On the Malware Detection Problem: Challenges & Novel Approaches

Marcus Botacin[1], Paulo Lício de Geus[2], André Grégio[1]

[1]Ph.D.
Federal University of Paraná (UFPR)
mfbotacin@inf.ufpr.br

[2]Co-Advisor
Institute of Computing - UNICAMP
paulo@lasca.ic.unicamp.br

[1]Advisor
Federal University of Paraná (UFPR)
gregio@inf.ufpr.br

Topics

Topics

Research Question

Why malware detection is still an open problem?

Formalization

1. **Why did current malware research work failed on providing greater security to actual systems?**
   1. Which types of research work have been conducted so-far?
   2. How research works have been conducted so-far?
   3. What are the limits and implications of this current scenario?
2. **What could be done to improve future malware research work to be successful in operating on actual scenarios?**
   1. Which type of research could be developed to support real-world needs?
   2. Which methods could be applied to malware research work developments to make them more successful in handling actual malware?
   3. Who are the stakeholder involved in designing research solutions that can be evolved to operate in actual scenarios?

Research Plan

Roadmap

- Systematic review of malware research literature.
- Identify development gaps fields.
- Bridge a sub-problem in each field.

Guideline

- Contributing in broadness in addition to contributing in depth.

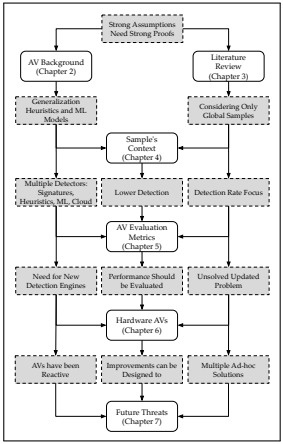


Figure: Thesis Organization

Topics

Publication

Figure: **Source:**
`https://www.sciencedirect.com/science/article/pii/S0167404821003242`

Which AVs to analyze?

Table: **Analyzed AVs.**

AV	Version	MD5
Avast	19.7.4674.0	172ee63bf3e0fa54abd656193d225013
AVG	19.8.4793.0	0d19e6fc1a4d239e02117f174d00d024
BitDefender	24.0.14.74	0e54eab75c8fd4059f3e97f771c737de
F-Secure	21.05.103.0	2393777281f3a9b11832558f5f3c0bce
Kaspersky	20.0.14.1085	7dc4fb6f026f9713dca49fc1941b22ce
MalwareBytes	3.0.0.199	9c69b2a22080c53521c6e88bd99686a1
Norton	22.17.1.50	2f1f762658dc7e41ecc66abd0270df97
TrendMicro	12.0	f8b8a3701ec53c7e716cf5008fad9aa1
Vipre	11.0.4.2	77a9dbd31ed5ebe490011ffa139afe03
WinDefender	4.18.1902.5	Built-in W10

What to analyze?

- Installation
- Uninstallation
- Updates
- Modularity
- Signatures
- Databases
- Real-Time Checks
- Machine Learning
- Cloud Scans
- Heuristics
- Attack Surface
- Self-Protection

Academic Production

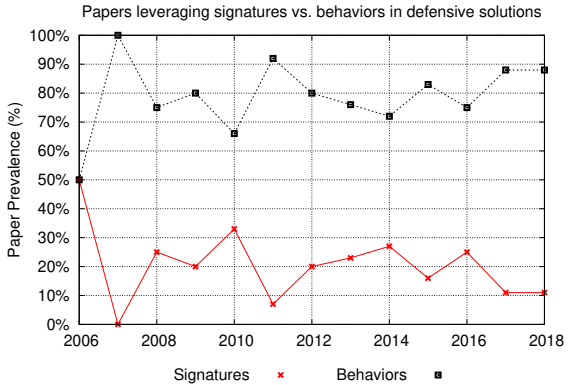


Figure: **Source:** Challenges and Pitfalls in Malware Research (2021).

Malware Detection Methods. Signatures vs. Behavioral (e.g., Machine Learning) approaches.

