# Malware Analysis with FCA

**Supplementary material for the paper "A Formal Concept Analysis Approach to Hierarchical Description of Malware Threats"**

Manuel Ojeda-Hernández     Domingo López-Rodríguez

Ángel Mora

## Table of contents

# 1 Introduction

This document accompanies the paper **A Formal Concept Analysis Approach to Hierarchical Description of Malware Threats**. It is intended to give a more detailed view on the processing done in the main manuscript to infer the hierarchical relations among different malware threats.

We interleave explanations with sample code to enhance the replicability of the results. This document and the required code are stored in the GitHub repository Malaga-FCA-group/VirusTotal-Malware-Hierarchy.

# 2 Setup

Let us prepare the environment to perform the study. We will need R and RStudio. In the following subsections, we describe which packages and auxiliar functions are needed.

## 2.1 Packages needed

Let us load the required packages to perform all the processing:

```
library(jsonlite)                                    ①
library(tidyjson)
library(tidyverse)                                   ②
library(data.table)                                  ③
```

① Needed to operate with JSON files.
② Needed for cleaning up the data.
③ Needed to manage tabular data.

We will also need the `fcaR` library to perform the operations with FCA tools. Please, install the latest development version from GitHub:

```
# Note: the remotes package is needed.
remotes::install_github("neuroimaginador/fcaR")
```

Then, we can load the library functions by doing:

```
library(fcaR)
```

## 2.2 Auxiliary functions

We have some accompanying auxiliar functions for particular steps in the processing.

```r
source("parse_results.R")
source("names_cleanup.R")
source("transform_name_pattern.R")
```

# 3 Data availability

Data for this study has been provided by VirusTotal as a set of JSON files containing information about scanned files: permissions and activities detected in the file, and the result of scanning the suspicious file with more than 70 antiviruses.

For more details on accessing the reports generated for single files, you can visit https://developers.virustotal.com/reference/overview.

For demosntration purposes, we will use the dataset provided by VirusTotal, whose JSON files are located in the "Android" folder beneath the current folder (where this files resides).

```r
folder <- here::here("Android")                                      ①

# List of JSON files
files <- list.files(path = folder,                                   ②
                    pattern = "json$",
                    full.names = TRUE)
```

① `folder` points to the "Android" subfolder.
② Returns a list of all the files in that folder whose extension is `json`.

# 4 Data preprocessing

Let us begin with an example of the relevant parts of a JSON file. We will use this example throughout this document to show the process performed on the data.

```
{
  "Bkav": {
    "detected": [false],
    "version": ["1.3.0.9899"],
    "result": {},
```

```
    "update": ["20211102"]
  },
  "Lionic": {
    "detected": [true],
    "version": ["4.2"],
    "result": ["Adware.AndroidOS.Adlo.A!c"],
    "update": ["20211103"]
  },
  "Symantec": {
    "detected": [false],
    "version": ["1.16.0.0"],
    "result": {},
    "update": ["20211103"]
  }
}
```

**Detection table**

Note that we are interested in having a table with what each antivirus has detected, for each file. For the sample JSON above, it would look like the following:

| Engine | Result |
|---|---|
| Bkav | NA |
| Lionic | Adware.AndroidOS.Adlo.A!c |
| Symantec | NA |
| ⋮ | ⋮ |

This can be achieved (for all the files at once) with the following code:

```
  results <- files |>
    lapply(\(f) jsonlite::fromJSON(f)$scans |>                    ①
           parse_results()) |>                                    ②
    purrr::reduce(dplyr::full_join, by = "engine")                ③
```

① Import each file and access to the `scans` field.
② For each one, we parse the results, giving two columns, one with the name of the engines and the other with the result of the detection: `NA` means no detection; otherwise, the name of the detected threat.
③ Make a full join of all the tables.

Now, we have a table with:

- One row for each antivirus used in the detections.
- One column called `engine` that stores the names of the antiviruses.
- One column per scanned file.

We want to tidy this table up:

1. Mark the NAs with the character string "NA".
2. Store the antivirus names in a variable to use it later.
3. Remove the `engine` column as it is redundant.
4. Transpose the table to have files as rows.
5. Add as row names the names of the scanned files and as column names the engines used. These two points are needed by FCA, since our attributes are the set of tags given by the different engines, and must be in columns.

These five items are implemented in the following code:

```
results[is.na(results)] <- "NA"                              ①
used_engines <- results$engine                              ②
results$engine <- NULL                                      ③
results <- data.table::transpose(results)                   ④
rownames(results) <- basename(files)                        ⑤
colnames(results) <- used_engines
```

Up to this moment, we have obtained a matrix as in the following example:

|          | Bkav | Lionic                   | Symantec | $\cdots$ |
|----------|------|--------------------------|----------|----------|
| file00001| NA   | Adware.AndroidOS.Adlo.A!c| NA       | $\cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$             | $\vdots$ | $\vdots$ |

# 5 Computations with FCA tools

Now, we present the transformations made in this dataset in order to have it processed using FCA tools. For the sake of simplicity, we will constraint the dataset to a subset of the engines used:

```
my_engines <- c("Avast-Mobile", "Avira", "ESET-NOD32", "Kaspersky", "McAfee",
"Microsoft")

results <- results[, colnames(results) %in% my_engines]
```

Doing so, we can obtain interesting results with less computaitonal effort, so this notebook can be executed more easily in any computer.

Now, let us build a formal context from the above table. Since the values of each attribute are nominal (the tags given by the corresponding antivirus), we must perform a scaling on the context to obtain a binary table.

Let us explain what a nominal scaling is. Suppose that we have the following column in our table:

| | av |
|---|---|
| file1 | tag1 |
| file2 | tag2 |
| file3 | NA |
| file4 | tag1 |
| file5 | tag3 |

Here, we only represent one column (`av`) since scalings in FCA are performed on attributes in an independent manner, that is, each attribute is processed independently of the others, even maybe with a different type of scaling.

Since we need to have a binary data table, we use the following transformation rule, that details how to encode each value in that column with binary representation:

| | av = NA | av = tag1 | av = tag2 | av = tag3 |
|---|---|---|---|---|
| NA | × | | | |
| tag1 | | × | | |
| tag2 | | | × | |
| tag3 | | | | × |

In this case, the nominal scaling coincides with what is termed "one-shot encoding" in other Machine Learning fields. This transformation leads us to a binary formal context:

| | av = NA | av = tag1 | av = tag2 | av = tag3 |
|---|---|---|---|---|
| file1 | | × | | |
| file2 | | | × | |
| file3 | × | | | |
| file4 | | × | | |
| file5 | | | | × |

With `fcaR`, this process is handled automatically by doing:

```
# Formal context with all the objects and attributes
fc <- FormalContext$new(results)
```

```
# Nominal scaling: each column is transformed into n columns,
# each one with a binary value.
fc$scale(attributes = fc$attributes,
         type = "nominal")
```

This produces a context with 183 objects (scanned files) and 406 attributes (pairs "antivirus = tag"). Let us show the first attributes:

McAfee = !02f9c9bb715b, McAfee = !03eaa0113ccf, McAfee = !041a4a561b51, McAfee = !05906bbf77a9, McAfee = !07e0c50a8a28, McAfee = !092d858c2721, McAfee = !0b40c7b97ac3, McAfee = !0c5c3d793761, McAfee = !0edb4e42346f and McAfee = !0eeb70a4f783

The meaning of attribute `Symantec = PUA.Gen.2` is as follows: if it is marked as present for a given file, then the antivirus Symantec had detected the `PUA.Gen.2` malware in that file. As a particular case, if the attribute `Symantec = NA` is marked for a file, this means that Symantec did not detect any malware in that file.

We will perform a transformation in these names to get them as in the paper, that, we want to transform the patterns `antivirus = tag` into $\langle \text{antivirus}, \text{tag} \rangle$ and `antivirus = NA` into $\langle \text{antivirus}, \varnothing \rangle$.

```
fc$attributes <- transform_name_pattern(fc$attributes)
```

This command has transformed the previous list of attributes to:

$\langle \text{McAfee, !02f9c9bb715b} \rangle$, $\langle \text{McAfee, !03eaa0113ccf} \rangle$, $\langle \text{McAfee, !041a4a561b51} \rangle$, $\langle \text{McAfee, !05906bbf77a9} \rangle$, $\langle \text{McAfee, !07e0c50a8a28} \rangle$, $\langle \text{McAfee, !092d858c2721} \rangle$, $\langle \text{McAfee, !0b40c7b97ac3} \rangle$, $\langle \text{McAfee, !0c5c3d793761} \rangle$, $\langle \text{McAfee, !0edb4e42346f} \rangle$ and $\langle \text{McAfee, !0eeb70a4f783} \rangle$

## 5.1 Identification of equivalent tags

We now perform clarification in the formal context, that helps in determining equivalent attributes, that is, we will say that $\langle \text{antivirus1}, \text{tag1} \rangle \equiv \langle \text{antivirus2}, \text{tag2} \rangle$ if the set of files where antivirus1 detected the malware named tag1 coincides with the set of files where antivirus2 detected the malware tag2.

```
# Group equal columns/rows
fc2 <- fc$clarify(TRUE)
```

The new formal context has 195 attributes (columns), what means that some of the attributes in the original formal context had equivalences. We will list those equivalences in Section 6.1. For now, we give an example:

$$\langle\text{McAfee, !0edb4e42346f}\rangle \quad \equiv \langle\text{ESET-NOD32, a variant of /addisplay.tapcore.b potentially}$$
$$\text{unwanted}\rangle \equiv \langle\text{Avira, /andr.addisplay.amaa.gen}\rangle$$

Here, the meaning of this equivalence is that every file that is assigned the tag `!0edb4e42346f` by McAfee has also been assigned the corresponding tags from ESET-NOD32 and Avira. And viceversa, every file assigned to the above ESET-NOD32 or Avira tags is also assigned to `!0edb4e42346f` by McAfee. This means that these tags determine exactly the same malware (conditioned to the scope of the dataset used).

