# Отчет Virustotal [PDF]

### Список антивирусов, которые обнаружили угрозы.

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

### Список антивирусов, которые не обнаружили угрозы.

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

### 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 |
| ClamAV | Xls.Dropper.Agent-7398287-0 |
| CTX | txt.trojan.chartres |
| Sangfor | Trojan.Generic-Macro.Save.ec3db0ab |
| Arcabit | GT:VB.Heur2.Chartres.1.FE9B894C |
| 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 |
| Tencent | Script.Trojan-Downloader.Generic.Mcnw |
| 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 |
| Google | Detected |
| Kingsoft | Win32.Infected.AutoInfector.a |
| Microsoft | Trojan:O97M/Obfuse.CP |
| ViRobot | HTML.Z.Agent.48950 |
| ZoneAlarm | HEUR:Trojan-Downloader.Script.Generic |
| GData | GT:VB.Heur2.Chartres.1.FE9B894C |
| Varist | ABTrojan.KOEJ- |
| MAX | malware (ai score=82) |
| Ikarus | Trojan-Dropper.VBA.Agent |
| Fortinet | VBA/Agent.BCF0!tr |
| AVG | Other:Malware-gen [Trj] |

### 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