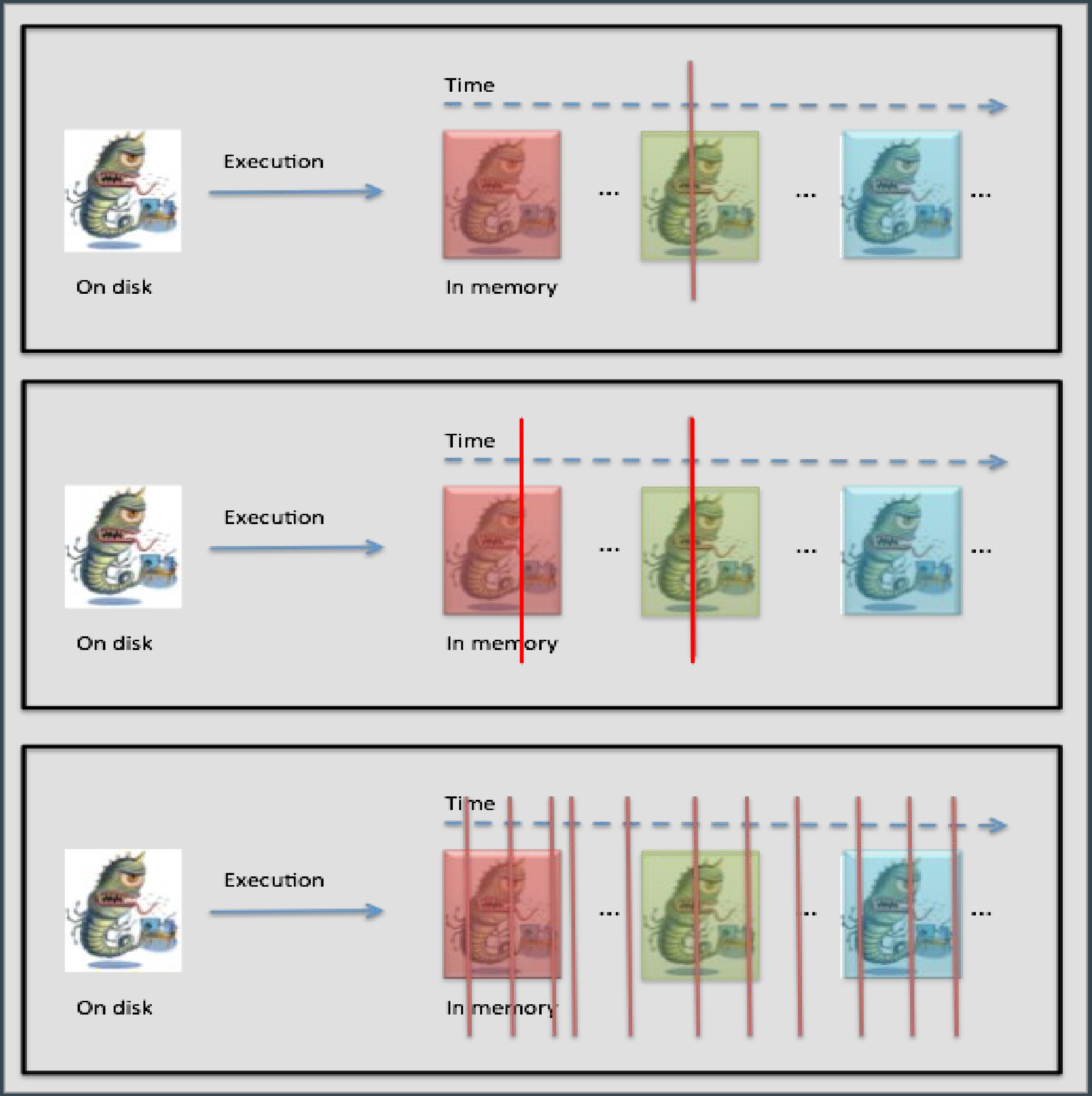
Memory Based Dynamic Malware Analysis

•••

Endre Bangerter, Jonas Wagner
Benjamin Urech, Patrick Schläpfer

Security Engineering Lab
Bern University of Applied Sciences

Memory forensics



Investigation

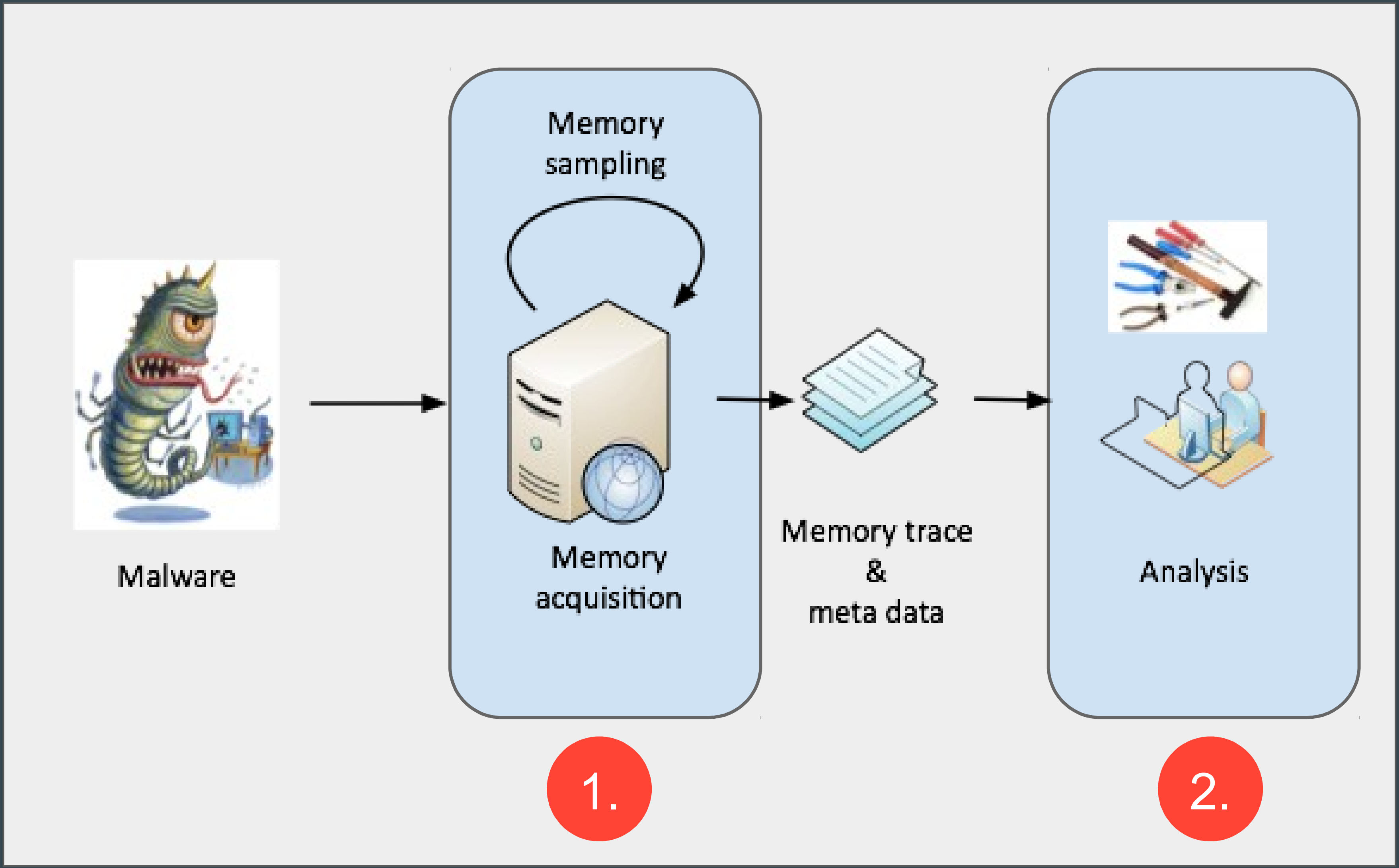
State Diffing

Memory tracing

Memory tracing

- Comprehensive capture of *full system behavior*, based on memory introspection
- May capture transient memory contents (i.e., short lived data & code)
