MAIK MORGENSTERN / LENNART HOFFMANN

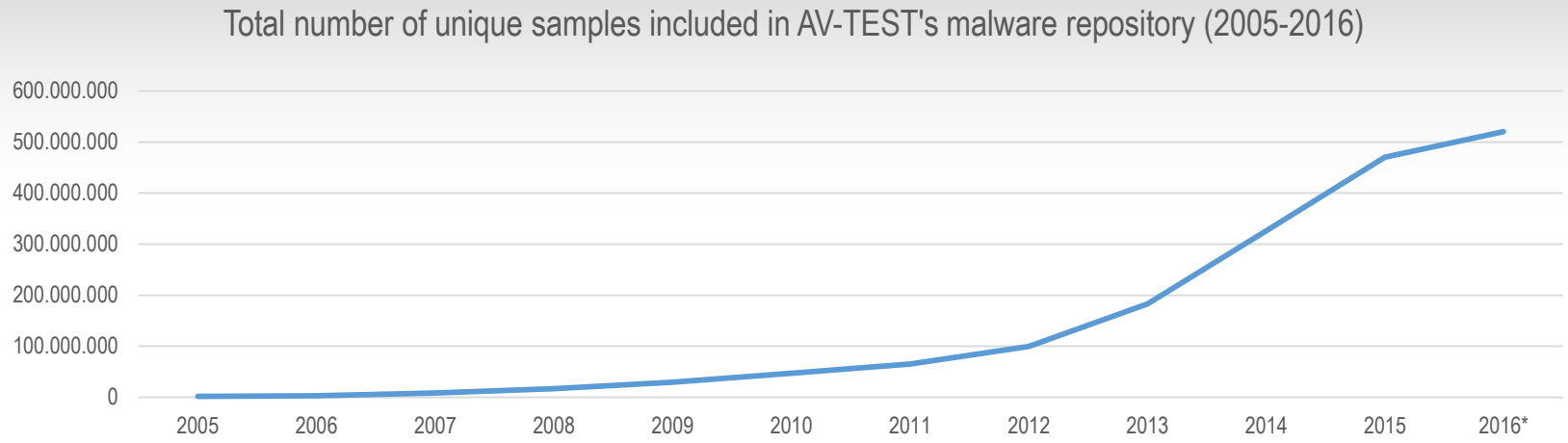
CARO Workshop 2016

INTERACTIVE GRAPHICAL EXPLORATION OF MALWARE BEHAVIOR

Agenda

- Motivation
- Technical Background
- Implementation
- Examples

Motivation



- AV-TEST received over **140 million** new malware samples in **2015**
- AV-TEST processed **hundreds of thousands** malware samples with its **dynamic analysis** in the last few months
- Are we still identifying the **new**, **interesting** and **important malware**?

Motivation


```
<file name="C:\Users\vtc\AppData\Local\Temp\nsr2122.tmp\LangDLL.dll" size="5632" md5="7e856702410e5598296a9c056c273db2" sha256="394d7d46b5e1ea621cfcc4f0bc8609d5ad8d42074186cddb
<file name="C:\Users\vtc\AppData\Local\Temp\nsr2122.tmp\AdvSplash.dll" shortname="C:\Users\vtc\AppData\Local\Temp\nsr2122.tmp\ADVSPL~1.DLL" size="6144" md5="555dc0088d360673e40
<file name="C:\Users\vtc\AppData\Local\Temp\nsr2122.tmp\Splash.dll" size="4096" md5="1b09e815aa989f5de0e0bd05d9a6dccd" sha256="dabb3fe93848b8289c3a01c7f3f58047334a2f94fdbedef05
<file name="C:\Users\vtc\AppData\Local\Temp\nsr2122.tmp\ioSpecial.ini" shortname="C:\Users\vtc\AppData\Local\Temp\nsr2122.tmp\IOSPEC~1.INI" size="729" md5="91cf7a34c67cb141915f
<file name="C:\Users\vtc\AppData\Local\Temp\nsr2122.tmp\Dialer.dll" size="3584" md5="9537200d7e7bcee10ff26ff487e2d753" sha256="d5a8f74b580158630e03bf379620022a1b354bdc41bfd375d
<file name="C:\Users\vtc\AppData\Local\Temp\nsr2122.tmp\BgImage.dll" size="7680" md5="254fdcec89b09610fcd6536ac8286087" sha256="fbfd18a279877766c0d4ab3249576f1aef6c65f10078853a
<file name="c:\download\viper.exe" flag="32" size="896838" md5="ca6e4676d4312c2972a58c5c053e2de4" sha256="2a7c70638055f4c59f66b7050434475762f9f1f9340f7f9199e86f0a118e5ce2" ref=
<value key="HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count" value="HRZR_PGYFRFFVBA" flag="96" type
<value key="HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\qbjaybnq" value="ivcre.rkr" flag="6"
<value key="HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\WmiApRpl\Performance" value="Last Counter" flag="96" type="REG_DWORD" data="8216" />
<value key="HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\WmiApRpl\Performance" value="Last Help" flag="96" type="REG_DWORD" data="8217" />
<value key="HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\WmiApRpl\Performance" value="First Counter" flag="96" type="REG_DWORD" data="8050" />
<value key="HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\WmiApRpl\Performance" value="First Help" flag="96" type="REG_DWORD" data="8051" />
<value key="HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\WmiApRpl\Performance" value="Object List" flag="96" type="REG_SZ" data="8050 8056 8066 8076 8096 8140 8150 8188 819
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\PROVIDERS\Performance" value="Performance Refreshed" flag="96" type="REG_DWORD" data="1" />
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wbem\PROVIDERS\Performance" value="Performance Data" flag="96" type="REG_BINARY" data="KBsAAAEAAAAAAAAAAEAAAABgbAAAAJAAAAmgAAAAE
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib" value="Last Help" flag="96" type="REG_DWORD" data="8217" />
<value key="HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib" value="Last Counter" flag="96" type="REG_DWORD" data="8216" />
<process id="1872" name="explorer.exe" parentid="1864" path="C:\\Windows\\explorer.exe" creationtime="2016-05-03T12:27:57.310" flag="8" cmdline="C:\\Windows\\Explorer.EXE">
    <modules>
        <module name="Explorer.EXE" path="C:\\Windows\\Explorer.EXE" />
        <module name="msi.dll" path="C:\\Windows\\SYSTEM32\\msi.dll" />
        <module name="msiltcfg.dll" path="C:\\Windows\\SYSTEM32\\msiltcfg.dll" />
        <module name="gameux.dll" path="C:\\Windows\\System32\\gameux.dll" flag="4" />
        <module name="tiptsf.dll" path="C:\\Program Files\\Common Files\\microsoft shared\\ink\\tiptsf.dll" />
        <module name="MsftEdit.dll" path="C:\\Windows\\SYSTEM32\\MsftEdit.dll" />
        <module name="ieframe.dll" path="C:\\Windows\\System32\\ieframe.dll" />
        <module name="msxml6.dll" path="C:\\Windows\\System32\\msxml6.dll" />
        <module name="StructuredQuery.dll" path="C:\\Windows\\System32\\StructuredQuery.dll" />
        <module name="mssprxy.dll" path="C:\\Windows\\system32\\mssprxy.dll" />
        <module name="searchfolder.dll" path="C:\\Windows\\system32\\searchfolder.dll" />
        <module name="PhotoMetadataHandler.dll" path="C:\\Windows\\system32\\PhotoMetadataHandler.dll" />
        <module name="Windows.UI.Xaml.dll" path="C:\\Windows\\System32\\Windows.UI.Xaml.dll" />
        <module name="Windows.UI.dll" path="C:\\Windows\\System32\\Windows.UI.dll" />
        <module name="ondemandconnroutehelper.dll" path="C:\\Windows\\SYSTEM32\\ondemandconnroutehelper.dll" />
        <module name="srchadmin.dll" path="C:\\Windows\\System32\\srchadmin.dll" />
        <module name="SettingMonitor.dll" path="C:\\Windows\\system32\\SettingMonitor.dll" />
        <module name="elscore.dll" path="C:\\Windows\\system32\\elscore.dll" />
        <module name="WSSync.dll" path="C:\\Windows\\system32\\WSSync.dll" />
        <module name="WSShared.dll" path="C:\\Windows\\system32\\WSShared.dll" />
        <module name="WSClient.dll" path="C:\\Windows\\system32\\WSClient.dll" />
        <module name="wincorlib.DLL" path="C:\\Windows\\system32\\wincorlib.DLL" />
        <module name="Windows.UI.Search.dll" path="C:\\Windows\\system32\\Windows.UI.Search.dll" />
        <module name="cscobj.dll" path="C:\\Windows\\System32\\cscobj.dll" />
        <module name="SqmApi.dll" path="C:\\Program Files\\Windows Portable Devices\\SqmApi.dll" />
        <module name="PortableDeviceTypes.dll" path="C:\\Windows\\System32\\PortableDeviceTypes.dll" />
```