## 5.2 Construction of the concept lattice

The concept lattice of the clarified formal context is isomorphic to that of the original formal context, but it is easier to compute due to the reduced number of attributes. Thus, we will compute the concept lattice from this new context.

```
fc2$find_concepts()
```

This lattice consists of 265 concepts. Let us show it in Figure 1.
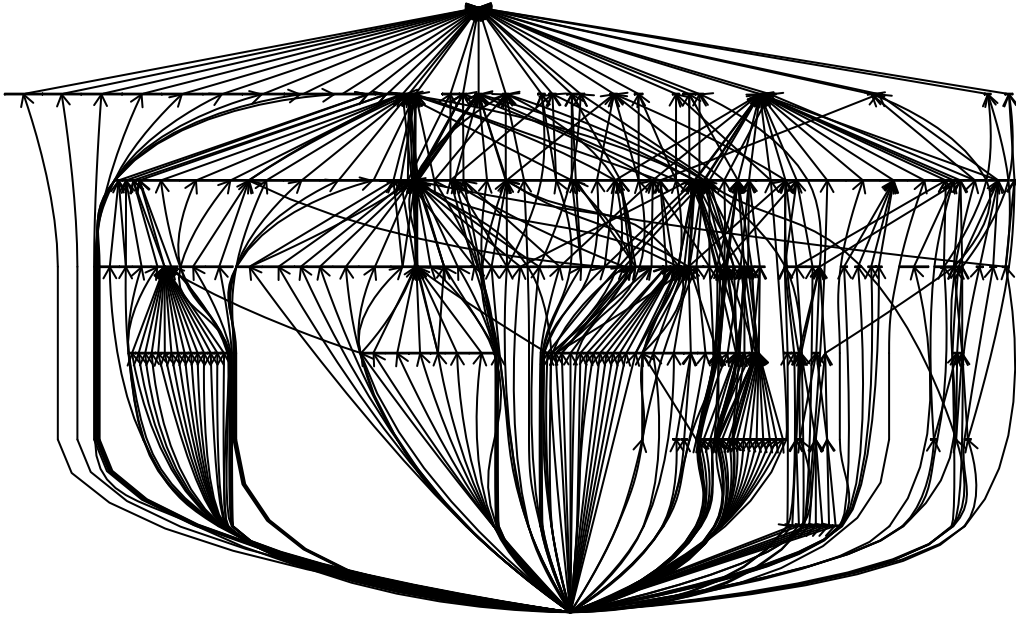


Figure 1: Concept lattice of our formal context.

### 5.2.1 Meaning of concepts

Let us inspect the meaning of a concept in this scenario with an example. The following is a concept of our formal context:

$$(A, B) \quad \text{with} \quad \begin{cases} A = & \{\text{cd581c0251f2b1e7559c4b5830.json,} \\ & \text{fb1bd5c6486f120268c0803901.json,} \\ & \text{44ed7c95e37adfa1e90cc55847.json}\} \\ B = & \{\langle \text{Kaspersky, not-a-virus:heur:.os.adlo.b}\rangle, \\ & \langle \text{Avast-Mobile, :evo-gen}\rangle, \\ & \langle \text{Avira, /agent.mer.gen}\rangle, \\ & \langle \text{Microsoft, :script/wacatac.b!ml}\rangle\} \end{cases}$$

$A$ is a set of files (objects in our formal context) and $B$ is a set of tags or identifiers given by different antivirus systems to each file (attributes). The names of the files have been shortened for the sake of readability. The fact that this is a concept means that the common attributes of all the files in $A$ are those in $B$ (there is no other attribute shared by these three files). That is, the identifiers expressed in $B$ are the ones of the malware detected in all these files. There is no other malware identifier in common among these files.

And conversely, the only three files that have been assigned the identifiers given in $B$ are those in $A$. No file outside $A$ has all the identifiers in $B$.

This explanation, in terms of the problem at hand, is what allow us to talk about malware *families*, *categories* or *classes*.

### 5.2.2 How to use the concept hierarchy to determine subfamily relations between identifiers

The following explanation extends and explains the study done on the hierarchy of malware as presented in the manuscript in Tables 2 and 3.

Let us consider we want to study an identifier of the form $\langle \text{antivirus, tag} \rangle$:

1. Look for the *attribute concept* corresponding to $\langle \text{antivirus, tag} \rangle$. Let us call it $C$.
2. Check if $C$ is a coatom:

   a. If it is a coatom, $\langle \text{antivirus, tag} \rangle$ is a generic tag, it is not a subtype of another tag.
   b. If it is not a coatom:
      i. If it has only one upper neighbour $(A, B)$ then $\langle \text{antivirus, tag} \rangle$ is strictly contained in the intersection of all the identifiers in $B$.
      ii. If it has more than one upper neighbour, let $\{(A_i, B_i)\}$ be the set of its upper neighbours. Then the identifier $\langle \text{antivirus, tag} \rangle$ corresponds exactly to the intersection of all the identifiers in $\cup_i B_i$.

The following code, using `fcaR` methods, allows us to compute these hierarchical dependencies:

```
# Let us build lists of generic types and of subfamilies
contained <- list()
equal <- list()
coatoms <- list()
top <- fc2$concepts$top()
for (name in fc2$attributes) {

  # Compute the corresponding attribute concept
  C <- fc2$att_concept(name)

  # Check if it is a coatom
  Upper <- fc2$concepts$upper_neighbours(C)
  if (Upper$sub(1) %==% top) {

    # If it is, add it to the list of coatoms
    coatoms[[name]] <- C$get_intent()

  } else {

    # Otherwise, check how many upper neighbours it has
    if (Upper$size() == 1) {

      # Only one: properly contained in its parent concept.
      contained[[name]] <- Upper$sub(1)$get_intent()

    } else {

      # More than one: it is equal to the intersection of the
      # identifiers in all its parent concepts.
      # Thus, make the union (%|%) of all the intents of the
      # upper neighbours.
      equal[[name]] <- Upper$to_list() |>
        lapply(\(x) x$get_intent()) |>
        purrr::reduce(`%|%`)

    }

  }

}
```

Some of the coatoms (generic tags) are:

⟨ESET-NOD32, a variant of /downloader.agent.jn⟩, ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ and ⟨Microsoft, ransom:win32/eris⟩

The whole set of generic tags is listed in Section 6.2. Let us now inspect subclassses or subfamilies. We have found two kinds of relations between subfamilies:

- A tag coincides with the intersection of another set of tags or identifiers: ⟨av0, tag0⟩ = ⟨av1, tag1⟩ ∩ ⟨av2, tag2⟩ ∩ . . .

This expression must be understood as: "Every file whose identifier is tag0 by the antivirus av0, also receives the identifiers tag$i$ by every antivirus av$i$. And conversely, if a file is assigned all the tag$i$ identifiers by the corresponding av$i$, then it will also have the identifier tag0 given by av0."

For instance: ⟨McAfee, !02f9c9bb715b⟩ = ⟨ESET-NOD32, a variant of /.gzb⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.a⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Avira, ∅⟩ ∩ ⟨Microsoft, :os/multiverze⟩

Every time a file is assigned **all** the identifiers in the right hand side, it will also be assigned !02f9c9bb715b from McAfee, and viceversa.

- A tag is properly contained in the intersection of another set of tags or identifiers: ⟨av0, tag0⟩ ⊊ ⟨av1, tag1⟩ ∩ ⟨av2, tag2⟩ ∩ . . .

This expression must be understood as: "Every file whose identifier is tag0 by the antivirus av0, also receives the identifiers tag$i$ by every antivirus av$i$. But there are files which are assigned all the tag$i$ identifiers by the corresponding av$i$, that **do not have** the identifier tag0 given by av0."

For instance: ⟨McAfee, !0c5c3d793761⟩ ⊊ ⟨ESET-NOD32, a variant of /.hvn⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :script/sabsik.fl.b!ml⟩

With this information, we can confirm that ⟨McAfee, !0c5c3d793761⟩ is an identifier that conforms a proper subfamily inside the malware classes defined by the identifiers in the right hand side.

In Section 6.3 we present the entire set of (proper) subfamilies.

# 6 Result listings

In this section, we will show the relations found using the concept lattice and the clarification of the context.

For the sake of clarity, we use the expression [⟨av1, tag1⟩, ⟨av2, tag2⟩, . . .] to denote that ⟨av1, tag1⟩, ⟨av2, tag2⟩, . . . are all equivalent identifiers.

## 6.1 Equivalences found

⟨McAfee, !03eaa0113ccf⟩ ≡ ⟨ESET-NOD32, a variant of /spy.androrat.ak⟩ ≡ ⟨Kaspersky, heur:backdoor.os.climap.a⟩ ≡ ⟨Avast-Mobile, :androrat-k⟩ ≡ ⟨Avira, /androrat.b.gen⟩ ≡ ⟨Microsoft, :os/androrat.a!mtb⟩

⟨McAfee, !041a4a561b51⟩ ≡ ⟨ESET-NOD32, a variant of /spy.smsspy.it⟩ ≡ ⟨Kaspersky, heur:-spy.os.smforw.ff⟩ ≡ ⟨Avast-Mobile, :smforw-ut⟩ ≡ ⟨Avira, /styricka.d.gen⟩ ≡ ⟨Microsoft, :os/smforw.f⟩

⟨McAfee, !05906bbf77a9⟩ ≡ ⟨Avira, /andr.agent.fjub.gen⟩

⟨McAfee, !0b40c7b97ac3⟩ ≡ ⟨Avast-Mobile, :smsreg-cxq⟩

⟨McAfee, !0edb4e42346f⟩ ≡ ⟨ESET-NOD32, a variant of /addisplay.tapcore.b potentially unwanted⟩ ≡ ⟨Avira, /andr.addisplay.amaa.gen⟩

⟨McAfee, !1014e9dfb449⟩ ≡ ⟨ESET-NOD32, a variant of /sms.agent.ddy⟩ ≡ ⟨Kaspersky, heur:-sms.os.agent.acl⟩ ≡ ⟨Avast-Mobile, :fakeplayer-i⟩ ≡ ⟨Microsoft, :os/fakeplayer!rfn⟩

⟨McAfee, !10a9bb90535e⟩ ≡ ⟨ESET-NOD32, a variant of /addisplay.dowgin.bx potentially unwanted⟩ ≡ ⟨Kaspersky, not-a-virus:heur:.os.dowgin.i⟩ ≡ ⟨Avira, /andr.dowgin.bs.gen⟩

⟨McAfee, !19295d19d0ac⟩ ≡ ⟨ESET-NOD32, a variant of /jsmshider.o⟩ ≡ ⟨Avast-Mobile, :smsreg-cce ⟩

