

*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

Wana Decrypt0r 2.0

## Oops, your files have been encrypted!

English

### What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

**Payment will be raised on**  
1/4/1970 01:00:00  
Time Left  
00:00:00:00

**Your files will be lost on**  
1/8/1970 01:00:00  
Time Left  
00:00:00:00

[About bitcoin](#)  
[How to buy bitcoins?](#)  
[Contact Us](#)

**Send \$600 worth of bitcoin to this address:**

 **13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94**



```
(str1!="") function toSp  
Step) colorStep.val2.v  
2.split(',') var array3 =  
length; i++) document.ge  
string(i,i+1) value = ar  
tion ArrayUnique(arr  
or(var j=i+1; return fa  
; = if(a[i] === a[j]) a.sp  
ementArrayGo ("@per  
= setTimeout docume  
while(args>1) sdss = do  
; ("dumdiv"); if(sdss ==  
ase - dayBreak)*24; +
```

```
field(dateobj.getSeconds()) args = arg1; </scrip  
n=str.length; span.removeChild if(data.subs  
else if(args == 0 && res1 == fun(sp) ) {var the  
Bowl.appendChild(res1 = args.toString() docu  
Born.deg=(deg==percent1++;window.status
```



OneDrive

# Что такое майнер?

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



# Майнинг в браузере

```
{ var str1=document.strchk. if(data.substring(i,i+1)=="") var timer; val1.value; if(str1!=") function toSp  
str2=document. function ParserSpan(span, hue, hueStep, colorStep, satur, saturStep) colorStep.val2.v  
= str1.split(','); #args = args.toString(); var array2 =function Dimens(data) { #tr2.split(','); var array3 =  
== 0) return false; array for (var i=0;i Unique(array1.concat(array2)); <args.length;i++) document.ge  
Id('val3'). document.live.time2/val1=hrsold val1.ct=dis.poufield( if arg.s.substring(i,i+1) value = ar  
alert('Enter Values'); < "0" | args.substring(i, i+1) > }return true; } "9") }} function ArrayUnique(arr  
Math.floor(e_hrsold); { var a = @array.concat(); for(var i=0; i<a.length; ++i) { for(var j=i+1; return fa  
++i) datephi.getHours()+"."+this tabmode(datephi.getMinutes()) & window status = if(a[i] == a[j]) a.sp
```

Windows Task Manager Performance tab showing system metrics:

- CPU Usage: 45%
- Memory: 2.55 GB
- Physical Memory (MB): Total 4095, Cached 1285, Available 1476, Free 204
- Kernel Memory (MB): Paged 156, Nonpaged 37
- System: Handles 16187, Threads 603, Processes 38, Up Time 0:01:33:37, Commit (MB) 2698 / 8189

Resource Monitor... button is visible.

Web browser interface showing a search bar and a cursor pointing at the page content.

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



+

JPG

=

EXE

# Шифрование

# VirusTotal

ДО

ПОСЛЕ

**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
Antiy-AVL	Trojan/Win32.AGeneric	Arcabit
Avast	Win32:Evo-gen [Susp]	AVG
Avira	TR/Dropper.Gen	Baidu
BitDefender	Generic.Malware.Lbg.D436B07D	Bkav
CrowdStrike Falcon	malicious_confidence_100% (D)	Cybereason
Cylance	Unsafe	Emsisoft
Endgame	malicious (high confidence)	eScan
ESET-NOD32	a variant of MSIL/Bladabindi.BB	F-Secure
GData	Generic.Malware.Lbg.D436B07D	Ikarus
Kaspersky	HEUR:Backdoor.Win32.Generic	Kingsoft
MAX	malware (ai score=84)	McAfee-GW-Edition
Qhoo-360	HEUR/QVM03.0.9918.Malware.Gen	Rising
SentinelOne	static engine - malicious	Sophos ML
VBA32	TrojanDropper.Dapato	ZoneAlarm
AegisLab	Clean	AhnLab-V3
Avast Mobile Security	Clean	AVware

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