

Schroedinger's Pet(ya)

INCIDENTS

27 JUN 2017

4 minute read



// AUTHORS

Expert

GREAT

UPDATE June 28th, 2017: After an analysis of the encryption routine of the malware used in the Petya/ExPetr attacks, we have thought that the threat actor cannot decrypt victims' disk, even if a payment was made. It appears this malware campaign was designed as a wiper pretending to be ransomware. Read more: [ExPetr/Petya/NotPetya is a Wiper, Not Ransomware](#)

GREAT WEBINARS

- 13 MAY 2021, 1:00PM

GReAT Ideas. Balalaika Edition

BORIS LARIN, DENIS LEGEZO
- 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

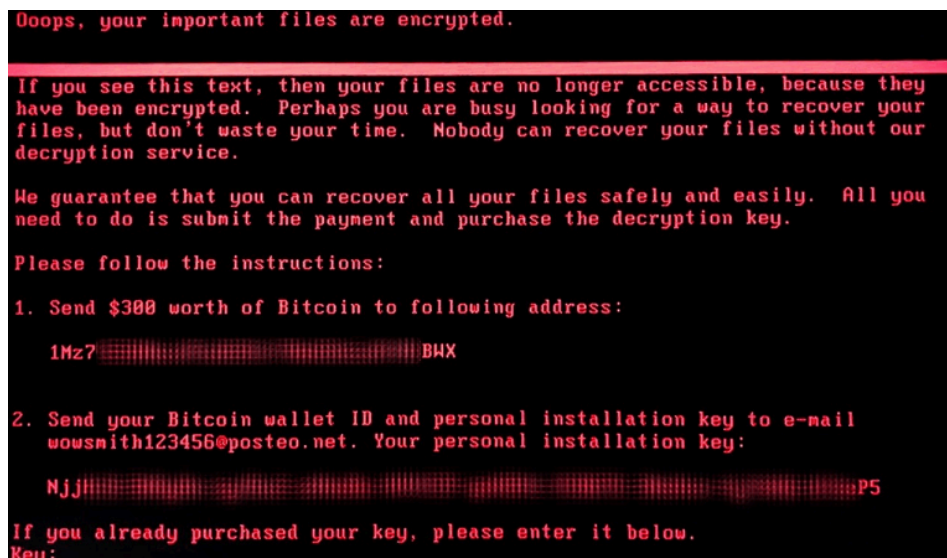
GReAT Ideas. Powered by SAS: malware attribution and next-gen IoT honeypots

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

Earlier today (June 27th), we received reports about a new wave of ransomware attacks (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:



Doops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:
1Mz7 [redacted] BWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
NjJH [redacted] P5

If you already purchased your key, please enter it below.
Key:

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:

fronts

IVAN KWIATKOWSKI, MAHER YAMOUT,
NOUSHIN SHABAB, PIERRE DELCHER, FÉLIX AIME,
GIAMPAOLO DEDOLA, SANTIAGO PONTIROLI

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

Our investigation is ongoing and our findings are far from final at this time. Despite rampant public speculation, the following is what we can confirm from our independent analysis:

How does the ransomware spread?

To capture credentials for spreading, the ransomware uses custom tools, a la Mimikatz. These extract credentials from the lsass.exe process. After extraction, credentials are passed to PsExec tools or WMI for distribution inside a network.

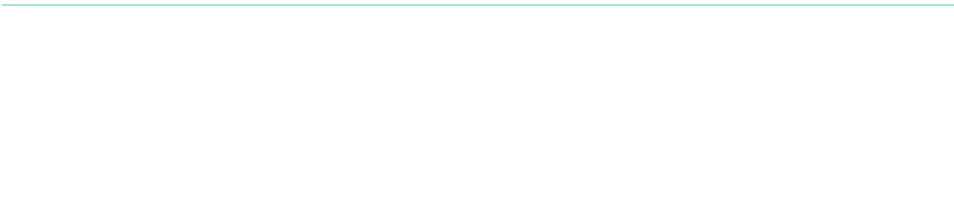
Other observed infection vectors include:

- A modified EternalBlue exploit, also used by WannaCry.
- The EternalRomance exploit – a remote code execution exploit targeting Windows XP to Windows 2008 systems over TCP port 445 (Note: patched with MS17-010).
- An attack against the update mechanism of a third-party Ukrainian software product called MeDoc.

