REVERSING
2020

Yara with a touch of Science

Christiaan Beek

McAfee™

#Whoaml

SEARCHING

ATR

60%

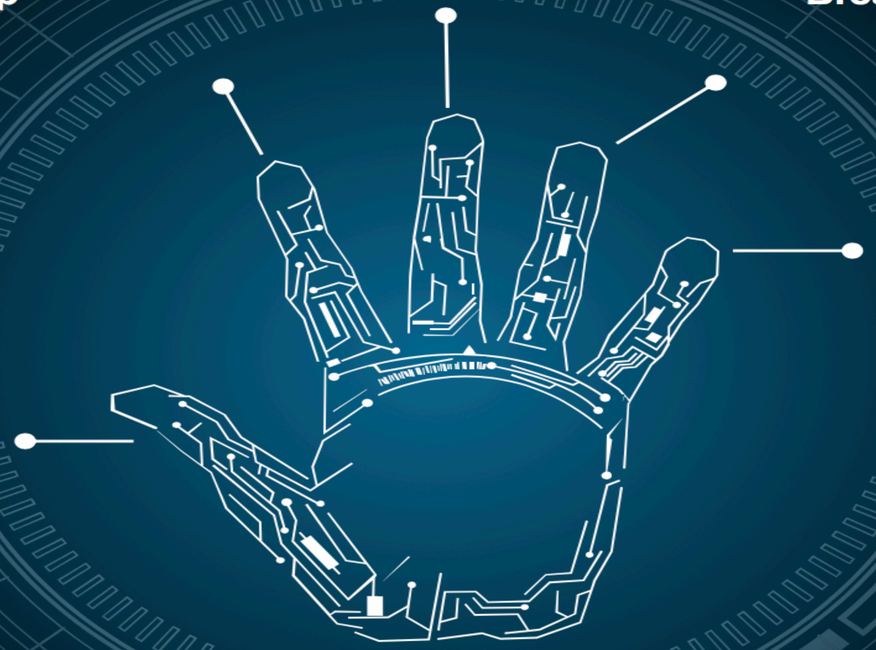
Lead Scientist
Sr. Principal Engineer

5%

Sleep

10%

Breaker of Things



10%

SecuritySopher
MITRE ATT&CK

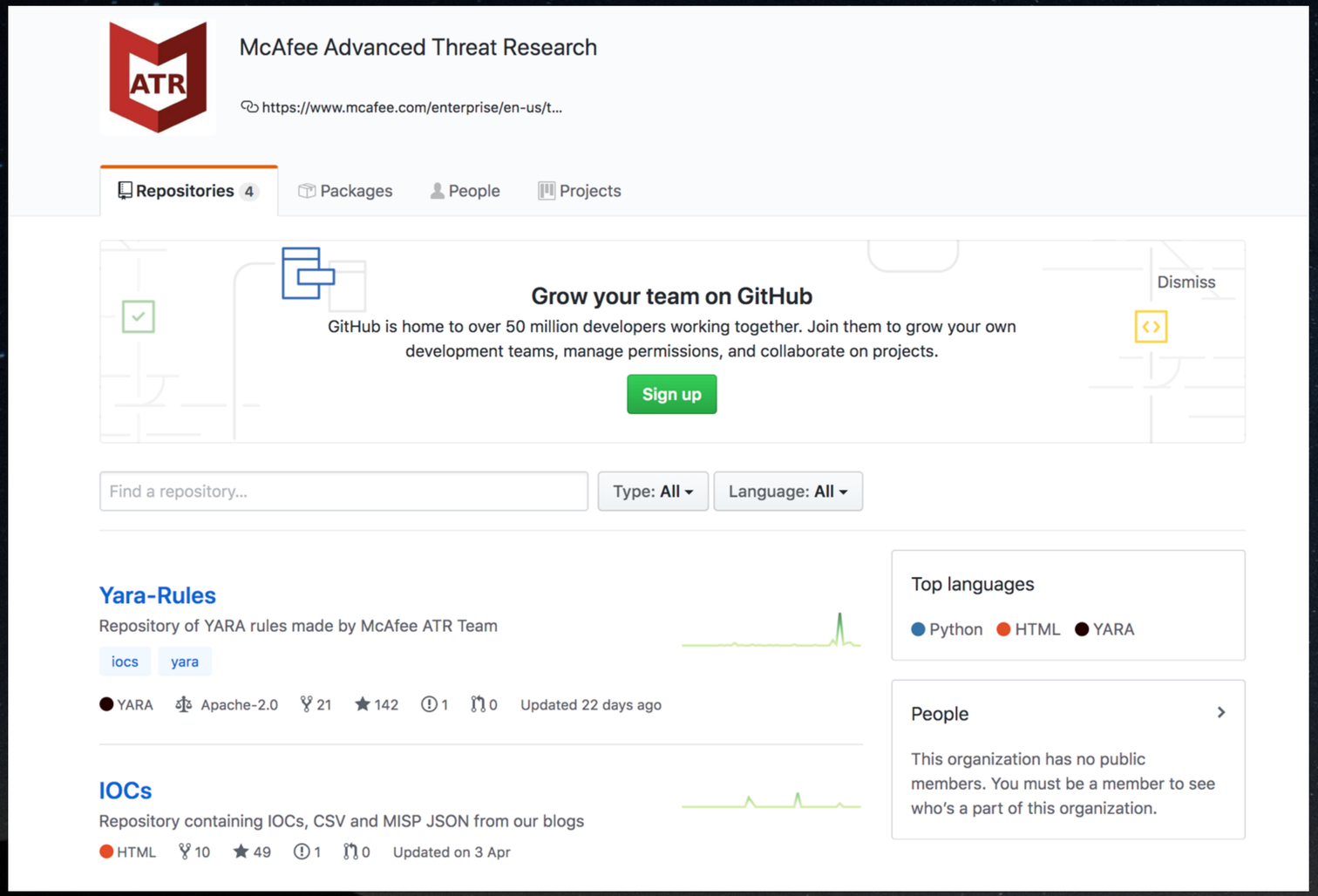
5%

Teacher

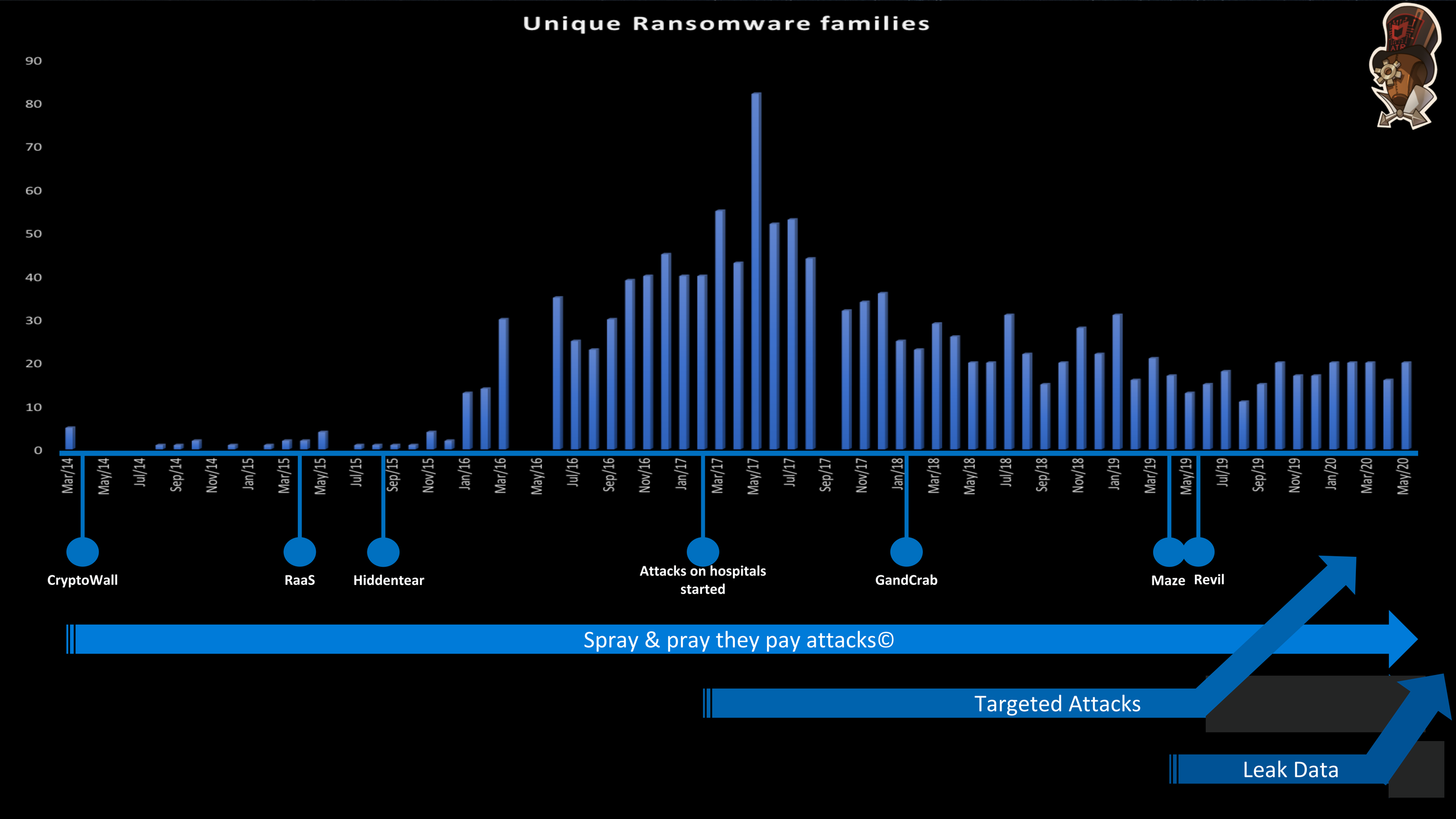
https://www.nomoreransom.org

@ChristiaanBeek

https://github.com/advanced-threat-research



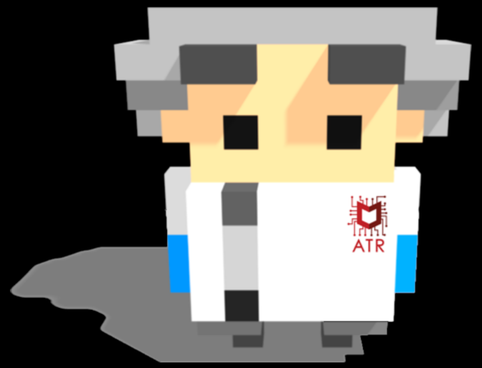
RANSOM_Sodinokibi.yar	Update RANSOM_Sodinokibi.yar
RANSOM_acroware.yar	Update RANSOM_acroware.yar
RANSOM_amba.yar	Update RANSOM_amba.yar
RANSOM_coronavirus.yar	Update RANSOM_coronavirus.yar
