Отчет Virustotal PDF

Список антивирусов, которые обнаружили угрозы.

Lionic, MicroWorld-eScan, Sangfor, Symantec, ESET-NOD32, Avast, Kaspersky, BitDefender, Emsisoft, DrWeb, VIPRE, FireEye, GData, Google, Kingsoft, Arcabit, Microsoft, Varist, Tencent, CTX, Ikarus, Fortinet, AVG, alibabacloud

Список антивирусов, которые не обнаружили угрозы.

Bkav, ClamAV, CMC, CAT-QuickHeal, Skyhigh, ALYac, Malwarebytes, Zillya, K7AntiVirus, K7GW, CrowdStrike, Baidu, VirIT, TrendMicro-HouseCall, Cynet, NANO-Antivirus, SUPERAntiSpyware, Rising, F-Secure, TrendMicro, Sophos, huorong, Jiangmin, Avira, Antiy-AVL, Gridinsoft, Xcitium, ViRobot, AhnLab-V3, Acronis, McAfee, TACHYON, VBA32, Zoner, Yandex, MaxSecure, Panda, Avast-Mobile, SymantecMobileInsight, BitDefenderFalx, McAfeeD, Elastic, APEX, Paloalto, Trapmine, Alibaba, Webroot, Cylance, SentinelOne, tehtris, Trustlook, DeepInstinct

Сравнение с заданным списком.

Fortinet	обнаружил
McAfee	не обнаружил
Yandex	не обнаружил
Sophos	не обнаружил

Обнаруженные уязвимости

Lionic	Trojan.Script.Chartres.4!c
MicroWorld-eScan	GT:VB.Heur2.Chartres.1.FE9B894C
Sangfor	Trojan.Generic-Macro.Save.ec3db0ab
Symantec	Trojan.Gen.NPE
ESET-NOD32	VBA/TrojanDropper.Agent.AXB
Avast	Other:Malware-gen [Trj]
Kaspersky	UDS:DangerousObject.Multi.Generic
BitDefender	GT:VB.Heur2.Chartres.1.FE9B894C
Emsisoft	GT:VB.Heur2.Chartres.1.FE9B894C (B)
DrWeb	X97M.DownLoader.459
VIPRE	GT:VB.Heur2.Chartres.1.FE9B894C
FireEye	GT:VB.Heur2.Chartres.1.FE9B894C
GData	GT:VB.Heur2.Chartres.1.FE9B894C
Google	Detected
Kingsoft	Win32.Infected.AutoInfector.a
Arcabit	GT:VB.Heur2.Chartres.1.FE9B894C
Microsoft	Trojan:O97M/Obfuse.CP
Varist	ABTrojan.KOEJ-
Tencent	Script.Trojan-Downloader.Generic.Mcnw
CTX	txt.trojan.chartres
Ikarus	Trojan-Dropper.VBA.Agent
Fortinet	VBA/Agent.BCF0!tr
AVG	Other:Malware-gen [Trj]
alibabacloud	Trojan[dropper]:MSOffice/Obfuse.CX

Ключевые моменты из отчёта VirusTotal Sandbox о поведении вредоноса.

Список доменов и IP-адресов, с которыми вредонос общается.

Hostname	IP
fp2e7a.wpc.phicdn.net	192.229.211.108
fp2e7a.wpc.2be4.phicdn.net	

Использованные техники атак:

T1071
T1497
T1497
T1497
T1057
T1010
T1083
T1083
T1082
T1082

Файл проанализирован следущими песочницами:

CAPE Sandbox, VirusTotal Jujubox, VirusTotal Observer, Zenbox