Star Gazing

Using A Galaxy of YARA Methods to Pursue an Apex Actor

The Disclaimers

Did not do IR & no knowledge of targets

No attribution or leaked documents herein

IDGAF about catching Future Samples

Personal Research; Not Reflective of My Employer

This talk is a journey in exploring malware similarity via YARA

TABLE OF CONTENTS

01
INTRODUCTION

FIRST – THANK YOUS

@ConnorSecurity

@wxs

@jgrosfelt

@arieljt

@williballenthin

@jags

@_marklech_

@xorhex

@qutluch

@craiu

@notareverser

@cbecks2

PFTP TR Team

Insikt Group

@ stvemillertime

@TheQueenofELF

@ plusvic

@BitsofBinary

@CyberOverDrive

@edeca

& MANY MORE

The Lamberts

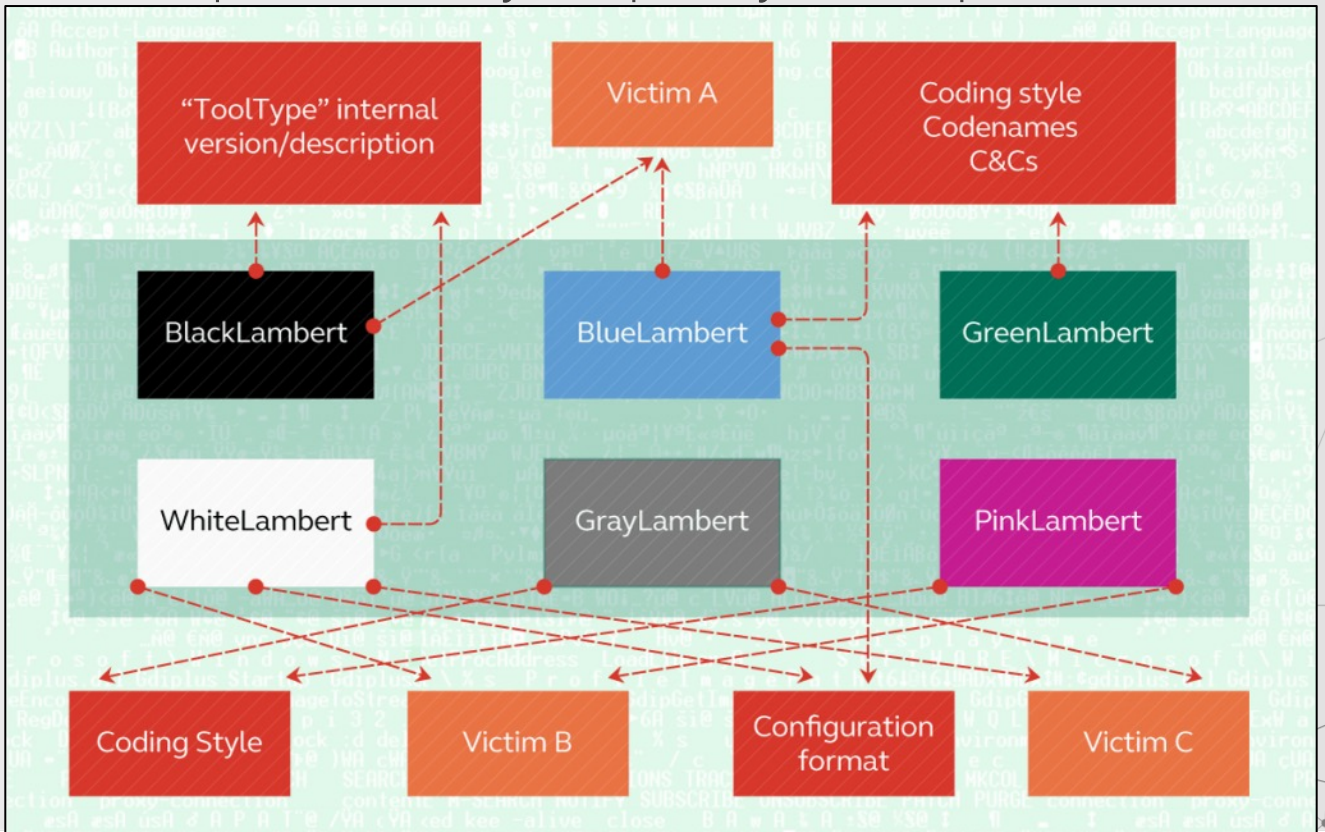
Longhorn
BRIGHTCONSTELLATION
APT-C-39

02

THE PROBLEM

PROBLEM

50+ samples linked by Kaspersky but no public evidence



PROBLEM

Lots of colors of Lambert

But most knowledge is in private reporting + breadcrumbs

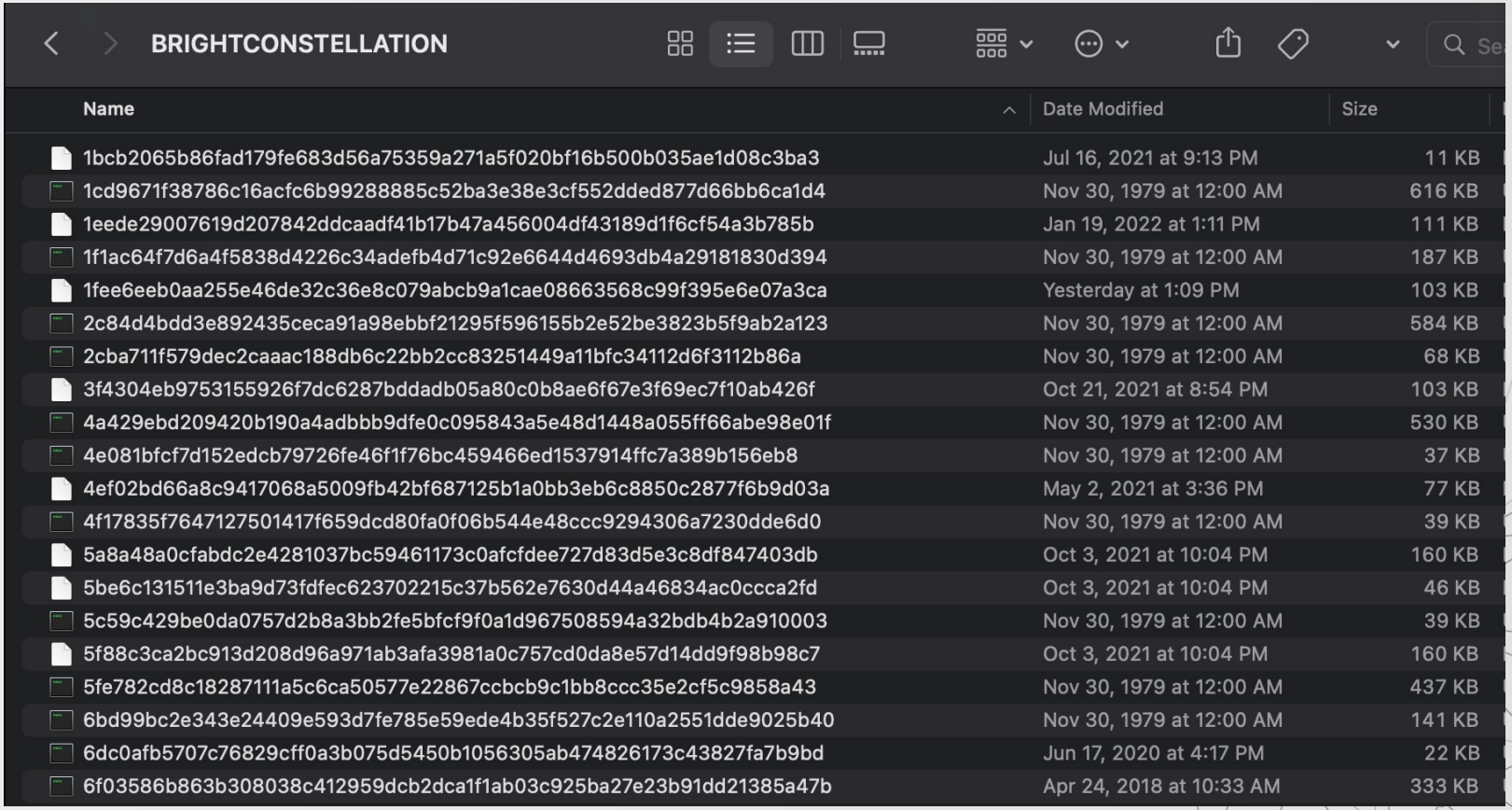
1 AV signature name

Kaspersky	! HEUR:Trojan.Multi.Lamberts.gen
ESET-NOD32	! A Variant Of Win32/ColoredLambert.A

03

CLUSTERING TIME

STARTING PLACE



INITIAL METHODOLOGY

(Ab)use PE Format to Find Feature Overlaps

Use YARA’s console to print overlaps YARA already knows

Use Ronnie to produce table for viewing

Find something resilient

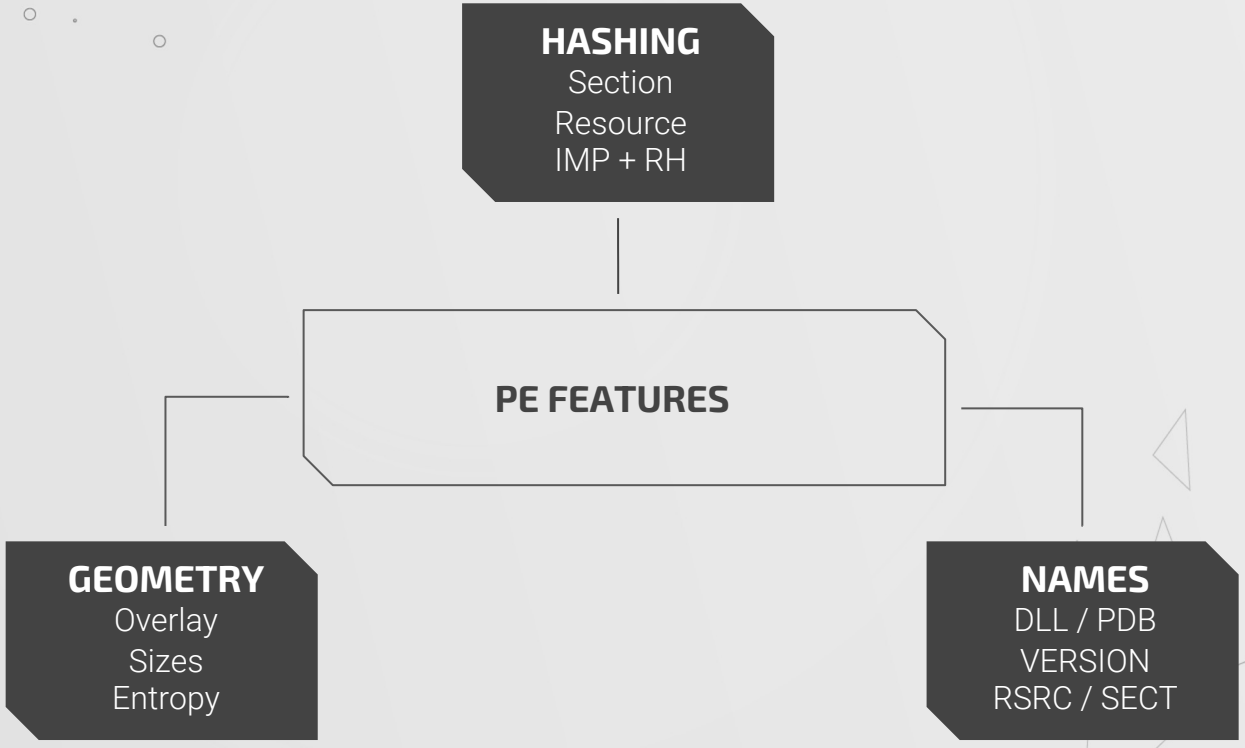
TOOLING CHOICES

Initial Tools:

- YARA
- Binary Refinery
- Python
- Ronnie.py <3 Steve Miller

Behavioral Analysis was largely useless anyway

INITIAL METHOD



INITIAL SAMPLE SURFACE AREA

[:great-job:] LIGHT WEIGHT! Heres the sorted table:

hash.md5	pe.timestamp	pe.imphash()	pe.dll_name	filesize
b7aec730f727984c24a7d065313b52fe				21010
c7acb3c811f3f7df0a37ba6053ef169a				128498
db6862153b4d1a010e858803e92586d7	2002-06-10 10:28:56 (1023719336)	c28a94c9ba3bae95c96166a6b4c2409f	acpid.sys	76928
e0127cc8567b0d8d8bb6d205a258283b	2002-06-12 14:56:13 (1023908173)	0bf0ba25ab08875a4a48403bf8d2aedd	hiddrv.sys	77184
23df2b8320cd5954aa6700819cdb0faa	2003-12-11 07:25:19 (1071145519)	cf0f4b6c800b833cca0e686847c01561	a.dll	354816
03bc7a8584fadeceb3d948304b531c3f	2004-10-06 06:01:21 (1097056881)	3fb945c27dd84f3ab2a43dd3037f73f2	a.dll	461312
c55a70c3413818cb5be7913002c1c486	2004-10-09 17:09:44 (1097356184)	6fd784161557889f4b71e261de19e4a1	a.dll	331264
116f4e1288862c4f8714e133cf45a1e8	2005-01-31 12:21:53 (1107192113)	0327406b8d00f8fb9703b409d9b1bd17	~DT4569.tmp	4608
95db8d2f033a30d239f109a9e9d05cf6	2005-07-07 11:29:52 (1120750192)	70aa590b218f22f05575f3767728fd35	mnmdf.sys	77184
ba38a75f6b2669098710b56afdf1d7d1	2005-12-06 18:20:36 (1133911236)	c923e86a79c858ac29273479b498473b		122880

hash.md5	pe.timestamp	pe.imphash()	pe.dll_name	filesize
116f4e1288862c4f8714e133cf45a1e8	2005-01-31 12:21:53 (1107192113)	0327406b8d00f8fb9703b409d9b1bd17	~DT4569.tmp	4608
9359a61e225f396aede1fa381390c42e	2007-03-02 17:18:03 (1172873883)	05dbabe1fb046a965eaf4b9a9570529e	~EE112.tmp	4608
9384f4007c492d4fa040924f31c00166	2009-12-05 17:50:13 (1260053413)	9b6b6a7858e17fb0b17e1c1428330343	LangDLL.dll	5632
c17103ae9072a06da581dec998343fc1	2009-12-05 17:50:21 (1260053421)	2017f2acbdaa42ab3e4adeb8b4c37e7b	System.dll	11264
be60ff4b7f4953d84b2d9b8961792ef1	2015-08-19 14:51:02 (1440010262)	3a8ef5ede43b2137e235a0653e41e4e5	dll.dll	13312
c2bca118b4a72faf3e975ddf82108b42	2015-03-10 14:37:29 (1426012649)	3a8ef5ede43b2137e235a0653e41e4e5	dll.dll	13312
20288f1e7daeb6fa664f350df7e6eef6	2012-08-16 07:46:19 (1345117579)	55fc5145c5e1259d841932b599ea46d2	svc_dll.dll	14848
325b008aec81e5aaa57096f05d4212b5	2009-12-05 17:50:12 (1260053412)	b1cd0d78f652ce5fc63f0879371af012	InstallOptions.dll	14848
c06d422656ca69827f63802667723932	2015-02-25 11:50:18 (1424883018)	d6451a47b682063cdfe7e40db1b856aa		15872
bd5f8b4384bc364a86fa57ced654685b	2015-05-12 11:10:23 (1431443423)	653cdb1395f76ba98be0a3eba3f9ffc6	dll.dll	15872
2b25e21e0c3cc6eee7a640cbc55cc86e	2015-03-10 14:37:28 (1426012648)	653cdb1395f76ba98be0a3eba3f9ffc6	dll.dll	15872
060d32ef4e1467ee15ae53753035be65	2014-03-20 11:16:19 (1395328579)	653cdb1395f76ba98be0a3eba3f9ffc6	dll.dll	15872
a40ce601a37640bce3ef53fa9c186df4	2015-01-04 18:20:15 (1420413615)	653cdb1395f76ba98be0a3eba3f9ffc6	dll.dll	15872
d4dffdcf3c948c2587aee2997cab99f0	2015-05-04 14:35:27 (1430764527)	653cdb1395f76ba98be0a3eba3f9ffc6	dll.dll	15872

SURFACE AREA

```
rule imphash
{
    condition:
        console.log("pe.imphash() == ", pe.imphash())
}
```

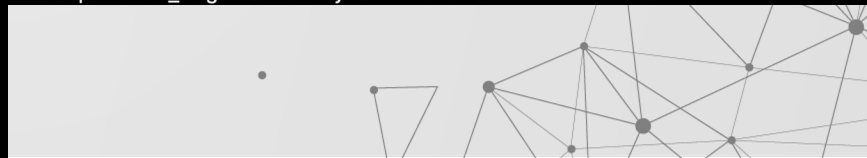
```
$ yara ~/Desktop/evil.yar Lamberts/ -r | sort | uniq -c | sort -rn
   6 pe.imphash() == 8eb1269a8647f0f5d2caed350d9c4020
   5 pe.imphash() == a4eb1e2be9d15d875c6451da74d6d2c1
   5 pe.imphash() == 87d4444a2cb3254ac4da1968a7e41f5c
   5 pe.imphash() == 653cdb1395f76ba98be0a3eba3f9ffc6
   3 pe.imphash() == d41d8cd98f00b204e9800998ecf8427e
   3 pe.imphash() == a5f2981ac470d17bc79355655444f478
   3 pe.imphash() == a33d3ce7194c24e0f1741dacd3b9ddca
   3 pe.imphash() == 91dd0c2a90509140d1a830bb8a207f72
   3 pe.imphash() == 0ece189d2de69be31b69cae6e9533d20
   3 pe.imphash() == 0753e4caf43ea9b3195fb91520a02930
   2 pe.imphash() == f1d3dd97fd156df30fcac1333ff23a9f
   2 pe.imphash() == ec6aa061cf1a7fc265ab830b5e52b674
   2 pe.imphash() == d6b1fbc854b6afe97f80837ab06d088a
   2 pe.imphash() == d1e0d0c068313e63bbd192c5b8ac5d58
```

SURFACE AREA

```
rule richheaderhash
{
    condition:
        console.log("hash.md5(pe.rich_signature.clear_data) == ", hash.md5(pe.rich_signature.clear_data))
}
```

```
$ yara ~/Desktop/evil.yar Lamberts/ -r | sort | uniq -c | sort -rn
   6 hash.md5(pe.rich_signature.clear_data) == 48ba0f54f81febc969fd28d784c897d0
   6 hash.md5(pe.rich_signature.clear_data) == 2a3f6381e856430d41e25b46f95a2daa
   5 hash.md5(pe.rich_signature.clear_data) == bfa45b9a0b5adf3ea4aa9609fd215437
   5 hash.md5(pe.rich_signature.clear_data) == 634787a46ba2f8f80ba351e9907424ea
   3 hash.md5(pe.rich_signature.clear_data) == d60e5ccda3e19fab0430bc2bbaed7101
   3 hash.md5(pe.rich_signature.clear_data) == bd4f08587ead9f643e4218ccf01950cb
   3 hash.md5(pe.rich_signature.clear_data) == 7b5c7e6ecd6b150f3fbc67976bdbaa41
   3 hash.md5(pe.rich_signature.clear_data) == 56548344e0f97143bf88c419956fba04
   3 hash.md5(pe.rich_signature.clear_data) == 1c26f36f35cf9431da3b6c802c6fb73e
   2 hash.md5(pe.rich_signature.clear_data) == dcda1a40333c313ad524840c59cee7a2
   2 hash.md5(pe.rich_signature.clear_data) == d851f014f6498f147b231890a0a06139
   2 hash.md5(pe.rich_signature.clear_data) == ad6d2ce84919d290f6244e511df4fa03
   2 hash.md5(pe.rich_signature.clear_data) == a3a0b4709b2002ef83c3712fbca5dcf4
   2 hash.md5(pe.rich_signature.clear_data) == 83b3c170ccc7e5605edd7521f53d02d4
   2 hash.md5(pe.rich_signature.clear_data) == 8307973bd7cb1f765fe185237944d16d
   2 hash.md5(pe.rich_signature.clear_data) == 6e591ae88ffa1906948d1ab9efd31511
   2 hash.md5(pe.rich_signature.clear_data) == 67113ad18c973f91560efd35eccd6130
   2 hash.md5(pe.rich_signature.clear_data) == 66e2996d42ad3690c02d369f85fa5fd7
   2 hash.md5(pe.rich_signature.clear_data) == 1787f6b0c4f6b7ed29c9aae81f74ea5d
```

```
$ yara ~/Desktop/evil.yar Lamberts/ -r | sort | uniq -c | sort -rn
   6 pe.rich_signature.key 0x6847c87b
   6 pe.rich_signature.key 0x1a569c98
   5 pe.rich_signature.key 0xd0565c15
   5 pe.rich_signature.key 0x95d85edd
   3 pe.rich_signature.key 0xbec81e6a
   3 pe.rich_signature.key 0xba2b6b49
   3 pe.rich_signature.key 0xa19a753b
   3 pe.rich_signature.key 0x8ea198bd
   3 pe.rich_signature.key 0x742dcb6e
   2 pe.rich_signature.key 0xd4d59be3
   2 pe.rich_signature.key 0xc8569c15
   2 pe.rich_signature.key 0xb8122404
   2 pe.rich_signature.key 0xab8a07b5
   2 pe.rich_signature.key 0xa5c65dc8
```



