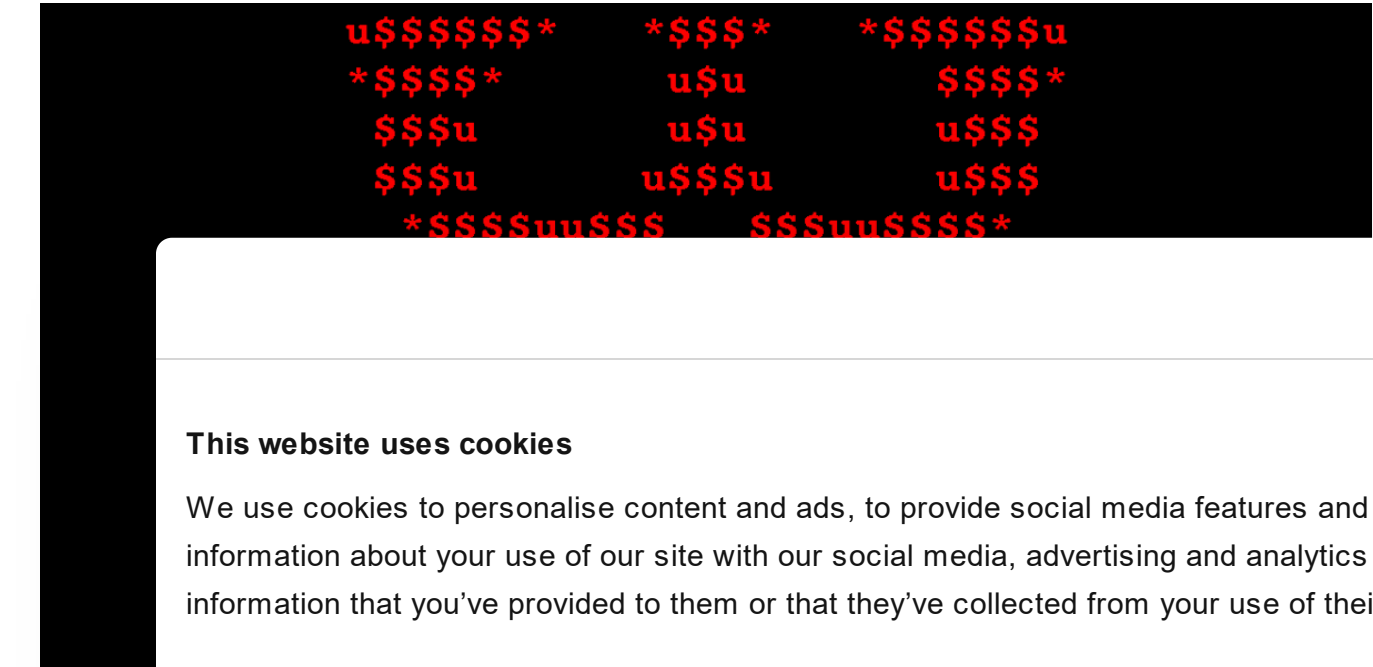


Schroedinger's Pet(ya)