IMPORTANT: A single infected system on the network possessing administrative credentials is capable of spreading this infection to all the other computers through WMI or PSEXEC.

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:

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

- For all files, one AES-128 key is generated.
- This AES key is encrypted with threat actors' public RSA-2048 key.
- Encrypted AES keys are saved to a README file.
- Keys are securely generated.

The criminals behind this attack are asking for \$300 in Bitcoins to deliver the key that decrypts the ransomed data, payable to a unified Bitcoin account. Unlike Wannacry, this technique would work because the attackers are asking the victims to send their wallet numbers by e-mail to "wowsmith123456@posteo.net", thus confirming the transactions. We have seen reports this email account has already been shut down, effectively making the full chain decryption for existing victims impossible at this time.

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:Exploit.Win32.Generic

IOCs

1	0d17179693755b810403a972f4466afb
2	42b2ff216d14c2c8387c8eabfb1ab7d0
3	71b6a493388e7d0b40c83ce903bc6b04
4	e285b6ce047015943e685e6638bd837e
5	e595c02185d8e12be347915865270cca

Yara rules

Download [Yara rule expetr.yara as a ZIP](#) archive.

```
rule ransomware_exPetr {
meta:

copyright = "Kaspersky Lab"
description = "Rule to detect PetrWrap ransomware samples"
last_modified = "2017-06-27"
author = "Kaspersky Lab"
hash = "71B6A493388E7D0B40C83CE903BC6B04"
version = "1.0"

strings:

$a1 =
"MIIBCgKCAQEAXP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAY
T0O65Cr8PjIQlnTeHkXEjfO2n2JmURWV/uHB0ZrIQ/wcYJBwLhQ9Eq
J3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFL
Cy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNN
pgq+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.ov
a.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vc
b.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:
```

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 the "unsubscribe" link that I find at the bottom of any e-mail sent

```
(uint16(0) == 0x5A4D) and
(filesize<1000000) and
(any of them)
}
```

DATA ENCRYPTION

FINANCIAL MALWARE

MALWARE DESCRIPTIONS


MBR

PETYA

RANSOMWARE

VULNERABILITIES AND EXPLOITS

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 *

Comment

ANGELO M.
Posted on June 27, 2017. 7:46 pm

Do we know if Petya encrypts beyond the MBR? or does it stop there?

Reply

VALENTYN BUDKIN
Posted on June 27, 2017. 10:00 pm

No, it isn't. It begins to encrypt files on disk C. Disk D unconfirmed yet.

Reply

S

Posted on June 27, 2017, 8:35 pm

Salve Costin.

I could see in the code cached credential reuse and replication. So it goes beyond ETERNALBLUE.

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

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

FOL

Posted on June 28, 2017. 4:49 pm

excuse me guys but who do you think you two are to decide for others how valued their data is to them??

Its none of your business if my data are valued 3k to me and I'm willing to pay \$300 to get it. But with this posteo noobs and your logic ppl lost data, lost another \$300 as ransom pay – total FAIL. While attackers get ransom money and don't need to bother with decryption key – WIN.

Don't you guys have basic level of logical thinking? You are hitting victims and not attackers.

To get you into perspective, because it looks like you lack it. Say your kid is kidnaped for ransom, kidnapers contact you with their demands but phone company decide to block their or your number to prevent communication , to prevent criminals to get profit and teach other criminals the lesson, too bad your kid is gonna die in the process. You are ridiculous.

