Number of malwares 75 魚拓: https://pcmatic.jp/pro/security/Detection_capture.pdf 最新版: https://pcmatic.jp/pro/security/Detection_realscore.pdf

VIRUSTOTAL

AV Engine detections by VirusTotal from the latest security colums (マルウェア起動防御率)

【主旨】各社AVエンジンのマルウェア検知速度をVirusTotalによって測定した結果。PC Maticマルウェア分析官が24時間以内にデジタルフォレンジックを完了するまでの間、顧客企業が緊急的に起動許可を与えるためローカルホワイトリストへ追加後、マルウェアを確実に停止できるエンジン選定の参考資料として作成。即座にマルウェアを検出する能力が高くなければ併用する意味がないため。

【注意点】マルウェアが検出できなくても、ヒューリスティックエンジンにより実行プロセスが強制終了させられるなどマルウェアが活動できない場合もあるため、本表で「0」でも、必ずしもマルウェア感染が発生する訳ではない。また「1」のマルウェアと判定されているエンジンであっても、VirusTotalにマルウェア検体が送信された直後はマルウェアとして判定できず、本表での経過時間内にマルウェアとして判定されるまでの間は、マルウェア感染が発生する可能性がある。アプリケーション・ホワイトリスティング方式のエンジン(PC Matic等)の場合、マルウェアのハッシュ値が起動許可に分類されていない場合は、マルウェア起動阻止による防御とした。同種エンジンでは、マルウェア分析官により善良との判断により起動許可が与えられない限り、実行可能ファイルは起動できないためマルウェア感染は発生しない。

PC Matic 個人版 Microsoft Defender以外併用不可。法人版は単体利用も併用も可能

記事掲載	報告後経過日数	マルウェア名称とリンク	全体検出率	Acronis	Avast AVG	Avira	BitDefender (スーパーセキュリティZERO)	Cylance	CrowdStrike Falcon	ESET	F-Secure	Fortinet	K7 (ウイルスセキュリティZERO)	Kaspersky	Malwarebytes	McAfee (個人版)	Microsoft Defender (Windows標準)	Panda (Watchguard)	PC Matic	Sophos	Symantec (notron)	Trendmicro	Webroot
				マルウェア起動防御率																			
				8%	75%	51%	63%	50%	42%	72%	28%	76%	40%	85%	32%	69%	71%	44%	100%	53%	84%	44%	37%
2023/9/27	43	ZenRAT Malware	70%	0	1	0	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1	0	0
2023/8/25	*	CollectionRAT	55%	0	1	0	1	1	0	1	0	1	0	1	0	1	1	0	1	1	1	0	0
2023/8/23	*	Bronze Starlight espionage campaign	80%	0	1	1	0	1	1	0	1	1	0	1	1	1	1	1	1	1	1	1	1
2023/8/23	*	Scarab Ransomware	20%	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	1	0	0	0	1
2023/8/19	*	Chinese espionage campaign	80%	1	1	1	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	0	0
2023/8/9	*	Vietnamese WannaCry	85%	1	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0
2023/8/8	*	ScarCruft stealer	85%	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1
2023/8/2	*	Vietnamese novel campaign	85%	0	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1
2023/8/1	*	STARK#MULE Attack Campaign	85%	0	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	0
2023/7/25	*	Novel Open Source Supply Chain Attack	35%	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1	0	0
2023/7/20	*	WyrmSpy	45%	0	1	0	0	0	0	1	0	1	1	1	0	1	1	0	1	0	1	0	0
2023/7/19	*	Revamped Sardonic Backdoor	25%	0	0	0	1	0	0	0	0	0	0	1	0	0	1	0	1	0	1	0	0
2023/7/15	*	LokiBot Campaign	60%	0	1	1	1	0	0	1	1	1	0	1	0	1	1	0	1	0	1	1	0
2023/7/4	*	SmugX Campaign	50%	0	1	0	1	0	0	1	0	1	1	1	0	1	0	0	1	1	1	0	0
2023/6/29	*	ThirdEye Infostealer	95%	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2023/6/27	*	IcedID DLL payload	70%	0	1	0	1	1	0	1	0	1	1	1	1	1	1	1	1	1	1	0	0
2023/6/22	*	Backdoor by Flea	70%	0	1	1	0	1	1	0	0	1	0	1	1	1	1	1	1	1	1	0	1
2023/6/20	*	OnlyDcRatFans Malware	30%	0	1	0	1	0	0	0	0	1	0	1	0	0	0	0	1	0	1	0	0
2023/6/19	*	Mystic Stealer	95%	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2023/6/16	*	Shuckworm powershell	45%	0	1	0	1	0	0	1	1	1	0	1	0	0	0	0	1	1	1	0	0
2023/6/9	*	Stealth soldier backdoor	85%	0	1	1	1	1	0	1	1	1	0	1	1	1	1	1	1	1	1	1	1
2023/6/1	*	Horabot Banking trojan	85%	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1
2023/5/26	*	CosmicEnergy malware	20%	0	0	0	0	0	0	1	0	0	0	1	0	1	0	0	1	0	0	0	0
2023/5/12	*	Greatness phishing	42%	0	1	0	1	0	0	1	0	1	0	1	0	1	0	0	1	0		1	0
2023/5/11	*	Aurora stealer	53%	0	1	0	1	1	0	1	0	1	0	0	1	1	0	0	1	1		0	1
2023/5/7	*	trojanized LetsVPN installer	42%	0	1	1	0	0	0	0	1	1	0	1	0	0	0	0	1	1		0	1
2023/5/4	*	double DLL sideloading	42%	0	1	1	0	0	0	1	1	1	0	1	0	0	0	0	1	1		0	0

