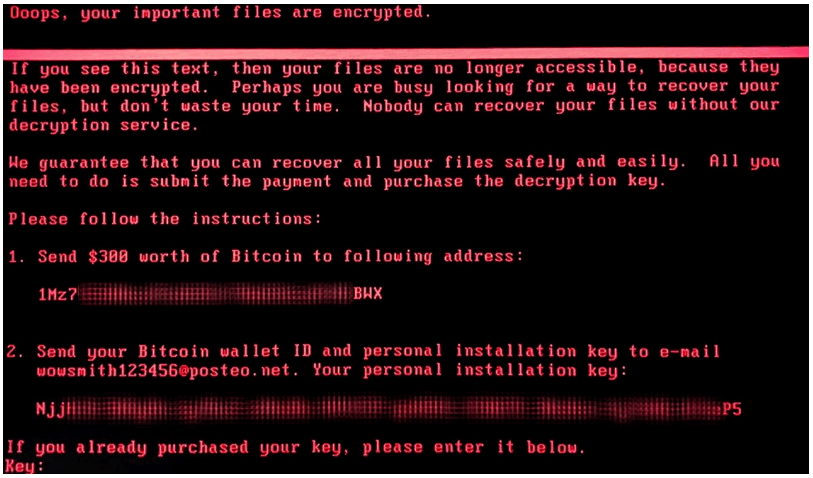
Schroedinger's Pet(ya)

By GReAT

Published: 2017-06-27 · Archived: 2026-04-05 16:11:43 UTC

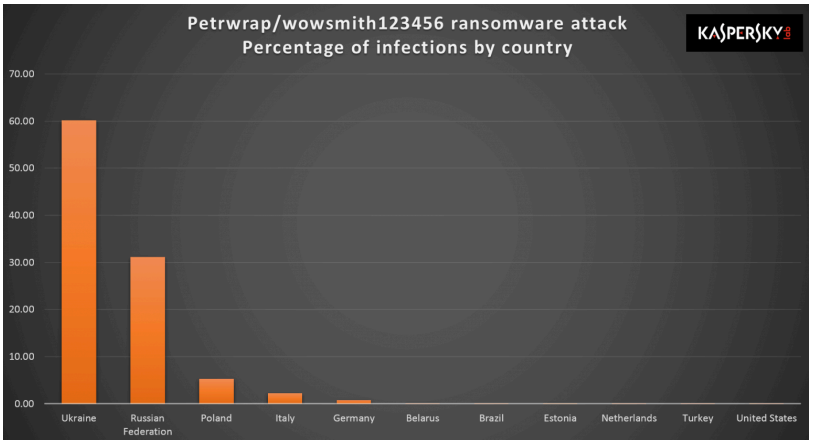
UPDATE June 28th, 2017: After an analysis of the encryption routine of the malware used in the Petya/ExPetr attacks, we have thought that the threat actor cannot decrypt victims' disk, even if a payment was made. It appears this malware campaign was designed as a wiper pretending to be ransomware. Read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

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:



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 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 WMIC 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.

```
GetLocalTime(&SystemTime);
runTimeMinutes = HowMuchMinutesIWasRunning();
if ( runTimeMinutes < 10 )
  runTimeMinutes = 10;
v2 = (runTimeMinutes + 3) % 60 + SystemTime.wMinute;
v3 = ((runTimeMinutes + 3) / 60 + SystemTime.wHour) % 24;
if ( GetSystemDirectoryW(&Buffer, 0x30Cu) && PathAppendW(&Buffer, L"shutdown.exe /r /f") )
{
  if ( sub_10008494() )
  {
    v4 = L"/RU \"SYSTEM\" ";
    if ( !(dword_1001F144 & 4) )
      v4 = (const wchar_t *)&unk_10014388;
    wsprintfW(&v6, L"schtasks %ws/Create /SC once /TN \"\" /TR \"%ws\" /ST %02d:%02d", v4, &Buffer, v3, v2);
  }
  else
  {
    wsprintfW(&v6, L"at %02d:%02d %ws", v3, v2, &Buffer);
  }
  v7 = 0;
  v0 = ExecCmdExe(0);
}
```

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.

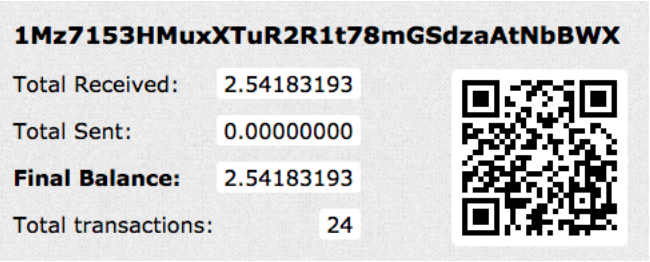
Resources 1 and 2 of malware binary contain two versions of a standalone tool (32-bit and 64-bit) that tries to extract logins and passwords of logged on users. The tool is run by the main binary. All extracted data is transferred back to the main module via a named pipe with a random GUID-like name.

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 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

	0df7179693755b810403a972f4466afb 42b2ff216d14c2c8387c8eabfb1ab7d0 71b6a493388e7d0b40c83ce903bc6b04 e285b6ce047015943e685e6638bd837e 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/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iI
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.p
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:

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