It has a EULA, it must be legit

Ștefan Cătălin Hanu, Ștefan Moșoi, Marius Lucaci

Bitdefender

Bitdefender

Agenda

- Malware evolution
- Potentially Unwanted Applications
- The End User License Agreement (EULA)
- Our experiment
- Understanding the processing flow
- Results
- Conclusions
- Q&A

Bitdefender

Malware evolution

- In the past, malware provided a statement about the creator's abilities
- Why not use their skills and earn some money?
- Latest trends show the evolution of malware towards monetary gain
- Working in this environment is dangerous and might have serious legal repercussions
- Advertising has been around for a long time so why not bring it to the ever growing IT market?

Bitdefender

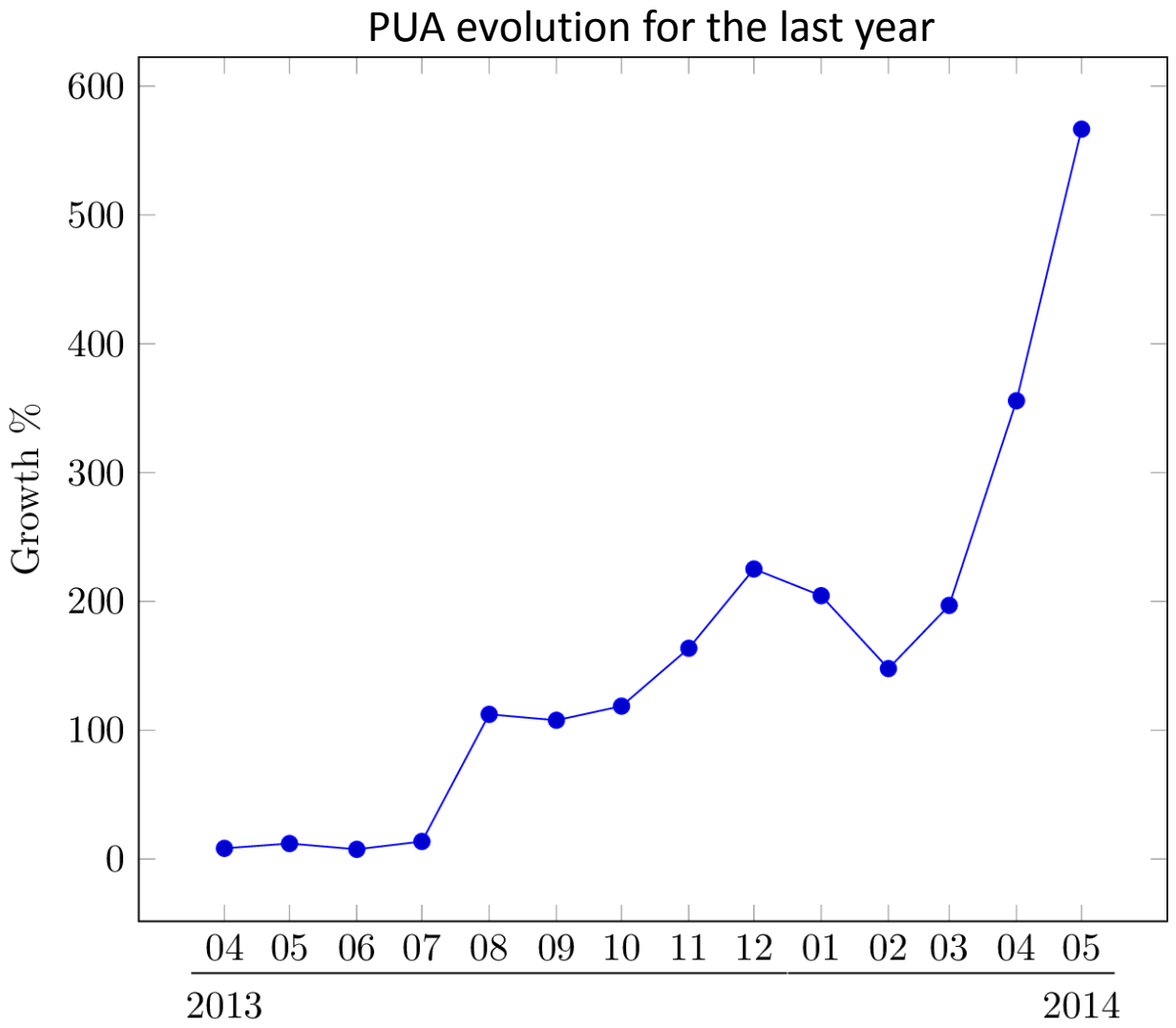
Potentially Unwanted Applications

- Broad definition: we define Potentially Unwanted Applications (PUAs) as computer programs that in some circumstances employ techniques that circumvent security measures or have a negative effect on the user's interaction with specific applications or actions.

