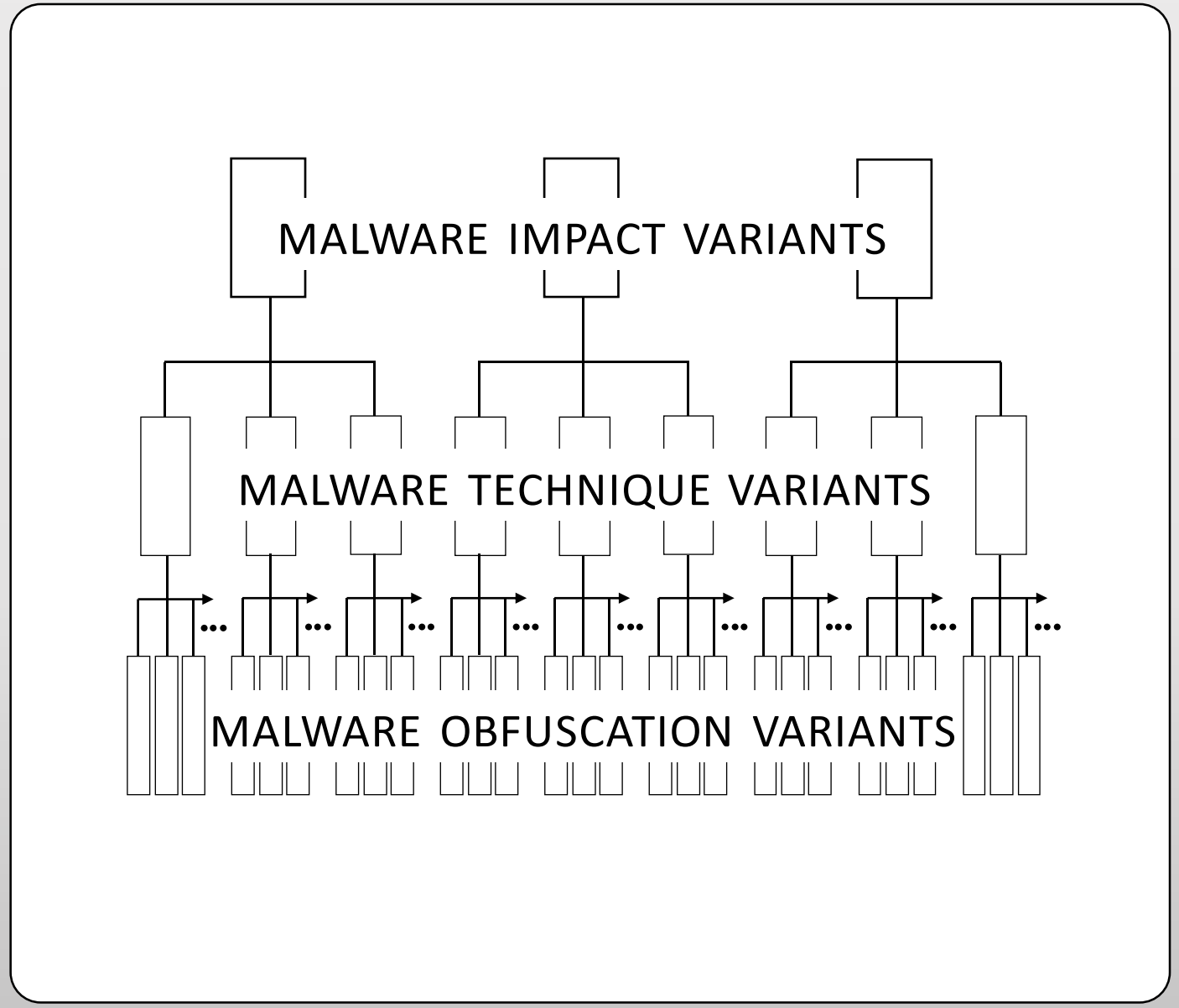
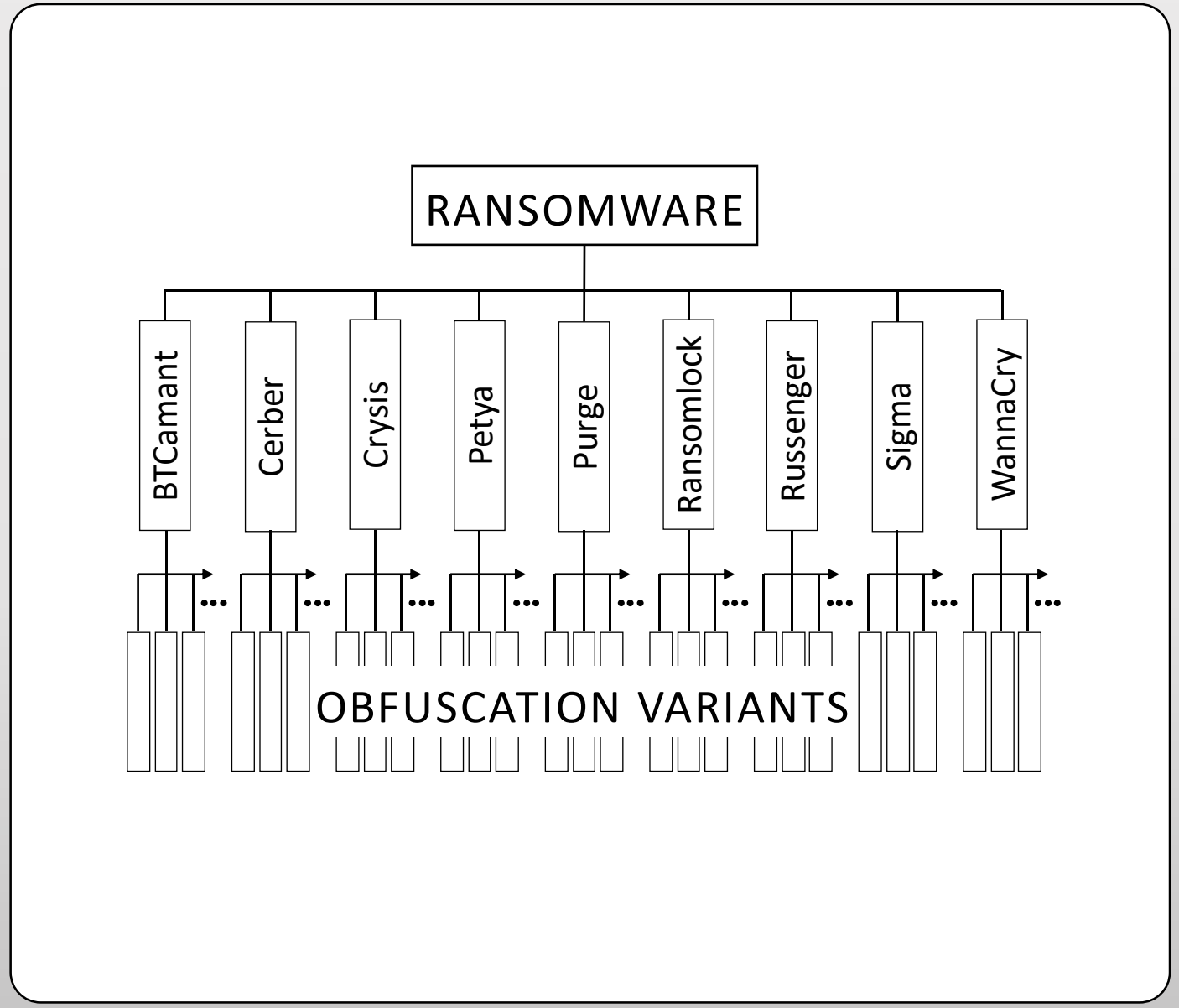
Hierarchical Classes of Malware