Signatures in Practice

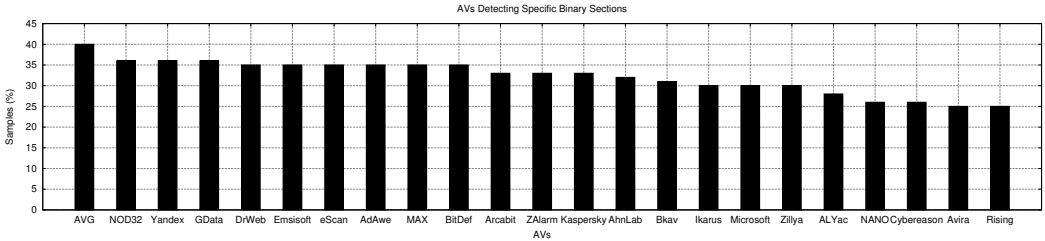


Figure: **Signature Prevalence.** Around a third of the AV's detections are based on specific section's contents.

Topics

Publication

Figure: **Link:**
`https://www.sciencedirect.com/science/article/pii/S0167404821001115`

Malware Literature Venues

Table: **Selected Papers**. Distribution per year (2000 – 2018) and per venue.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Total
USENIX (Security, LEET & WOOT)	1	0	0	0	0	1	1	6	2	3	7	8	10	12	9	7	9	13	6	95
CCS	0	0	0	0	0	0	0	2	4	6	6	7	11	9	11	14	2	11	6	89
ACSAC	0	0	0	0	2	3	2	4	4	1	3	8	10	7	10	6	3	7	8	78
IEEE S&P	0	1	0	0	0	1	3	2	1	0	0	10	17	12	3	6	4	5	3	68
DIMVA	0	0	0	0	0	4	4	3	8	2	3	0	8	4	8	7	7	5	4	67
NDSS	0	0	0	0	1	0	2	0	3	3	3	3	2	4	5	4	9	7	3	49
RAID	0	0	1	0	0	1	3	0	0	0	0	0	3	5	5	3	4	3	3	31
ESORICS	0	0	0	0	0	1	0	0	2	1	0	0	2	3	3	0	1	1	0	14
Total	1	1	1	0	3	11	15	17	24	16	22	36	63	56	54	47	39	52	33	491

A Method for Malware Research

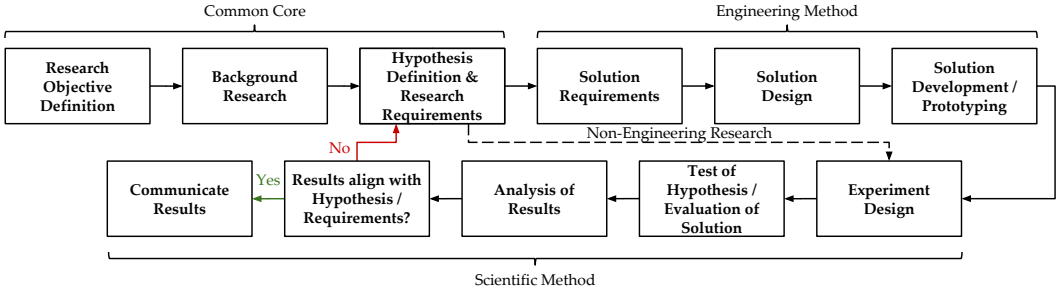
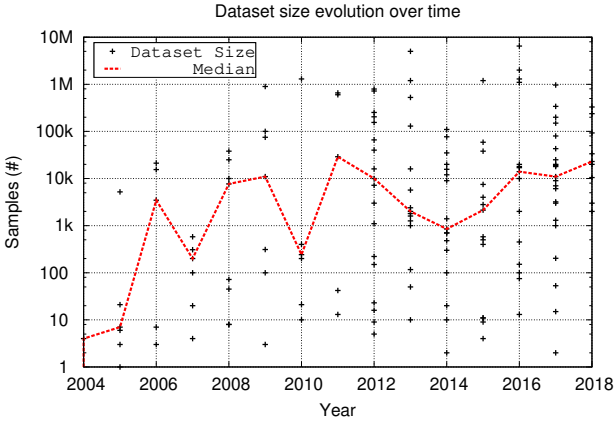


Figure: **Malware Research Method.** Integrating Science and Engineering.

Dataset Sizes



Dataset Size Definition

How to define how many samples are representative? Shouldn't we have some kind of guideline?

Summary

1. Inbalance in research work types.
2. Solutions developed not informed by previous study's data.
3. Most work still don't clearly state threat models.
4. Failure in positioning work as prototypes or real-world solutions.
5. Offline and online solutions developed and evaluated using the same criteria.
6. No dataset definition criteria.
7. Few attention to dataset representativity.
8. Most studies are not reproducible.
9. Sandbox execution criteria are not explained.
10. Non-homogeneous AV labels are still a problem.

