Newsletter - June 2014

ToolsWatch Team
NJ OUCHN & MJ SOLER

Tools! Lots of Tools Released!

During June 2014, we published 14 **Posts** with **10 News Tools**.

Organized by Date

- Wireshark v1.10.8 Released
- [New Tool] OWASP iOSForensic v1.0 Released
- [New Tool] Maligno v1.1 Released
- Lynis v1.5.6 Released
- THC-Hydra v8.0 Released
- [New Tool] ArchAssault v2014.06.01 – Arch Linux ISO for Penetration Testers Released
- [New Tool] Responder v2.0.9 – AD/Windows Environment Takeover Tool Released
- [New Tool] Automater v2.0 – Information Gathering Tool Released
- PEStudio v8.29 – Static Investigation of Executables Released
- [New Tool] Antak WebShell – PowerShell Console Released
- [New Tool] YASAT v755 (Yet Another Stupid Audit Tool) Released
- [New Tool] MazeBolt DDoS Simulation SaaS Released
- [New Tool] Snoopy v0.1 – Tracking and Profiling Mobiles Users Released
- [New Tool] Shellter v1.0 A Dynamic ShellCode Injector – Released

Black Hat USA 2014: Arsenal Tools Speaker List

We are very pleased to announce that Black Hat Team has released the Lineup for Arsenal Vegas 2014. BH Arsenal is a Tool/Demo area where independent researchers and the open source community will showcase some awesome weapons.

http://www.toolswatch.org/?p=45832

Developer Corner

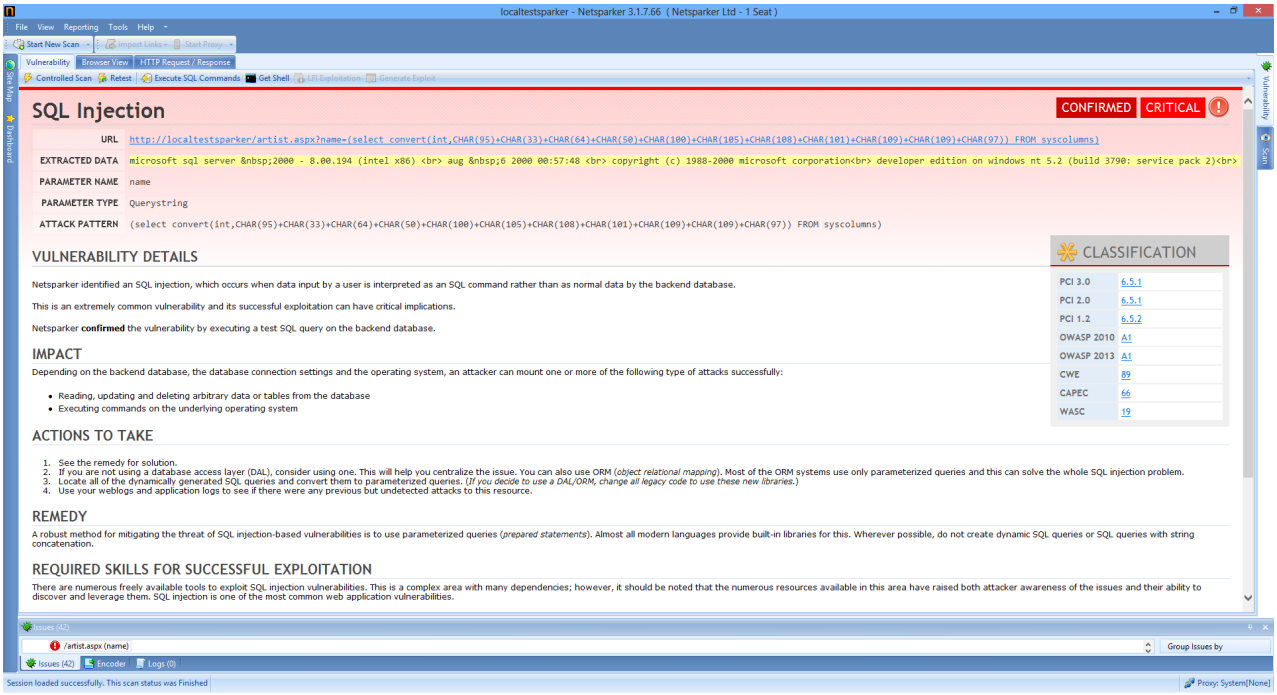
This is a **new section** where some developers have the possibility to tell us about their tools.