RANSOM_cuba.yar	Create RANSOM_cuba.yar
RANSOM_jeff_dev.yar	Update and rename RANSOM_jeff_dev to RANSOM_jeff_dev.yar
RANSOM_locdoor.yar	Update RANSOM_locdoor.yar
RANSOM_netwalker.yar	Update RANSOM_netwalker.yar
RANSOM_ragnarlocker.yar	Create RANSOM_ragnarlocker.yar
RANSOM_shrug2.yar	Update RANSOM_shrug2.yar
RANSOM_termite.yar	Update and rename RANSOM_termite to RANSOM_termite.yar
RANSOM_wannaren.yar	Create RANSOM_wannaren.yar
Ransom_Maze.yar	Added Maze yara-rule


Unique Ransomware families
90
80
70
60
50
40
30
20
10
0
Mar/14
May/14
Jul/14
Sep/14
Nov/14
Jan/15
Mar/15
May/15
Jul/15
Sep/15
Nov/15
Jan/16
Mar/16
May/16
Jul/16
Sep/16
Nov/16
Jan/17
Mar/17
May/17
Jul/17
Sep/17
Nov/17
Jan/18
Mar/18
May/18
Jul/18
Sep/18
Nov/18
Jan/19
Mar/19
May/19
Jul/19
Sep/19
Nov/19
Jan/20
Mar/20
May/20
CryptoWall
RaaS
Hiddentear
Attacks on hospitals started
GandCrab
Maze
Revil
Spray & pray they pay attacks©
Targeted Attacks
Leak Data

```
rule crime_win_cryptowall :
{
  meta:
    version = "1"
    description = "Cryptowall malware"

  strings:
    $mz = {4d 5a}
    $a1 = "Vocal AppWizard-Generated Applications"
    $a2 = "DDrawDoc"
    $a3 = "CDrawViez"
    $a4 = "C:\\Users\\M\\Desktop\\vc\\draw_XP\\Release\\draw.pdb"

  condition:
    ($mz at 0) and (1 of ($a*))
}
```

Tools:

