

WanaCrypt0r – What we know so far

Jake Williams

SANS Instructor / Founder Rendition Infosec

rsec.us

@MalwareJake

Agenda

- Quick overview
- What we know about WanaCrypt0r
- Some cool reversing stuff
- Staying safe
- Should MS answer about MS17-010?
- Closing thoughts and questions

Quick Overview

Why are we even here?

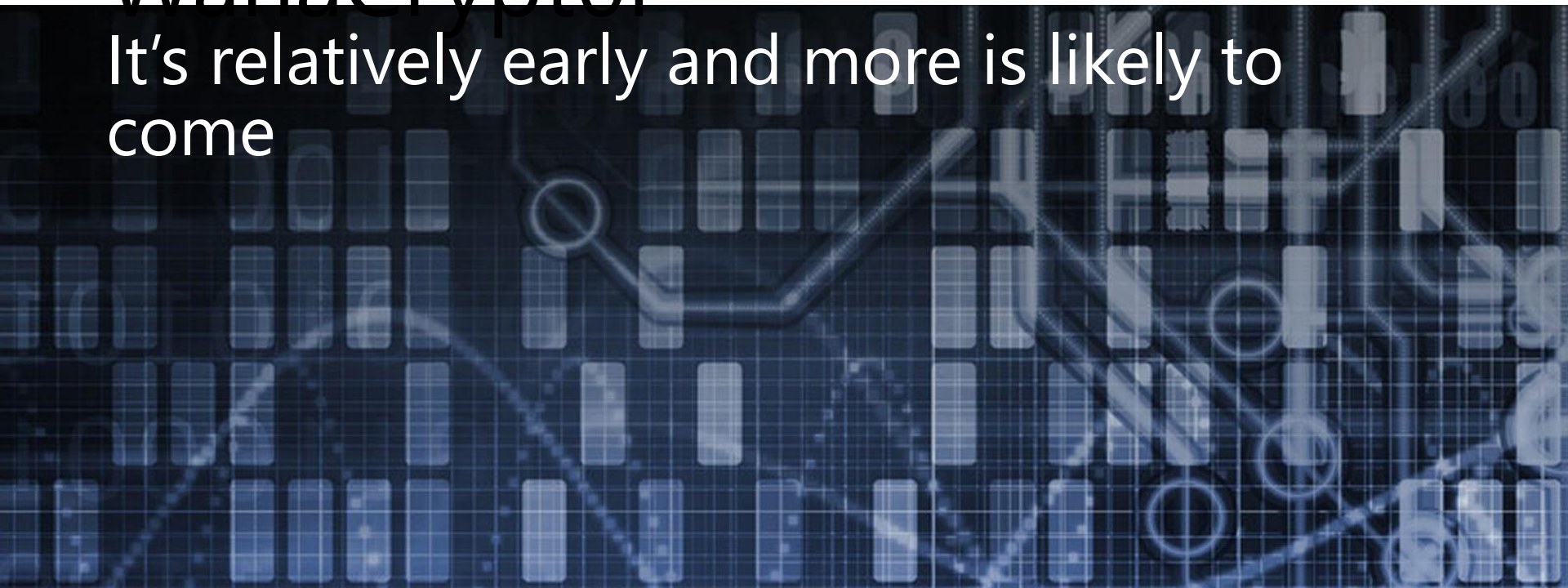
The background of the lower half of the slide is a dark blue, almost black, grid. Overlaid on this grid are various glowing blue elements: a prominent line graph with a peak and a dip, several circular nodes connected by lines, and various rectangular shapes that look like data points or components of a system. The overall aesthetic is futuristic and technical.

WanaCry first appears 12MAY17

- NHS hospitals in England reportedly turning away ambulances, 16 hospitals reportedly hit
- Telefonica was reportedly suffering outages
- Russia interior ministry
- German train station in Frankfurt
- Fedex was reported infected

What we know about WanaCrypt0r

It's relatively early and more is likely to
come



How is it spreading?

- There are two key components - a worm and a ransomware package
- The worm appears to be spreading using leaked NSA exploit ETERNALBLUE and DOUBLEPULSAR
 - Targets machines using SMB

Current Status

- The malware has a kill switch that terminates if this domain resolves
- Might have been anti-analysis, but it's now registered and neuters the malware
- My favorite domain of all time:
 - www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

Some people are paying



morb
@m0rb

Total Transactions: 42
Total BTC Received: 7.14505182BTC
Total Est. USD: \$11689.23332700
[#wannacry](#) [#wcrypt](#)

e.g. 115HrrV ServkAJCftWsBMPLb6S3jBAQM7y

115p7UMMngo1pMvkhHijcRdfJNXj6LrLn

Total Received: 1.19397749

Total Sent: 0.00000000

Final Balance: 1.19397749

Total transactions: 9

Recent transactions:



Some cool reversing stuff

Now you're just showing off...

The background of the slide is a dark blue grid with various technical and scientific diagrams overlaid. These include a circuit board with a central component, a DNA double helix structure, and a network graph with nodes and connecting lines. The overall aesthetic is futuristic and technical.

The password...