Variation of malware binaries may be considered hierarchically by categorizing malware first by cyber-threat type (malware impact), second by malware family (malware technique), and third by detection evasion polymorphs and metamorphs (obfuscation variation).



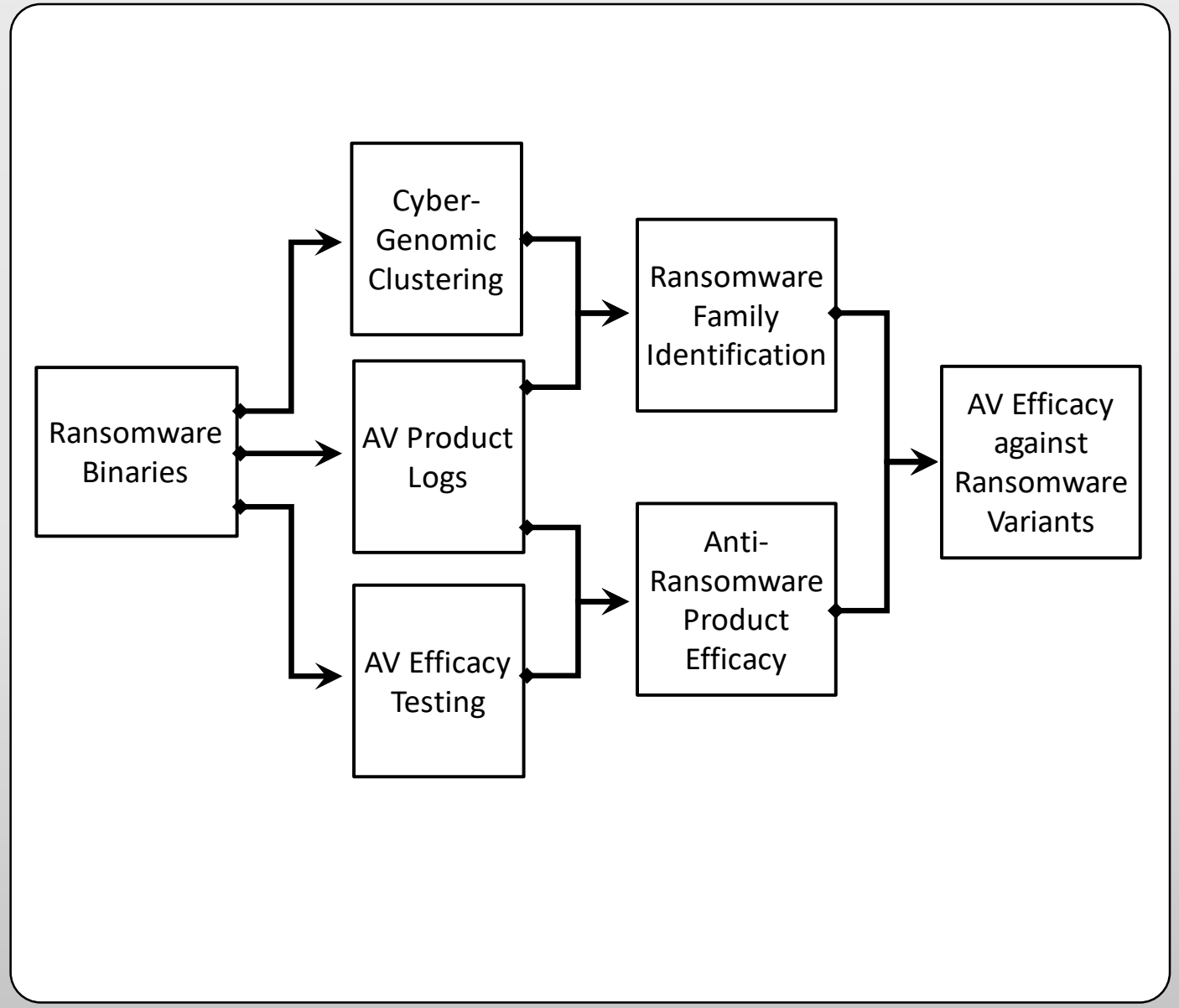
Hierarchy for Ransomware

This study focuses on the obfuscation variants of ransomware binaries. Candidate binaries were filtered for: (i) malicious ransomware functionality; (2) usability in simulated ransomware attacks in testing labs; (3) susceptibility to cyber-genomic cluster analysis.