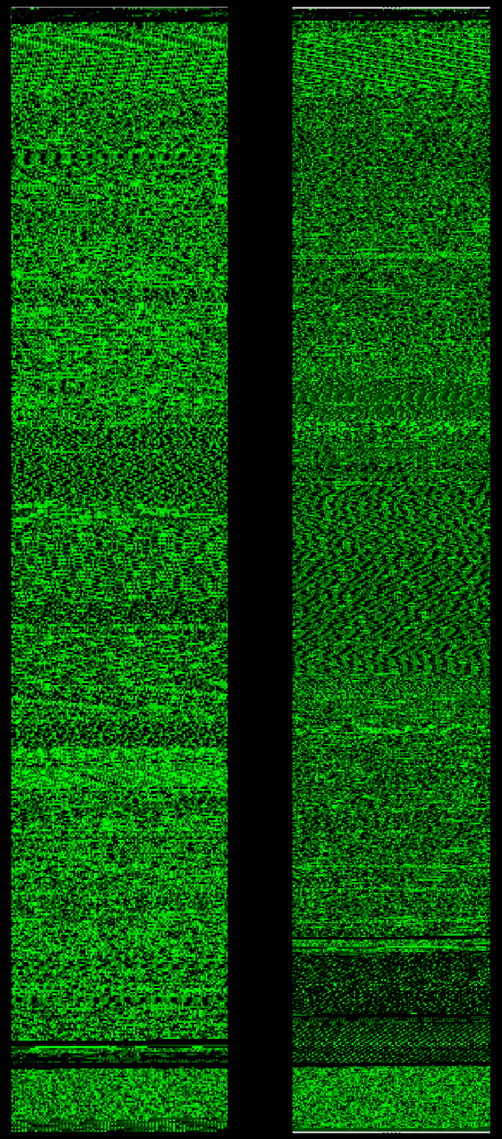
- STRINGS CLI
- PEStudio CLI
- VT
- IDA /R2
- Jupyter Notebook

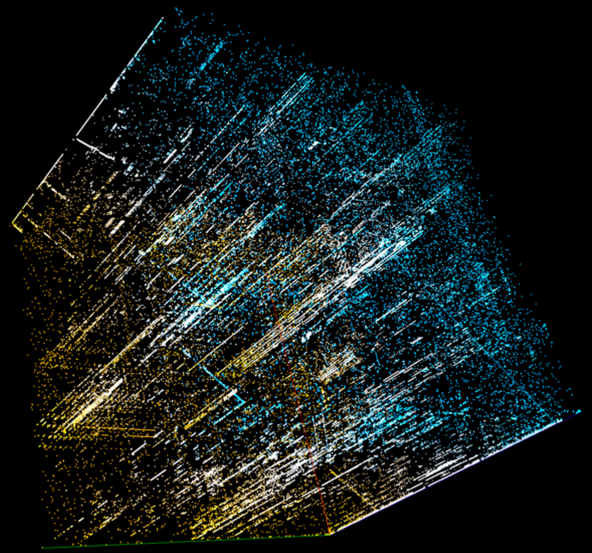


- And when lazy: YaraGen

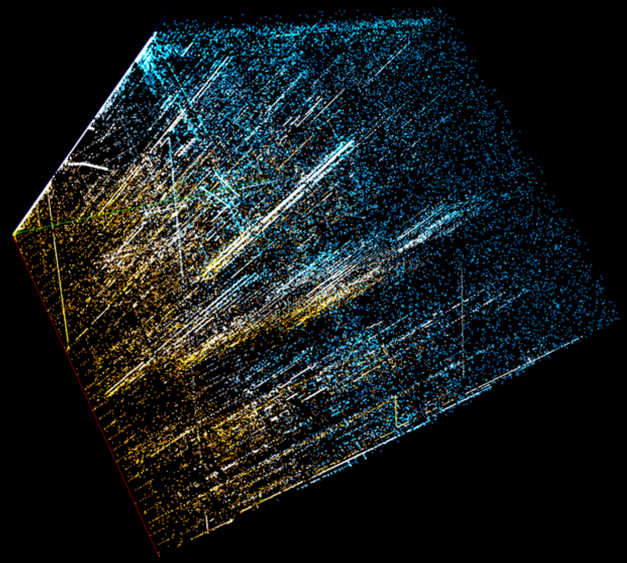
McAfee

Visual inspection





Ransom Family in 2019



Ransom Family in 2020

Yara rule writing

```
import "pe"

rule crime_ransom_Netwalker
{
	meta:

		description = "Rule to track Netwalker ransomware family"
		author = "@ChristiaanBeek"
		version: "1.0"
		reference = "internal"
		date = "2020-06-08"
		malware_type: "ransomware"
		mitre_att: "T1068, T1055, T1089"
		actor_type: "Cybercrime"
		actor: "Unknown"
		sha256 = "0991a0ee5f503640a2d7bed032cf176e69ed6adfc798a339dd59d583e2e3f3a7"
	strings:

		$code1 = { 6A ?? 8B ?? ?? 83 ?? ?? 5? 8B ?? ?? 5? E8 ?? ?? ?? ?? 83 ?? ?? 85 ?? 0F 85 }
		$code2 = { 8B ?? ?? 8A ?? 88 ?? ?? 8B ?? ?? 83 ?? ?? 89 ?? ?? 0F B6 ?? ?? 85 ?? 75 }
		$code3 = { 8B ?? ?? 8B ?? ?? 5? E8 ?? ?? ?? ?? 83 ?? ?? 89 ?? ?? 83 ?? ?? ?? 0F 84 }
		$code4 = { 0F B6 ?? ?? C1 ?? ?? 81 E? ?? ?? ?? ?? 8B ?? ?? 03 ?? ?? 88 ?? E9 }
		$code5 = { 8B ?? ?? 5? E8 ?? ?? ?? ?? 83 ?? ?? 89 ?? ?? 83 ?? ?? ?? 0F 84 }


	condition:
		uint16(0) == 0x5a4d and any of ($code*)
}
```