EXPORT SURFACE AREA

[:great-job:] LIGHT WEIGHT! Heres the sorted table:

hash.md5	pe.export_details[0].name	pe.export_details[1].name	pe.export_details[2].name	pe.export_details[3].name
c17103ae9072a06da581dec998343fc1	Alloc	Call	Copy	Free
0ca4f3e99e9a6f834bf6eaf8209a8147	DllCanUnloadNow			ServiceMain
5b92b64e41353ecf11ddd908d365ad45	DllCanUnloadNow			ServiceMain
7bfa16de414bdd6e02aeb9c5f1fbc586	DllCanUnloadNow			ServiceMain
060d32ef4e1467ee15ae53753035be65	DllInstall	DllRegisterServer	HandlerEx	ServiceMain
20288f1e7daeb6fa664f350df7e6eef6	DllInstall	DllRegisterServer	HandlerEx	ServiceMain
2b25e21e0c3cc6eee7a640cbc55cc86e	DllInstall	DllRegisterServer	HandlerEx	ServiceMain
5dbdade5d72feca45c6bc08f05d9bdb0	DllInstall	DllRegisterServer	HandlerEx	ServiceMain
7260cd78fbe583da47f992fca5bb4137	DllInstall	DllRegisterServer	HandlerEx	ServiceMain
82e950a2caf7844cc305c94ad1cc1288	DllInstall			
a40ce601a37640bce3ef53fa9c186df4	DllInstall	DllRegisterServer	HandlerEx	ServiceMain
b76e8611057d9607c6ce0acc0ba4de2b	DllInstall	DllRegisterServer	HandlerEx	ServiceMain
bd5f8b4384bc364a86fa57ced654685b	DllInstall	DllRegisterServer	HandlerEx	ServiceMain
be60ff4b7f4953d84b2d9b8961792ef1	DllInstall			
c2bca118b4a72faf3e975ddf82108b42	DllInstall			
d4dffdcf3c948c2587aee2997cab99f0	DllInstall	DllRegisterServer	HandlerEx	ServiceMain
9384f4007c492d4fa040924f31c00166	LangDialog			
b9317bd833531f51024624611940461d	PrintLog			
116f4e1288862c4f8714e133cf45a1e8	_DT4569@16			
116f4e1288862c4f8714e133cf45a1e8	_DT4569@16			
9359a61e225f396aede1fa381390c42e	_EE112@16			
95db8d2f033a30d239f109a9e9d05cf6	__DriverEntry@4			
db6862153b4d1a010e858803e92586d7	__DriverEntry@4			
e0127cc8567b0d8d8bb6d205a258283b	__DriverEntry@4			
325b008aec81e5aaa57096f05d4212b5	dialog	initDialog	show	

EXPORT SURFACE AREA

hash.md5	pe.export_details[0].name	pe.export_details[1].name	pe.export_details[2].name	pe.export_details[3].name	pe.export_details[4].name
db6862153b4d1a010e858803e92586d7	__DriverEntry@4				
dbf3d9bb35b9fa1b4badb8d92254472c					
dc16e14338041e38fcc971061ba913ce					
dd8c03517abc9760d662ad51555f030b					
debf0b01fc1250b5dc5f1995695906ab					
e0127cc8567b0d8d8bb6d205a258283b	__DriverEntry@4				
e26f345e7ac9bd2c6760f7f8dc2c0589					
e3625e12e95611c5a27e2c96744049ad			init1	init2	
e435293a62e3dfddf4df7ce3e401b908					
e77fdf98475ffec06434e2cdba1b0b5b					
f0b812de90184e91ce2ec056e7ef3279					
f4a3b72a8fb620ec9dc12458c1d840b7					
f4d88c0475c498af2fdd4167fcc25d02					
f8e9b773334e48e08df20e45f062156f					
fab76458bea1cdeb5795021148ff6866					
fbf386dd6f3c6cb027daa8b48d1f1c73					
fcff4ef89ae104d69fc177f041273040					
c17103ae9072a06da581dec998343fc1	Alloc	Call	Copy	Free	Get
03bc7a8584fadeceb3d948304b531c3f				DllMain	ServiceMain
7260cd78fbe583da47f992fca5bb4137	DllInstall	DllRegisterServer	HandlerEx	ServiceMain	_IsOperandReg@8
b76e8611057d9607c6ce0acc0ba4de2b	DllInstall	DllRegisterServer	HandlerEx	ServiceMain	_IsOperandReg@8

DELAYED IMPORT SURFACE AREA

pe.number_of_delayed_imports	pe.number_of_delayed_imported_functions	pe.delayed_import_details[0].library_name	pe.delayed_import_details[0].functions[0].name
1	4	ADVAPI32.dll	LookupPrivilegeValueW
1	4	ADVAPI32.dll	LookupPrivilegeValueW
3	15	SHLWAPI.dll	PathRemoveExtensionW
3	15	SHLWAPI.dll	PathRemoveExtensionW
3	15	SHLWAPI.dll	PathRemoveExtensionW
3	15	SHLWAPI.dll	PathRemoveExtensionW
3	89	pdh.dll	PdhGetFormattedCounterArrayW
3	89	pdh.dll	PdhGetFormattedCounterArrayW
3	89	pdh.dll	PdhGetFormattedCounterArrayW
3	89	pdh.dll	PdhGetFormattedCounterArrayW
3	89	pdh.dll	PdhGetFormattedCounterArrayW
3	89	pdh.dll	PdhGetFormattedCounterArrayW
3	89	pdh.dll	PdhGetFormattedCounterArrayW
3	89	pdh.dll	PdhGetFormattedCounterArrayW
3	89	pdh.dll	PdhGetFormattedCounterArrayW
6	49	USER32.dll	wsprintfW
6	59	SHLWAPI.dll	StrCmpIW
6	64	SHLWAPI.dll	PathAppendW
7	88	ADVAPI32.dll	RegCloseKey
8	58	ADVAPI32.dll	RegCloseKey
8	58	ADVAPI32.dll	RegCloseKey
8	58	ADVAPI32.dll	RegCloseKey
8	58	ADVAPI32.dll	RegCloseKey
8	58	ADVAPI32.dll	RegCloseKey
8	58	ADVAPI32.dll	RegCloseKey
8	58	ADVAPI32.dll	RegCloseKey

DEV FINGERPRINTS SURFACE AREA

[:great-job:] LIGHT WEIGHT! Heres the sorted table:

hash.md5	pe.dll_name	pe.pdb_path
060d32ef4e1467ee15ae53753035be65	dll.dll	
07171cde2a842704f568f04e3ca81d6a		
0b49bd4f441a75638c6fe4c95873db2e		
0ca4f3e99e9a6f834bf6eaf8209a8147	mdmm.exe	
0e370c31a447fe06ebec733cb134e6a5		
0f43e34b1039136edb6cc8d6db201d0d		
0faf02a82b0f978037c4aededbe886a1		
116f4e1288862c4f8714e133cf45a1e8	~DT4569.tmp	
fbf386dd6f3c6cb027daa8b48d1f1c73	winlib.dll	
6870f4548fe2f9c5fe22b3ecb0a12c6c		C:\\VCcode\\aaa\\x64\\Debug\\aaa.pdb
42793c3ed137f999b525b1020b52d432	sfxrar.exe	D:\\Projects\\WinRAR\\sfx\\build\\sfxrar32\\Release\\sfxrar.pdb
03bc7a8584fadeceb3d948304b531c3f	a.dll	a
23df2b8320cd5954aa6700819cdb0faa	a.dll	a
5f060940b231db5ba3fff4cb12abb7f7		a
c55a70c3413818cb5be7913002c1c486	a.dll	a
d6f6ffd201709e4f03cef21b1fec5f25		a
db6862153b4d1a010e858803e92586d7	acpid.sys	acpid.pdb
c06d422656ca69827f63802667723932		c:\\users\\bot\\fluxwire-cmake\\delta\\mswin-x86\\build\\base\\cmake\\ddk_node\\objfre_wxp_x86\\i386\\node.pdb
e0127cc8567b0d8d8bb6d205a258283b	hiddrv.sys	hiddrv.pdb
95db8d2f033a30d239f109a9e9d05cf6	mnmdf.sys	mnmdf.pdb
8eb5c5ed448288ee3b7536f571284631		x
ab3dd8522484795b00e22bb068a3c921		x
e3625e12e95611c5a27e2c96744049ad	library.dll	x

VERSION INFORMATION

52d750ab9e557cf4f358a63593be6e99	CompanyName	ACARD Technology Corp.
52d750ab9e557cf4f358a63593be6e99	CompanyName	ACARD Technology Corp.
cb0a0f2dbe26cca92eb08083e1705c68	CompanyName	ACARD Technology Corp.
4a16643a1c0ddb03f4833d28f80edcad	CompanyName	BIOS Innovations
4dcd011b08ff854b3789c3188b8ee95b	CompanyName	BIOS Innovations
5f060940b231db5ba3fff4cb12abb7f7	CompanyName	BIOS Innovations
853c44d5408781395f3ac65e768f7e65	CompanyName	BIOS Innovations
d6f6ffd201709e4f03cef21b1fec5f25	CompanyName	BIOS Innovations
a4863fcea90680a474a6eaa1e790ace5	CompanyName	Fujitsu Corporation
d857d7e49324a67bbf3e0f845a273a19	CompanyName	Fujitsu Corporation
20a7f3c5d958fac3d57f9e9fc2b089bd	CompanyName	Intel Corporation
41fe4ea8912918cedd6528ab99f3d999	CompanyName	Intel Corporation
6c466283e7f8757973ba253aa6080d8c	CompanyName	Intel Corporation
6d1e003143b5a5b6cc3cba9c5433c07a	CompanyName	Intel Corporation
99ef1e473ac553cf80f6117b2e95e79b	CompanyName	Intel Corporation
0ca4f3e99e9a6f834bf6eaf8209a8147	CompanyName	Microsoft Corporation
1a27ba4f541d3f6066c90822f9f25e9f	CompanyName	Microsoft Corporation
2a8d9b5c18d314a36e7ef82f0ac3635e	CompanyName	Microsoft Corporation
36ffcdbc7a8b97da6c8c62af2f7f1a9f	CompanyName	Microsoft Corporation
42f43edc9937e4aa5f985773f5ea9daa	CompanyName	Microsoft Corporation
452d86e050ad691dfc46a7abc0ef8a2f	CompanyName	Microsoft Corporation
517d86f7f494a9d7f2405020b44521eb	CompanyName	Microsoft Corporation
5483c7da065e548aa2f189592484190d	CompanyName	Microsoft Corporation

SHARED CHUNKS

```
$ yara ~/Desktop/evil.yar Lamberts/ -r | sort | uniq -c | sort -rn
  16 section hash d41d8cd98f00b204e9800998ecf8427e
   9 resource hash 78c1666916c7e5d7e70d094efbb52ca987f70ac66c907f40f36472e3b0e2bf7f
   7 section hash a1d25fab0f0999169575e729273ac450
   7 section hash 97ce0f6491eda9e959ad7a31f7c5f292
   7 section hash 858cb90d03013fac19c46c642c1611f0
   6 section hash ade88025b419858a8c8cb9da7c7f5173
   6 section hash 9f2ba27d2524b238cb3ce52046c6774a
   6 section hash 9749856b31ec6a427016d7007d70a9f0
   6 section hash 92c98668604ed21149b03e31495acc1b
   6 section hash 06918aea158501659ba39942b836c34f
   6 overlay hash cd7cbf283d421cbf1d19f0376cbc806201a5a7b3
   5 section hash e5cdb6e07b6684e73be979c811012b52
   5 section hash bb64d581a5d7f9c414f2d8d57ef63eee
   5 section hash 7b1dd2c61803a4e05ffd83f241dde3c6
   5 section hash 52e2298e4d6acfdf9ebeaeea8e57ba57
   5 section hash 452b6fc2259f4b05f0f2bf7676beaf28
   5 section hash 196a75ebab89a7d6d4941d65828dd06b
   5 section hash 07a16c1689d4dabe67b14d0bb5e35f8d
   5 resource hash d9e7bdd805880c1a4cc245d8ef4ac433f851d02831a96dfe1c75f8d7f8aaf6c3
   5 resource hash c3675aa8f4cbb131096bc70d001c9759fac2c1d66e9dfe7d33f21a802ed600be
   5 resource hash a302c696826b1ddf9a7e4914a933707834c1707e259283848c4590a3de4a035b
```

SHARED FEATURES

EXPORT NAMES

PARADOX
MARIANASTRENCH

MEDDLER
CUTTINGTIES
RATIONLIST

RESOURCE HASH

~PDB PATH

WHITEWASHED
BLACKBOX
MARIANASTRENCH

SHARED RESOURCE

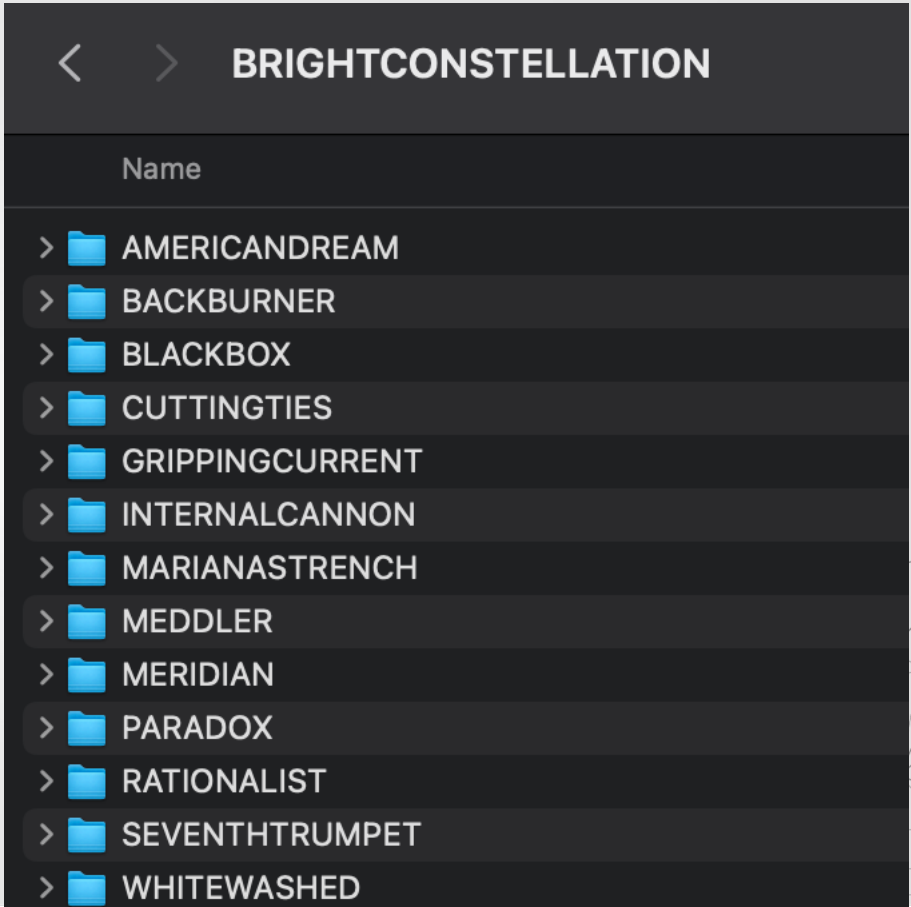
```
$ emit CUTTINGTIES/2c84d4bdd3e892435ceca91a98ebbf21295f596155b2e52be3823b5f9ab2a123 | perc STRING | peek
01.106 kB; 39.38% entropy; data
000: 00 00 0A 00 53 00 6D 00 61 00 72 00 74 00 20 00 43 00 61 00 72 00 64 00 11  ....S.m.a.r.t...C.a.r.d..
019: 00 53 00 6D 00 61 00 72 00 74 00 20 00 43 00 61 00 72 00 64 00 20 00 48 00  .S.m.a.r.t...C.a.r.d...H.
032: 65 00 6C 00 70 00 65 00 72 00 14 00 53 00 6D 00 61 00 72 00 74 00 20 00 43  e.l.p.e.r...S.m.a.r.t...C
04B: 00 61 00 72 00 64 00 20 00 49 00 6E 00 73 00 65 00 72 00 74 00 69 00 6F 00  .a.r.d...I.n.s.e.r.t.i.o.
064: 6E 00 12 00 53 00 6D 00 61 00 72 00 74 00 20 00 43 00 61 00 72 00 64 00 20  n...S.m.a.r.t...C.a.r.d..
07D: 00 52 00 65 00 6D 00 6F 00 76 00 61 00 6C 00 DD 00 4D 00 61 00 6E 00 61 00  .R.e.m.o.v.a.l...M.a.n.a.
096: 67 00 65 00 73 00 20 00 61 00 63 00 63 00 65 00 73 00 73 00 20 00 74 00 6F  g.e.s...a.c.c.e.s.s...t.o
0AF: 00 20 00 73 00 6D 00 61 00 72 00 74 00 20 00 63 00 61 00 72 00 64 00 73 00  ...s.m.a.r.t...c.a.r.d.s.
0C8: 20 00 72 00 65 00 61 00 64 00 20 00 62 00 79 00 20 00 74 00 68 00 69 00 73  ..r.e.a.d...b.y...t.h.i.s
0E1: 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 2E 00 20 00 49 00  ...c.o.m.p.u.t.e.r.....I.
$ emit RATIONALIST/6bd99bc2e343e24409e593d7fe785e59ede4b35f527c2e110a2551dde9025b40 | perc STRING | peek
01.106 kB; 39.38% entropy; data
000: 00 00 0A 00 53 00 6D 00 61 00 72 00 74 00 20 00 43 00 61 00 72 00 64 00 11  ....S.m.a.r.t...C.a.r.d..
019: 00 53 00 6D 00 61 00 72 00 74 00 20 00 43 00 61 00 72 00 64 00 20 00 48 00  .S.m.a.r.t...C.a.r.d...H.
032: 65 00 6C 00 70 00 65 00 72 00 14 00 53 00 6D 00 61 00 72 00 74 00 20 00 43  e.l.p.e.r...S.m.a.r.t...C
04B: 00 61 00 72 00 64 00 20 00 49 00 6E 00 73 00 65 00 72 00 74 00 69 00 6F 00  .a.r.d...I.n.s.e.r.t.i.o.
064: 6E 00 12 00 53 00 6D 00 61 00 72 00 74 00 20 00 43 00 61 00 72 00 64 00 20  n...S.m.a.r.t...C.a.r.d..
07D: 00 52 00 65 00 6D 00 6F 00 76 00 61 00 6C 00 DD 00 4D 00 61 00 6E 00 61 00  .R.e.m.o.v.a.l...M.a.n.a.
096: 67 00 65 00 73 00 20 00 61 00 63 00 63 00 65 00 73 00 73 00 20 00 74 00 6F  g.e.s...a.c.c.e.s.s...t.o
0AF: 00 20 00 73 00 6D 00 61 00 72 00 74 00 20 00 63 00 61 00 72 00 64 00 73 00  ...s.m.a.r.t...c.a.r.d.s.
0C8: 20 00 72 00 65 00 61 00 64 00 20 00 62 00 79 00 20 00 74 00 68 00 69 00 73  ..r.e.a.d...b.y...t.h.i.s
0E1: 00 20 00 63 00 6F 00 6D 00 70 00 75 00 74 00 65 00 72 00 2E 00 20 00 49 00  ...c.o.m.p.u.t.e.r.....I.
```

SURFACE AREA

13 Families Clustered

Still ~35-ish Files

More to Do!



REPEAT

Using just features does not :

- Express how samples related to one-another
- Account for updated versions of the same tool
- Provide resilient detection

04

LET'S GET WEIRD

Evolving our YARA Methods

CAN YARA FIND CODE?

HOW LAZY CAN I BE?

Opening a hex editor takes eyeballs
Disassembly takes skill (not guilty)

But YARA knows some things – like where some code is

CODE EXECUTING SECTIONS

Sections that YARA knows have code AND can execute

```
rule Sector_Hashing {

condition:
    for any var_sect in pe.sections: (
        var_sect.characteristics and (pe.SECTION_CNT_CODE or pe.SECTION_MEM_EXECUTE)
        and
        console.log("SECTOR HASH",
        hash.md5(var_sect.raw_data_offset, 0x100))
        )
}
```

Give us a partial-section (sector) hash

thanks David Cannings & Qutluch <3 <3

BLOCKS OF CODE

```
$ yara ~/Desktop/evil.yar Lamberts/ -r | sort | uniq -c | sort -rn
  17 section hash d41d8cd98f00b204e9800998ecf8427e
   8 SECTOR hash d99eb1e503cac3a1e90450d0c07e3ffc
   7 section hash a1d25fab0f0999169575e729273ac450
   7 section hash 97ce0f6491eda9e959ad7a31f7c5f292
   7 section hash 858cb90d03013fac19c46c642c1611f0
   7 SECTOR hash 2ee541d7be730e72f7b8557218782850
   6 section hash ade88025b419858a8c8cb9da7c7f5173
   6 section hash 9f2ba27d2524b238cb3ce52046c6774a
   6 section hash 9749856b31ec6a427016d7007d70a9f0
   6 section hash 92c98668604ed21149b03e31495acc1b
   6 section hash 06918aea158501659ba39942b836c34f
   6 SECTOR hash 51a9e4c7561700dc9e54babd20e9a804
```

BLOCKS OF CODE

```
rule APT_ZZ_BrightConstellation_RATIONALIST_SectorHash
{
    condition:
        for any var_sect in pe.sections:
        (hash.md5( var_sect.raw_data_offset, 0x100 ) == "d99eb1e503cac3a1e90450d0c07e3ffc" )
}
```

```
$ emit RATIONALIST/15d2669d1e303b226f206c69554d67d121dd6a997b7883cbb081c5b00a3fe259 | vsect .text | snip :0x100 | md5 -t
d99eb1e503cac3a1e90450d0c07e3ffc
$ emit RATIONALIST/15d2669d1e303b226f206c69554d67d121dd6a997b7883cbb081c5b00a3fe259 | vsect .text | snip :0x100 | peek -W 30
------------------------------------------------------------------------------------------------------------------------
00.256 kB; 45.16% entropy; data
------------------------------------------------------------------------------------------------------------------------
000: 33 C0 C3 CC CC CC CC CC CC CC CC CC CC CC CC C3 CC CC CC CC CC CC CC CC CC CC CC CC CC  3...............................
01E: CC CC 3D 80 00 00 00 73 06 B8 01 00 00 00 C3 3D 00 40 00 00 73 06 B8 02 00 00 00 C3 3D 00  ..=....s.......=.@..s.......=.
03C: 00 20 00 73 06 B8 03 00 00 00 C3 3D 00 00 00 10 1B C0 83 C0 05 C3 CC CC CC CC CC CC CC CC  ...s.......=....................
05A: CC CC CC CC CC CC 85 C0 7D 06 B8 0A 00 00 00 C3 3D 80 00 00 00 7D 06 B8 01 00 00 00 C3 3D  ........}.......=....}.......=
078: 00 40 00 00 7D 06 B8 02 00 00 00 C3 3D 00 00 20 00 7D 06 B8 03 00 00 00 C3 33 C9 3D 00 00  .@..}.......=....}.......3.=..
096: 00 10 0F 9D C1 83 C1 04 8B C1 C3 CC CC CC CC CC CC CC CC CC CC CC CC CC CC 85 C0 7D 0B  ..............................}.
0B4: 03 C0 8B C8 83 C8 FF 2B C1 EB 02 03 C0 3D 80 00 00 00 73 06 B8 01 00 00 00 C3 3D 00 40 00  .......+.....=....s.......=.@.
0D2: 00 73 06 B8 02 00 00 00 C3 3D 00 00 20 00 73 06 B8 03 00 00 00 C3 3D 00 00 00 10 1B C0 83  .s.......=....s.......=.......
0F0: C0 05 C3 CC CC CC CC CC CC CC CC CC CC CC CC                                              ................
------------------------------------------------------------------------------------------------------------------------
```


CAN WE DO BETTER?