Find Vulnerabilities in your Web Applications with Netsparker

Malicious hackers are constantly looking for vulnerable web applications to hack into and steal sensitive business intelligence data, customer information, credit card numbers and more.

The more your business relies on web applications the more of a target these web applications become because they are available 24/7 and are unprotected. Web application vulnerabilities can be automatically detected and are easily exploited.

You can find web application vulnerabilities such as **SQL Injection** and **Cross-site Scripting** (XSS) with the Netsparker Web Application Security Scanner before hackers do and ensure that your web applications, business operations and reputation are protected. Netsparker is the only fully automated **False Positive Free** web application security scanner that detects vulnerabilities on websites and in web applications and reports extensive details about every detected vulnerability.



Netsparker is the only False-positive-free web application security scanner

www.netsparker.com

Tools! Lots of Tools Released!

Wireshark v1.10.8 Released

Wireshark is the world's foremost network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It is the de facto (and often de jure) standard across many industries and educational institutions.

http://www.toolswatch.org/?p=45843

[New Tool] OWASP iOSForensic v1.0 Released

iosForensic is a python tool to help in forensics analysis on iOS. It get files, logs, extract sqlite3 databases and uncompress .plist files in xml. It is licensed under the GNU GPL v3 License.

http://www.toolswatch.org/?p=45840

[New Tool] Maligno v1.1 Released

Maligno is an open source penetration testing tool that serves Metasploit payloads. It generates shellcode with msfvenom and transmits it over HTTP or HTTPS. The shellcode is encrypted with AES and encoded with Base64 prior to transmission. Maligno is licensed under the FreeBSD license.

http://www.toolswatch.org/?p=45823

Lynis v1.5.6 Released

Lynis is an auditing tool which tests and gathers (security) information from Unix based systems. The audience for this tool are security and system auditors, network specialists and system maintainers.

http://www.toolswatch.org/?p=45217

THC-Hydra v8.0 Released

THC-Hydra – the best parallized login hacker: for Samba, FTP, POP3, IMAP, Telnet, HTTP Auth, LDAP, NNTP, MySQL, VNC, ICQ, Socks5, PCNFS, Cisco and more. Includes SSL support and is part of Nessus.

http://www.toolswatch.org/?p=45202

[New Tool] ArchAssault v2014.06.01 – Arch Linux ISO for Penetration Testers Released

The ArchAssault Project is an Arch Linux derivative for penetration testers, security professionals and all-around Linux enthusiasts. This means we import the vast majority of the official upstream Arch Linux packages, these packages are unmodified from their upstream source.

http://www.toolswatch.org/?p=45199

[New Tool] Responder v2.0.9 – AD/Windows Environment Takeover Tool Released

Responder is a LLMNR, NBT-NS and MDNS poisoner, with built-in HTTP/SMB/MSSQL/FTP/LDAP rogue authentication server supporting NTLMv1/NTLMv2/LMv2, Extended Security NTLMSSP and Basic HTTP authentication.

http://www.toolswatch.org/?p=45189

[New Tool] Automater v2.0 – Information Gathering Tool Released

Automater is a URL/Domain, IP Address, and Md5 Hash OSINT tool aimed at making the analysis process easier for intrusion Analysts.

http://www.toolswatch.org/?p=45174

PEStudio v8.29 – Static Investigation of Executables Released

PEStudio is a unique tool that performs the static investigation of 32-bit and 64-bit executable. PEStudio is free for private non-commercial use only.

http://www.toolswatch.org/?p=45072

[New Tool] Antak WebShell – PowerShell Console Released

Antak is a webshell written in C#.Net which utilizes powershell. Antak is a part of Nishang.

http://www.toolswatch.org/?p=45058

[New Tool] YASAT v755 (Yet Another Stupid Audit Tool) Released

YASAT (Yet Another Stupid Audit Tool) is a simple stupid audit tool. Its goal is to be as simple as possible with minimum binary dependencies (only sed, grep and cut). Second goal is to document each test with maximum information and links to official documentation.

http://www.toolswatch.org/?p=45044

[New Tool] MazeBolt DDoS Simulation SaaS Released

MazeBolt DDoS Simulation offers a real-time, controlled DDoS attack on your network providing you with actionable insights on your current security posture. The simulation is an attack which replicates some of the most sophisticated attacks seen in recent years.