McAfee

Yara rule writing

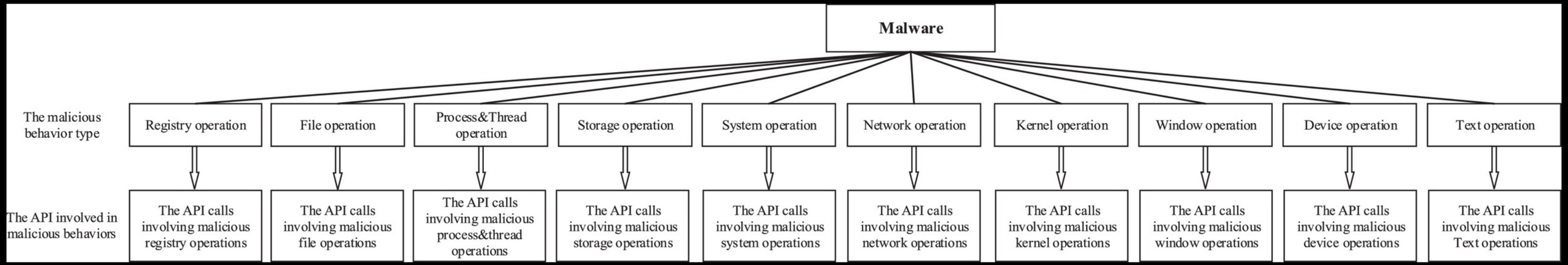
```
import "pe"

/* Private rule(s) used at the end in public rule(s)

private rule PE_check {
condition:
uint16(0) == 0x5A4D and
uint32(uint32(0x3C)) == 0x00004550
}

Private rule payload1 {
strings:
$code1 = { 6A ?? 8B ?? ?? 83 ?? ?? 5? 8B ?? ?? 5? E8 ?? ?? ?? ?? 83 ?? ?? 85 ?? 0F 85 }
$code2 = { 8B ?? ?? 8A ?? 88 ?? ?? 8B ?? ?? 83 ?? ?? 89 ?? ?? 0F B6 ?? ?? 85 ?? 75 }
Condition:
$code1 or $code2
}

Private rule payload2 {
strings:
$code3 = { 8B ?? ?? 8B ?? ?? 5? E8 ?? ?? ?? ?? 83 ?? ?? 89 ?? ?? 83 ?? ?? ?? 0F 84
Condition:
$code3
}


rule crime_ransom_Netwalker
{
        meta:

                description = "Rule to track Netwalker ransomware family"
                author = "@ChristiaanBeek"
                version: "1.0"
                reference = "internal"
                date = "2020-06-08"
                malware_type: "ransomware"
                mitre_att: "T1068, T1055, T1089"
                actor_type: ""
                actor: "Unknown"Cybercrime


        condition:
                PE_Check and payload1 or payload2
}
```

