tripwire
CONFIDENCE: SECURED

Sweet Security

Deploying a Defensive Raspberry Pi

Travis Smith
Senior Security Research Engineer
Tripwire Inc.
tsmith@tripwire.com

Why

- Industrial Control Systems
- Internet of Things

PROTECT THE UNPATCHABLE

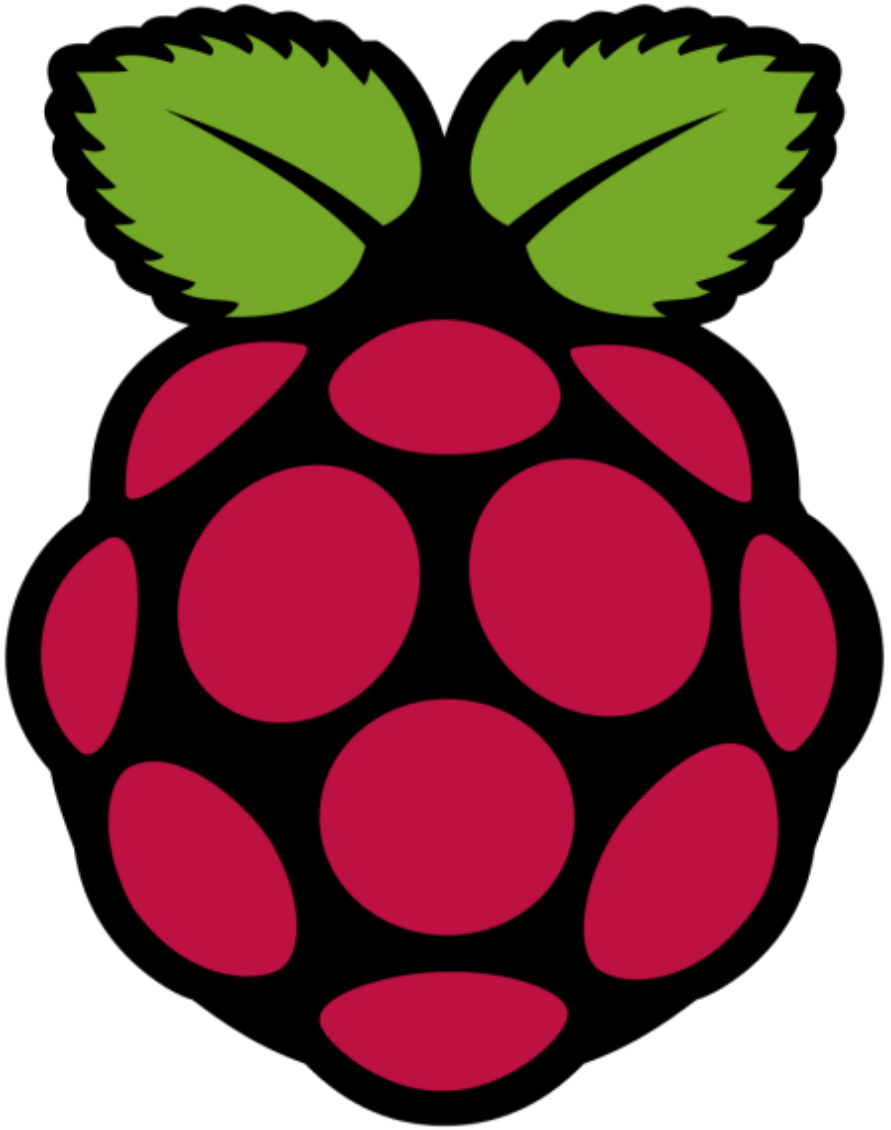
The Hardware

- Raspberry Pi 2 Model B
- 16GB+ Micro SD
- Case
- Micro USB Power Supply

Install the OS

Options

- Raspbian (Debian Wheezy)
- NOOBS
- Ubuntu Mate (maybe)
- Windows 10 IOT Core (no way)



Bro IDS

Overview

Full Packet Capture

```
73 65 72 20 72 6F 6F 74 20 62 79 20 28 75 69 64 ser root by (uid
3D 30 29 89 70 94 50 E4 ED 0A 00 99 00 00 00 99 =0).p.P.........
00 00 00 52 54 00 DA 2C 4C 52 54 00 DA 98 99 08 ...RT..,LRT.....
00 45 00 00 8B 00 00 40 00 40 11 43 37          .E.....@.@.C7...
               A4 DF 02 02 00 77 79 82 3C 37 38 ,.........wy.<78
3E 4E 6F 76 20 20 33 20 31 32 3A 31 37 3A 30 31 >Nov  3 12:17:01
20 64 61 74 61 62 61 73 65 20 2F 55 53 52 2F 53  database /USR/S
42 49 4E 2F 43 52 4F 4E 5B 31 38 31 33 35 5D 3A BIN/CRON[18135]:
20 28 72 6F 6F 74 29 20 43 4D 44 20 28 20 20 20  (root) CMD (
63 64 20 2F 20 26 26 20 72 75 6E 2D 70 61 72 74 cd / && run-part
73 20 2D 2D 72 65 70 6F 72 74 20 2F 65 74 63 2F s --report /etc/
63 72 6F 6E 2E 68 6F 75 72 6C 79 29 89 70 94 50 cron.hourly).p.P
13 04 0B 00 88 00 00 00 88 00 00 00 52 54 00 DA .............RT..
2C 4C 52 54 00 DA 98 99 08 00 45 00 00 7A 00 00 ,LRT......E..z..
40 00 40 11 43 48                               A4 DF @.@.CH...,......
02 02 00 66 AD DD 3C 38 36 3E 4E 6F 76 20 20 33 ...f..<86>Nov  3
20 31 32 3A 31 37 3A 30 31 20 64 61 74 61 62 61  12:17:01 databa
73 65 20 43 52 4F 4E 5B 31 38 31 33 34 5D 3A 20 se CRON[18134]:
70 61 6D 5F 75 6E 69 78 28 63 72 6F 6E 3A 73 65 pam_unix(cron:se
73 73 69 6F 6E 29 3A 20 73 65 73 73 69 6F 6E 20 ssion): session
63 6C 6F 73 65 64 20 66 6F 72 20 75 73 65 72 20 closed for user
72 6F 6F 74 42 71 94 50 62 6E 05 00 3C 00 00 00 rootBq.Pbn..<...
3C 00 00 00 52 54 00 0D 5E C5 52 54 00 DA 2C 4C <...RT..^.RT..,L
08 06 00 01 08 00 06 04 00 01 52 54 00 DA 2C 4C ..........RT..,L
            00 00 00 00 00 00                   00 00 ..............+..
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Bro IDS

conn.log
dhcp.log
dnp3.log
dns.log
ftp.log
http.log
irc.log
known_services.log
modbus.log
ius.log
smtp.log
snmp.log
ssh.log
ssl.log
syslog.log
tunnel.log
intel.log
notice.log

Bro IDS

Installation

Install Required Dependencies

- `$ sudo apt-get install cmake make gcc g++ flex bison libpcap-dev libssl-dev python-dev swig zlib1g-dev`

Download Bro Source Code

- `$ wget` https://www.bro.org/downloads/release/bro-2.4.tar.gz

Unpack