- Adware and bundlers walk a dangerous path on the limits of legality
- Is it worth the risk?

Potentially Unwanted Applications

- Rising the number of installations increases the earnings for PUA creators
- This is sometimes achieved with the help of social engineering techniques and clandestine installations
- What happens when the user accepts the implications of installing a software?



Bitdefender

The End User License Agreement (EULA)

- In some countries, the End User License Agreement (EULA) is a legally binding contract between the user and the software publisher
- Companies that produce PUAs often try to justify the software behavior by the legal implications of the user accepting the EULA
- Do users really read it?

Bitdefender

The End User License Agreement (EULA)

- In some countries, the End User License Agreement (EULA) is a legally binding contract between the user and the software publisher

- Companies that produce PUAs often try to justify the software behavior by the legal implications of the user accepting the EULA

- Do users really read it? → statistics say that "more than **50%** of the users take less than **8 seconds**"

Bitdefender

The End User License Agreement (EULA)

- The legal terminology combined with unnecessary and sometimes voluntary language obfuscation makes reading this contract a daunting task for the average user

Bitdefender

The End User License Agreement (EULA)

- The legal terminology combined with unnecessary and sometimes voluntary language obfuscation makes reading this contract a daunting task for the average user
- And let's not forget: some of these things are huge!

> This Agreement is a contract between you and PayPal and applies to your use of the Services. The terms of the Acceptable Use Policy, and Merchant Gift Vouchers Policy located on the "Legal Agreements" landing page are incorporated by reference into this Agreement and provide additional terms and conditions related to the Services. All future Changes set out in the Policy Update already published on the "Legal Agreements" landing page of the PayPal website at the time you register for the Services are incorporated by reference into this Agreement and will take effect as specified in that Policy Update. The terms of the PayPal MasterCard Rewards Programme are also incorporated by reference into this Agreement and apply to your use of PayPal Credit. A copy of these terms will be provided to you when you are successfully approved for PayPal Credit. The above mentioned documents are "Ancillary Documents" for the purpose of this Agreement. For the avoidance of doubt, neither the Ancillary Documents nor the parts of this Agreement that incorporate the terms of the Ancillary Documents constitute "framework contracts" for the

Bitdefender

The End User License Agreement (EULA)

- The legal terminology combined with unnecessary and sometimes voluntary language obfuscation makes reading this contract a daunting task for the average user
- And let's not forget: some of these things are huge!

purpose of the EU Payment Services Directive (2007/64/EC) or any implementation of that directive in the EU or EEA (including, without limitation, the UK Payment Services Regulations 2009). This Agreement, together with other legal terms and legally required disclosures relating to your use of the PayPal Service will be provided to you, at all times on the PayPal website(s) (typically located on the "Legal Agreements" landing page). This information may also be sent to you or appear in places on the PayPal website(s) or otherwise where relevant to your use of the PayPal Services.
By registering for the Services, you must read, agree with and accept all of the terms and conditions contained in this Agreement (including the Policy Updates, policies and reward terms referred to above). This Agreement is provided to you and concluded in English. You agree that any use by you of the Services shall constitute your acceptance of the Agreement and we recommend that you store or print-off a copy of the Agreement (including all policies) for your records.

Bitdefender

The End User License Agreement (EULA)

- The legal terminology combined with unnecessary and sometimes voluntary language obfuscation makes reading this contract a daunting task for the average user
- And let's not forget: some of these things are huge!

PayPal may require you to have a PayPal Account to use the Services (including, without limitation, to send or receive payments or to use PayPal as a means of logging into third party services).

IMPORTANT
This is an important document which you must consider carefully when choosing whether to use the Services at any time. Please read the terms of this Agreement carefully before agreeing to it. This Agreement also highlights certain risks on using the Services together with guidance on how to safely carry out online payments via PayPal.
You are solely responsible for understanding and complying with any and all laws, rules and regulations of your specific jurisdiction that may be applicable to you in connection with your use of the PayPal Services, including but not limited to, those related to export or import activity, taxes or foreign currency

Bitdefender

The End User License Agreement (EULA)

- The legal terminology combined with unnecessary and sometimes voluntary language obfuscation makes reading this contract a daunting task for the average user
- And let's not forget: some of these things are huge!

> Please note the following risks and key terms applicable to your use of the PayPal Services:
> Risk of payment reversals
> Payments received in your PayPal Account may be reversed at a later time, for example, if such a payment is subject to a Chargeback, Reversal, Claim or otherwise invalidated. This means that for some of our sellers, payments received into their Account may be returned to the sender or otherwise removed from their Account after they have been paid and/or delivered any goods or services sold.
> A key eligibility requirement of the Seller Protection Programme is that the seller must post the item to the address which appears on the transaction details page. If the item is delivered in person or if a seller posts the item to a different address (for example, if the buyer asks that you send to another address on the basis that it is a "work address" or a "gift" address) then you will not be eligible for re-imbursement under the terms of the programme.