McAfee

Ransomware Building blocks

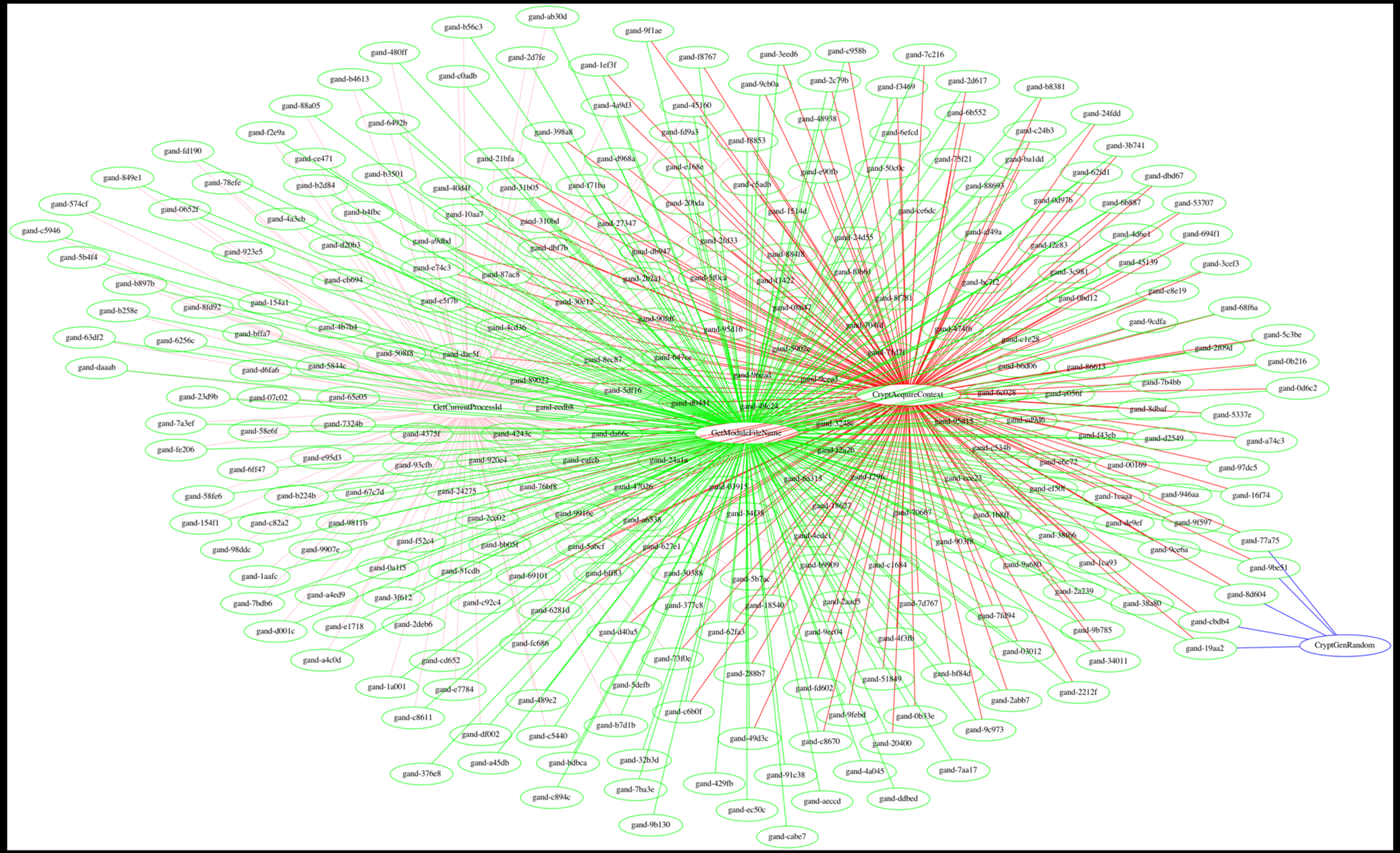
McAfee

Ransomware Building blocks



Ransom Family A	Ransom Family B	Ransom Family C	Ransom Family D	Ransom Family E	Ransom Family F	Ransom Family G
			CryptAcquireContextA			
FindClose						
FindFirstFileW	CryptAcquireContextW	CryptAcquireContextA		CryptAcquireContextW		
		CryptGenRandom				
FindNextFileW					GetCurrentProcessId	
					GetCurrentThreadId	
		FindClose			GetEnvironmentStringsW	
	CryptGenRandom	FindFirstFileExA		CryptGenRandom		
		FindNextFileA	FindClose		GetModuleFileNameA	
		GetCurrentProcessId	FindFirstFileW		GetModuleFileNameW	
			FindNextFileW			CryptGenRandom
MoveFileExW		GetCurrentThreadId	GetCurrentProcessId			
	FindClose	GetEnvironmentStringsW	GetCurrentThreadId			
	FindFirstFileExA	GetModuleFileNameA	GetEnvironmentStringsW	FindClose		
	FindNextFileA	GetModuleFileNameW	GetModuleFileNameA	FindFirstFileW		
			GetModuleFileNameW		TerminateProcess	
	GetCurrentProcessId			FindNextFileW		
	GetCurrentThreadId		MoveFileW			
	GetEnvironmentStringsW					
	GetModuleFileNameA					
						FindFirstFileW
	MoveFileExW					FindNextFileW
			TerminateProcess			GetCurrentProcessId
				MoveFileExW		