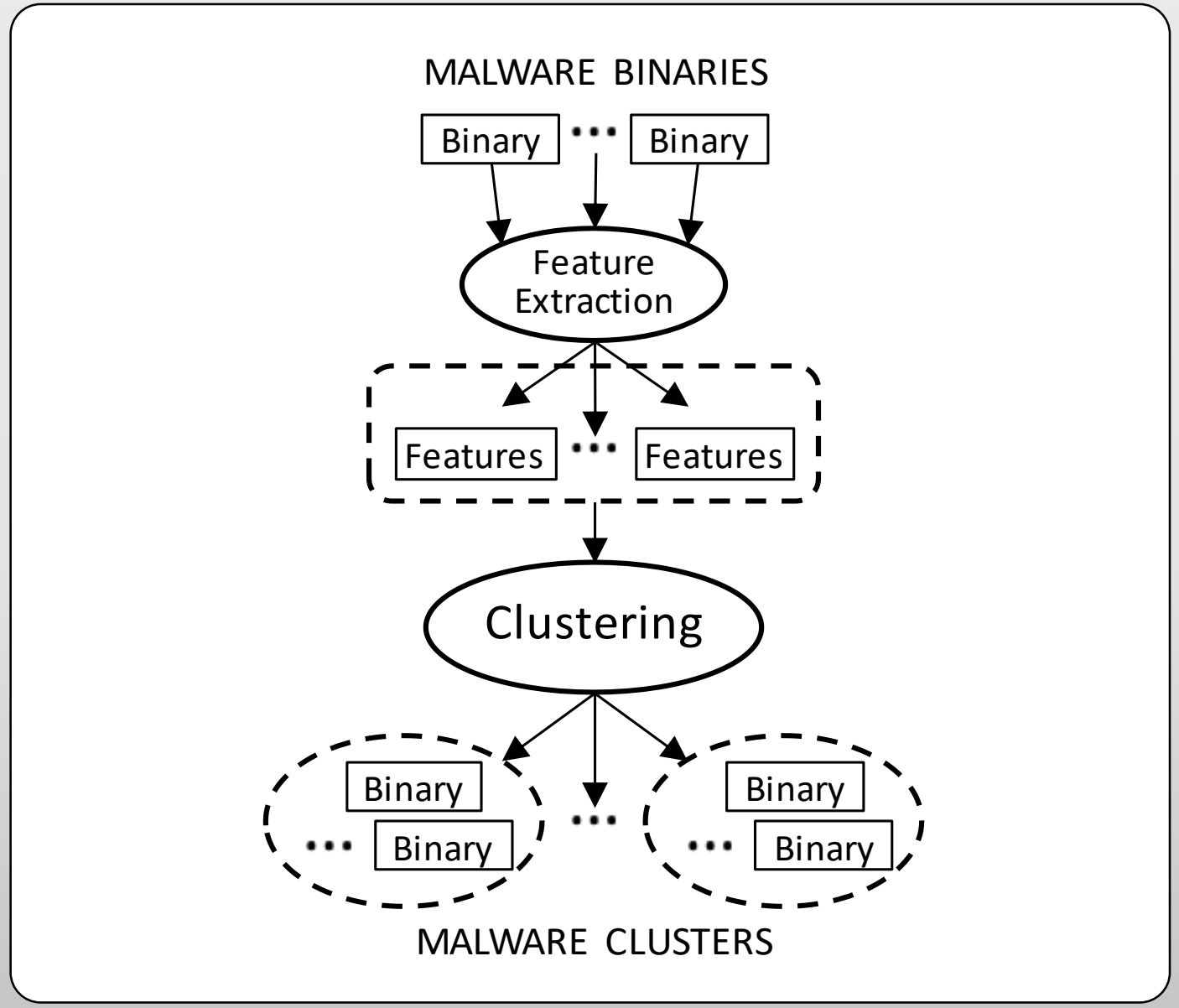
Experiment Process Flow

Experiment process flow. Ransomware binaries were used to determine the ability of anti-malware products to detect obfuscation variants (e.g., polymorphs) of particular ransomware families.