@David: also WTH? ppl who lost their data DESERVED it? (ofc clicking links with admin user is lame), so lets punish them by preventing them to get unlock key but let attackers profit...can you please elaborate on this, with your logic, how attackers are losing profit here? (hint bitcoins to their wallet can flow freely)

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

Reply

E K

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/>

IN THE SAME CATEGORY

XZ backdoor: Hook analysis

Assessing the Y, and How, of the XZ Utils incident

XZ backdoor story – Initial analysis

A hack in hand is worth two in the bush

QBot banker delivered through business correspondence

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)
- * 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 KOLESNIKOV

Posted on June 28, 2017. 2:15 pm

Good description. Kaspersky sites are locked in Ukraine. As a result we can't use Kaspersky antivirus here.

Reply

JEREMY SMITH

Posted on June 28, 2017. 4:00 pm

Do we need to make any changes in our KSC in order to block this? I'm relatively new to managing the KSC so sorry if the question is "Bad".

Reply

VALPARAISO

Posted on June 28, 2017. 7:42 pm

@Valentin Kolesnikov – you can access Kaspersky Lab websites that are not in Russian language or in RUnet zone. Try .com, .co.uk, etc. As of my best knowledge, Ukrainian customers and users can use already installed software from Ukraine. New users may have to get their copy of Kaspersky Lab security software from EU or other, non Russian domains. Give it a try. Right 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

0X1KNJ

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 C:/Windows (see @OxAmit'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 harddrives 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 and KTS 2017 .
- 3) how to block the perfc.dat and pSexec.exe using group policy editor built in windows by applocker

Reply

JOSH BRANUM

Posted on July 11, 2017, 5:20 am

We were hit with win32.bitcovar.v. One qq.com email all local app files encrypted. No price given and only server hit that i can tell. Cloud backups unaffected. Going to keep local backups off network.




Reply



// LATEST POSTS

SAS	MALWARE DESCRIPTIONS	CRIMEWARE REPORTS	CRIMEWARE REPORTS
The Crypto Game of Lazarus APT: Investors vs. Zero-days	Grandoreiro, the global trojan with grandiose goals	Stealer here, stealer there, stealers everywhere!	Analysis of the Crypt Ghouls group: continuing the investigation into a series of attacks on Russia
BORIS LARIN, VASILY BERDNIKOV	GREAT	GREAT	KASPERSKY

// LATEST WEBINARS

 THREAT INTELLIGENCE AND IR	 TECHNOLOGIES AND SERVICES	 CYBERTHREAT TALKS	 TRAININGS AND WORKSHOPS
04 SEP 2024, 5:00PM 60 MIN Inside the Dark Web: exploring the human side of cybercriminals ANNA PAVLOVSKAYA	13 AUG 2024, 5:00PM 60 MIN The Cybersecurity Buyer's Dilemma: Hype vs (True) Expertise OLEG GOROBETS, ALEXANDER LISKIN	16 JUL 2024, 5:00PM 60 MIN Cybersecurity's human factor – more than an unpatched vulnerability OLEG GOROBETS	09 JUL 2024, 4:00PM 60 MIN 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.



// SUBSCRIBE TO OUR WEEKLY E-MAILS

The hottest research right in your inbox

 **Subscribe**

☐

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

APT (Targeted attacks)	APT reports	Archive
Secure environment (IoT)	Malware descriptions	All tags
Mobile threats	Security Bulletin	Webinars
Financial threats	Malware reports	APT Logbook
Spam and phishing	Spam and phishing reports	Statistics
Industrial threats	Security technologies	Encyclopedia
Web threats	Research	Threats descriptions
Vulnerabilities and exploits	Publications	KSB 2023
All threats	All categories	

© 2024 AO Kaspersky Lab. All Rights Reserved.
Registered trademarks and service marks are the property of their respective owners.

[Privacy Policy](#) | [License Agreement](#)
| [Cookies](#)