Ransomware Revealed:
Robbed With a Wooden Gun

Brian Baskin
Senior Threat Researcher
Carbon Black
Threat Analysis Unit (TAU)

Swee Lai Lee
Malware Analyst
Carbon Black
Threat Analysis Unit (TAU)
What are we talking about?

nRansom

Your computer has been locked. You can only unlock it with the special unlock code.

go to protonmail.com and create an account.
Send an email to 1_kill_yourself_1@protonmail.com.
We will not respond immedatly. After we reply, you must send at least 10 nude pictures of you. After that we will have to verify that the nudes belong to you.
Once you are verified, we will give you your unlock code and sell your nudes on the deep web

Got your unlock code and sent your nudes?
Submit your unlock code here

Unlock
Psychology of Forcing Payment

- Early ransomware required actual, large-scale destruction to set tone
- Public expectation of highly secure encryption with payment being only method of escape
- Newer ransomware capitalizing from this to create fake, or weak, ransomware
  - Even if it doesn’t work, people expect that it would, and pay anyway
Psychology of Forcing Payment

- **Consumer Ransomware**
  - “Gotcha” ransomware (porn, piracy, etc)
  - Force infection through want (software downloads, game cracks)
  - Force payment through risk of exposure

- **Enterprise Ransomware**
  - Force infection through acceptable social norms (emailed Invoices)
  - Use urgency to override judgment
  - Force payment through lack of recovery
Trigger an Immediate Response

Oppsops!!
Time Left: 23:58:34

At the expiration of time all your files will be made public on the internet, and the PC will be permanently locked!
Let’s Talk About Being Fake Again
What Did Victims See?

We will not respond immediately. After we reply, you must send at least 10 nude pictures of you. After that we will have to verify that the nudes belong to you. Once you are verified, we will give you your unlock code and sell your nudes on the deep web.
It’s Not Real, Is it?

Thomas the Tank Engine Ransomware Wants to See You Naked
It’s Not Real, Is it?

NRansom: It's not just your nudes, it's also your Bitcoin

This Ransomware Demands Nudes Instead of Bitcoin

It was inevitable.
How do we know it’s fake?

- Files dropped and used:
  
  AxInterop.WMPLib.dll
  Interop.WMPLib.dll
  nRansom.exe
  Tools\your-mom-gay.mp3
How do we know it’s fake?

```csharp
private void Button1_Click(object sender, EventArgs e)
{
    bool flag = Conversions.ToDouble(this.TextBox1.Text) == 12345.0;
    if (flag)
    {
        this.Hide();
        MyProject.Forms.Form2.Show();
    }
    else
    {
        this.unlockerror();
    }
}
```
Yet, the Impact

Kevin Beaumont
@GossiTheDog

That nudes ransomware, which isn’t even in wild, has more press coverage than CCleaner trojan—which infected millions of PCs at banks, govs.

12:27 PM - 22 Sep 2017
AutismLocker

listen to me you big juicy nut. Your computer has been locked. There are 2 ways to unlock it. In order to get the special code You must record yourself gunning down innocent children or send me 15 of your nudes. Send the recording or the nudes to j[REDACTED]@india.com and we will make sure you kill more than 17 people in the recording or make sure the nudes belong to you, and then you will get the code. Once I get the recording/pics I will put them on /b/. Remember, Hitler did nothing wrong
private void Button1_Click(object sender, EventArgs e)
{
    bool flag = Conversions.ToDouble(this.TextBox1.Text) == 12324354.0;
    if (flag)
    {
        this.Hide();
    }
}
The darknet sites are not existing, its just an example text. The other things are right, except the darknet thing. Its possible to get the key, but if I going to do a new trojan, or new version of this then I will add real ways to get the key :) If you wanna that I going to do a 2.0 or a new trojan, then write it below in the comments. Thanks if you wanna chat with me, contact me easily in discord: iCoreX#1337

Time: 3367
Warning! Do you got .NET Framework '4.5' (not 4.0)? If you are not running it with .NET Framework '4.5' then the TROJAN won't work! If you got .NET Framework '4.5' then press on 'yes' if not then on 'no'!
February 22, 2018

Annabelle ransomware a horror show for users

Horror fans know the consequences of an encounter with the evil doll Annabelle - users should similarly beware of the same-named ransomware, which possesses a bag of evil tricks to wreak havoc on an infected computer.

Last year we heard similar conversations about ransomware, which has yet to loosen its grip on organizations around the world. According to research from Enterprise Strategy Group (ESG), 63 percent of companies experienced an attempted ransomware attack in 2017, and a newly discovered variant, Annabelle, is seemingly designed to wreak as much havoc as possible.