The End User License Agreement (EULA)

- The legal terminology combined with unnecessary and sometimes voluntary language obfuscation makes reading this contract a daunting task for the average user
- And let’s not forget: some of these things are huge!

You can help protect yourself from the risks of a payment being reversed from your Account by following the criteria set out in the PayPal Seller Protection Programme and by following the other guidance provided to sellers as set out in the "Security Centre" accessible via every page of the PayPal website.
We may close, suspend, or limit your access to your Account or our Services, and/or limit access to your funds to the extent and for so long as reasonably needed to protect against the risk of liability (see section 10.2h) if you violate this Agreement including the PayPal Acceptable Use Policy, or any other agreement you enter into with PayPal. For the avoidance of doubt, we may permanently block your account for breach of section 10.6 (Information about you).
Risk of payments being held by PayPal
Please note that although you may only have one PayPal Account, your Account has two separate and distinct functionalities, the payment functionality and the reserve functionality.

Bitdefender

The End User License Agreement (EULA)

- The legal terminology combined with unnecessary and sometimes voluntary language obfuscation makes reading this contract a daunting task for the average user
- And let’s not forget: some of these things are huge!

Your ability to access funds in your Account and to execute payment transactions from your Account will depend upon which functionality the funds are subject to at any given time. For the purposes of this Agreement:

- The element of your Account which constitutes the payment functionality will be known as the "Payment Account". The Payment Account is the operational part of your Account through which you have access to funds and which can be used for the execution of payment transactions.
- The element of your Account which constitutes the reserve functionality will be known as the "Reserve Account". Your access to the Reserve Account is restricted and you have no ability to access funds in the Reserve Account or to execute payment transactions over funds in the Reserve Account. Funds held in the Reserve Account may be marked, for example, "Pending", "Uncleared", "Held".

The End User License Agreement (EULA)

- The legal terminology combined with unnecessary and sometimes voluntary language obfuscation makes reading this contract a daunting task for the average user
- And let's not forget: some of these things are huge!

Examples of when funds may be held by PayPal to mitigate risks include when those funds are subject to:

- an eCheque, Add funds or Top-up bank transfer payment (see section 3.7)
- Merchant processing delay (see section 3.9)
- Reserve (see section 10.4)
- Payment review (see section 4.3)
- Payment Hold (see section 10.5)
- Restricted Activity and actions taken by PayPal (see sections 9 and 10)

Disputes

If you wish to open a Dispute through PayPal's Online Resolution Centre you must do so within 45 days (or, if you are claiming as a registered UK resident user of PayPal, 180 days) of making your payment.

Payment execution

Bitdefender

The End User License Agreement (EULA)

- The legal terminology combined with unnecessary and sometimes voluntary language obfuscation makes reading this contract a daunting task for the average user
- And let's not forget: some of these things are huge!

> Please note that PayPal will execute a valid Payment Order made by you through your Payment Account and credit the payment service provider of the person to whom you are sending your payment as soon as the payment schemes available to PayPal allow (which can be within the next Business Day) following the date you gave us your valid Payment Order. This execution time is subject to certain conditions and more detail around execution of Payment Orders is set out in section 3.1 of this Agreement.
> You must consider such risks and guidance when using PayPal.
> For more information about the PayPal service, please read our Key Payment and Service Information.
> The headings and subheadings below are for reference only and do not limit the scope of each section.
> Some capitalised terms have specific definitions, and we have provided them in section 15 or otherwise in the text of this Agreement. You will also find underlined words in this Agreement and on our website that hyperlink to relevant information.

Bitdefender

The End User License Agreement (EULA)

- The legal terminology combined with unnecessary and sometimes voluntary language obfuscation makes reading this contract a daunting task for the average user
- And let’s not forget: some of these things are huge!
- This is only the first 1257 words. There are in excess of 25000 in the PayPal EULA

Bitdefender

The End User License Agreement (EULA)