- Hard to evade, reconstruction of system states from memory
- Novel techniques and algorithms to conduct dynamic malware analysis

System perspective



Memory acquisition

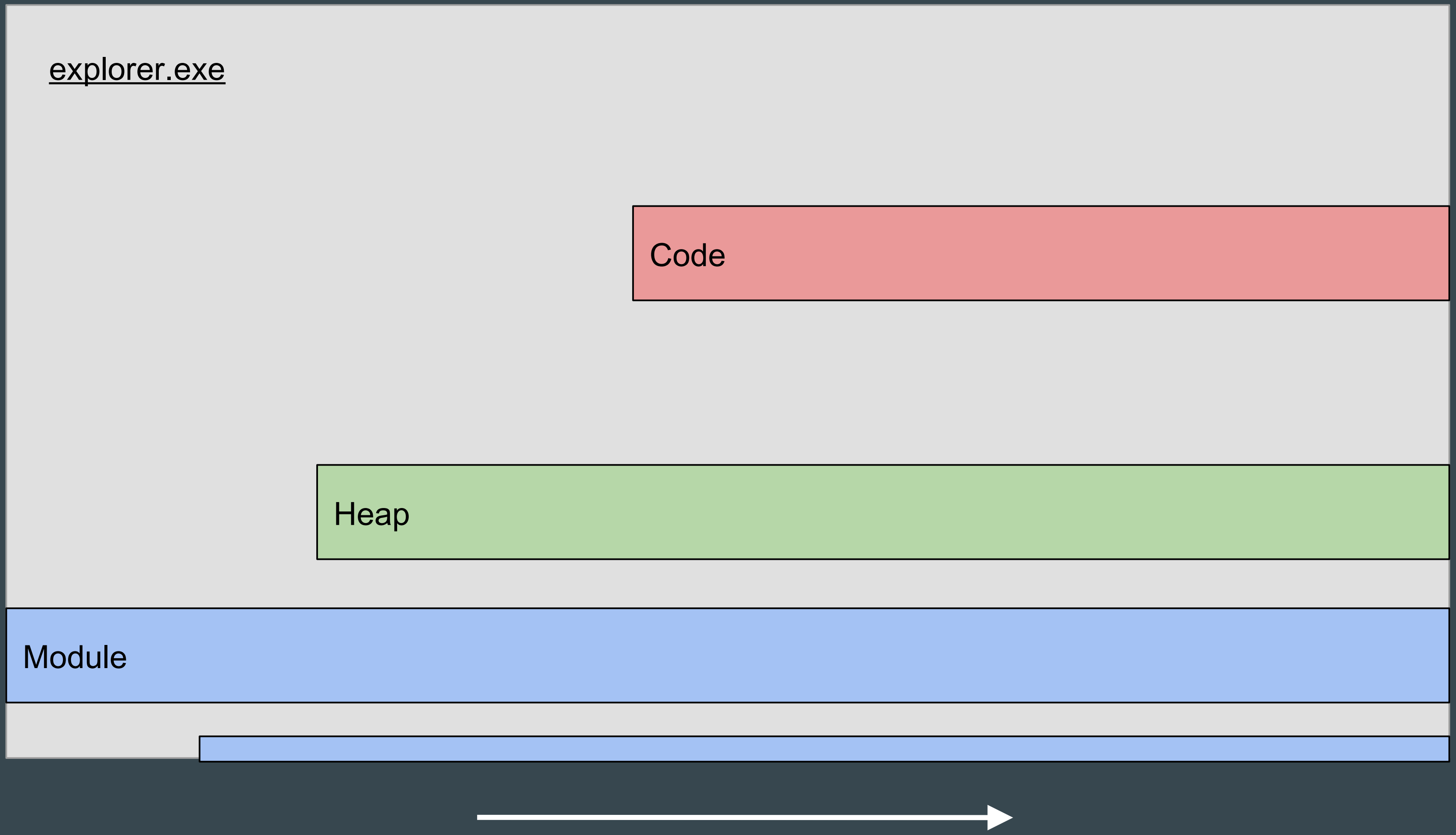
- Based on virtual machine introspection, e.g. hook KVM core functionalities
- Trigger a new snapshot on certain guest events, e.g. system calls
- Good performance, e.g. 100 snaps/sec while having an interactive VM
- Operating system independence and stealth