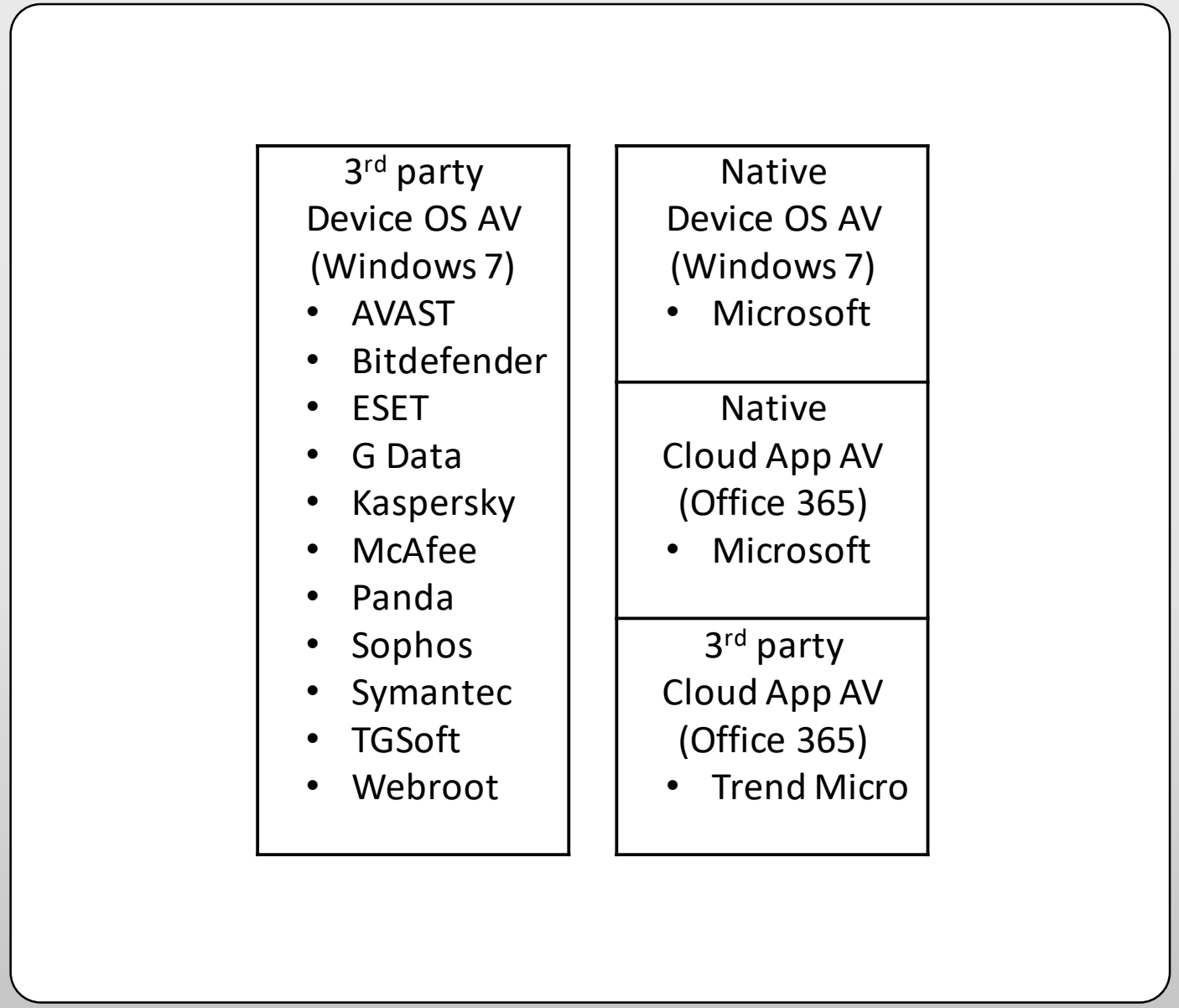
Cyber-Genomic Clustering

General process for cyber-genomic clustering of malware binaries into malware clusters.



Anti-Malware Products

Anti-malware products used in this study.



Anti-Malware Comparative Tests

In this study, anti-malware test results from several independent test labs were used for comparison. In general, there were three types of tests used: (i) general malware variants; (ii) ransomware variants; and (iii) variants of the WannaCry ransomware.

Reference AV Product Test	Independent Test Lab	Test Date	Test Report
Real World Protection Test	AV Comparatives *Austria*	Jul-Nov 2017	[T1]
Anti-Ransomware Test	AVLab *Poland*	Oct 2016	[T2]
Real World Testing (0 Day)	AV-Test *Germany*	Nov-Dec 2017	[T3]
Anti-Ransomware Test	MRG-Effitas *UK/Serbia*	Apr 2017	[T4]
Cloud Application Security Test	Veszprog *Hungary*	Jan 2018	[T5]
Reactive & Proactive Tests	Virus Bulletin *UK*	Dec 2017	[T6]