```
$ sudo ./configure --prefix=/opt/nsm/bro
$ sudo make
$ sudo make install
```

*This Step Takes Awhile…

Network Configuration

Network Gateway

- Pro: No additional hardware needed
- Pro: Simple setup
- Con: Attackers can bypass device by connecting directly to actual gateway/router
- Con: Performance implications

Network Configuration

Span/Mirror Port

- Pro: No additional hardware needed
- Pro: All traffic will be monitored
- Pro: Raspberry Pi isn’t inline
- Con: Home/SMB network equipment may not support Span/Mirror ports

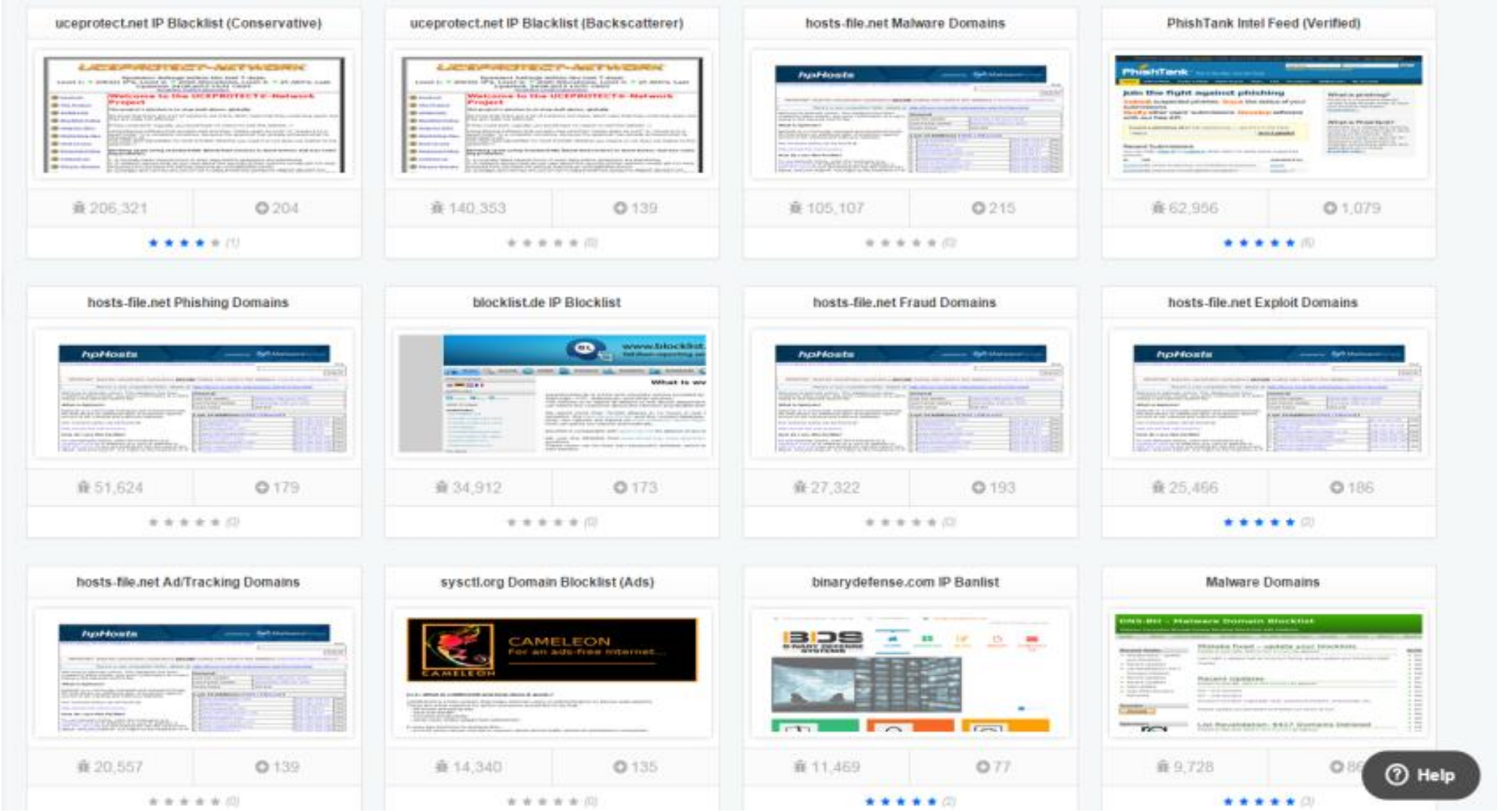
Network Configuration

In-Line

- Pro: All traffic will be monitored
- Con: Raspberry Pi is in-line with all network traffic
- Con: Performance implications
- Con: Additional hardware required

Critical Stack

Threat Intel/Info Made Easy



Critical Stack

Overview

Critical Stack Agent

ID	NAME	LAST UPDATED	INDICATOR COUNT
1	Matsnu-Botnet-(Master-Feed)	04/03/15-10:20-am-(-0400)	9
2	C&Cs-IP-List	04/15/15-10:30-am-(-0400)	134
3	Cryptolocker-(Master-Feed)	04/14/15-01:43-pm-(-0400)	0
4	Post-Tovar-GameOver-Zeus-(Master-Feed)	03/26/15-02:12-pm-(-0400)	0
5	Tinybanker-/-Tinba-(Master-Feed)	03/26/15-02:12-pm-(-0400)	132
6	PushDo-Malware-(Master-Feed)	03/26/15-02:12-pm-(-0400)	0
7	Known-Tor-Exit-Nodes	04/16/15-11:16-am-(-0400)	6567
8	Cyber-Crime-Tracker	04/17/15-02:30-pm-(-0400)	3163
9	Zeus-Tracker:-Configs	03/26/15-02:14-pm-(-0400)	88
10	Zeus-Tracker:-Drop-Zones	03/26/15-02:14-pm-(-0400)	50
11	Zeus-Tracker:-Binaries	04/16/15-11:35-am-(-0400)	59
12	SSL-Blacklist-(SSLBL)	03/26/15-02:12-pm-(-0400)	546
13	Palevo:-Domain-Block-List	04/07/15-11:58-am-(-0400)	15
14	Palevo:-IP-Block-List	03/26/15-02:13-pm-(-0400)	14
15	Zeus-Tracker:-Domain-Block-List	03/30/15-01:23-pm-(-0400)	589
16	SpyEye:-IP-Block-List	02/19/15-01:08-pm-(-0500)	84
17	SpyEye:-Domain-Block-List	02/25/15-05:57-pm-(-0500)	127
18	PhishTank-Intel-Feed-(Verified)	04/16/15-04:57-pm-(-0400)	27734
19	Abuse-Reporting-and-Blacklisting	04/16/15-11:27-am-(-0400)	7666
20	DShield-Domain-List-(Low-Sev)	03/26/15-02:12-pm-(-0400)	4400
21	DShield-Domain-List-(High-Sev)	04/17/15-01:17-pm-(-0400)	4039
22	DShield-Domain-List-(Medium-Sev)	03/26/15-02:12-pm-(-0400)	4231
23	Malware-Domains	04/17/15-01:16-pm-(-0400)	11659
24	Scam-Domains-(Fake/Malware/Drive-By)	04/16/15-11:27-am-(-0400)	4833
25	ET:-Known-Compromised-Hosts	04/16/15-03:01-pm-(-0400)	1080
26	C&Cs-Domains	04/15/15-10:30-am-(-0400)	473
27	IP-Bad-Reputation-(Mail)	04/14/15-06:42-pm-(-0400)	101
28	IP-Bad-Reputation-(HTTP/HTTPS)	02/13/15-01:46-pm-(-0500)	87
29	IP-Bad-Reputation-(Scan)	04/01/15-04:51-pm-(-0400)	414
30	Ponmocup:-Malware-Domains	03/26/15-02:13-pm-(-0400)	12
31	Ponmocup:-Malware-IPs	04/03/15-03:38-pm-(-0400)	31
32	Ponmocup:-Botnet-IPs	04/15/15-03:57-pm-(-0400)	8
33	MTA:-Suspicious-ip/domain-(All)	03/17/15-07:43-am-(-0400)	129
34	Bebloh:-IP-List	03/27/15-07:25-pm-(-0400)	7
35	Bebloh:-Domain-List	03/26/15-02:12-pm-(-0400)	17

100+ Threat Feeds

1,000,000+ Indicators

Critical Stack

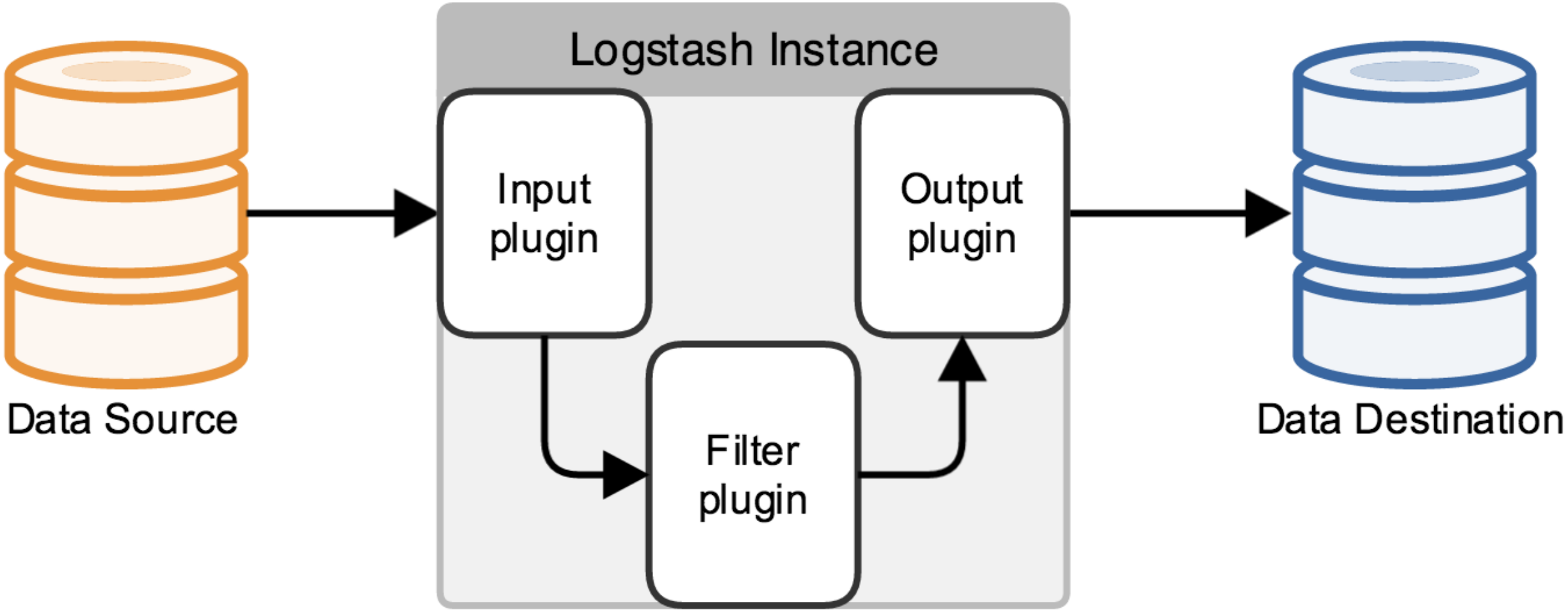
Install