AV-TEST dynamic analysis tool

Motivation

2016-05-02 20:38:53,193	**VirtualProtectEx**	Protection: 0x00000040 ProcessHandle: 0xffffffff Address: 0x30001634 Size: 0x00000004	success	0x00000001
2016-05-02 20:38:53,193	**VirtualProtectEx**	Protection: 0x00000020 ProcessHandle: 0xffffffff Address: 0x30001634 Size: 0x00000004	success	0x00000001
2016-05-02 20:38:53,203	**LdrLoadDll**	Flags: 1244912 BaseAddress: 0x31240000 FileName: wwlib.dll	success	0x00000000
2016-05-02 20:38:53,203	**LdrGetProcedureAddress**	Ordinal: 0 FunctionName: FMain FunctionAddress: 0x31244562 ModuleHandle: 0x31240000	success	0x00000000
2016-05-02 20:38:53,203	**LdrGetProcedureAddress**	Ordinal: 0 FunctionName: wdCommandDispatch FunctionAddress: 0x31621275 ModuleHandle: 0x31240000	success	0x00000000
2016-05-02 20:38:53,203	**LdrGetProcedureAddress**	Ordinal: 0 FunctionName: wdGetApplicationObject FunctionAddress: 0x315c1c06 ModuleHandle: 0x31240000	success	0x00000000
2016-05-02 20:38:53,203	**RegOpenKeyExW**	Handle: 0x000000a0 Registry: 0x80000002 SubKey: Software\Microsoft\Windows\Current	success	0x00000000

Cuckoo Sandbox on malwr.com

Motivation

- **Raw Output** of **dynamic malware analysis** can be
  - Huge chunks of text
  - Not intuitive
  - Not nice to view
  - → **Not nice to work with as a human**
- Processing the data is only possible with automation, manual analysis is difficult und time consuming
- **Automated processing** performs a defined task
  - Does this very **well and fast,** e.g. classifying behavior as malicious or benign
  - → **Often doesn‘t find (interesting) anomalies**

Motivation

- Even **abstracted data** is **difficult** to process as human

2a7c70638055f4c59f66b7050434475762f9f1f9340f7f9199e86f0a118e5ce2

Features

Name	Ergebnis
createsExecutablesInNonstandardDirectories	true
createsFilesInNonstandardDirectories	true
createsTemporaryFiles	true
createsTemporaryFiles.1	true
createsTemporaryFiles.2	true
numberOfCreatedFiles	+ 20
numberOfCreatedValues	+ 1
numberOfDeletedProcesses	+ 5
numberOfExecutableFiles	+ 18
numberOfModifiedValues	+ 10
numberOfUsedToplevelDirectories	+ 1
ratioOfExecutables	RATIO 0.9
ratioOfNonstandardDirectories	RATIO 1
ratioOfSystemValues	RATIO 0.18181819
ratioOfTemporaryFiles	RATIO 1
ratioOfValues2Files	RATIO 0.3548387

5740dca78846706facb5160ccc671a7b0c3abfcd7a6e85748ae0f1aad036ac9e

Features

Name	Ergebnis
createsCopyOfInstaller	true
createsFilesInNonstandardDirectories	true
createsRegFileLink	true
createsTemporaryFiles	true
createsTemporaryFiles.1	true
createsTemporaryFiles.2	true
createsTemporaryFiles.3	true
deletesExecutedSample	true
loadsDllFromNonstandardDirectory	true
modifiesBrowserSettings	true
modifiesBrowserSettings.IE	true
modifiesExistingFiles	true
modifiesSystemSettings	true
modifiesSystemSettings.current_user	true
modifiesSystemSettings.current_user.4	true
numberOfCreatedFiles	+ 414
numberOfCreatedFinalFiles	+ 405
numberOfCreatedKeys	+ 6

