# **When Malware Changed Its Mind:** An Empirical Study of Variable Program Behaviors in the Real World

**Erin Avllazagaj[1],** Ziyun Zhu[2], Leyla Bilge[3], Davide Balzarotti[4], Tudor Dumitraş[1]

[1]University of Maryland, College Park

[2]Facebook

[3]NortonLifeLock Research Group

[4]EURECOM

# Malware Behavior Changes Across Environments

# Malware Behavior Changes Across Environments

- Missing libraries, different language settings, etc.[1]

[1] Lindorfer et al. "Detecting environment-sensitive malware." *RAID*, 2011.

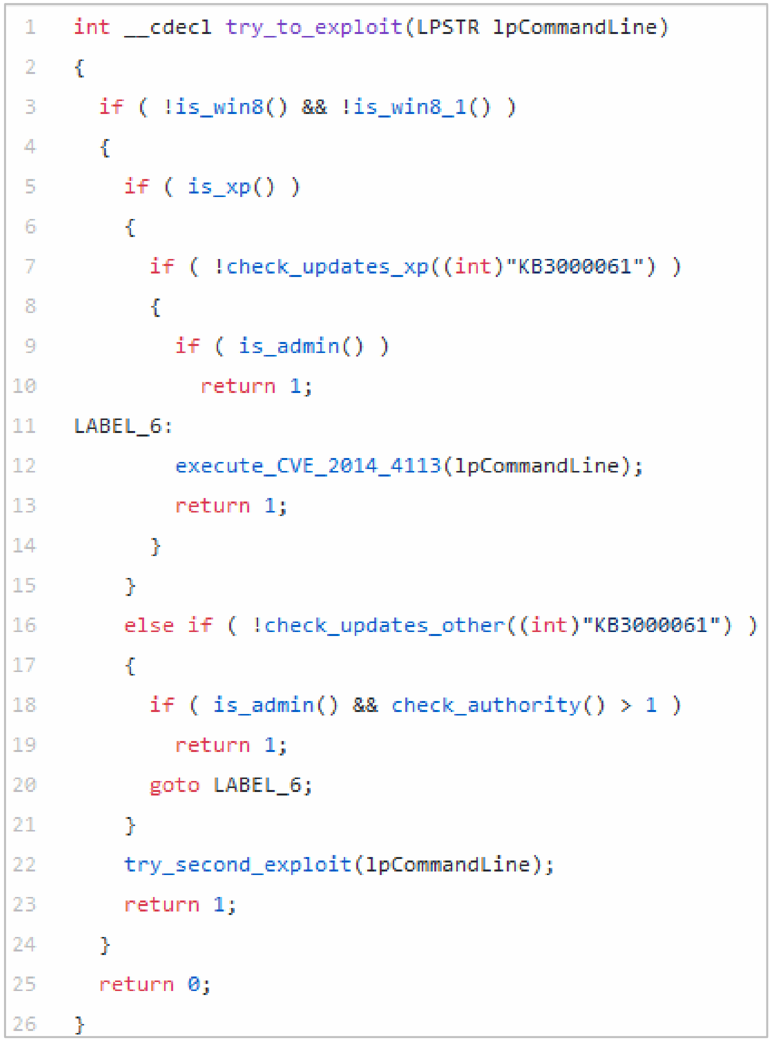
# Malware Behavior Changes Across Environments

- Missing libraries, different language settings, etc.[1]
- Prudent practices[2]:
  - "[…] caution generalizing from a single OS version […]"

[1] Lindorfer et al. "Detecting environment-sensitive malware." *RAID*, 2011.
[2] Rossow et al. "Prudent practices for designing malware experiments: Status quo and outlook." IEEE S&P, 2012.

# Malware Behavior Changes Across Environments

- Example: Ramnit Worm

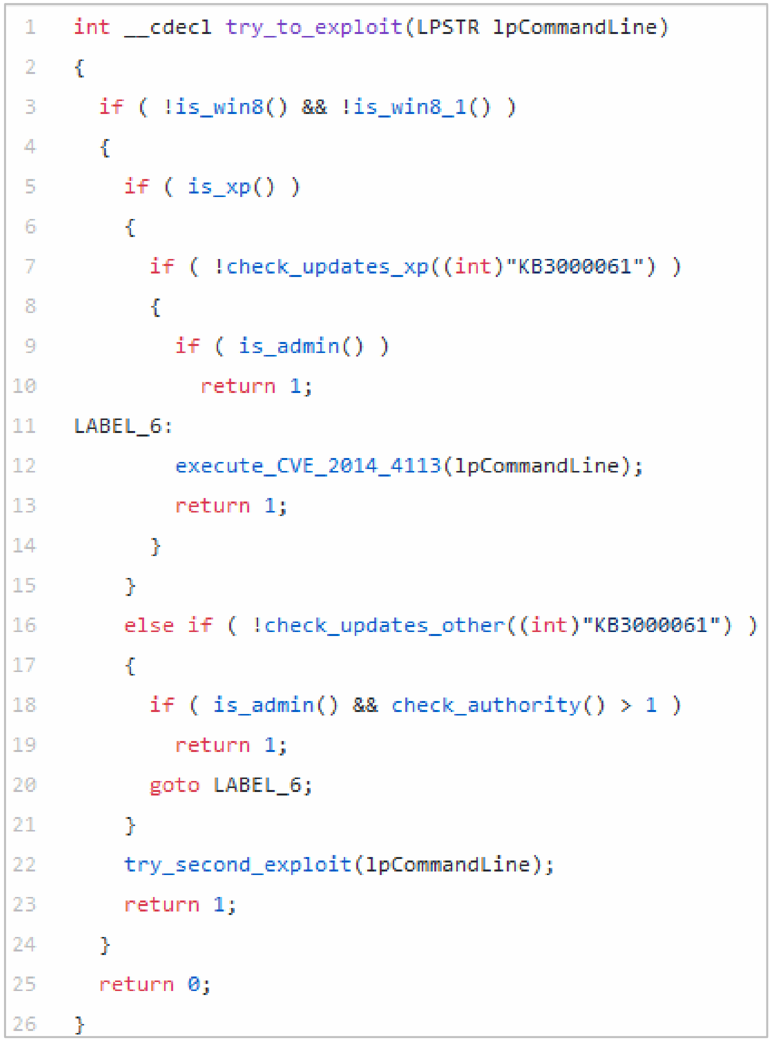


```
int __cdecl try_to_exploit(LPSTR lpCommandLine)
{
  if ( !is_win8() && !is_win8_1() )
  {
    if ( is_xp() )
    {
      if ( !check_updates_xp((int)"KB3000061") )
      {
        if ( is_admin() )
          return 1;
LABEL_6:
        execute_CVE_2014_4113(lpCommandLine);
        return 1;
      }
    }
    else if ( !check_updates_other((int)"KB3000061") )
    {
      if ( is_admin() && check_authority() > 1 )
        return 1;
      goto LABEL_6;
    }
    try_second_exploit(lpCommandLine);
    return 1;
  }
  return 0;
}
```

