Antivirus Detection Names

Antivirus detection names are useful for

TRIAGE

INDICATOR - MALWARE FAMILY IDENTIFICATION

INITIAL RISK ASSESSMENT

What is an antivirus detection name?

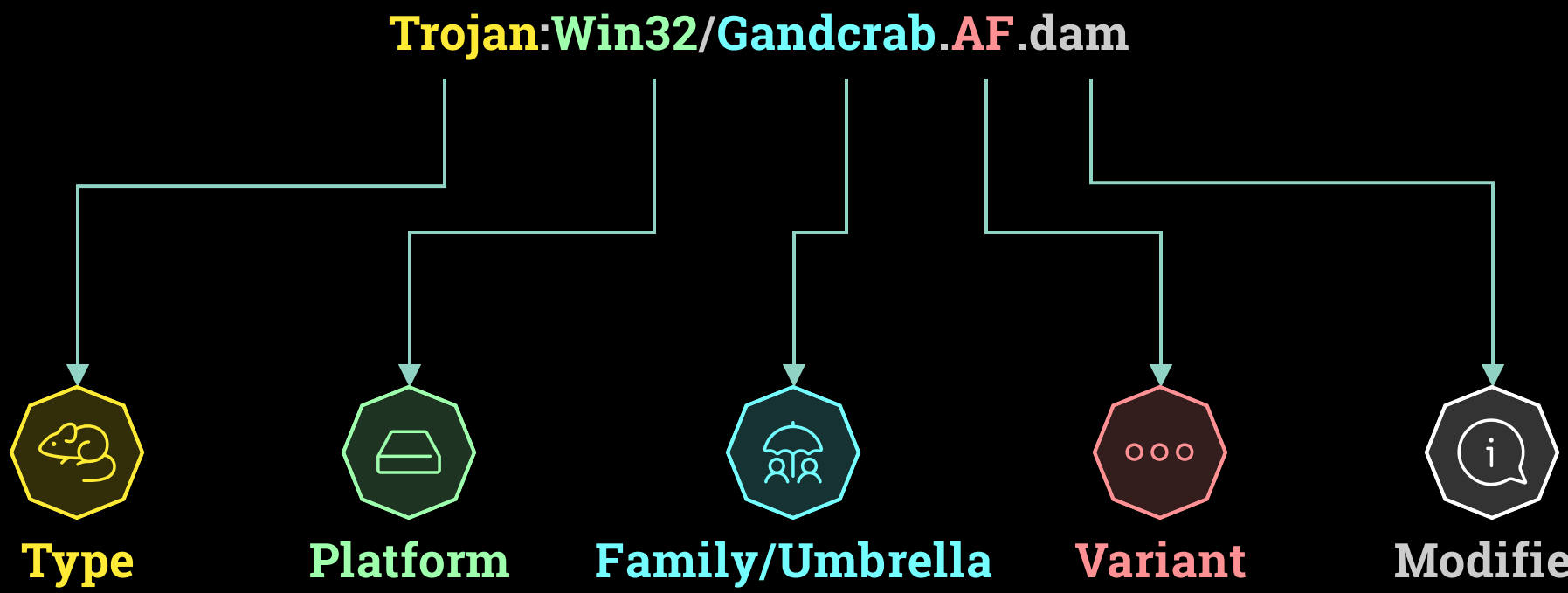
The malware name that an antivirus product shows upon finding malware artifacts on a system.

They are readable names which map to certain detection signatures or technologies.

Who creates antivirus detection names?

1. automatic systems
2. malware analysts

Basic Components



Basic Components

PLATFORM

- specifies execution environment
- e.g. language, framework, operating system, architecture

TYPE

- malware type
- describes main behavior of malware

FAMILY/UMBRELLA

- malware family or
- umbrella term or
- antivirus detection component

VARIANT

- signature counter or id
- internal info for antivirus company
- old: malware variant, but not applicable anymore

MODIFIER

- optional
- additional info about malware type or signature characteristics

Default values

TROJAN

- Default **Type** if actual malware type is unknown

AGENT

- Default for **Family/Umbrella** component

Antivirus vendors and their naming schemes

AV Vendor	Format	Example
Avast	Platform:Type1-Modifier \[Type2\]	VBS:Downloader-ARK [Trj]
AVG	Type Family.Variant	Trojan horse Crypt8.BHVG
Avira	Modifier/[Type.]Family.Variant	TR/AD.SodinoRansom.wcoir
Bitdefender	[Modifier:[Platform.]]Type.Family[.Modifier].Variant	Gen:Trojan.Mresmon.Gen.1
ESET	[Modifier] Platform/[Type.]Family.Variant Type	a variant of MSIL/TrojanDropper.Agent.BPM trojan
G DATA	Platform.Type.Family.Variant[@Modifier]	MSIL.Backdoor.Yantac.A@susp