```
$ wget https://intel.criticalstack.com/client/critical-stack-intel-arm.deb
$ sudo dpkg -i critical-stack-intel-arm.deb
```

Add the API Key

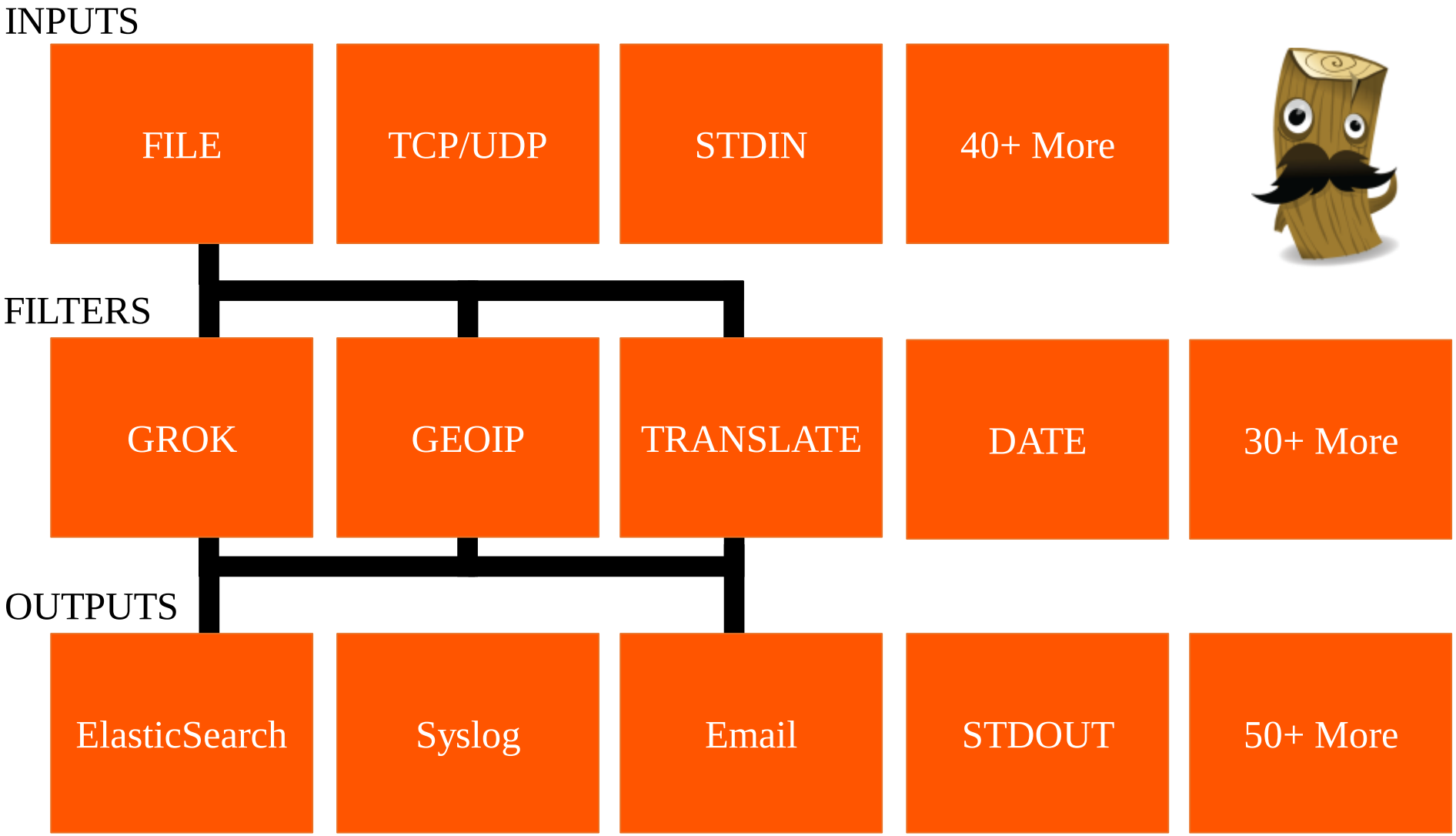
- `$ sudo -u critical-stack critical-stack-intel api <key>`

Logstash


Logstash Instance
Input plugin
Output plugin
Filter plugin
Data Source
Data Destination

Logstash

Overview



Logstash

Overview

- Utilizing Custom Patterns
- GROK Message Filtering
- Adding Custom Fields
- Adding Geo IP Data
- Date Match
- Using Translations for Threat Intel

Elasticsearch

Install