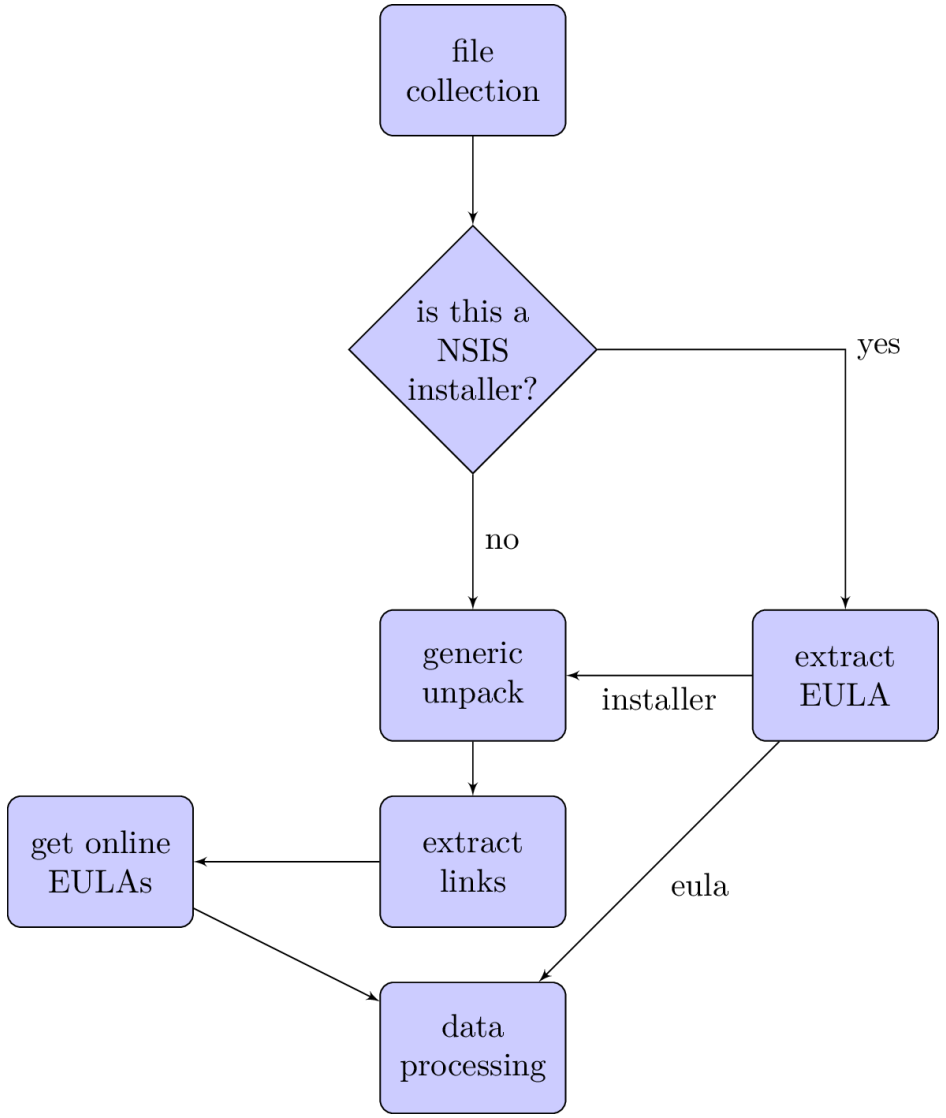
- “We collect Non-personal and Personal Information in order to provide and operate SOFTWARE and to make SOFTWARE and related services customized as possible to your interests and preferences. We also use the information for statistical and analytics, research and technical support; this enable us to further develop, customize and improve SOFTWARE based on Users’ common preferences and uses and to enable us to provide our Users with a better user experience, with more relevant products, offers and deals and other marketing materials.”
- Could also be written as “We collect Non-personal and Personal Information in order to provide targeted advertisements”