Motivation

- Even **abstracted data** is **difficult** to process as human

2a7c70638055f4c59f66b7050434475762f9f1f9340f7f9199e86f0a118e5ce2

Features

Name	Ergebnis
createsExecutablesInNonstandardDirectories	true
createsFilesInNonstandardDirectories	true
createsTemporaryFiles	true
createsTemporaryFiles.1	true
createsTemporaryFiles.2	true
numberOfCreatedFiles	+ 20
numberOfCreatedValues	1
numberOfDeletedProcesses	5
numberOfExecutableFiles	+ 18
numberOfModifiedValues	+ 10
numberOfUsedToplevelDirectories	+ 1
ratioOfExecutables	RATIO 0.9
ratioOfNonstandardDirectories	RATIO 1
ratioOfSystemValues	RATIO 0.18181819
ratioOfTemporaryFiles	RATIO 1
ratioOfValues2Files	RATIO 0.3548387

5740dca78846706facb5160ccc671a7b0c3abfcd7a6e85748ae0f1aad036ac9e

Features

Name	Ergebnis
createsCopyOfInstaller	true
createsFilesInNonstandardDirectories	true
createsRegFileLink	true
createsTemporaryFiles	true
createsTemporaryFiles.1	true
createsTemporaryFiles.2	true
createsTemporaryFiles.3	true
delesExecutedSample	true
deleteFilesNonstandardDirectory	true
modifiesBrowserSettings	true
modifiesBrowserSettings.IE	true
modifiesExistingFiles	true
modifiesSystemSettings	true
modifiesSystemSettings.current_user	true
modifiesSystemSettings.current_user.4	true
numberOfCreatedFiles	+ 414
numberOfCreatedFinalFiles	+ 405
numberOfCreatedKeys	+ 6

Visualize it!

Technical Background - Sunshine

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

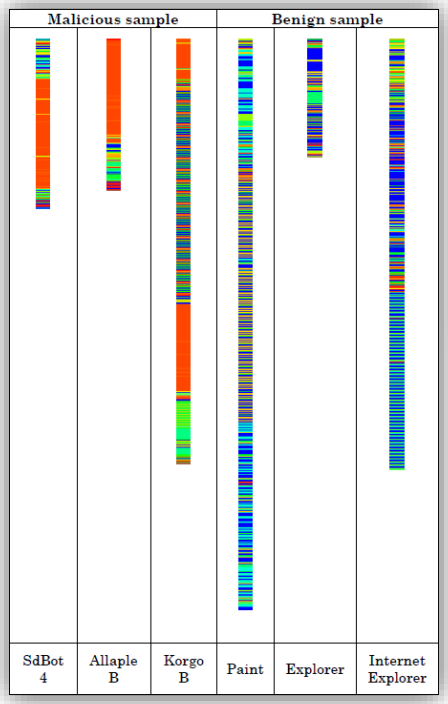
SUNSHINE
behavior control

- ~ 100 Machines
- **Dynamic Data Analysis**: controlled execution of malware samples on non-infected systems
- Can run on both virtual and physical hardware
- Monitors
  - Modifications of the **filesystem**
  - Modifications of the **registry**
  - **Processes** and their modules
  - System areas in the **memory**
  - Incoming and outgoing **network traffic**
- Assigns a **flag for every action**: CREATED, MODIFIED, DELETED, NOFLAG

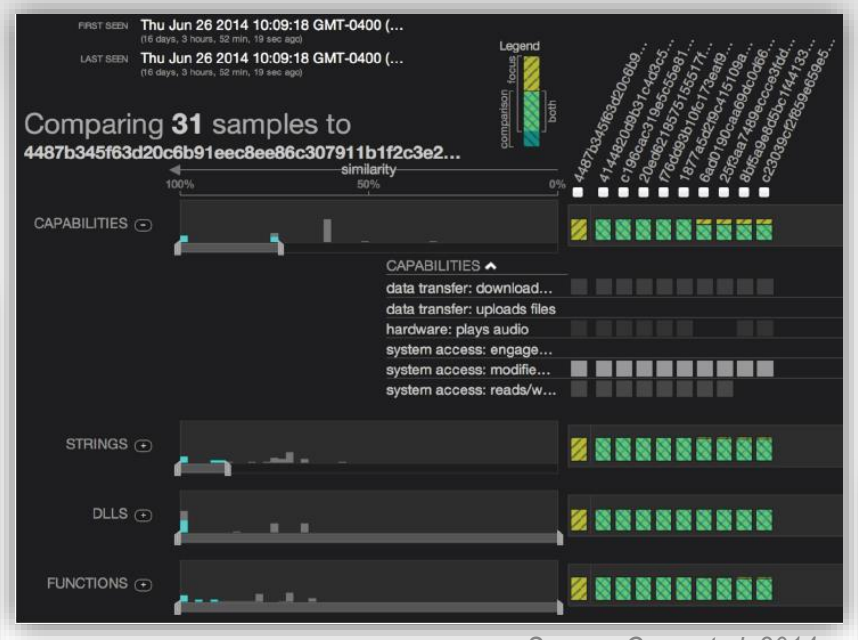
Data Analysis

- Behavior report is usually **huge**
- Features are extracted as a layer of abstraction and to reduce the data size
- We use three different types of features
  - **Boolean** features
  - **Aggregation** features
  - **Ratio** features
- Features can have sub-features
- These Features are combined into a **feature vector** describing the behavior of a sample
- Further usage of the feature vector: **classification**, …