By Andy Norton February 23, 2018
Kids are off limits!
Are They Serious?

cd %USERPROFILE%
for /r %%v in (*.rbxl) do %USERPROFILE%\runtime -e -p apples "%%v"
for /r %%v in (*.rbxm) do %USERPROFILE%\runtime -e -p apples "%%v"
for /r %%v in (*.rbxm) do %USERPROFILE%\runtime -e -p apples "%%v"
for /r %%v in (*.lua) do %USERPROFILE%\runtime -e -p apples "%%v"
for /r %%v in (*.rbxl) do del "%%v"
for /r %%v in (*.rbxm) do del "%%v"
for /r %%v in (*.rbxm) do del "%%v"
for /r %%v in (*.lua) do del "%%v"
cd %USERPROFILE%
del runtime.exe
del license.bat
How Secure is it Really?
Hello Buddy! if you see this message all your important files are been crypted :) 
What can you do? You can pay with bitcoin and wait 10 min for decryption!
It's very easy! Don't you know how to purchase bitcoin? www.localbitcoins.com it's your place!
If Antivirus block the crypter, you'll be unable to decrypt...
If is this your case, go to in any of this website:

http://www.24fkxhnr3cdtvwmy.onion.to
http://24fkxhnr3cdtvwmy.onion.nu
http://24fkxhnr3cdtvwmy.onion.link
Your Windows has been Locked by ByteLocker

How can I unlock my windows??
It's easy pay 150 dollars to bitcoin adress below and we will get you decryption code

Bitcoin Adress: XXXX-XXXX-XXXX-XXXX

Enjoy (:)

How can I unlock my windows??
It's easy pay 150 dollars to bitcoin adress below and we will get you decryption code

Bitcoin Adress: XXXX-XXXX-XXXX-XXXX

Enter Decryption Key

Buy BitCoins
Unlock My Windows
JF Ransomware

All of your files have been encrypted!

```csharp
bool flag = e.KeyCode == Keys.Return;
if (flag)
{
    bool flag2 = this.code.Text == "Saus2018";
    if (flag2)
    {
    
```
Your Windows has been Banned

Dear Windows User, Your PC have been banned and we are sorry to say that we are now Hijacking (legally) because of Fake V
To Know more ab

Solution Found!!!
Yes, To Unlock Your PC Now, You can 2 things. You have to play us in order to Unblock your pc or we will delete all of your files now!

Payment Information:
We are demanding: 200$ (USD)
Send it Via Paypal to: microsoftyber@hackindex.com
Robbed with Rubber Bullets
It’s still bad, right?

Got your unlock code and sent your nudes?
Submit your unlock code here.

Fuck You

Unhandled exception has occurred in your application. If you click Continue, the application will ignore this error and attempt to continue. If you click Quit, the application will close immediately.

Conversion from string "covfe" to type 'Double' is not valid.

Details
Continue
Quit

Carbon Black.
using (AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider())
{
    aesCryptoServiceProvider.Key = Convert.FromBase64String("PjTsAwwF56cICkIyDAQhtR==");
    aesCryptoServiceProvider.IV = new byte[]
    {
        0,
        1,
        0,
        3,
        5,
        3,
        0,
        1,
        0,
        0,
        0,
        0,
        0,
        0,
        6,
        7,
        6,
        0
    };
    Class96.EncryptData(FilePath, aesCryptoServiceProvider, FilePath + FileExt);
SamSam Broken Decryption

- Adversary-driven, command line-based
- Introduced via open RDP, JBoss, Winshock, etc
- Mimikatz and PowerShell to deploy
- Creates encryption key for each targeted host
- Manual monitoring of encryption to ensure
Poorly written decryptor would corrupt restores
Half-hearted error detection

catch (Exception ex)
{
    Console.WriteLine("Key is not correct format : " + ex.Message);
    if (File.Exists(encryptedFilePath))
    {
        File.Delete(encryptedFilePath);
    }
}

public static byte[] RSAEncryptBytes(byte[] datas, string keyXml)
{
    byte[] result = null;
    using (RSACryptoServiceProvider rsacryptoServiceProvider = new RSACryptoServiceProvider(2048))
    {
        rsacryptoServiceProvider.FromXmlString(keyXml);
        result = rsacryptoServiceProvider.Encrypt(datas, true);
    }
    return result;
}

public static byte[] GetBytesFromStrings(string str)
How Do You Tell the Difference
Identifying A Strain

- Leverage Online Identification Methods
  - [https://id-ransomware.malwarehunterteam.com](https://id-ransomware.malwarehunterteam.com)
  - [https://id-ransomware.blogspot.com](https://id-ransomware.blogspot.com)

![Kirk]

This ransomware has no known way of decrypting data at this time.

It is recommended to backup your encrypted files, and hope for a solution in the future.

Identified by:
- ransomshe_filename: RANSOM_NOTE.txt
- ransomshe_email: kirk.payments@scryptmail.com

Click here for more information about Kirk
Applying What We Discussed

Being a smart victim

● Know your escape routes
  ○ Have sufficient backups
  ○ Have ability to promptly determine root cause
    ■ Delivery mechanism suggests level of threat
    ■ Endpoint monitoring

● Perform very basic analysis
  ○ Quickly identify ransomware strains
    ■ Determine type, how authentic, if there’s known decryptors
  ○ Identify if ransomware is easily defeatable
  ○ Just Run Strings
Questions?

Brian Baskin
bbaskin@carbonblack.com

Swee Lai Lee
sweelai.lee@carbonblack.com