Bitdefender

Our experiment

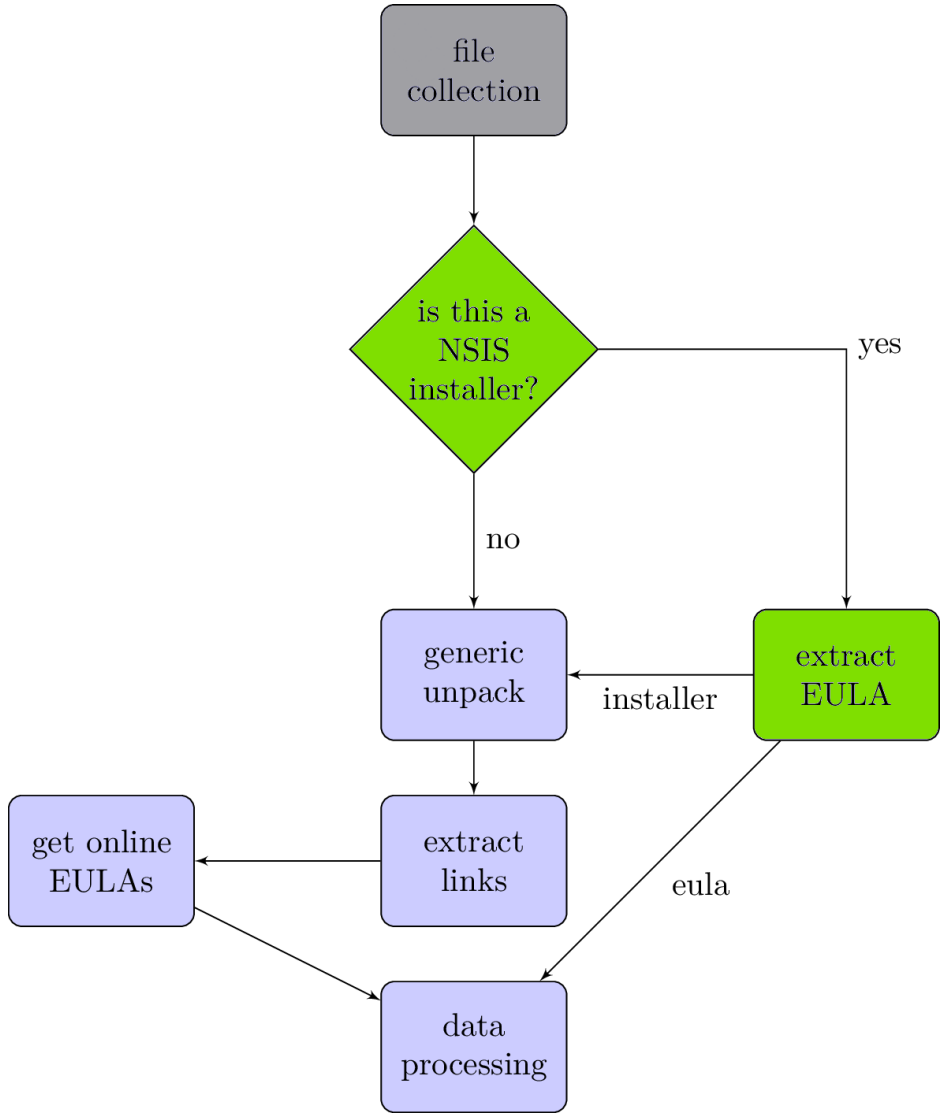
- The usage of specific legal terms and adherence to a common writing standard allows us to create algorithms that can classify EULAs
- This is a great task for Natural Language Processing (NLP), supervised learning and of course, Python
- We processed about 1 million PE binaries in order to extract the EULA text