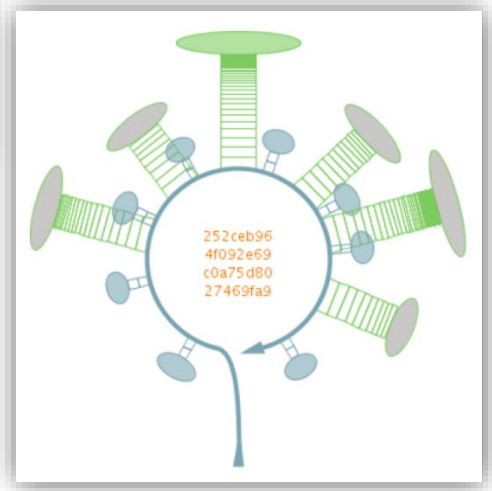
Visualization



Source: Shaid, Maarof 2014



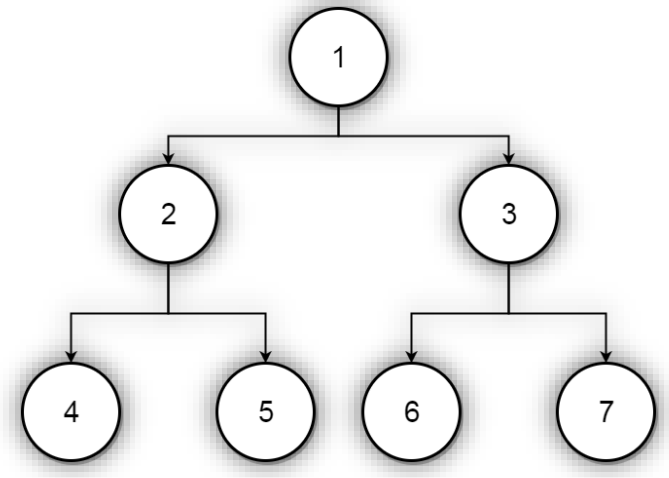
Source: Gove et al. 2014

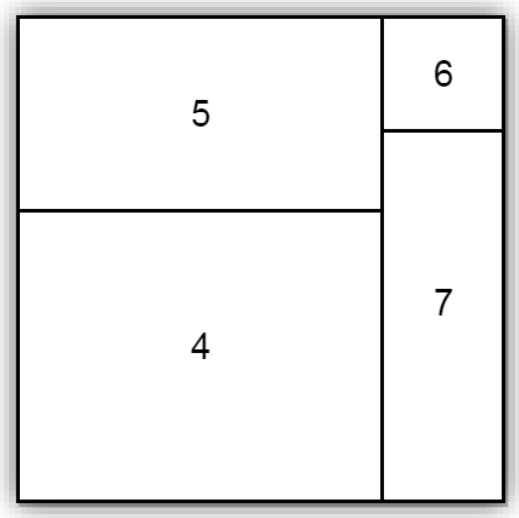


Source: Zhuo, Nadji 2012

Visualization

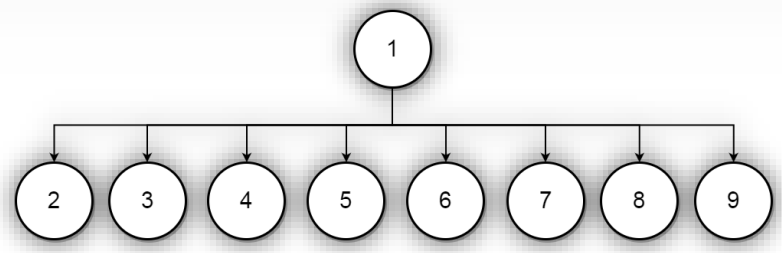
- Features can have sub-features → **hierarchical visualization**
- Selection of hierarchical visualization techniques is limited
- Options: **node-link** and **space-filling** Diagram (e.g. a Treemap)

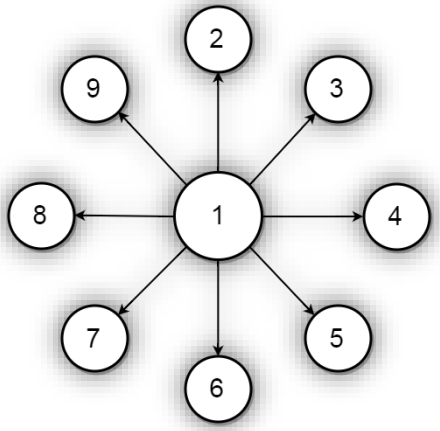




Visualization

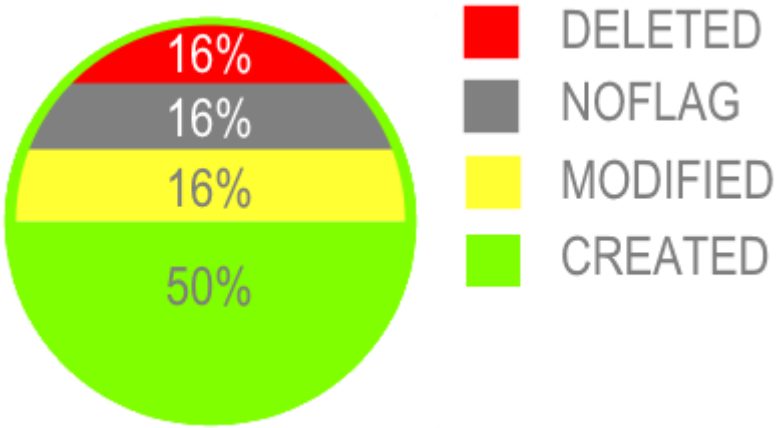
- **Treemaps** generally unfit since comparison between them is hard
  - Aggregation features usually dominate the Treemap, while Boolean features disappear
- Common **top-down tree visualizations** are also unsuitable because of the high number of nodes
- → **radial trees**