⟨McAfee, !217286377fec⟩ ≡ ⟨ESET-NOD32, a variant of /addisplay.youmi.a potentially unwanted⟩ ≡ ⟨Avira, /andr.youmi.b.gen⟩

⟨McAfee, !21b2930ee550⟩ ≡ ⟨ESET-NOD32, a variant of /lovetrap.r⟩ ≡ ⟨Kaspersky, not-a-virus:heur:monitor.os.agent.by⟩ ≡ ⟨Avast-Mobile, :agent-mga ⟩ ≡ ⟨Avira, /stalk.lovetrack.srkh.gen⟩

⟨McAfee, !22c0a8828f11⟩ ≡ ⟨ESET-NOD32, a variant of /.iva⟩ ≡ ⟨Avira, /dropper.fjvv.gen⟩

⟨McAfee, !26af7b239baa⟩ ≡ ⟨Avira, /clicker.amac.gen⟩

⟨McAfee, !27c80f826081⟩ ≡ ⟨ESET-NOD32, a variant of /smsreg.qh potentially unsafe⟩ ≡ ⟨Avast-Mobile, :smsreg-cci ⟩

⟨McAfee, !2d3809d0ee53⟩ ≡ ⟨ESET-NOD32, a variant of /wifikill.e potentially unsafe⟩ ≡ ⟨Kaspersky, heur:hacktool.os.wifikill.c⟩ ≡ ⟨Avast-Mobile, :wifikill-l ⟩ ≡ ⟨Avira, spr/andr.wifikill.a.gen⟩ ≡ ⟨Microsoft, :win32/occamy.c03⟩

⟨McAfee, !34f4de7847ed⟩ ≡ ⟨Kaspersky, not-a-virus:heur:risktool.os.wapron.dkj⟩ ≡ ⟨Avira, /wapron.heur.gen⟩

⟨McAfee, !37f600f5c0ff⟩ ≡ ⟨ESET-NOD32, a variant of /.cgt⟩ ≡ ⟨Kaspersky, heur:-dropper.os.hqwar.bb⟩ ≡ ⟨Avira, /dropper.fiti.gen⟩ ≡ ⟨Microsoft, :win32/ymacco.aa1d⟩

⟨McAfee, !41be721c4fcb⟩ ≡ ⟨ESET-NOD32, a variant of /sms.agent.adf⟩ ≡ ⟨Kaspersky, heur:-sms.os.agent.az⟩ ≡ ⟨Avast-Mobile, :sms-acr ⟩ ≡ ⟨Avira, /smsagent.ez.gen⟩ ≡ ⟨Microsoft, :os/sendsms.b!mtb⟩

⟨McAfee, !4300f16bee72⟩ ≡ ⟨Avast-Mobile, apk:crepmalware⟩ ≡ ⟨Microsoft, :win32/mson.a!ml⟩

⟨McAfee, !433e1fbff2f2⟩ ≡ ⟨ESET-NOD32, a variant of /clicker.kn⟩ ≡ ⟨Kaspersky, not-a-virus:heur:risktool.os.dnotua.bbsx⟩ ≡ ⟨Avira, /clicker.pag.gen⟩

⟨McAfee, !4960ca7dc787⟩ ≡ ⟨Avast-Mobile, :dropper-zq⟩

⟨McAfee, !4dc3d31060d4⟩ ≡ ⟨ESET-NOD32, /scamapp.cq potentially unwanted⟩ ≡ ⟨Kaspersky, not-a-virus:heur:risktool.os.dnotua.bbqx⟩ ≡ ⟨Avira, /andr.scamapp.fjts.gen⟩ ≡ ⟨Microsoft, :os/dnotua.a!mtb⟩

⟨McAfee, !4ef2bdf37187⟩ ≡ ⟨ESET-NOD32, a variant of /smforw.k⟩ ≡ ⟨Avast-Mobile, :smforw-br⟩ ≡ ⟨Avira, /smsforward.m.gen⟩

⟨McAfee, !518d985b5d90⟩ ≡ ⟨Microsoft, :os/spynote.e⟩

⟨McAfee, !52d56041f319⟩ ≡ ⟨ESET-NOD32, /.bt⟩ ≡ ⟨Kaspersky, heur:-sms.os.agent.ql⟩ ≡ ⟨Avast-Mobile, :fakeinst-aic⟩

⟨McAfee, !56563dfd00ed⟩ ≡ ⟨ESET-NOD32, a variant of /addisplay.waps.d potentially unwanted⟩ ≡ ⟨Avast-Mobile, apk:repmetagen ⟩ ≡ ⟨Avira, /andr.agent.fkcp.gen⟩ ≡ ⟨Microsoft, :os/wapsx.a!mtb⟩

⟨McAfee, !6b3516c2e2a1⟩ ≡ ⟨ESET-NOD32, a variant of /sms.agent.acg⟩ ≡ ⟨Avast-Mobile, :sms-az⟩ ≡ ⟨Avira, /smsagent.dx.gen⟩

⟨McAfee, !6e812cf2d3fe⟩ ≡ ⟨ESET-NOD32, a variant of /.aey⟩ ≡ ⟨Avast-Mobile, :smsreg-cxl⟩

⟨McAfee, !6fac26f92bad⟩ ≡ ⟨ESET-NOD32, a variant of /.tencentprotect.c potentially unsafe⟩ ≡ ⟨Kaspersky, not-a-virus:heur:.os.hiddenad.jn⟩

⟨McAfee, !71a0171bcea9⟩ ≡ ⟨ESET-NOD32, a variant of /hiddad.hi⟩ ≡ ⟨Kaspersky, not-a-virus:heur:.os.hiddenad.kx⟩ ≡ ⟨Avira, /hidad.agent.pap.gen⟩ ≡ ⟨Microsoft, :os/hiddad⟩

⟨McAfee, !7e7fcd69e6b6⟩ ≡ ⟨ESET-NOD32, a variant of /hypay.c potentially unsafe⟩ ≡ ⟨Kaspersky, not-a-virus:heur:risktool.os.agent.cc⟩ ≡ ⟨Avast-Mobile, :agent-mfv ⟩ ≡ ⟨Microsoft, tool:os/multiverze⟩

⟨McAfee, !857fe1d61832⟩ ≡ ⟨ESET-NOD32, a variant of /obfus.rl⟩ ≡ ⟨Kaspersky, not-a-virus:heur:.os.vuad.d⟩ ≡ ⟨Avast-Mobile, :ultimasms-a scam⟩ ≡ ⟨Avira, /obfuscated.fjhi.gen⟩ ≡ ⟨Microsoft, :os/ultimasms.a!mtb⟩

⟨McAfee, !861c383642a7⟩ ≡ ⟨Kaspersky, not-a-virus:uds:risktool.os.smsreg.mq⟩

⟨McAfee, !86d0620e6ea2⟩ ≡ ⟨ESET-NOD32, a variant of /smsreg.gq potentially unsafe⟩ ≡ ⟨Avira, spr/andr.smsreg.ku.gen⟩

⟨McAfee, !870c614fb6e5⟩ ≡ ⟨ESET-NOD32, /aio.a potentially unwanted⟩ ≡ ⟨Avira, spr/andr.aio.d.gen⟩ ≡ ⟨Microsoft, :os/aio.a!mtb⟩

⟨McAfee, !87b3bbab81d3⟩ ≡ ⟨ESET-NOD32, /scamapp.cr potentially unwanted⟩ ≡ ⟨Kaspersky, not-a-virus:heur:risktool.os.scamapp.f⟩

⟨McAfee, !97094bd83bbd⟩ ≡ ⟨ESET-NOD32, a variant of /spy.agent.bav⟩ ≡ ⟨Kaspersky, heur:-sms.os.agent.abh⟩ ≡ ⟨Avast-Mobile, :sms-pa⟩ ≡ ⟨Avira, /smsagent.gf.gen⟩

⟨McAfee, !9761d9d85394⟩ ≡ ⟨Microsoft, program:win32/ymacco.aaa6⟩

⟨McAfee, !9774b8704437⟩ ≡ ⟨ESET-NOD32, a variant of /sms.agent.fv⟩ ≡ ⟨Kaspersky, heur:-sms.os.opfake.a⟩ ≡ ⟨Avast-Mobile, :smssend-aht⟩ ≡ ⟨Avira, /sms.femto.a.gen⟩ ≡ ⟨Microsoft, :win32/occamy.cf1⟩

⟨McAfee, !97ee1b59effe⟩ ≡ ⟨ESET-NOD32, a variant of /agent.aut⟩ ≡ ⟨Kaspersky, heur:-downloader.os.agent.gz⟩ ≡ ⟨Avast-Mobile, :uten-dc⟩ ≡ ⟨Avira, /spy.agent.ahd.gen⟩ ≡ ⟨Microsoft, misleading:os/smsreg.a!xp⟩

⟨McAfee, !98a8b909ead5⟩ ≡ ⟨ESET-NOD32, a variant of /spy.savestealer.b⟩ ≡ ⟨Kaspersky, heur:.os.savestealer.b⟩

⟨McAfee, !9d7989c69e72⟩ ≡ ⟨Microsoft, :script/sabsik.te.b!ml⟩

⟨McAfee, !a155d6fbeffe⟩ ≡ ⟨Kaspersky, heur:hacktool.os.metasploit.j⟩ ≡ ⟨Avira, /dldr.agent.bi.gen⟩

⟨McAfee, !aab1e4cc9b65⟩ ≡ ⟨ESET-NOD32, a variant of /agent.bas⟩ ≡ ⟨Kaspersky, heur:-sms.os.agent.abw⟩

⟨McAfee, !b015f717e76b⟩ ≡ ⟨Avast-Mobile, :revo-op⟩ ≡ ⟨Microsoft, :win32/occamy.c88⟩

⟨McAfee, !b04f5a35d92c⟩ ≡ ⟨ESET-NOD32, a variant of /addisplay.revmob.a potentially unwanted⟩ ≡ ⟨Avira, /andr.revmob.a.gen⟩