ENTRY POINT & EXPORTS

```
rule EntryPoint_Partial_Hash
{
    condition:
        console.log("EntryPoint_Partial_Hash: ", hash.md5(pe.entry_point, 20))
}

rule Export_Partial_Hash
{
    condition:
        for all thing in pe.export_details:(
          thing.offset != 0x0 and
          console.log("ExportFunc_Partial_Hash: ", hash.md5(thing.offset, 20)))
}
```

SAVE A HEADACHE

Put most of the YARA rule in output of the console logging

```
rule Export_Partial_Hash
{
    condition:
        for all thing in pe.export_details:(
          thing.offset != 0x0 and
          console.log("rule ExportFunc_Partial_Hash { condition: for any thing in pe.export_details:( thing.offset != 0x0 and
          hash.md5(thing.offset, 20) == ", hash.md5(thing.offset, 20)))
}
```

Ignore format strings (newline/tabs) to sort properly

TIGHTER CLUSTERS

```
rule APT_ZZ_BrightConstellation_MARIANASTRENCH_ExportFunc_Partial_Hash {
    condition:
        for any thing in pe.export_details:(
            thing.offset != 0x0 and
            hash.md5(thing.offset, 20) == "e14e7ac2c4957c6752979ea8644a6099"
            )
}
```

Listing: cad99954df82588ebd1176427559f86dc98543...

```
                        undefined4 __stdcall HandlerEx(int param_1)
undefined4              EAX:4          <RETURN>
int                     Stack[0x4]:4   param_1
                        0x12e8  3  HandlerEx
                        Ordinal_3
                        lpHandlerProc_100012e8
                        HandlerEx
100012e8 8b 44 24 04    MOV        EAX,dword ptr [ESP + param_1]
100012ec 48             DEC        EAX
100012ed 74 0a          JZ         LAB_100012f9
100012ef 48             DEC        EAX
100012f0 74 44          JZ         LAB_10001336
100012f2 48             DEC        EAX
100012f3 74 35          JZ         LAB_1000132a
100012f5 48             DEC        EAX
100012f6 48             DEC        EAX
100012f7 75 1b          JNZ        LAB_10001314

                        LAB_100012f9
100012f9 33 c0          XOR        EAX,EAX
100012fb a3 8c 52       MOV        [DAT_1000528c],EAX
         00 10
10001300 c7 05 84       MOV        dword ptr [DAT_10005284],0x1
         52 00 10
         01 00 00 00
1000130a a3 94 52       MOV        [DAT_10005294],EAX
         00 10
1000130f a3 98 52       MOV        [DAT_10005298],EAX
         00 10
```

Decompile: HandlerEx - (cad99954df82588ebd1176427559f86dc9...

```
1
2  /* WARNING: Globals starting with '_' overlap smaller symbols at the same address */
3  /* lpHandlerProc parameter of RegisterServiceCtrlHandlerExA
4     */
5
6  undefined4 HandlerEx(int param_1)
7
8  {
9                      /* 0x12e8  3  HandlerEx */
10   if (param_1 != 1) {
11     if (param_1 == 2) {
12       _DAT_10005284 = 7;
13       goto LAB_10001314;
14     }
15     if (param_1 == 3) {
16       _DAT_10005284 = 4;
17       goto LAB_10001314;
18     }
19     if (param_1 != 5) goto LAB_10001314;
20   }
21   _DAT_1000528c = 0;
22   _DAT_10005284 = 1;
23   _DAT_10005294 = 0;
24   _DAT_10005298 = 0;
25 LAB_10001314:
26   SetServiceStatus(hServiceStatus_1000529c,(LPSERVICE_STATUS)&lpServiceStatus_10005280
27   return 0;
28 }
29
```

SOME WINS!

EXPORT HASHING

CUTTINGTIES
MARIANASTRENCH
BLOODLETTER

ENTRYPOINT HASHING

BLACKBOX
INVISIBLEENEMY
MARIANASTRENCH
RATIONALIST
EXISTENCE

DATA DIR HASHING

AMERICANDREAM
INVISIBLEENEMY
MARIANASTRENCH

SECTOR HASHING

BACKBURNER
BLOODLETTER
PARAMOUNT
SEVENTHTRUMPET
WHITEWASHED
AMERICANDREAM


OUTFOX OURSELVES

NOT CODE BUT

We could hash each PE data directory?

Why? Cause Wes questioned if it would work

```
$ yara ~/Desktop/Testing/code_overlap_brrrr.yar Lamberts/ -r | sort | uniq -c | sort -rn | grep -v d41d8cd98f00b204e9800998ecf8427e | grep pe.data_directories
   9 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_RESOURCE].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_RESOURCE].size) == df212b863f4d8f862d3090b75aa7e7d5
   9 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_EXPORT].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_EXPORT].size) == 39f247ca938e8fbe15ec5560bf3c400d
   9 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT].size) == bfbe2be892e4cc41f5f0f6e621e33c0f
   6 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_TLS].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_TLS].size) == 3e4d06eefe1df446e9be15d6e425d9c3
   6 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_IMPORT].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_IMPORT].size) == 49d845b4a643044c8797dd8c25e0d978
   6 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_IAT].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_IAT].size) == 9c08b392f7a8577f997faac5eecc0eeb
   6 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_BASERELOC].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_BASERELOC].size) == d484dba4f272a335039295e20cca78fd
   5 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG].size) == 5e1477de2b9cf70fa363599481915c0f
   5 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_IMPORT].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_IMPORT].size) == 390aad75ea9c6c47e88e1f1ceec13871
   5 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_IMPORT].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_IMPORT].size) == 268a2a7064f3aa9bfc14a84cbdcb7634
   5 hash.md5(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_IMPORT].virtual_address),pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_IMPORT].size) == 093ce688523835d93407bc1fd65add38
```

```
rule APT_ZZ_BrightConstellation_INTERNALCANNON_Data_Dir_CONFIG {
     condition:
        hash.md5(
            pe.rva_to_offset(
                pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG].virtual_address),
                    pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG].size)
                == "b0ec5ec4a00eff6f182d0e042481033b"
}
```

WHAT IF ... ??

What if we hash the ENDS of the sections that can execute code??

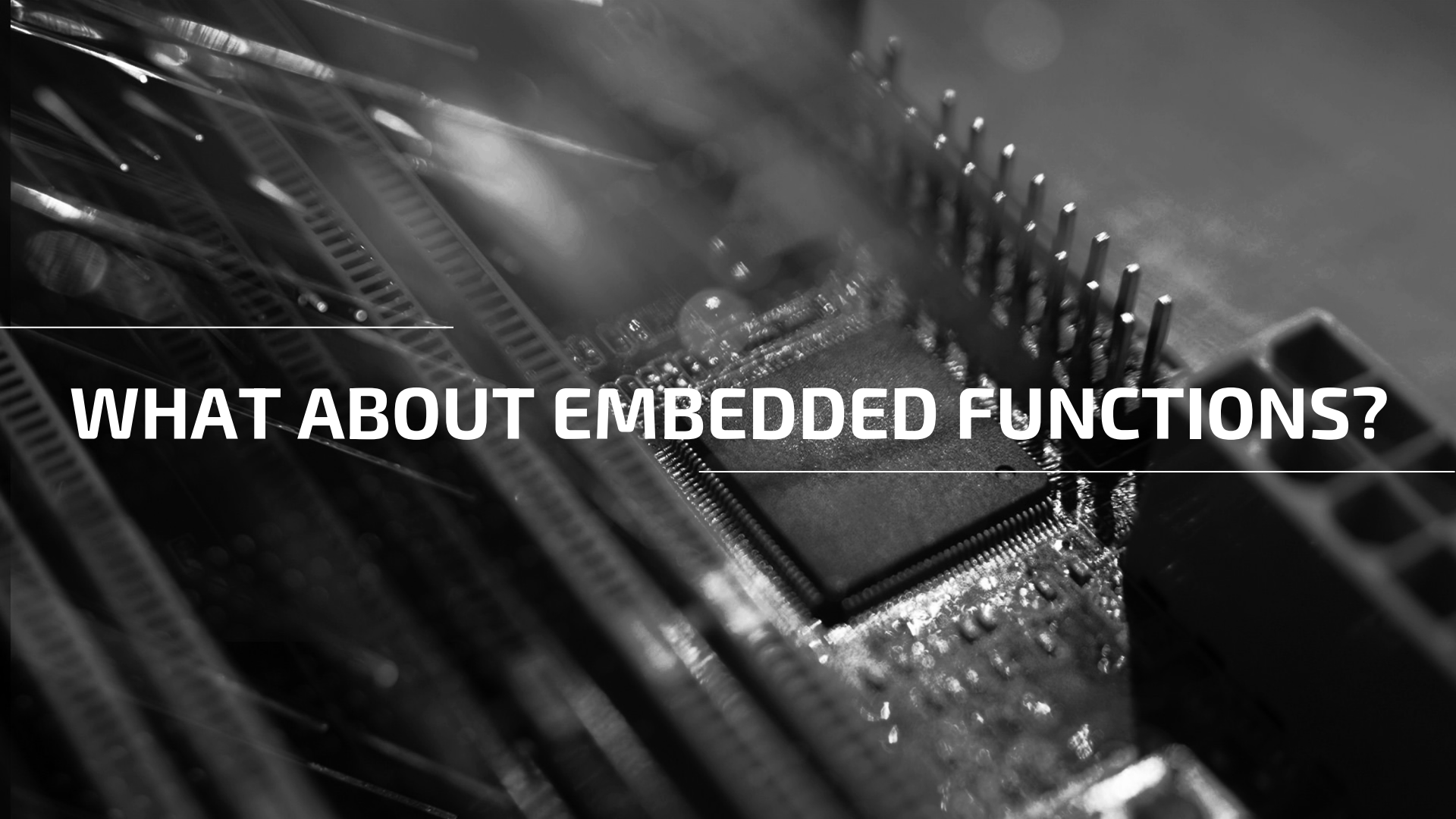
```
rule Last_sector_of_Section_hash {
    condition: for any var_sect in pe.sections: (
    hash.md5((
        (var_sect.raw_data_offset+var_sect.raw_data_size) - 0x100)
        , 0x100 ) == "89d30305ecf9937fec80e52e9ded52c9"
)
}
```

WHAT IF ... ??

You find incorrect overlaps

```
$ emit 1eede29007619d207842ddcaadf41b17b47a456004df43189d1f6cf54a3b785b | vsect .rsrc | snip 0x194f9: | peek -W 25
--------------------------------------------------------------------------------------------------------
00.263 kB; 34.36% entropy; ASCII text, with no line terminators
--------------------------------------------------------------------------------------------------------
000: 41 44 44 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 49 4E 47 58 58 50  ADDINGXXPADDINGPADDINGXXP
019: 41 44 44 49 4E 47 50 41 44 44 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44  ADDINGPADDINGXXPADDINGPAD
032: 44 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 49 4E 47 58 58 50 41 44  DINGXXPADDINGPADDINGXXPAD
04B: 44 49 4E 47 50 41 44 44 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 49  DINGPADDINGXXPADDINGPADDI
064: 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 49 4E 47 58 58 50 41 44 44 49  NGXXPADDINGPADDINGXXPADDI
07D: 4E 47 50 41 44 44 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 49 4E 47  NGPADDINGXXPADDINGPADDING
096: 58 58 50 41 44 44 49 4E 47 50 41 44 44 49 4E 47 58 58 50 41 44 44 49 4E 47  XXPADDINGPADDINGXXPADDING
0AF: 50 41 44 44 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 49 4E 47 58 58  PADDINGXXPADDINGPADDINGXX
0C8: 50 41 44 44 49 4E 47 50 41 44 44 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41  PADDINGPADDINGXXPADDINGPA
0E1: 44 44 49 4E 47 58 58 50 41 44 44 49 4E 47 50 41 44 44 49 4E 47 58 58 50 41  DDINGXXPADDINGPADDINGXXPA
--------------------------------------------------------------------------------------------------------
```

Good at finding specific volume of padding?


WHAT ABOUT EMBEDDED FUNCTIONS?

FIND CALLED FUNCTIONS

```
rule console_entrypoint_called_funcs {
    condition:
        for all i in (pe.entry_point .. pe.entry_point+25):
            (
            uint8(i) == 0xe8
            and console.log("called function partial hash: ",
            hash.md5((int32(i+1)) + (i+5), 14))
            )
}
```

FIND CALLED FUNCTIONS FROM EXPORTS

```
rule console_export_called_funcs {

    condition:
        for all exp in pe.export_details: (
            for all i in (exp.offset .. exp.offset+25):
                (
                    uint8(i) == 0xe8
                    and console.log("called function in export hash: ",
                    hash.md5((int32(i+1)) + (i+5), 14))
                )
        )
}
```

FIND CALLED FUNCTIONS FROM EXPORTS

```
rule APT_ZZ_BrightConstellation_ESCAPEARTIST_ExportFunc_Calls
{

    condition:
    for any exp in pe.export_details: (
        for any i in (exp.offset .. exp.offset+25):
            (
            uint8(i) == 0xe8
            and (
                hash.md5((int32(i+1)) + (i+5), 14) == "ae7bcdd3baca438db51eeb78b318106e"
             )))
}
```

```
                    ****************************************
                    DWORD __stdcall Ordinal_1(void)
          DWORD       EAX:4          <RETURN>
                    0x4678  1
                    Ordinal_1
00404678 8b ff        MOV         EDI,EDI
0040467a 56           PUSH        ESI
0040467b 6a 01        PUSH        0x1
0040467d ff 35 68     PUSH        dword ptr [DAT_0044ca68]
         ca 44 00
00404683 e8 5a 7a     CALL        FUN_0040c0e2
         00 00
00404688 8b f0        MOV         ESI,EAX
0040468a 56           PUSH        ESI
0040468b e8 ff ec     CALL        FUN_0043338f
         02 00
```

```
1
2  DWORD Ordinal_1(void)
3
4  {
5    DWORD DVar1;
6
7                        /* 0x4678  1   */
8    DVar1 = FUN_0040c0e2(DAT_0044ca68,1);
9    FUN_0043338f(DVar1);
10   return DVar1;
11 }
12
```

FIND CALLED FUNCTIONS FROM EXPORTS

```
rule APT_ZZ_BrightConstellation_ESCAPEARTIST_ExportFunc_Calls
{

    condition:
    for any exp in pe.export_details: (
        for any i in (exp.offset .. exp.offset+25):
            (
            uint8(i) == 0xe8
            and (
                hash.md5((int32(i+1)) + (i+5), 14) == "ae7bcdd3baca438db51eeb78b318106e"
             )))
}
```

```
0043338f 8b ff          MOV         EDI,EDI
00433391 55             PUSH        EBP
00433392 8b ec          MOV         EBP,ESP
00433394 ff 75 08       PUSH        dword ptr [EBP + param_1]
00433397 68 00 02       PUSH        0x200
         00 00
0043339c 68 80 27       PUSH        DAT_00452780
         45 00
004333a1 6a 00          PUSH        0x0
004333a3 68 c0 2d       PUSH        DAT_00402dc0
         40 00
004333a8 e8 03 7e       CALL        FUN_0043b1b0
         00 00
004333ad 83 c4 10       ADD         ESP,0x10
004333b0 50             PUSH        EAX
004333b1 ff 15 94       CALL        dword ptr [->MSVCRT.DLL::printf]
         11 40 00
```

IDIOTIC ITERATION

```
rule funcs_on_funcs_on_funcs {
    condition:
        for all i in (pe.entry_point+15 .. pe.entry_point+30):
            (
            uint8(i) == 0xe8
            and
                for all j in ((int32(i+1) + (i+5)) .. ((int32(i+1) + (i+5)) + 30)):
                (
                uint8(j) == 0xe8 and
                console.log("teriarty_func_hash: ", hash.md5((int32(j+1) + (j+5)), 15))
                )
            )
}
```

USE CASE?

Introduces provenance: detect function & where it came from

May be a useful last resort?

Testing on absolute calls (0xff) was useless -> usually pointers to imported Win APIs

MORE WINS!

EXPORT CALLED FUNC HASHING

BLACKBOX
ESCAPEARTIST

ENTRYPOINT CALLED FUNC HASHING

BLACKBOX
GRIPPINGCURRENT
INVISIBLEENEMY
RATIONALIST

TERTIARY FUNCTION HASHING

BLACKBOX

Name	Date Modified	Size	Kind
AMERICANDREAM	Today at 8:58 AM	--	Folder
BACKBURNER	Today at 8:58 AM	--	Folder
BLACKBOX	Today at 8:58 AM	--	Folder
BLOODLETTER	Today at 8:58 AM	--	Folder
COMPOSURE	Today at 8:59 AM	--	Folder
CUTTINGTIES	Today at 8:59 AM	--	Folder
ESCAPEARTIST	Today at 8:59 AM	--	Folder
EXISTENCE	Today at 8:59 AM	--	Folder
GRIPPINGCURRENT	Today at 8:59 AM	--	Folder
INTERNALCANNON	Today at 9:00 AM	--	Folder
INVISIBLEENEMY	Today at 9:00 AM	--	Folder
LEVELER	Today at 9:00 AM	--	Folder
LIGHTHOUSE	Today at 9:00 AM	--	Folder
MARIANASTRENCH	Today at 9:00 AM	--	Folder
MEDDLER	Today at 9:00 AM	--	Folder
MERIDIAN	Today at 9:00 AM	--	Folder
PARADOX	Today at 9:00 AM	--	Folder
PARAMOUNT	Today at 9:00 AM	--	Folder
RATIONALIST	Today at 9:00 AM	--	Folder
SEVENTHTRUMPET	Today at 9:01 AM	--	Folder
WHITEWASHED	Today at 9:01 AM	--	Folder

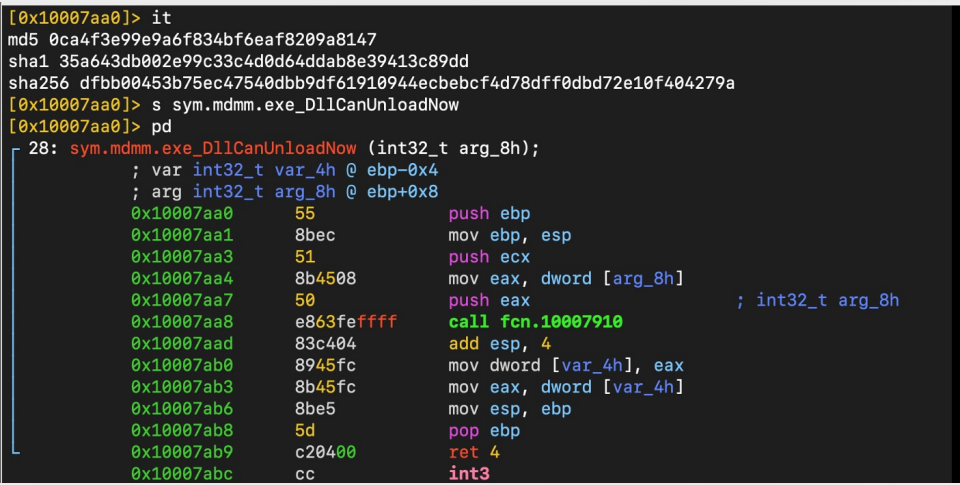
05

STARING AT THE ABYSS

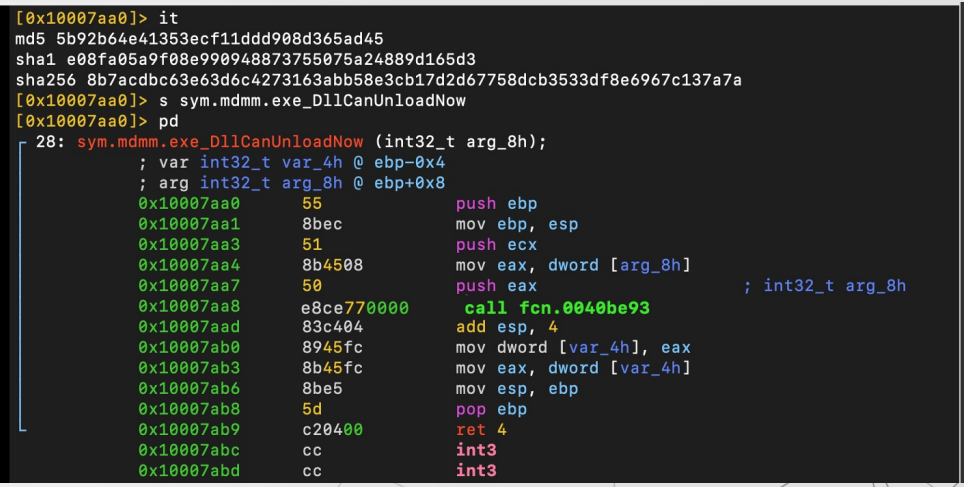
Using Python-based Tooling to Draw Our Linkages