Understanding the processing flow



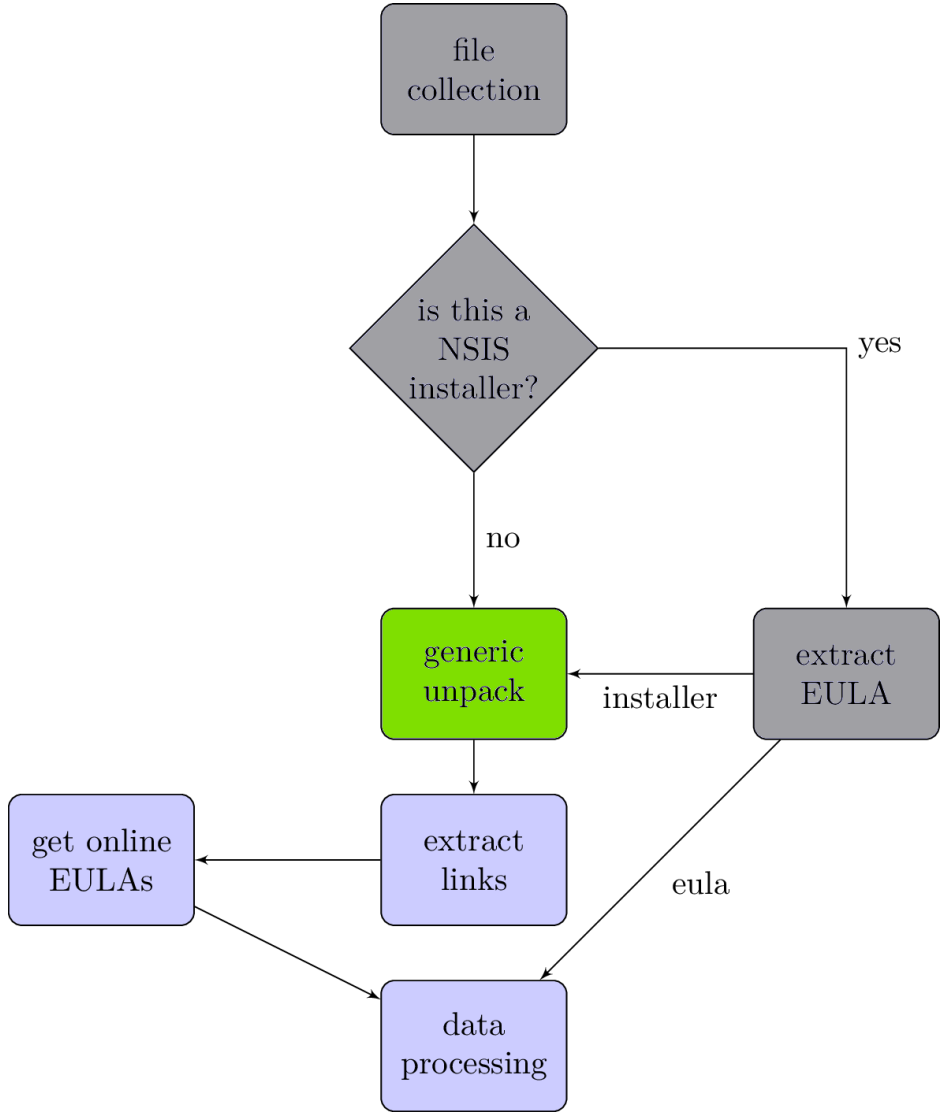
Understanding the processing flow

- Nullsoft (NSIS) installers are processed separately
- The installer can have a different EULA than the components extracted from it