```
$ wget https://download.elastic.co/elasticsearch/elasticsearch/elasticsearch-1.7.1.deb
$ sudo dpkg –i elasticsearch-1.7.1.deb
```

*Update cluster name in yml file

Logstash

Install

```
$ wget https://download.elastic.co/logstash/logstash/logstash-1.5.3.tar.gz
$ sudo mv /opt/logstash-1.5.3/ /opt/logstash
$ cd /opt/logstash
$ bin/logstash -e 'input { stdin { } } output { stdout { } }'
```

FFI Not Available!!! Oh no!

Logstash

Custom ARM Install

First, install Apache ANT

- `$ sudo apt-get install ant`

Next, clone the JFFI repo

- `$ git clone https://github.com/jnr/jffi.git`

Build JFFI with ANT

- `$ cd jffi`
- `$ ant jar`

Copy code to Logstash

- `$ sudo cp build/jni/libjffi-1.2.so /opt/logstash/vendor/jruby/lib/jni/arm-Linux/`

Logstash

Custom ARM Install

Install ZIP

- `$ sudo apt-get install zip`

```
$ cd /opt/logstash/vendor/jruby/lib
$ zip -g jruby-complete-1.7.11.jar jni/arm-Linux/libjffi-1.2.so
$ /opt/logstash/bin/logstash -e 'input { stdin { } } output { stdout
{ } }'
```

Magic!!!!!

Kibana

Install

```
$ wget https://download.elastic.co/kibana/kibana/kibana-4.1.0-linux-x86.tar.gz
$ sudo mkdir /opt/kibana
$ cd /opt/kibana
$ bin/kibana
```

Another error?? Your node needs another ARM!

Kibana

Custom ARM Install

```
$ wget http://node-arm.herokuapp.com/node_latest_armhf.deb
$ sudo dpkg -i node_latest_armhf.deb
$ sudo mv /opt/kibana/node/bin/node /opt/kibana/node/bin/node.orig
$ sudo mv /opt/kibana/node/bin/npm /opt/kibana/node/bin/npm.orig
$ sudo ln -s /usr/local/bin/node /opt/kibana/node/bin/node
$ sudo ln -s /usr/local/bin/npm /opt/kibana/node/bin/npm
$ /opt/kibana/bin/kibana
```

Kibana

Up and Running

Discover Visualize Dashboard Settings

Indices Advanced Objects About

Index Patterns

Warning No default index pattern. You must select or create one to continue.

Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are used to identify the Elasticsearch index to run search and analytics against. They are also used to configure fields.

☑ **Index contains time-based events**

☐ **Use event times to create index names**

Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

logstash-*

Unable to fetch mapping. Do you have indices matching the pattern?

Logstash

Configuration

```
input {
        file {
                path => "/opt/bro/logs/current/*.logs"
                start_position => "beginning"
        }
}
output {
        elasticsearch {
                host => localhost
                cluster => "elasticsearch-clustername"
        }
}
```

Logstash

Configuration

```
filter {
      grok {
            match => {
                  "message" => "%{IP:client} %{WORD:method}
{URIPATHPARAM:request} %{NUMBER:bytes} %{NUMBER:duration}"
            }
      }
}
```

Logstash

Configuration

```
filter {
      grok {
            patterns_dir => "/opt/logstash/custom_patterns"
            match => {
                  message => "%{291009}"
            }
      }
}
```

Logstash

Configuration

Create a Rule File

/opt/logstash/custom_patterns/bro.rule

291009 (?<start_time>\d+\.\d{6})\s+(?<uid>\S+)\s+(?:(?<evt_srcip>[\d\.]+)|(?<evt_srcipv6>[\w:]+)|-)\s+(?:(?<evt_srcport>\d+)|-)\s+(?:(?<evt_dstip>[\d\.]+)|(?<evt_dstipv6>[\w:]+)|-)\s+(?:(?<evt_dstport>\d+)|-)\s+(?<fuid>\S+)\s+(?<file_mime_type>\S+)\s+(?<file_description>\S+)\s+(?<seen_indicator>\S+)\s+(?<seen_indicator_type>[^:]+::\S+)\s+(?<seen_where>[^:]+::\S+)\s+(?<source>\S+(?:\s\S+)*)$

Logstash

Configuration

```
filter {
        if [message] =~ /^((\d{10}\.\d{6})\t([\d\.]+)([\d\.]+)\t(\d+)\t(\d+)\t(\w+))/ {
                grok {
                        patterns_dir => "/opt/logstash/custom_patterns"
                        match => {
                                message => "%{291001}“
                        }
                }
        }
}
```

Remove Capture Groups

~~291001~~ (?<~~start_time~~>\d{10}\.\d{6})\t(?~~<evt_srcip~~>[\d\.]+)\t(?~~<evt_dstip~~>[\d\.]+)\t(?~~<evt_srcport~~>\d+)\t…

Logstash

Configuration