REALLY FIND CODE

We MUST disassemble



```
[0x10007aa0]> it
md5 0ca4f3e99e9a6f834bf6eaf8209a8147
sha1 35a643db002e99c33c4d0d64ddab8e39413c89dd
sha256 dfbb00453b75ec47540dbb9df61910944ecbebcf4d78dff0dbd72e10f404279a
[0x10007aa0]> s sym.mdmm.exe_DllCanUnloadNow
[0x10007aa0]> pd
┌ 28: sym.mdmm.exe_DllCanUnloadNow (int32_t arg_8h);
│           ; var int32_t var_4h @ ebp-0x4
│           ; arg int32_t arg_8h @ ebp+0x8
│           0x10007aa0      55              push ebp
│           0x10007aa1      8bec            mov ebp, esp
│           0x10007aa3      51              push ecx
│           0x10007aa4      8b4508          mov eax, dword [arg_8h]
│           0x10007aa7      50              push eax                    ; int32_t arg_8h
│           0x10007aa8      e863feffff      call fcn.10007910
│           0x10007aad      83c404          add esp, 4
│           0x10007ab0      8945fc          mov dword [var_4h], eax
│           0x10007ab3      8b45fc          mov eax, dword [var_4h]
│           0x10007ab6      8be5            mov esp, ebp
│           0x10007ab8      5d              pop ebp
└           0x10007ab9      c20400          ret 4
            0x10007abc      cc              int3
```



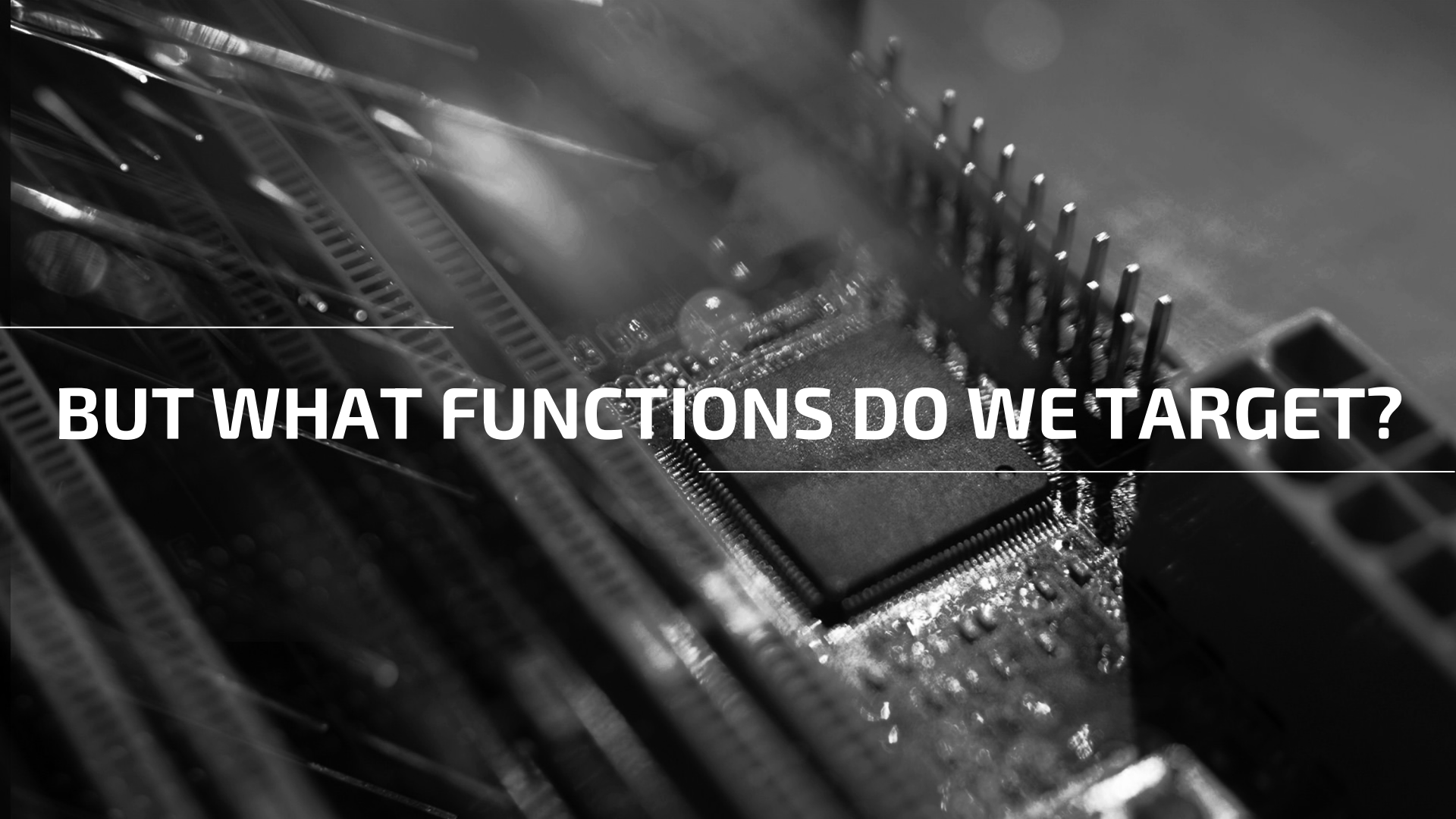
```
[0x10007aa0]> it
md5 5b92b64e41353ecf11ddd908d365ad45
sha1 e08fa05a9f08e990948873755075a24889d165d3
sha256 8b7acdbc63e63d6c4273163abb58e3cb17d2d67758dcb3533df8e6967c137a7a
[0x10007aa0]> s sym.mdmm.exe_DllCanUnloadNow
[0x10007aa0]> pd
┌ 28: sym.mdmm.exe_DllCanUnloadNow (int32_t arg_8h);
│           ; var int32_t var_4h @ ebp-0x4
│           ; arg int32_t arg_8h @ ebp+0x8
│           0x10007aa0      55              push ebp
│           0x10007aa1      8bec            mov ebp, esp
│           0x10007aa3      51              push ecx
│           0x10007aa4      8b4508          mov eax, dword [arg_8h]
│           0x10007aa7      50              push eax                    ; int32_t arg_8h
│           0x10007aa8      e8ce770000      call fcn.0040be93
│           0x10007aad      83c404          add esp, 4
│           0x10007ab0      8945fc          mov dword [var_4h], eax
│           0x10007ab3      8b45fc          mov eax, dword [var_4h]
│           0x10007ab6      8be5            mov esp, ebp
│           0x10007ab8      5d              pop ebp
└           0x10007ab9      c20400          ret 4
            0x10007abc      cc              int3
            0x10007abd      cc              int3
```

And account for changes to addresses

ID FUNCS WITH RIZIN

```
[0x004158ae]> afll
addr       name   size xrefsTo xrefsFrom calls nbbs edges cc cost noreturn min bound  range max bound  locals args frame loops
-------------------------------------------------------------------------------------------------------------------------------
0x004158ae entry0 435  9       45        16    42   60    20 208  false    0x00415606 690   0x004158b8 6      0    44    4
0x0040d49a main   310  5       32        14    21   33    14 141  false    0x0040d49a 310   0x0040d5d0 8      0    40    0
```

```
[0x004158ae]> afll~$!3:2
Do you want to print 678 lines? (y/N) y
addr       name                                size xrefsTo xrefsFrom calls nbbs edges cc cost noreturn min bound  range max bound  locals args frame loops
-------------------------------------------------------------------------------------------------------------------------------------------------------------
0x00415474 fcn.00415474                        59   133     1         0     1    0     1  21   false    0x00415474 59    0x004154af 5      1    24    0
0x004154af fcn.004154af                        17   132     0         0     1    0     1  11   false    0x004154af 17    0x004154c0 1      0    0     0
0x0040ebb7 fcn.0040ebb7                        31   103     2         2     3    2     3  22   false    0x0040ebb7 31    0x0040ebd6 0      1    12    0
0x00411225 fcn.00411225                        192  94      5         2     17   24    9  96   false    0x00411225 192   0x004112e5 3      1    32    0
0x00402f10 fcn.00402f10                        134  90      1         1     9    11    6  63   false    0x00402f10 243   0x00403003 1      1    24    0
0x0040eb7d fcn.0040eb7d                        20   62      2         2     1    0     1  14   false    0x0040eb7d 20    0x0040eb91 0      1    12    0
0x0040eb26 fcn.0040eb26                        5    47      1         0     1    1     0  2    false    0x0040eb26 5     0x0040eb2b 0      0    8     1
0x00403440 fcn.00403440                        93   46      8         6     9    13    6  63   false    0x00403440 93    0x0040349d 0      1    16    0
0x00401320 fcn.00401320                        627  28      33        5     68   90    63 331  false    0x00401320 627   0x00401593 0      1    24    4
0x0040eada fcn.0040eada                        30   27      0         0     4    5     3  18   false    0x0040eada 30    0x0040eaf8 0      3    4     0
0x00410f98 fcn.00410f98                        20   26      2         2     1    0     1  14   false    0x00410f98 20    0x00410fac 0      1    12    0
0x00407416 fcn.00407416                        22   26      2         1     1    0     1  10   false    0x00407416 22    0x0040742c 0      2    12    0
0x00410fac fcn.00410fac                        20   25      2         2     1    0     1  14   false    0x00410fac 20    0x00410fc0 0      1    12    0
```


BUT WHAT FUNCTIONS DO WE TARGET?

LET FLOSS DECIDE

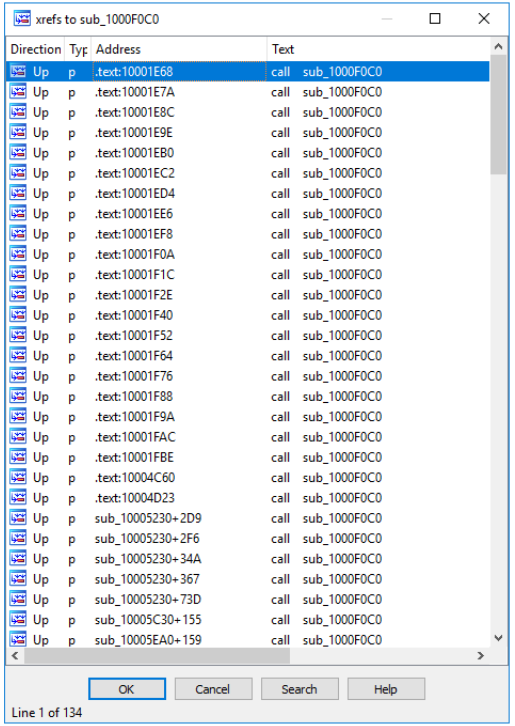
Mandiant Tool – Thanks Willi & Moritz for your Help!!

```
$ floss 487c1bdb65634a794fa5e359c383c94945ce9f0806fcad46440e919ba0e6166e -x

CreateNamedPipeA finished with Error-%d
http://%s%s
http://toysbagonline.com/reviews
http://purewatertokyo.com/list
http://pinkgoat.com/input
http://yellowlion.com/remove
http://salmonrabbit.com/find
http://bluecow.com/input

Most likely decoding functions: 487c1bdb65634a794fa5e359c383c94945ce9f0806fcad46440e919ba0e6166e
address       score
----------  -------
0x1000F0C0  1.24067
0x10002020  1.168
0x1000F290  1.09133
0x1000BD70  1.08467
0x10008CE0  1.08467
0x1001E48E  1.07067
0x10002960  1.004
0x100180BC  0.95133
0x10002630  0.872
0x1000F3F0  0.87067
```

```
. .text:10001EDC     mov     ds:672030h, eax
. .text:10001EE1     push    66AB6Ch
. .text:10001EE6     call    sub_1000F0C0
. .text:10001EEB     add     esp, 4
. .text:10001EEE     mov     ds:672034h, eax
. .text:10001EF3     push    66AB7Ch
. .text:10001EF8     call    sub_1000F0C0
. .text:10001EFD     add     esp, 4
. .text:10001F00     mov     ds:672038h, eax
. .text:10001F05     push    66AB8Ch
. .text:10001F0A     call    sub_1000F0C0
. .text:10001F0F     add     esp, 4
. .text:10001F12     mov     ds:67203Ch, eax
. .text:10001F17     push    66ABA0h
. .text:10001F1C     call    sub_1000F0C0
. .text:10001F21     add     esp, 4
. .text:10001F24     mov     ds:672040h, eax
. .text:10001F29     push    66ABB0h
. .text:10001F2E     call    sub_1000F0C0
. .text:10001F33     add     esp, 4
. .text:10001F36     mov     ds:672044h, eax
. .text:10001F3B     push    66ABC0h
. .text:10001F40     call    sub_1000F0C0
. .text:10001F45     add     esp, 4
. .text:10001F48     mov     ds:672048h, eax
. .text:10001F4D     push    66ABD0h
. .text:10001F52     call    sub_1000F0C0
. .text:10001F57     add     esp, 4
. .text:10001F5A     mov     ds:67204Ch, eax
. .text:10001F5F     push    66ABE0h
. .text:10001F64     call    sub_1000F0C0
. .text:10001F69     add     esp, 4
. .text:10001F6C     mov     ds:672050h, eax
. .text:10001F71     push    66ABF0h
. .text:10001F76     call    sub_1000F0C0
. .text:10001F7B     add     esp, 4
. .text:10001F7E     mov     ds:672054h, eax
```



FLOSS 2.0

Uses vivisect emulation to find likely decoding functions

Use those functions as a feeder for disassembly

```
def get_floss_funcs(file):
  candidates = []
  vw = viv_utils.getWorkspace(file)
  functions = vw.getFunctions()
  func_features, lib_funcs = floss.identify.find_decoding_function_features(vw, functions)
  # dict from function VA (int) to score (float)
  func_scores = {
      fva: features["score"]
      for fva, features in func_features.items()
  }

  # list of tuples (score (float), function VA (int)) sorted descending
  func_scores = sorted([
      (score, fva)
      for fva, score in func_scores.items()
  ], reverse=True)
  for score, fva in func_scores:
    if score > 0.90: # can we make this a user-input variable? or just take the top 5 highest scoring funcs?
      offset = f"{fva:x}"
      func = offset.lower()
      candidates.append(func)
  return candidates
```

RIZIN

Use Rizin to disassemble

```python
class FileAnalysis(object):
    """Holds the strategies and file information as well as the rz p

    def __init__(self, filepath:str, strategies:list):
        """
        self.rz = rzpipe.open(filepath)
        self.rz.cmd("aaaa")
        self.file_hash = json.loads(self.rz.cmd("itj"))['sha256']
        self.file_path = filepath

        self.strategies = []
        for each in strategies:
            if not issubclass(each, FunctionFinder):
                raise ValueError(f"{type(each)} is not a FunctionFinder")
            self.strategies.append(each)

        self.interesting_function_addrs = defaultdict(list)
        self.functions = []
```

```python
def floss_func_parsing(file):
    analysis = FileAnalysis(file, [])
    funclist = processing.get_floss_funcs(file)
    rz = analysis.rz
    rz.cmd('aaaa')
    json_blob = rz.cmd('aflj')
    data = json.loads(json_blob)
    for func in data:
        for name in funclist:
            if name in func['name']:
                if func['size'] > 50:
                    if func['size'] < 600:
                        fun = FunctionFeature(rz, name)
                        print(fun)
                        analysis.functions.append(fun)

    rz.cmd('q')
    return analysis
```

RIZIN

Use Rizin to zignature (masking!)

```python
# Get the signature output
raw_data = rz.cmd("zj")
if len(raw_data) == 0:
  raise Exception(f"Failed to get data from signature for {symbol}")
```

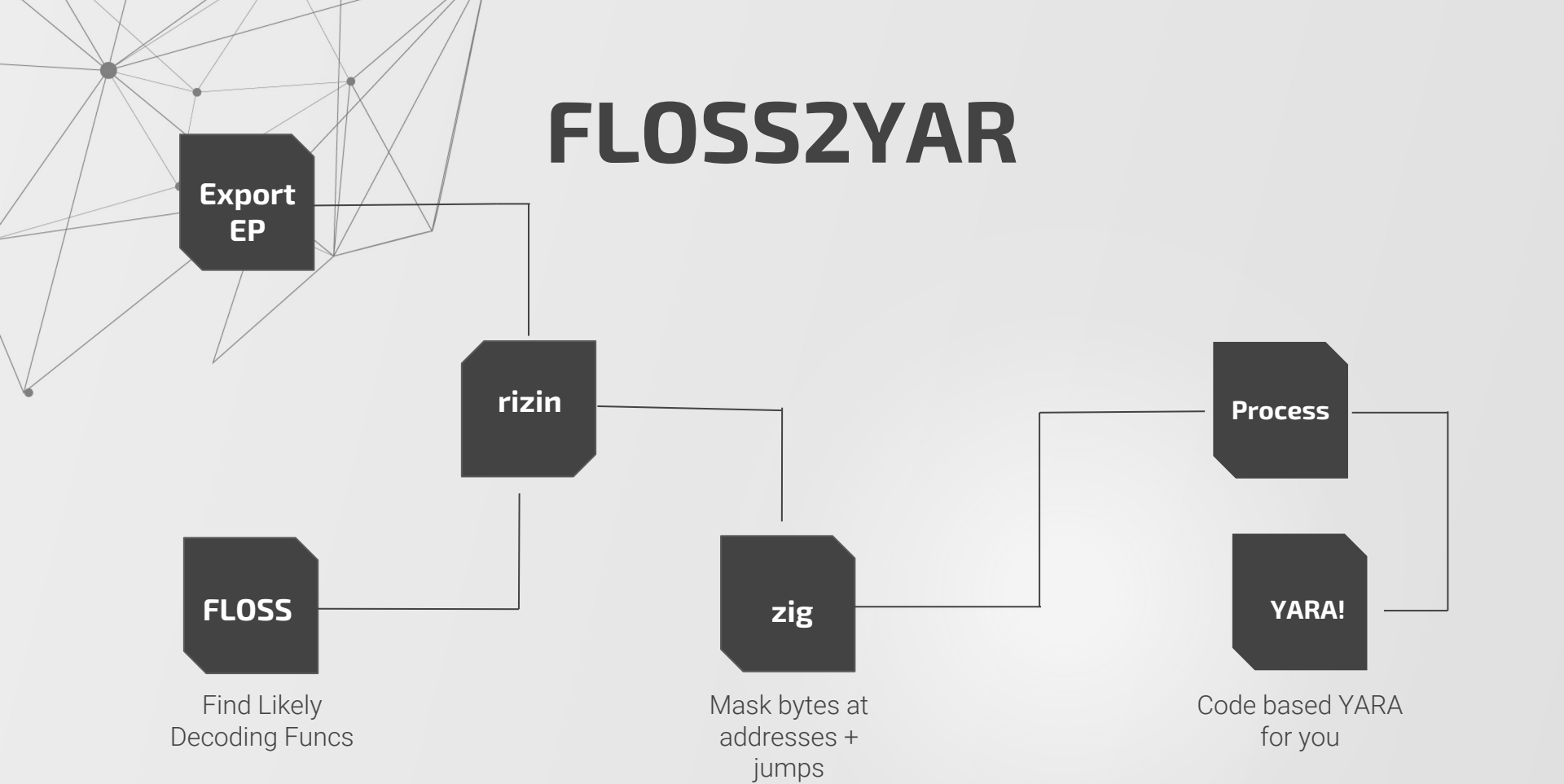
```python
def masked_asm_str(self) -> str:
  """Return an ascii hex string with ?? masking out parts of the instruction"""
  if self._masked_asm_str is not None:
    return self._masked_asm_str

  ret_str = []
  for x,y in zip(self.bytes, self.mask):
    if x & y == 0:
      ret_str.append("??")
    else:
      ret_str.append(f"{x & y:02X}")
  self._masked_asm_str = " ".join(ret_str)
  return self._masked_asm_str
```

```
rule floss2yar_fcn_00417b22 {
meta:
        author = "floss2yar"
        date = "2022-08-20"
        version = "1.0"
        hash = "39b8f93cdffa0c7a3210b7b39483c535a339fbd150d0d5f36cd0783350d367c3"

strings:
        $fcn_00417b22 = {8B FF 55 8B EC 53 56 8B 75 08 57 8B F9 0F BE 47 08 8A 4E 08 56 88 4F 08 57 88 46 08 E8 ?? ?? ?? ?? 8B 5E 08 8B 57
08 C1 E3 17 C1 FB 17 33 DA 8B C2 C1 E0 17 B9 ?? ?? ?? ?? C1 F8 1F 23 D9 33 DA 89 5F 08 C1 E0 08 33 46 08 5F 23 C1 31 46 08 5E 5B 5D C2 04 ?
?}
 /*
            ; CALL XREF from fcn.00419d1e @ 0x419d41
┌ fcn.00417b22 (int32_t arg_8h);
            ; arg int32_t arg_8h @ ebp+0x8
            0x00417b22      8bff           mov   edi, edi
            0x00417b24      55             push  ebp
            0x00417b25      8bec           mov   ebp, esp
            0x00417b27      53             push  ebx
            0x00417b28      56             push  esi
            0x00417b29      8b7508         mov   esi, dword [arg_8h]
            0x00417b2c      57             push  edi
            0x00417b2d      8bf9           mov   edi, ecx
            0x00417b2f      0fbe4708       movsx eax, byte [edi + 8]
            0x00417b33      8a4e08         mov   cl, byte [esi + 8]
            0x00417b36      56             push  esi                   ; int32_t arg_8h
            0x00417b37      884f08         mov   byte [edi + 8], cl
            0x00417b3a      57             push  edi                   ; int32_t arg_ch
            0x00417b3b      884608         mov   byte [esi + 8], al
            0x00417b3e      e8a0feffff     call  fcn.004179e3
            0x00417b43      8b5e08         mov   ebx, dword [esi + 8]
            0x00417b46      8b5708         mov   edx, dword [edi + 8]
            0x00417b49      c1e317         shl   ebx, 0x17
            0x00417b4c      c1fb17         sar   ebx, 0x17
            0x00417b4f      33da           xor   ebx, edx
            0x00417b51      8bc2           mov   eax, edx
            0x00417b53      c1e017         shl   eax, 0x17
            0x00417b56      b900010000     mov   ecx, 0x100            ; 256
            0x00417b5b      c1f81f         sar   eax, 0x1f
            0x00417b5e      23d9           and   ebx, ecx
```