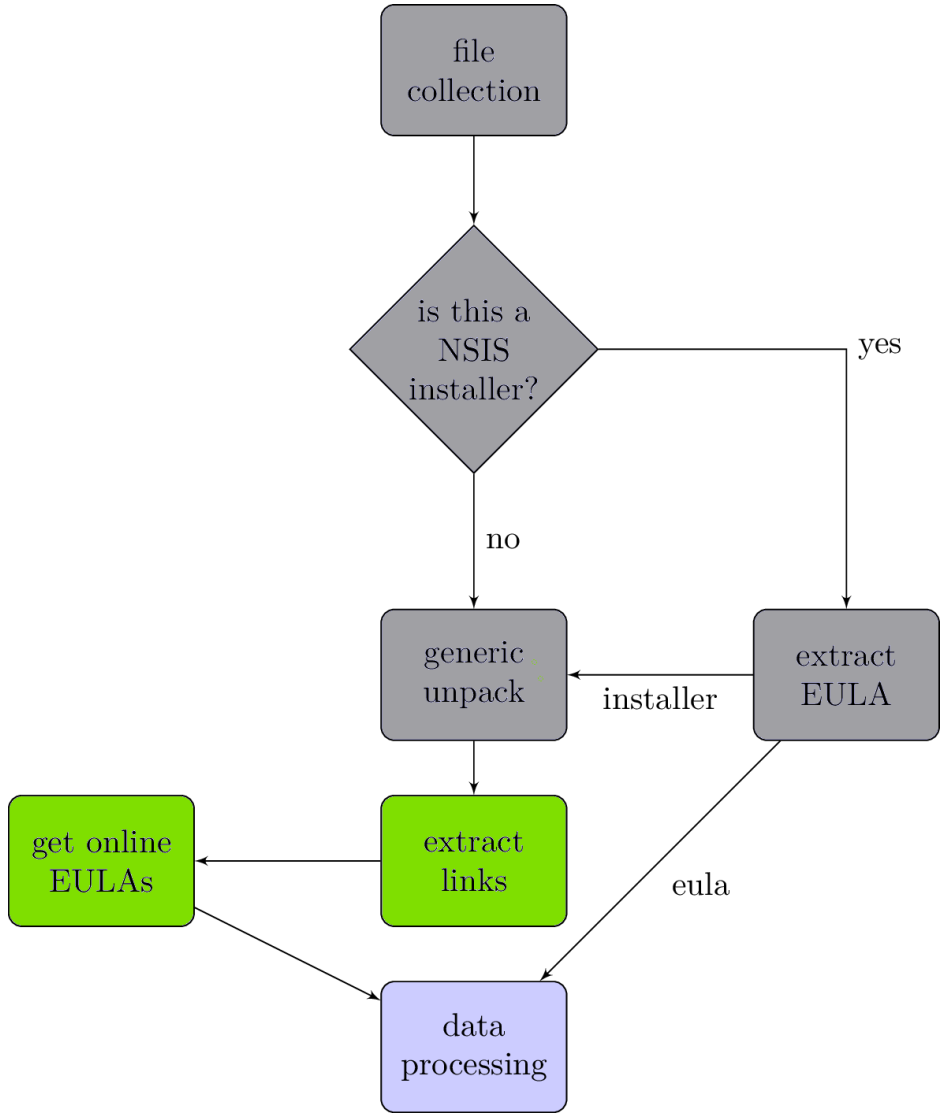
Understanding the processing flow

- We used a combination of in-house engines and publically available software



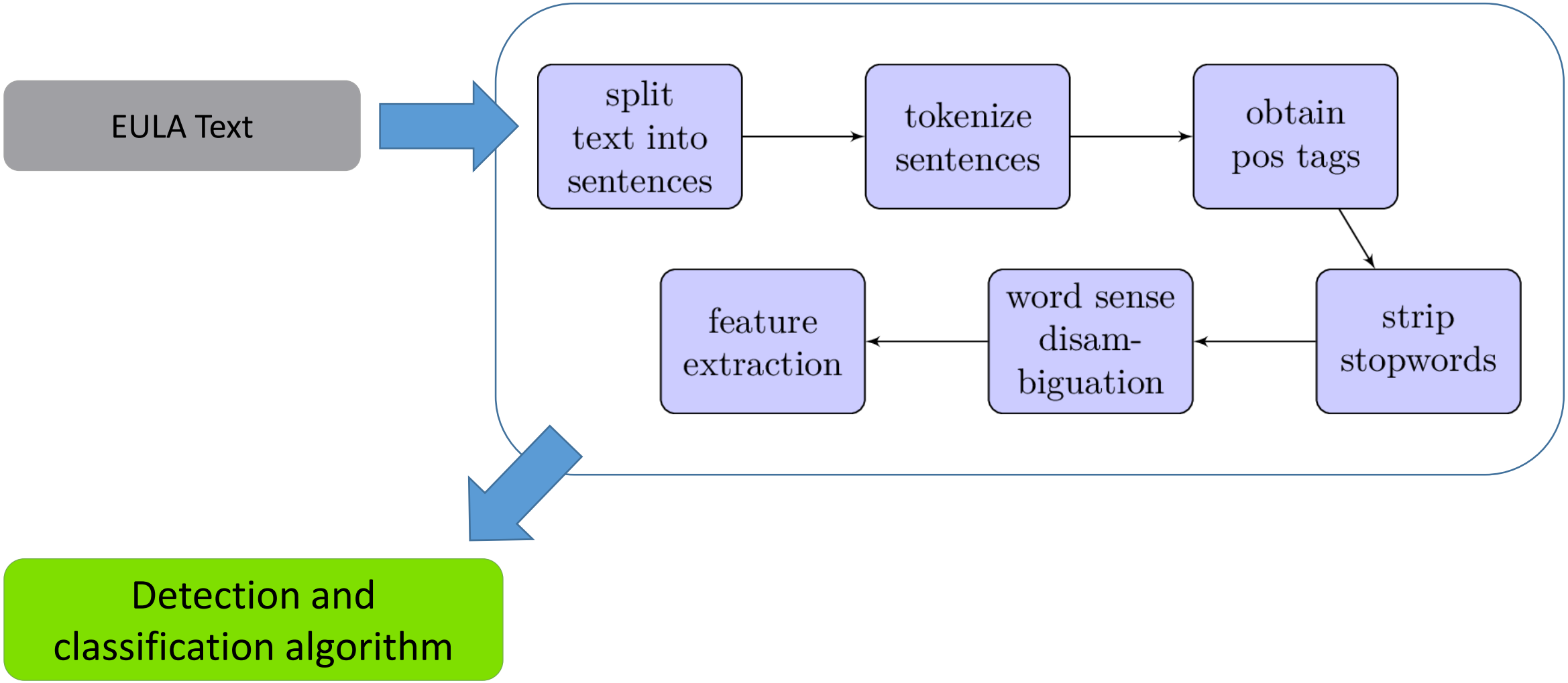
Understanding the processing flow

- We used a combination of regular expressions and extraction of words and word combinations that might be part of a website link or IP address
- Download the webpage and search for EULA references
- Retrieve and strip the EULA



Bitdefender

Understanding the processing flow



Bitdefender

Understanding the processing flow

1. Original text: “The Software is supported by various types of advertising displayed in your browser. These advertisements may be targeted to queries you make through your browser.”

2. Split text into sentences:
   - First sentence: “The Software is supported by various types of advertising displayed in your browser.”
   - Second sentence: “These advertisements may be targeted to queries you make through your browser.”