http://www.toolswatch.org/?p=45040

[New Tool] Snoopy v0.1 – Tracking and Profiling Mobiles Users Released

Snoopy is a distributed tracking and profiling framework which can perform interesting tracking and profiling of mobile users through the use of WiFi.

http://www.toolswatch.org/?p=45034

[New Tool] Shellter v1.0 A Dynamic ShellCode Injector – Released

Shellter is a dynamic shellcode injection tool aka dynamic PE infector. It can be used in order to inject shellcode into native Windows applications (currently 32-bit apps only). The shellcode can be something yours or something generated through a framework, such as Metasploit.

http://www.toolswatch.org/?p=44999

Papers

(IN)SECURE Magazine Issue #42 Released

(IN)SECURE Magazine is a freely available digital security magazine discussing some of the hottest information security topics.

http://www.toolswatch.org/?p=45818

Developer Corner

This is a new section where some developers have the possibility to tell us about their tools.

In this month the following tools:

- **Jan Seidl** with GoldenEye: A brief history about his tool and how has changed.
- **Beenu Arora** with Hook Analyser.

GoldenEye

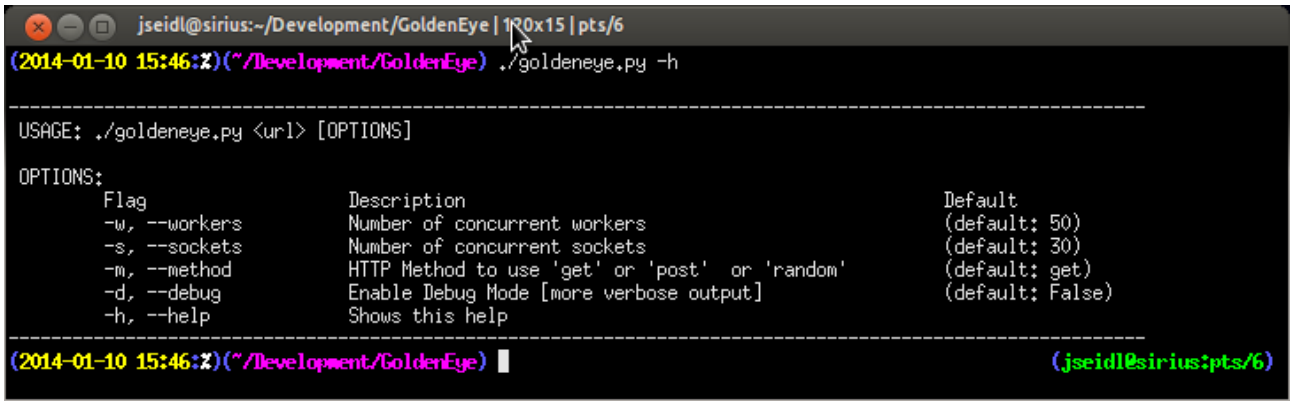
GoldenEye is a HTTP/S Layer 7 Denial-of-Service Testing Tool. It uses KeepAlive (and Connection: keep-alive) paired with Cache-Control options to persist socket connection busting through caching (when possible) until it consumes all available sockets on the HTTP/S server, by **Jan Seidl**.

When I first presented Golden Eye to the world at Hackers 2 Hackers Conference in Brazil back in 2012 as a side-note release on my "Super effective denial of service attacks" I had no idea that the project would have the expression that now, over one and a half year.

Back in 2009, I had watched to a presentation by Nelson Brito on Hackers 2 Hackers Conference on using randomness and unpredictable behavior to avoid detection. The desire to fiddle with randomness and deceiving software detection started right there. In parallel, there was a discussion going about denial-of-service attacks being trivial to detect and block.

I first started the project in order to make a few tweaks in Barry Shteiman's HULK (HTTP Unbearable Load King) in order to bypass a mod_security mitigation for that was very flaky (it relied on a certain Python's urllib2 characteristic -- always sending headers in the same order). It began very simple, I extended Barry's current code and just got rid of urllib2 and replaced with httplib. It did the trick, the signature was now foiled and HULK was alive again.

I wasn't satisfied with the current state of my mods since it was still possible to detect and stop through (many) other means. I started pulling out features that would add a more unpredictable behavior without being natural (off the RFC, common/valid values and such). Despite from randomizing the HTTP headers' order, I've randomized their quantity and values, the HTTP methods used, the querystring data generator routine and such. Soon it became something completely different than the original HULK code and gained it's own name, Golden Eye, as an anecdote with LOIC, the infamous HTTP Flooder.



