Научно-исследовательская работа на тему: «Вирусология»

Подготовили ученики 10 «Б» класса:
Петров Семён и Могилевский Матвей
Научный руководитель:
Манузина Любовь Леонидовна

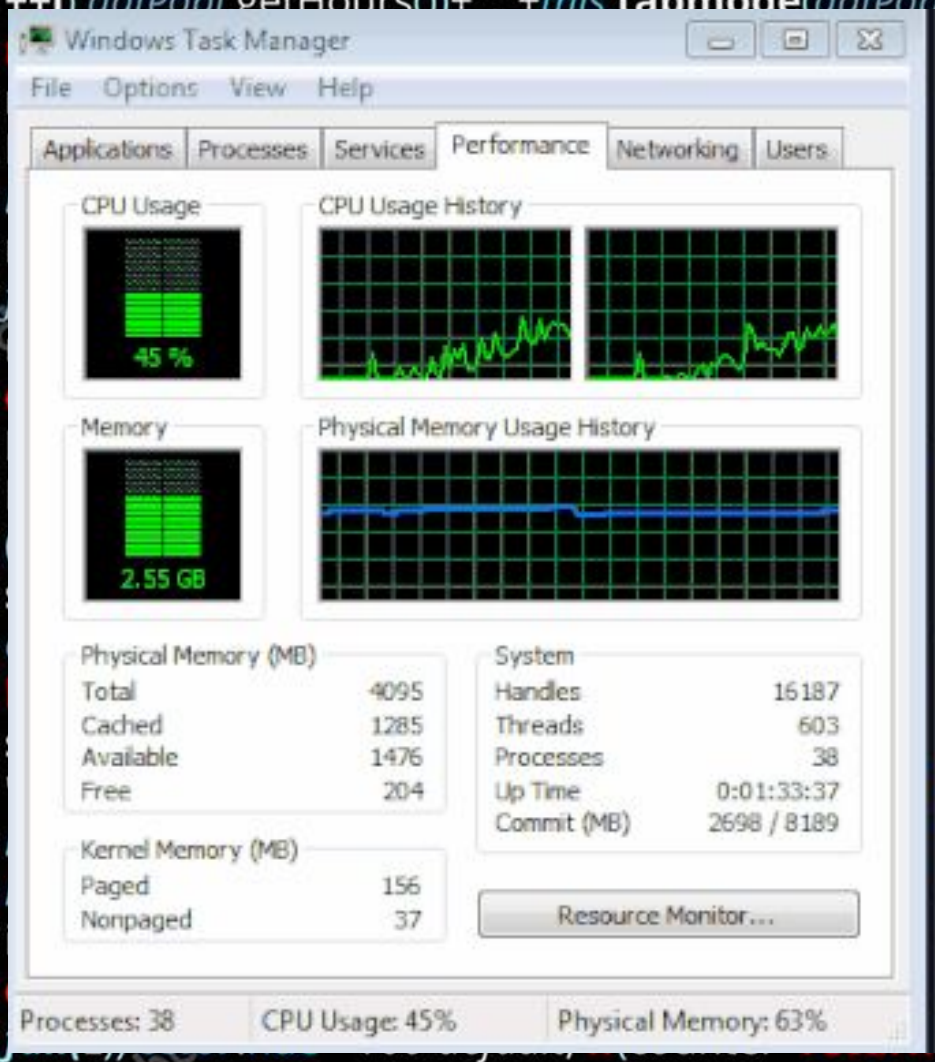
*Цель работы: Исследовать механизм работы некоторых вирусов и рассказать об опасности заражения вашего **ПК***