Topics

Publication

RESEARCH-ARTICLE

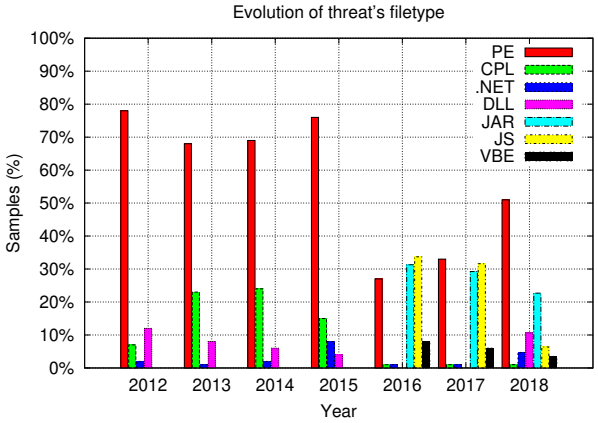
One Size Does Not Fit All: A Longitudinal Analysis of Brazilian Financial Malware

Authors: Marcus Botacin, Hojjat Aghakhani, Stefano Ortolani, Christopher Kruegel, Giovanni Vigna, Daniela Oliveira, Paulo Lício De Geus, André Grégio Authors Info & Affiliations

Publication: ACM Transactions on Privacy and Security • January 2021 • Article No.: 11 • https://doi.org/10.1145/3429741

Figure: **Link:** `https://dl.acm.org/doi/10.1145/3429741`

Brazilian Financial Malware Filetypes.



Brazilian malware filetypes.

Varied file formats are prevalent over the years.

Brazilian Financial Malware

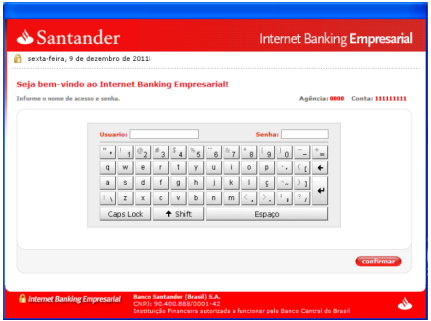


Figure: Passive Banker Malware for Santander bank waiting for user's credential input.

Figure: Passive Banker Malware for Itaú bank waiting for user's credential input.

Contextual Issues: Mobile Banking

RESEARCH-ARTICLE

The Internet Banking [in]Security Spiral: Past, Present, and Future of Online Banking Protection Mechanisms based on a Brazilian case study

Authors: Marcus Botacin, Anatoli Kalysch, André Grégio Authors Info & Affiliations

Publication: ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security • August 2019 • Article No.: 49 • Pages 1–10 • https://doi.org/10.1145/3339252.3340103

Figure: **Source:** `https://dl.acm.org/doi/10.1145/3339252.3340103`

Brazilian Financial Malware on Mobile

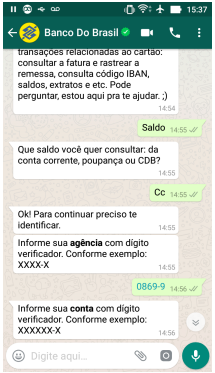


Figure: **BB's Whatsapp chatbot.**

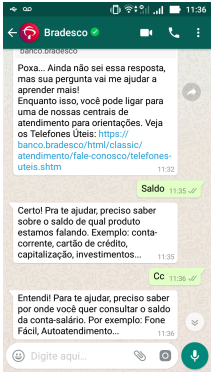


Figure: **Bradesco's Whatsapp chatbot.**

Research Impact

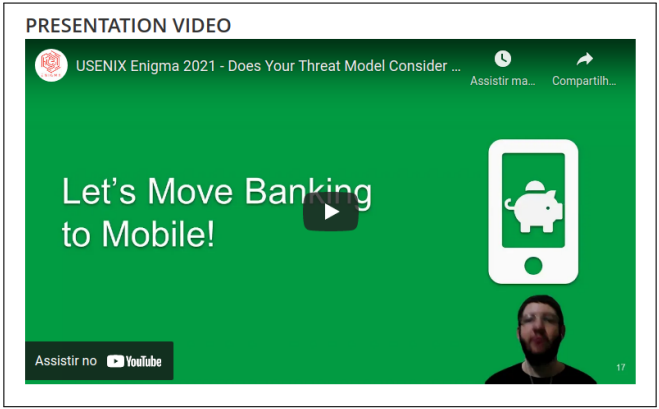


Figure: **Source:** `https://www.usenix.org/conference/enigma2021/presentation/botacin`