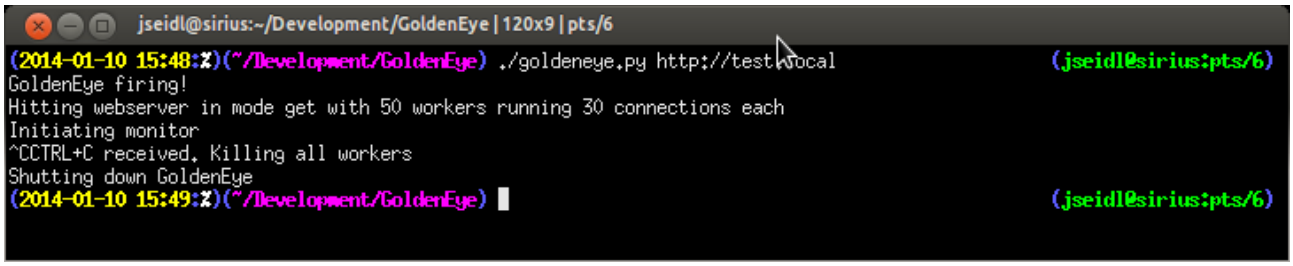
After H2HC, I had the opportunity to present that same talk (and thus Golden Eye) to several conferences in Brazil and it started to get a some local attention. Later in 2013 I submitted to PacketStorm tools and it started to get some global visibility.

A time after that I was fooling around with hacking over mobile on my personal phone and thought: *If a device this size could run Golden Eye, it would be interesting*. Although that could be done by running linux or trying to hack Python to work into the native OS, I decided to swallow my self-respect and learn Java to port the Python program natively to the Android platform. Golden Eye mobile was born.

The mobile version not only worked but it performed *better* than the Python one. I was outraged. How could this be happening? Where are the Python nordic viking gods now? After some research, I saw that the GIL (Global Interpreter Lock) -- a threading feature on Python was slowing me down and I needed to switch from multi-threading to multiprocessing because "*This lock is necessary mainly because CPython's memory management is not thread-safe*". I had to make major modifications to the Python implementation but it got the job done and made the 2.0 version release. Finally Python was winning over Java again and I could sleep in peace.

In January, I had the pleasure of having this release posted this release on ToolsWatch and it helped gaining more and more global users and reposts on other several sites.
Earlier this year I found out that Juniper Netscreen IDS had rolled out a signature for GoldenEye so I quickly downloaded their signature database (it was openly available) and realized that I've left some legacy HULK code that wasn't made to be stealth: Referers and User-Agents. I've left only search-engine's referrals and started picking random user agents from a precompiled extensive file.

Then some guy at Emerging Threats' emerging-sigs mailing-list posted a signature for Golden Eye also, this time for Snort. I decided to quit picking user-agents from a list and made a random generator. Also some more tweaks and BAM, another signature busted. Release 2.1 was rolled out and announced through a blog post and on my twitter account. A few days later was also published on ToolsWatch again! The following month several other sites reposted this release, several twitter accounts mentioned the tool and several other retweeted them. It was the most successful release so far!



In May I was presenting GoldenEye (along with other privacy-related presentation) at Forum Internacional do Software Livre (International Free Software Forum) at Porto Alegre, Brazil and had the pleasure to meet Torsten Gröte from the F-Droid project, which added the GoldenEye Mobile APK to the project and now people can download up-to-date Golden Eye APKs that otherwise would have been pulled out from the Google Play Store due the nature of the tool.

Another great friend I made there was João Eriberto, a brazilian Debian Maintainer. We met at random during lunch, talked for a while and after some more talk he had ready a debian package for Golden Eye that is on the verge of entering the main repository.

I also found out that Golden Eye is on the official repository of BlackArch and ArchAssault Linux pentesting distributions. I hope someday someone will be brave to maintain a package for Kali and many other distributions, even the installation process from the git repository being trivial.

So far, the numbers are: 2 IDS signatures (Juniper Netscreen and Snort), 3 linux distribution's repositories, 18 blog posts, 30+ tweets, tons of presentation, repository and website views and counting! I'm happy that the tool is being appreciated and helpful for many people! It's good to pay back to the community after having relied on its tools when learning most of which I know by now.