Analysis

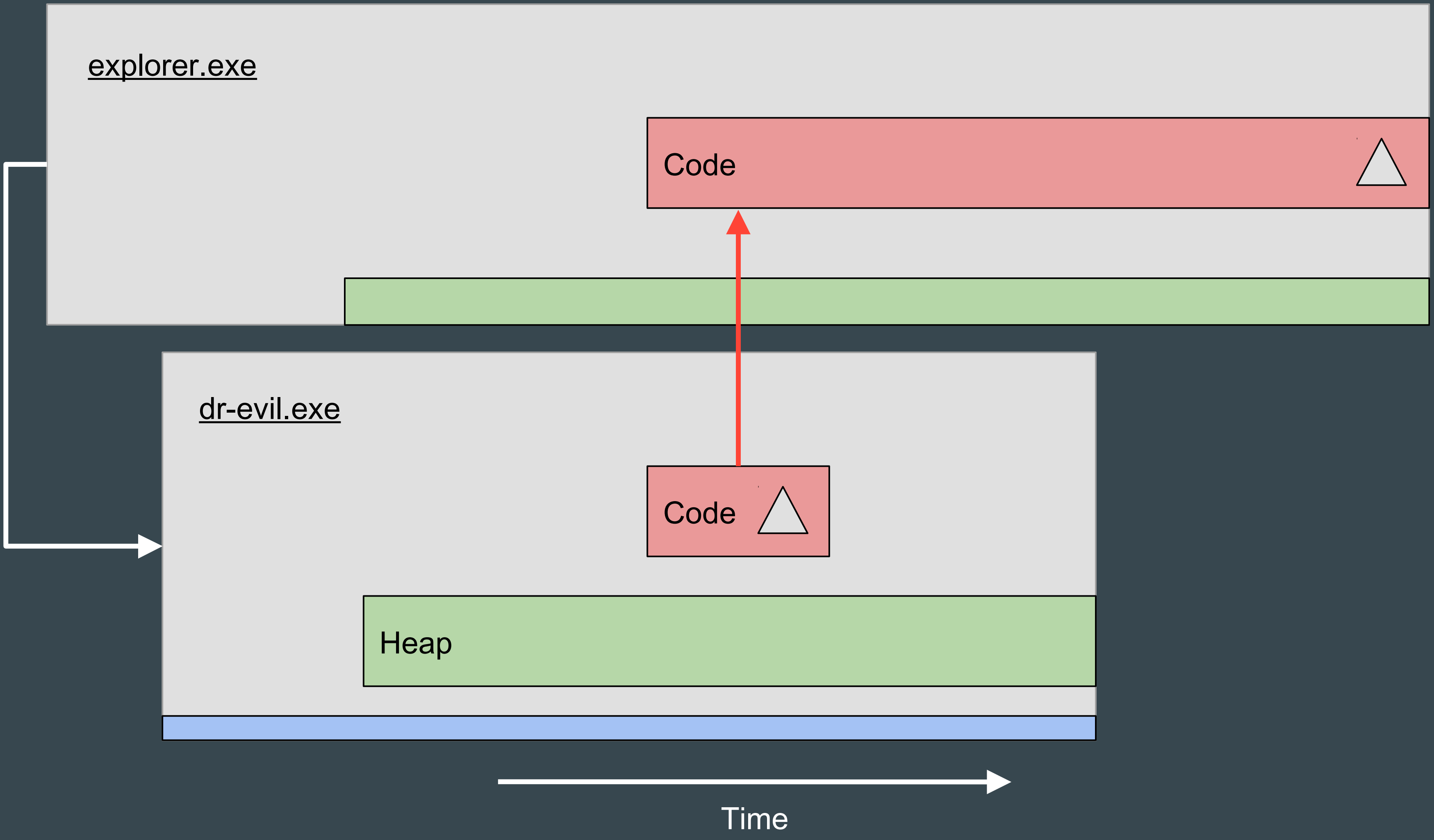
- Bridge the semantic gap

- Type 1: Data structure diffing
- Type 2: Content inspection
- Type 3: Temporal content inspection

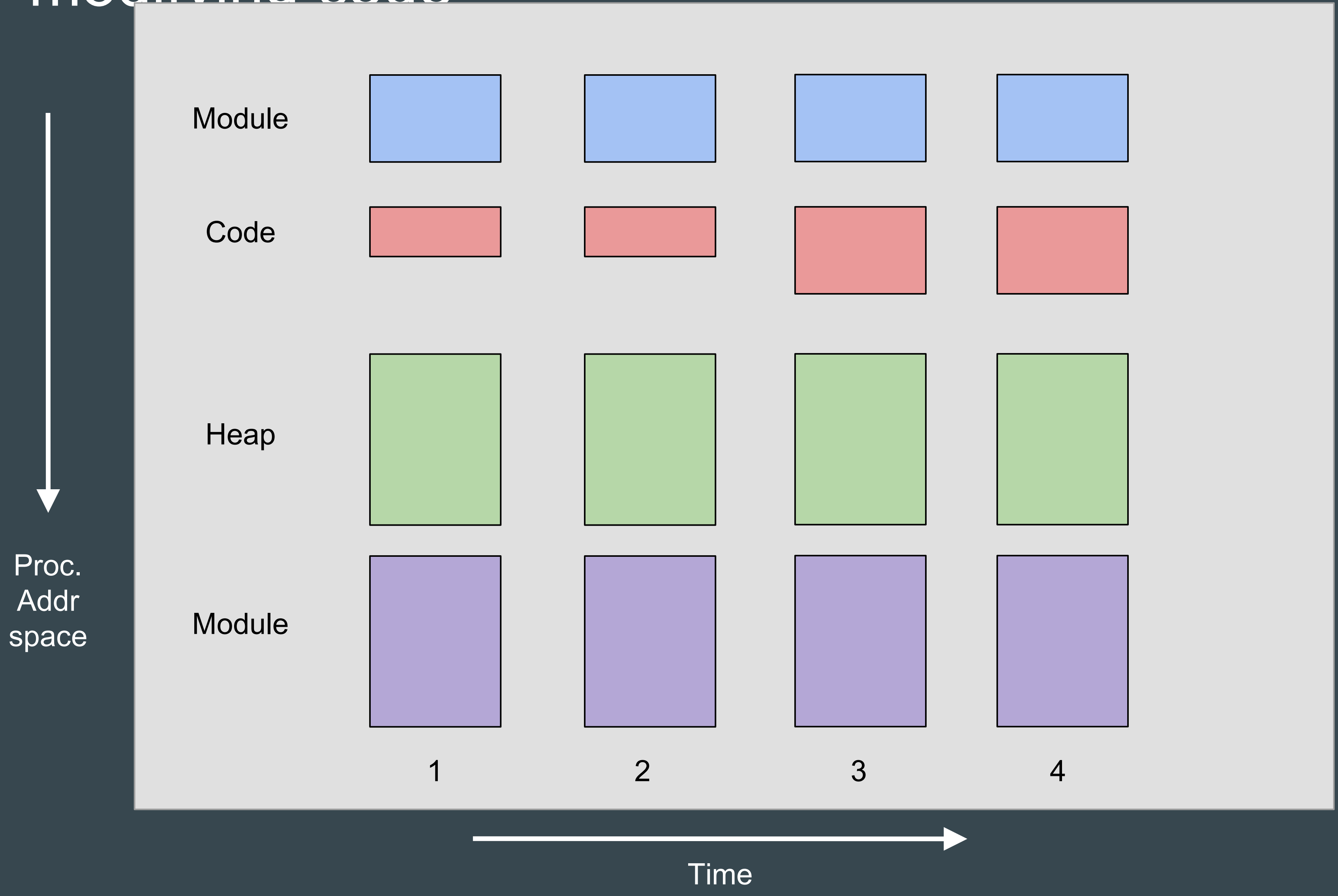
Type 1: Data structure diffing - Code injections