Topics

Publication

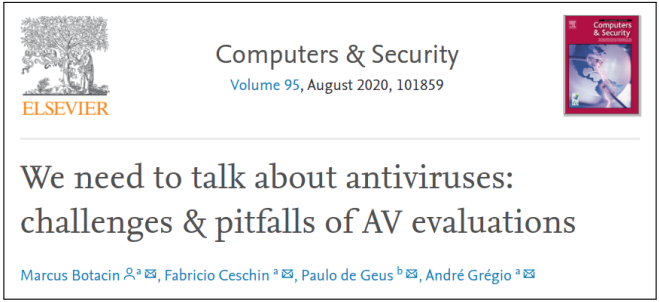
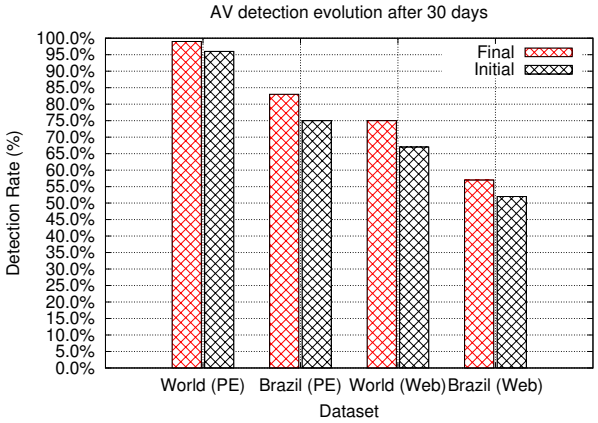


Figure: **Source:** `https://www.sciencedirect.com/science/article/pii/S0167404820301310`

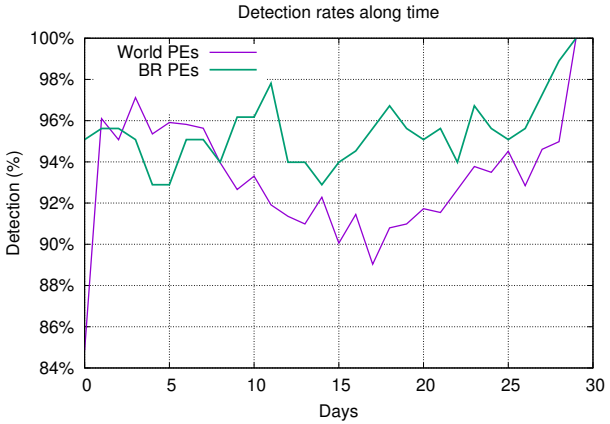
Detection Rates Over Time (1/2)



Initial and Final Detection Rates.

Detection rates increase in a 30-day period.

Detection Rates Over Time (2/2)



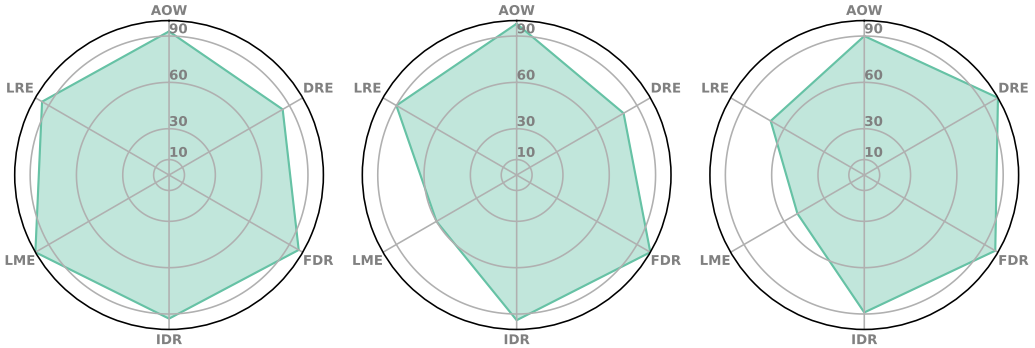
Detection Regression.