```
filter {
        if [message] =~ /^(\d+\.\d{6}\s+\S+\s+(?:[\d\.]+|[\w:]+|-)\s+(?:\d+|-)\s+(?:[\d\.]+|[\w:]+|-
)\s+(?:\d+|-)\s+\S+\s+\S+\s+\S+\s+\S+\s+[^:]+::\S+\s+[^:]+::\S+\s+\S+(?:\s\S+)*$)/ {
                grok{
                        patterns_dir => "/opt/logstash/custom_patterns"
                        match => {
                                message => "%{291009}"
                        }
                        add_field => [ "rule_id", "291009" ]
                        add_field => [ "Device Type", "IPSIDSDevice" ]
                        add_field => [ "Object", "Process" ]
                        add_field => [ "Action", "General" ]
                        add_field => [ "Status", "Informational" ]
                }
        }
}
```

Logstash

Configuration

```
filter {
  …..all normalization code above here….
  geoip {
   source => "evt_dstip"
   target => "geoip_dst"
   database => “/opt/logstash/GeoLiteCity.dat“
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][longitude]}"]
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][latitude]}"]
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][city\_name]}"]
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][continent\_code]}"]
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][country\_name]}"]
   add_field => ["[geoip_dst][coordinates]","%{[geoip_dst][postal\_code]}“
  }
  mutate {
    convert => [ "[geoip_dst][coordinates]", "float"]
  }
}
```

New ElasticSearch Template Needed

Logstash

Configuration

```
curl -XGET localhost:9200/_template/logstash
{"logstash":{
        "order":0,
        "template":"logstash-*",
        "settings":{
                "index.refresh_interval":"5s"
        },
        "mappings":{
                "properties":{
                        "geoip":{
                                "dynamic":true,
                                "properties":{
                                        "location":{
                                                "type":"geo_point"
                                        }
                                },
                                "type":"object"
                        },
                        …
```

```
{~~"logstash":{~~
        ~~"order":0,~~
        "template":"logstash-*",
        "settings":{
                "index.refresh_interval":"5s"
        },
        "mappings":{
                "properties":{
                        "geoip_dst":{
                                "dynamic":true,
                                "properties":{
                                        "location":{
                                                "type":"geo_point"
                                        }
                                },
                                "type":"object"
                        },
                        …
```

```
curl -XPUT localhost:9200/_template/logstash -d ‘….’
```

Logstash

Configuration

```
filter {
        ....all normalization code above here….
        ….all GeoIP code here....
        date {
                match => [ "start_time", "UNIX" ]
        }
}
```

Logstash

Configuration

```
filter {
      …bro normalization stuff…
       translate {
            field => "evt_dstip"
            destination => "maliciousIP"
            dictionary_path => '/opt/logstash/IP.yaml'
      }
}
```

But what goes in IP.yaml?

Logstash

Configuration

- Dictionary Hash in standard YAML format

```
“1.2.3.4”: “Very Bad IP”
“abc123”: “Very Bad MD5”
```

- Install the translate plugin
  - $ cd /opt/logstash
  - $ bin/plugin install logstash-filter-translate

Logstash

Configuration

- TOR Exit IP: https://check.torproject.org/exit-addresses
- Malicious IP: http://www.malwaredomainlist.com/hostslist/ip.txt

- Automate the scraping of available intel
- Populate the YAML Files

torexit.yaml

```
"162.247.72.201": "YES"
"24.187.20.8": "YES"
"193.34.117.51": "YES"
```

Logstash

Configuration

```
if  "YES" in [tor_IP]  {
   email  {
      options => [ "smtpIporHost", "SMTP_HOST",
       "port", "SMTP_PORT",
       "userName", "EMAIL_USER",
       "password", "EMAIL_PASS",
       "authenticationType", "plain",
       "starttls","true"]
          from => "<EMAIL_USER>"
          subject => "Tor Exit IP Detected on Home Network"
          to => "<EMAIL_USER>"
          via => "smtp"
          htmlbody => htmlBody } }
```

Logstash

htmlBody