Type 2: Content inspection - Code injection behavior

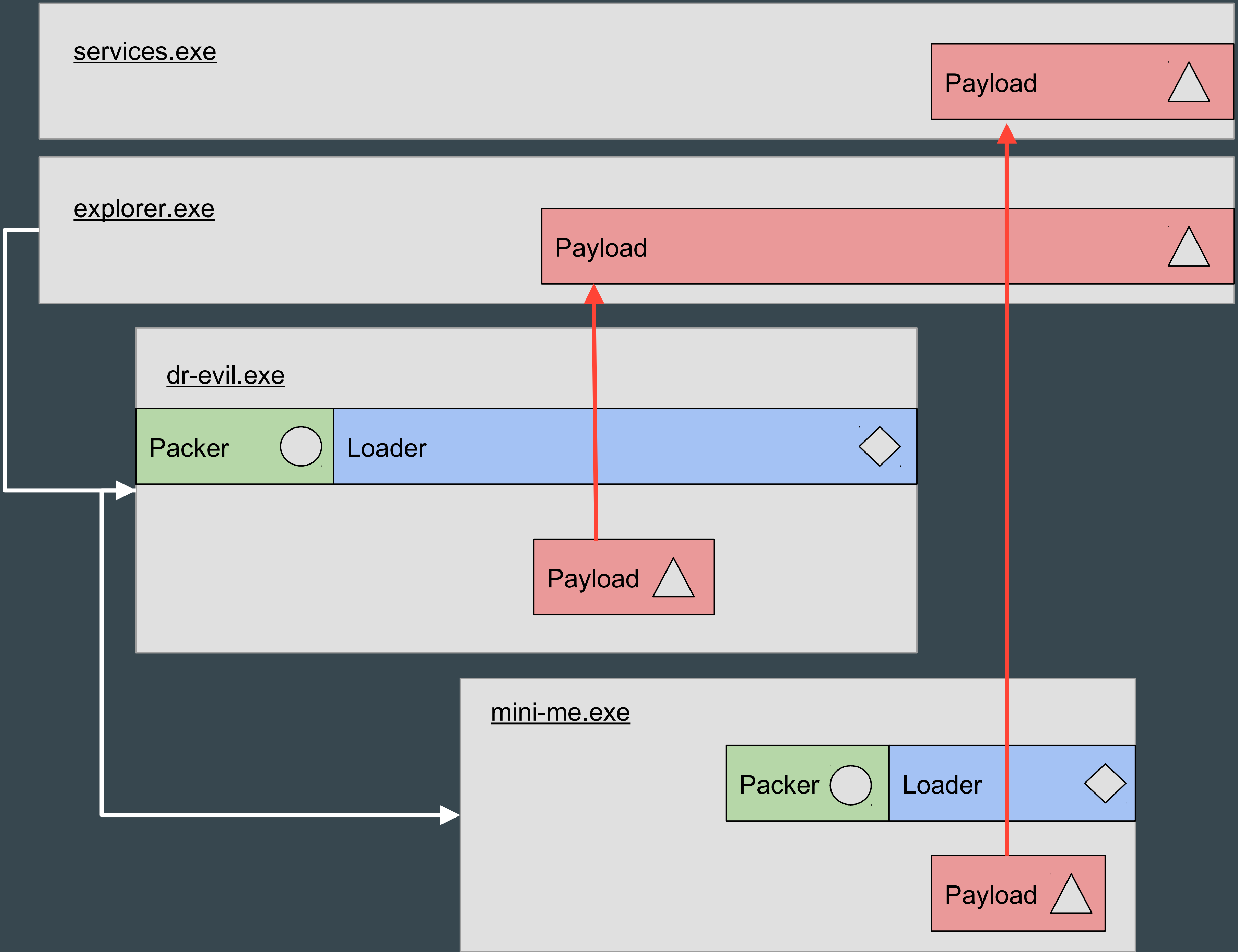


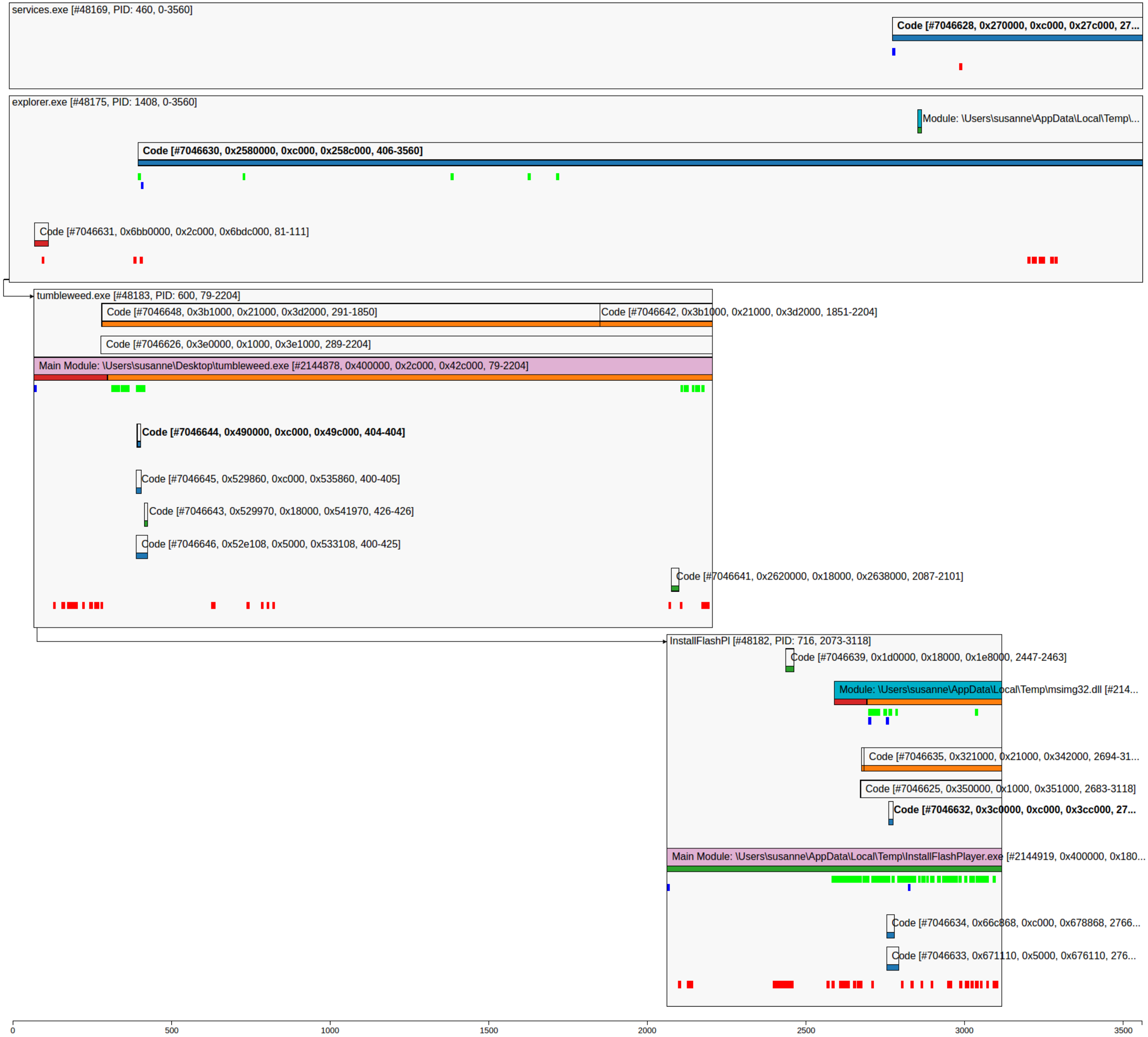
Type 3: Temporal content inspection - Self-modifying code