Jan Seidl is a passionate for *NIX, BSD, C & Python. Security professional and researcher, recently focused on SCADA security, dedicated pentester and malware reverse analyst with large experience administering servers, networks and applications' security. Author of the book "Segurança de Automação Industrial and SCADA" (pt_BR) and the infosec blog http://wroot.org and is currently CTO from TI Safe Segurança da Informação.

Hook Analyser

Hook Analyser is a freeware application which allows an investigator/analyst to perform "static & run-time / dynamic" analysis of suspicious applications, also gather (analyse & co-related) threat intelligence related information (or data) from various open sources on the Internet, by **Beenu Arora**.

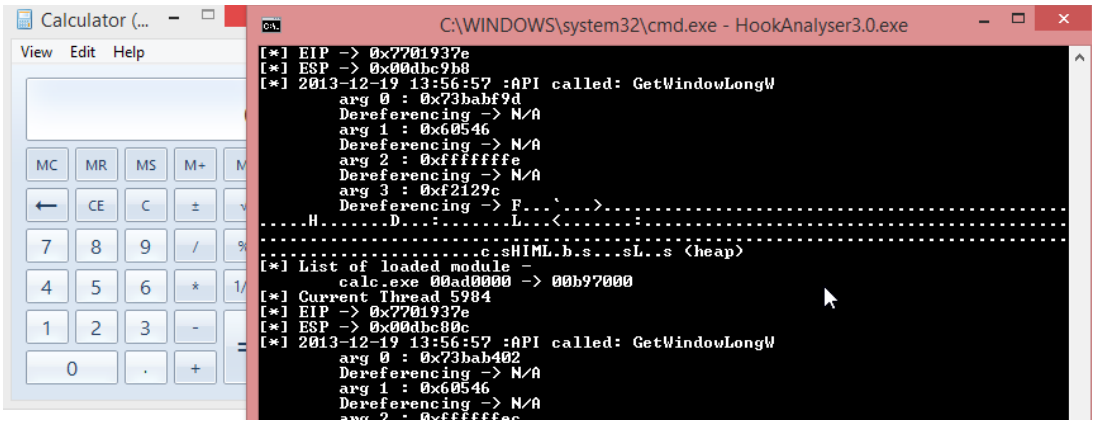
The project/utility has six (6) key functionalities -

1. **Spawn and Hook to Application** - This feature allows analyst to spawn an application, and hook into it. The module performs the following:

    a. PE validation
    b. Static malware analysis.
    c. Other options (such as pattern search or dump all)
    d. Type of hooking (Automatic, Smart or manual)
    e. Spawn and hook

    With the 'hook' module, there are three types of hooking being supported –

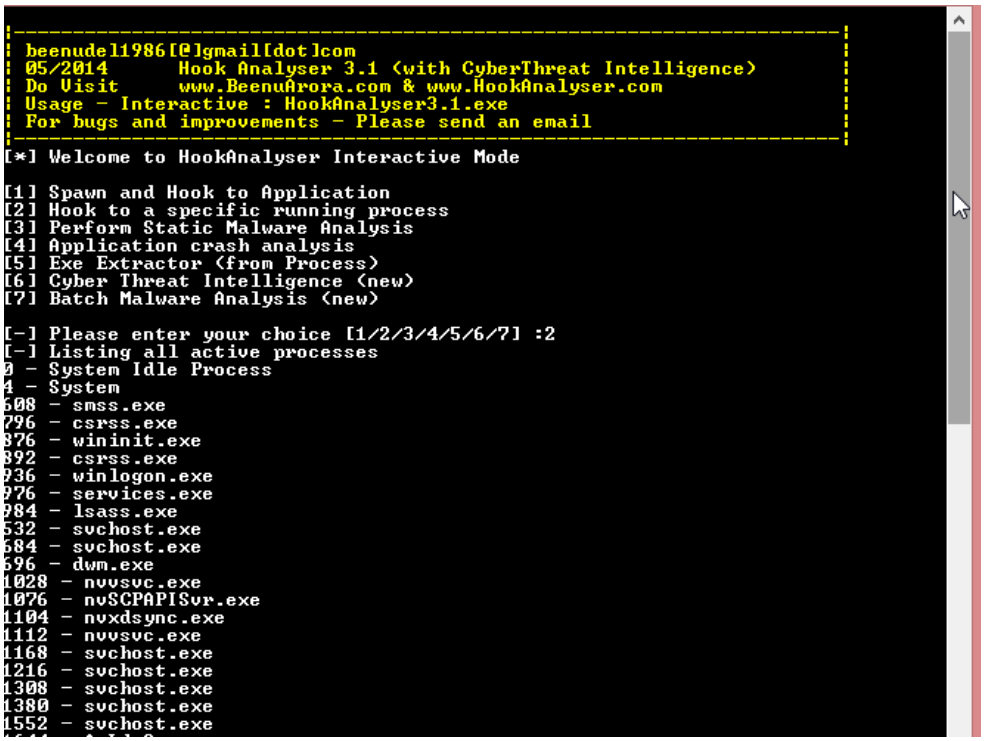
    a) Automatic – The tool will parse the application import tables, and based upon that will hook into specified APIs
    b) Manual – On this, the tool will ask end-user for each API, if it needs to be hooked.
    c) Smart – This is essentially a subset of automatic hooking however, excludes uninteresting APIs.