INCIDENTS

27 JUN 2017

4 minute read



GREAT WEBINARS

13 MAY 2021, 1:00PM

GReAT Ideas. Balalaika Edition

BORIS LARIN, DENIS LEGEZO

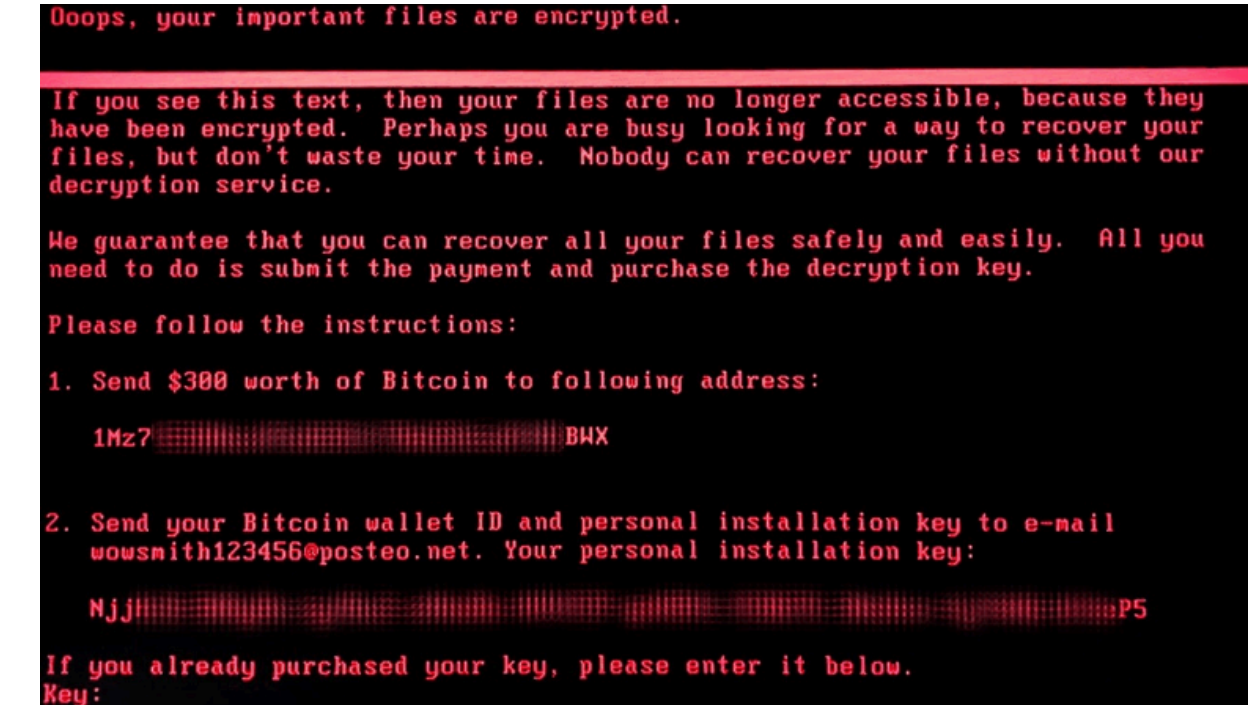
// AU

Expert

GReAT

UPDATE: The Petya/ExPetr ransomware attack is still ongoing, and it is not clear if a payment will be made. The ransomware is still active, and it is not clear if a payment will be made. The ransomware is still active, and it is not clear if a payment will be made.

Earlier today, a ransomware attack (referred in the media by several names, including Petya, Petrwrap, NotPetya and exPetr) spreading around the world, primarily targeting businesses in Ukraine, Russia and Western Europe. If you were one of the unfortunate victims, this screen might look familiar:



22 JUL 2020, 2:00PM

GReAT Ideas. Powered by SAS: threat hunting and new techniques

DMITRY BESTUZHEV, COSTIN RAIU, PIERRE DELCHER,
BRIAN BARTHOLOMEW, BORIS LARIN, ARIEL JUNGHEIT,
FABIO ASSOLINI

Kaspersky Lab solutions successfully stop the attack through the System Watcher component. This technology protects against ransomware attacks by monitoring system changes and rolling back any potentially destructive actions.

At this time, our telemetry indicates more than 2,000 attacks:

Our inve
public sp

Cookiebot
by Usercentrics

How

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary	Preferences	Statistics	Marketing
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Show details >

How This website uses cookies

To capture and analyse your use of our site, we use cookies. We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Other ok	Necessary	Preferences	Statistics	Marketing
<ul style="list-style-type: none">• A mo• The E• Wi	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- A mo
- The E
Wind
- An at
MeD

- The E Wind

- An at
MeD

IMPORT
credent
or PSEXEC.

Show details >

What does the ransomware do?

The malware waits for 10-60 minutes after the infection to reboot the system. Reboot is scheduled using system facilities with “at” or “schtasks” and “shutdown.exe” tools.

Once it reboots, it starts to encrypt the MFT table in NTFS partitions, overwriting the MBR with a customized loader with a ransom note. More details on the ransom note below.

Network survey

The malware enumerates all network adapters, all known server names via NetBIOS and also retrieves the list of current DHCP leases, if available. Each and every IP on the local network and each server found is checked for open TCP ports 445 and 139. Those machines that have these ports open are then attacked with one of the methods described above.

Password extraction

Resources 1 and 2 of malware binary contain two versions of a standalone tool (32-bit and 64-bit) that tries to extract logins and passwords of logged on users. The tool is run by the main binary. All extracted data is transferred back to the main module via a named pipe with a random GUID-like name.

File Decryption

Are there any hopes of decrypting files for victims already infected? Unfortunately, the ransomware uses a standard, solid encryption scheme so this appears unlikely unless a subtle implementation mistake has been made. The following specifics apply to the encryption mechanism:

- For a
- This
- Encr
- Keys

The crim
the rans
work bec
“wowsm
email ac
existing

FROM THE SAME AUTHORS

Grandoreiro, the global trojan with grandiose goals

Stealer here, stealer there, stealers everywhere!

Exotic SambaSpy is now dancing with Italian users

BlindEagle flying high in Latin America

EastWind campaign: new CloudSorcerer attacks on government organizations in Russia



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

At the time of writing, the Bitcoin wallet has accrued 24 transactions totalling 2.54 BTC or just under \$6,000 USD.

