BadRabbit Ransomware

What is Ransomware? Ransomware is a malicious software that encrypts the files and locks device, such as a computer, tablet or smartphone and then demands a ransom to unlock it. Recently, a dangerous ransomware named 'BadRabbit' has been affecting computers in Russia and countries in east Europe.

What is BadRabbit Ransomware? BadRabbit (assigned by GroupIB) is a ransomware virus that affects Microsoft Windows based systems. This ransomware outbreak has had a considerable impact in the affected countries. This is ransomware is reported to be an improved variant of NotPetya ransomware. It demands a ransom of $280 worth of Bitcoins (0.05 BTC).

What makes it dangerous? It encrypts the files using the attacker's RSA-2048 public key and prevents access to the system. It targets specific file extensions:

> *3ds 7z accdb ai asm asp aspx avhd back bak bmp brw c cab cc cer cfg conf cpp crt cs ctl cxx dbf der dib disk djvu doc docx dwg eml fdb gz h hdd hpp hxx iso java jfif jpe jpeg jpg js kdbx key mail mdb msg nrg odc odf odg odi odm odp ods odt ora ost ova ovf p12 p7b p7c pdf pem pfx php pmf png ppt pptx ps1 pst pvi py pyc pyw qcow qcow2 rar rb rtf scm sln sql tar tib tif tiff vb vbox vbs vcb vdi vfd vhd vhdx vmc vmdk vmsd vmtm vmx vsdx vsv work xls xlsx xml xvd zip*

Also, unlike WannaCry, this ransomware **does not have a kill switch**. It also **has the capability to spread laterally. This is of major concern if the ransomware virus lands on machines with administrative privileges.**

How does it spread? The ransomware spreads as a drive-by download on infected websites. It also comes disguised as Adobe flash update. It is also being reported that the ransomware virus spreads by stealing login credentials using WMIC / Mimikatz tools. It also spreads by brute-forcing authentication of SMB shares. It also uses EnternalRomance exploit to spread within the network.

What is its impact? So far the malware has been dominant in Russia and eastern European countries. The affected entities include three Russian websites, including that of Interfax and Fontanka, an airport in Ukraine, an underground railway station in Kiev, the capital city of Ukraine.

How to prevent infection? Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection / attacks:

- Restrict execution of powershell /WSCRIPT/ PSEXEC / WMIC / MIMIKATZ in enterprise environment Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled. Script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.
- Block the execution of files

- C: \ windows \ infpub.dat
- C: \ Windows \ cscc.dat

It prevents the ransomware from running, but doesn't stop it spreading on the network.

- Restrict Scheduled Tasks: viserion_, rhaegal, drogon
- In order to prevent infection users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010 (https://technet.microsoft.com/library/security/MS17-010) and June 2017 Security Update (https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/40969d56-1b2a-e711-80db-000d3a32fc99_ This fixes the CVE-2017-0199
- To prevent data loss Users & Organisations are advised to take backup of Critical Data
- Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1. (https://support.microsoft.com/en-us/help/2696547)
- Restrict TCP ports 139 and 445 traffic to where it is absolutely needed using router ACLs
- Use private VLANs if your edge switches support this feature
- Use host based firewalls to limit communication on TCP ports 139 and 445, especially between workstations

Indicators of Compromise

Following are IOCs as reported by various security researchers (some of these are from unofficial sources and hence should be used with caution):

- **Hashes**
  - Dropper:
    - 630325cac09ac3fab908f903e3b00d0dadd5fdaa0875ed8496fcbb97a558d0da
  - Payload:
    - 8ebc97e05c8e1073bda2efb6f4d00ad7e789260afa2c276f0c72740b838a0a93 C:\Windows\dispci.exe (diskcryptor client)
    - 682ADCB55FE4649F7B22505A54A9DBC454B4090FC2BB84AF7DB5B0908F3B7806 C:\Windows\cscc.dat (x32 diskcryptor drv)
    - 0b2f863f4119dc88a22cc97c0a136c88a0127cb026751303b045f7322a8972f6 C:\Windows\cscc.dat (x64 diskcryptor drv)
    - 579FD8A0385482FB4C789561A30B09F25671E86422F40EF5CCA2036B28F99648 C:\Windows\infpub.dat
    - 2f8c54f9fa8e47596a3beff0031f85360e56840c77f71c6a573ace6f46412035 (mimikatz-like x86)

- 301b905eb98d8d6bb559c04bbda26628a942b2c4107c07a02e8f753bdcfe347c (mimikatz-like x64)

- **Compromised website**
  - 1dnscontrol[.]com
  - caforssztxqzf2nm[.]onion (Payment site)
  - 185.149.120[.]3/scholargoogle/ (Inject URL)
  - 1dnscontrol[.]com/flash_install.php (Distribution URL)
  - argumentiru[.]com
  - www.fontanka[.]ru
  - grupovo[.]bg
  - www.sinematurk[.]com
  - www.aica.co[.]jp
  - spbvoditel[.]ru
  - argumenti[.]ru
  - www.mediaport[.]ua
  - blog.fontanka[.]ru
  - an-crimea[.]ru
  - www.t.ks[.]ua
  - most-dnepr[.]info
  - osvitaportal.com[.]ua
  - www.otbrana[.]com
  - calendar.fontanka[.]ru
  - www.grupovo[.]bg
  - www.pensionhotel[.]cz
  - www.online812[.]ru
  - www.imer[.]ro
  - novayagazeta.spb[.]ru
  - i24.com[.]ua
  - bg.pensionhotel[.]com
  - ankerch-crimea[.]ru

- **Yara Rule Set**
  - https://github.com/Neo23x0/signature-base/blob/master/yara/crime_badrabbit.yar

- **File Information**

File Name	Malware Family	Description

infopub.dat	Win32/Diskcoder.D	Diskcoder
dispci.exe	Win32/Diskcoder.D	Lockscreen
Win32/RiskWare.Mimikatz.X	Mimikatz	(32-bits)
Win64/Riskware.Mimikatz.X	Mimikatz	(64-bits)
install_flash_player.exe	Win32/Diskcoder.D	Dropper
page-main.js	JS/Agent.NWC	JavaScript on compromised sites

References:

- Cert-In Advisory on BadRabbit - http://cert-in.org.in/
- https://gist.github.com/roycewilliams/a723aaf8a6ac3ba4f817847610935cfb
- https://www.group-ib.com/blog/badrabbit
- https://www.zscaler.com/blogs/research/bad-rabbit-new-petya-ransomware-variant
- https://www.welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back
- http://blog.talosintelligence.com/2017/10/bad-rabbit.html?m=1#more
- https://securelist.com/bad-rabbit-ransomware/82851/
- https://blog.malwarebytes.com/threat-analysis/2017/10/badrabbit-closer-look-new-version-petyanotpetya/