Spawn and Hook

2. **Hook to a specific running process**-The option allows analyst to hook to a running (active) process. The module performs the following operations –

    a. List all running process
    b. Identify the running process executable path.
    c. Perform static malware analysis on executable (fetched from process executable path)
    d. Other options (such as pattern search or dump all)
    e. Type of hooking (Automatic, Smart or manual)
    f. Hook to a specific running process
    g. Hook and continue the process

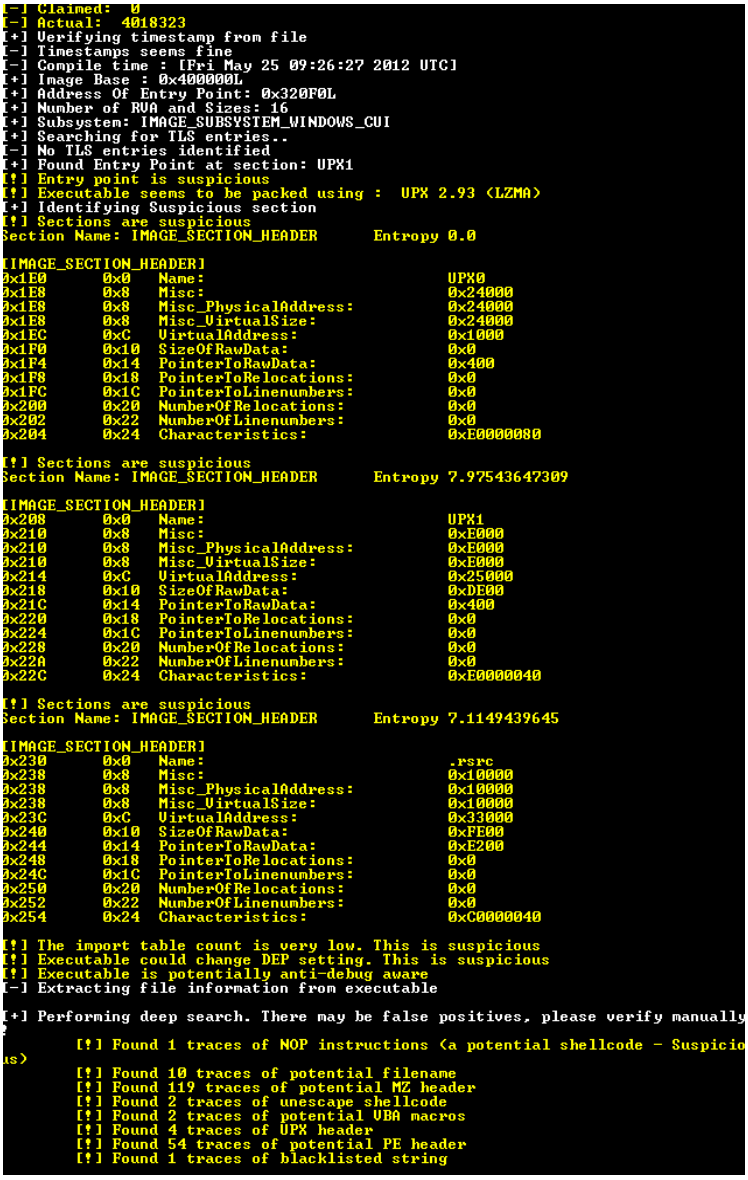


Hook to a Process

3. **Static Malware Analysis** - This module is one of the most interesting and useful module of Hook Analyser, which performs scanning on PE or Widows executables (and DLLs) to identify potential malware traces.