⟨McAfee, !b25e2a555543⟩ ≡ ⟨Avira, /spyagent.fgyp.gen⟩

| | |
|---|---|
| ⟨McAfee, !b389bbea204e⟩ | ≡ ⟨ESET-NOD32, a variant of /fakeadblocker.a⟩ ≡ ⟨Kaspersky, not-a-virus:heur:.os.fakeadblocker.a⟩ ≡ ⟨Avira, /agent.srgm.gen⟩ |
| ⟨McAfee, !b8456ae6435a⟩ | ≡ ⟨ESET-NOD32, a variant of /addisplay.dowgin.dq potentially unwanted⟩ ≡ ⟨Kaspersky, heur:-dropper.os.agent.nu⟩ ≡ ⟨Microsoft, dos:os/multiverze⟩ |
| ⟨McAfee, !b8e631cc1d85⟩ | ≡ ⟨ESET-NOD32, a variant of /mtk.m⟩ ≡ ⟨Avira, /mtk.q.gen⟩ |
| ⟨McAfee, !bf3e6f490724⟩ | ≡ ⟨ESET-NOD32, a variant of /.ima⟩ ≡ ⟨Avira, /dropper.fkar.gen⟩ |
| ⟨McAfee, !c601b36c59ee⟩ | ≡ ⟨ESET-NOD32, a variant of generik.jnudyrh⟩ ≡ ⟨Avira, /spyagent.fkgc.gen⟩ |
| ⟨McAfee, !cc37847a1e4b⟩ | ≡ ⟨ESET-NOD32, a variant of /downloader.agent.fs⟩ ≡ ⟨Kaspersky, not-a-virus:heur:.os.agent.n⟩ ≡ ⟨Avast-Mobile, :agent-ovb⟩ ≡ ⟨Microsoft, ransom:os/lockscreen!rfn⟩ |
| ⟨McAfee, !cee4b1fae8a4⟩ | ≡ ⟨ESET-NOD32, a variant of /spy.agent.bom⟩ ≡ ⟨Kaspersky, heur:-banker.os.ubel.b⟩ ≡ ⟨Avira, /dropper.fkbp.gen⟩ ≡ ⟨Microsoft, spy:os/smsthief.l!mtb⟩ |
| ⟨McAfee, !d12c8b1082cf⟩ | ≡ ⟨ESET-NOD32, a variant of /morcut.c⟩ ≡ ⟨Kaspersky, heur:-spy.os.mekir.gen⟩ ≡ ⟨Avast-Mobile, :morcut-g⟩ ≡ ⟨Avira, /morcut.btr.gen⟩ ≡ ⟨Microsoft, :win32/ymacco.aae8⟩ |
| ⟨McAfee, !d71c100730cf⟩ | ≡ ⟨Avira, /dropper.shedun.ad.gen⟩ |
| ⟨McAfee, !dc62253c662d⟩ | ≡ ⟨ESET-NOD32, a variant of /smsreg.oq potentially unsafe⟩ ≡ ⟨Kaspersky, heur:-sms.os.agent.ty⟩ ≡ ⟨Avast-Mobile, :agent-isv⟩ ≡ ⟨Avira, /smsagent.rb.gen⟩ |
| ⟨McAfee, !e4d20eec9337⟩ | ≡ ⟨ESET-NOD32, a variant of /addisplay.revmob.b potentially unwanted⟩ ≡ ⟨Avira, /andr.revmob.c.gen⟩ |
| ⟨McAfee, !e691edcca810⟩ | ≡ ⟨ESET-NOD32, /sms.agent.jy⟩ ≡ ⟨Kaspersky, heur:-sms.os.agent.w⟩ ≡ ⟨Avast-Mobile, :agent-eic⟩ ≡ ⟨Avira, /smsagent.d.gen⟩ ≡ ⟨Microsoft, :os/sendsms.a!mtb⟩ |
| ⟨McAfee, !e92883f17efa⟩ | ≡ ⟨Kaspersky, not-a-virus:heur:risktool.os.dnotua.aacf⟩ ≡ ⟨Avast-Mobile, :dnotua-cf adw⟩ ≡ ⟨Avira, /andr.dnotua.frxx.gen⟩ |
| ⟨McAfee, !e98106d26174⟩ | ≡ ⟨ESET-NOD32, a variant of /agent.sl⟩ ≡ ⟨Kaspersky, heur:-dropper.os.agent.bu⟩ ≡ ⟨Avast-Mobile, :dropper-pz⟩ |
| ⟨McAfee, !e9b1bdf2a86a⟩ | ≡ ⟨ESET-NOD32, a variant of /hiddad.abf⟩ |
| ⟨McAfee, !f273c0aa75f2⟩ | ≡ ⟨Avira, /dropper.fgls.gen⟩ |
| ⟨McAfee, !f2ca8ad3c954⟩ | ≡ ⟨Kaspersky, not-a-virus:heur:risktool.os.dnotua.aacp⟩ ≡ ⟨Avast-Mobile, :agent-roy ⟩ ≡ ⟨Avira, /locker.mv.gen⟩ |

| | |
|---|---|
| ⟨McAfee, !f539f058e64d⟩ | ≡ ⟨ESET-NOD32, a variant of /monitor.tifamily.q⟩ ≡ ⟨Kaspersky, not-a-virus:heur:monitor.os.monitorminor.l⟩ ≡ ⟨Avast-Mobile, apk:repmetagen⟩ ≡ ⟨Avira, /andr.agent.fkac.gen⟩ |
| ⟨McAfee, !f5b9e3e836c8⟩ | ≡ ⟨ESET-NOD32, a variant of /.dbm⟩ ≡ ⟨Avast-Mobile, :agent-sfm⟩ ≡ ⟨Microsoft, dropper:os/agent.b!mtb⟩ |
| ⟨McAfee, !f8e1f5741f0d⟩ | ≡ ⟨Avast-Mobile, :agent-qel ⟩ ≡ ⟨Avira, /clicker.ohk.gen⟩ |
| ⟨McAfee, !fe8c6500ef6e⟩ | ≡ ⟨Avira, /agent.vca⟩ |
| ⟨McAfee, /tripoli⟩ | ≡ ⟨Avira, /banker.faar.gen⟩ |
| ⟨McAfee, adwind-fdwb.jar!be68bbb422d0⟩ | ≡ ⟨Avira, /.fgxw.gen⟩ ≡ ⟨Microsoft, :os/vigorf.a⟩ |
| ⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩ | ≡ ⟨Avira, /smsreg.ybd.gen⟩ |
| ⟨ESET-NOD32, a variant of /.dmj⟩ | ≡ ⟨Kaspersky, heur:-banker.os.bray.i⟩ ≡ ⟨Avira, /agent.fkec.gen⟩ |
| ⟨ESET-NOD32, a variant of /.evt⟩ | ≡ ⟨Avira, /dropper.fimo.gen⟩ |
| ⟨ESET-NOD32, a variant of /.izk⟩ | ≡ ⟨Avira, /banker.fkcg.gen⟩ |
| ⟨ESET-NOD32, a variant of /addisplay.waps.i potentially unwanted⟩ | ≡ ⟨Kaspersky, not-a-virus:heur:.os.agent.ep⟩ ≡ ⟨Avira, /andr.waps.i.gen⟩ ≡ ⟨Microsoft, :win32/bitrep.b⟩ |
| ⟨ESET-NOD32, a variant of /dropper.shedun.v⟩ | ≡ ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩ ≡ ⟨Microsoft, dropper:os/shedun.a!mtb⟩ |
| ⟨ESET-NOD32, a variant of /spy.agent.bat⟩ | ≡ ⟨Kaspersky, heur:-spy.os.spynote.an⟩ |
| ⟨ESET-NOD32, a variant of /spy.agent.bmp⟩ | ≡ ⟨Kaspersky, heur:-banker.os.bray.j⟩ ≡ ⟨Avira, /spyagent.fjzb.gen⟩ ≡ ⟨Microsoft, spy:os/bray.a⟩ |
| ⟨ESET-NOD32, a variant of /spy.agent.btn⟩ | ≡ ⟨Kaspersky, heur:-spy.os.agent.zq⟩ ≡ ⟨Avira, /spyagent.fkfl.gen⟩ |
| ⟨ESET-NOD32, a variant of /spy.spymax.e⟩ | ≡ ⟨Kaspersky, heur:-spy.os.spynote.ai⟩ ≡ ⟨Avast-Mobile, :spymax-ar spy⟩ ≡ ⟨Avira, /spymax.srkk.gen⟩ ≡ ⟨Microsoft, :os/spynote.h⟩ |

⟨Kaspersky, heur:-banker.os.bray.pac⟩ ≡ ⟨Avira, /dropper.fjkv.gen⟩

⟨Kaspersky, heur:-banker.os.fakecalls.k⟩ ≡ ⟨Microsoft, dropper:os/bankeragent.x⟩

⟨Kaspersky, heur:-dropper.os.agent.v⟩ ≡ ⟨Avira, /.ac.gen⟩

⟨Kaspersky, heur:.os.agent.aw⟩ ≡ ⟨Avira, /smssend.h.gen⟩

## 6.2 Generic tags

⟨McAfee, ∅⟩ ⟨Microsoft, program:os/multiverze⟩

⟨ESET-NOD32, a variant of /.gzb⟩ ⟨Microsoft, ransom:win32/eris⟩

⟨ESET-NOD32, a variant of /addisplay.mobby.i potentially unwanted⟩ ⟨Microsoft, spy:os/bray.a!mtb⟩

⟨ESET-NOD32, a variant of /clicker.jv⟩ [⟨McAfee, !03eaa0113ccf⟩, ⟨ESET-NOD32, a variant of /spy.androrat.ak⟩, ⟨Kaspersky, heur:backdoor.os.climap.a⟩, ⟨Avast-Mobile, :androrat-k⟩, ⟨Avira, /androrat.b.gen⟩, ⟨Microsoft, :os/androrat.a!mtb⟩]

⟨ESET-NOD32, a variant of /downloader.agent.jn⟩ [⟨McAfee, !041a4a561b51⟩, ⟨ESET-NOD32, a variant of /spy.smsspy.it⟩, ⟨Kaspersky, heur:-spy.os.smforw.ff⟩, ⟨Avast-Mobile, :smforw-ut⟩, ⟨Avira, /styricka.d.gen⟩, ⟨Microsoft, :os/smforw.f⟩]

