Indicators of Compromise Ransomware TeslaCrypt Malware

Kevin Kelly
April 2017
GIAC GCIH, GCED, GCIA

Objective

- Indicators of Compromise
- Ransomware – TeslaCrypt Variant
- Obstacles to Overcome
- Virtual vs. Bare Metal Systems
- Open Source Tools
  - Basics
  - Other Tools
- Ransomware's Self Preservation
- Summary
- Questions

Indicators of Compromise

- Physical characteristics
- Live sample TeslaCrypt Ransomware
  - Touches many files, processes, registry keys
  - Encrypts mapped drives
- To pay or not to pay

Investigations

- Why mention investigations?
- Paradigm for investigations – the closer to the target the better results
  - Time
  - Proximity
  - People
- Crucial to get information collected as soon as possible

Ransomware

- RansomWareSample.exe
  - f3b12a197d732cda29d6d9e698ea58bf
  - Simpler sample of TeslaCrypt
- RansomWareSampleM.exe
  - 5df8b61f8355fa08eb90d6d2837dba0e
  - Improved version
    - Parses all mapped drives
    - Eliminate threats – disabling procexp.exe, cmd.exe, etc..

Obstacles to Overcome

- Collecting datasets without being encrypted
- Too much data collected
- Virtual machine aware
- Disabled utilities that kill processes
- Delete shadow volume backup Files

Virtual vs. Bare Metal systems

- Virtual
  - Snap shot
  - Add open source VMs – Kali, SIFT
  - Restart quickly
  - Reconfigure
  - Network
  - Has identifiers
- Bare Metal
  - Mimic production build
  - Only option
  - Overhead
    - Restarting
    - Recording monitor
    - Space and power

Tools for Windows O/S

- Three basic programs
  - Sysinternals Suite, Microsoft
  - WireShark, open source community
  - Fiddler, Telerik
- Other helpful tools
  - Hex-editor
  - MD5deep – or other hashing program

Sysinternals Suite

- Suite of tools for debugging and analyzing Windows
- Map over the Internet to http://live.sysinternals.com
  - Read only files
- Many tools to choose
  - dependent on the investigation

Process Monitor

- Collects file system, registry and process/thread activity
  - Filters key to using Process Monitor
    - [Operation is Process Create]
    - Filter the malware process and processes spawned
    - Default filter - modify
- Process Tree, Autoscroll, Capture, Clear
- Does not collect key strokes or mouse movements

Autoruns

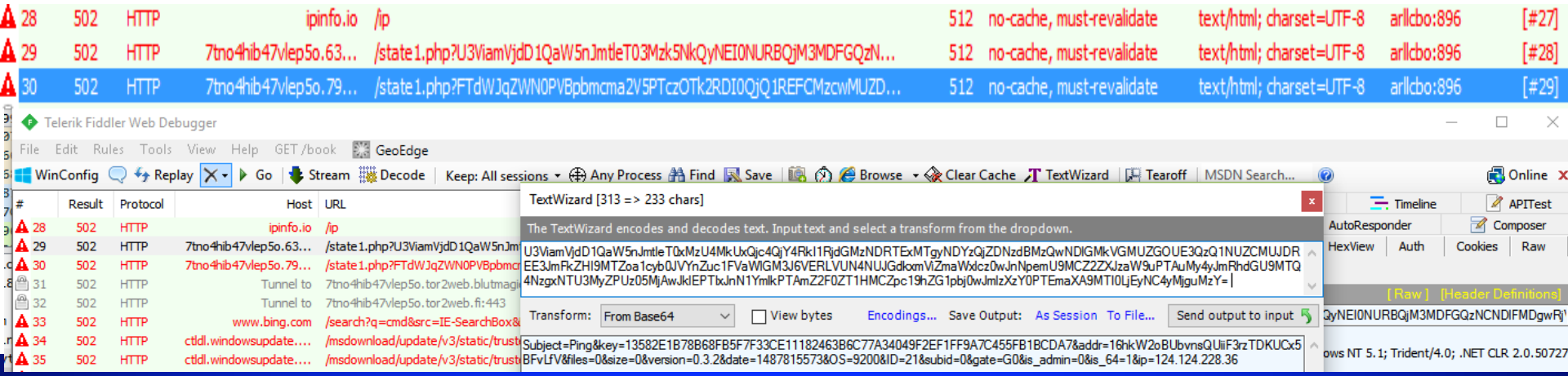
- Two applications, command line and GUI interface.
- Places to startup things in Windows
  - Registry keys, boot
  - Drivers, browse plugins, browser helper objects, services, codec
- Autorunc default startup apps.

Wireshark

- Packet analyzer and collector
- Follow streams
  - Client – Server conversations
  - Data passed
- Conversations and endpoints
  - Command and Control (C2C)
  - Exfiltration

Fiddler

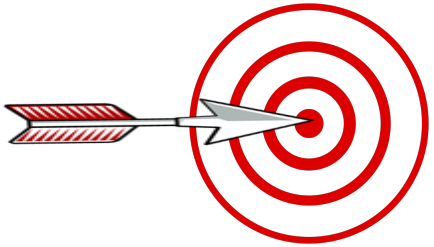
- Flow data
- Composer tab
- HTTP request methods
- Data put on or leaving network



Ransomware Self Protection

- Ransomware
  - VM aware
  - Aware of tools that can terminate it
    - Process explorer – procexp
    - Cmd.exe
  - Look for alternatives
    - Windows Task manager kills processes
    - Rename targeted software

Summary



- Collection data closest to the incident
- Analyze data
  - What? - So what?
- What makes this unique
- Focus on indicators
- Pass information to critical teams
- Plenty of open source solutions
  - Never stop learning
  - Right tool at the right time