    a. PE file validation
    b. Signed file/malware detection and certificate extraction
    c. CRC and timestamps validation
    d. PE properties such as Image Base, Entry point, sections, subsystem
    e. TLS entry detection.

f. Entry point verification (if falls in suspicious section)
g. Suspicious entry point detection
h. Packer detection
i. Signature trace (extended from malware analyser project), such as Anti VM aware, debug aware, keyboard hook aware etc. This particular function searches for more than 20 unique malware behaviours (using 100's of signature).
j. Import Intel scanning.
k. Deep search (module)
l. Online search of MD5 (of executable) on Threat Expert.
m. String dump (ASCII)
n. Executable file information
o. Hexdump
p. PEfile info dumping
q. ...and more.



Static Analysis

4. **Application crash analysis** - This module enables exploit researcher and/or application developer to analyse memory content when an application crashes. This module essentially displays data in different memory register (such as EIP).

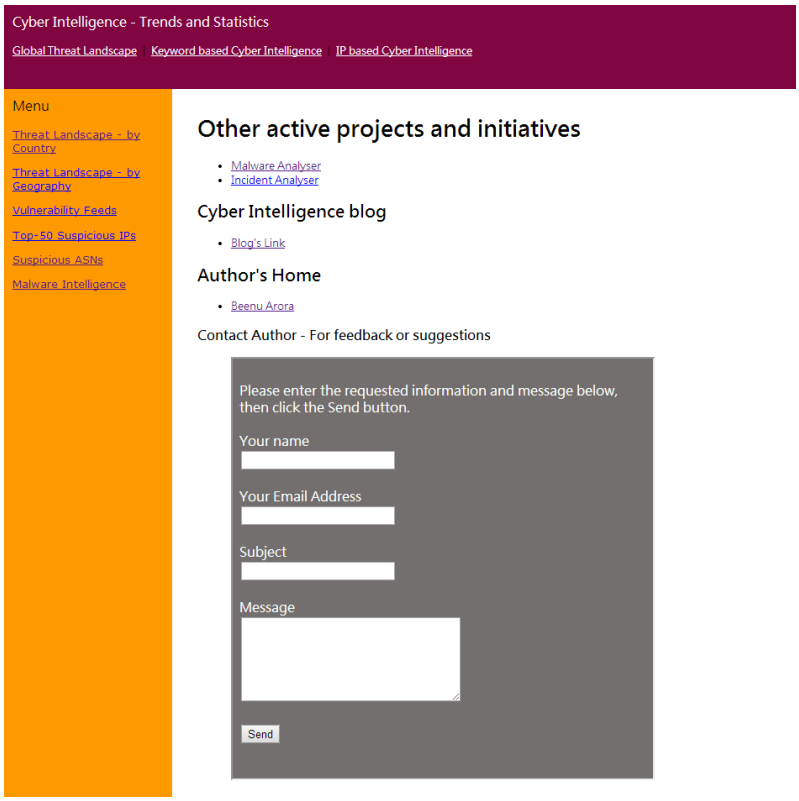
    - Application crash analysis video demonstration: http://www.youtube.com/watch?v=msYo7pPsu6A

5. **Exe extractor** - This module essentially extracts executables from running process/s, which could then be further analysed using Hook Analyser, Malware Analyser or other solutions. This module is useful for incident responders.

6. **Cyber Threat Intelligence** - This module is being created to gather, analyse and visualise information related to Cyber Threats and vulnerabilities. The module can be run using HookAnalyser.exe (via Option 6), or can be run directly.