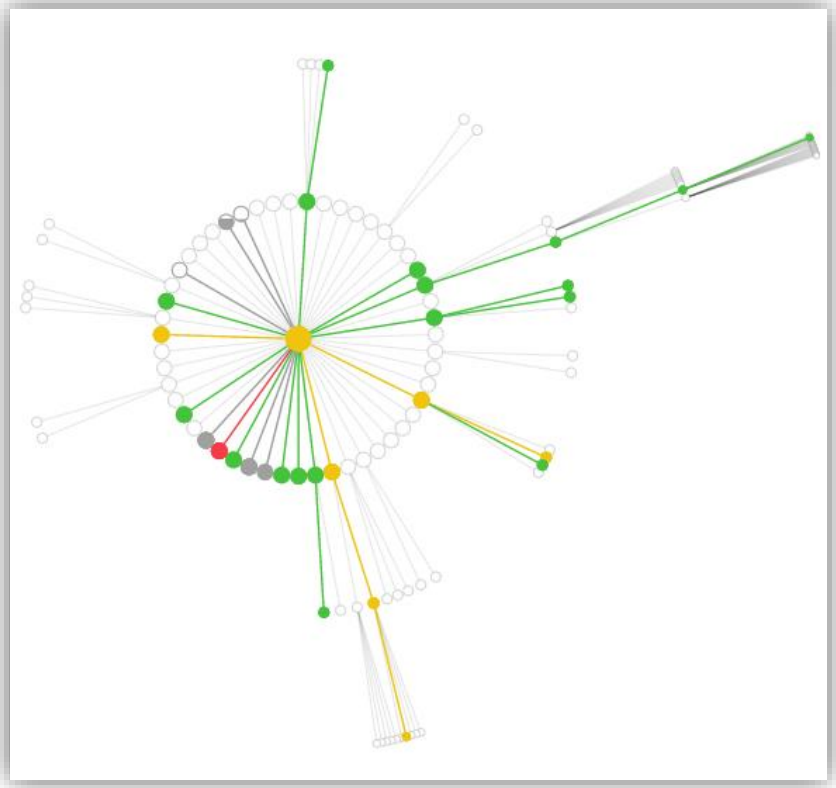
Visualization

- Differentiating between nodes might still be **difficult**
- To make it easier, triggered nodes (value > 0) are **highlighted** and **colored**
- The used colors depend on the distribution of the associated flags
- The filling level depends on the maximum value inside the data set



Visualization

- Edges are colored according to the **most frequently used flag** of the node the edge is pointing at
- Node size depends on its **level**
- → **Nodes further away from the root node are drawn tinier**



Implementation

- Frontend: Javascript (p5JS)
- Backend: Java (Spring Framework)
- 4 months of development
- ~8000 Lines of Code
- 40 files

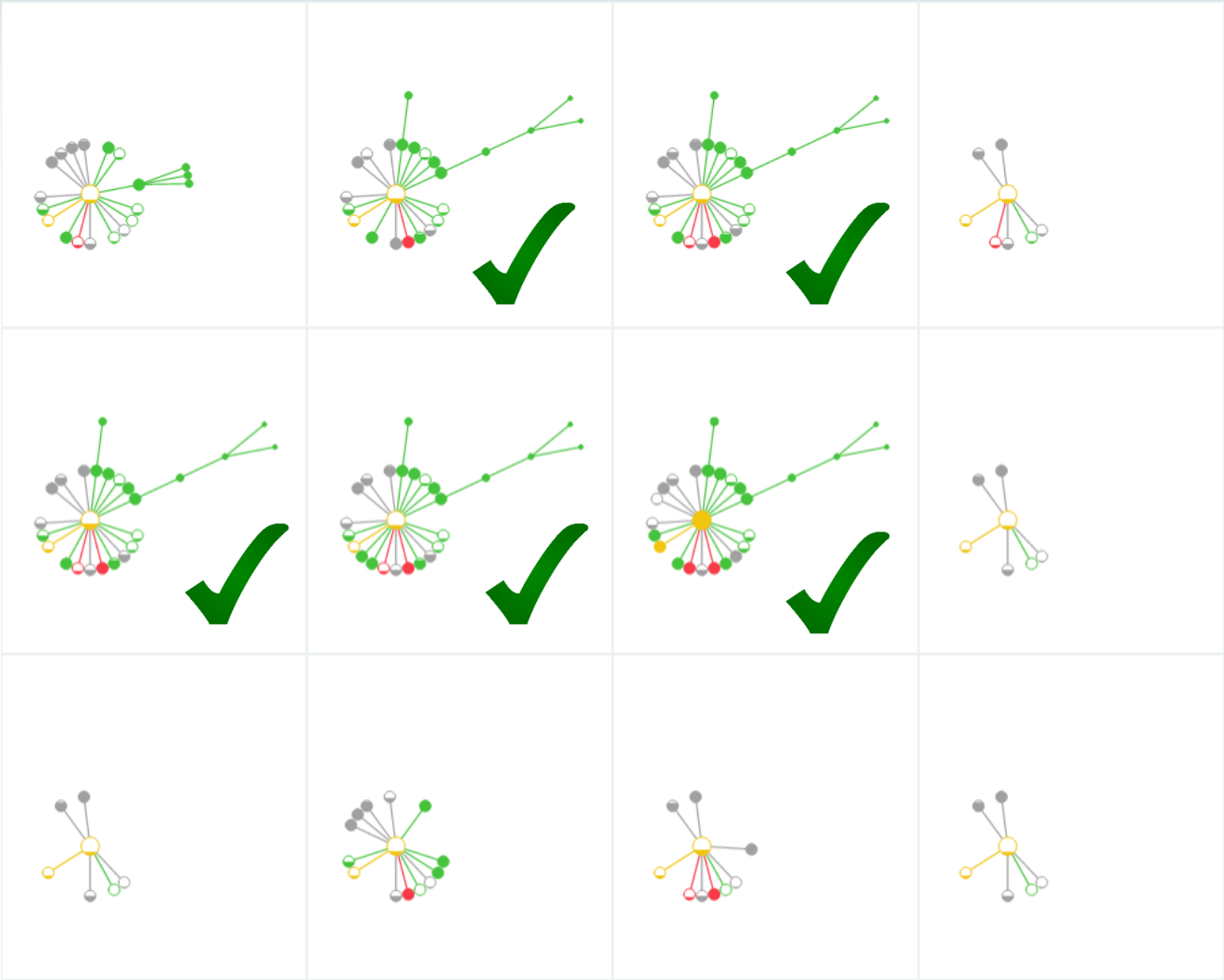
Examples

- Several **mail attachments** from April 27th, **same kind of mail**
- Varying static detection, varying dynamic classification