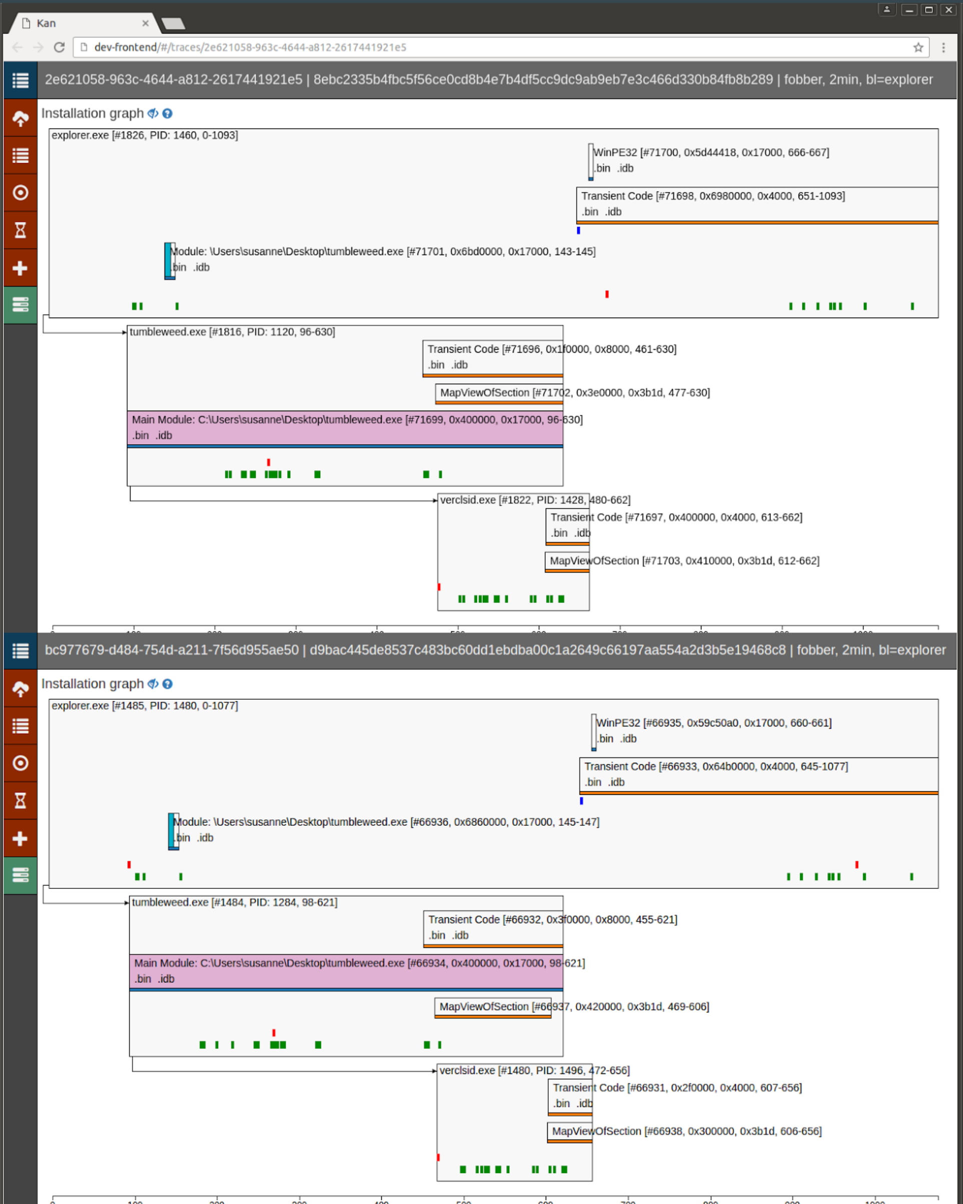
Type 1-3: Detecting code phases

- Characterize code phases: packer, loader, payload, etc. based on their lifetime in memory
- Detection of points in time where code is stable
- Remove redundancies through pattern matching


services.exe
Payload
explorer.exe
Payload
dr-evil.exe
Packer
Loader
Payload
mini-me.exe
Packer
Loader
Payload