FLOSS2YAR


Export EP
rizin
Process
FLOSS
zig
YARA!
Find Likely Decoding Funcs
Mask bytes at addresses + jumps
Code based YARA for you

LIMITATIONS

Can miss functions

May catch legitimate or statically-linked lib functions

No databasing / whitelisting

Future:

- basic blocks
- rules based on capability or functionality

ALTERNATIVES

yara-signator

Binlex

Intezer

KTAE

I built it to learn not compete :)

The Lamberts APT

```
.00016D87: 6A10      push    010
.00016D89: 8811      mov     [ecx],dl
.00016D8B: 8A5001    mov     dl,[eax][1]
.00016D8E: 325301    xor     dl,[ebx][1]
.00016D91: 885101    mov     [ecx][1],dl
.00016D94: 8A5002    mov     dl,[eax][2]
.00016D97: 325302    xor     dl,[ebx][2]
.00016D9A: 885102    mov     [ecx][2],dl
.00016D9D: 8A5003    mov     dl,[eax][3]
.00016DA0: 325303    xor     dl,[ebx][3]
.00016DA3: 885103    mov     [ecx][3],dl
.00016DA6: 8A5004    mov     dl,[eax][4]
.00016DA9: 325304    xor     dl,[ebx][4]
.00016DAC: 885104    mov     [ecx][4],dl
.00016DAF: 8A5005    mov     dl,[eax][5]
.00016DB2: 325305    xor     dl,[ebx][5]
.00016DB5: 885105    mov     [ecx][5],dl
.00016DB8: 8A5006    mov     dl,[eax][6]
.00016DBB: 325306    xor     dl,[ebx][6]
.00016DBE: 885106    mov     [ecx][6],dl
.00016DC1: 8A5007    mov     dl,[eax][7]
.00016DC4: 325307    xor     dl,[ebx][7]
.00016DC7: 885107    mov     [ecx][7],dl
.00016DCA: 8A5008    mov     dl,[eax][8]
.00016DCD: 325308    xor     dl,[ebx][8]
.00016DD0: 885108    mov     [ecx][8],dl
.00016DD3: 8A5009    mov     dl,[eax][9]
.00016DD6: 325309    xor     dl,[ebx][9]
.00016DD9: 885109    mov     [ecx][9],dl
.00016DDC: 8A500A    mov     dl,[eax][00A]
.00016DDF: 32530A    xor     dl,[ebx][00A]
.00016DE2: 88510A    mov     [ecx][00A],dl
.00016DE5: 8A500B    mov     dl,[eax][00B]
.00016DE8: 32530B    xor     dl,[ebx][00B]
.00016DEB: 88510B    mov     [ecx][00B],dl
.00016DEE: 8A500C    mov     dl,[eax][00C]
.00016DF1: 32530C    xor     dl,[ebx][00C]
.00016DF4: 88510C    mov     [ecx][00C],dl
```

WhiteLambert 1.2 driver

2f60906ca535eb958389e6aed454c2a2

```
.0040D8FB: 6A10      push    010
.0040D8FD: 8811      mov     [ecx],dl
.0040D8FF: 8A5001    mov     dl,[eax][1]
.0040D902: 325301    xor     dl,[ebx][1]
.0040D905: 885101    mov     [ecx][1],dl
.0040D908: 8A5002    mov     dl,[eax][2]
.0040D90B: 325302    xor     dl,[ebx][2]
.0040D90E: 885102    mov     [ecx][2],dl
.0040D911: 8A5003    mov     dl,[eax][3]
.0040D914: 325303    xor     dl,[ebx][3]
.0040D917: 885103    mov     [ecx][3],dl
.0040D91A: 8A5004    mov     dl,[eax][4]
.0040D91D: 325304    xor     dl,[ebx][4]
.0040D920: 885104    mov     [ecx][4],dl
.0040D923: 8A5005    mov     dl,[eax][5]
.0040D926: 325305    xor     dl,[ebx][5]
.0040D929: 885105    mov     [ecx][5],dl
.0040D92C: 8A5006    mov     dl,[eax][6]
.0040D92F: 325306    xor     dl,[ebx][6]
.0040D932: 885106    mov     [ecx][6],dl
.0040D935: 8A5007    mov     dl,[eax][7]
.0040D938: 325307    xor     dl,[ebx][7]
.0040D93B: 885107    mov     [ecx][7],dl
.0040D93E: 8A5008    mov     dl,[eax][8]
.0040D941: 325308    xor     dl,[ebx][8]
.0040D944: 885108    mov     [ecx][8],dl
.0040D947: 8A5009    mov     dl,[eax][9]
.0040D94A: 325309    xor     dl,[ebx][9]
.0040D94D: 885109    mov     [ecx][9],dl
.0040D950: 8A500A    mov     dl,[eax][00A]
.0040D953: 32530A    xor     dl,[ebx][00A]
.0040D956: 88510A    mov     [ecx][00A],dl
.0040D959: 8A500B    mov     dl,[eax][00B]
.0040D95C: 32530B    xor     dl,[ebx][00B]
.0040D95F: 88510B    mov     [ecx][00B],dl
.0040D962: 8A500C    mov     dl,[eax][00C]
.0040D965: 32530C    xor     dl,[ebx][00C]
.0040D968: 88510C    mov     [ecx][00C],dl
```

BlackLambert font exploit

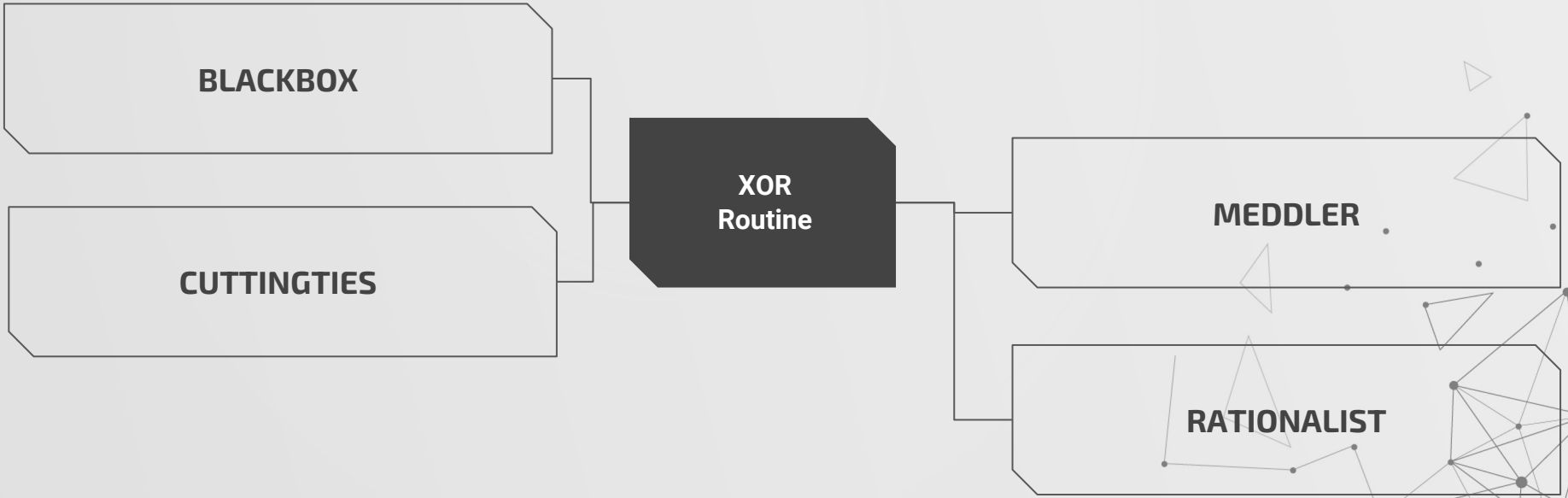
99ef1e473ac553cf80f6117b2e95e79b

```
.0040C76B: 6A10      push    010
.0040C76D: 8811      mov     [ecx],dl
.0040C76F: 8A5001    mov     dl,[eax][1]
.0040C772: 325301    xor     dl,[ebx][1]
.0040C775: 885101    mov     [ecx][1],dl
.0040C778: 8A5002    mov     dl,[eax][2]
.0040C77B: 325302    xor     dl,[ebx][2]
.0040C77E: 885102    mov     [ecx][2],dl
.0040C781: 8A5003    mov     dl,[eax][3]
.0040C784: 325303    xor     dl,[ebx][3]
.0040C787: 885103    mov     [ecx][3],dl
.0040C78A: 8A5004    mov     dl,[eax][4]
.0040C78D: 325304    xor     dl,[ebx][4]
.0040C790: 885104    mov     [ecx][4],dl
.0040C793: 8A5005    mov     dl,[eax][5]
.0040C796: 325305    xor     dl,[ebx][5]
.0040C799: 885105    mov     [ecx][5],dl
.0040C79C: 8A5006    mov     dl,[eax][6]
.0040C79F: 325306    xor     dl,[ebx][6]
.0040C7A2: 885106    mov     [ecx][6],dl
.0040C7A5: 8A5007    mov     dl,[eax][7]
.0040C7A8: 325307    xor     dl,[ebx][7]
.0040C7AB: 885107    mov     [ecx][7],dl
.0040C7AE: 8A5008    mov     dl,[eax][8]
.0040C7B1: 325308    xor     dl,[ebx][8]
.0040C7B4: 885108    mov     [ecx][8],dl
.0040C7B7: 8A5009    mov     dl,[eax][9]
.0040C7BA: 325309    xor     dl,[ebx][9]
.0040C7BD: 885109    mov     [ecx][9],dl
.0040C7C0: 8A500A    mov     dl,[eax][00A]
.0040C7C3: 32530A    xor     dl,[ebx][00A]
.0040C7C6: 88510A    mov     [ecx][00A],dl
.0040C7C9: 8A500B    mov     dl,[eax][00B]
.0040C7CC: 32530B    xor     dl,[ebx][00B]
.0040C7CF: 88510B    mov     [ecx][00B],dl
.0040C7D2: 8A500C    mov     dl,[eax][00C]
.0040C7D5: 32530C    xor     dl,[ebx][00C]
.0040C7D8: 88510C    mov     [ecx][00C],dl
```

