



# TOOL TALK

```

01110100110100101001110100101110101110101
10011101100011100110011101011001100111000
00011100001001010001110100111110100
10001011010101110011100111001110011
01100110101001111010011110100111001
10000 COMBO_FIX 100111011101110111011101
1100.ico/.icns/.png01011101110111011101
1001110512x51201110111011101110111011101
1011101100011011110111011101110111011101
110//chrisringesen\\0111011101110111011101
0001110000100101000111011101110111011101
10001011010101110011100111011101110111011
0110011010100111101001110110110110110011001
10011101101010101001110011101011101010101
11001101010111011010100011101011010101001
011001101110101010111010101110101110001100
10101010111010101110101001110101010001110:

```





## Topics We Will Be Covering Today

- What is **ASAP**?
- Brief overview of the malware removal process
- What is ComboFix?
- What kind of infections does ComboFix remove?
- How does ComboFix stack up against specialty products from commercial companies?



# Alliance of Security Analysis Professionals

- Collective of internet security oriented websites/forums and trained helpers
- Provide security related support to computer end users for free
- Non-profit, volunteer network
- TechSupportForum.com / WhatTheTech.com / Many More



## The Malware Removal Process

- Malware removal is like detective work
- Evaluate noticeable symptoms
- Gather more information about the infected computer
- **DDS / aswMBR / GMER's Rookit Scanner**
- Get a complete picture → develop a plan of attack
- Run specialty tools
- Clean up remnants



## What Is ComboFix?

- **ComboFix** is a powerful malware removal tool
- Created by **sUBs**
- Freeware!
- Runs on Windows XP (32-bit) / Vista (32-bit and 64-bit) / 7 (32-bit and 64-bit)
- The Swiss Army Knife of malware removal – targets too many infections to list



## What ComboFix is Not

- Does **NOT** provide active protection against malicious threats
- Does **NOT** replace your antivirus software
- **NOT** for commercial use
- Should **NOT** be used without trained supervision



## ComboFix Features

- Ability to remove and collect new, unknown malware with a script
- Removes very stubborn **rootkit/bootkit/MBR** infections (ex: TDSS, TDL3, TDL4, ZeroAccess)
- Third party tools (**FixTDSS, TDSSKiller**) from large AV software vendors **claim** to remove remove variants of **Tidserv** and **ZeroAccess**
- So how do they stack up against ComboFix?



## TDSSKiller (Kaspersky)

- Good
  - Easy to use, Intuitive/elegant interface
  - Free
  - Fast scan times
  - Good at removing TDSS/TDL variants
  - Log shows drivers currently on the system and info about the MBR





## TDSSKiller (Kaspersky)

- Bad
  - Rarely successful at removing ZeroAccess
  - Sometimes will not even detect ZeroAccess
  - No ability to use custom scripts
  - Only removes several types of rootkits



## Malwarebytes Anti-Malware

- Good
  - Removes rogue anti-virus/system maintenance software
  - Removes trojan horses that other software cannot remove
  - Free (basic version)
  - Easy to use, elegant interface



## Malwarebytes Anti-Malware

- Bad
  - Does not remove rootkits/bootkits and other complex infections
  - Log only shows what infections were removed
  - Scanning takes time



## Conclusion

- Which tool should you use?
- All of them!
- **TDSSKiller** for analysis (find out which driver is being patched by a rootkit)
- **ComboFix** as a frontliner
- **Malwarebytes** to remove rogues and/or clean up remnants



# Resources

- [http://fc06.deviantart.net/fs71/i/2010/226/d/c/Combo Fix Icon by chrisringeisen.png](http://fc06.deviantart.net/fs71/i/2010/226/d/c/Combo_Fix_Icon_by_chrisringeisen.png)
- <http://asap.maddoktor2.com/>
- <http://www.malwareremoval.com>
- <http://www.techsupportforum.com>
- <http://www.whatthetech.com>



## Getting In Touch

- Harry Trieu
- [harry@harrytrieu.com](mailto:harry@harrytrieu.com)
- (562) 507-1654