Analysis Dan Runtime Analysis." *Journal Of Software Engineering Ampera* 1 (3). Https://Doi.Org/10.51519/Journalsea.V1i3.53.

Sinambela, Samuel, Aditya Robbi Pangestu, Rangga Feriyanto, And Fakultas Ilmu Komputer. 2020. "Analisis Aplikasi Malware Pada Android Dengan Metode Statik" 3: 2621–4970.

Army, A. (2023). Sms Eye. [online] GitHub. Available at: https://github.com/AbyssalArmy/SmsEye [Accessed 28 Dec. 2023].

Tarnowski, Ireneusz. 2023. "How To Use Cyber Kill Chain Model To Build Cybersecurity?" *Wroclaw Centre For Networking And Supercomputing, Wroclaw University Of Science And Technology*.

Valsamakis, Konstantinos. 2021. "University Of Piraeus School Of Information And Communication Technologies Department Of Digital Systems Postgraduate Program Of Studies Msc Digital Systems Security Windows Malware Analysis."

Victorius, Epifanio Juang, Avon Budiyono, Ahmad Almaarif, And S Kom. 2019. "Analisis Deteksi Malware Remote Access Trojan Menggunakan Dynamic Malware Analysis Detection Tools Berbasis Behaviour Malware Detection Analysis Of Remote Access Trojan With Behaviour-Based Dynamic Malware Analysis Detection Tools." In *E-Proceeding Of Engineering*.

Yang, Li, Lijun Wang, And Dongdong Zhang. 2017. "Malicious Behavior Analysis Of Android GUI Based On ADB." In *Proceedings - 2017 IEEE International Conference On Computational Science And Engineering And IEEE/IFIP International Conference On Embedded And Ubiquitous Computing, CSE And EUC 2017*. Vol. 2. Https://Doi.Org/10.1109/CSE-EUC.2017.211.

Yilmaz, Saliha, And Mastaneh Davis. 2023. "Hidden Permissions On Android: A Permission-Based Android Mobile Privacy Risk Model." In *European Conference On Information Warfare And Security, ECCWS*. Vol. 2023-June. Https://Doi.Org/10.34190/Eccws.22.1.1453.

Yong Wong, Miuyin, Matthew Landen, Manos Antonakakis, Douglas M. Blough, Elissa M. Redmiles, And Mustaque Ahamad. 2021. "An Inside Look Into The Practice Of Malware Analysis." In *Proceedings Of The ACM Conference On Computer And Communications Security*. Https://Doi.Org/10.1145/3460120.3484759.

Yuniati, Trihastuti, Aris Rafael Tambunan, And Yoso Adi Setyoko. 2022. "Implementasi Static Analysis Dan Background Process Untuk Mendeteksi

Malware Pada Aplikasi Android Dengan Mobile Security Framework." *LEDGER : Journal Informatic And Information Technology* 1 (2). Https://Doi.Org/10.20895/Ledger.V1i2.848.

Yusnanto, Tri, Muhammad Abdul Muin, And Sugeng Wahyudiono. 2022. "Analisa Infrastruktur Jaringan Wireless Dan Local Area Network (WLAN) Meggunakan Wireshark Serta Metode Penetration Testing Kali Linux." *Journal On Education* 4 (4). Https://Doi.Org/10.31004/Joe.V4i4.2175.

Lockheed Martin (2023). Cyber Kill Chain. [online] Lockheed Martin. Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Sadlek, L., Celeda, P. and Tovarnak, D. (2022). Identification of Attack Paths Using Kill Chain and Attack Graphs. NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. [online] doi:https://doi.org/10.1109/noms54207.2022.9789803.

Tarnowski, I. (2023). How to use cyber kill chain model to build cybersecurity? Wroclaw Centre for Networking and Supercomputing, Wroclaw University of Science and Technology.