https://cert.pl/en/posts/2017/09/ramnit-in-depth-analysis/

# Malware Behavior Changes Across Environments

- Example: Ramnit Worm
  - Exploits CVE-2013-3660
    - Line 22
    - Local Privilege escalation on Win 7
    - Creates hundreds of **mutexes**
      - until exploit succeeds

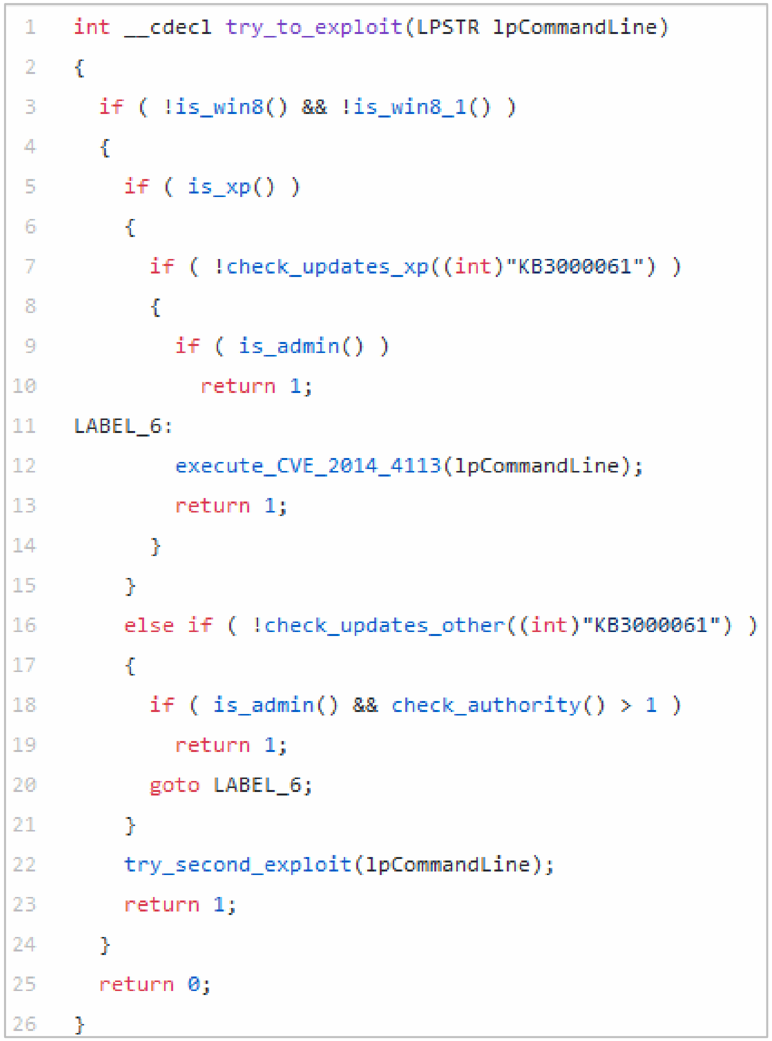


```
1  int __cdecl try_to_exploit(LPSTR lpCommandLine)
2  {
3    if ( !is_win8() && !is_win8_1() )
4    {
5      if ( is_xp() )
6      {
7        if ( !check_updates_xp((int)"KB3000061") )
8        {
9          if ( is_admin() )
10           return 1;
11 LABEL_6:
12         execute_CVE_2014_4113(lpCommandLine);
13         return 1;
14       }
15     }
16     else if ( !check_updates_other((int)"KB3000061") )
17     {
18       if ( is_admin() && check_authority() > 1 )
19         return 1;
20       goto LABEL_6;
21     }
22     try_second_exploit(lpCommandLine);
23     return 1;
24   }
25   return 0;
26 }
```

https://cert.pl/en/posts/2017/09/ramnit-in-depth-analysis/

# Malware Behavior Changes Across Environments

- Example: Ramnit Worm
  - Exploits CVE-2013-3660
    - Line 22
    - Local Privilege escalation on Win 7
    - Creates hundreds of **mutexes**
      - until exploit succeeds
  - Only works on:
    - vulnerable OS versions
    - when run in **non-admin**



```
 1  int __cdecl try_to_exploit(LPSTR lpCommandLine)
 2  {
 3    if ( !is_win8() && !is_win8_1() )
 4    {
 5      if ( is_xp() )
 6      {
 7        if ( !check_updates_xp((int)"KB3000061") )
 8        {
 9          if ( is_admin() )
10            return 1;
11  LABEL_6:
12          execute_CVE_2014_4113(lpCommandLine);
13          return 1;
14        }
15      }
16      else if ( !check_updates_other((int)"KB3000061") )
17      {
18        if ( is_admin() && check_authority() > 1 )
19          return 1;
20        goto LABEL_6;
21      }
22      try_second_exploit(lpCommandLine);
23      return 1;
24    }
25    return 0;
26  }
```

https://cert.pl/en/posts/2017/09/ramnit-in-depth-analysis/

# Research Questions

**RQ1:** Variability analysis in the wild

- What parts of the execution trace vary more? And by how much?

# Research Questions

**RQ1:** Variability analysis in the wild

- What parts of the execution trace vary more? And by how much?