Antivirus vendors and their naming schemes

AV Vendor	Format	Example
Kaspersky	[Modifier:]Type.Platform.Family[.Variant]	HEUR:Trojan.Win32.Nymaim.gen
McAfee	Platform/Family Type Platform/Family.Variant.Modifier	RDN/Generic BackDoor W32/HLLP.11042.gen
Microsoft	Type:Platform/Family.Variant[!Modifier]	Trojan:Win32/Reveton.T!lnk
Trendmicro (old)	Type_Family.Variant	TROJ_GEN.R002C0WGH19
Trendmicro (new)	Type.Platform.Family.Variant.Modifier	
Symantec	Type.Family.Variant Platform.Family.Variant	Trojan.Gen.MBT

Specific vs unspecific detection names

SPECIFIC

- more likely true positive
- most specific: identify malware family, e.g., WannaCry
- medium specific: name characteristics of malware, e.g., FakeAdobe

UNSPECIFIC

- more false positive prone
- mostly automatically created, without knowledge about the malware underneath
  - blocklist entries
  - machine learning
  - heuristic detection technologies

Specific vs unspecific detection names

SPECIFIC

tend to have small Variant component

- small variant: MSIL.Trojan-Spy.Cyborg.C
- long variant: MSIL.Trojan-Spy.Cyborg.LDJFSB

tend to have a concrete Type

do not use Agent as Family/Umbrella component

UNSPECIFIC - KEYWORDS

@gen, Gen, GEN, Generic

@susp, Suspicious, a variant of

HEUR, heuristic, Heur

Unsafe, Dangerous, Score, Malicious, confidence

!ml, .ml, AI

Agent

Kazy, Razy, Zusy, Graftor,

WisdomEyes, Artemis

Malicious_confidence_100% (W)	Cylance	Unsafe
W32/Trojan.QCQR-8401	DrWeb	Trojan.Gozi.345
Unsafe.AI_Score_100%	Emsisoft	Trojan.Agent.DGAT (B)
Malicious (high Confidence)	eScan	Trojan.Agent.DGAT
Win32/Spy.Ursnif.BP	F-Secure	Trojan.Agent.DGAT
W32/Agent.FFF1!tr	GData	Trojan.Agent.DGAT
Trojan.Win32.Krypt	K7AntiVirus	Spyware (0052a9701)
Spyware (0052a9701)	Kaspersky	Trojan-Spy.Win32.Ursnif.aahi
Trojan.FakeMS	McAfee	Artemis!15B2A3D1E076
Artemis!Trojan	Microsoft	TrojanSpy:Win32/Wastenif
Trojan.Win32.Ursnif.fisrkm	Palo Alto Networks	Generic.ml
Trj/CI.A	Qihoo-360	Win32/Trojan.Spy.fd1
Spyware.Ursnif!8.1DEF (CLOUD)	Sophos AV	Troj/Agent-AZXV
Heuristic	Symantec	Trojan Horse
Win32.Trojan-spy.Ursnif.Dzag	Trapmine	Malicious.high.ml.score
TROJ_GEN.F0C2C00J518	TrendMicro-HouseCall	TROJ_GEN.F0C2C00J518
TrojanSpy.Ursnif!SgNrrf7pyRI	ZoneAlarm by Check Point	Trojan-Spy.Win32.Ursnif.aahi

Legend

green - specific, includes family identification

blue - specific, descriptive without identification

not marked - unspecific, no information

Key words in Umbrella names

Key word	Meaning
Kryptik, Krypt, Cryptik, Crypt, Packed	Packed file
Obfus	Obfuscated file, mostly used for malicious script files
Injector, Inject	Packed file that injects into a process
AntiXY	Protection mechanism against XY, e.g. AntiAV means the file might incapacitate AV programmes, AntiVM means it might refuse to run in a Virtual Machine
FakeXY, XYFake	The file imitates XY, e.g. FakeAdobe imitates an Adobe product. This is often done via third party tools that change the icon and version information of the file
Corrupt, Corrupted, Malformed	The file is corrupt.

Key words in Umbrella names

Key word	Meaning
Patched	The file was modified which makes it suspicious.
Agent	Default name for unknown or insignificant malware family
Razy, Kazy, Zusy, Graftor	Bitdefender technology
WisdomEyes	Baidu technology
Artemis	McAfee technology

Myth 1

~~**DETECTION NAMES ARE A FORM OF MALWARE CLASSIFICATION**~~

Detection names are mappings to Antivirus signatures or Antivirus technologies.

They often do not identify malware at all and sometimes incorrectly.

Myth 2

~~"TROJAN" MEANS THE MALWARE IS A TROJAN HORSE~~

For most AV vendors "Trojan" is the default value for the Type component.

Whenever the actual malware type is unknown, "Trojan" is used.

"Trojan" in a detection name has no meaning.

Myth 3

~~CARO NAMING CONVENTIONS DESCRIBE TODAY'S DETECTION NAMES~~

The CARO naming conventions were an attempt to classify malware but they are not applicable for today's malware landscape.

Today's detection names are influenced by CARO but have their own naming schemes.