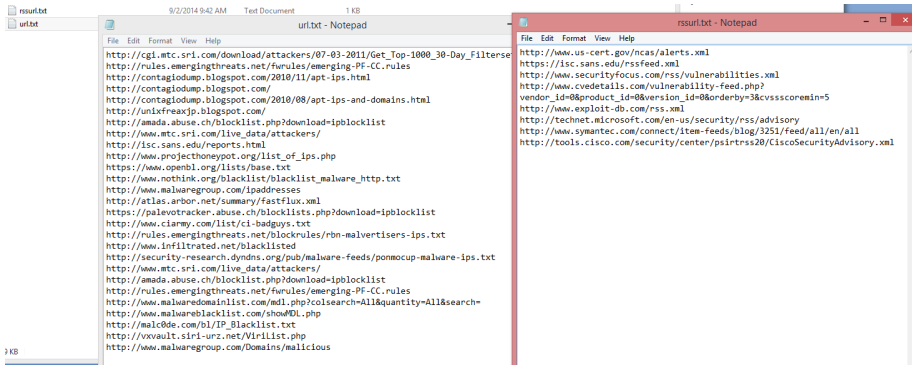
    Demo videos : #1 and #2

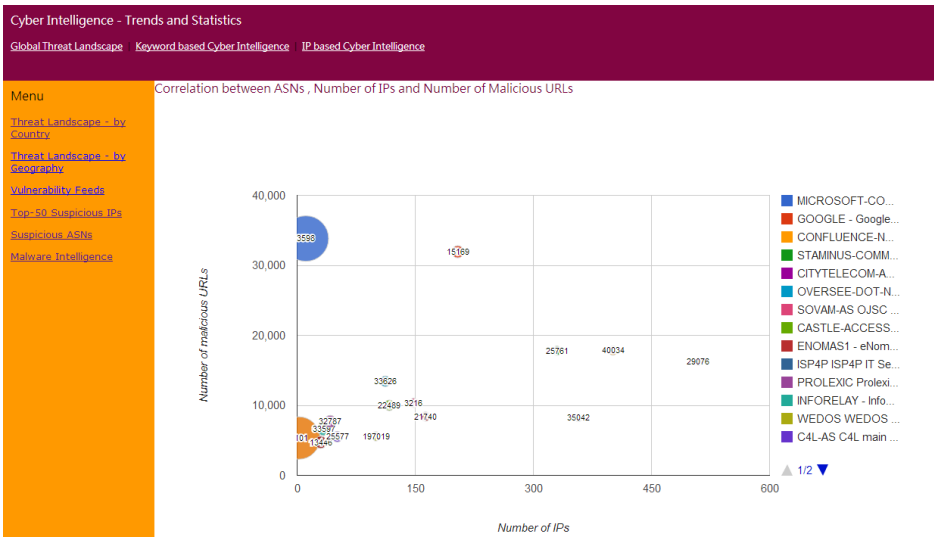
    The module present information on a web browser (with dashboard alike representation). It has three (3) presentations -
    - Global threat landscape
    - Keyword based intelligence
    - IP based intelligence



Cyber Threat Intelligence

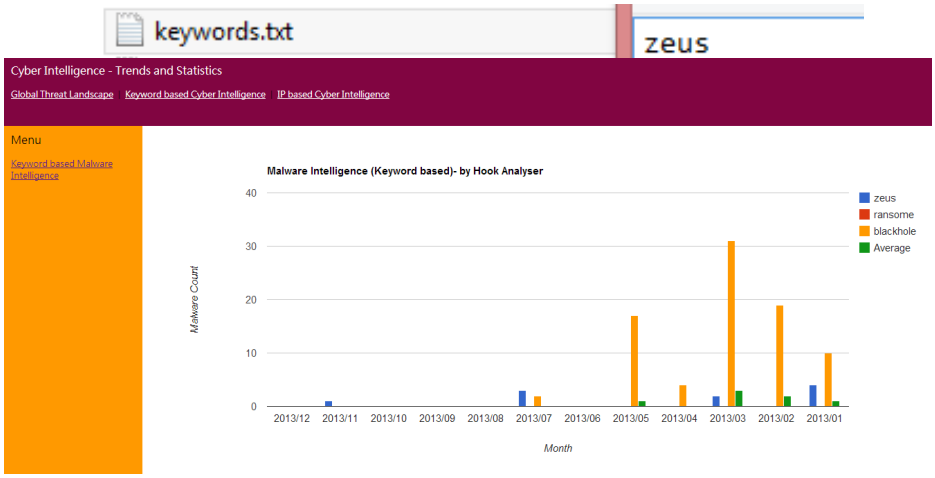
- Global threat landscape - You can specify URLs which has list of malicious IP addresses (to pull information from) and RSS feeds. The software also has a predefined sources where it pulls information from.





Global threat landscape

- Keyword based intelligence - You can insert keywords into the text file - keywords.txt and the software will attempt to extract information related to them.



Keyword based intelligence

Beenu Arora is working as a Cyber security professional at a highly-reputed professional services consulting firm (in Melbourne) and has over six years of Information Technology (IT) security experience in the design, implementation and auditing of complex information systems, with more than five years of experience in the security strategy & operations for resources industry. He has been known for releasing free and open source softwares /solutions.