**RQ2:** Invariant analysis in the wild

- Can we find behavioral invariants across executions?

# Research Questions

**RQ1:** Variability analysis in the wild

- What parts of the execution trace vary more? And by how much?

**RQ2:** Invariant analysis in the wild

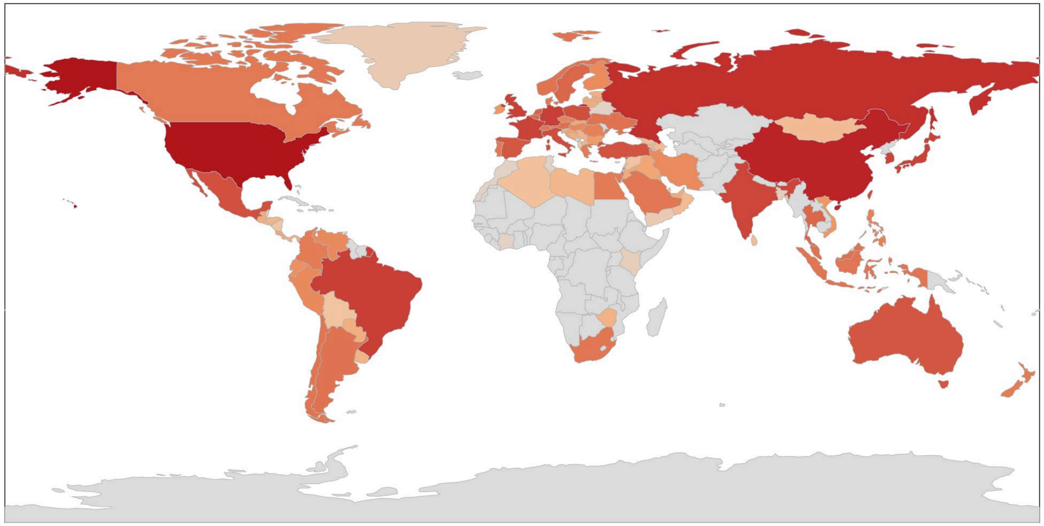
- Can we find behavioral invariants across executions?

**RQ3:** Impact of variability

- What is the impact of variability on malware detection and clustering?

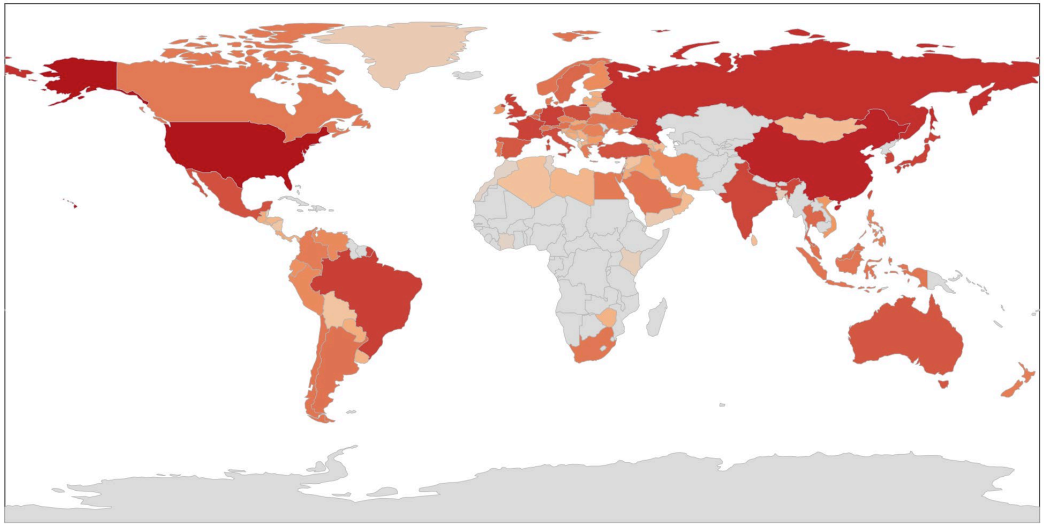
# The Dataset

- **7.6M** execution traces
- **5.4M** real users' machines in **>100 countries** in the world
- From **2018**



# The Dataset

- **7.6M** execution traces
- **5.4M** real users' machines in **>100 countries** in the world
- From **2018**
- No private data is collected, passive recording



# The Dataset (introduction)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach.id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| Mtx. Create | mtx!asjkf | - | … | ABC | 5243523 | abd |
| … | … | … | … | … | … | … |

# The Dataset (introduction)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach.id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| Mtx. Create | mtx!asjkf | - | … | ABC | 5243523 | abd |
| … | … | … | … | … | … | … |

(split by hash)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach.id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | … | … |

| Action type | File name | File path | … | sample Hash | Exec.id | Mach.id |
|---|---|---|---|---|---|---|
| Mtx. Create | mtx!asjkf | - | … | ABC | 5243523 | abd |
| … | … | … | … | ABC | … | … |

# The Dataset (introduction)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach.id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| Mtx. Create | mtx!asjkf | - | … | ABC | 5243523 | abd |
| … | … | … | … | … | … | … |

(split by hash)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach.id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | … | … |

| Action type | File name | File path | … | sample Hash | Exec.id | Mach.id |
|---|---|---|---|---|---|---|
| Mtx. Create | mtx!asjkf | - | … | ABC | 5243523 | abd |
| … | … | … | … | ABC | … | … |

Using VirusTotal labels and AVClass[1] (**2019**) we found:

**22K** benign, **2.4K** malware and **1.6K** PUP

[1] Sebastián et al. "Avclass: A tool for massive malware labeling." *RAID*, 2016.

