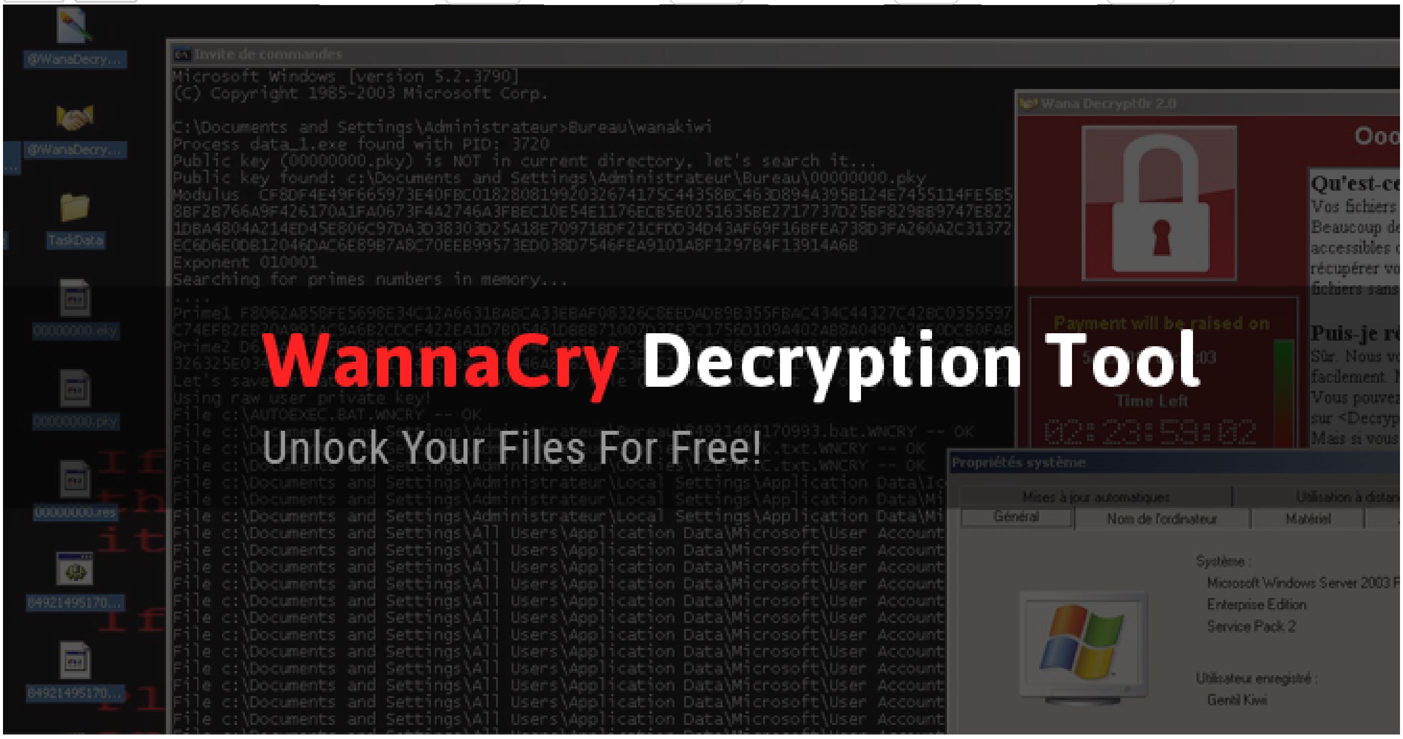
The Hacker News™
Security in a serious way

WannaCry Ransomware Decryption Tool Released; Unlock Files Without Paying Ransom

Thursday, May 18, 2017 Swati Khandelwal



```
Microsoft Windows [version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrateur>Bureau\wanakiwi
Process data_1.exe found with PID: 3720
Public key (0000000.pky) is NOT in current directory, let's search it...
Public key found: c:\Documents and Settings\Administrateur\Bureau\00000000.pky
Modulus  CF8DF4E49F665973E40FBC0182808199203267417 5C44358BC463D894A395B124E7455114FE5B5
8BF2B766A9F426170A1FA0673F4A2746A3FBEC10E54E1176ECB5E0251635BE2717737D25BF829BB9747E822
1D8A4804A214ED45E806C97DA3D38303D25A18E709718DF21CFDD34D43AF69F16BFEA738D3FA260A2C31372
EC6D6E0D812046DAC6E89B7A8C70EEB99573ED038D7546FEA9101A8F129784F13914A68
Exponent 010001
Searching for primes numbers in memory...
```

If your PC has been infected by WannaCry – the ransomware that wreaked havoc across the world last Friday – you might be lucky to get your locked files back without paying the ransom of $300 to the cyber criminals.