2023/5/4	*	Earth Longzhi rootkit	53%	0	0	0	1	1	1	1	0	1	0	1	0	1	0	0	1	1		1	0
2023/5/2	*	ROKRAT APT(mfc100.dll)	70%	0	1	1	1	1	1	0	1	1	1	1	0	1	1	0	1	1	0	0	1
2023/4/29	*	ViperSoftX info-stealing malware	15%	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0
2023/4/26	*	PowerLess Backdoor by Iranian	15%	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	1	0	0
2023/4/25	*	PaperCut exploite	5%	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
2023/4/25	*	Tomiris Golang implant	85%	0	1	1	1	1	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1
2023/4/22	*	Bumblebee Malware	55%	0	1	1	1	0	0	1	1	1	0	1	0	0	1	0	1	0	1	1	0
2023/4/22	*	W32/EvilExtractor.A!tr	25%	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	1	0	0
2023/4/21	*	MgBot Malware	60%	0	1	1	1	1	1	0	1	1	0	1	0	1	0	1	1	0	1	0	0
2023/4/19	*	Carbanak Backdoor	85%	0	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
2023/4/14	*	GuLoader	40%	0	1	1	1	0	0	0	1	0	0	1	0	0	1	0	1	0	1	0	0
2023/4/13	*	Lazarus DeathNote Campaign	90%	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1
2023/4/12	*	Nokoyawa ransomware	95%	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2023/4/6	*	CryptoClippy	15%	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	1	0	0
2023/4/5	*	eFile.com hacked trojan	25%	0	0	0	0	0	1	0	0	0	0	1	0	1	1	0	1	0	0	0	0
2023/4/5	*	ALPHV Ransomware variant	80%	0	1	0	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0
2023/4/4	*	Money Message double extortion attack	95%	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2023/3/31	*	3CX Supply Chain Attack	40%	0	0	0	0	0	0	1	0	1	1	0	0	0	1	0	1	1	1	1	0
2023/3/29	*	clipboard-injector attack	30%	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	1	1	0	1
2023/3/27	*	Dark Power ransomware	80%	0	1	1	1	1	1	1	0	1	1	1	0	1	1	1	1	0	1	1	1
2023/3/24	*	PowerMagic backdoor	55%	0	1	1	1	0	0	1	0	1	0	1	0	1	1	0	1	0	1	1	0
2023/3/24	*	BlackGuard stealer 新種	80%	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	0	0