→ **Which file can be used for testing?**

*Incident Name	Sample Date	Sha256	Size	Sample notPe*		PEDumpHas	*VTes	VT Gro	*Mars	*Class.	
IMG4251067555-JPG.scr	16-04-27 10:03	ef525893b00a61	33219	view *	✖	43b09d20d7	22 %	MALW	●	GOODWARE	66,67 %
IMG7431582762-JPG.scr	16-04-27 09:29	d730910c0cf028	41472	view	✖	f6850a0a01	22 %	MALW	●	MALWARE	94,44 %
IMG5360612155-JPG.scr	16-04-27 08:25	290fb8dc150e68	41472	view	✖	400aa02061	26 %	MALW	●	MALWARE	99,89 %
IMG1208335660-JPG.scr	16-04-27 07:01	21953719db1fba	41472	view	✖	6ae664b70b	22 %	ANY	●	MALWARE	99,89 %
IMG9773906219-JPG.scr	16-04-27 06:48	52576443cb2c1b	41472	view	✖	6a314ce24d	17 %	ANY	●	MALWARE	94,44 %
IMG4593570354-JPG.scr	16-04-27 05:24	0ad208e694cbb7	41472	view	✖	75c6a029ac	17 %	ANY	●	MALWARE	99,89 %
IMG1308661721-JPG.scr	16-04-27 04:37	99dd9430b322a	41472	view	✖	9e2a1deb54	17 %	ANY	●	MALWARE	99,89 %
IMG0522787902-JPG.scr	16-04-27 04:14	008f6a4a4c7732	41472	view	✖	e78627d264	22 %	ANY	●	MALWARE	99,89 %
IMG9760798309-JPG.scr	16-04-27 03:56	fd5a60a4ac40a6	9879	view *	✖	0dd029e35e	9 %	ANY	●	MALWARE	100,00 %
IMG0949848712-JPG.scr	16-04-27 03:56	c0e2e4f1c9a209	3111	view *	✖	da3c973428	9 %	ANY	●	MALWARE	100,00 %
IMG2951539997-JPG.scr	16-04-27 02:58	c9badbe8d1a09	9803	view *	✖	0dd029e35e	9 %	ANY	●	GOODWARE	100,00 %
IMG8513652687-JPG.scr	16-04-27 02:53	397c0853e03b3f	43008	view	✖	15e91fdd91	48 %	MALW	●	MALWARE	94,44 %

Examples



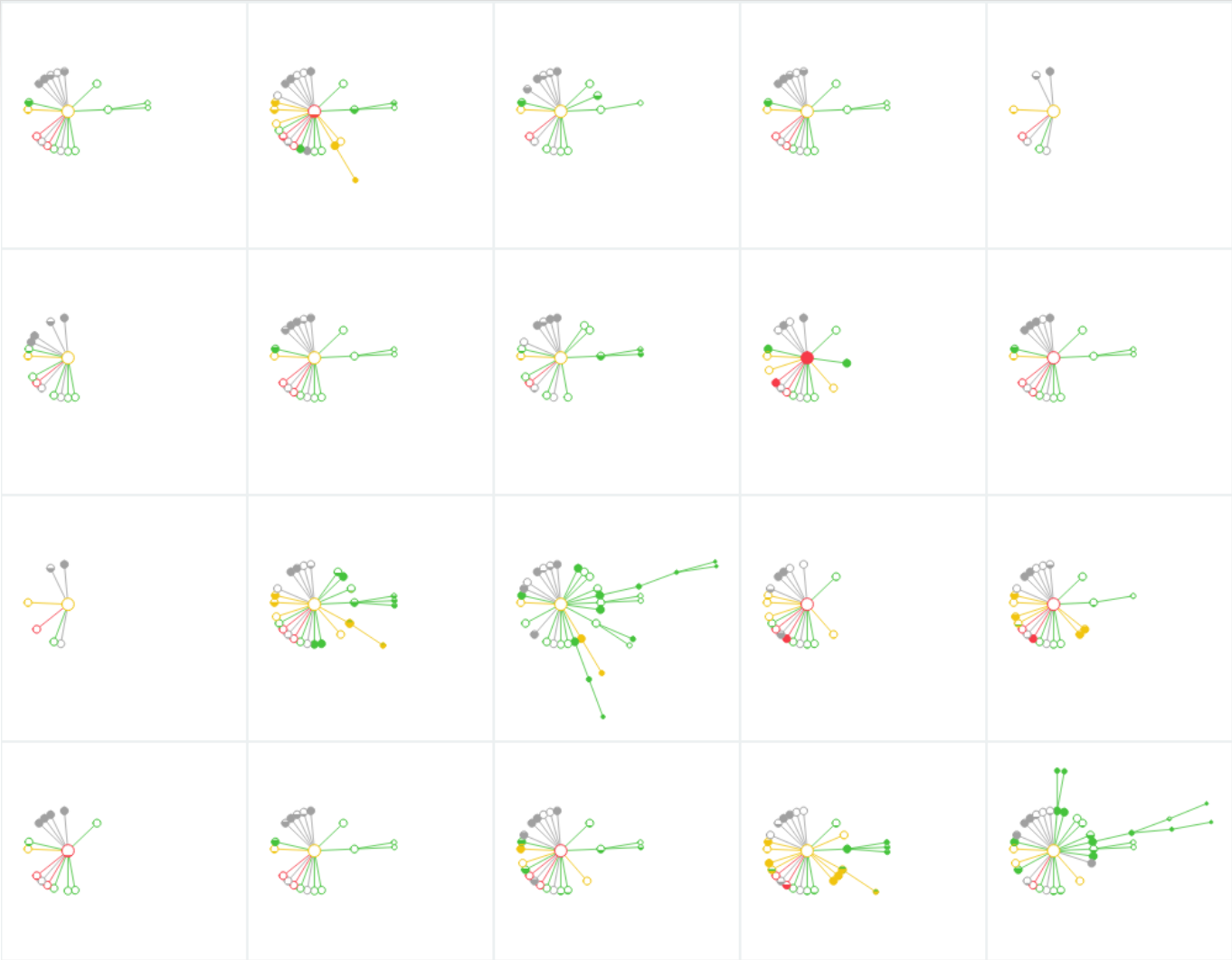
Examples

- Selecting a random set of 53 different dynamic analyses
- Anything interesting in there? Any clusters? Which behaviors are currently often used?