Some samples stop being detected after some time.

Summary.

- Initial Detection Rate (IDR)
- Final Detection Rate (FDR)
- Attack Opportunity Window (AOW)
- Detection Regression (DRE)
- Label Regression (LRE)
- Label Meaningfulness (LME)

Multi-Dimensional AV Evaluation.



(a) **AV1.** Recommended for incident response teams.

(b) **AV2.** Recommended for corporate users.

(c) **AV3.** Recommended for domestic users.

Figure: **AV's operational aspects**, considering the six proposed metrics.

Evaluation Metrics Adoption

> To take these factors into account, six anti-virus evaluation metrics are proposed in [BO20]. While each of them can certainly contribute to a more realistic assessment of an AV solution, some are more suitable than others for a given user profile, thus providing the methodology devised by Botacin *et al.* [BO20] with additional and much-needed flexibility.

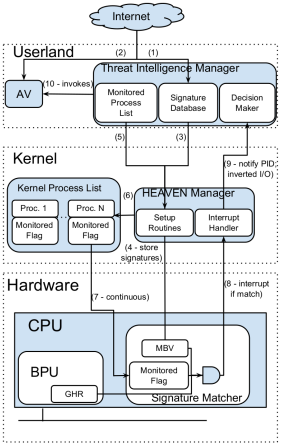
Figure: **Dissertation Source:**
`https://www.royalholloway.ac.uk/media/16565/techreport-giusepperaffa.pdf`.

> **3.4 Test Methodology**
>
> The recent work by Botacin *et al.* [BO20] has emphasized the importance of testing the detection rate of AV programs multiple times during an observation period. This approach, in fact, provides a more comprehensive evaluation, as it allows identifying possible regression effects and quantifying the effectiveness and efficiency of the anti-virus update mechanism.
>
> Therefore, taking into account the results of the study [BO20], the AVs considered for this project have been tested by executing four scans of the same set of malware samples over the course of three weeks. Each scan was run after updating the AV signature database.

Figure: **Dissertation Source:**
`https://www.royalholloway.ac.uk/media/16565/techreport-giusepperaffa.pdf`.

Topics

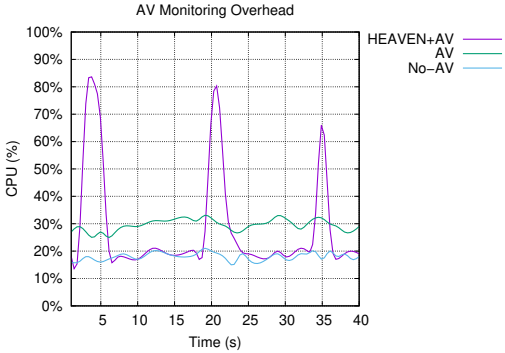
Hardware AV Architecture



2-level Architecture

Do not fully replace AVs, but add efficient matching capabilities to them.

Performance Characterization



2-Phase HEAVEN CPU Performance

The inspection phase causes occasional, and quick bursts of CPU usage. The AV operating alone incurs a continuous 10% performance overhead.

Hardware Solutions: Branch-Based Signatures

Figure: **Source:** `https://www.sciencedirect.com/science/article/abs/pii/S0957417422004882`

Hardware Solutions: FPGA AV

Figure: **Source:** `https://ieeexplore.ieee.org/document/9034972/`

Hardware Solutions: SMC Detector

Original Paper | Published: 13 February 2020

The self modifying code (SMC)-aware processor (SAP): a security look on architectural impact and support

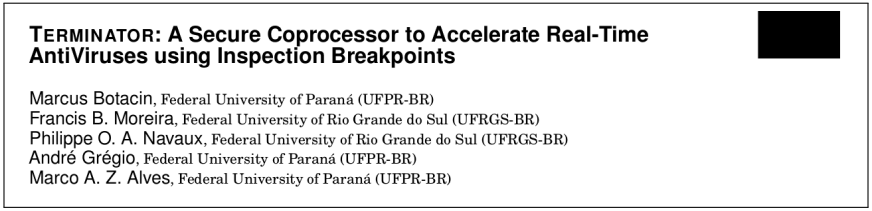
Marcus Botacin, Marco Zanata & André Grégio

Journal of Computer Virology and Hacking Techniques **16**, 185–196(2020) | Cite this article