services.exe [#48169, PID: 460, 0-3560]
Code [#7046628, 0x270000, 0xc000, 0x27c000, 27...
explorer.exe [#48175, PID: 1408, 0-3560]
Module: \Users\susanne\AppData\Local\Temp\...
Code [#7046630, 0x2580000, 0xc000, 0x258c000, 406-3560]
Code [#7046631, 0x6bb0000, 0x2c000, 0x6bdc000, 81-111]
tumbleweed.exe [#48183, PID: 600, 79-2204]
Code [#7046648, 0x3b1000, 0x21000, 0x3d2000, 291-1850]
Code [#7046642, 0x3b1000, 0x21000, 0x3d2000, 1851-2204]
Code [#7046626, 0x3e0000, 0x1000, 0x3e1000, 289-2204]
Main Module: \Users\susanne\Desktop\tumbleweed.exe [#2144878, 0x400000, 0x2c000, 0x42c000, 79-2204]
Code [#7046644, 0x490000, 0xc000, 0x49c000, 404-404]
Code [#7046645, 0x529860, 0xc000, 0x535860, 400-405]
Code [#7046643, 0x529970, 0x18000, 0x541970, 426-426]
Code [#7046646, 0x52e108, 0x5000, 0x533108, 400-425]
Code [#7046641, 0x2620000, 0x18000, 0x2638000, 2087-2101]
InstallFlashPl [#48182, PID: 716, 2073-3118]
Code [#7046639, 0x1d0000, 0x18000, 0x1e8000, 2447-2463]
Module: \Users\susanne\AppData\Local\Temp\msimg32.dll [#214...
Code [#7046635, 0x321000, 0x21000, 0x342000, 2694-31...
Code [#7046625, 0x350000, 0x1000, 0x351000, 2683-3118]
Code [#7046632, 0x3c0000, 0xc000, 0x3cc000, 27...
Main Module: \Users\susanne\AppData\Local\Temp\InstallFlashPlayer.exe [#2144919, 0x400000, 0x180...
Code [#7046634, 0x66c868, 0xc000, 0x678868, 2766...
Code [#7046633, 0x671110, 0x5000, 0x676110, 276...
0
500
1000
1500
2000
2500
3000
3500

Finding correlations between samples



Kan

dev-frontend/#/traces/2e621058-963c-4644-a812-2617441921e5

2e621058-963c-4644-a812-2617441921e5 | 8ebc2335b4fbc5f56ce0cd8b4e7b4df5cc9dc9ab9eb7e3c466d330b84fb8b289 | fobber, 2min, bl=explorer

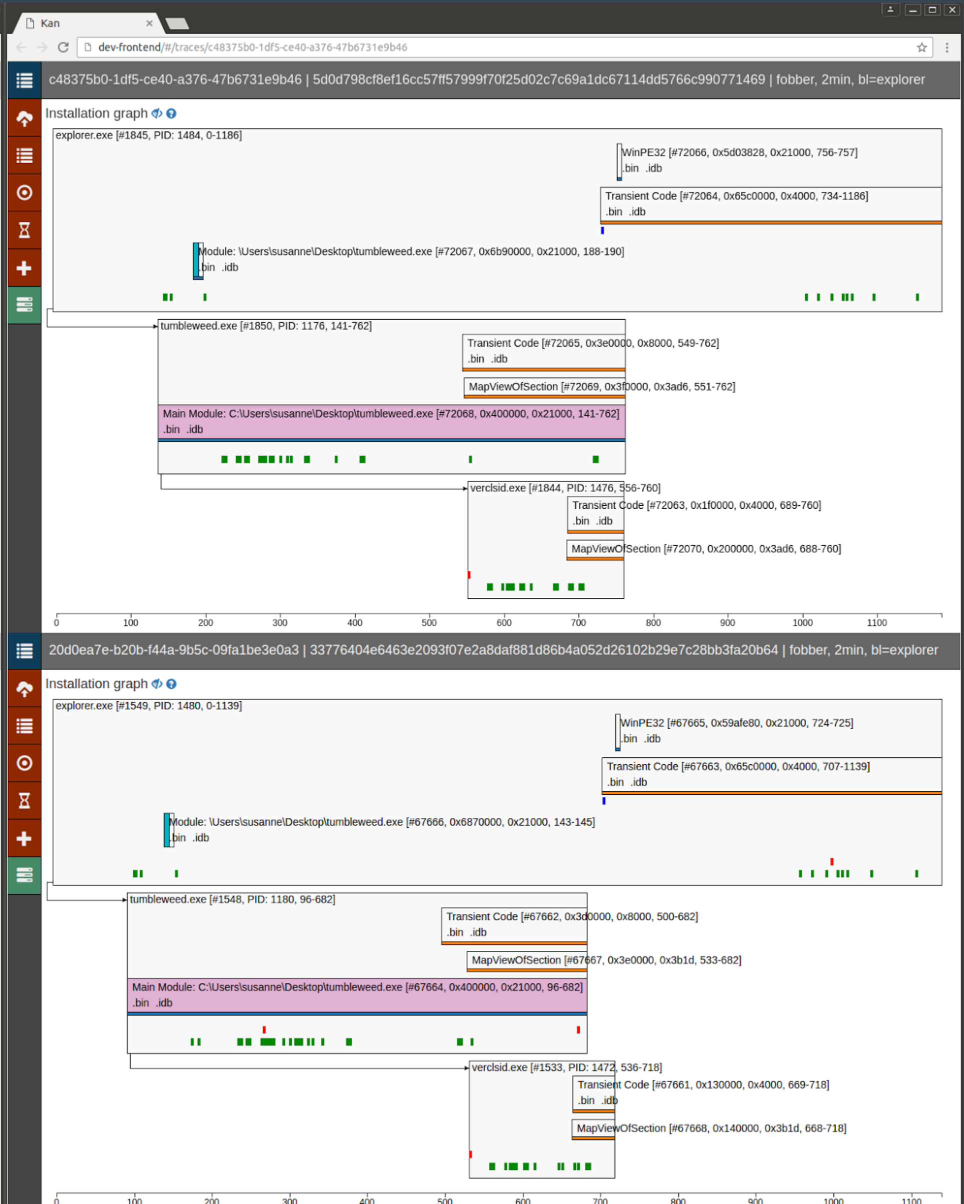
Installation graph

explorer.exe [#1826, PID: 1460, 0-1093]
WinPE32 [#71700, 0x5d44418, 0x17000, 666-667]
.bin .idb
Transient Code [#71698, 0x6980000, 0x4000, 651-1093]
.bin .idb
Module: \Users\susanne\Desktop\tumbleweed.exe [#71701, 0x6bd0000, 0x17000, 143-145]
.bin .idb
tumbleweed.exe [#1816, PID: 1120, 96-630]
Transient Code [#71696, 0x1f0000, 0x8000, 461-630]
.bin .idb
MapViewOfSection [#71702, 0x3e0000, 0x3b1d, 477-630]
Main Module: C:\Users\susanne\Desktop\tumbleweed.exe [#71699, 0x400000, 0x17000, 96-630]
.bin .idb
verclsid.exe [#1822, PID: 1428, 480-662]
Transient Code [#71697, 0x400000, 0x4000, 613-662]
.bin .idb
MapViewOfSection [#71703, 0x410000, 0x3b1d, 612-662]

bc977679-d484-754d-a211-7f56d955ae50 | d9bac445de8537c483bc60dd1ebdba00c1a2649c66197aa554a2d3b5e19468c8 | fobber, 2min, bl=explorer