# The Dataset (introduction)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach.id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| Mtx. Create | mtx!asjkf | - | … | ABC | 5243523 | abd |
| … | … | … | … | … | … | … |

(split by hash)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach.id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | … | … |

| Action type | File name | File path | … | sample Hash | Exec.id | Mach.id |
|---|---|---|---|---|---|---|
| Mtx. Create | mtx!asjkf | - | … | ABC | 5243523 | abd |
| … | … | … | … | ABC | … | … |

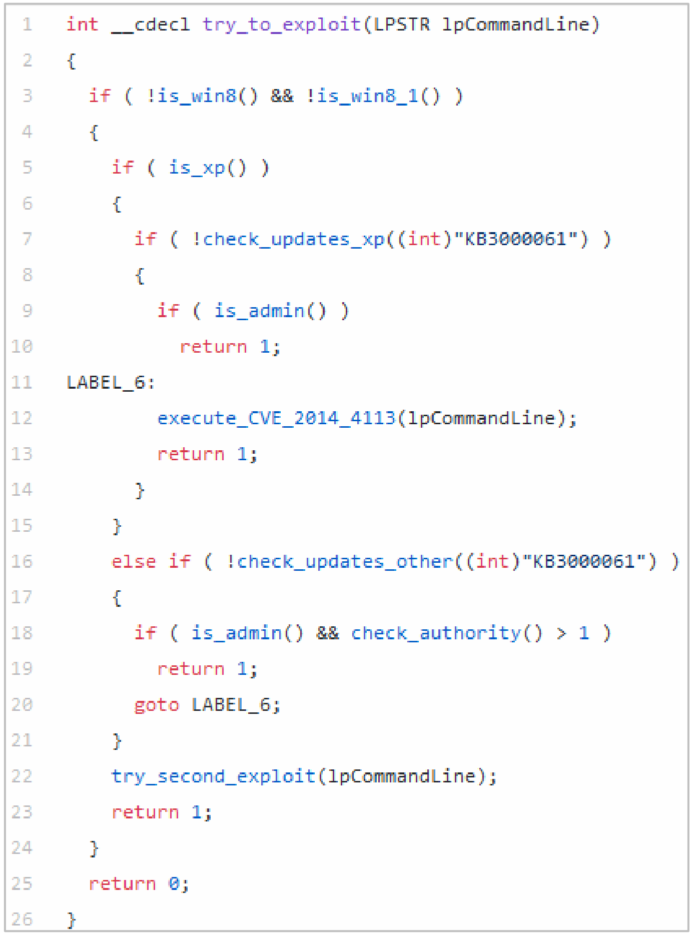
Using VirusTotal labels and AVClass[1] **(2019)** we found:

**22K** benign, **2.4K** malware and **1.6K** PUP

[1] Sebastián et al. "Avclass: A tool for massive malware labeling." *RAID*, 2016.

# RQ1: Variability Analysis In The Wild

- Ramnit worm exploit

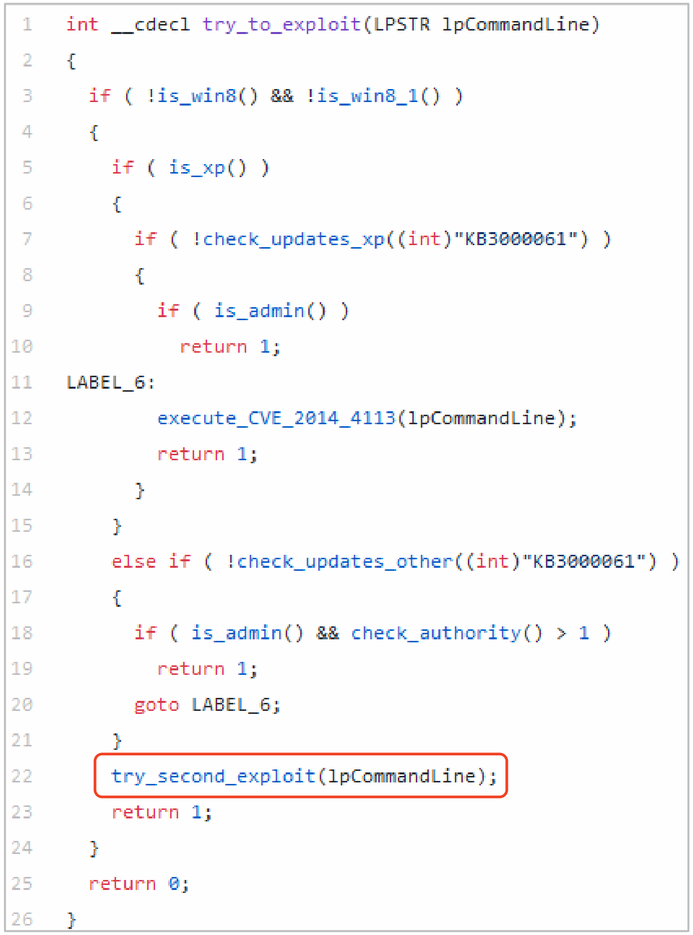


```
int __cdecl try_to_exploit(LPSTR lpCommandLine)
{
  if ( !is_win8() && !is_win8_1() )
  {
    if ( is_xp() )
    {
      if ( !check_updates_xp((int)"KB3000061") )
      {
        if ( is_admin() )
          return 1;
LABEL_6:
        execute_CVE_2014_4113(lpCommandLine);
        return 1;
      }
    }
    else if ( !check_updates_other((int)"KB3000061") )
    {
      if ( is_admin() && check_authority() > 1 )
        return 1;
      goto LABEL_6;
    }
    try_second_exploit(lpCommandLine);
    return 1;
  }
  return 0;
}
```

https://cert.pl/en/posts/2017/09/ramnit-in-depth-analysis/

# RQ1: Variability Analysis In The Wild

- Ramnit worm exploit
- When this line is reached
  - ~100 more mutex create events
  - based on the **machine**



```
int __cdecl try_to_exploit(LPSTR lpCommandLine)
{
  if ( !is_win8() && !is_win8_1() )
  {
    if ( is_xp() )
    {
      if ( !check_updates_xp((int)"KB3000061") )
      {
        if ( is_admin() )
          return 1;
LABEL_6:
        execute_CVE_2014_4113(lpCommandLine);
        return 1;
      }
    }
    else if ( !check_updates_other((int)"KB3000061") )
    {
      if ( is_admin() && check_authority() > 1 )
        return 1;
      goto LABEL_6;
    }
    try_second_exploit(lpCommandLine);
    return 1;
  }
  return 0;
}
```

https://cert.pl/en/posts/2017/09/ramnit-in-depth-analysis/

# RQ1: Variability Analysis In The Wild (machines)

Methodology

(for each hash)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | setup .exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | … | … |

# RQ1: Variability Analysis In The Wild (machines)

Methodology

(for each hash)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | … | … |

**(Group by machine ID and remove executions after week 0)**

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | 2 | abc |

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | 22222.exe | CSIDL_PROFILE | … | AAA | 4 | aaa |
| … | … | … | … | AAA | 3 | aaa |

# RQ1: Variability Analysis In The Wild (machines)

Methodology

(for each hash)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | setup .exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | … | … |

(Group by machine ID and remove executions after week 0)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | setup .exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | 2 | abc |

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | 22222.exe | CSIDL_PROFILE | … | AAA | 4 | aaa |
| … | … | … | … | AAA | 3 | aaa |

| | |
|---|---|
| File Creations: | 5 |
| Mutex Creations: | 2 |
| … | |
| **Total: 52** | |

| | |
|---|---|
| File Creations: | 5 |
| Mutex Creations: | 42 |
| … | |
| **Total: 92** | |

# RQ1: Variability Analysis In The Wild (machines)

Methodology

(for each hash)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | setup .exe | CSIDL_PR OFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | … | … |

(Group by machine ID and remove executions after week 0)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | setup .exe | CSIDL_PR OFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | 2 | abc |

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | 2222 2.exe | CSIDL_PR OFILE | … | AAA | 4 | aaa |
| … | … | … | … | AAA | 3 | aaa |

File Creations: 5
Mutex Creations: 2
…
**Total: 52**

File Creations: 5
Mutex Creations: 42
…
**Total: 92**

[ 45, … , 52 , … , 92 , … , 100 ] → IQR → 92 – 52 = **40**

# RQ1: Variability Analysis In The Wild (machines)

Methodology

(for each hash)

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | … | … |

**(Group by machine ID and remove executions after week 0)**

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | 2 | abc |

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | 22222.exe | CSIDL_PROFILE | … | AAA | 4 | aaa |
| … | … | … | … | AAA | 3 | aaa |

File Creations: 5
Mutex Creations: 2
…
**Total: 52**

File Creations: 5
Mutex Creations: 42
…
**Total: 92**

Analysis in the paper

[ 45, … , 52 , … , 92 , … , 100 ]

IQR → 92 – 52 = **40**

MARYLAND
CYBERSECURITY CENTER

# RQ1: Variability Analysis In The Wild (machines)

IQR → 92 – 52 = **40**

IQR → **10**

IQR → **0**

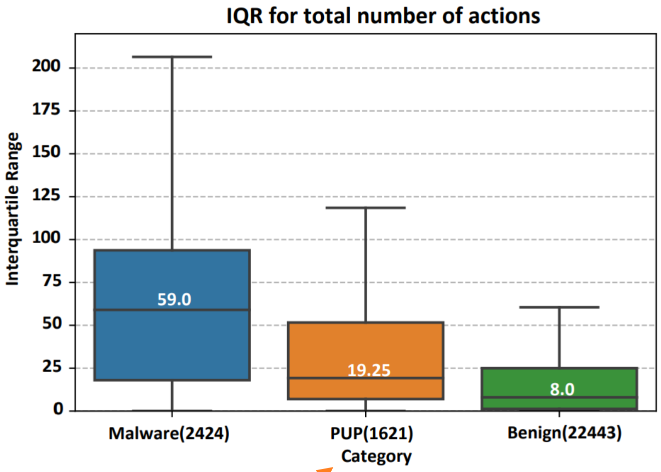
IQR → **100**

…

IQR → **60**

For all malware (blue boxplot)

For all PUP (orange boxplot)

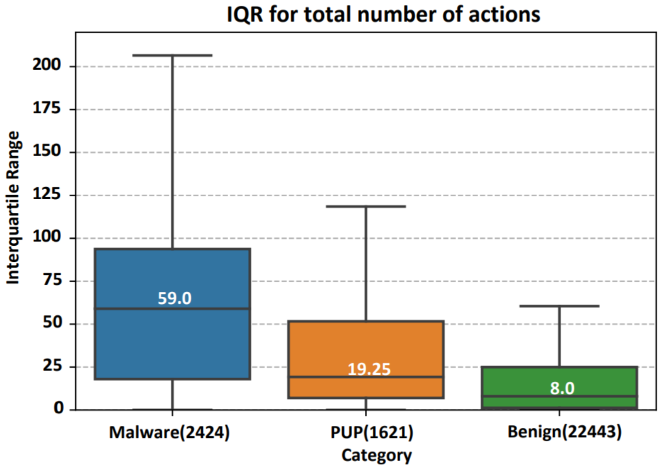


…

For all benigns (green boxplot)

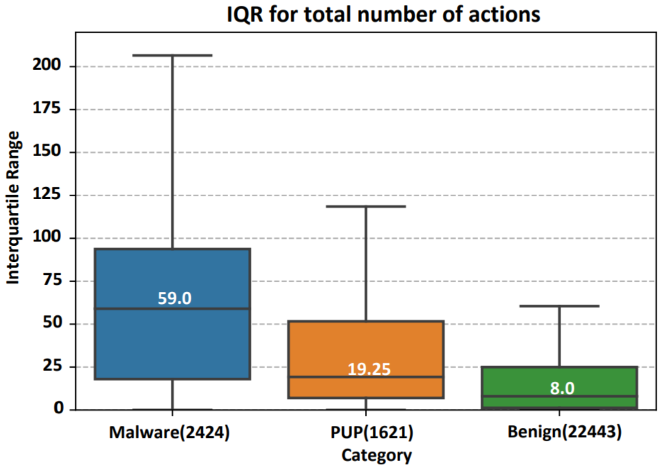
# RQ1: Variability Analysis In The Wild (machines)