```
"Traffic has been detected coming from or going to a TOR Exit Node
IP Address.  <br/><br/>
<b>Source IP: </b>%{evt_srcip}<br/>
<b>Source Port: </b>%{evt_srcport}<br/>
<b>Destination IP: </b>%{evt_dstip}<br/>
<b>Destination Port: </b>%{evt_dstport}<br/><br/>
<b>Raw Log: </b>%{message}"
```

Logstash

Alerts

- TOR IP Addresses
- Malicious IP Addresses
- Malicious File Hashes
- Bro IDS intel.log results
- Bro IDS notice.log results
- Connections to China/Russia/Others
- Device Specific Connection Whitelisting

kibana

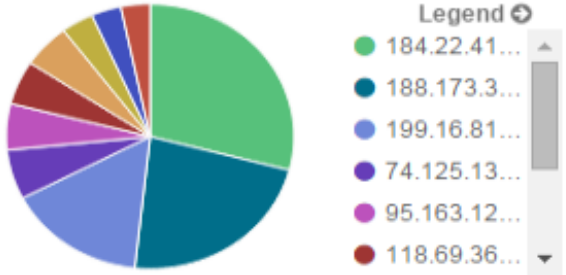
Discover | Visualize | Dashboard | Settings | Last 5 years

Logstash - Bro Base

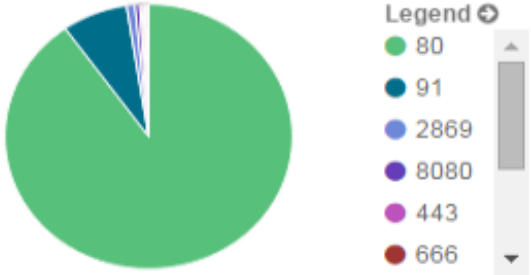
*

Date Chart of Log Sources

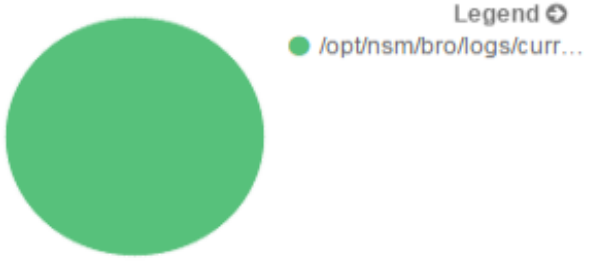
Top Destination IP



Top 10 Destination Ports



Top Log Sources

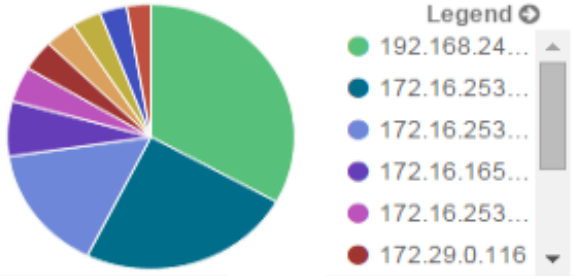


Log Count

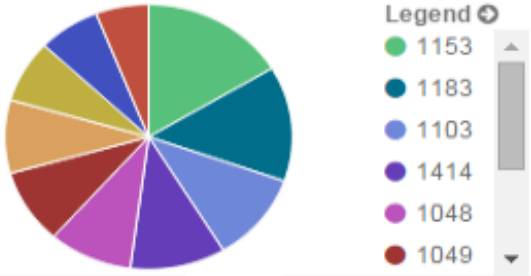
7,604

Count

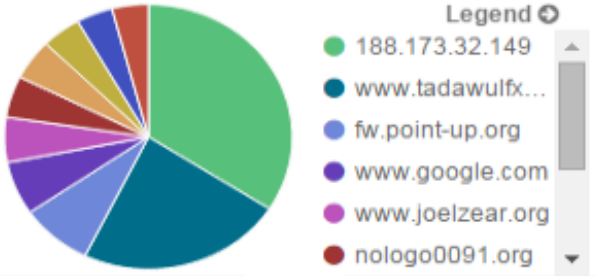
Top Source IP



Top 10 Source Ports



Top 10 Web Sites



Monthly Log Count

@timestamp per month	Count
December 31st 2010, 23:00:00.000	10
July 1st 2011, 00:00:00.000	99
August 1st 2011, 00:00:00.000	8

kibana

Discover | Visualize | Dashboard | Settings | Last 30 minutes

_ThreatIntel_MaliciousIPs

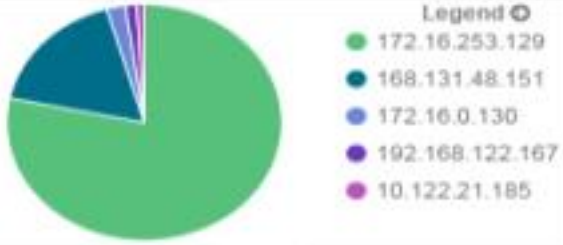
*

_ThreatIntel_MaliciousIP_Map_DST