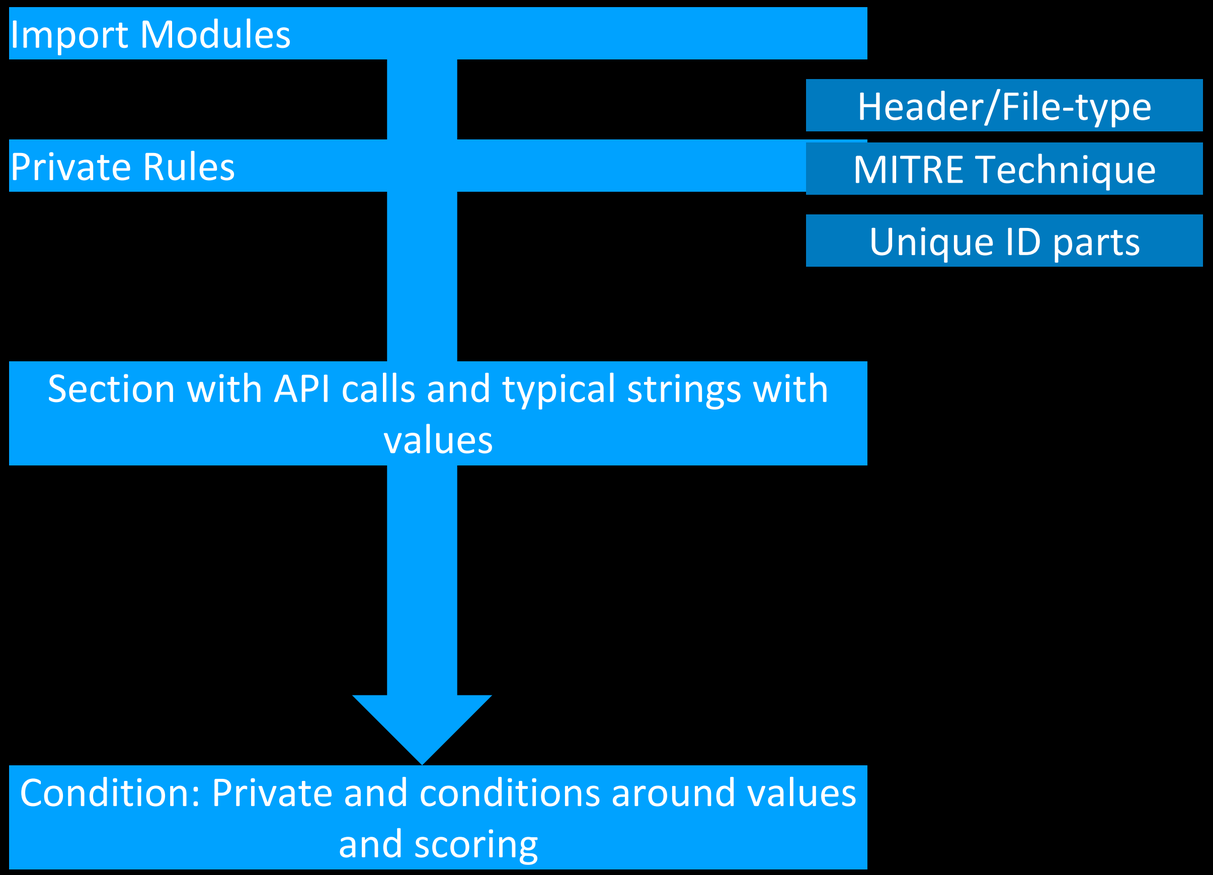
McAfee


gand-ab30d
gand-b56c3
gand-9f1ae
gand-480ff
gand-2d7fe
gand-1ef3f
gand-f8767
gand-3eed6
gand-c958b
gand-7c216
gand-b4613
gand-c0adb
gand-9cb0a
gand-2c79b
gand-f3469
gand-2d617
gand-b8381
gand-88a05
gand-4a9d3
gand-45160
gand-48938
gand-6b552
gand-24fdd
gand-f2e9a
gand-6492b
gand-398a8
gand-fd9a3
gand-f8853
gand-6efcd
gand-c24b3
gand-3b741
gand-fd190
gand-ce471
gand-21bfa
gand-d968a
gand-e168e
gand-e90fb
gand-50c0c
gand-75f21
gand-ba1dd
gand-62fd1
gand-dbd67
gand-849e1
gand-78efe
gand-b3501
gand-b2d84
gand-40d4f
gand-31b05
gand-f71ba
gand-c5adb
gand-88693
gand-0d976
gand-6b887
gand-53707
gand-574cf
gand-0652f
gand-b4fbc
gand-10aa7
gand-3108d
gand-27347
gand-20bda
gand-f514d
gand-ce6dc
gand-af49a
gand-4d6e1
gand-694f1
gand-c5946
gand-4a3cb
gand-d20b3
gand-a98bd
gand-dbf7b
gand-db947
gand-2fd33
gand-24d55
gand-f2e83
gand-923e5
gand-e74c3
gand-87ac8
gand-884f8
gand-3c981
gand-45139
gand-3cef3
gand-5b4f4
gand-cb694
gand-2bf2a1
gand-5f0ca
gand-f1422
gand-f0b61
gand-bc712
gand-b897b
gand-154a1
gand-e5f7b
gand-30e12
gand-87781
gand-0bd12
gand-e8e19
gand-8fd92
gand-08b47
gand-68f6a
gand-b258e
gand-4b7b4
gand-90fd0
gand-95d16
gand-704fd
gand-47406
gand-9cdfa
gand-63df2
gand-6256c
gand-bffa7
gand-4cd36
gand-e1e28
gand-5c3be
gand-2f09d
gand-daaab
gand-d6fa6
gand-5844c
gand-508f8
gand-dae5f
gand-8ec87
gand-647ce
gand-5002e
gand-78d2f
gand-b6d06
gand-86613
gand-0b216
gand-23d9b
gand-07c02
gand-65e05
gand-89022
gand-9bca4
gand-9cca3
gand-7b4bb
gand-0d6c2
gand-5df16
gand-df431
gand-eed88
gand-8dbaf
gand-7a3ef
gand-58e6f
gand-7324b
gand-4375f
gand-4243c
gand-da66c
gand-32486
gand-95815
gand-ed0d6
gand-5337e
gand-fe206
gand-e95d3
gand-93cfb
gand-920c4
gand-eafeb
gand-24a1a
gand-12a2b
gand-f43eb
gand-d2549
gand-a74c3
gand-6ff47
gand-58fe6
gand-b224b
gand-67c7d
gand-24275
gand-76bf8
gand-47026
gand-03915
gand-ba318
gand-129fc
gand-ece23
gand-efe72
gand-00169
gand-97dc5
gand-ef50f
gand-1eaaa
gand-946aa
gand-16f74
gand-154f1
gand-c82a2
gand-9811b
gand-2cc02
gand-991cc
gand-a6538
gand-34138