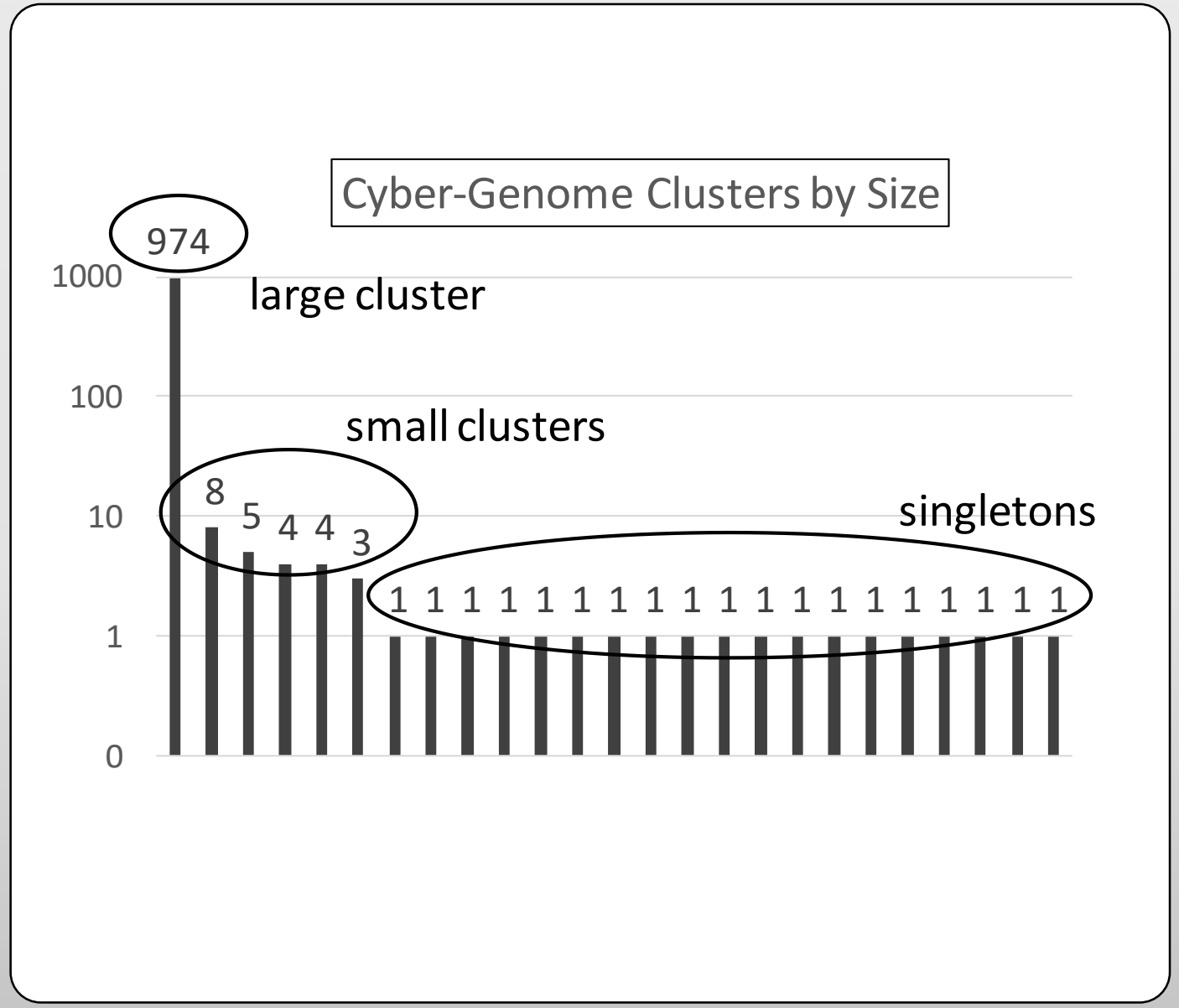
Ransomware Families

Ransomware family names identified in the clusters of ransomware binaries.

Ransomware Family	also known as	Enigma removal reference
BTCamant	HydraCrypt Genasom	[E1]
Cerber	HPCerber Zerber	[E2]
Crypto-Blocker	Blocker	[E3]
Crysis	Crusis Criaki	[E4]
Globe		[E5]
GlobeImposter	FakeGlobe	[E6]
Petya	Petr	[E7]
Purge	Purgen	[E8]
Ransomlock	Foreign Reveton	[E9]
Russenger		[E10]
Sigma		[E11]
UmbreCrypt	HydraCrypt	[E12]
WannaCryptor	WannaCry WanaCrypt	[E13]