Here’s our shortlist of recommendations on how to survive ransomware attacks:

- Run a robust anti-malware suite with embedded anti-ransomware protection such as System Watcher from Kaspersky Internet Security.
- Make sure you update Microsoft Windows and all third party software. It’s crucial to apply the MS17-010 bulletin immediately.
- Do not run open attachments from untrusted sources.
- Backup sensitive data to external storage and keep it offline.

Kaspersky Lab corporate customers are also advised to:

- Check that all protection mechanisms are activated as recommended; and that KSN and System Watcher components (which are enabled by default) are not disabled.

- As an additional measure for corporate customers is to use [Application Privilege Control](#) to [deny any access](#) (and thus possibility of interaction or execution) for all the groups of applications to the file with the name “perfc.dat” and PSEXec utility (part of the Sysinternals Suite)
- You can alternatively use [Application Startup Control](#) component of Kaspersky Endpoint Security to block the execution of the PSEXec utility (part of the Sysinternals Suite), but please use Application Privilege Control in order to block the “perfc.dat”.
- Configure and enable the Default Deny mode of the Application Startup Control component of Kaspersky Endpoint Security to ensure and enforce the proactive defense against this, and other attacks.

For sysadmins, our products detect the samples used in the attack by these verdicts:

- UDS:DangerousObject.Multi.Generic
- Trojan-Ransom.Win32.ExPetr.a
- HEUR:Trojan-Ransom.Win32.ExPetr.gen

Our behavior detection engine SystemWatcher detects the threat as:

- PDM:Trojan.Win32.Generic
- PDM

IOCs

1	0df71
2	42b2f
3	71b6a
4	e285b
5	e595c

Yara

Download

rule ransom

meta:

copyright

descript

last_modified = "2017-08-27"

author = "Kaspersky Lab"

hash = "71B6A493388E7D0B40C83CE903BC6B04"

version = "1.0"

strings:

\$a1 =

"MIIBCgKCAQEAXP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjlQlnTeHkXEjfO2n2JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmdrRliUEUw6o3pt5pNOskfOJbMan2TZu" fullword wide

\$a2 =

".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsd.vsv.work.xls" fullword wide

\$a3 = "DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED" fullword ascii

\$a4 = "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx" fullword ascii

\$a5 = "wowsmith123456@posteo.net." fullword wide

condition:



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

Subscribe to our weekly e-mails

The hottest research right in your inbox

Email(Required)

☐ I agree to provide my email address to “AO Kaspersky Lab” to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking

(uint16(0) == 0x5A4D) and

(filesize<1000000) and

(any of them)

}

DATA ENCRYPTION

FINANCIAL MALWARE

MALWARE DESCRIPTIONS


MBR

PETYA

RANSOMWARE

VULNERABILITIES AND EXPLOITS

the “unsubscribe” link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

 **Subscribe**

Schroedinger’s Pet(ya)

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

Type your comment here

Name *

Email *

Comments

ANGELO M.

Posted on Jun 28, 2017 10:06 am

Do we know if the

Reply

VALENTIN

Posted on Jun 28, 2017 10:06 am

No, I don't know

Reply

S

Posted on Jun 28, 2017 10:06 am

Salve Carlo

I could send you

ETERNAL

Reply

COSTIN

Posted on June 28, 2017. 8:15 am

Absolutely. Please check the section “How does the ransomware spread?” in the blogpost.

Reply

JERAMY

Posted on June 27, 2017. 10:59 pm

Is the MFT also encrypted with the method you describe for file encryption?

Reply

FOL

Posted on June 28, 2017. 9:06 am

why did idiots at posteo blocked that email?

If someone sent payment in step 1 and now wants to retrieve/confirm it to attackers he is basically scammed by posteo.net which is preventing victims to get their key!

Reply

KIARA

Posted on June 28, 2017. 1:57 pm

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

They're preventing these criminals from profiting from crime... pretty simple

Reply

LORDKEN

Posted on June 28, 2017. 6:39 pm

@Kiara: why do you comment when you don't have a clue?

posteo.net blocked email account of attackers that was set up to receive >emails<

from victims begging for decryption keys. -emphasis on emails, not money.

Attacker's bitcoin wallet is open (it cannot be blocked for that matter) and can continue to receive payments. It doesn't have anything to do with blocked email account.

So how are attackers prevented from taking profit?

Reply

DAVID LAPHAM

Posted on June 28, 2017. 2:53 pm

Fol — I for one think Posteo did the right thing. The way to fight ransomware, it to make it

unprofitable. Some people will do anything to get their stuff back, including pay a ransom.

This is what those behind Petya bank on. Sure, some will get scammed, but they deserve it.

Reply

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary☒

Preferences☐

Statistics☐

Marketing☐

Show details >

By your logic guys lets nuke London, if there wont be any ppl alive terrorist will stop their attacks [there]. Mission complete!