- At least 50% of the malware:
  - **59** missing or additional actions

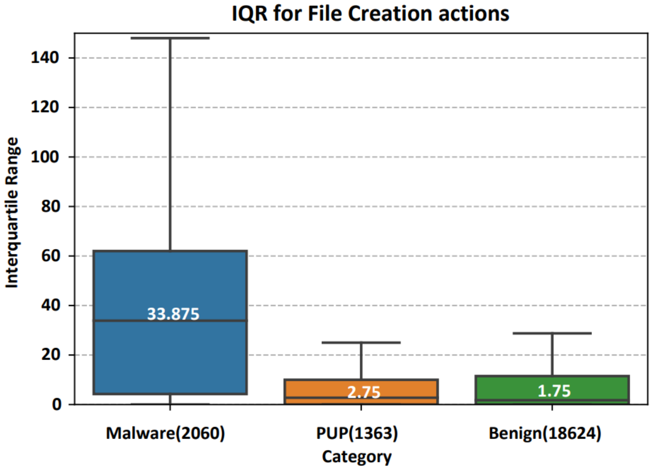


# RQ1: Variability Analysis In The Wild (machines)

- At least 50% of the malware:
  - 59 missing or additional actions



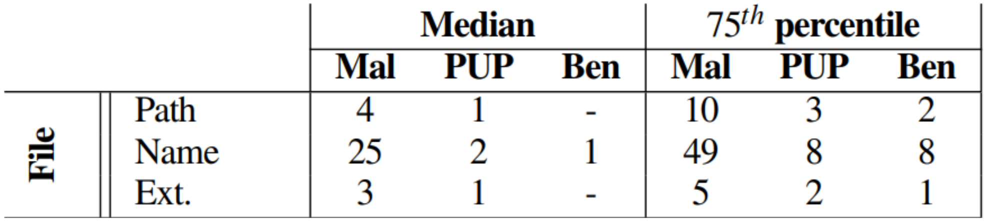
- File creation
  - The major source of machine-induced variability in malware.



# RQ1: Variability Analysis In The Wild (machines)

- Methodology:
  - IQR of the number of unique parameter values across different machines.

- Number of unique file names varies by **25** across machines



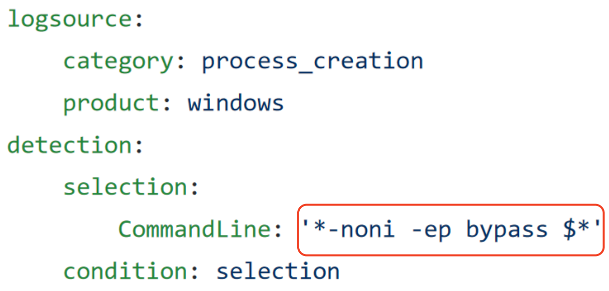
| | | Median | | | 75th percentile | | |
|---|---|---|---|---|---|---|---|
| | | **Mal** | **PUP** | **Ben** | **Mal** | **PUP** | **Ben** |
| **File** | Path | 4 | 1 | - | 10 | 3 | 2 |
| | Name | 25 | 2 | 1 | 49 | 8 | 8 |
| | Ext. | 3 | 1 | - | 5 | 2 | 1 |

# RQ1 Summary

- High variability in malware across machines
  - File Creation makes up most of variability in malware
  - File name is the most variable parameter

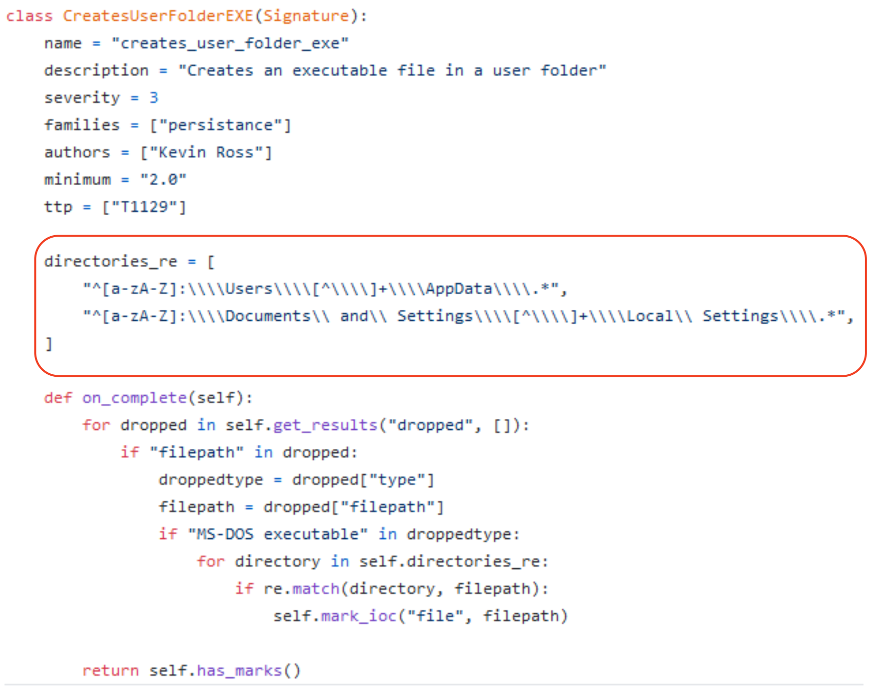
# RQ2: Invariant Analysis In The Wild

- Focus on action-parameter pair
  - used in Sigma
  - used in cuckoo



```
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine: '*-noni -ep bypass $*'
    condition: selection
```