_ThreatIntel_MaliciousIP_DST

_ThreatIntel_MaliciousIP_Map_SRC

_ThreatIntel_MaliciousIP_SRC



_ThreatIntel_MaliciousIP_Count_DST

8

Unique count of evt_dstip.raw

_ThreatIntel_MaliciousIP_Count_SRC

5

Unique count of evt_srcip.raw

_ThreatIntel_MaliciousIP_DateChart

kibana

Discover | Visualize | Dashboard | Settings

Last 12 hours

_CriticalStack

*

_CriticalStack_IntelMap

_CriticalStack_IndicatorTypes

_CriticalStack_IntelADDR_Sources

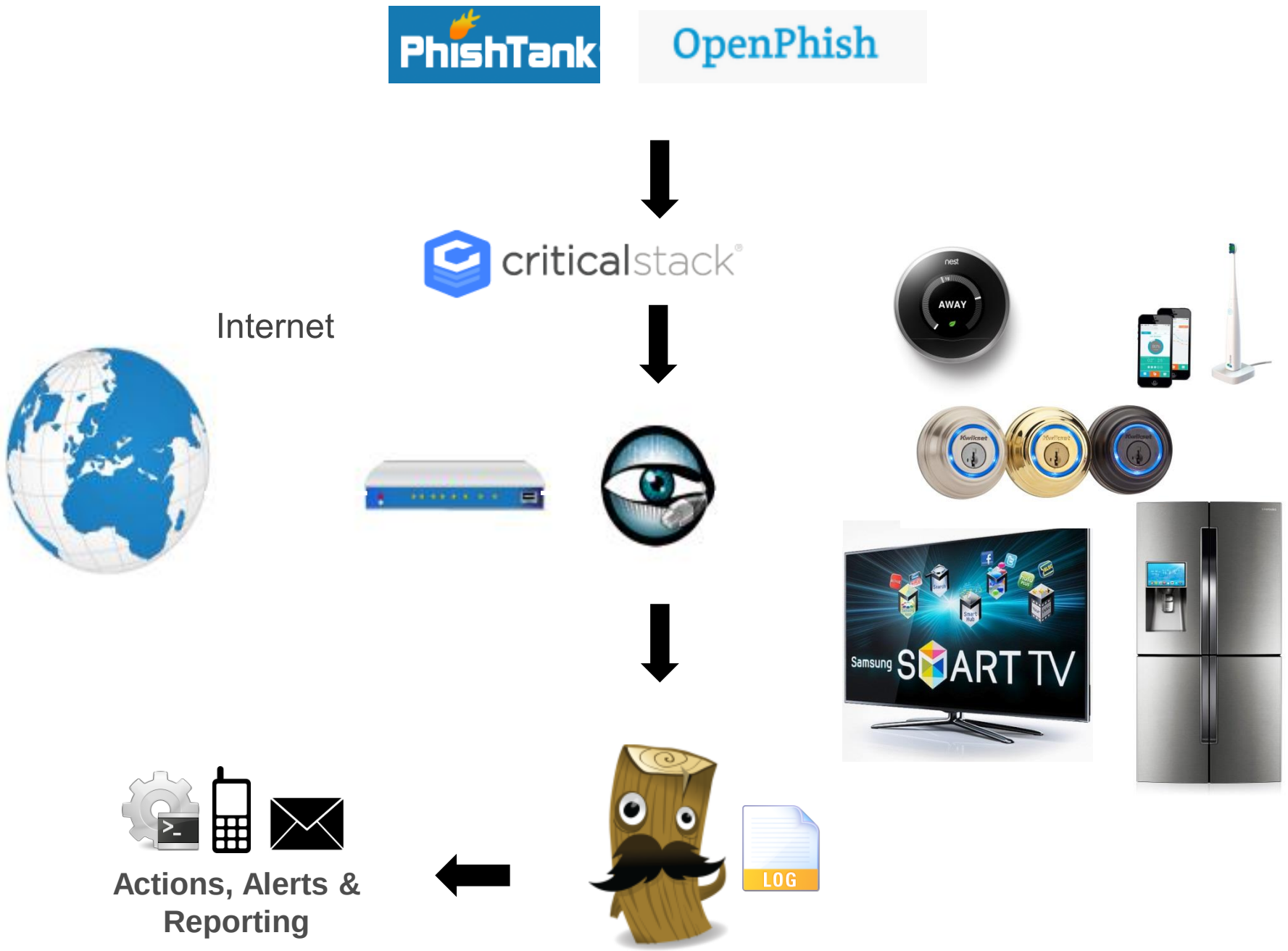
_CriticalStack_IntelDomain_Sources

Easy Button

AKA shell scripts

GitHub repository with scripts and config files to automate the complete process

https://github.com/travisfsmith/sweetsecurity


PhishTank
OpenPhish
criticalstack
Internet
nest
AWAY
Samsung SMART TV
LOG
Actions, Alerts &
Reporting


THAT'S NOT ENOUGH
WE NEED TO GO DEEPER

Device Discovery

NMAP

- Scheduled nmap scan of subnet
  - `sudo nmap -sn 192.168.0.1/255.255.255.0 -oX nmap.xml`
- Parse XML file for new devices
  - New devices added to SQLite DB
    - IP Address & MAC Address
  - Email alerts when new devices found
  - Add as a target into OpenVAS!

https://github.com/TravisFSmith/SweetSecurity/blob/master/networkDiscovery.py

RPI Vuln Scanner

It works, but it's slow

- Install
  - Dependencies
  - OpenVAS-Libraries
  - OpenVAS-Scanner
  - OpenVAS-Manager
  - OpenVAS-CLI
  - Greenbone Security Assistant