2 (2 of 4) 1 2 3 4 25

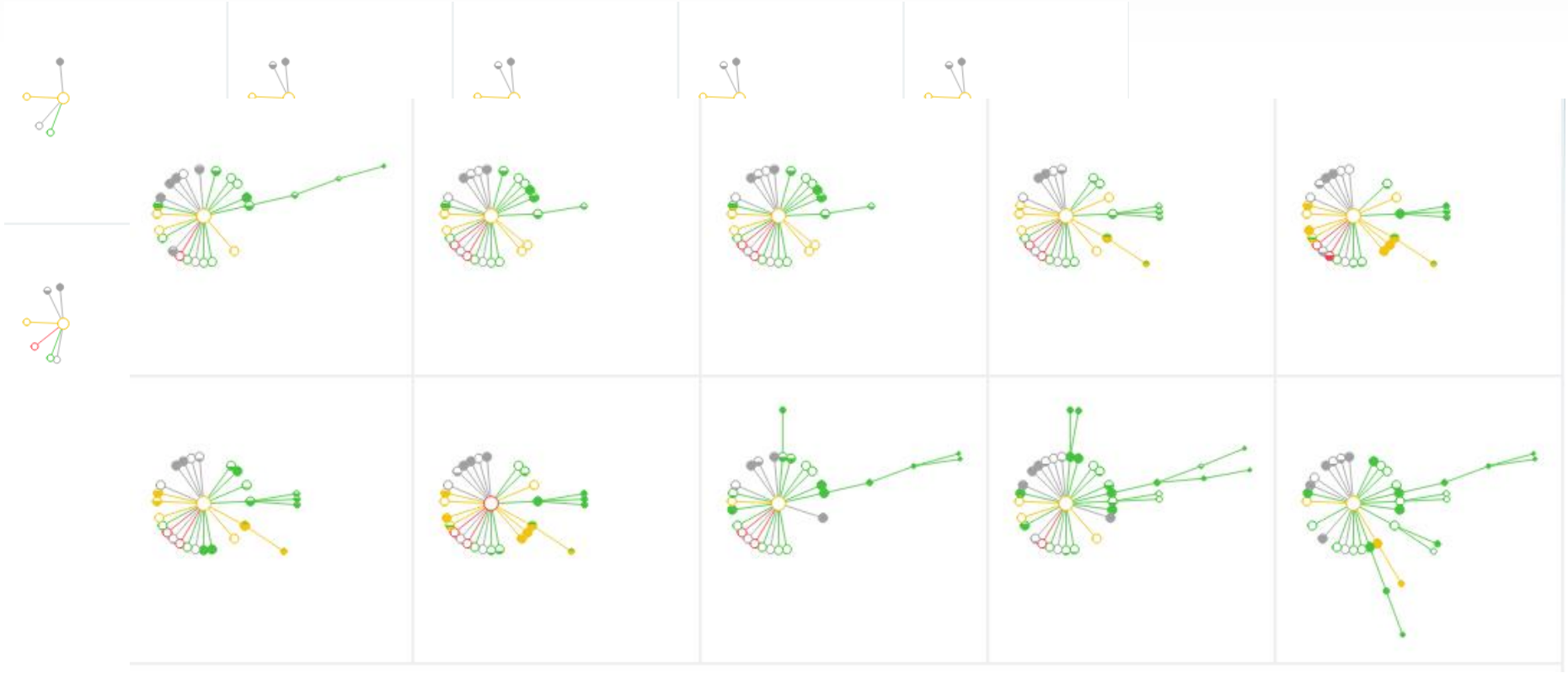
*Path URL	*Incident Name	Sample Date	Sha256	Size	Sample notPe*	PEDumpHash	*VTest	VT Group	*Mars	*Class.	*Conf.
http://down.ffplay.net/download/FFPlaySetup.exe	FFPlaySetup.exe	16-05-14 18:40	a3faa0841fbca30	1442189	view	3c1910a353bc7c	0 %	ANY		MALWARE	94,44 %
http://pekalongan.site/meii000040414.zip	meii000040414.zip	16-05-14 18:23	92c0a173fb4a04	20480	view	e7e3b7357a0b5	13 %	ANY		MALWARE	100,00 %
http://52kupan.com:81/d.php?file1456984582ZO38USR.e	2.28.exe.exe	16-05-14 18:20	cc8f3aa45a53cdt	32664	view *	65c1ecd8648ef7	13 %	ANY		MALWARE	100,00 %
http://www.applicationtourdownload.com/WVI6OTRQU1V	LibreOffice-21562-dp.exe	16-05-14 18:19	3f35bfc8f9a3259	980199	view	9e13db88aaf5c1	17 %	ANY		MALWARE	100,00 %
http://goodearthprogram.com/docs/c.exe	c.exe	16-05-14 18:03	d620e4d618969	256000	view	e690f5fb1f8e6c9	39 %	MALWARE		MALWARE	99,89 %
http://xiazai.51jetso.com/378/Setup_20009.exe	Setup_20009.exe	16-05-14 17:59	35d802f54ef2558	97484	view	843d6e8690d4e	26 %	PUA		MALWARE	100,00 %
http://falco3d.com/distributives/TorkvenSetup.exe	TorkvenSetup.exe	16-05-14 17:57	624d60fbb5d164	51641066	view	fc8f1378261f70d	9 %	ANY		MALWARE	100,00 %
http://www.exeupp.com/T27/Server.exe?download_token	Server.exe	16-05-14 17:57	94e55ca295213a	24064	view	3f0ab49b37c214	96 %	MALWARE		MALWARE	99,15 %
http://www.alltricks.co.in/5555553.exe	5555553.exe	16-05-14 17:57	62c5a72ce319ca	483840	view	746e96e11f2acd	39 %	MALWARE		MALWARE	100,00 %
http://isp.tupopop.com/?key=WJqbYJ547CMRTizYztXdav.	InstallMonster_Download_Manager.exe	16-05-14 17:56	05ae95d1338aaf	939300	view	b14df81604dd20	35 %	PUA		MALWARE	100,00 %
http://www.dkhoctf.com/m/challenge/992c8ae1cd0f776d7	992c8ae1cd0f776d790240d1fb69f5ee30c118af.exe	16-05-14 17:56	6cd9cacfa7173f1	17920	view	a21dc0d7b27e2f	17 %	MALWARE		MALWARE	100,00 %
http://all-baza.com/registro-cita.php	cita13-05.exe	16-05-14 17:26	298436dfd87fb14	28672	view	c200cbd5c77de2	13 %	ANY		MALWARE	99,15 %
http://down.dxias.com/?/kakaotalk-30355/bkill/kakaotalku	kakaotalkufffduffdufffdu0@84_kakaotalk-30355.exe	16-05-14 17:23	9f19caf76e5d645	68414	view	5adb310216bc6	35 %	MALWARE		MALWARE	100,00 %
http://www.egloodx.tech/info.php?id=1.1.5.26&monitor=1	m5hue.exe	16-05-14 17:06	a7e05a6028550	738816	view	87604b47fa6f3d	17 %	MALWARE		MALWARE	100,00 %
http://DOWN2.7R7Z.COM/setup_534pvgp.exe	setup_534pvgp.exe	16-05-14 17:05	09d37469178b1	203628	view	0d5b12d0721c9	17 %	PUA		MALWARE	94,44 %
http://site1371820587.tempsite.ws/FastComercio-Window	FastComercio-Windows-Instalador.exe	16-05-14 17:04	18e126f41deb63	43430168	view	aed5aa94ca592	4 %	ANY		MALWARE	94,44 %
http://snekam.lt/Stub.exe	Stub.exe	16-05-14 17:04	08131fb80fd754c	1340928	view	f7f043a94fe91f0	22 %	MALWARE		MALWARE	100,00 %
http://soft.31dns.net/soft/%E6%95%B0%E6%8D%AE%E	数据恢复.exe	16-05-14 17:00	672dd003b0fcecf	4913344	view	dfb46c6ec48c58	4 %	ANY		MALWARE	94,44 %