⟨ESET-NOD32, multiple detections⟩ [⟨McAfee, !2d3809d0ee53⟩, ⟨ESET-NOD32, a variant of /wifikill.e potentially unsafe⟩, ⟨Kaspersky, heur:hacktool.os.wifikill.c⟩, ⟨Avast-Mobile, :wifikill-l ⟩, ⟨Avira, spr/andr.wifikill.a.gen⟩, ⟨Microsoft, :win32/occamy.c03⟩]

⟨ESET-NOD32, ∅⟩ [⟨McAfee, !41be721c4fcb⟩, ⟨ESET-NOD32, a variant of /sms.agent.adf⟩, ⟨Kaspersky, heur:-sms.os.agent.az⟩, ⟨Avast-Mobile, :sms-acr ⟩, ⟨Avira, /smsagent.ez.gen⟩, ⟨Microsoft, :os/sendsms.b!mtb⟩]

| | |
|---|---|
| ⟨Kaspersky, ∅⟩ | [⟨McAfee, !857fe1d61832⟩, ⟨ESET-NOD32, a variant of /obfus.rl⟩, ⟨Kaspersky, not-a-virus:heur:.os.vuad.d⟩, ⟨Avast-Mobile, :ultimasms-a scam⟩, ⟨Avira, /obfuscated.fjhi.gen⟩, ⟨Microsoft, :os/ultimasms.a!mtb⟩] |
| ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ | [⟨McAfee, !9774b8704437⟩, ⟨ESET-NOD32, a variant of /sms.agent.fv⟩, ⟨Kaspersky, heur:-sms.os.opfake.a⟩, ⟨Avast-Mobile, :smssend-aht⟩, ⟨Avira, /sms.femto.a.gen⟩, ⟨Microsoft, :win32/occamy.cf1⟩] |
| ⟨Avast-Mobile, :evo-gen⟩ | [⟨McAfee, !97ee1b59effe⟩, ⟨ESET-NOD32, a variant of /agent.aut⟩, ⟨Kaspersky, heur:-downloader.os.agent.gz⟩, ⟨Avast-Mobile, :uten-dc⟩, ⟨Avira, /spy.agent.ahd.gen⟩, ⟨Microsoft, misleading:os/smsreg.a!xp⟩] |
| ⟨Avast-Mobile, ∅⟩ | [⟨McAfee, !d12c8b1082cf⟩, ⟨ESET-NOD32, a variant of /morcut.c⟩, ⟨Kaspersky, heur:-spy.os.mekir.gen⟩, ⟨Avast-Mobile, :morcut-g⟩, ⟨Avira, /morcut.btr.gen⟩, ⟨Microsoft, :win32/ymacco.aae8⟩] |
| ⟨Avira, ∅⟩ | [⟨McAfee, !e691edcca810⟩, ⟨ESET-NOD32, /sms.agent.jy⟩, ⟨Kaspersky, heur:-sms.os.agent.w⟩, ⟨Avast-Mobile, :agent-eic⟩, ⟨Avira, /smsagent.d.gen⟩, ⟨Microsoft, :os/sendsms.a!mtb⟩] |
| ⟨Microsoft, :os/clicker.b!mtb⟩ | [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨Microsoft, :os/multiverze⟩ | [⟨ESET-NOD32, a variant of /spy.agent.bat⟩, ⟨Kaspersky, heur:-spy.os.spynote.an⟩] |
| ⟨Microsoft, :script/sabsik.fl.b!ml⟩ | [⟨Kaspersky, heur:-dropper.os.agent.v⟩, ⟨Avira, /.ac.gen⟩] |
| ⟨Microsoft, :script/wacatac.b!ml⟩ | [⟨Kaspersky, heur:.os.agent.aw⟩, ⟨Avira, /smssend.h.gen⟩] |
| ⟨Microsoft, ∅⟩ | |

## 6.3 Subfamilies

### 6.3.1 Tags that coincide with the intersection of parent identifiers

⟨McAfee, !02f9c9bb715b⟩    ⟨ESET-NOD32, a variant of /.gzb⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.a⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Avira, ∅⟩ ∩ ⟨Microsoft, :os/multiverze⟩

⟨McAfee, !190b85d5b007⟩    ⟨Kaspersky, not-a-virus:heur:risktool.os.smsreg.mq⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ∅⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩]

⟨McAfee, !376e9e596258⟩    ⟨Avast-Mobile, :spymax-d spy⟩ ∩ ⟨Avira, ∅⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.bat⟩, ⟨Kaspersky, heur:-spy.os.spynote.an⟩]

⟨McAfee, !5720b5e8f3bd⟩    ⟨ESET-NOD32, a variant of /.gzb⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.a⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :script/sabsik.fl.b!ml⟩

⟨McAfee, !5a145a055fb1⟩    ⟨ESET-NOD32, a variant of /.hvn⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Avira, ∅⟩ ∩ ⟨Microsoft, program:os/multiverze⟩

⟨McAfee, !7d5e9382d046⟩    ⟨ESET-NOD32, a variant of /.gzb⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.hiddenad.ot⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :win32/phonzy.a!ml⟩

⟨McAfee, !cede65505eff⟩    ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ∅⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.btn⟩, ⟨Kaspersky, heur:-spy.os.agent.zq⟩, ⟨Avira, /spyagent.fkfl.gen⟩]

⟨McAfee, !d7f7cde83db8⟩    ⟨ESET-NOD32, a variant of /.ixe⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩

⟨Kaspersky, not-a-virus:heur:.os.ewind.hz⟩    ⟨ESET-NOD32, multiple detections⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩

⟨Avast-Mobile, :spymax-d spy⟩    ⟨Avira, ∅⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.bat⟩, ⟨Kaspersky, heur:-spy.os.spynote.an⟩]

⟨Avira, /agent.fjnr.gen⟩    ⟨McAfee, ∅⟩ ∩ ⟨ESET-NOD32, a variant of /downloader.agent.jn⟩ ∩ ⟨Kaspersky, heur:-downloader.os.agent.jy⟩ ∩ ⟨Avast-Mobile, :metasploit-q ⟩ ∩ ⟨Microsoft, hacktool:os/mesploit.a⟩

⟨Avira, /andr.agent.fokp.gen⟩    ⟨ESET-NOD32, a variant of /addisplay.mobby.i potentially unwanted⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩

| | |
|---|---|
| ⟨Avira, /dldr.fnaa.gen⟩ | ⟨McAfee, ∅⟩ ∩ ⟨ESET-NOD32, a variant of /downloader.agent.jn⟩ ∩ ⟨Kaspersky, heur:-downloader.os.agent.jy⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ∅⟩ |
| ⟨Microsoft, hacktool:os/mesploit.a⟩ | ⟨ESET-NOD32, a variant of /downloader.agent.jn⟩ ∩ ⟨Kaspersky, heur:-downloader.os.agent.jy⟩ ∩ ⟨Avast-Mobile, :metasploit-q ⟩ |
| [⟨McAfee, !05906bbf77a9⟩, ⟨Avira, /andr.agent.fjub.gen⟩] | ⟨ESET-NOD32, multiple detections⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.ewind.hz⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, program:os/multiverze⟩ |
| [⟨McAfee, !19295d19d0ac⟩, ⟨ESET-NOD32, a variant of /jsmshider.o⟩, ⟨Avast-Mobile, :smsreg-cce ⟩] | ⟨Microsoft, :script/wacatac.b!ml⟩ ∩ [⟨Kaspersky, heur:.os.agent.aw⟩, ⟨Avira, /smssend.h.gen⟩] |
| [⟨McAfee, !22c0a8828f11⟩, ⟨ESET-NOD32, a variant of /.iva⟩, ⟨Avira, /dropper.fjvv.gen⟩] | ⟨Kaspersky, heur:-dropper.os.hqwar.bk⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩ |
| [⟨McAfee, !26af7b239baa⟩, ⟨Avira, /clicker.amac.gen⟩] | ⟨ESET-NOD32, ∅⟩ ∩ ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, apk:repsandbox⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩ |
| [⟨McAfee, !27c80f826081⟩, ⟨ESET-NOD32, a variant of /smsreg.qh potentially unsafe⟩, ⟨Avast-Mobile, :smsreg-cci ⟩] | ⟨Microsoft, :script/sabsik.fl.b!ml⟩ ∩ [⟨Kaspersky, heur:.os.agent.aw⟩, ⟨Avira, /smssend.h.gen⟩] |
| [⟨McAfee, !34f4de7847ed⟩, ⟨Kaspersky, not-a-virus:heur:risktool.os.wapron.dkj⟩, ⟨Avira, /wapron.heur.gen⟩] | ⟨ESET-NOD32, a variant of /.jiagu.d potentially unsafe⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, program:os/multiverze⟩ |

[⟨McAfee, !4300f16bee72⟩, ⟨Avast-Mobile, apk:crepmalware⟩, ⟨Microsoft, :win32/mson.a!ml⟩]

⟨ESET-NOD32, multiple detections⟩ ∩ ⟨Kaspersky, ∅⟩ ∩ ⟨Avira, ∅⟩

[⟨McAfee, !433e1fbff2f2⟩, ⟨ESET-NOD32, a variant of /clicker.kn⟩, ⟨Kaspersky, not-a-virus:heur:risktool.os.dnotua.bbsx⟩, ⟨Avira, /clicker.pag.gen⟩]

⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, :os/clicker.b!mtb⟩

[⟨McAfee, !4960ca7dc787⟩, ⟨Avast-Mobile, :dropper-zq⟩]

⟨ESET-NOD32, a variant of /.aev⟩ ∩ ⟨Microsoft, :win32/occamy.aa⟩ ∩ [⟨Kaspersky, heur:-dropper.os.agent.v⟩, ⟨Avira, /.ac.gen⟩]

[⟨McAfee, !6fac26f92bad⟩, ⟨ESET-NOD32, a variant of /.tencentprotect.c potentially unsafe⟩, ⟨Kaspersky, not-a-virus:heur:.os.hiddenad.jn⟩]

⟨Avast-Mobile, ∅⟩ ∩ ⟨Avira, ∅⟩ ∩ ⟨Microsoft, :win32/presenoker⟩

[⟨McAfee, !86d0620e6ea2⟩, ⟨ESET-NOD32, a variant of /smsreg.gq potentially unsafe⟩, ⟨Avira, spr/andr.smsreg.ku.gen⟩]

⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, :win32/presenoker⟩

[⟨McAfee, !87b3bbab81d3⟩, ⟨ESET-NOD32, /scamapp.cr potentially unwanted⟩, ⟨Kaspersky, not-a-virus:heur:risktool.os.scamapp.f⟩]

⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, ∅⟩ ∩ ⟨Microsoft, ∅⟩

[⟨McAfee, !9761d9d85394⟩, ⟨Microsoft, program:win32/ymacco.aaa6⟩]   ⟨ESET-NOD32, a variant of /addisplay.mobby.i potentially unwanted⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.ewind.kp⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Avira, ∅⟩

[⟨McAfee, !a155d6fbeffe⟩, ⟨Kaspersky, heur:hacktool.os.metasploit.j⟩, ⟨Avira, /dldr.agent.bi.gen⟩]   ⟨ESET-NOD32, a variant of /downloader.agent.jn⟩ ∩ ⟨Avast-Mobile, :metasploit-q ⟩ ∩ ⟨Microsoft, ∅⟩

[⟨McAfee, !b25e2a555543⟩, ⟨Avira, /spyagent.fgyp.gen⟩]   ⟨ESET-NOD32, multiple detections⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.ewind.hz⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩

[⟨McAfee, !b8e631cc1d85⟩, ⟨ESET-NOD32, a variant of /mtk.m⟩, ⟨Avira, /mtk.q.gen⟩]   ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩

[⟨McAfee, !bf3e6f490724⟩, ⟨ESET-NOD32, a variant of /.ima⟩, ⟨Avira, /dropper.fkar.gen⟩]   ⟨Kaspersky, heur:-dropper.os.hqwar.bk⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, :os/multiverze⟩

[⟨McAfee, !e92883f17efa⟩, ⟨Kaspersky, not-a-virus:heur:risktool.os.dnotua.aacf⟩, ⟨Avast-Mobile, :dnotua-cf adw⟩, ⟨Avira, /andr.dnotua.frxx.gen⟩]   ⟨ESET-NOD32, ∅⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩

[⟨McAfee, !e9b1bdf2a86a⟩, ⟨ESET-NOD32, a variant of /hiddad.abf⟩]   ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Avira, ∅⟩ ∩ ⟨Microsoft, program:os/multiverze⟩

[⟨McAfee, !f273c0aa75f2⟩, ⟨Avira, /dropper.fgls.gen⟩]   ⟨ESET-NOD32, a variant of /.fnn⟩ ∩ ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ∅⟩

[⟨McAfee, !f2ca8ad3c954⟩, ⟨Kaspersky, not-a-virus:heur:risktool.os.dnotua.aacp⟩, ⟨Avast-Mobile, :agent-roy ⟩, ⟨Avira, /locker.mv.gen⟩]     ⟨ESET-NOD32, a variant of /clicker.jv⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩

[⟨McAfee, !f8e1f5741f0d⟩, ⟨Avast-Mobile, :agent-qel ⟩, ⟨Avira, /clicker.ohk.gen⟩]     ⟨ESET-NOD32, a variant of /clicker.jv⟩ ∩ ⟨Kaspersky, ∅⟩ ∩ ⟨Microsoft, :os/clicker.b!mtb⟩

[⟨McAfee, /tripoli⟩, ⟨Avira, /banker.faar.gen⟩]     ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.bat⟩, ⟨Kaspersky, heur:-spy.os.spynote.an⟩]

[⟨ESET-NOD32, a variant of /.dmj⟩, ⟨Kaspersky, heur:-banker.os.bray.i⟩, ⟨Avira, /agent.fkec.gen⟩]     ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩

[⟨ESET-NOD32, a variant of /addisplay.waps.i potentially unwanted⟩, ⟨Kaspersky, not-a-virus:heur:.os.agent.ep⟩, ⟨Avira, /andr.waps.i.gen⟩, ⟨Microsoft, :win32/bitrep.b⟩]     ⟨McAfee, ∅⟩ ∩ ⟨Avast-Mobile, ∅⟩

[⟨Kaspersky, heur:-banker.os.bray.pac⟩, ⟨Avira, /dropper.fjkv.gen⟩]     ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩

### 6.3.2 Tags properly contained in the intersection of parent identifiers

| | |
|---|---|
| ⟨McAfee, !07e0c50a8a28⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.bmp⟩, ⟨Kaspersky, heur:-banker.os.bray.j⟩, ⟨Avira, /spyagent.fjzb.gen⟩, ⟨Microsoft, spy:os/bray.a⟩] |
| ⟨McAfee, !092d858c2721⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !0c5c3d793761⟩ | ⟨ESET-NOD32, a variant of /.hvn⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :script/sabsik.fl.b!ml⟩ |
| ⟨McAfee, !0eeb70a4f783⟩ | ⟨ESET-NOD32, a variant of /.iyt⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨Kaspersky, heur:-banker.os.bray.pac⟩, ⟨Avira, /dropper.fjkv.gen⟩] |
| ⟨McAfee, !100c1f7997f3⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !152ab367f6c0⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !1d576bceef0a⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !1dc3e0df2b72⟩ | ⟨Kaspersky, not-a-virus:heur:risktool.os.smsreg.mq⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |
| ⟨McAfee, !1e07e4821182⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !1fcc38149cf4⟩ | ⟨ESET-NOD32, a variant of /addisplay.mobby.i potentially unwanted⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.ewind.kp⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /andr.agent.fokp.gen⟩ ∩ ⟨Microsoft, :os/ewind.a⟩ |
| ⟨McAfee, !2943331e1bd4⟩ | ⟨ESET-NOD32, a variant of /.ixe⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :script/sabsik.fl.b!ml⟩ |
| ⟨McAfee, !30049fd14310⟩ | ⟨ESET-NOD32, a variant of /.iyt⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨Kaspersky, heur:-banker.os.bray.pac⟩, ⟨Avira, /dropper.fjkv.gen⟩] |

| | |
|---|---|
| ⟨McAfee, !372d9fbeab97⟩ | ⟨Kaspersky, not-a-virus:heur:risktool.os.smsreg.mq⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |
| ⟨McAfee, !38f46450ec4e⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.btn⟩, ⟨Kaspersky, heur:-spy.os.agent.zq⟩, ⟨Avira, /spyagent.fkfl.gen⟩] |
| ⟨McAfee, !3a9d8bf77a82⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !41f9ce42ed53⟩ | ⟨ESET-NOD32, a variant of /.iyt⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨Kaspersky, heur:-banker.os.bray.pac⟩, ⟨Avira, /dropper.fjkv.gen⟩] |
| ⟨McAfee, !436482c1bf89⟩ | ⟨Kaspersky, not-a-virus:heur:risktool.os.smsreg.mq⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |
| ⟨McAfee, !46b876999b18⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !4a9775227534⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !4c1ba739a19a⟩ | ⟨ESET-NOD32, a variant of /.iyt⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨Kaspersky, heur:-banker.os.bray.pac⟩, ⟨Avira, /dropper.fjkv.gen⟩] |
| ⟨McAfee, !56b17a7b2031⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !58b808ba0b90⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.btn⟩, ⟨Kaspersky, heur:-spy.os.agent.zq⟩, ⟨Avira, /spyagent.fkfl.gen⟩] |
| ⟨McAfee, !5ce4733849f2⟩ | ⟨Kaspersky, not-a-virus:heur:risktool.os.smsreg.mq⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |
| ⟨McAfee, !5d12844f3c59⟩ | ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |

| | |
|---|---|
| ⟨McAfee, !623f3d059fe5⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !7199c8e5ef83⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !72b80100f4b5⟩ | ⟨ESET-NOD32, a variant of /.ixe⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :script/sabsik.fl.b!ml⟩ |
| ⟨McAfee, !766804b26c4b⟩ | ⟨ESET-NOD32, a variant of /.hvn⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩ |
| ⟨McAfee, !8a04b268c0ad⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.bmp⟩, ⟨Kaspersky, heur:-banker.os.bray.j⟩, ⟨Avira, /spyagent.fjzb.gen⟩, ⟨Microsoft, spy:os/bray.a⟩] |
| ⟨McAfee, !8f5a7ab3618f⟩ | ⟨ESET-NOD32, /spy.agent.bwa⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨Kaspersky, heur:-banker.os.bray.pac⟩, ⟨Avira, /dropper.fjkv.gen⟩] |
| ⟨McAfee, !919a1900c529⟩ | ⟨ESET-NOD32, a variant of /addisplay.mobby.i potentially unwanted⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /andr.agent.fokp.gen⟩ |
| ⟨McAfee, !93ddea2c991a⟩ | ⟨ESET-NOD32, a variant of /addisplay.mobby.i potentially unwanted⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.ewind.kp⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /andr.agent.fokp.gen⟩ ∩ ⟨Microsoft, :os/ewind.a⟩ |
| ⟨McAfee, !97476b7b4994⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !9aa9ed3d4306⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨ESET-NOD32, a variant of /.dmj⟩, ⟨Kaspersky, heur:-banker.os.bray.i⟩, ⟨Avira, /agent.fkec.gen⟩] |
| ⟨McAfee, !a1dcd5d388af⟩ | ⟨ESET-NOD32, a variant of /.iyt⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨Kaspersky, heur:-banker.os.bray.pac⟩, ⟨Avira, /dropper.fjkv.gen⟩] |
| ⟨McAfee, !a5b338a748d0⟩ | ⟨Kaspersky, not-a-virus:heur:risktool.os.smsreg.mq⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |

| | |
|---|---|
| ⟨McAfee, !add20546890d⟩ | ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩ ∩ [⟨ESET-NOD32, a variant of /.evt⟩, ⟨Avira, /dropper.fimo.gen⟩] |
| ⟨McAfee, !b0b54fc28aa1⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨ESET-NOD32, a variant of /.dmj⟩, ⟨Kaspersky, heur:-banker.os.bray.i⟩, ⟨Avira, /agent.fkec.gen⟩] |
| ⟨McAfee, !b3697a6e8fc4⟩ | ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩ ∩ [⟨ESET-NOD32, a variant of /.evt⟩, ⟨Avira, /dropper.fimo.gen⟩] |
| ⟨McAfee, !b4ada9b0b45d⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !bc1b04c491bf⟩ | ⟨ESET-NOD32, /spy.agent.bwa⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨Kaspersky, heur:-banker.os.bray.pac⟩, ⟨Avira, /dropper.fjkv.gen⟩] |
| ⟨McAfee, !bd7c9aee03b2⟩ | ⟨ESET-NOD32, a variant of /.hvn⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩ |
| ⟨McAfee, !c5b53b908443⟩ | ⟨Kaspersky, not-a-virus:heur:risktool.os.smsreg.mq⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |
| ⟨McAfee, !ce28ca783759⟩ | ⟨Kaspersky, not-a-virus:heur:risktool.os.smsreg.mq⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |
| ⟨McAfee, !d64dcc75a998⟩ | ⟨Kaspersky, not-a-virus:heur:risktool.os.smsreg.mq⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |
| ⟨McAfee, !d93278e58557⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨ESET-NOD32, a variant of /.dmj⟩, ⟨Kaspersky, heur:-banker.os.bray.i⟩, ⟨Avira, /agent.fkec.gen⟩] |
| ⟨McAfee, !de4d4a92b49b⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.bmp⟩, ⟨Kaspersky, heur:-banker.os.bray.j⟩, ⟨Avira, /spyagent.fjzb.gen⟩, ⟨Microsoft, spy:os/bray.a⟩] |
| ⟨McAfee, !e312d3e7906c⟩ | ⟨ESET-NOD32, a variant of /.hvn⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :script/sabsik.fl.b!ml⟩ |

| | |
|---|---|
| ⟨McAfee, !e73bd0b90af0⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !e777adc22f2a⟩ | ⟨Avast-Mobile, :shedun-v⟩ ∩ ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨McAfee, !e99147cfc18a⟩ | ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ransom:win32/eris⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |
| ⟨McAfee, !f49c91a8e037⟩ | ⟨ESET-NOD32, a variant of /.hvn⟩ ∩ ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ ∩ ⟨Microsoft, :script/sabsik.fl.b!ml⟩ |
| ⟨McAfee, !fee8f87a75d1⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.bmp⟩, ⟨Kaspersky, heur:-banker.os.bray.j⟩, ⟨Avira, /spyagent.fjzb.gen⟩, ⟨Microsoft, spy:os/bray.a⟩] |
| ⟨ESET-NOD32, /spy.agent.bwa⟩ | ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨Kaspersky, heur:-banker.os.bray.pac⟩, ⟨Avira, /dropper.fjkv.gen⟩] |
| ⟨ESET-NOD32, a variant of /.aev⟩ | [⟨Kaspersky, heur:-dropper.os.agent.v⟩, ⟨Avira, /.ac.gen⟩] |
| ⟨ESET-NOD32, a variant of /.fnn⟩ | ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ |
| ⟨ESET-NOD32, a variant of /.hvn⟩ | ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ |
| ⟨ESET-NOD32, a variant of /.ixe⟩ | ⟨Kaspersky, not-a-virus:heur:.os.adlo.b⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ |
| ⟨ESET-NOD32, a variant of /.iyt⟩ | ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, spy:os/bray.a!mtb⟩ ∩ [⟨Kaspersky, heur:-banker.os.bray.pac⟩, ⟨Avira, /dropper.fjkv.gen⟩] |
| ⟨ESET-NOD32, a variant of /.jiagu.d potentially unsafe⟩ | ⟨Microsoft, program:os/multiverze⟩ |
| ⟨Kaspersky, heur:-downloader.os.agent.jy⟩ | ⟨ESET-NOD32, a variant of /downloader.agent.jn⟩ |
| ⟨Kaspersky, heur:-dropper.os.hqwar.bk⟩ | ⟨Avast-Mobile, :evo-gen⟩ |
| ⟨Kaspersky, not-a-virus:heur:.os.adlo.a⟩ | ⟨ESET-NOD32, a variant of /.gzb⟩ |
| ⟨Kaspersky, not-a-virus:heur:.os.ewind.kp⟩ | ⟨ESET-NOD32, a variant of /addisplay.mobby.i potentially unwanted⟩ |

| | |
|---|---|
| ⟨Kaspersky, not-a-virus:heur:.os.hiddenad.ot⟩ | ⟨ESET-NOD32, a variant of /.gzb⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /agent.mer.gen⟩ |
| ⟨Kaspersky, not-a-virus:heur:risktool.os.smsreg.bzq⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ [⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩] |
| ⟨Kaspersky, not-a-virus:uds:.os.ewind.kp⟩ | ⟨McAfee, !919a1900c529⟩ ∩ ⟨ESET-NOD32, a variant of /addisplay.mobby.i potentially unwanted⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /andr.agent.fokp.gen⟩ |
| ⟨Avast-Mobile, :metasploit-q ⟩ | ⟨ESET-NOD32, a variant of /downloader.agent.jn⟩ |
| ⟨Avast-Mobile, :shedun-v⟩ | [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨Avast-Mobile, apk:repsandbox⟩ | ⟨Kaspersky, ∅⟩ |
| ⟨Avira, /agent.hutg⟩ | [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |
| ⟨Avira, /agent.mer.gen⟩ | ⟨Avast-Mobile, :evo-gen⟩ |
| ⟨Avira, /savesteal.ybc.gen⟩ | ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, program:os/multiverze⟩ ∩ [⟨McAfee, !98a8b909ead5⟩, ⟨ESET-NOD32, a variant of /spy.savestealer.b⟩, ⟨Kaspersky, heur:.os.savestealer.b⟩] |
| ⟨Microsoft, :os/ewind.a⟩ | ⟨ESET-NOD32, a variant of /addisplay.mobby.i potentially unwanted⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Avira, /andr.agent.fokp.gen⟩ |
| ⟨Microsoft, :win32/bitrepeyp.b⟩ | ⟨Avast-Mobile, ∅⟩ |
| ⟨Microsoft, :win32/occamy.aa⟩ | [⟨Kaspersky, heur:-dropper.os.agent.v⟩, ⟨Avira, /.ac.gen⟩] |
| ⟨Microsoft, :win32/phonzy.a!ml⟩ | ⟨Avast-Mobile, :evo-gen⟩ |
| ⟨Microsoft, :win32/presenoker⟩ | ⟨Avast-Mobile, ∅⟩ |
| [⟨McAfee, !0b40c7b97ac3⟩, ⟨Avast-Mobile, :smsreg-cxq⟩] | ⟨Avira, /agent.hutg⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩] |

[⟨McAfee, !0edb4e42346f⟩, ⟨ESET-NOD32, a variant of /addisplay.tapcore.b potentially unwanted⟩, ⟨Avira, /andr.addisplay.amaa.gen⟩]

⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, program:os/multiverze⟩

[⟨McAfee, !1014e9dfb449⟩, ⟨ESET-NOD32, a variant of /sms.agent.ddy⟩, ⟨Kaspersky, heur:-sms.os.agent.acl⟩, ⟨Avast-Mobile, :fakeplayer-i⟩, ⟨Microsoft, :os/fakeplayer!rfn⟩]

⟨Avira, ∅⟩

[⟨McAfee, !10a9bb90535e⟩, ⟨ESET-NOD32, a variant of /addisplay.dowgin.bx potentially unwanted⟩, ⟨Kaspersky, not-a-virus:heur:.os.dowgin.i⟩, ⟨Avira, /andr.dowgin.bs.gen⟩]

⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, :win32/bitrepeyp.b⟩

[⟨McAfee, !217286377fec⟩, ⟨ESET-NOD32, a variant of /addisplay.youmi.a potentially unwanted⟩, ⟨Avira, /andr.youmi.b.gen⟩]

⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, :win32/bitrepeyp.b⟩

[⟨McAfee,  ⟨Microsoft, ∅⟩
!21b2930ee550⟩,
⟨ESET-NOD32, a
variant of /lovetrap.r⟩,
⟨Kaspersky, not-a-
virus:heur:monitor.os.agent.by⟩,
⟨Avast-Mobile,
:agent-mga ⟩, ⟨Avira,
/stalk.lovetrack.srkh.gen⟩]

[⟨McAfee,  ⟨Avast-Mobile, ∅⟩
!37f600f5c0ff⟩,
⟨ESET-NOD32, a
variant of /.cgt⟩,
⟨Kaspersky, heur:-
dropper.os.hqwar.bb⟩,
⟨Avira,
/dropper.fiti.gen⟩,
⟨Microsoft,
:win32/ymacco.aa1d⟩]

[⟨McAfee,  ⟨Avast-Mobile, :evo-gen⟩
!4dc3d31060d4⟩,
⟨ESET-NOD32,
/scamapp.cq
potentially unwanted⟩,
⟨Kaspersky, not-a-
virus:heur:risktool.os.dnotua.bbqx⟩,
⟨Avira,
/andr.scamapp.fjts.gen⟩,
⟨Microsoft,
:os/dnotua.a!mtb⟩]

[⟨McAfee,  ⟨Kaspersky, ∅⟩ ∩ ⟨Microsoft, ∅⟩
!4ef2bdf37187⟩,
⟨ESET-NOD32, a
variant of /smforw.k⟩,
⟨Avast-Mobile,
:smforw-br⟩, ⟨Avira,
/smsforward.m.gen⟩]

[⟨McAfee,  ⟨Avast-Mobile, :spymax-d spy⟩ ∩ ⟨Avira, ∅⟩ ∩ [⟨ESET-NOD32, a
!518d985b5d90⟩,  variant of /spy.agent.bat⟩, ⟨Kaspersky, heur:-spy.os.spynote.an⟩]
⟨Microsoft,
:os/spynote.e⟩]

[⟨McAfee, !52d56041f319⟩, ⟨ESET-NOD32, /.bt⟩, ⟨Kaspersky, heur:-sms.os.agent.ql⟩, ⟨Avast-Mobile, :fakeinst-aic⟩]     ⟨Avira, ∅⟩ ∩ ⟨Microsoft, ∅⟩

[⟨McAfee, !56563dfd00ed⟩, ⟨ESET-NOD32, a variant of /addisplay.waps.d potentially unwanted⟩, ⟨Avast-Mobile, apk:repmetagen ⟩, ⟨Avira, /andr.agent.fkcp.gen⟩, ⟨Microsoft, :os/wapsx.a!mtb⟩]     ⟨Kaspersky, ∅⟩

[⟨McAfee, !6b3516c2e2a1⟩, ⟨ESET-NOD32, a variant of /sms.agent.acg⟩, ⟨Avast-Mobile, :sms-az⟩, ⟨Avira, /smsagent.dx.gen⟩]     ⟨Kaspersky, ∅⟩ ∩ ⟨Microsoft, ∅⟩