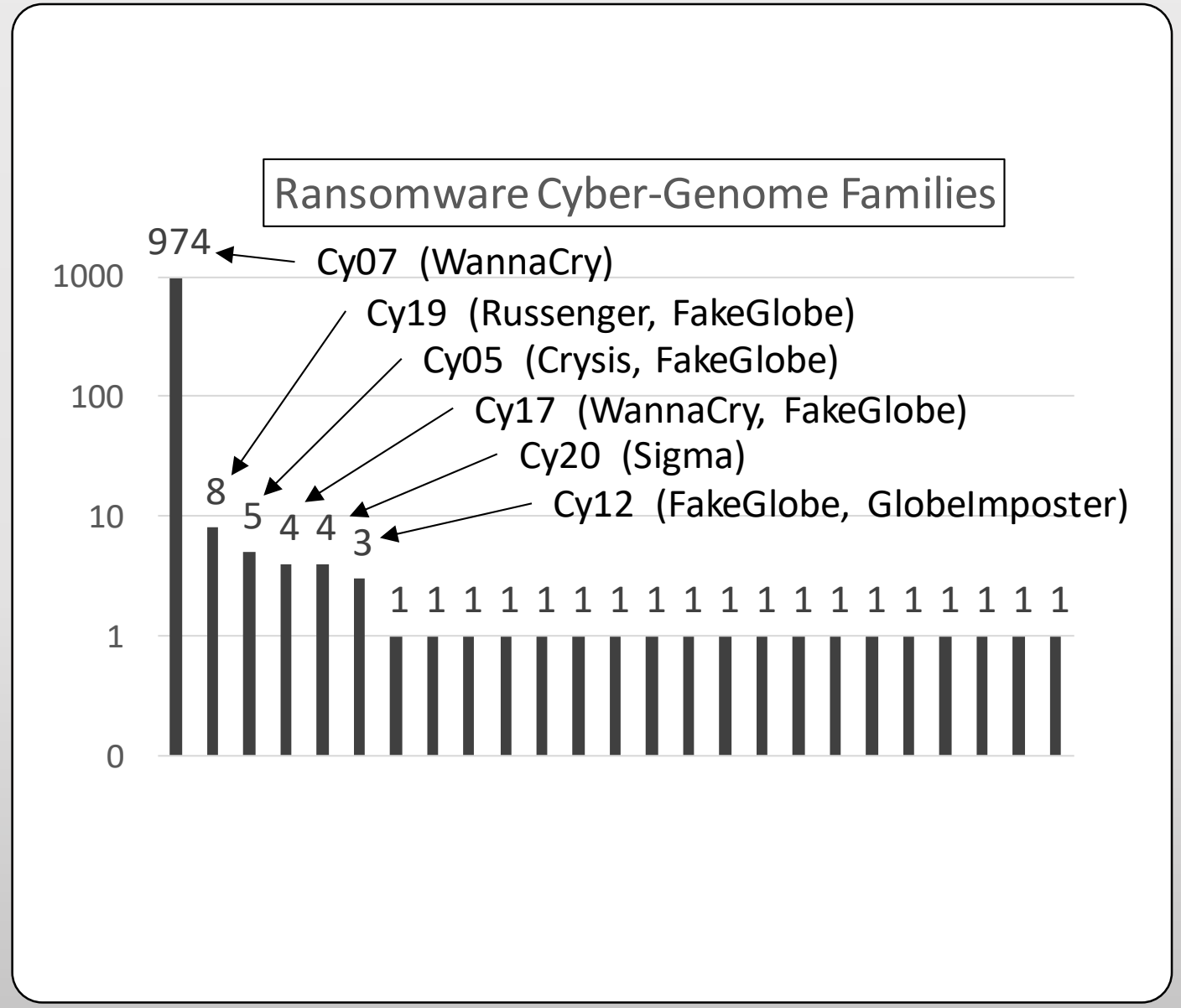
Cyber-Genome Clusters by Size

Cyber-genomic analysis was used to cluster ransomware binaries according to observable traits in each binary.



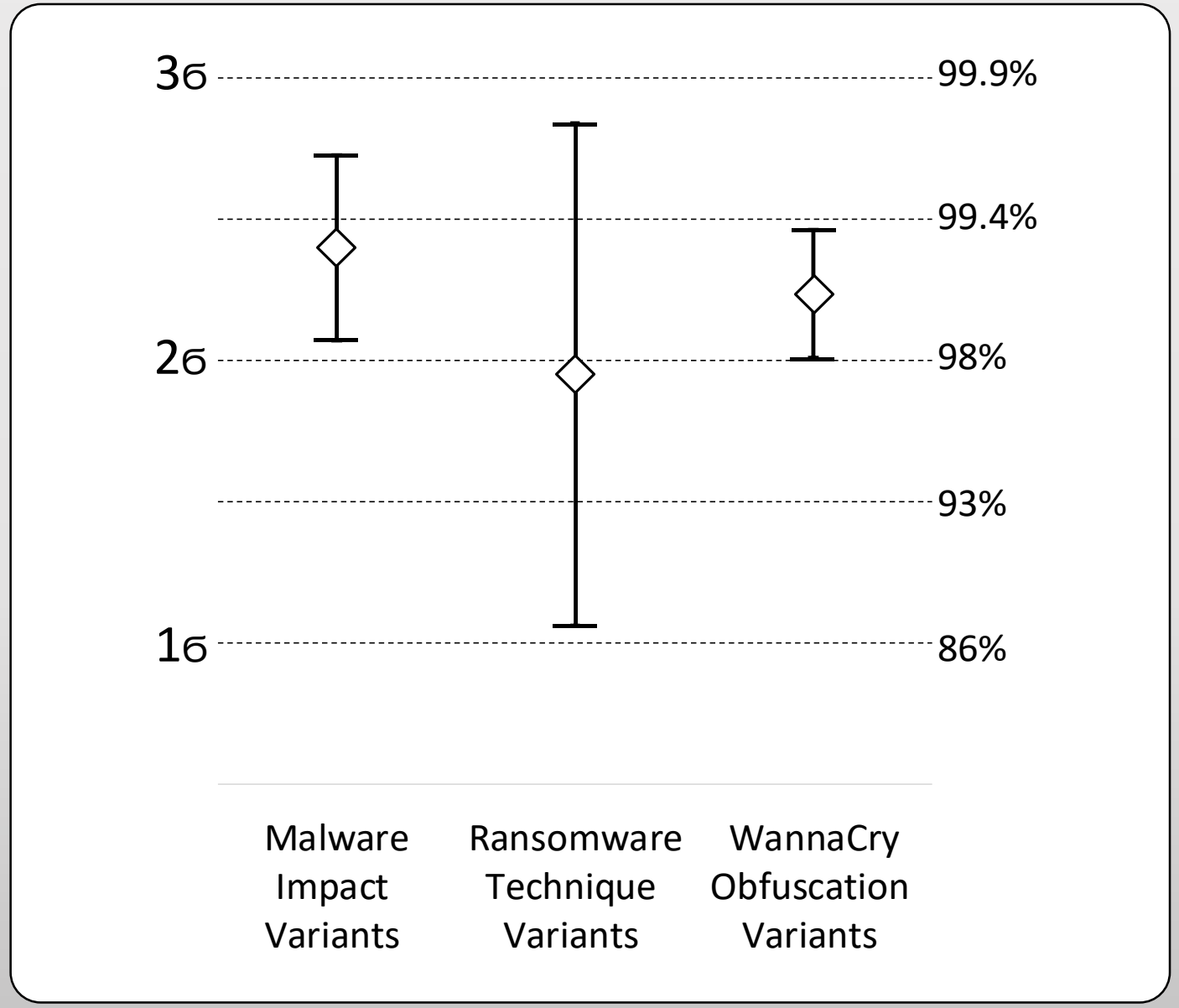
Aligning Clusters to Families

AV log files for 11 AV products provided some association between clusters and ransomware families but with limited consensus across products within clusters.