gand-18627
gand-70667
gand-1b8f1
gand-1e9ef
gand-9f597
gand-98ddc
gand-9907e
gand-f52c4
gand-bb05f
gand-5abcf
gand-627e1
gand-4edc1
gand-38f06
gand-903f8
gand-9ce6a
gand-77a75
gand-1aafc
gand-0a1f5
gand-51cdb
gand-69101
gand-bf183
gand-80388
gand-5b7ac
gand-b9809
gand-cf684
gand-9a680
gand-1ea93
gand-9be51
gand-7bdb6
gand-a4ed9
gand-3f612
gand-c92c4
gand-6281d
gand-377c8
gand-18540
gand-2aad5
gand-7d767
gand-2a239
gand-38a80
gand-8d604
gand-d001c
gand-e1718
gand-2deb6
gand-d40a5
gand-62fa3
gand-9ec04
gand-4f3fb
gand-7fd94
gand-9b785
gand-cbdb4
gand-a4c0d
gand-fc686
gand-73f0e
gand-03012
gand-19aa2
CryptGenRandom
gand-cd652
gand-34011
gand-1a001
gand-e7784
gand-5defb
gand-288b7
gand-fd602
gand-51849
gand-bf84d
gand-2212f
gand-489e2
gand-2abb7
gand-c8611
gand-c6b0f
gand-9febd
gand-0b33e
gand-9c973
gand-df002
gand-b7d1b
gand-c5440
gand-49d3c
gand-c8670
gand-20400
gand-a45db
gand-bdbca
gand-32b3d
gand-376e8
gand-91c38
gand-4a045
gand-7aa17
gand-429fb
gand-7ba3e
gand-aeccd
gand-ddbed
gand-c894c
gand-ec50c
gand-9b130
gand-cabe7
GetCurrentProcessId
GetModuleFileName
CryptAcquireContext

Combining it all

McAfee

Combining it all



McAfee

```
rule Ransom_Hunter {
  meta:
    title = "Hunting for ransomware samples"
    author = "Christiaan Beek @ChristiaanBeek"

  strings:
$s11 = "GetLastError" fullword // weight 3.54
 $s12 = "Sleep" fullword // weight 3.53
 $s13 = "EnterCriticalSection" fullword // weight 3.45
 $s14 = "SetFilePointer" fullword // weight 3.26
 $s15 = "GetCurrentThreadId" fullword // weight 3.18
 $s16 = "LeaveCriticalSection" fullword // weight 3.07
 $s17 = "DeleteCriticalSection" fullword // weight 3.03
 $s18 = "MultiByteToWideChar" fullword // weight 2.99
 $s19 = "TlsGetValue" fullword // weight 2.96
 $s20 = "WideCharToMultiByte" fullword // weight 2.86
 $s21 = "UnhandledExceptionFilter" fullword // weight 2.83
 $s22= "TerminateProcess" fullword // weight 2.79
……..

condition:

Private AND (( #s11 * 3.54) + (#$s12 * 3.53) + (#$s13 * 3.45)…… > certain value.
```

Questions?

THANK YOU

REVERSING 2020