Adrien Guinet, a French security researcher from Quarkslab, has discovered a way to retrieve the secret encryption keys used by the WannaCry ransomware for free, which works on Windows XP, Windows 7, Windows Vista, Windows Server 2003 and 2008 operating systems.

WannaCry Ransomware Decryption Keys

The WannaCry's encryption scheme works by generating a pair of keys on the victim's computer that rely on prime numbers, a "public" key and a "private" key for encrypting and decrypting the system’s files respectively.

To prevent the victim from accessing the private key and decrypting locked files himself, WannaCry erases the key from the system, leaving no choice for the victims to retrieve the decryption key except paying the ransom to the attacker.

But here's the kicker: WannaCry *"does not erase the prime numbers from memory before freeing the associated memory,"* says Guinet.

Based on this finding, Guinet released a WannaCry ransomware decryption tool, named **WannaKey**, that basically tries to retrieve the two prime numbers, used in the formula to generate encryption keys from memory, and works on Windows XP only.

Note: Below I have also mentioned another tool, dubbed *WanaKiwi*, that works for Windows XP to Windows 7.

"*It does so by searching for them in the wcry.exe process. This is the process that generates the RSA private key. The main issue is that the CryptDestroyKey and CryptReleaseContext does not erase the prime numbers from memory before freeing the associated memory.*" says Guinet

So, that means, this method will work only if:

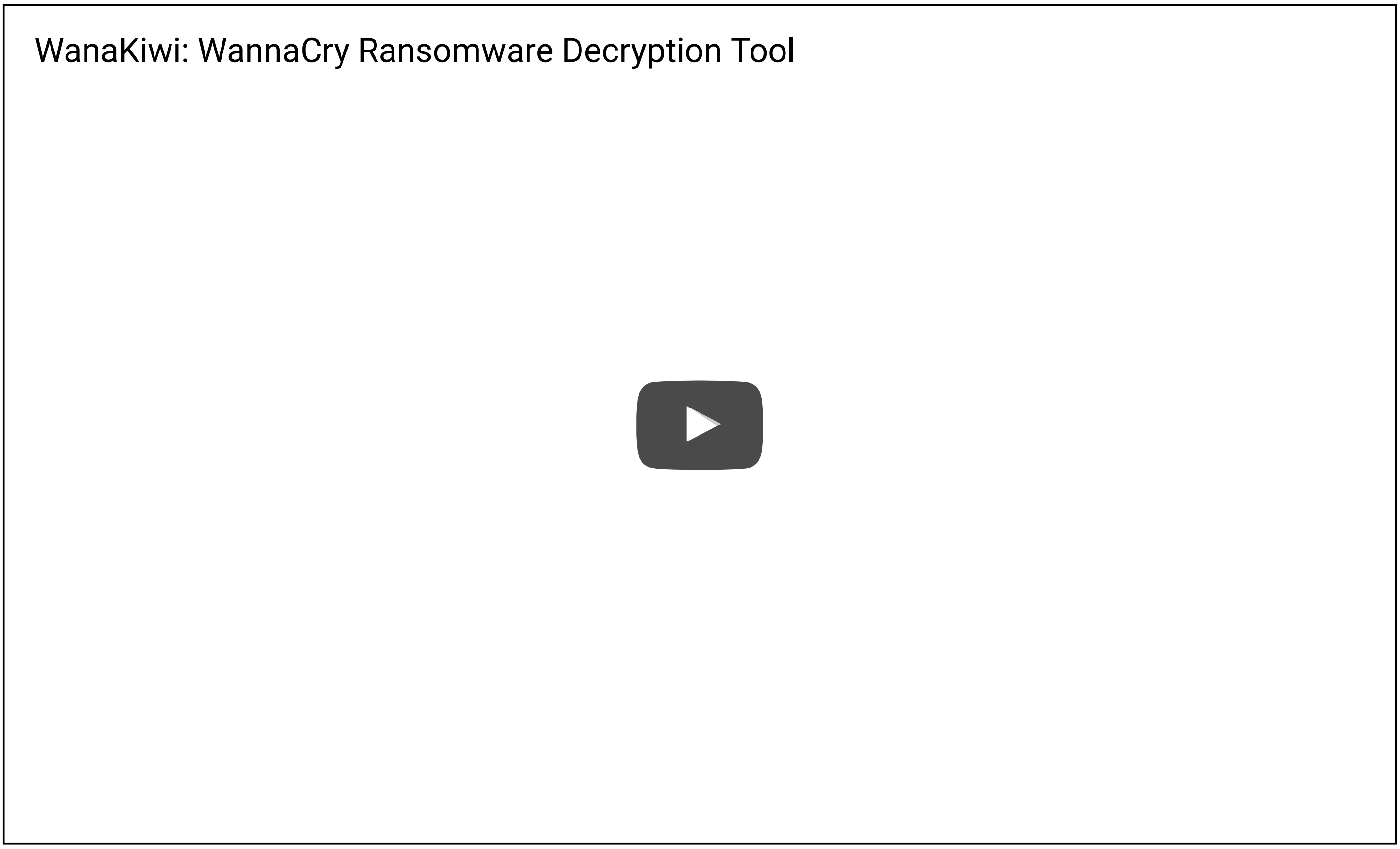
- The affected computer has not been rebooted after being infected.
- The associated memory has not been allocated and erased by some other process.