198 Accesses | **3** Altmetric | Metrics

Figure: **Source:** `https://link.springer.com/article/10.1007/s11416-020-00348-w`

Hardware Solutions: Real-Time Processor



TERMINATOR: A Secure Coprocessor to Accelerate Real-Time AntiViruses using Inspection Breakpoints

Marcus Botacin, Federal University of Paraná (UFPR-BR)
Francis B. Moreira, Federal University of Rio Grande do Sul (UFRGS-BR)
Philippe O. A. Navaux, Federal University of Rio Grande do Sul (UFRGS-BR)
André Grégio, Federal University of Paraná (UFPR-BR)
Marco A. Z. Alves, Federal University of Paraná (UFPR-BR)

Figure: **Source:** To Appear Soon (ACM TOPS).

Result: Performance penalty reduction

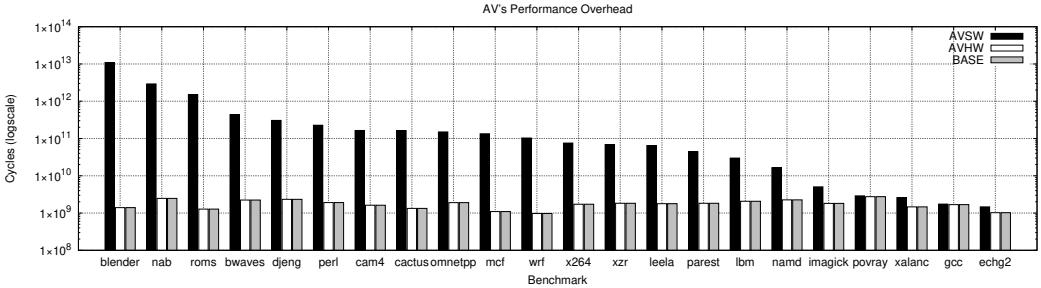
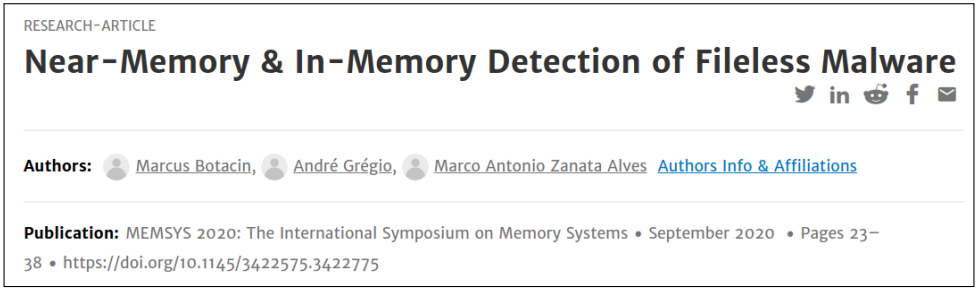


Figure: **Performance evaluation when tracking all function calls.** Comparison between execution without AV (BASE), execution with software AV, and execution with the proposed coprocessor model.

Topics

Publication



RESEARCH-ARTICLE

Near-Memory & In-Memory Detection of Fileless Malware

Authors: Marcus Botacin, André Grégio, Marco Antonio Zanata Alves Authors Info & Affiliations

Publication: MEMSYS 2020: The International Symposium on Memory Systems • September 2020 • Pages 23–38 • https://doi.org/10.1145/3422575.3422775

Figure: **Link:** `https://dl.acm.org/doi/10.1145/3422575.3422775`

Malware Identification based on Near- and In-Memory Evaluation (MINIME)