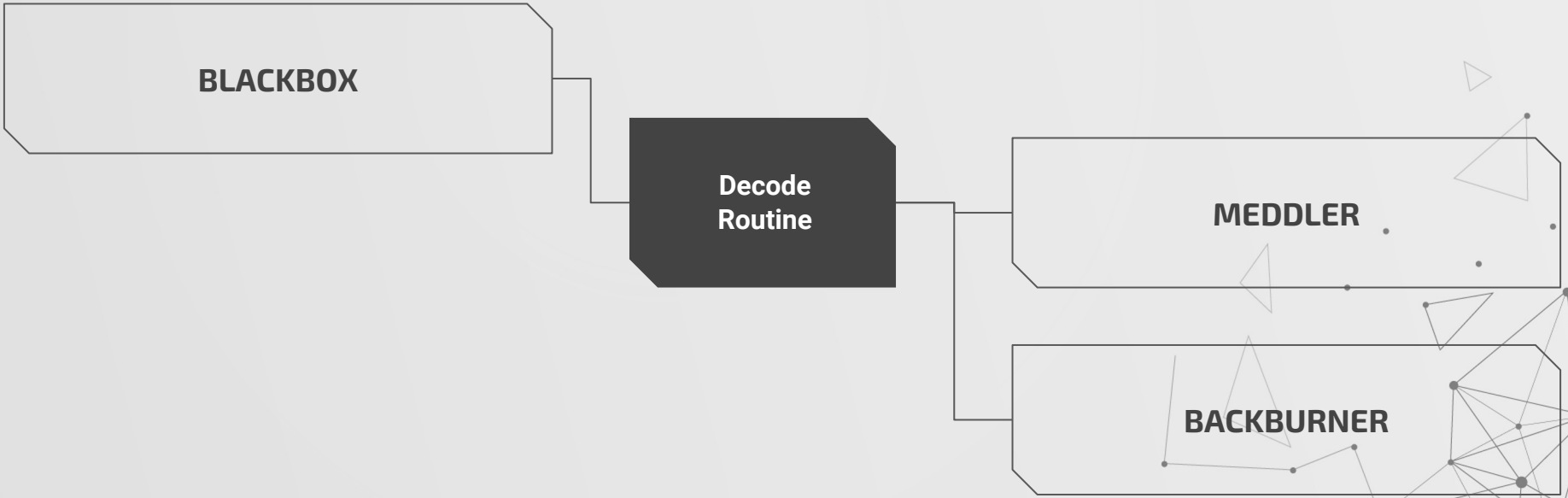
BrownLambert

6c466283e7f8757973ba253aa6080d8c

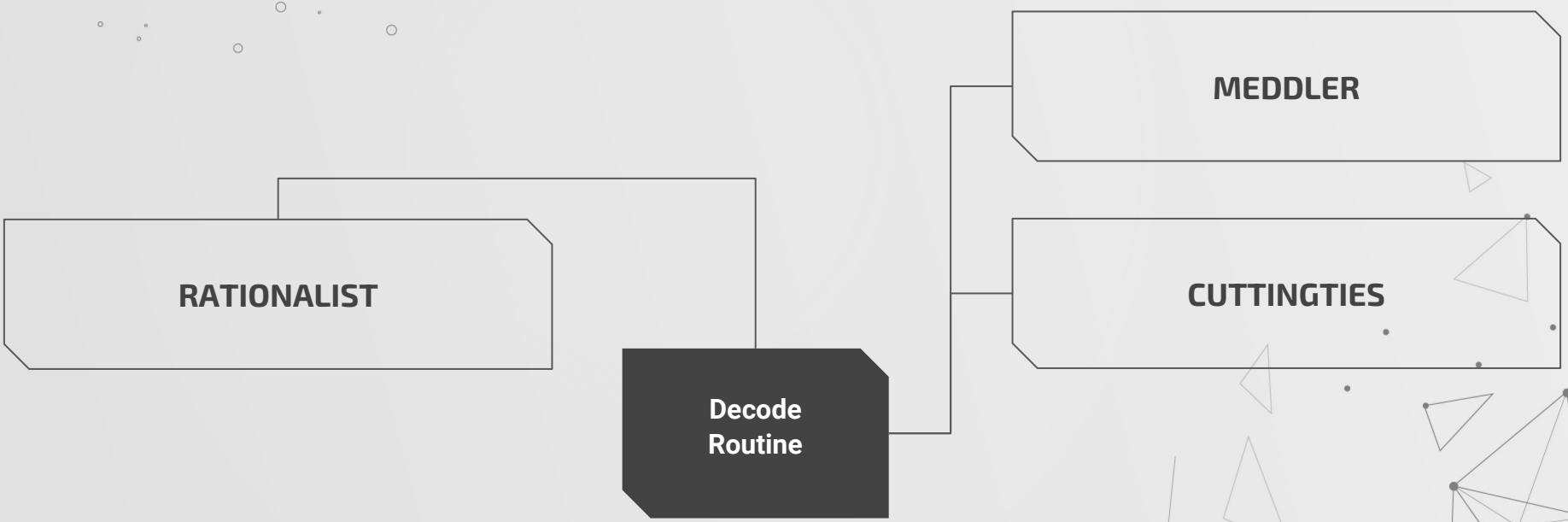
ANCHOR



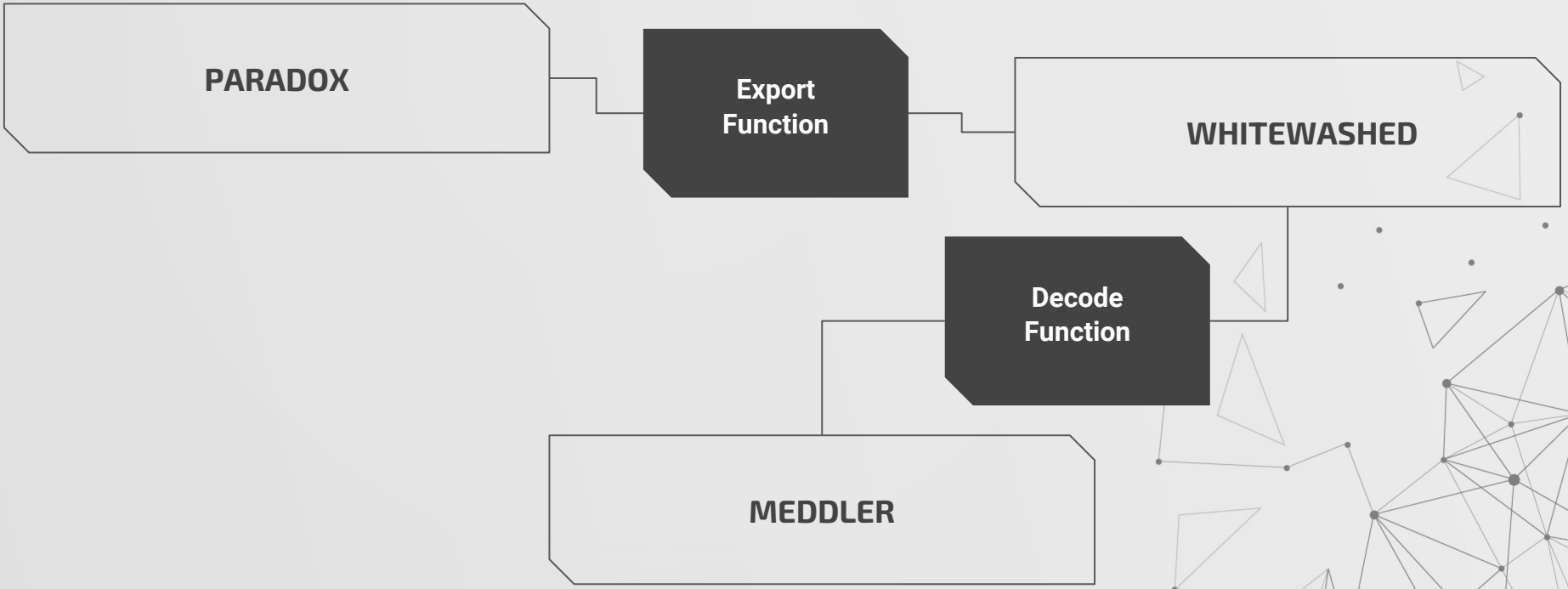
ANCHOR



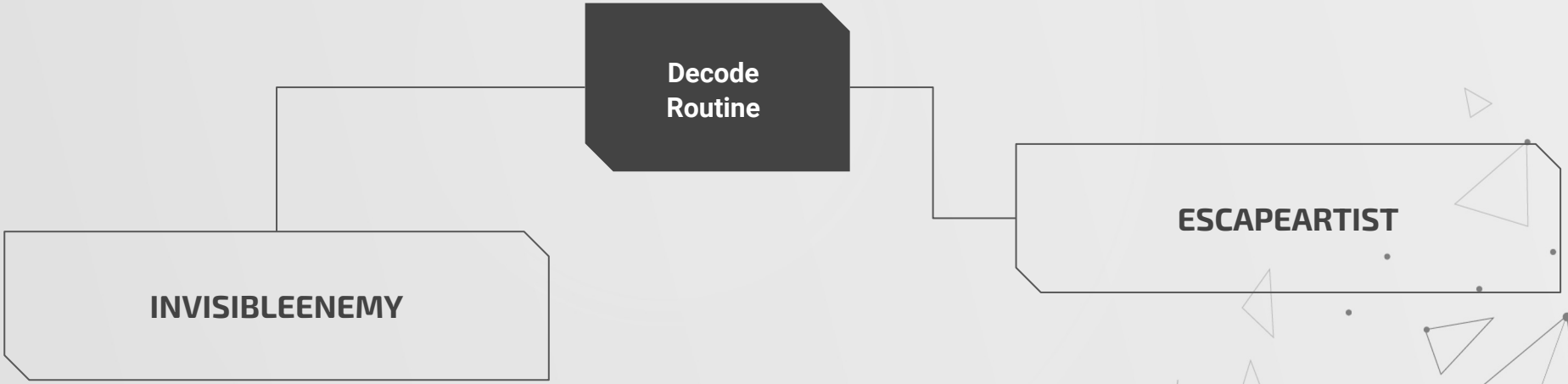
ANCHOR



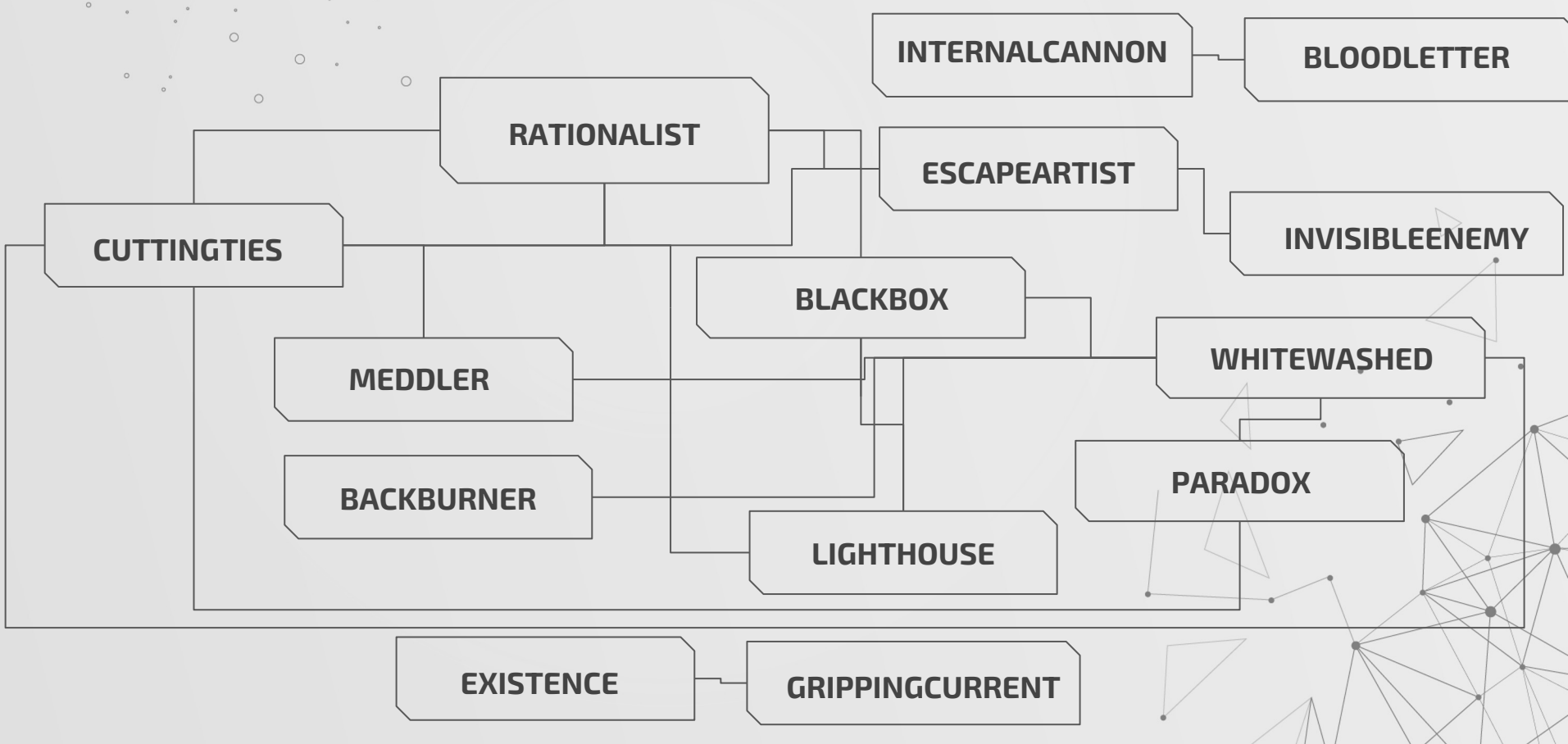
ANCHOR


PARADOX
Export Function
WHITEWASHED
Decode Function
MEDDLER

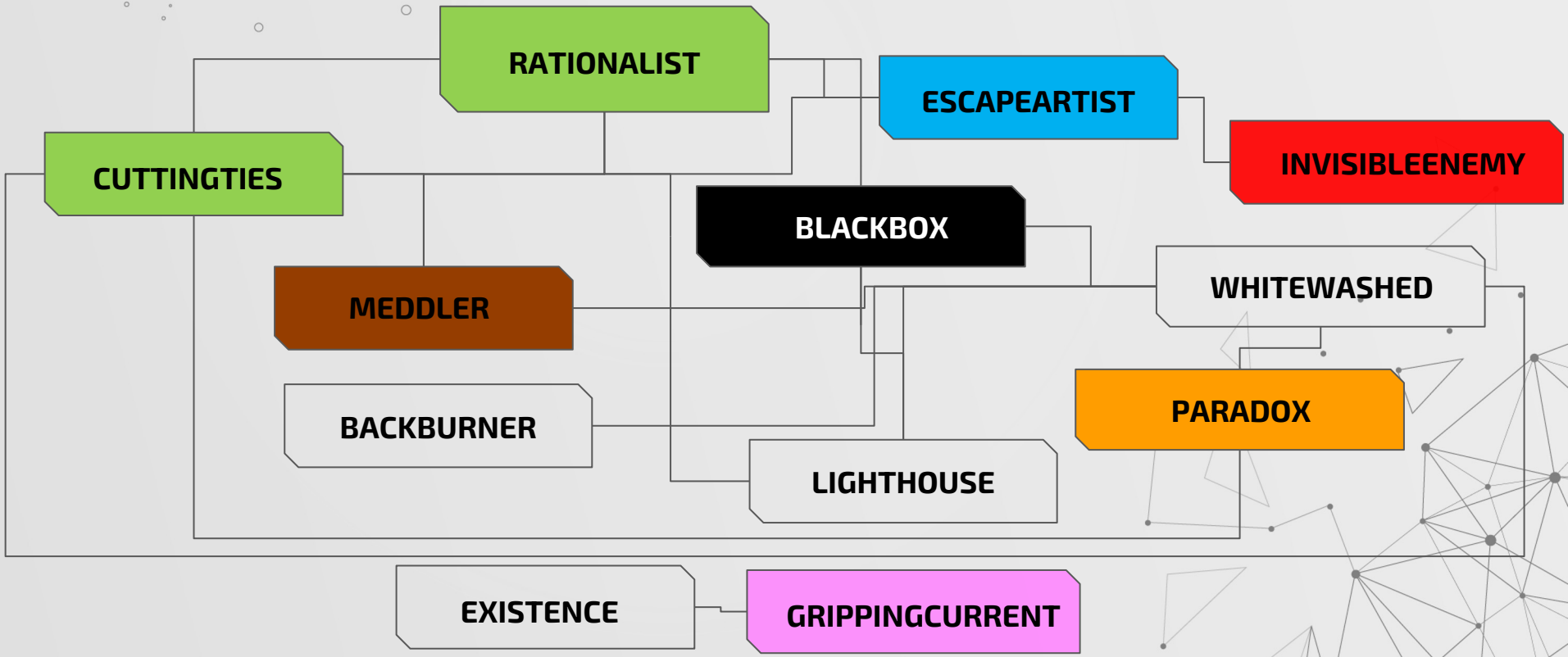
ANCHOR



CONSTELLATIONS



CONSTELLATIONS



MISSING FAMILIES

AMERICANDREAM
COMPOSURE
MARIANASTRENCH
MERIDIAN
PARAMOUNT
SEVENTHTRUMPET

21 ‘Families’ Total

14 Families Linked

6 Families Left Out to Dry

*bold indicates single sample

ASTRONOMICAL OBSERVATIONS

No reliance on code-signing

No AV evasion tricks

Some delayed imports

Plaintext OR Encryption

Spoofing advertising corps

Little timestamp spoofing

Files Usually <300KB

No user deception (icons)

Reliance on Windows services

Nothing execution focused

Hide from sysadmin not user

Scrub rev. history not PDB path

MIA FAMILIES

Probably Missing:

- TuxedoLambert
- PurpleLambert
- GreyLambert
- CyanLambert
- VioletLambert
- Any modules
- Lambert names that I don’t know :D

OVERLAP OBSERVATIONS

Same ‘type’ of tooling is what is getting found; creates a bias in this dataset

Author could be overthinking overlaps & the families could be 1-2 big families (or modules)

At limit without data showing how samples interact, how they are loaded, and how they communicate (named pipes)

RULES & TOOLS

BRIGHTCONSTELLATION RULES: https://pastebin.com/tEL8PZdn

FLOSS2YAR: https://github.com/g-les/floss2yar

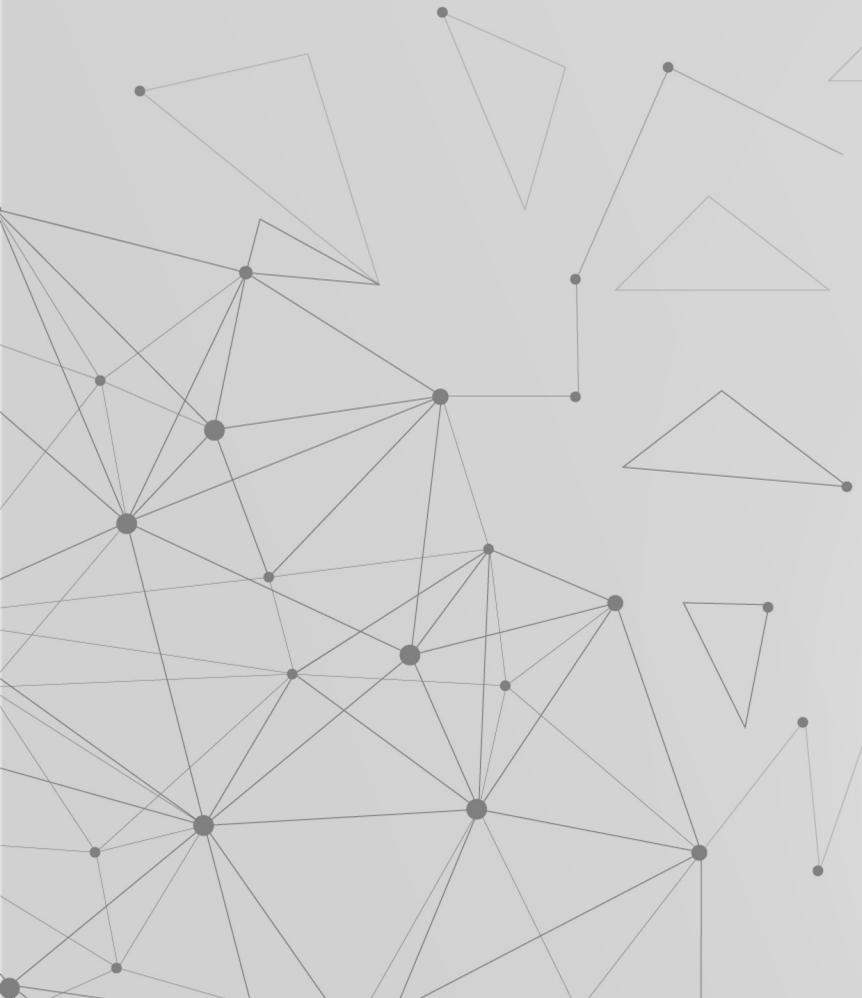
CONSOLE RULESET:
https://gist.github.com/g-les/e816389becd93209e588c905f553803a

OUTLOOK

YARA IS **FLEXIBLE** ENOUGH FOR **WACKY** IDEAS

NOT THE END OF BRIGHTCONSTELLATION
BUT EVEN APEX ACTORS **LEAVE ARTIFACTS**

IF IT DOESN'T EXIST YET, **BUILD IT**



Questions?

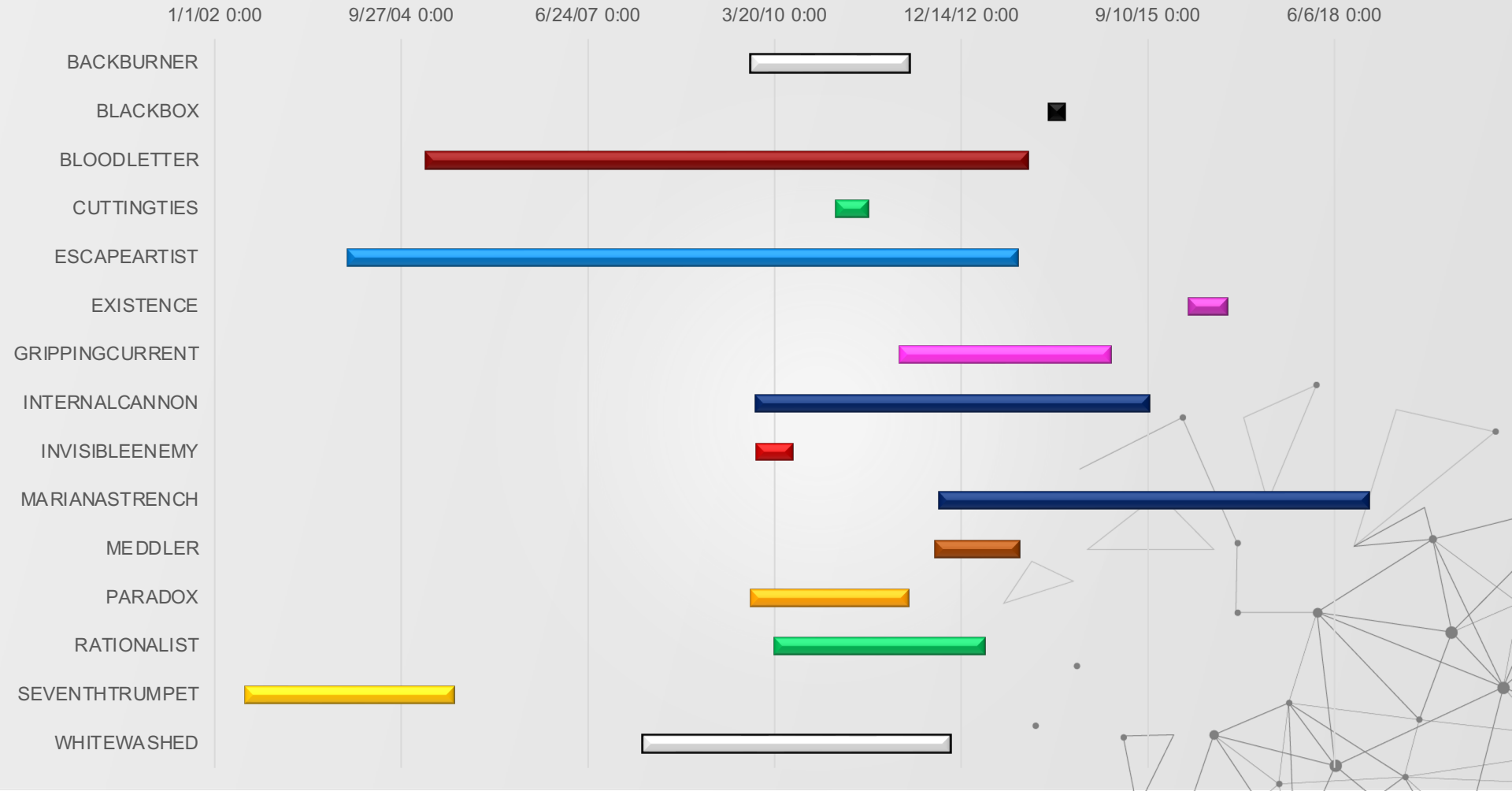
@greglesnewich
glesnewich (KeyBase)

APPENDIX

05.5

The Actual Families!

BRIGHTCONSTELLATION TELESCOPE



AMERICANDREAM

SAMPLES

- 75c0b7cdd54fa280a4517d917de370ec61854c7e319cf0d4b20c8ae580b2d932
- 635912c7a685aa75a4067ba15ac896b8fdbaa8593a67f4b04701d0b1c8e0496d
- Bc04d96757f65f92d25a93d666c5ba2ec88af1feb571af495456a46b62958ba4

ALIAS

- DePriMon

FEATURES

- Section hashes
- BASERELOC
- EXCEPTION
- IAT
- Imphash
- Rich Header
- Similar PE Versioning to BLACKBOX
  - Microsoft Unified Security Protocol Provider

BACKBURNER

Driver & Orchestrator (maybe?)

SAMPLES

- ea2ea2ae0d92e9b186ccb313fb8961cf9d6716a80588a87545f71f2a2b48a63d
- e5eb118f58abdfde6c6b0a694c78e4181e8993da5f36e43c855fdfa7976d6893

Pretty-Print Victim Profile

OS Version : %d.%d (build %d)

Driver Version : %s

Remote Peer Addr : %d.%d.%d.%d:%d

Local TCP Port : %d

Current MAC Address : %02x:%02x:%02x:%02x:%02x:%02x

MSS : %d bytes

NDIS module : %#x - %#x

STRINGS + FEATURES

- Loaded by **WHITEDWASHED**
- \\??\\pipe**ddxpipe**.%d
- **KAPERSKY**
- Extensive commands offered to operator
- Lots of Debug strings:
  - **bye... ;(**
  - [read_from_pipe] Pipe timeout (STATUS_PIPE_LISTENING)!
  - %s [parent-pid] <cmdline>
  - Unable to enumerate processes.
  - Unable to find target process.
  - Unable to create named pipe!

ALIAS

- White Lambert Payload

BLACKBOX

SAMPLES

- b8734ada49e290d12a5a178a67e5ae45e1e3348e54a1f57ef4cdb92ff8c84086
- 39024a39e063227f7d53cb2cf47af72214ba19a64488acac57e3577e28e0e569
- 425bbe7020fc443a8311099c2b74b1c6419700317603aae73988adb4113a8bff
- 2156adcaae541ea1718ea52ce07bd1555cdcf25e9919f3208958f8c195f34286
- 94c9400a7c092d39b053b98d3fb9b241ebd40d820894fa0aaf806d5f813eba06
- 65bc1695e971256824646f9f316ada2e54420493d0d47fd1b6a59d45a32b69d0
- 9ad54b0c8e78b24be55b762fb67aebe5b946e35bd0bff3fef9106908cd5c1729
- 1cd9671f38786c16acfc6b99288885c52ba3e38e3cf552dded877d66bb6ca1d4

FEATURES

- winlib.dll
- Hardcoded URIs:
  - **&a=mouse**
  - **upload.php**
- RPC usage
- Obfuscated strings similar to **RATIONALIST**

COMMANDS

- ipconfig
- netsh
- netstat

ALIAS

- Black Lambert/LH1

BLOODLETTER

Multi-Stage Multi-Component Plaintext Loader

SAMPLES

- 30246c5a4094bfc775b20a62d5fe267427a5d27571ffa81ec1c21e6d6d744a3d
- e505e24282cfde4af060a7b9cb76f8999a5585a563baf4d8e9911f9d9c3bb3c3
- 56270e3c685249a16a8d9c4322302318055c69238b8196b6c19f6629c7f378c4
- 41730ccfadf4741ead3c3c144c612f938dd43956be91d5abb3e6519c46152eaa

FEATURES

- .tmp DLL Names
- Embedded Plaintext PEs in RSRC
- Built in 2007; Loader from 2008
- Intermediate Payload Export: _EE112@16 DLL name: ~EE112.tmp
- Raw TCP Beacon
- **WebAdM** service
- Eventually drops **INTERNALCANNON**

```
00000000  59 4d 53 47 00 0f 00 00  00 09 00 57 00 00 00 00   YMSG.... ...W....
00000010  00 00 00 00 31 c0 80 4d  4e 45 70 c0 80            ....1..M NEp..
```

https://tria.ge/220804-ywmphabegn/behavioral1#report

COMPOSURE

SAMPLES

- 3762102384a546afd47aa40f599fca7840a5887df5f57301f9fb5c2a0e725ca2

ALIAS

- Grey Lambert ?

FEATURES

- Huawei PE Information
- High entropy resource (name: 1024)

```
[$ emit Testing/SampleDump/Lamberts/COMPOSURE/3762102384a546afd47aa40f599fca7840a5887df5f57301f9fb5c2a0e725ca2 | perc [| peek
--------------------------------------------------------------------------------------------------------------------------------
00.164 MB; 99.98% entropy; data
  path = RCDATA/1024/0
--------------------------------------------------------------------------------------------------------------------------------
0000000: 30 4A 74 F8 8E 6B 88 4F 5B B0 6E BE 22 A9 C0 C9 68 4E F9 A0 D9 14 0C 50 63 9F 0F 0A C8 05  0Jt..k.O[.n."...hN.....Pc.....
000001E: 03 04 4C 51 BD FB 6F 93 02 79 22 7C 91 44 29 F8 33 EB 3E 34 04 C7 22 C3 A5 98 6F C1 CA 8A  ..LQ..o..y"|.D).3.>4.."...o...
000003C: 92 2A 0E 5F A9 46 DF 88 28 F1 D5 EB 6B 55 EF 52 1F 1D 3A 67 F0 52 7F 86 FD 49 51 08 94 9C  .*._.F..(...kU.R..:g.R...IQ...
000005A: 9C 21 76 D1 96 5A 0E 7F B3 4D D1 24 F5 07 46 29 53 56 7A 53 6F C8 A8 2D 02 7B 55 D7 72 47  .!v..Z...M.$..F)SVzSo..-.{U.rG
0000078: 0F CB 7A 66 DA 14 A1 0B 27 C5 FF AF 35 59 51 20 51 2D B2 BA E7 DE 71 1E 9A E3 15 F5 0B FF  ..zf....'...5YQ.Q-....q.......
0000096: 3F F3 2B 6D 23 F3 71 7A 9B 38 F4 1C C9 64 48 C1 9F 86 8B 0F 11 35 B9 2D 27 2B 81 90 DC 8E  ?.+m#.qz.8...dH......5.-'+....
00000B4: 84 F9 2D E3 A8 82 CA 0C 2E 73 C5 BB ED CD 25 57 DC 29 09 7A 7B 2B F9 1C 22 F6 C0 F5 3B DE  ..-......s....%W.).z{+.."...;.
00000D2: ED 8A FE 3E BA BE C7 6B 77 98 7E 63 BB 91 76 DF 52 C5 C6 62 E9 80 D3 97 BC 57 5A 8A 51 9D  ...>...kw.~c..v.R..b.....WZ.Q.
00000F0: DB F2 2C 2B 4D B6 C9 CB E2 69 80 FE A4 36 1F 39 71 1C CC 60 2D 69 07 EF 19 62 2E 7F F0 BD  ..,+M....i...6.9q..`-i...b....
000010E: 20 AF C5 DB 40 24 1F 6F 2E 13 18 D0 5C 74 DB AE E8 DE 13 F1 A2 03 84 14 60 4C 2B 0F 22 AE  ....@$.o....\t.........`L+."
--------------------------------------------------------------------------------------------------------------------------------
```

CUTTINGTIES

HTTPS-Based Backdoor

SAMPLEs

- 2c84d4bdd3e892435ceca91a98ebbf21295f596155b2e52be3823b5f9ab2a123
- 8b7acdbc63e63d6c4273163abb58e3cb17d2d67758dcb3533df8e6967c137a7a
- 83c2fee47f488db956e33d379eae5e0e3b656c878ddde211ee79d35637cbc2ce
- dfbb00452b75ea47540dbb0df61910

FEATURES

- mdmm.exe
- Hardcoded C2s in Plaintext Config in .data
- WebBoundary + HTTP Format Strings
- Service: **iwasvc**