https://github.com/SigmaHQ/sigma

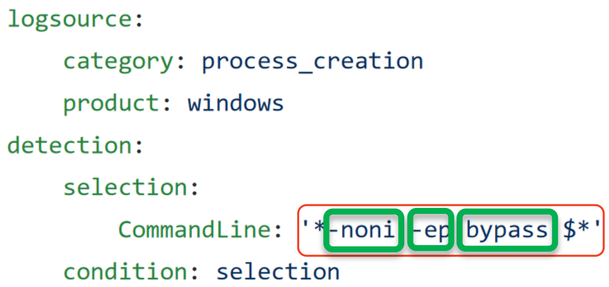


```
class CreatesUserFolderEXE(Signature):
    name = "creates_user_folder_exe"
    description = "Creates an executable file in a user folder"
    severity = 3
    families = ["persistance"]
    authors = ["Kevin Ross"]
    minimum = "2.0"
    ttp = ["T1129"]

    directories_re = [
        "^[a-zA-Z]:\\\\Users\\\\[^\\\\]+\\\\AppData\\\\.*",
        "^[a-zA-Z]:\\\\Documents\\ and\\ Settings\\\\[^\\\\]+\\\\Local\\ Settings\\\\.*",
    ]

    def on_complete(self):
        for dropped in self.get_results("dropped", []):
            if "filepath" in dropped:
                droppedtype = dropped["type"]
                filepath = dropped["filepath"]
                if "MS-DOS executable" in droppedtype:
                    for directory in self.directories_re:
                        if re.match(directory, filepath):
                            self.mark_ioc("file", filepath)

        return self.has_marks()
```

https://github.com/cuckoosandbox/community/tree/master/modules/signatures

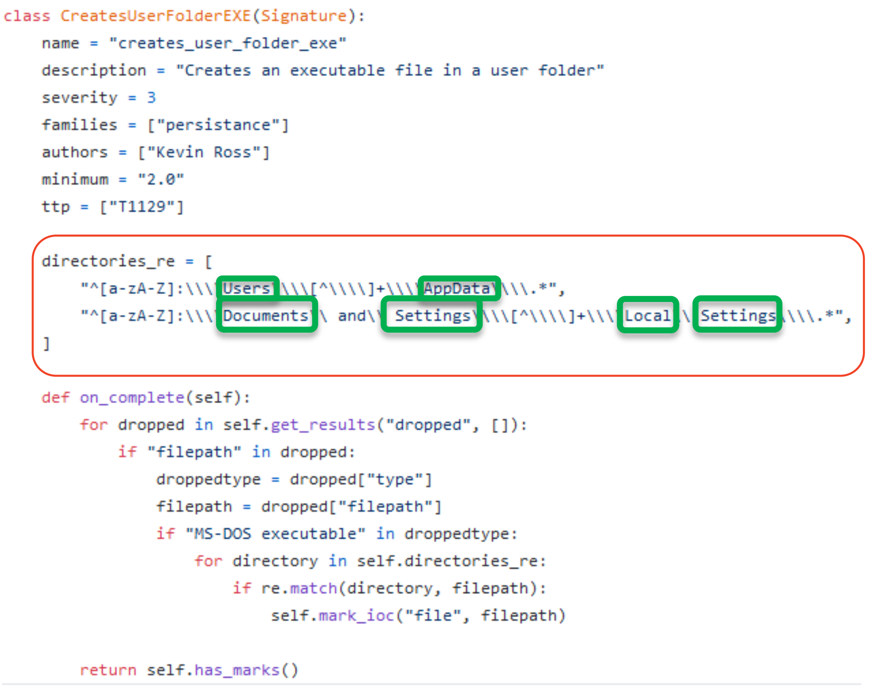
# RQ2: Invariant Analysis In The Wild

- Focus on action-parameter pair
  - used in Sigma
  - used in cuckoo



```
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine: '*-noni -ep bypass $*'
    condition: selection
```

https://github.com/SigmaHQ/sigma



```
class CreatesUserFolderEXE(Signature):
    name = "creates_user_folder_exe"
    description = "Creates an executable file in a user folder"
    severity = 3
    families = ["persistance"]
    authors = ["Kevin Ross"]
    minimum = "2.0"
    ttp = ["T1129"]

    directories_re = [
        "^[a-zA-Z]:\\\\Users\\\\[^\\\\]+\\\\AppData\\\\.*",
        "^[a-zA-Z]:\\\\Documents\\ and\\ Settings\\\\[^\\\\]+\\\\Local\\ Settings\\\\.*",
    ]

    def on_complete(self):
        for dropped in self.get_results("dropped", []):
            if "filepath" in dropped:
                droppedtype = dropped["type"]
                filepath = dropped["filepath"]
                if "MS-DOS executable" in droppedtype:
                    for directory in self.directories_re:
                        if re.match(directory, filepath):
                            self.mark_ioc("file", filepath)

        return self.has_marks()
```

https://github.com/cuckoosandbox/community/tree/master/modules/signatures

# RQ2: Invariant Analysis In The Wild

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| File Create | setup.exe | CSIDL_PROFILE | … | AAA | 1 | abc |
| … | … | … | … | AAA | … | … |

| Action type | File name | File path | … | sample Hash | Exec.id | Mach. id |
|---|---|---|---|---|---|---|
| Mtx. Create | mtx!asjkf | - | … | ABC | 5243523 | abd |
| … | … | … | … | ABC | … | … |

Extract parameter values

CSIDL_PROFILE
icon.png.wnry
setup.exe
cmd.exe|del|virus.exe

mtx!asjkf
CSIDL_PROFILE/folder1
runprogram.exe
icon.png
CSIDL_APPDATA/bin
config.ini
setup.exe

Split them by delimiter

CSIDL_PROFILE
icon
png
wnry
setup
exe
cmd
del
virus

mtx!asjkf
CSIDL_PROFILE
folder1
runprogram
exe
icon
png
CSIDL_APPDATA
bin
config
ini
setup
exe

# RQ2: Invariant Analysis In The Wild

CSIDL_PROFILE
icon
png
wnry
setup
exe
cmd
del
virus

mtx!asjkf
CSIDL_PROFILE
folder1
runprogram
exe
icon
png
CSIDL_APPDATA
bin
config
ini
setup
exe

(Remove values that appear in benign samples)

**wnry** → appears in 30/50 machines → **60%**
**virus** → appears in 10/50 machines → **20%**

appear in **65%** of the machines

# RQ2: Invariant Analysis In The Wild

- How to maximize coverage?
  - **Assumption:** Sandbox is undetectable.