Examples



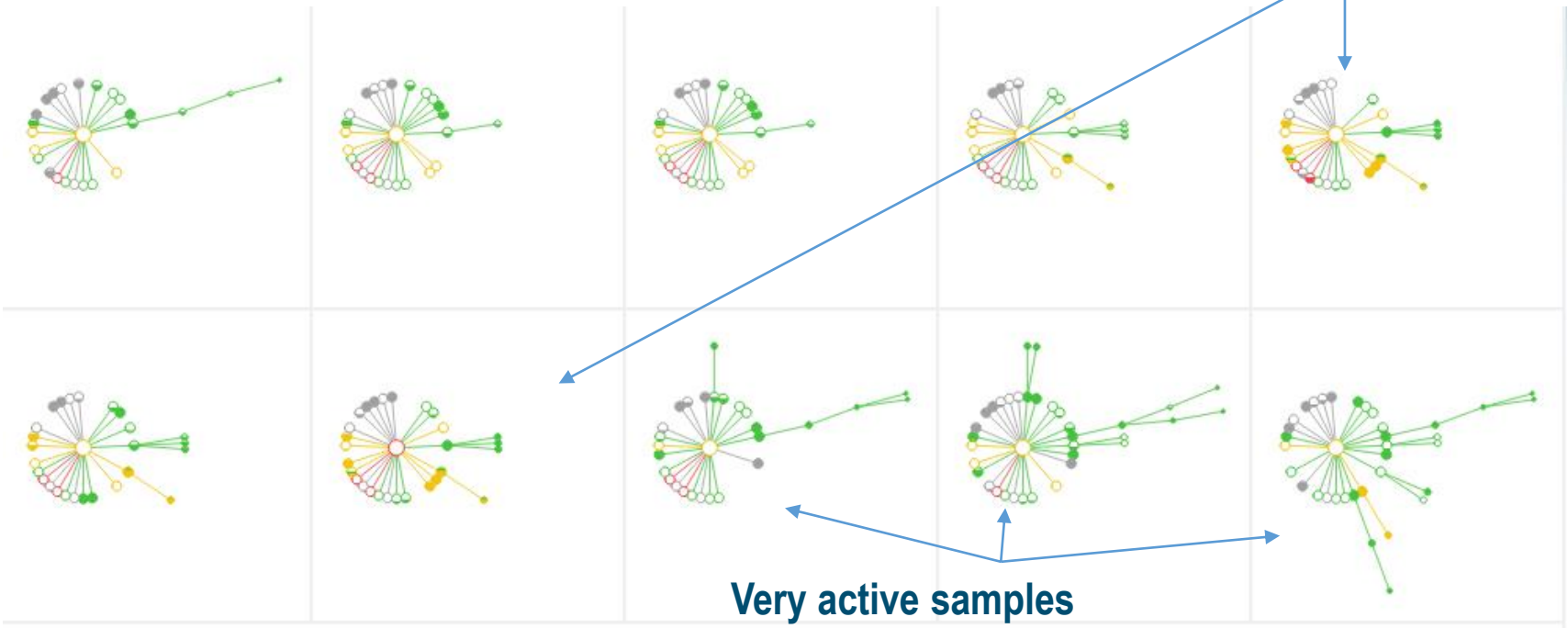
Examples

- Sort by activity from little to much



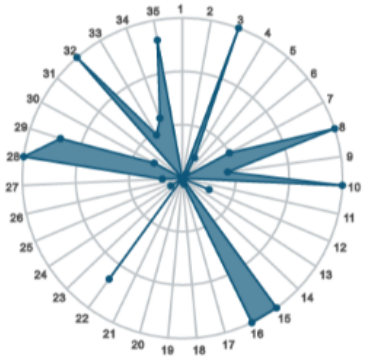
Examples

- Spotting interesting samples



Examples

- Closer look at one interesting sample



Summary

Hash (Sapas)

298436dfd87fb14cbd20b83b0a1c0ec4b4ce21be4aa4653d4790bbd7a9e77af5

VTest	Result
FileType	PE32 executable (GUI) Intel 80386, for MS Windows
detectionGroup	MALWARE
detectionName	GENERIC
detectionType	TROJ_DOWN

Feature-List

Feature	Wert
changesPolicies	0
___older_os_version_and_current_user	0
___older_os_version_and_local_machine	0
createsCopyOfInstaller	0
createsDebuggerEntry	1
createsExecutablesInNonstandardDirectories	4
createsFilesInNonstandardDirectories	5
createsNtfsAds	0
createsRegFileLink	2
createsRestartHook	2

Examples

- Looking for certain behaviors

Examples

- Malware vs. PUA vs. Goodware

Malware (Bjlog)

PUA (Bundler)

PUA (Bundler)

Malware (Locky)

PUA (Installcore)

Clean App

Clean App

PUA (?)

SUMMARY

- Fun to work with, but real use cases still rare
  - Sample verification works well
  - Illustrating PR material
  - Doing first research/investigation steps on interesting samples
- More extensions planned/possible
  - Include network traffic
  - Include static attributes
  - Certain use cases, e.g. displaying only malicious features to find Goodware or PUA that behaves suspicious
- Visualizing output of other dynamic analysis systems possible
  - Raw output →Feature Vector →Visualization

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

@avtestorg (English) & @avtestde (German)

Follow us on facebook.com/avtestorg

Current test results at https://www.av-test.org

Thank you for your attention!