- The malware contains the hardcoded password WNcry@2017

```
lea    eax, [ebp+ExistingFileName]
push   eax                ; lpPathName
call   ds:SetCurrentDirectoryA
push   1                  ; Source
call   sub_4010FD
mov    [esp+6F4h+var_6F4], offset aWncry@2017 ; "WNcry@2017"
push   ebx                ; hModule
call   sub_401DAB
call   sub_401E9E
push   ebx                ; lpExitCode
push   ebx                ; dwMilliseconds
push   offset CommandLine ; "attrib +h ."
call   sub_401064
push   ebx                ; lpExitCode
push   ebx                ; dwMilliseconds
push   offset aIcacs_GrantEv ; "icacs . /grant Everyone:F /T /C /Q"
call   sub_401064
add    esp, 20h
call   sub_40170A
```

The resource...

- The malware drops a encrypted zip file from a resource named "XIA"

```
; int __cdecl sub_401DAB(HMODULE hModule, char *Source)
sub_401DAB proc near

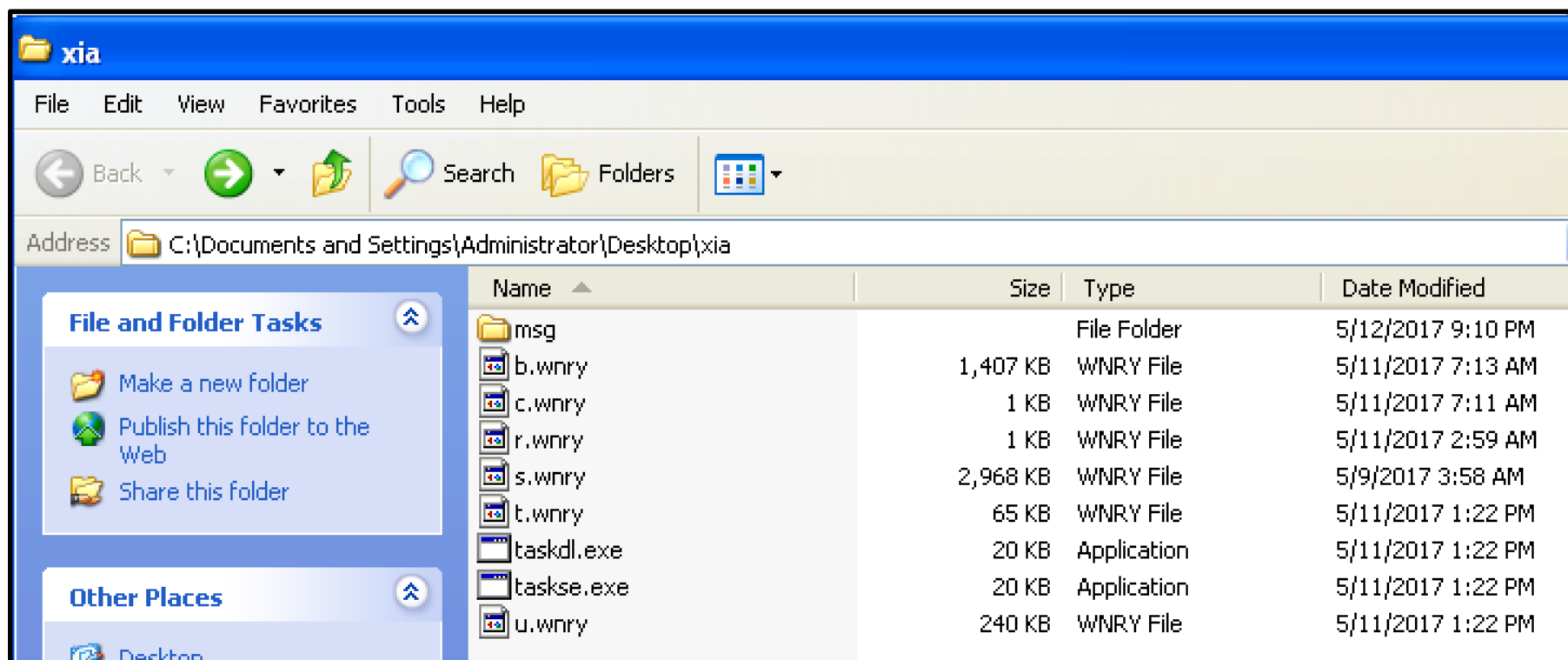
Src= dword ptr -12Ch
FileName= byte ptr -128h
hModule= dword ptr 8
Source= dword ptr 0Ch

push    ebp
mov     ebp, esp
sub     esp, 12Ch
push    esi
push    edi
push    offset Type          ; "XIA"
push    80Ah                ; lpName
push    [ebp+hModule]       ; hModule
call    ds:FindResourceA
mov     esi, eax
test    esi, esi
jz     short loc_401E07
```



Extracting the resource (2)

- Now just unzip it using the password to get these files



The screenshot shows a Windows Explorer window titled 'xia' with the address bar set to 'C:\Documents and Settings\Administrator\Desktop\xia'. The main pane displays a list of files and folders:

Name	Size	Type	Date Modified
msg		File Folder	5/12/2017 9:10 PM
b.wnry	1,407 KB	WNRY File	5/11/2017 7:13 AM
c.wnry	1 KB	WNRY File	5/11/2017 7:11 AM
r.wnry	1 KB	WNRY File	5/11/2017 2:59 AM
s.wnry	2,968 KB	WNRY File	5/9/2017 3:58 AM
t.wnry	65 KB	WNRY File	5/11/2017 1:22 PM
taskdl.exe	20 KB	Application	5/11/2017 1:22 PM
taskse.exe	20 KB	Application	5/11/2017 1:22 PM
u.wnry	240 KB	WNRY File	5/11/2017 1:22 PM

The left sidebar shows 'File and Folder Tasks' (Make a new folder, Publish this folder to the Web, Share this folder) and 'Other Places' (Desktop).

More fun secrets

- Now just unzip it using the password to get these files

```
sift$ file *
b.wnry:      PC bitmap, Windows 3.x format, 800 x 600 x 24
c.wnry:      data
msg:         directory
r.wnry:      ASCII text, with CRLF line terminators
s.wnry:      Zip archive data, at least v1.0 to extract
taskdl.exe:  PE32 executable (GUI) Intel 80386, for MS Windows
taskse.exe:  PE32 executable (GUI) Intel 80386, for MS Windows
t.wnry:      data
u.wnry:      PE32 executable (GUI) Intel 80386, for MS Windows
```

What's the other zip?

- It appears the other zip is tor.exe (and supporting files)

```
sift$ unzip -l s.wnry
Archive:  s.wnry
  Length      Date    Time    Name
-----
          0  2000-01-01  00:00   Data/
          0  2017-05-09  16:58   Data/Tor/
          0  2000-01-01  00:00   Tor/
 3197106  2000-01-01  00:00   Tor/libeay32.dll
   719217  2000-01-01  00:00   Tor/libevent-2-0-5.dll
   417759  2000-01-01  00:00   Tor/libevent_core-2-0-5.dll
   411369  2000-01-01  00:00   Tor/libevent_extra-2-0-5.dll
   523262  2000-01-01  00:00   Tor/libgcc_s_sjlj-1.dll
    92599  2000-01-01  00:00   Tor/libssp-0.dll
   711459  2000-01-01  00:00   Tor/ssleay32.dll
 3098624  2000-01-01  00:00   Tor/tor.exe
   107520  2000-01-01  00:00   Tor/zlib1.dll
-----
 9278915                               12 files
```



Convenience is key

- Trying to be convenient for people to find the decryptor

```
SET ow = WScript.CreateObject("WScript.Shell")
SET om = ow.CreateShortcut("C:\@WanaDecryptor@.exe.lnk")
om.TargetPath = "C:\@WanaDecryptor@.exe"
om.Save
```


Staying Safe

Even if you can't patch, you CAN stay safe



Patch, patch, patch

- If you want to stay safe from this, patching is really the only serious option
- The patch has been available since March...
- If you can't patch (for instance you are on Windows Server 2003), consider network segmentation

Network Segmentation

- Restrict TCP port 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 445, especially between workstations
- BONUS: This will help protect against lateral movement as well!

What about MS17-010?

Yeah, there's something fishy going on here



How did this get out?

- The Shadow Brokers released data about the exploit in January
 - However the actual exploit was kept secret
- Microsoft mysteriously patched the exploit in March after missing its first Patch Tuesday ever in February

What can Microsoft tell the public?


- How was the vulnerability disclosed?
- Who disclosed it?
- Before it was disclosed, does Microsoft has telemetry showing that it was used to hack victims in the wild before January?
- Did the rate of exploitation increase after January?

This is unprecedented

- There's no precedent for Microsoft releasing this data, but the whole event is unprecedented
- There has never been a leak of nation state hacking tools before
- Read more here:
 - bit.ly/MS17010-petition

Closing thoughts and questions

Take your best shot



Takeaways

- 60 day patching cycles aren't okay
 - I'm personally amazed it took this long
- Be ready for more attacks like this in the future
 - Attackers are getting more sophisticated and will benefit from leaked NSA and CIA hacking program data and tools
- Don't forget that WikiLeaks has a trove of CIA hacking tools that remain unreleased to us
 - But who knows who else has them???

May 12, 2017 DOUBLEPULSAR

- During the live webcast, I said that DOUBLEPULSAR infections for Internet connected hosts were up
- This was based on a sampling error. The current numbers are as follows:



Jake Williams @MalwareJake · 11m

Latest Internet wide DOUBLEPULSAR scans:

Listening TCP 445: 3,078,509

Responded to SMB request: 1,298,343

Infected with DOUBLEPULSAR: 23,104



Don't Ignore This Threat

- After the webcast, multiple people emailed me and asked if they should work the weekend to patch or if the kill switch mitigated this
 - This is an individual risk decision
- But there will be a new variant of this, and probably sooner than later
 - I think ignoring it is probably a career limiting move for most

That's all folks!

Thanks for your time

Jake Williams – Rendition Infosec

www.rsec.us

@MalwareJake