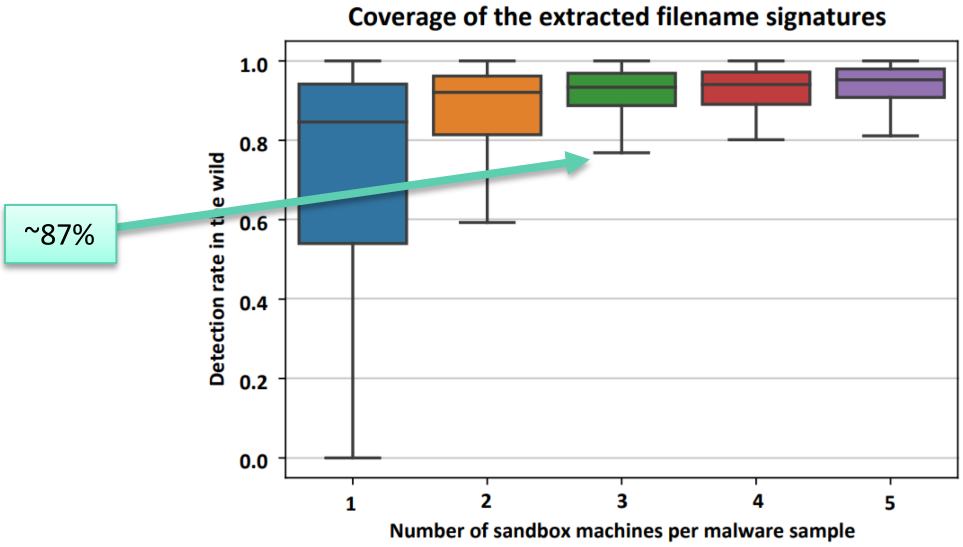
# RQ2: Invariant Analysis In The Wild

- How to maximize coverage?
  - **Assumption:** Sandbox is undetectable.

- Pick **n** machines to get the bag of tokens
  - Check how much coverage would we get on the other machines.

# RQ2: Invariant Analysis In The Wild

- How to maximize coverage?
  - Maximum coverage in 3 randomly generated machines
    - For file name tokens
  - One file name token doesn't appear in all machines.
    - Use more than 1 file name



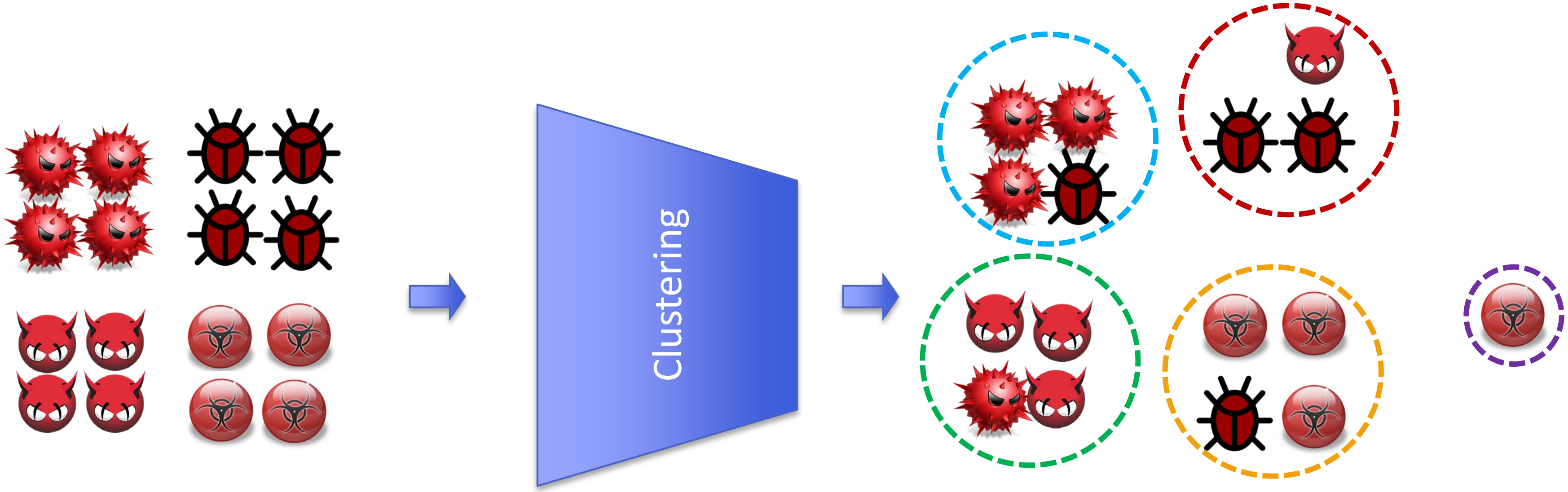
# RQ3: Impact Of Variability

- In terms of:
  - Clustering
  - Anomaly detection (AccessMiner[1])

[1] Lanzi, et al. "Accessminer: using system-centric models for malware protection." *CCS* 2010.

# RQ3: Impact Of Variability (clustering)

- Methodology:
  - Get 4 executions per malware sample in the same week
  - Reproduce the clustering by Bailey et al.[1]



[1] Bailey et al., Automated Classification and Analysis of Internet Malware, RAID 2007

# RQ3: Impact Of Variability (clustering)

- Results (out of **2424** malware samples):
  - 1,624 (67%) in the same cluster
  - 655 (27%) in 2 clusters
  - 121 (5%) in 3 clusters
  - 24 (1%) in 4 different cluster

# RQ3: Impact of variability (clustering)

- Results (out of **2424** malware samples):
  - 1,624 (67%) in the same cluster
  - 655 (27%) in 2 clusters
  - 121 (5%) in 3 clusters
  - 24 (1%) in 4 different cluster

clustering results with 1 trace per sample
may not correctly cluster malware into families

# Conclusions

# Conclusions

- First measurement of malware behavior at scale:
  - Single trace per malware sample is not enough

# Conclusions

- First measurement of malware behavior at scale:
  - Single trace per malware sample is not enough

- Variability in malware is greater than PUP and benign
  - Across both time and machines

# Conclusions

- First measurement of malware behavior at scale:
  - Single trace per malware sample is not enough
- Variability in malware is greater than PUP and benign
  - Across both time and machines
- It’s still feasible to find invariant in malware behavior
  - AV vendors can safely do it

# Thank you!

**Erin Avllazagaj**

albocode@umd.edu