"*In order to work, your computer must not have been rebooted after being infected. Please also note that you need some luck for this to work (see below), and so it might not work in every case!,*" Guinet says.

"*This is not really a mistake from the ransomware authors, as they properly use the Windows Crypto API.*"

While WannaKey only pulls prime numbers from the memory of the affected computer, the tool can only be used by those who can use those prime numbers to generate the decryption key manually to decrypt their WannaCry-infected PC's files.

WanaKiwi: WannaCry Ransomware Decryption Tool



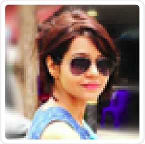
WanaKiwi: WannaCry Ransomware Decryption Tool

Good news is that another security researcher, Benjamin Delpy, developed an easy-to-use tool called "**WanaKiwi**," based on Guinet's finding, which simplifies the whole process of the WannaCry-infected file decryption.

All victims have to do is download WanaKiwi tool from Github and run it on their affected Windows computer using the command line (cmd).

WanaKiwi works on Windows XP, Windows 7, Windows Vista, Windows Server 2003 and 2008, confirmed Matt Suiche from security firm Comae Technologies, who has also provided some demonstrations showing how to use WanaKiwi to decrypt your files.

Although the tool won't work for every user due to its dependencies, still it gives some hope to WannaCry's victims of getting their locked files back for free even from Windows XP, the aging, largely unsupported version of Microsoft's operating system.

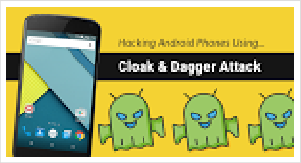


Swati Khandelwal

Technical Writer, Security Blogger and IT Analyst. She is a Technology Enthusiast with a keen eye on the Cyberspace and other tech related developments.

Decryption Keys, Ransomware, Ransomware Decrypt Tool, Ransomware Decryption Software, Unlock Files, WanaKiwi, WannaCry Ransomware

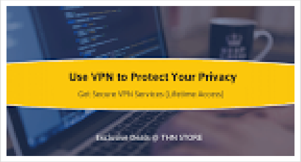
★ Latest Stories



All Android Phones Vulnerable to Extremely Dangerous Full Device Takeover Attack
Researchers have discovered a new attack, dubbed 'Cloak and Dagger', that works against all versions of Android, up to version ...

Wanna Cry Again? NSA’s Windows 'EsteemAudit' RDP Exploit Remains Unpatched
Brace yourselves for a possible 'second wave' of massive global cyber attack, as SMB (Server Message Block) was not the only ne...

7-Year-Old Samba Flaw Lets Hackers Access Thousands of Linux PCs Remotely
A 7-year-old critical remote code execution vulnerability has been discovered in Samba networking software that could allow a r...


Use VPN to Protect Your Privacy
Get Secure VPN Services (Lifetime Access)
Exclusive Deals @ THN STORE

Secure VPN Services With Lifetime Subscription (Save up to 95%) - Limited Time Deal
PRIVACY – a bit of an Internet buzzword nowadays, because the business model of the Internet has now shifted towards data colle...

Microsoft Unveils Special Version of Windows 10 For Chinese Government
China is very strict about censorship, which is why the country has become very paranoid when it comes to adopting foreign tech...

Comments (42)

TRENDING STORIES

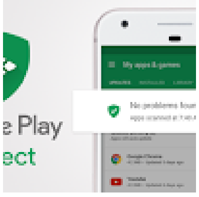
WannaCry Ransomware Decryption Tool Released; Unlock Files Without Paying Ransom

WikiLeaks Reveals 'Athena' CIA Spying Program Targeting All Versions of Windows

Beware! Subtitle Files Can Hack Your Computer While You're Enjoying Movies

Newly Found Malware Uses 7 NSA Hacking Tools, Where WannaCry Uses 2

7-Year-Old Samba Flaw Lets Hackers Access Thousands of Linux PCs Remotely



Google Adds New Behavior-Based Malware Scanner To Every Android Device

The Best Password Managers of 2016

More Hacking Groups Found Exploiting SMB Flaw Weeks Before WannaCry

Wanna Cry Again? NSA's Windows 'EsteemAudit' RDP Exploit Remains Unpatched