2023/3/24	*	Gallium APT41 trojan	70%	0	1	1	1	0	1	1	0	1	1	1	0	1	1	1	1	0	1	0	1
2023/3/23	*	NAPLISTENER	15%	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1
2023/3/22	*	PowerMagic installer	55%	0	1	1	1	0	0	1	0	1	0	1	0	1	1	0	1	0	1	1	0
2023/3/20	*	EMOTET Variant dll 亜種	85%	0	1	1	1	0	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
2023/3/17	*	Winter Vivern payload Aperetif	70%	0	1	1	1	1	0	1	0	1	0	1	0	1	1	1	1	0	1	1	1
2023/3/17	*	BianLian Ransomware	70%	0	1	1	1	0	1	1	0	1	1	0	0	1	1	1	1	1	1	1	0
2023/3/17	*	SILKLOADER dropper	65%	0	1	1	1	1	0	1	0	1	0	1	0	1	1	1	1	0	1	1	0
2023/3/9	*	SYS01 Stealer trojan	55%	0	1	1	0	0	0	1	0	1	1	1	0	1	1	0	1	0	1	0	1
2023/3/8	*	EMOTET Variant dll 新種	10%	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0
2023/3/4	*	MedusaLocker ransomware	50%	0	1	0	1	0	0	1	0	0	0	1	0	1	1	1	1	1	1	0	0
2023/3/3	*	MQsTTang backdoor.	70%	0	1	1	1	0	1	1	0	1	1	1	0	1	1	1	1	0	1	0	1
2023/2/28	*	EXFILTRATOR-22	50%	0	1	0	1	0	1	1	0	0	1	1	0	1	1	0	1	0	1	0	0
2023/2/28	*	PureCrypter downloader	60%	1	1	1	1	1	0	1	0	1	1	1	0	0	1	0	1	0	1	0	0
2023/2/27	*	PureCrypter	65%	1	1	1	1	1	0	1	0	1	1	1	0	0	1	0	1	0	1	1	0
2023/2/24	*	Backdoor.Atharvan	26%	0	0	0	0		0	0	0	0	0	1	0	1	0	0	1	0	1	0	1
2023/2/24	*	WinorDLL64	50%	0	0	0	0	1	1	1	0	0	0	1	0	1	1	0	1	1	1	1	0
2023/2/20	*	WhiskerSpy Backdoor	30%	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	1	1	0	1	0
2023/2/18	*	OxtaRAT Backdoor	40%	0	1	0	0	1	0	1	0	1	0	0	0	1	0	0	1	1	0	0	1
2023/2/16	*	havocC2	80%	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	0	1	1	0
2023/2/11	*	Maui ransomeware	55%	0	1	0	0	0	0	1	0	1	1	0	1	1	1	0	1	1	1	1	0
2023/2/11	*	WasabiSeed VBS	40%	0	1	0	0	0	0	1	0	1	0	1	0	0	1	0	1	0	1	1	0
2023/2/10	*	Downloader.Graphiron	79%	0	0	1	1	1		1	0	1	1	1	1	1	1	1	1	0	1	1	1
2023/2/10	*	Enigma_Downloader	75%	0	1	1	1	1	0	0	1	1	0	1	1	1	1	1	1	1	1	1	0

2023/2/7	*	Silver malware	53%	0	1	0	1	1		0	0	1	0	1	0	1	0	0	1	1	1	1	0
2023/1/23	*	Boldmove	30%	0	0	1	0	0	0	1	0	1	0	0	0	0	1	0	1	0	1	0	0
2023/1/20	*	Vidars 1.8	32%	0	0	0	1	0		1	0	0	0	1	0	0	1	0	1	1	0	0	0

検出…1 / 検出なし…0