Bitdefender

Understanding the processing flow

3. Tokenize sentences:

ID	Word
1	The
2	Software
3	is
4	supported
5	by
6	various
7	types

ID	Word
8	of
9	advertising
10	displayed
11	in
12	your
13	browser

Bitdefender

Understanding the processing flow

4. Obtain part of speech (POS) tags:

ID	Word	POS
1	The	DT
2	Software	NNP
3	is	VBZ
4	supported	VBN
5	by	IN
6	various	JJ
7	types	NNS

ID	Word	POS
8	of	IN
9	advertising	NN
10	displayed	VBN
11	in	IN
12	your	PRP
13	browser	NN

POS	Description
DT	Determiner
NNP	Proper noun, singular
VBZ	Verb, 3rd person singular present
VBN	Verb, past participle
IN	Preposition or subordinating conjunction
JJ	Adjective
NNS	Noun, plural
NN	Noun, singular or mass

Understanding the processing flow

5. Strip the stop words:

ID	Word	POS
1	The	DT
2	Software	NNP
~~3~~	~~is~~	~~VBZ~~
4	supported	VBN
~~5~~	~~by~~	~~IN~~
6	various	JJ
7	types	NNS

ID	Word	POS
~~8~~	~~of~~	~~IN~~
9	advertising	NN
10	displayed	VBN
~~11~~	~~in~~	~~IN~~
~~12~~	~~your~~	~~PRP~~
13	browser	NN

POS	Description
DT	Determiner
NNP	Proper noun, singular
VBZ	Verb, 3rd person singular present
VBN	Verb, past participle
IN	Preposition or subordinating conjunction
JJ	Adjective
NNS	Noun, plural
NN	Noun, singular or mass

Bitdefender

Understanding the processing flow

6. Word sense disambiguation:

Original word	WordNet	Porter	Lancaster	SnowBall
advertisement	ad	advertis	advert	advertis
advertisement	ad	advertiz	advert	advertiz
advertising	ad	advertis	advert	advertis
advertising	ad	advert	advert	advert
advert	ad	advert	advert	advert
advertise	advertise	advertis	advert	advertis
advertiser	advertiser	advertis	advert	advertis

Understanding the processing flow

6. Word sense disambiguation:

ID	Word	POS
1	the	DT
2	software	NNP
~~3~~	~~is~~	~~VBZ~~
4	support	VBN
~~5~~	~~by~~	~~IN~~
6	assorted	JJ
7	type	NNS

ID	Word	POS
~~8~~	~~of~~	~~IN~~
9	ad	NN
10	display	VBN
~~11~~	~~in~~	~~IN~~
~~12~~	~~your~~	~~PRP~~
13	browser	NN

POS	Description
DT	Determiner
NNP	Proper noun, singular
VBZ	Verb, 3rd person singular present
VBN	Verb, past participle
IN	Preposition or subordinating conjunction
JJ	Adjective
NNS	Noun, plural
NN	Noun, singular or mass

Understanding the processing flow

6. Feature extraction:
   - Top 10000 from the word frequency for the entire document lot
   - Top 10000 from the frequency of combinations of two or three words from sentences
   - 20000 features is not a feasible number to work with
   - We tested four feature selectors
7. We use a linear classifier called One side Perceptron to classify the documents

Bitdefender

Results

Feature selector	False positives	Detection rate	Accuracy
F1	10	92.86%	96.49%
F2	13	94.65%	97.32%
ProcDiff	12	96.60%	98.24%
AbsProcDiff	15	94.88%	97.44%

- F1 is $\frac{\mu_A - \mu_C}{\rho_A + \rho_C}$
- F2 is $\frac{(\mu_A - \mu_T)^2 + (\mu_C - \mu_T)^2}{\rho_A^2 + \rho_C^2}$
- ProcDiff is the difference between the percentage of clean and adware samples that share the same feature
- AbsProcDiff is the absolute value of ProcDiff
- The FP column represents the number of false positives while Se is the sensitivity and Acc the accuracy

Bitdefender

Conclusions

- Understanding the EULA might be the first step into providing a generic way of detecting multiple adware families

Bitdefender

Conclusions

- Understanding the EULA might be the first step into providing a generic way of detecting multiple adware families

Conclusions

- Understanding the EULA might be the first step into providing a generic way of detecting multiple adware families
- Lets consider the following definitions:
  - Static detection = analyzing the file based on its binary content
  - Dynamic detection = analyzing a file based on its behavior

Conclusions

- Understanding the EULA might be the first step into providing a generic way of detecting multiple adware families
- Lets consider the following definitions:
  - Static detection = analyzing the file based on its binary content
  - Dynamic detection = analyzing a file based on its behavior

Our method might be considered a 3rd type:

- **Eula based detection = detecting a binary file based on it's creator's own description of it's behavior**

Conclusions

- Understanding the EULA might be the first step into providing a generic way of detecting multiple adware families
- Lets consider the following definitions:
  - Static detection = analyzing the file based on its binary content
  - Dynamic detection = analyzing a file based on its behavior

Our method might be considered a 3rd type:

- **Eula based detection = detecting a binary file based on it's creator's own description of it's behavior**

Bitdefender

Q&A