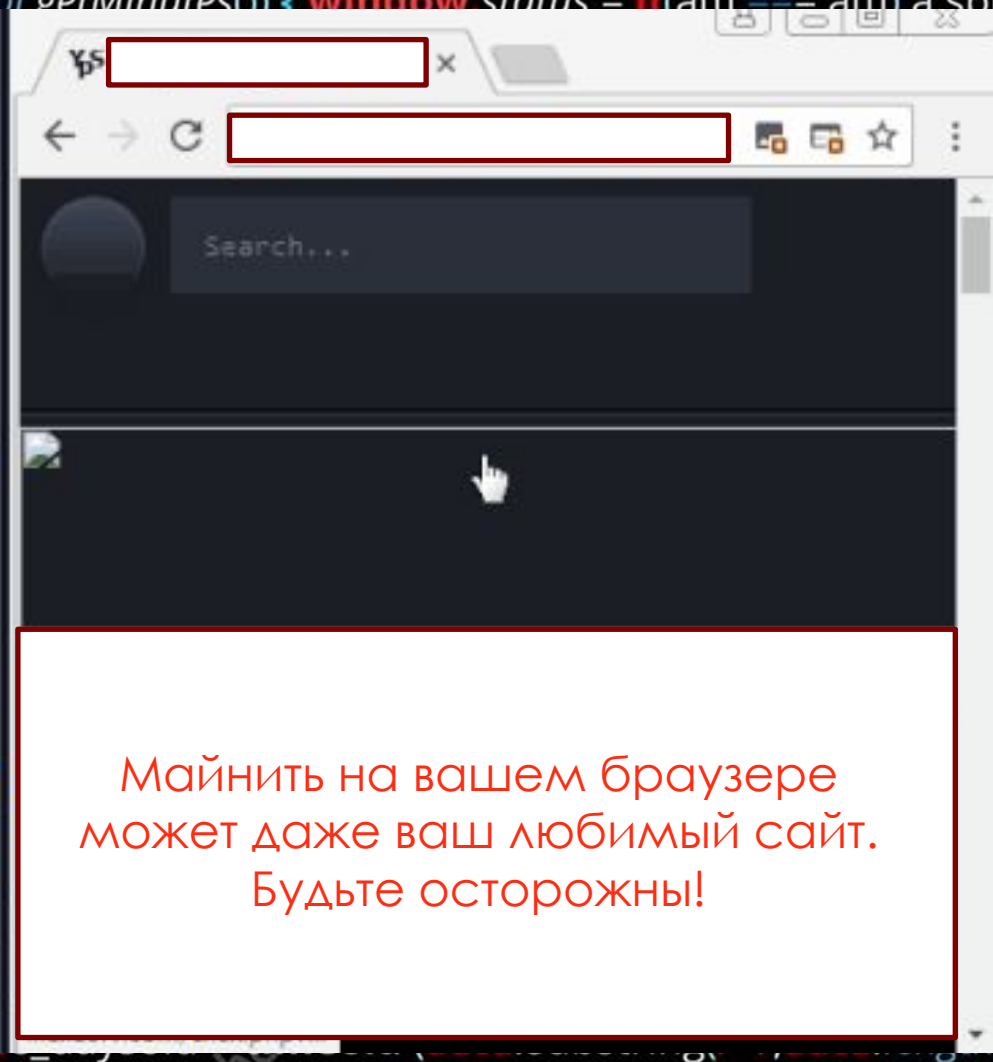
OneDrive

Что такое майнер?

- Вирус (от англ. *mining — добыча полезных ископаемых)*
- Использует ресурсы вашего компьютера
- Используется для пассивного заработка

Майнинг в браузере





Майнить на вашем браузере
может даже ваш любимый сайт.
Будьте осторожны!