Reply

EK

Posted on June 29, 2017. 12:20 am

Looks like victims won't get their data back anyway:

<https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/>

Reply

ABSENT

Posted on June 29, 2017. 6:53 am

* The email firm obviously doesn't want an ongoing association with this – shutting it down means fewer questions from fewer people.

* It's the old "never negotiate with terrorists" mantra extended to this (capitulate and more will come)

* It does go a bit further – pretty much (in a “pop quiz, hotshot” kind of way) “shoot the hostage” to try to take away power from the attacker, but there’s still a basis for it (agree with it or not)

A hack in hand is worth two in the bush

QBot banker delivered through business correspondence

* This only works if there's an info campaign that victims believe, before they pay. Those who've already paid are screwed over – they're the fire-break-cull aiming to halt the spread of people making payments & in the longer run, discourage future attacks (if people believe they won't be able to get keys, they're less likely to pay, meaning they're less attractive targets, reducing the appeal of the attack.

* Those who haven't paid yet, still don't get their systems back, which would be a criticism of it weren't for the reports the attackers never provided keys to people before the email shutdown and possibly have no a desire or ability to decrypt – that outcome is an argument for the “never negotiate stance” – you simply can't trust the buggers!

With the “never negotiate” stance, it was normal that negotiations are taking place, but privately to prevent attracting copy-cats. With a public BC wallet, you can't hide the payments, so capitulation is always visible.

On a side note, who the hell is going to exchange any blocks from that wallet given its had international news coverage?

Reply

HENRI-MICHEL
Posted on June 28, 2017. 9:55 am

If I rename “shutdown.exe”, the described routine should fail. What happen in this case ?

Reply

VALENTIN K
Posted on Jun

Good de
antivirus

Reply

JEREMY SM
Posted on Jun

Do we ne
managin

Reply

VALPARAISO
Posted on Jun

@Valenti
or in RUr
can use
Kaspers

protection is worth a try.

Reply

VALPARAISO
Posted on June 28, 2017. 7:51 pm

@Jeremy Smith – do you mean Kaspersky Security Cloud? It's adaptive security service available in the UK. Short answer is no action required, because it uses all preventive engines required to be safe from NotPetya. Anyway, the top rule applies also here – do not open anything that you're not expecting to come and double-check the source of email or message you've been sent. It looks like NotPetya is mainly targeting companies of different size, especially those who have offices in the Ukraine or business ties to it. This is why Maersk, lots of Russian and some Polish and German transport companies got hit badly. All have to do tax paperwork in the Ukraine, because of their local offices. Key infection channel seem to be tax reporting software called M.E.Doc.

Reply

OX1KNJ
Posted on June 28, 2017. 7:58 pm

Cool description! But what about Mischa? In my laptop, Symantec encryption at start-up prevented #NotPetya from running at reboot and I then found the infamous “perfc” file in



This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Necessary	Preferences	Statistics	Marketing

Show details >

C:/Windows (see @0xAmit's vaccine on twitter). However, I see that I cannot access some .xls and .doc files, as if they were encrypted... Mischa is real???

Reply

DRAFT
Posted on June 28, 2017. 8:49 pm

If computer is using FAT32 instead of the NTFS, is that new Petya capable of encrypting the disk?
FAT32 doesn't possess MFT, how that ransomware behaves in that case? Thanks!

Reply

JJACK
Posted on June 29, 2017. 8:15 am

The same question, with FAT32 😊 – Anyone knows?

Reply

VARADHARAJAN K
Posted on June 29, 2017. 5:27 pm

- 1) Whether it encrypts MBR in all haddrives or only os drive ?
 - 2) How to prevent the petya for home users , give me the detail instructions , for blocking of perfc.dat file and the PSxec.exe utility by using KIS 2017 an d KTS 2017 .
 - 3) how to prevent the petya for home users by using KIS 2017 and KTS 2017 .
- applocker

Reply

JOSH BRAN
Posted on Jul

We were
and only
network.

Reply

// LA

New product

Get your business' security to the Next level

Cookiebot

by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary

Preferences

Statistics

Marketing

Show details

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.

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.

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.

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.



// SUBMAILS

The hottest

Subscribe

Cookiebot
by Usercentrics

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services.

Necessary



Preferences



Statistics



Marketing



Show details >

kaspersky

THREATS

- APT (Targeted attacks)
- Secure environment (IoT)
- Mobile threats
- Financial threats
- Spam and phishing
- Industrial threats
- Web threats
- Vulnerabilities and exploits
- All threats

CATEGORIES

- APT reports
- Malware descriptions
- Security Bulletin
- Malware reports
- Spam and phishing reports
- Security technologies
- Research
- Publications
- All categories

OTHER SECTIONS

- Archive
- All tags
- Webinars
- APT Logbook
- Statistics
- Encyclopedia
- Threats descriptions
- KSB 2023