ALIAS

- Green Lambert

```
GET /login.php?d=https://update.iweb-apps.net&session=806285aa10d300f0d4919ab1164ca398476cd0566cef81c7483f89c90ebd4901 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3)
Host: update.iweb-apps.net
Connection: Keep-Alive
Cache-Control: no-cache
```

```
06.770 kB; 86.99% entropy; data
  offset = 0x3C400
    path = .data
```

```
0000: 44 5F 53 4E 00 69 77 61 73 76 63 00 2D 00 00 00 02 00 00 00 44 5F 53 44 4E 00 49 6E 74 65  D_SN.iwasvc.-.......D_SDN.Inte
001E: 67 72 61 74 65 64 20 57 65 62 20 41 70 70 6C 69 63 61 74 69 6F 6E 20 53 76 63 00 4B 00 00  grated.Web.Application.Svc.K..
003C: 00 02 00 00 00 44 5F 53 44 00 50 72 6F 76 69 64 65 73 20 6D 61 6E 61 67 65 6D 65 6E 74 20  .....D_SD.Provides.management.
005A: 61 6E 64 20 63 6F 6E 66 69 67 75 72 61 74 69 6F 6E 20 66 6F 72 20 69 6E 74 65 67 72 61 74  and.configuration.for.integrat
0078: 65 64 20 77 65 62 20 61 70 70 73 00 15 00 00 00 02 00 00 00 44 5F 53 47 00 6E 65 74 73 76  ed.web.apps.........D_SG.netsv
0096: 63 73 00 17 00 00 00 02 00 00 00 44 5F 49 44 4E 00 70 6E 70 64 33 64 78 30 00 14 00 00 00  cs.........D_IDN.pnpd3dx0.....
00B4: 02 00 00 00 44 5F 47 4E 00 43 49 52 43 55 53 00 18 00 00 00 02 00 00 00 44 5F 53 54 4E 00  ....D_GN.CIRCUS.........D_STN.
00D2: 46 49 52 45 45 41 54 45 52 00 23 00 00 00 02 00 00 00 44 5F 54 48 00 68 74 74 70 3A 2F 2F  FIREEATER.#.......D_TH.http://
00F0: 77 77 77 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 00 40 00 00 00 02 00 00 00 44 5F 4C 50 00 68 74  www.google.com.@.......D_LP.ht
010E: 74 70 73 3A 2F 2F 75 70 64 61 74 65 2E 69 77 65 62 2D 61 70 70 73 2E 6E 65 74 7C 68 74 74  tps://update.iweb-apps.net|htt
012C: 70 73 3A 2F 2F 37 39 2E 31 37 32 2E 31 39 33 2E 32 38 00 18 00 00 00 02 00 00 00 44 5F 53  ps://79.172.193.28.........D_S
014A: 43 4C 00 6C 6F 67 69 6E 2E 70 68 70 00 1A 00 00 00 02 00 00 00 44 5F 53 43 43 00 67 65 74  CL.login.php.........D_SCC.get
0168: 63 6F 6E 66 2E 70 68 70 00 1A 00 00 00 02 00 00 00 44 5F 53 43 46 00 67 65 74 66 69 6C 65  conf.php.........D_SCF.getfile
0186: 2E 70 68 70 00 1A 00 00 00 02 00 00 00 44 5F 53 43 55 00 75 70 6C 6F 61 64 32 2E 70 68 70  .php.........D_SCU.upload2.php
01A4: 00 17 00 00 00 02 00 00 00 44 5F 53 43 45 00 73 68 6F 77 2E 70 68 70 00 19 00 00 00 02 00  .........D_SCE.show.php.......
```


```
06.770 kB; 86.99% entropy; data
  offset = 0x3C400
    path = .data
```

```
0000: 44 5F 53 4E 00 69 77 61 73 76 63 00 2D 00 00 00 02 00 00 00 44 5F 53 44 4E 00 49 6E 74 65  D_SN.iwasvc.-.......D_SDN.Inte
001E: 67 72 61 74 65 64 20 57 65 62 20 41 70 70 6C 69 63 61 74 69 6F 6E 20 53 76 63 00 4B 00 00  grated.Web.Application.Svc.K..
003C: 00 02 00 00 00 44 5F 53 44 00 50 72 6F 76 69 64 65 73 20 6D 61 6E 61 67 65 6D 65 6E 74 20  .....D_SD.Provides.management.
005A: 61 6E 64 20 63 6F 6E 66 69 67 75 72 61 74 69 6F 6E 20 66 6F 72 20 69 6E 74 65 67 72 61 74  and.configuration.for.integrat
0078: 65 64 20 77 65 62 20 61 70 70 73 00 15 00 00 00 02 00 00 00 44 5F 53 47 00 6E 65 74 73 76  ed.web.apps.........D_SG.netsv
0096: 63 73 00 17 00 00 00 02 00 00 00 44 5F 49 44 4E 00 70 6E 70 64 33 64 78 30 00 14 00 00 00  cs.........D_IDN.pnpd3dx0.....
00B4: 02 00 00 00 44 5F 47 4E 00 43 49 52 43 55 53 00 18 00 00 00 02 00 00 00 44 5F 53 54 4E 00  ....D_GN.CIRCUS.........D_STN.
00D2: 46 49 52 45 45 41 54 45 52 00 23 00 00 00 02 00 00 00 44 5F 54 48 00 68 74 74 70 3A 2F 2F  FIREEATER.#.......D_TH.http://
00F0: 77 77 77 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 00 40 00 00 00 02 00 00 00 44 5F 4C 50 00 68 74  www.google.com.@.......D_LP.ht
010E: 74 70 73 3A 2F 2F 75 70 64 61 74 65 2E 69 77 65 62 2D 61 70 70 73 2E 6E 65 74 7C 68 74 74  tps://update.iweb-apps.net|htt
012C: 70 73 3A 2F 2F 37 39 2E 31 37 32 2E 31 39 33 2E 32 38 00 18 00 00 00 02 00 00 00 44 5F 53  ps://79.172.193.28.........D_S
014A: 43 4C 00 6C 6F 67 69 6E 2E 70 68 70 00 1A 00 00 00 02 00 00 00 44 5F 53 43 43 00 67 65 74  CL.login.php.........D_SCC.get
0168: 63 6F 6E 66 2E 70 68 70 00 1A 00 00 00 02 00 00 00 44 5F 53 43 46 00 67 65 74 66 69 6C 65  conf.php.........D_SCF.getfile
0186: 2E 70 68 70 00 1A 00 00 00 02 00 00 00 44 5F 53 43 55 00 75 70 6C 6F 61 64 32 2E 70 68 70  .php.........D_SCU.upload2.php
01A4: 00 17 00 00 00 02 00 00 00 44 5F 53 43 45 00 73 68 6F 77 2E 70 68 70 00 19 00 00 00 02 00  .........D_SCE.show.php.......
```

ESCAPEARTIST

SAMPLES

- d63b9860475c76da94c058e459b150ff37a5c6fd7d031f752f3444db65f5177b
- 9ab910a5591441633dcaac53dd6d748c5c64442773261607df0d28db76e11c10
- 39b8f93cdffa0c7a3210b7b39483c535a339fbd150d0d5f36cd0783350d367c3

ALIAS

- Blue Lambert ?

FEATURES

- **PDB Path**: a
- PDB Age == 0x01
- **DLL Name**: a.dll
- Multiple Unnamed Exports
- B64-ish STRING resources
- Super high entropy overlay

OVERLAPS:

- ReadFile Func w/ **RATIONLIST**
- Memset Func w/ **CUTTINGTIES**
- sBox w/ **INVISIBLEENEMY**

EXISTENCE

Loader

SAMPLES

- 57e7eff080c057dfc107fca8f4d9b61adfa797a75a301871fea08854aa771074
- a8b3f3c21eca80ad47c4021148bc3aef66a90bcbfdf681c245af772356fe6b63
- 1960935bae8633167e0102199a0bb720293994cb885be3f35cd28cceba476b2c
- 757d1c276e614bfa6e8f1813213f4c466785d80355bd8bef35826cff4ce359f9

FEATURES

- **PDB**: x
- PDB Age == 0x02
- Additional PE in .data section
- Loads GRIPPINGCURRENT

```
81.408 kB; 93.40% entropy; data
  offset = 0x3A00
    path = .data
--------------------------------------------------------------------------------
00000: F5 A1 86 42 00 00 01 04 00 06 03 00 88 FB C5 CF E0 8C 02 00 8D 17  ...B............................
00016: 01 00 02 00 00 00 00 00 00 00 1C 00 00 00 00 02 02 00 12 00 00 00  ........................
0002C: AF 81 D7 F3 FF 26 BF A9 54 00 00 10 00 FF 08 02 02 00 01 00 12 00  .....&..T.....................
00042: 3D 01 EE 04 0F FB 4D 5A 90 00 03 0A AE 04 03 CB FF FF B8 B3 00 00  =.....MZ.....................
00058: C9 40 00 57 F8 77 03 0E 1F BA FF 0E 00 B4 09 CD 21 B8 01 B7 4C 04  .@.W.w..........!...L.
0006E: 54 68 FF 69 73 20 70 72 6F 67 72 FF 61 6D 20 63 61 6E 6E 6F FF 74  Th.is.progr.am.canno.t
00084: 20 62 65 20 72 75 6E DB 20 69 02 44 FF 4F 53 20 6D 6F 64 65 2E F6  .be.run..i.D.OS.mode..
0009A: 0D 0D 0A 24 43 0F CB 49 FE FB 61 8F 28 90 32 03 0F 73 5F EE 29 32  ...$C..I..a.(.2..s_.)2
000B0: 89 07 FB A8 EE 5B 32 8A 13 1E 91 32 DA C7 0F 5E 32 BB B6 07 4B ED  .....[2....2...^2...K.
000C6: EC 5D 32 8E 0F 5B 07 8B 23 5A 60 0F D8 59 07 B6 2F 07 C1 0F B1 5C  .]2..[..#Z`..Y../....\
--------------------------------------------------------------------------------
```

GRIPPINGCURRENT

Modular Backdoor

SAMPLES

- 4652ae6d417a6c157a673046a442e1f071bca0eab1b4404f0343b573c361b05a
- 286520e81964ff8b7b38850381369af81e8d69dcd72e1f3ad176e0b0efa6921f
- 396235673954365297d3c4a4407ae05c1636bf6c471567b4ff322e6f0a01389c
- c945ad1cf9460da1186174cfd01bacb39454ae0c60bc5a4976af3ba9c7c0c505
- ed8f68085a6486b7a49496246d8d6c029a3ae1b86d9d157a231083c1f0e48706

ALIAS

- Fluxwire / Corenty / Pink Lambert
- Loaded by EXISTENCE

STRINGS

- Plugins?
  - core_entry
  - plugin_entry
- cache-%08x.dat
- set /a z=%%z%%+1
- if "%%z%%"=="1000" goto Done
- del "%s"
- set /a y=%%y%%+1
- if "%%y%%"=="30" goto End
- if exist "%s" goto Repeat
- PDB Age == 0x01

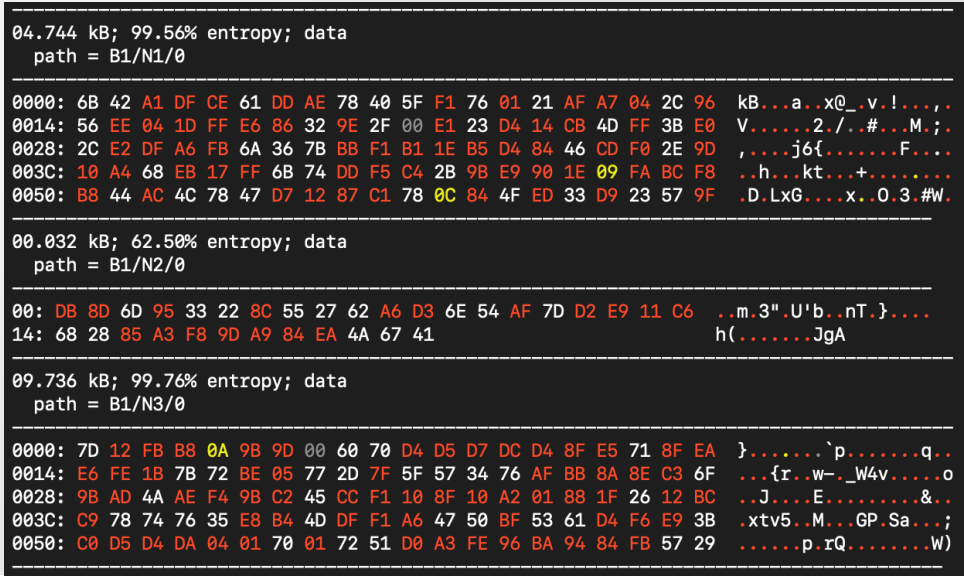
INTERNALCANNON

SAMPLES

- 91403abcf546fbeb310b2ee1603f3280f1b875695183da4c5f2102fc867fcc9b
- c9cd5c9609e70005926ae5171726a4142ffbccccc771d307efcd195dafc1e6b4b
- 3f4304eb9753155926f7dc6287bddadb05a80c0b8ae6f67e3f69ec7f10ab426f
- 7bb70ab14ad6003d77529f9edf9fa89dfde7656526f2393c07ae9d03455522f2
- 172e496fc433592c3c7760fb97451106b5188189987477e5a33b13b5eee685e9
- 1fee6eeb0aa255e46de32c36e8c079abcb9a1cae08663568c99f395e6e07a3ca

FEATURES

- Resource names: N1, N2, N3 + types: B1
- Also debug-string heavy



INVISIBLEENEMY

HTTP-Based Recon Backdoor

SAMPLES

- e7591998e01cc0bea4643f9c743114b3dcffcb3513b89ed57863f396aeefcce4
- 2cba711f579dec2caaac188db6c22bb2cc83251449a11bfc34112d6f3112b86a
- 21f727338a4f51d79ade48fdfd9e3e32e3b458719bf90745de31b898a80aaa65
- 30b11cd15d64c7a8c21c5173e806cd1b53736dda03cd67037a5401e96afae6f8
- 6790ef2b47a8a05ff4c2942b024f9895da30739253f4e5d5ef1897642289b7fc
- be7bf3c53e7249395e43a4ee7365a7fcfc3cb3a1e4dc053a5336e42f7ed5cc97
- db2054bc4ede207c3bbedd815ef5637c097cf93c7826bc6cdc2cc0d6a8a07edb

FEATURES

- Certificate in resource (for mTLS?)
- Custom HTTP Headers
  - X-MV-Version: 1.00
  - X-MV-Command
  - Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)
- Port-scanning + Backdoor capabilities
  - /agent/checkin
  - destroy-agent
  - exfil-file
  - run-scanner

ALIAS

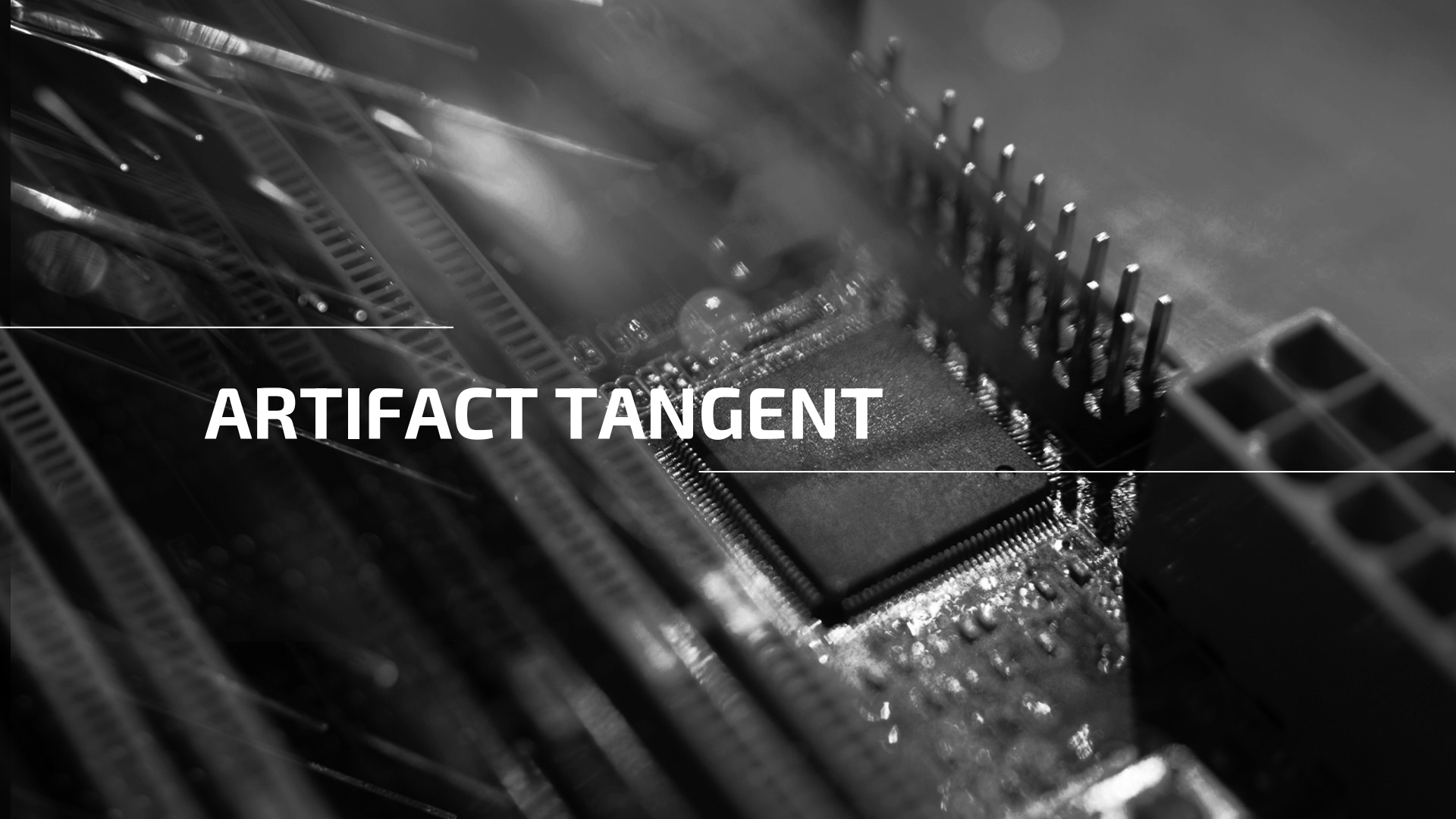
- Red Lambert

PDB Age == 0x70, 0x71

- Updated version of ESCAPEARTIST?
- One compile after another?

```
$ emit Desktop/Testing/SampleDump/Lamberts//INVISIBLEENEMY/e7591998e01cc0be
a4643f9c743114b3dcffcb3513b89ed57863f396aeefcce4 | pemeta
{
    "Debug": {
        "PdbPath": "a",
        "PdbAge": 112
    },
    "Header": {
        "Machine": "I386",
        "Subsystem": "Windows CUI",
        "MinimumOS": "Windows Vista",
        "RICH": [
            "[007dc627] [object] VS2005 build 50727",
            "[007bc627] [import] VS2005 build 50727",
            "[006dc627] [object] VS2005 build 50727",
            "[006ec627] [object] VS2005 build 50727",
            "[007cc627] [object] VS2005 build 50727",
            "[0078c627] [linker] VS2005 build 50727"
        ],
        "Type": "EXE",
        "Bits": 32,
        "ImageBase": "0x01000000",
        "ImageSize": 132096
    },
    "Version": {
        "CompanyName": "BIOS Innovations",
        "FileDescription": "Bios Compatibility Layer",
        "FileVersion": "6.1.6000.0",
        "LegalCopyright": "© BIOS Innovations LLC.  All rights reserved.",
        "ProductName": "Bios Compatibility Layer",
        "ProductVersion": "6.1.6000.0",
        "LangID": "040904B0",
        "Charset": "Unicode",
        "Language": "English (United States)"
    },
    "TimeStamp": {
        "Linker": "2009-12-08 16:00:14",
        "DbgDir": "2009-12-08 16:00:14"
    }
}
$
```

```
$ emit Desktop/Testing/SampleDump/Lamberts/INVISIBLEENEMY/21f727338a4f51d79ade
e31b898a80aaa65  | pemeta
{
    "Debug": {
        "PdbPath": "a",
        "PdbAge": 113
    },
    "Header": {
        "Machine": "I386",
        "Subsystem": "Windows CUI",
        "MinimumOS": "Windows Vista",
        "RICH": [
            "[007dc627] [object] VS2005 build 50727",
            "[007bc627] [import] VS2005 build 50727",
            "[006dc627] [object] VS2005 build 50727",
            "[006ec627] [object] VS2005 build 50727",
            "[007cc627] [object] VS2005 build 50727",
            "[0078c627] [linker] VS2005 build 50727"
        ],
        "Type": "EXE",
        "Bits": 32,
        "ImageBase": "0x01000000",
        "ImageSize": 132096
    },
    "Version": {
        "CompanyName": "BIOS Innovations",
        "FileDescription": "Bios Compatibility Layer",
        "FileVersion": "6.1.6000.0",
        "LegalCopyright": "© BIOS Innovations LLC.  All rights reserved.",
        "ProductName": "Bios Compatibility Layer",
        "ProductVersion": "6.1.6000.0",
        "LangID": "040904B0",
        "Charset": "Unicode",
        "Language": "English (United States)"
    },
    "TimeStamp": {
        "Linker": "2009-12-08 19:43:43",
        "DbgDir": "2009-12-08 19:43:43"
    }
}
$
```