[⟨McAfee, !6e812cf2d3fe⟩, ⟨ESET-NOD32, a variant of /.aey⟩, ⟨Avast-Mobile, :smsreg-cxl⟩]     ⟨Microsoft, :win32/occamy.aa⟩ ∩ [⟨Kaspersky, heur:-dropper.os.agent.v⟩, ⟨Avira, /.ac.gen⟩]

[⟨McAfee,          ⟨Avast-Mobile, :evo-gen⟩
!71a0171bcea9⟩,
⟨ESET-NOD32, a
variant of /hiddad.hi⟩,
⟨Kaspersky, not-a-
virus:heur:.os.hiddenad.kx⟩,
⟨Avira,
/hidad.agent.pap.gen⟩,
⟨Microsoft,
:os/hiddad⟩]

[⟨McAfee,          ⟨Avira, ∅⟩
!7e7fcd69e6b6⟩,
⟨ESET-NOD32, a
variant of /hypay.c
potentially unsafe⟩,
⟨Kaspersky, not-a-
virus:heur:risktool.os.agent.cc⟩,
⟨Avast-Mobile,
:agent-mfv ⟩,
⟨Microsoft,
tool:os/multiverze⟩]

[⟨McAfee,          ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, ∅⟩ ∩ [⟨ESET-NOD32,
!861c383642a7⟩,       /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩]
⟨Kaspersky, not-a-
virus:uds:risktool.os.smsreg.mq⟩]

[⟨McAfee,          ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, ∅⟩
!870c614fb6e5⟩,
⟨ESET-NOD32, /aio.a
potentially unwanted⟩,
⟨Avira,
spr/andr.aio.d.gen⟩,
⟨Microsoft,
:os/aio.a!mtb⟩]

| | |
|---|---|
| [⟨McAfee, !97094bd83bbd⟩, ⟨ESET-NOD32, a variant of /spy.agent.bav⟩, ⟨Kaspersky, heur:-sms.os.agent.abh⟩, ⟨Avast-Mobile, :sms-pa⟩, ⟨Avira, /smsagent.gf.gen⟩] | ⟨Microsoft, ∅⟩ |
| [⟨McAfee, !98a8b909ead5⟩, ⟨ESET-NOD32, a variant of /spy.savestealer.b⟩, ⟨Kaspersky, heur:.os.savestealer.b⟩] | ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, program:os/multiverze⟩ |
| [⟨McAfee, !9d7989c69e72⟩, ⟨Microsoft, :script/sabsik.te.b!ml⟩] | ⟨Avast-Mobile, :evo-gen⟩ ∩ [⟨ESET-NOD32, a variant of /spy.agent.btn⟩, ⟨Kaspersky, heur:-spy.os.agent.zq⟩, ⟨Avira, /spyagent.fkfl.gen⟩] |
| [⟨McAfee, !aab1e4cc9b65⟩, ⟨ESET-NOD32, a variant of /agent.bas⟩, ⟨Kaspersky, heur:-sms.os.agent.abw⟩] | ⟨Avast-Mobile, ∅⟩ ∩ ⟨Avira, ∅⟩ ∩ ⟨Microsoft, program:os/multiverze⟩ |
| [⟨McAfee, !b015f717e76b⟩, ⟨Avast-Mobile, :revo-op⟩, ⟨Microsoft, :win32/occamy.c88⟩] | ⟨ESET-NOD32, a variant of /.aev⟩ ∩ [⟨Kaspersky, heur:-dropper.os.agent.v⟩, ⟨Avira, /.ac.gen⟩] |
| [⟨McAfee, !b04f5a35d92c⟩, ⟨ESET-NOD32, a variant of /addisplay.revmob.a potentially unwanted⟩, ⟨Avira, /andr.revmob.a.gen⟩] | ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, program:os/multiverze⟩ |

[⟨McAfee,             ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, :win32/phonzy.a!ml⟩
!b389bbea204e⟩,
⟨ESET-NOD32, a
variant of
/fakeadblocker.a⟩,
⟨Kaspersky, not-a-
virus:heur:.os.fakeadblocker.a⟩,
⟨Avira,
/agent.srgm.gen⟩]

[⟨McAfee,             ⟨Avast-Mobile, ∅⟩ ∩ ⟨Avira, ∅⟩
!b8456ae6435a⟩,
⟨ESET-NOD32, a
variant of
/addisplay.dowgin.dq
potentially unwanted⟩,
⟨Kaspersky, heur:-
dropper.os.agent.nu⟩,
⟨Microsoft,
dos:os/multiverze⟩]

[⟨McAfee,             ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft,
!c601b36c59ee⟩,             :script/wacatac.b!ml⟩
⟨ESET-NOD32, a
variant of
generik.jnudyrh⟩,
⟨Avira,
/spyagent.fkgc.gen⟩]

[⟨McAfee,             ⟨Avira, ∅⟩
!cc37847a1e4b⟩,
⟨ESET-NOD32, a
variant of
/downloader.agent.fs⟩,
⟨Kaspersky, not-a-
virus:heur:.os.agent.n⟩,
⟨Avast-Mobile,
:agent-ovb⟩, ⟨Microsoft,
ransom:os/lockscreen!rfn⟩]

[⟨McAfee, !cee4b1fae8a4⟩, ⟨ESET-NOD32, a variant of /spy.agent.bom⟩, ⟨Kaspersky, heur:-banker.os.ubel.b⟩, ⟨Avira, /dropper.fkbp.gen⟩, ⟨Microsoft, spy:os/smsthief.l!mtb⟩]

⟨Avast-Mobile, :evo-gen⟩

[⟨McAfee, !d71c100730cf⟩, ⟨Avira, /dropper.shedun.ad.gen⟩]

⟨Avast-Mobile, :shedun-v⟩ ∩ [⟨ESET-NOD32, a variant of /dropper.shedun.v⟩, ⟨Kaspersky, heur:-dropper.os.wapnor.a⟩, ⟨Microsoft, dropper:os/shedun.a!mtb⟩]

[⟨McAfee, !dc62253c662d⟩, ⟨ESET-NOD32, a variant of /smsreg.oq potentially unsafe⟩, ⟨Kaspersky, heur:-sms.os.agent.ty⟩, ⟨Avast-Mobile, :agent-isv⟩, ⟨Avira, /smsagent.rb.gen⟩]

⟨Microsoft, :script/wacatac.b!ml⟩

[⟨McAfee, !e4d20eec9337⟩, ⟨ESET-NOD32, a variant of /addisplay.revmob.b potentially unwanted⟩, ⟨Avira, /andr.revmob.c.gen⟩]

⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, ∅⟩ ∩ ⟨Microsoft, :win32/bitrepeyp.b⟩

[⟨McAfee, !e98106d26174⟩, ⟨ESET-NOD32, a variant of /agent.sl⟩, ⟨Kaspersky, heur:-dropper.os.agent.bu⟩, ⟨Avast-Mobile, :dropper-pz⟩]

⟨Avira, ∅⟩ ∩ ⟨Microsoft, ∅⟩

[⟨McAfee, !f539f058e64d⟩, ⟨ESET-NOD32, a variant of /monitor.tifamily.q⟩, ⟨Kaspersky, not-a-virus:heur:monitor.os.monitorminor.l⟩, ⟨Avast-Mobile, apk:repmetagen⟩, ⟨Avira, /andr.agent.fkac.gen⟩]     ⟨Microsoft, ∅⟩

[⟨McAfee, !f5b9e3e836c8⟩, ⟨ESET-NOD32, a variant of /.dbm⟩, ⟨Avast-Mobile, :agent-sfm⟩, ⟨Microsoft, dropper:os/agent.b!mtb⟩]     ⟨Kaspersky, ∅⟩ ∩ ⟨Avira, ∅⟩

[⟨McAfee, !fe8c6500ef6e⟩, ⟨Avira, /agent.vca⟩]     ⟨ESET-NOD32, a variant of /downloader.agent.jn⟩ ∩ ⟨Kaspersky, heur:-downloader.os.agent.jy⟩ ∩ ⟨Avast-Mobile, :metasploit-q ⟩ ∩ ⟨Microsoft, hacktool:os/mesploit.a⟩

[⟨McAfee, adwind-fdwb.jar!be68bbb422d0⟩, ⟨Avira, /.fgxw.gen⟩, ⟨Microsoft, :os/vigorf.a⟩]     ⟨ESET-NOD32, a variant of /.fnn⟩ ∩ ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩

[⟨ESET-NOD32, /smsreg.ua potentially unsafe⟩, ⟨Avira, /smsreg.ybd.gen⟩]     ⟨Avast-Mobile, :evo-gen⟩

[⟨ESET-NOD32, a variant of /.evt⟩, ⟨Avira, /dropper.fimo.gen⟩]     ⟨Kaspersky, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ ⟨Microsoft, :script/wacatac.b!ml⟩

[⟨ESET-NOD32, a variant of /.izk⟩, ⟨Avira, /banker.fkcg.gen⟩]     ⟨McAfee, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩

37

[⟨ESET-NOD32, a variant of /spy.agent.bmp⟩, ⟨Kaspersky, heur:-banker.os.bray.j⟩, ⟨Avira, /spyagent.fjzb.gen⟩, ⟨Microsoft, spy:os/bray.a⟩]   ⟨Avast-Mobile, :evo-gen⟩

[⟨ESET-NOD32, a variant of /spy.agent.btn⟩, ⟨Kaspersky, heur:-spy.os.agent.zq⟩, ⟨Avira, /spyagent.fkfl.gen⟩]   ⟨Avast-Mobile, :evo-gen⟩

[⟨ESET-NOD32, a variant of /spy.spymax.e⟩, ⟨Kaspersky, heur:-spy.os.spynote.ai⟩, ⟨Avast-Mobile, :spymax-ar spy⟩, ⟨Avira, /spymax.srkk.gen⟩, ⟨Microsoft, :os/spynote.h⟩]   ⟨McAfee, ∅⟩

[⟨Kaspersky, heur:-banker.os.fakecalls.k⟩, ⟨Microsoft, dropper:os/bankeragent.x⟩]   ⟨McAfee, ∅⟩ ∩ ⟨Avast-Mobile, :evo-gen⟩ ∩ [⟨ESET-NOD32, a variant of /.izk⟩, ⟨Avira, /banker.fkcg.gen⟩]