RAT — *Remote Administration Tool*

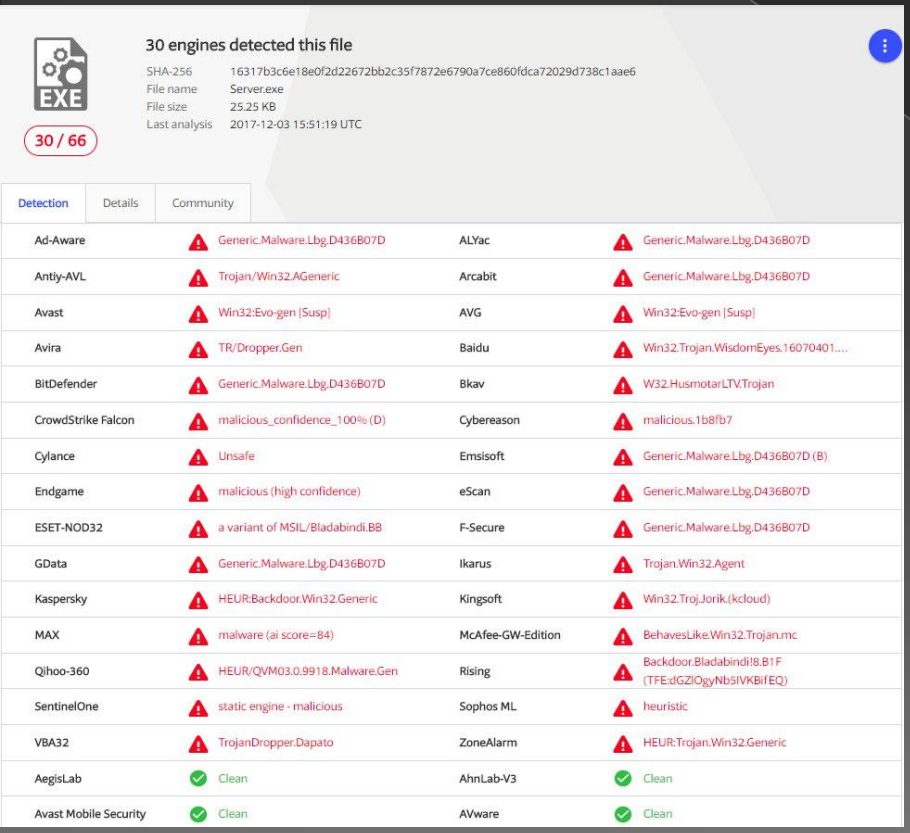
- **RAT** — в переводе — «средство удалённого администрирования» или «средство удалённого управления» или «крыса». Термин получил распространение среди системных администраторов и хакеров.

Склейка

Шифрование

VirusTotal

ДО



30 engines detected this file

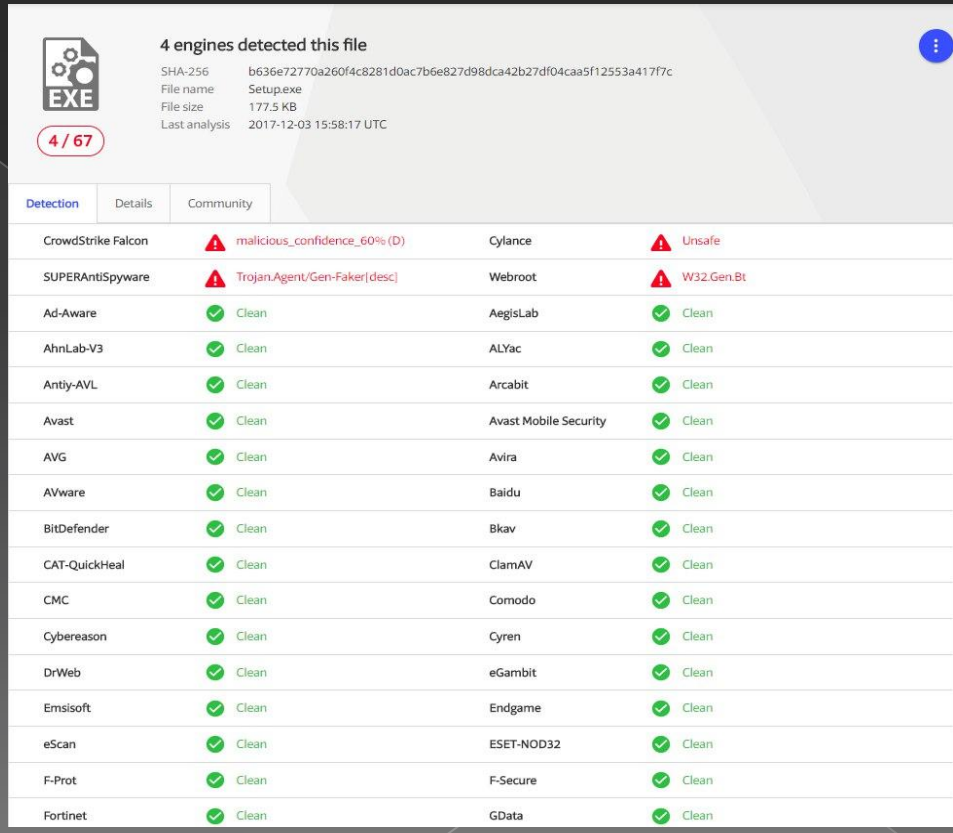
SHA-256 16317b3c6e18e0f2d22672bb2c35f7872e6790a7ce860fdca72029d738c1aae6
File name Server.exe
File size 25.25 KB
Last analysis 2017-12-03 15:51:19 UTC

