When Malware Meets Murphy

Mattijs van Ommeren
Principal Consultant at Nixu
Hack In The Box Amsterdam
Commsec Track
About Me

• Mattijs van Ommeren
• Principal Consultant at Nixu
• 15+ years experience in IT security
• Pentesting, incident handling, forensics, research

• Twitter: @alcyonsecurity
• E-mail: mattijs.vanommeren@nixu.com
The Bad Beginning

• First case of ransomware reported in 2005 (TROJ_CRYZI.P.A)
• Since 2012 spread across Europe and the U.S.
• 2013: Cryptolocker
Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers

Hollywood Presbyterian Medical Center had lost access to its computer systems since 5 February after hackers installed a virus that encrypted their files.

‘The quickest and most efficient way to restore our systems ... was to pay the ransom,’ said Allen Stefanek, president and chief executive of Hollywood Presbyterian Medical Center. Photograph: Mario Anzuoni/Reuters
## The Phone call

### The goal of 103-1.docx

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>MS-DOS Application</td>
<td>82 KB</td>
</tr>
</tbody>
</table>

*Publisher: Unknown Publisher*

This file does not have a valid digital signature that can be trusted by the publisher. You should only run software from publishers you trust.

**Warning:**

- The publisher could not be verified. Are you sure you want to run this software?
- Do you want to run it anyway?
Incident Handling Process

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons Learned
Preparation

- Policy
- Response Plan
- Communication Plan
- Documentation
- Access Control
- Tools
- Training
Identification

• User calls helpdesk and reports “strange file names”
• No ransom note
• No logs available
  – Logon/logoff events overwritten
  – File System Auditing disabled
Encryption in progress

• Active SMB session:
  – Netstat - ESTABLISHED 445/TCP
  – OPENFILES.EXE
  – Powershell Get-SMBOpenFile (Windows 2012 R2)

• Less volatile
  – Firewall connection logs
  – NETFLOW data
Containment

• Prevent it from getting worse
  – Unplug the network cable?
  – Set file shares to Read-only access
  – File/Share Canary

• FSRM File Screen (Windows 2008 and up)
  https://community.spiceworks.com/how_to/100368-cryptolocker-canary-detect-it-early

• File System Audit & Sinkhole
  http://www.freeforensics.org/2016/03/proactively-reacting-to-ransomware.html

  – Block C2 traffic
Which Files?

- Easily identifiable through new file extension

```
dir /s /a *_decode@india.com
```

924 files
File Explorer

- Find: _decode@india.com

954 files (!)
Powershell

Get-ChildItem Z:\ -Recurse *decode@india.com

The problem

924 files
Path Length Limitation

Maximum Path Length Limitation
In the Windows API (with some exceptions discussed in the following paragraphs), the maximum length for a path is MAX_PATH, which is defined as 260 characters. A local path is structured in the following order: drive letter, colon, backslash, name components separated by backslashes, and a terminating null character. For example, the maximum path on drive D is "D:\some 256-character path string<\NUL>" where "<\NUL>" represents the invisible terminating null character for the current system codepage. (The characters < > are used here for visual clarity and cannot be part of a valid path string.)

Note File I/O functions in the Windows API convert / to \ as part of converting the name to an NT-style name, except when using the "\?\" prefix as detailed in the following sections.

The Windows API has many functions that also have Unicode versions to permit an extended-length path for a maximum total path length of 32,767 characters. This type of path is composed of components separated by backslashes, each up to the value returned in the lpMaximumComponentLength parameter of the GetVolumeInformation function (this value is commonly 255 characters). To specify an extended-length path, use the "\?\" prefix. For example, "\?\D:\very long path".

Note The maximum path of 32,767 characters is approximate, because the "\?\" prefix may be expanded to a longer string by the system at run time, and this expansion applies to the total length.

The "\?\" prefix can also be used with paths constructed according to the universal naming convention (UNC). To specify such a path using UNC, use the "\?\UNC\" prefix. For example, "\?\\UNC\server\share", where "server" is the name of the computer and "share" is the name of the shared folder. These prefixes are not used as part of the path itself. They indicate that the path should be passed to the system with minimal modification, which means that you cannot use forward slashes to represent path separators, or a period to represent the current directory, or double dots to represent the parent directory. Because you cannot use the "\?\" prefix with a relative path, relative paths are always limited to a total of MAX_PATH characters.

There is no need to perform any Unicode normalization on path and file name strings for use by the Windows file I/O API functions because the file system treats path and file names as an opaque sequence of WCHARs. Any normalization that your application requires should be performed with this in mind, external of any calls to related Windows file I/O API functions.

When using an API to create a directory, the specified path cannot be so long that you cannot append an 8.3 file name (that is, the directory name cannot exceed MAX_PATH minus 12).

The Ersatz Elevator

SUBST S: "C:\This Is A Very, very, ... , very Long Folder Name"

DIR /s S:
No Access for you

- Access Denied to Administrator
- ICALCS /takeown?
  - Also affected by 260 char path limitation
  - Can be quickly circumvented by using SUBST
- Or...?
Robocopy FTW!

ROBOCOPY Z: NULL /E /B /L
Powershell & Robocopy

Let’s rebuild

• Good news
  – a valid backup exists (1 day old)
  – Backup solution does not suffer from Path Length Limitation

• But...
  – 1 TB
  – >100,000 files
  – What files to restore?
    • Don’t want to overwrite untouched files
The Wide Window

• Network restore
  – Decentralized file server
  – Connected through 40 Mbps WAN link
  – Restore time > 35 hrs
• Locally Restore to portable hard drive
  – Throughput 25-30 MB per second
  – Restore time approx. 4 hrs (excluding expedition time)

"Never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway."
— Andrew S. Tanenbaum
We are done, are we?

Well...
More affected files

• Certain files encrypted but NOT renamed by the ransomware
• How to identify?
  – Filter on Modified timestamp
  – Contains mix of legitimately edited files and malware encrypted files
More filtering

• Character Frequency Analysis
  – High Entropy -> encrypted file!
• Partially encrypted files
  – High entropy block
Lessons Learned/Recommendations

– Learn how to identify ransomware species
  • Artifacts, behavior
– Familiarize yourself with non-standard recovery scenario's
  • Can you selectively restore files based on certain criteria?
  • Can you still meet RTO?
– Consider File Share Canaries
– Malware is software and hence is fallible
  • Failure to append file extension
  • Other?
– Backups are key
And what might seem to be a series of unfortunate events may, in fact, be the first steps of a journey.

- Lemony Snicket
THE END