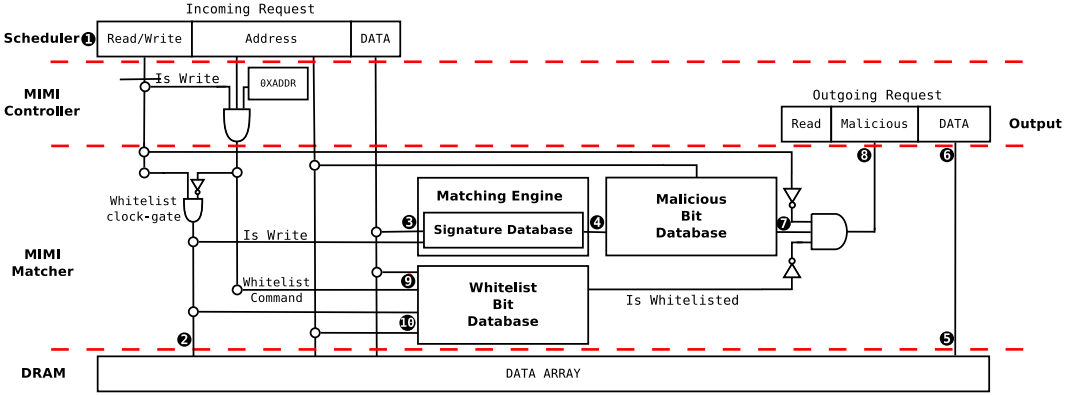
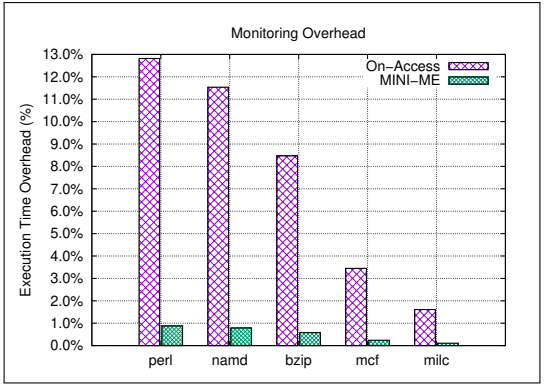


Figure: MINIME Architecture.

Performance Gains

MINIME vs. On-Access AVs

Significant performance gains even in the worst case.



Topics

Publications I

Table: **Published Papers.**

Paper	Venue	Research Type	Research Goal
[6]	Computers & Security	Landscape	Background
[9]	Computers & Security	Landscape	background
[2]	ACM TOPS	Landscape	Context
[14]	ACM ARES	Landscape	Context
[5]	Computers & Security	Landscape	Evaluation
[15]	ACM TOPS	Defensive	Hardware
[3]	Expert Systems	Defensive	Hardware
[16]	Springer JCVHT	Defensive	Hardware

Publications II

[10]	IEEE ReCoSoC	Defensive	Hardware
[8]	Springer JCVHT	Defensive	Hardware
[13]	ACM MEMSYS	Defensive	Hardware+Prediction
[7]	Springer JCVHT	Offensive	Predicting
[4]	DIMVA	Landscape	Application
[12]	Digital Investigation	Defensive	Application
[11]	ACM ROOTS	Defensive	Application
[1]	Springer ISC	Defensive	Application
[19]	IEEE TDSC	Defensive	Application
[17]	ACM ROOTS	Offensive	Application
[18]	ACM ROOTS	Offensive	Application

Publications III

Transition to Practice: Corvus Sandbox

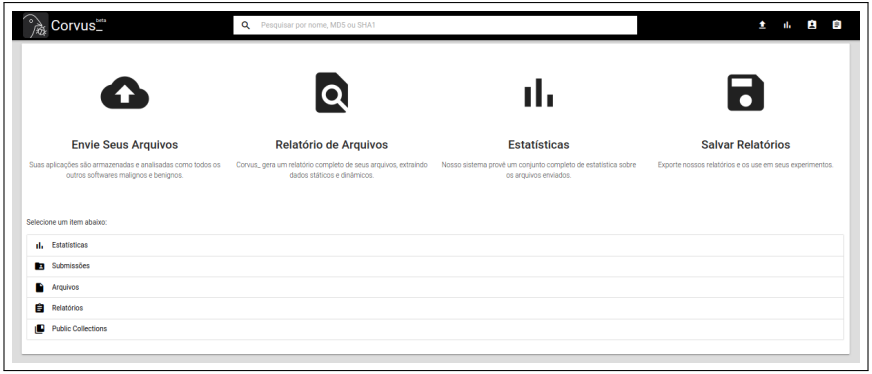


Figure: **Source:** `https://corvus.inf.ufpr.br/`

Topics

Summary

1. **Hypothesis:** Malware Research lacks a methodology.
2. **Contribution:** We proposed a possible methodology.
3. **Implications:**
   1. **The Need For Context**
      - Brazilian Financial Malware.
   2. **The Need For Better Evaluations**
      - AV Evaluation Metrics.
   3. **The Viability of Hardware Support**
      - Branch Predictor-Based Signature Matching.
   4. **The Need For Predicting the Future**
      - FIleless Malware Detection.