30 / 66

Detection | Details | Community

Ad-Aware	Generic.Malware.Lbg.D436B07D	ALYac	Generic.Malware.Lbg.D436B07D
Antiy-AVL	Trojan/Win32.AGeneric	Arcabit	Generic.Malware.Lbg.D436B07D
Avast	Win32:Evo-gen [Susp]	AVG	Win32:Evo-gen [Susp]
Avira	TR/Dropper.Gen	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Generic.Malware.Lbg.D436B07D	Bkav	W32.HusmotarLTV.Trojan
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason	malicious.1b8fb7
Cylance	Unsafe	Emsisoft	Generic.Malware.Lbg.D436B07D (B)
Endgame	malicious (high confidence)	eScan	Generic.Malware.Lbg.D436B07D
ESET-NOD32	a variant of MSIL/Bladabindi.BB	F-Secure	Generic.Malware.Lbg.D436B07D
GData	Generic.Malware.Lbg.D436B07D	Ikarus	Trojan.Win32.Agent
Kaspersky	HEUR:Backdoor.Win32.Generic	Kingsoft	Win32.Troj.Jorik.(kcloud)
MAX	malware (ai score=84)	McAfee-GW-Edition	BehavesLike.Win32.Trojan.mc
Qihoo-360	HEUR/QVM03.0.9918.Malware.Gen	Rising	Backdoor.Bladabindi!8.B1F (TFE:dGZlOgyNb5IVKBifEQ)
SentinelOne	static engine - malicious	Sophos ML	heuristic
VBA32	TrojanDropper.Dapato	ZoneAlarm	HEUR:Trojan.Win32.Generic
AegisLab	Clean	AhnLab-V3	Clean
Avast Mobile Security	Clean	AVware	Clean

ПОСЛЕ



4 engines detected this file

SHA-256 b636e72770a260f4c8281d0ac7b6e827d98dca42b27df04caa5f12553a417f7c
File name Setup.exe
File size 177.5 KB
Last analysis 2017-12-03 15:58:17 UTC

4 / 67

Detection | Details | Community

CrowdStrike Falcon	malicious_confidence_60% (D)	Cylance	Unsafe
SUPERAntiSpyware	Trojan.Agent/Gen-Faker[desc]	Webroot	W32.Gen.Bt
Ad-Aware	Clean	AegisLab	Clean
AhnLab-V3	Clean	ALYac	Clean
Antiy-AVL	Clean	Arcabit	Clean
Avast	Clean	Avast Mobile Security	Clean
AVG	Clean	Avira	Clean
AVware	Clean	Baidu	Clean
BitDefender	Clean	Bkav	Clean
CAT-QuickHeal	Clean	ClamAV	Clean
CMC	Clean	Comodo	Clean
Cybereason	Clean	Cyren	Clean
DrWeb	Clean	eGambit	Clean
Emsisoft	Clean	Endgame	Clean
eScan	Clean	ESET-NOD32	Clean
F-Prot	Clean	F-Secure	Clean
Fortinet	Clean	GData	Clean