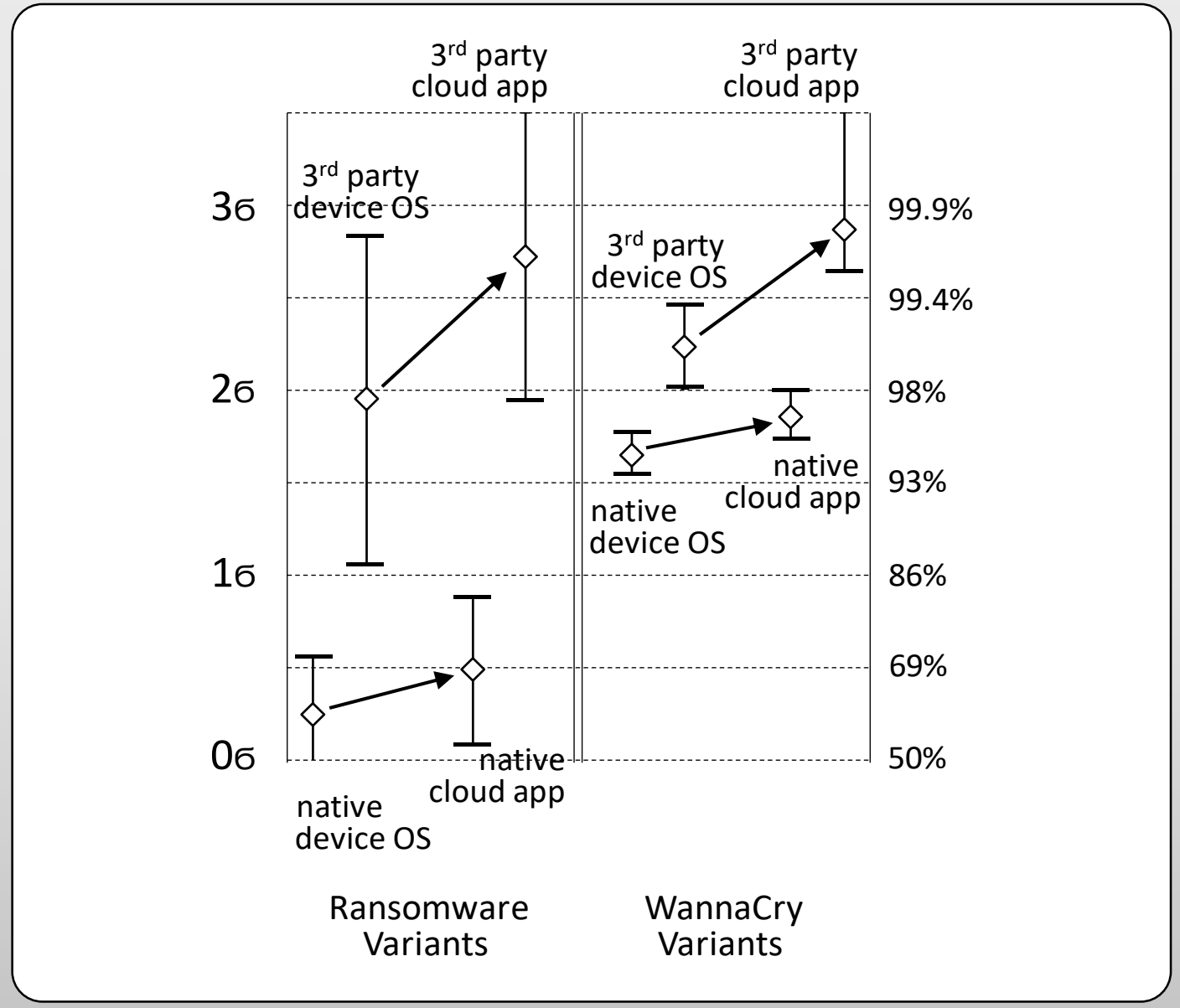
3rd Party Device OS AV Products

Malware variant detection rate by 3rd party device OS anti-malware products for three hierarchical levels of malware variation.



Device OS AV vs. Cloud App AV

Cloud app AV (user account) provides greater protection than device OS AV (endpoint) in measurements with and without supplemental 3rd party protection against variants of WannaCry and against ransomware variants in general.



Inferior Cloud App AV ?

The illusion that cloud app AV is inferior to device OS AV arises from the false comparison of 3rd party device OS AV with native cloud app AV.