Installation graph

explorer.exe [#1485, PID: 1480, 0-1077]
WinPE32 [#66935, 0x59c50a0, 0x17000, 660-661]
.bin .idb
Transient Code [#66933, 0x64b0000, 0x4000, 645-1077]
.bin .idb
Module: \Users\susanne\Desktop\tumbleweed.exe [#66936, 0x6860000, 0x17000, 145-147]
.bin .idb
tumbleweed.exe [#1484, PID: 1284, 98-621]
Transient Code [#66932, 0x3f0000, 0x8000, 455-621]
.bin .idb
Main Module: C:\Users\susanne\Desktop\tumbleweed.exe [#66934, 0x400000, 0x17000, 98-621]
.bin .idb
MapViewOfSection [#66937, 0x420000, 0x3b1d, 469-606]
verclsid.exe [#1480, PID: 1496, 472-656]
Transient Code [#66931, 0x2f0000, 0x4000, 607-656]
.bin .idb
MapViewOfSection [#66938, 0x300000, 0x3b1d, 606-656]



Kan

dev-frontend/#/traces/c48375b0-1df5-ce40-a376-47b6731e9b46

c48375b0-1df5-ce40-a376-47b6731e9b46 | 5d0d798cf8ef16cc57ff57999f70f25d02c7c69a1dc67114dd5766c990771469 | fobber, 2min, bl=explorer

Installation graph

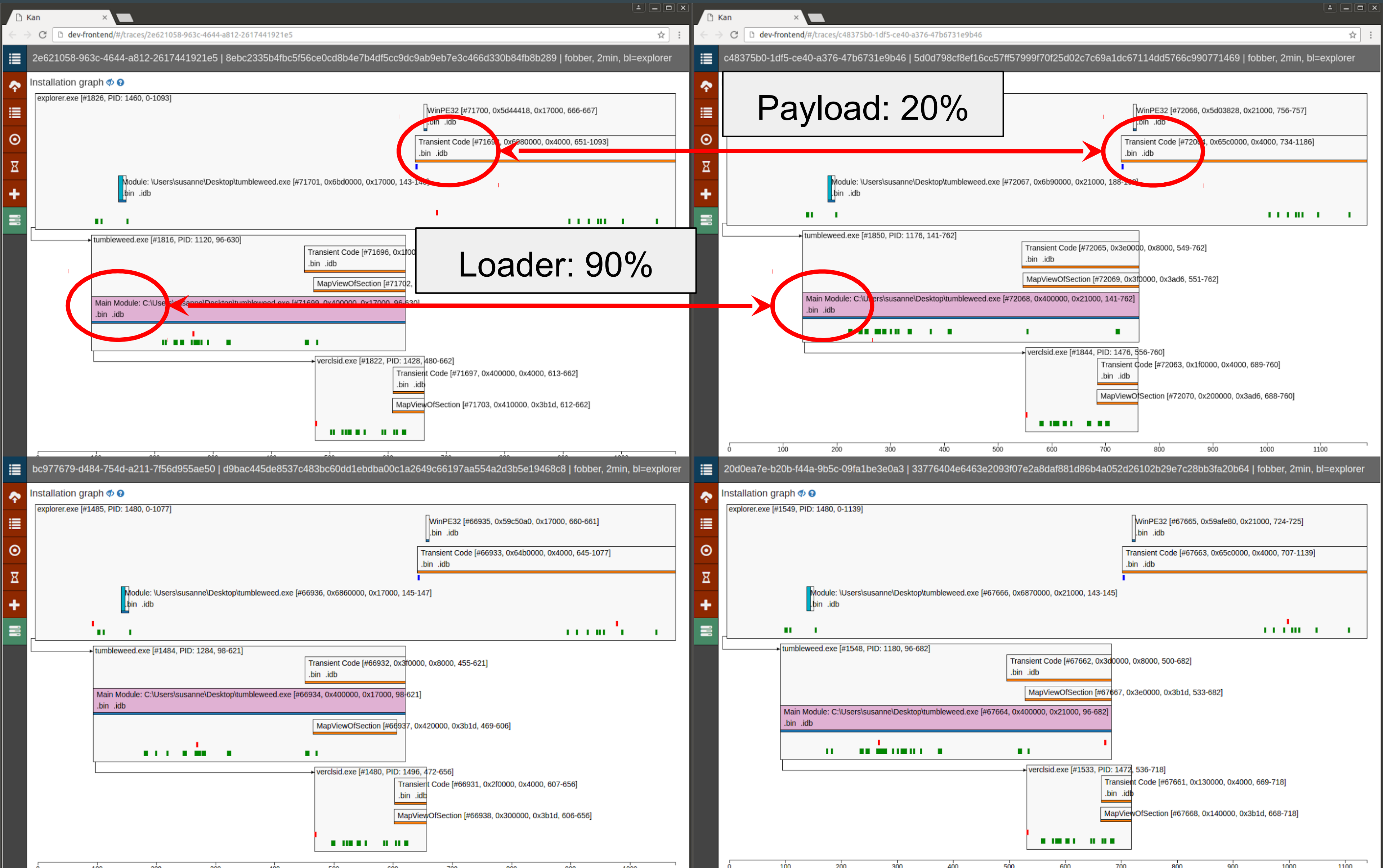
explorer.exe [#1845, PID: 1484, 0-1186]
WinPE32 [#72066, 0x5d03828, 0x21000, 756-757]
.bin .idb
Transient Code [#72064, 0x65c0000, 0x4000, 734-1186]
.bin .idb
Module: \Users\susanne\Desktop\tumbleweed.exe [#72067, 0x6b90000, 0x21000, 188-190]
.bin .idb
tumbleweed.exe [#1850, PID: 1176, 141-762]
Transient Code [#72065, 0x3e0000, 0x8000, 549-762]
.bin .idb
MapViewOfSection [#72069, 0x3f0000, 0x3ad6, 551-762]
Main Module: C:\Users\susanne\Desktop\tumbleweed.exe [#72068, 0x400000, 0x21000, 141-762]
.bin .idb
verclsid.exe [#1844, PID: 1476, 556-760]
Transient Code [#72063, 0x1f0000, 0x4000, 689-760]
.bin .idb
MapViewOfSection [#72070, 0x200000, 0x3ad6, 688-760]
0
100
200
300
400
500
600
700
800
900
1000
1100