Acknowledgement time

Thanks!

Questions? Comments?

References I


T. Beppler, M. Botacin, F. J. O. Ceschin, L. E. S. Oliveira, and A. Grégio.
L(a)ying in (test)bed.
In *Information Security*. Springer, 2019.


M. Botacin, H. Aghakhani, S. Ortolani, C. Kruegel, G. Vigna, D. Oliveira, P. L. D. Geus, and A. Grégio.
One size does not fit all: A longitudinal analysis of brazilian financial malware.
ACM TOPS, 2021.


M. Botacin, M. Z. Alves, D. Oliveira, and A. Grégio.
Heaven: A hardware-enhanced antivirus engine to accelerate real-time, signature-based malware detection.
Elsevier ESWA, 2022.

References II


M. Botacin, G. Bert ao, P. de Geus, A. Grégio, C. Kruegel, and G. Vigna.
On the security of application installers and online software repositories.
In *DIMVA*. Springer, 2020.


M. Botacin, F. Ceschin, P. de Geus, and A. Grégio.
We need to talk about antiviruses: Challenges & pitfalls of av evaluations.
Computers & Security, 2020.


M. Botacin, F. Ceschin, R. Sun, D. Oliveira, and A. Grégio.
Challenges and pitfalls in malware research.
Computers & Security, page 102287, 2021.

References III


M. Botacin, P. L. de Geus, and A. Grégio.
"vanilla" malware: vanishing antiviruses by interleaving layers and layers of attacks.
Comp. Vir. and Hack. Tech., Jun 2019.


M. Botacin, P. L. de Geus, and A. Grégio.
Leveraging branch traces to understand kernel internals from within.
Comp. Vir. and Hack. Tech., 2020.


M. Botacin, F. D. Domingues, F. Ceschin, R. Machnicki, M. A. Zanata Alves, P. L. de Geus, and A. Grégio.
Antiviruses under the microscope: A hands-on perspective.
Comp. & Sec., 2021.

References IV


M. Botacin, L. Galante, F. Ceschin, P. C. Santos, L. Carro, P. de Geus, A. Grégio, and M. A. Z. Alves.
The av says: Your hardware definitions were updated!
In *ReCoSoC*, 2019.


M. Botacin, L. Galante, P. de Geus, and A. Grégio.
Revenge is a dish served cold: Debug-oriented malware decompilation and reassembly.
In *ROOTS*. ACM, 2019.

References V


M. Botacin, V. H. Galhardo Moia, F. Ceschin, M. A. Amaral Henriques, and A. Grégio.
Understanding uses and misuses of similarity hashing functions for malware detection and family clustering in actual scenarios.
FSI: Digital Investigation, 2021.


M. Botacin, A. Grégio, and M. A. Z. Alves.
Near-memory & in-memory detection of fileless malware.
In *MEMSYS*. ACM, 2020.

References VI


M. Botacin, A. Kalysch, and A. Grégio.
The internet banking [in]security spiral: Past, present, and future of online banking protection mechanisms based on a brazilian case study.
In *ARES*. ACM, 2019.


M. Botacin, F. B. Moreira, P. O. A. Navaux, A. Grégio, and M. A. Z. Alves.
Terminator: A secure coprocessor to accelerate real-time antiviruses using inspection breakpoints.
ACM Trans. Priv. Secur., 25(2), mar 2022.

References VII


M. Botacin, M. Zanata, and A. Grégio.
The self modifying code (smc)-aware processor (sap): a security look on architectural impact and support.
Journal of Comp. Virology (JCVHT), 2020.


F. Ceschin, M. Botacin, H. M. Gomes, L. S. Oliveira, and A. Grégio.
Shallow security: On the creation of adversarial variants to evade machine learning-based malware detectors.
In *ROOTS*. ACM, 2019.

References VIII


F. Ceschin, M. Botacin, G. Lüders, H. M. Gomes, L. Oliveira, and A. Gregio.
No need to teach new tricks to old malware: Winning an evasion challenge with xor-based adversarial samples.
In *ROOTS*. ACM, 2020.


R. Sun, M. Botacin, N. Sapountzis, X. Yuan, M. Bishop, D. E. Porter, X. Li, A. Gregio, and D. Oliveira.
A praise for defensive programming: Leveraging uncertainty for effective malware mitigation.
IEEE TDSC, 2020.