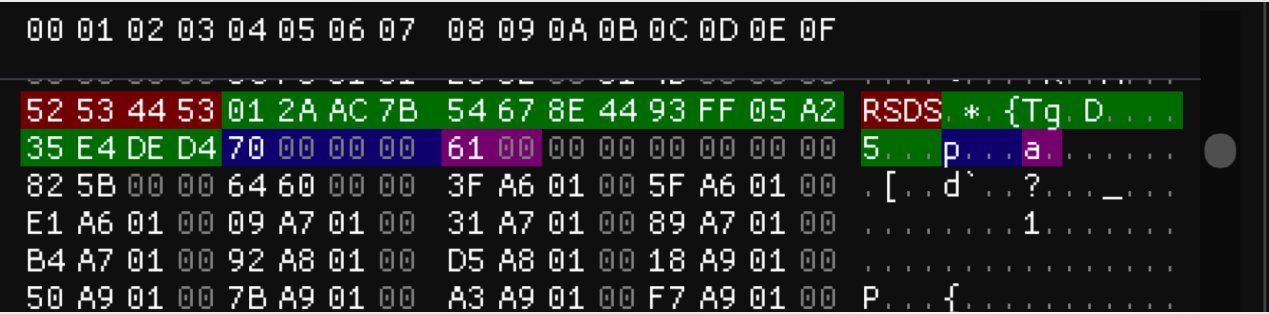

ARTIFACT TANGENT

```
$ emit INVISIBLEENEMY/21f727338a4f51d79ade48fdfd9e3e32e3b458719bf90745de31b898a80aaa65 | pemeta
{
    "Debug": {
        "PdbPath": "a",
        "PdbAge": 113
    },
    "Header": {
        "Machine": "I386",
        "Subsystem": "Windows CUI",
        "MinimumOS": "Windows Vista",
        "RICH": [
            "[007dc627] [object] VS2005 build 50727",
            "[007bc627] [import] VS2005 build 50727",
            "[006dc627] [object] VS2005 build 50727",
            "[006ec627] [object] VS2005 build 50727",
            "[007cc627] [object] VS2005 build 50727",
            "[0078c627] [linker] VS2005 build 50727"
        ],
        "Type": "EXE",
        "Bits": 32,
        "ImageBase": "0x01000000",
        "ImageSize": 132096
    },
```

```
rule INFO_Compiler_VS2005_build_50727 {
    condition:
        pe.rich_signature.toolid(1,0)
        and pe.rich_signature.toolid(123,50727)
        and pe.rich_signature.toolid(109,50727)
        and pe.rich_signature.toolid(125,50727)
        and pe.rich_signature.toolid(110,50727)
        and pe.rich_signature.toolid(126,50727)
        and pe.rich_signature.toolid(124,50727)
        and pe.rich_signature.toolid(120,50727)
}
```

```
$ emit ESCAPEARTIST//d63b9860475c76da94c058e459b150ff37a5c6fd7d031f752f3444db65f5177b | pemet
{
    "Debug": {
        "PdbPath": "a",
        "PdbAge": 1
    },
    "Header": {
        "Machine": "I386",
        "Subsystem": "Windows GUI",
        "MinimumOS": "Windows Vista",
        "RICH": [
            "[005f0fc3] [object] Windows Server 2003 SP1 DDK build 4035 (*)",
            "[005d0fc3] [import] Windows Server 2003 SP1 DDK build 4035 (*)",
            "[007bc627] [import] VS2005 build 50727",
            "[006dc627] [object] VS2005 build 50727",
            "[007ac627] [export] VS2005 build 50727",
            "[007dc627] [object] VS2005 build 50727",
            "[006ec627] [object] VS2005 build 50727",
            "[007cc627] [object] VS2005 build 50727",
            "[0078c627] [linker] VS2005 build 50727"
        ],
        "Type": "DLL",
        "Bits": 32,
        "ImageBase": "0x00400000",
        "ImageSize": 461312
```

MORE PDB ARTIFACTS

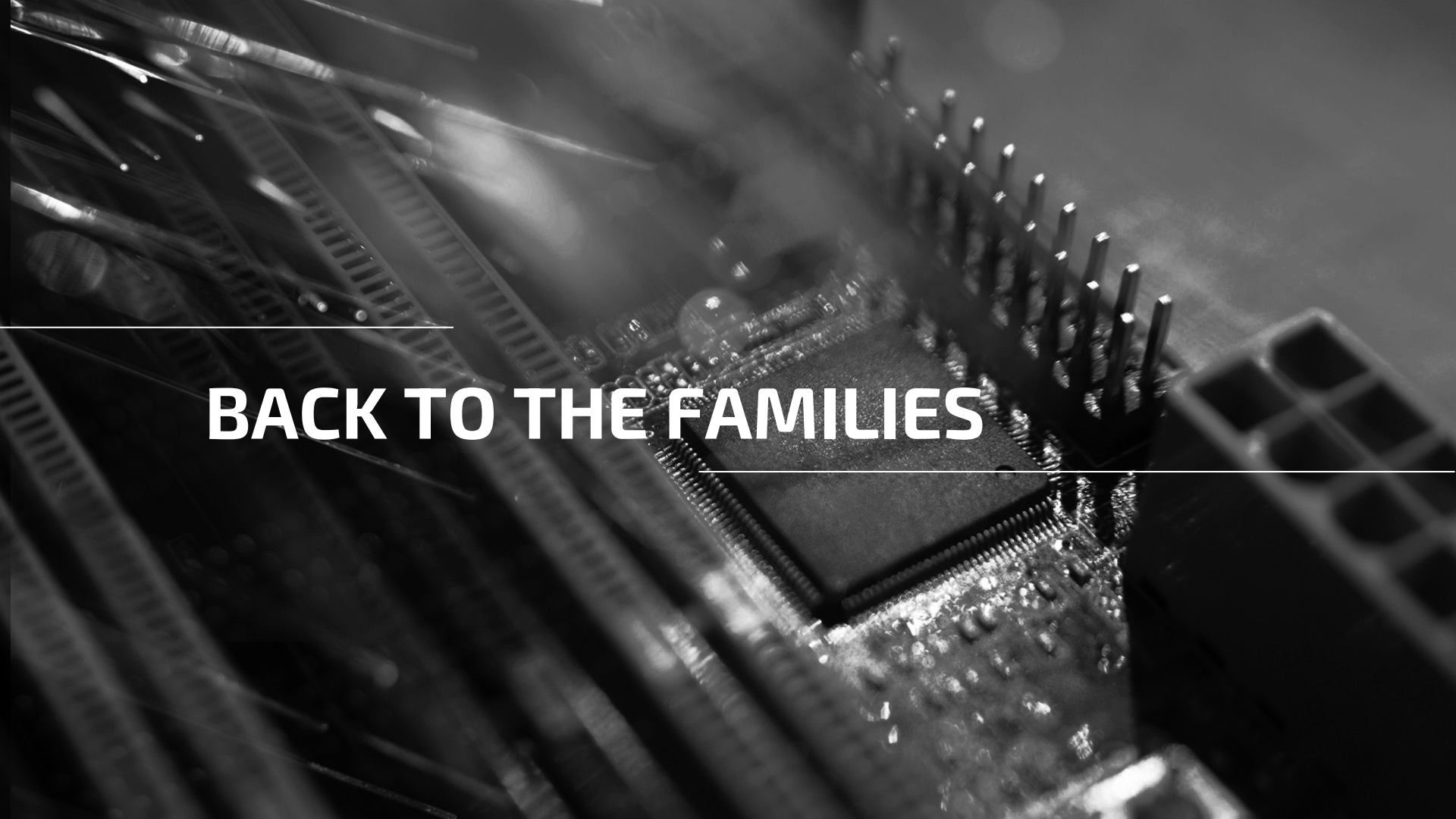



```
14
15  struct CodeView {
16      char signature[4] ;
17      u128 pdb_guid ;
18      u32 age ;
19      char pdb_path[] ;
20  };
```

Name	C		Type	Value
▼ codeview		0 0	struct CodeView	{ ... }
signature		0 0	String	"RSDS"
pdb_guid		0 0	u128	7bac2a01-6754-448e-ff93-e435a205d4de
age		0 0	u32	112 (0x70)
pdb_path		0 0	String	"a\x00"

PDB ARTIFACT MINING

pe.pdb_path	uint32(uint32(pe.rva_to_offset(pe.data_directories[pe.IMAGE_DIRECTORY_ENTRY_DEBUG].virtual_address)+(24))+20)
C:\\VCcode\\aaa\\x64\\Debug\\aaa.pdb	0x4 (4)
a	0x1 (1)
a	0x1 (1)
a	0x1 (1)
a	0x70 (112)
a	0x71 (113)
acpid.pdb	0x1 (1)
c:\\users\\bot\\fluxwire-cmake\\delta\\mswin-x86\\build\\base\\cmake\\ddk_node\\objfre_wxp_x86\\i386\\node.pdb	0x1 (1)
hiddrv.pdb	0x1 (1)
mnmdf.pdb	0x1 (1)
x	0x2 (2)
x	0x2 (2)
x	0x2 (2)


BACK TO THE FAMILIES

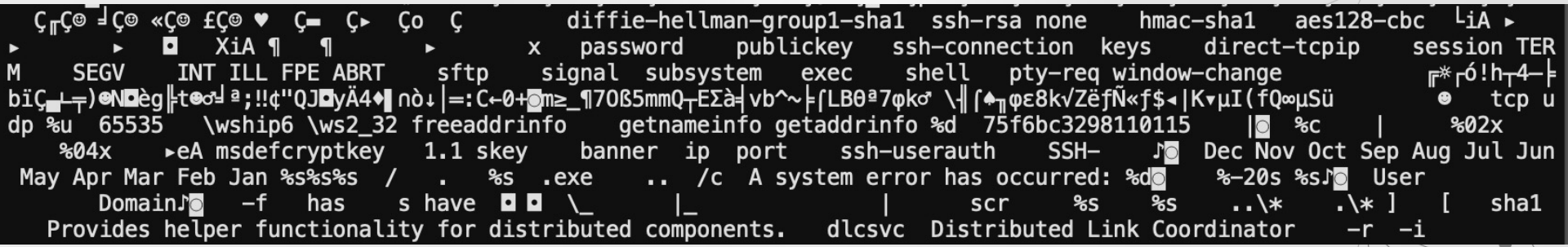
LIGHTHOUSE

SAMPLES

- 615193d5b17debdc026c61c67b0cf3eb65d0d
  dd68b8fa13bb3b902765be425ed
- Orchestrator?

FEATURES

- Version Info: dlcsvc
- Also runs as service **dlcsvc**
- Lots of **cryptography** & **communication** references



MARIANASTRENCH

SAMPLES

- 4f17835f7647127501417f659dcd80fa0f06b544e48ccc9294306a7230dde6d0
- 5c59c429be0da0757d2b8a3bb2fe5bfcf9f0a1d967508594a32bdb4b2a910003
- 16779abc1adc43713c52b70322865bcb39ee6f36a7e6dd0f2598dd5f9a48673b
- f2d38e3cdf225ba4a0883bc5dd457a2e0b00918d008a19059d88218f89da7441

FEATURES

- DLL Name: dll.dll
- Exports:
  - _IsOperandReg@8
  - _ParseInstruction@16
  - _ParseOperandAddress@8
- Create Service: **NativeService**
- Use of named pipes for internal comms

MEDDLER

SAMPLES

- 6f03586b863b308038c412959dcb2dca1f1ab03c925ba27e23b91dd21385a47b
- f17cb51bf0478f3cfa8a1b10ce40811c44c6e72aa0efb1e13e34eaf1b01d8cbc
- 15d9c9946bd4cea8cdac1d0c3415f6bab8460168c194048deb6b50932e1213fe
- 8d38afe922be801318e9292ed57450e4139315712694b9c27bbcf4818e5783e8
- 65b8bde4e1c8b9a881ee0f1d80756b8427d64ceaa0bfcf37f1a7f894622ee00d
- dfa80016b1d56f036c7f73ebb1912cd8b77e39a93b953f81f69635b320eb67cf

FEATURES

- OriginalName: MasStoDb.EXE (Mass Storage DB)
- 4 high entropy RCDATA resources (ID'd 1, 2, 3, 4)
- Rich Headers
- May load **BLACKBOX**

ALIAS

- Brown Lambert

MEDDLER

FEATURES

- 4 high entropy identically sized RCDATA resources (ID'd 1, 2, 3, 4) w/ identical headers

```
$ emit MEDDLER/dfa80016b1d56f036c7f73ebb1912cd8b77e39a93b953f81f69635b320eb67cf | perc [| peek -W 25 -l 5
--------------------------------------------------------------------------------
53.786 kB; 99.96% entropy; data
  path = RCDATA/1/0
--------------------------------------------------------------------------------
0000: 01 00 30 00 00 E1 D1 00 00 00 00 00 00 04 00 00 00 62 8A 9D DE E6 85 22 2E  ..0.............b.....".
0019: A2 9F 1B 8A 65 37 67 C2 D5 98 28 33 0B 52 B6 8B 45 51 02 01 18 A6 70 B4 85  ....e7g...(3.R..EQ....p..
0032: 92 F8 FE A3 12 DF 8E D7 16 96 E2 49 C6 B5 C3 DD C8 72 65 CB C0 97 AD E9 30  ...........I.....re.....0
004B: 78 F8 F0 F5 1D 9C AA BF 7A FC A9 E9 E0 11 D2 4F 40 BA 81 4D E8 BA A2 F3 24  x.......z......O@..M....$
0064: 8E 9F 7B AD 79 3F 55 02 94 76 91 3B 1D 76 B1 2A F5 DF EE 10 2B 8F A0 1D 5E  ..{.y?U..v.;.v.*....+...^
--------------------------------------------------------------------------------
53.786 kB; 99.96% entropy; data
  path = RCDATA/2/0
--------------------------------------------------------------------------------
0000: 01 00 30 00 00 E1 D1 00 00 01 00 00 00 04 00 00 00 62 8A 9D DE E6 85 22 2E  ..0.............b.....".
0019: A2 9F 1B 8A 65 37 67 C2 D5 98 28 33 0B 52 B6 8B 45 51 02 01 18 A6 70 B4 FE  ....e7g...(3.R..EQ....p..
```

MERIDIAN

SAMPLES

- 1f1ac64f7d6a4f5838d4226c34adefb4d71c92e6644d4693db4a29181830d394
- d332303937901c126e7e9722e39eaad328a8b792ed4e4372ce16cef4b48a3917

FEATURES

- Driver / Kernel Level Imports
- OriginalName: **shelldri**
- Tiny files, probably driver payload without configuration

```
int entry(undefined8 param_1,undefined8 param_2)

{
  uint uVar1;
  int iVar2;
  uint *puVar3;
  short *psVar4;
  undefined8 *puVar5;
  undefined local_res18 [8];
  code *local_res20;

  if (((DAT_0003f100 == 0) || (DAT_0003f100 == 0x2b992ddfa232)) &&
     (DAT_0003f100 = (_DAT_fffff78000000320 ^ 0x3f100) & 0xffffffffffff, DAT_0003f100 == 0)) {
    DAT_0003f100 = 0x2b992ddfa232;
  }
  DAT_0003f108 = ~DAT_0003f100;
  puVar3 = (uint *)ExAllocatePoolWithTag(1,&DAT_0002ba05,0x5741534a);
  FUN_000117ec((uint *)&DAT_00011970,2,puVar3);
  uVar1 = *puVar3;
  psVar4 = (short *)ExAllocatePoolWithTag(1,uVar1,0x5741534a);
  if (psVar4 != (short *)0x0) {
    iVar2 = RtlDecompressBuffer(0x102,psVar4,uVar1,puVar3 + 1,0x2ba01,local_res18);
    ExFreePoolWithTag(puVar3,0x5741534a);
```

PARADOX

SAMPLES

- 7792cededdb61ae249426c2fbb423dc50e1d5cd11c45155b7b91353ccd8937a0
- 79f4f0695989020c2b3cdbb9f459635c995164823868d446654dbc6dbd89cd52
- 8bade22161bf71a49955a66ec69809affbd2dde09dc84b94ede57e0d027e82e4

ALIAS

- Orange Lambert

FEATURES

- DLLs with no export names
- OriginalName: **avcnet.sys**
- Effort to avoid using WinAPIs

```
void __fastcall FUN_00011383(undefined4 param_1,uint *param_2)

{
  uint uVar1;
  uint uVar2;
  uint uVar3;
  int unaff_ESI;
  uint local_8;

  uVar3 = *param_2;
  uVar2 = param_2[1];
  local_8 = 0xc6ef3720;
  do {
    uVar1 = local_8 + 0x61c88647;
    uVar2 = uVar2 - ((uVar3 >> 5 ^ uVar3 << 4) + *(int *)(unaff_ESI + (local_8 >> 0xb & 3) * 4) +
                    (local_8 ^ uVar3));
    uVar3 = uVar3 - ((uVar2 >> 5 ^ uVar2 * 0x10) + *(int *)(unaff_ESI + (uVar1 & 3) * 4) +
                    (uVar1 ^ uVar2));
    local_8 = uVar1;
  } while (uVar1 != 0);
  *param_2 = uVar3;
  param_2[1] = uVar2;
  return;
}
```

PARAMOUNT

SAMPLES

- e6aefbfe8b268334ee052cf8f5ce6916e0827ffd86d4e86c5e1d72bad3a9010d

ALIAS

- Maybe DePriMon?

FEATURES

- Exports: PrintDebug / PrintLog
- 2 short, but high entropy resources
- Creates RegKey + Launches service after accessing resources

```
$ emit PARAMOUNT/e6aefbfe8b268334ee052cf8f5ce6916e0827ffd86d4e86c5e1d72bad3a9010d | perc [| peek -W 25
--------------------------------------------------------------------------------------------------------------
00.061 kB; 54.66% entropy; Non-ISO extended-ASCII text, with no line terminators
  path = RCDATA/1738/0
--------------------------------------------------------------------------------------------------------------
00: E1 B6 B6 DF DF B1 B1 D5 D5 BA BA CD CD BE BE 9E 9E DA DA BF BF D9 D9 B8 B8  ......................
19: CD CD A1 A1 D5 D5 F5 F5 A5 A5 D7 D7 BE BE D0 D0 A4 A4 84 84 C9 C9 A6 A6 C8  ......................
32: C8 A1 A1 D5 D5 BA BA C8 C8 C8 C8                                            ..........
--------------------------------------------------------------------------------------------------------------
00.067 kB; 59.50% entropy; Non-ISO extended-ASCII text, with no line terminators
  path = RCDATA/2835/0
--------------------------------------------------------------------------------------------------------------
00: AD EE EE D4 D4 88 88 DF DF B6 B6 D8 D8 BC BC D3 D3 A4 A4 D7 D7 8B 8B F8 F8  ......................
19: 81 81 F2 F2 86 86 E3 E3 8E 8E BD BD 8F 8F D3 D3 A4 A4 CD CD A3 A3 CE CE A0  ......................
32: A0 D0 D0 A2 A2 D6 D6 F8 F8 9C 9C F0 F0 9C 9C 9C 9C                          .................
--------------------------------------------------------------------------------------------------------------
```

RATIONALIST

HTTP-Based Backdoor + Info Stealer

SAMPLES

- 15d2669d1e303b226f206c69554d67d12
  1dd6a997b7883cbb081c5b00a3fe259
- 5f88c3ca2bc913d208d96a971ab3afa398
  1a0c757cd0da8e57d14dd9f98b98c7
- f3c60150ec27a84f612be0e87abfd643f31
  477b631be0901dce0fb47bb354f43

ALIAS

- Green Lambert

FEATURES

- Grabs credentials from Mozilla
- Updated version of **CUTTINGTIES**
- Creates a service: **Netqps**

STRINGS

- Content-Disposition: form-data; name="file"; filename="~up%02X.tmp"
- Content-Type: application/octet-stream
- {%02x%02x%02x%02x-%02x%02x-%02x%02x-%02x%02x-%02x%02x%02x%02x%02x%02x}
- ----------
  %02X%02X%02X%02X%02X%02X

```
GET /login.php?d=https://srv18.banner-add.com&session=318a98e640ab4905c61ae890420b8393e5eb6cf77d5e4b0599083d0915625ea0 HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/8.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET
CLR 3.0.30729; .NET CLR 3.5.30729; InfoPath.3)
Host: srv18.banner-add.com
Connection: Keep-Alive
Cache-Control: no-cache
```

SEVENTHTRUMPET

SAMPLES

- c8cfd7199468a8ca84adc4b455c4b3a855d226b2661e869506253fe5336b3ab9
- 7d7191441ef679e4b86ffdffffc98361c2789f6f2be9fe709c451d2b4f081b36
- 4ef02bd66a8c9417068a5009fb42bf687125b1a0bb3eb6c8850c2877f6b9d03a

ALIAS

- Gold Lambert

FEATURES

- Only kernel imports
- Linker timestamp from 2002...

STRINGS

- Looks for a driver to load: acpid.sys.__DriverEntry@4

WHITEWASHED

Multi-Stage Loader to Implant a Driver

SAMPLES

- e816b7495dc0730942b37a2198e16ee6f1e9312d1ab702d6724294f26aade0aa
- ebd34d687587378705ccaa555626b69b167f15446ddb17d949adb18721da1919
- 3652a7c4ce2387d910519cea4c0114ea20af0e3c05ffdad4928f79a7e5747a0d
- e806c60999997757c1e2d62fc7d9683df03b2cb08da407d0466d9feb4eb5e457

FEATURES

- Loads a driver from .data into service BiosSrv
- Very similar PDB & DLL Name to **ESCAPEARTIST**
- PDB Age == 0x01

STRINGS

- HTTP Headers

ALIAS

- White Lambert Loader

06

REFERENCES

References

- https://web.archive.org/web/20141111142313/http://www.fireeye.com/blog/technical/targeted-attack/2014/10/two-targeted-attacks-two-new-zero-days.html
- https://securelist.com/unraveling-the-lamberts-toolkit/77990/
- https://objective-see.org/blog/blog_0x68.html
- https://www.virusbulletin.com/virusbulletin/2019/01/vb2018-paper-draw-me-one-your-french-apts-expanding-our-descriptive-palette-cyber-threat-actors/#h4-lamberts-parallel-professional-development
- https://web.archive.org/web/20170410141039/https://www.symantec.com/connect/blogs/longhorn-tools-used-cyberespionage-group-linked-vault-7
    - https://web.archive.org/web/20170617220252/https://www.symantec.com/security_response/writeup.jsp?docid=2015-082518-2117-99&tabid=2
    - https://web.archive.org/web/20170617214701/https://www.symantec.com/security_response/writeup.jsp?docid=2017-040703-3623-99&tabid=2
    - https://web.archive.org/web/20170617203928/https://www.symantec.com/security_response/writeup.jsp?docid=2015-111823-1849-99&tabid=2
    - https://web.archive.org/web/20170617220233/https://www.symantec.com/security_response/writeup.jsp?docid=2017-040703-1537-99&tabid=2