20d0ea7e-b20b-f44a-9b5c-09fa1be3e0a3 | 33776404e6463e2093f07e2a8daf881d86b4a052d26102b29e7c28bb3fa20b64 | fobber, 2min, bl=explorer

Installation graph

explorer.exe [#1549, PID: 1480, 0-1139]
WinPE32 [#67665, 0x59afe80, 0x21000, 724-725]
.bin .idb
Transient Code [#67663, 0x65c0000, 0x4000, 707-1139]
.bin .idb
Module: \Users\susanne\Desktop\tumbleweed.exe [#67666, 0x6870000, 0x21000, 143-145]
.bin .idb
tumbleweed.exe [#1548, PID: 1180, 96-682]
Transient Code [#67662, 0x3d0000, 0x8000, 500-682]
.bin .idb
MapViewOfSection [#67667, 0x3e0000, 0x3b1d, 533-682]
Main Module: C:\Users\susanne\Desktop\tumbleweed.exe [#67664, 0x400000, 0x21000, 96-682]
.bin .idb
verclsid.exe [#1533, PID: 1472, 536-718]
Transient Code [#67661, 0x130000, 0x4000, 669-718]
.bin .idb
MapViewOfSection [#67668, 0x140000, 0x3b1d, 668-718]

Finding correlations between samples



Payload: 20%

Loader: 90%

dev-frontend/#/traces/2e621058-963c-4644-a812-2617441921e5

2e621058-963c-4644-a812-2617441921e5 | 8ebc2335b4fbc5f56ce0cd8b4e7b4df5cc9dc9ab9eb7e3c466d330b84fb8b289 | fobber, 2min, bl=explorer

dev-frontend/#/traces/c48375b0-1df5-ce40-a376-47b6731e9b46

c48375b0-1df5-ce40-a376-47b6731e9b46 | 5d0d798cf8ef16cc57ff57999f70f25d02c7c69a1dc67114dd5766c990771469 | fobber, 2min, bl=explorer

bc977679-d484-754d-a211-7f56d955ae50 | d9bac445de8537c483bc60dd1ebdba00c1a2649c66197aa554a2d3b5e19468c8 | fobber, 2min, bl=explorer

20d0ea7e-b20b-f44a-9b5c-09fa1be3e0a3 | 33776404e6463e2093f07e2a8daf881d86b4a052d26102b29e7c28bb3fa20b64 | fobber, 2min, bl=explorer

Kan
Installation graph
explorer.exe [#1826, PID: 1460, 0-1093]
WinPE32 [#71700, 0x5d44418, 0x17000, 666-667]
Transient Code [#71699, 0x6880000, 0x4000, 651-1093]
Module: \Users\susanne\Desktop\tumbleweed.exe [#71701, 0x6bd0000, 0x17000, 143-145]
tumbleweed.exe [#1816, PID: 1120, 96-630]
Transient Code [#71696, 0x1f00
MapViewOfSection [#71702,
Main Module: C:\Users\susanne\Desktop\tumbleweed.exe [#71698, 0x400000, 0x17000, 96-630]
verclsid.exe [#1822, PID: 1428, 480-662]
Transient Code [#71697, 0x400000, 0x4000, 613-662]
MapViewOfSection [#71703, 0x410000, 0x3b1d, 612-662]
WinPE32 [#72066, 0x5d03828, 0x21000, 756-757]
Transient Code [#72064, 0x65c0000, 0x4000, 734-1186]
Module: \Users\susanne\Desktop\tumbleweed.exe [#72067, 0x6b90000, 0x21000, 188-190]
tumbleweed.exe [#1850, PID: 1176, 141-762]
Transient Code [#72065, 0x3e0000, 0x8000, 549-762]
MapViewOfSection [#72069, 0x3f0000, 0x3ad6, 551-762]
Main Module: C:\Users\susanne\Desktop\tumbleweed.exe [#72068, 0x400000, 0x21000, 141-762]
verclsid.exe [#1844, PID: 1476, 556-760]
Transient Code [#72063, 0x1f0000, 0x4000, 689-760]
MapViewOfSection [#72070, 0x200000, 0x3ad6, 688-760]
explorer.exe [#1485, PID: 1480, 0-1077]
WinPE32 [#66935, 0x59c50a0, 0x17000, 660-661]
Transient Code [#66933, 0x64b0000, 0x4000, 645-1077]
Module: \Users\susanne\Desktop\tumbleweed.exe [#66936, 0x6860000, 0x17000, 145-147]
tumbleweed.exe [#1484, PID: 1284, 98-621]
Transient Code [#66932, 0x3f0000, 0x8000, 455-621]
Main Module: C:\Users\susanne\Desktop\tumbleweed.exe [#66934, 0x400000, 0x17000, 98-621]
MapViewOfSection [#66937, 0x420000, 0x3b1d, 469-606]
verclsid.exe [#1480, PID: 1496, 472-656]
Transient Code [#66931, 0x2f0000, 0x4000, 607-656]
MapViewOfSection [#66938, 0x300000, 0x3b1d, 606-656]
explorer.exe [#1549, PID: 1480, 0-1139]
WinPE32 [#67665, 0x59afe80, 0x21000, 724-725]
Transient Code [#67663, 0x65c0000, 0x4000, 707-1139]
Module: \Users\susanne\Desktop\tumbleweed.exe [#67666, 0x6870000, 0x21000, 143-145]
tumbleweed.exe [#1548, PID: 1180, 96-682]
Transient Code [#67662, 0x3d0000, 0x8000, 500-682]
MapViewOfSection [#67667, 0x3e0000, 0x3b1d, 533-682]
Main Module: C:\Users\susanne\Desktop\tumbleweed.exe [#67664, 0x400000, 0x21000, 96-682]
verclsid.exe [#1533, PID: 1472, 536-718]
Transient Code [#67661, 0x130000, 0x4000, 669-718]
MapViewOfSection [#67668, 0x140000, 0x3b1d, 668-718]
.bin .idb
0
100
200
300
400
500
600
700
800
900
1000
1100

Conclusion

- Novel memory acquisition technique
- Memory inspection based analysis
- Automate some aspects of reverse engineering
- Provide entry points for further analysis
- Delivers relevant artifacts for malware correlations

Questions?

https://sel.bfh.ch

-

jonas.wagner@bfh.ch