https://github.com/TravisFSmith/SweetSecurity/blob/master/installOpenVas.sh

OpenVAS

Integration with Network Discovery

- Add new devices as Scan Targets
- Create a scan task for our new target
  - “Full and fast” scan

Sweet Security

Sample Alert

NEW DEVICES FOUND ON NETWORK:

Host Name: 192.168.0.11 (B8:27:EB:xx:xx:xx)
IP4 Address: 192.168.0.11
MAC Address: B8:27:EB:xx:xx:xx
MAC Vendor: Raspberry Pi Foundation

Host Name: 192.168.0.222 (B8:D9:CE:xx:xx:xx)
IP4 Address: 192.168.0.222
MAC Address: B8:D9:CE:xx:xx:xx
MAC Vendor: Samsung

Commercial Options

AiProtection

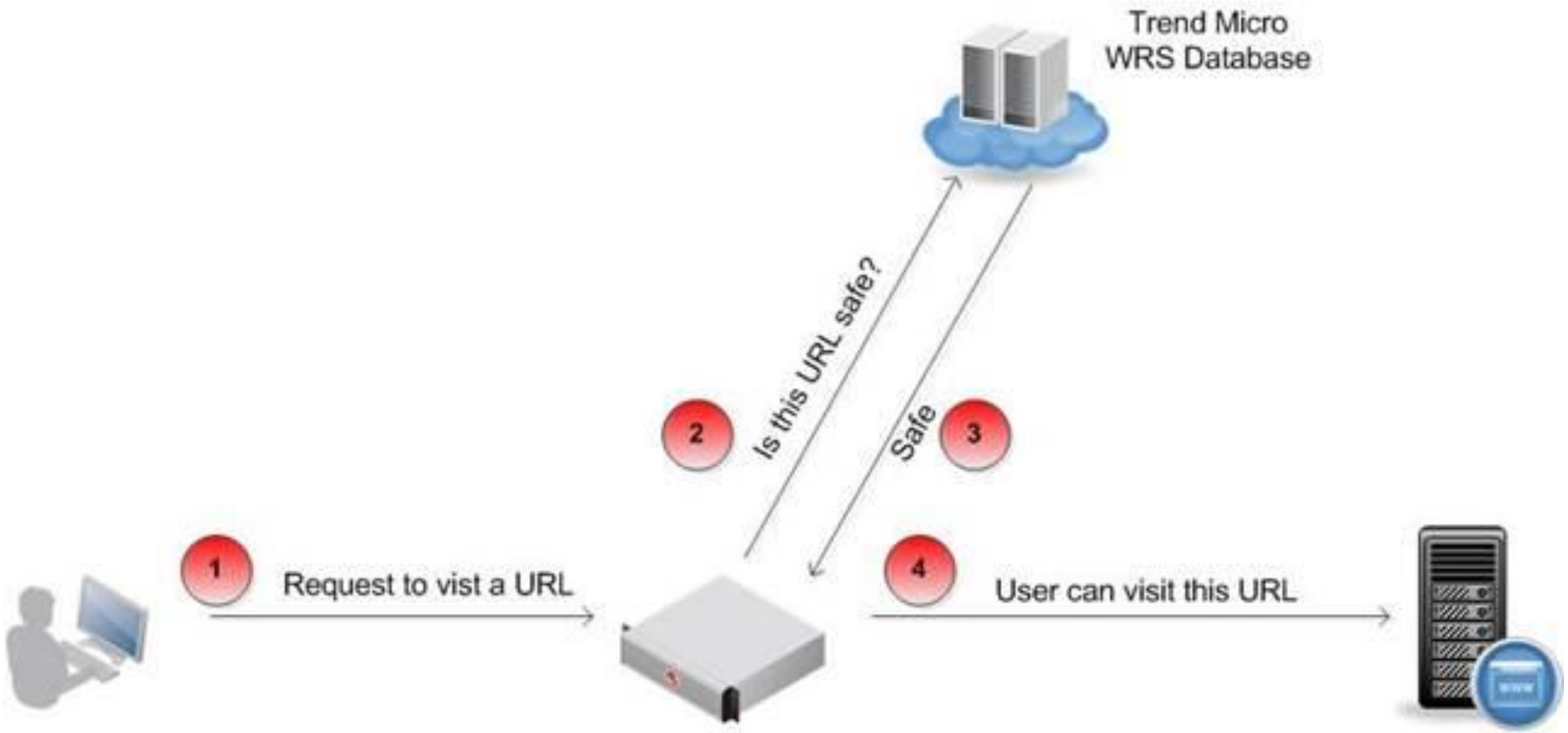
ASUS®

+

TREND MICRO™

AiProtection

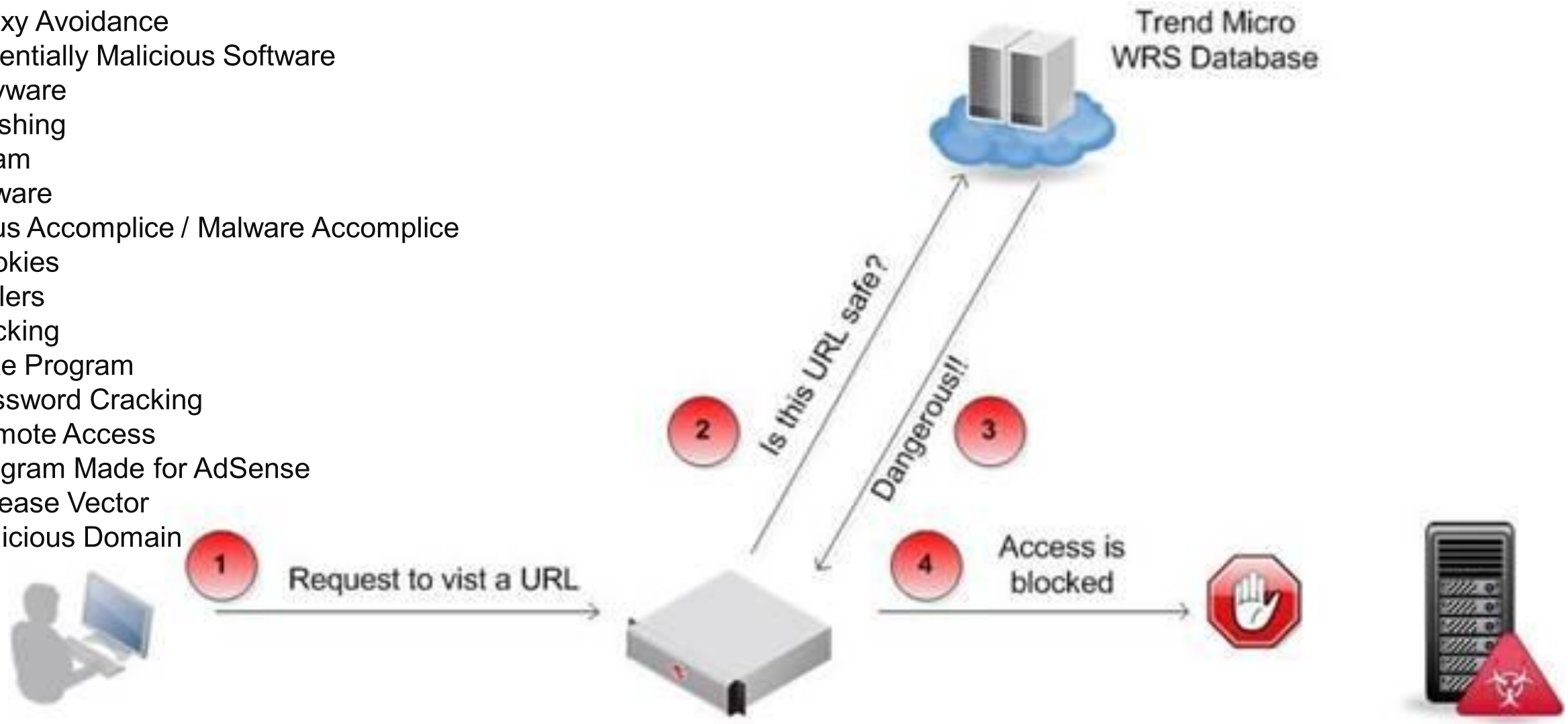
Web Reputation Service



AiProtection

Web Reputation Service

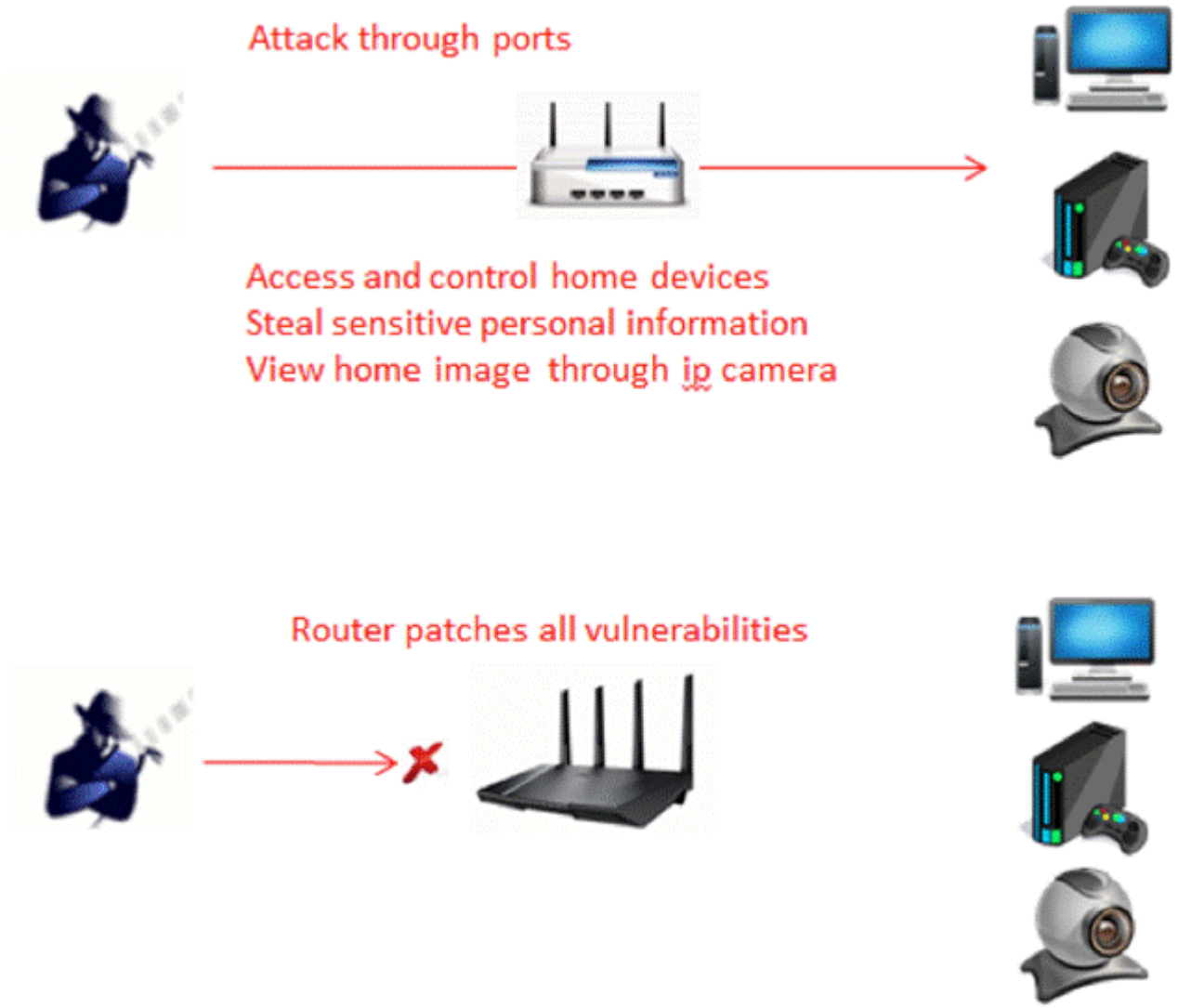
- Proxy Avoidance
- Potentially Malicious Software
- Spyware
- Phishing
- Spam
- Adware
- Virus Accomplice / Malware Accomplice
- Cookies
- Dialers
- Hacking
- Joke Program
- Password Cracking
- Remote Access
- Program Made for AdSense
- Disease Vector
- Malicious Domain



AiProtection

AutoPatching?

- Deep Packet Inspection (DPI)



AiProtection

Devices

- RT-AC5300 – $399.99
- RT-AC88U – $299.99
- RT-AC3100 – $299.99
- RT-AC3200 – $249.99
- RT-AC68P – $199.99
- RT-AC87U – $219.99
- RT-AC68U – $199.99
- RT-AC56U – $109.99

- SweetSecurity ~ $65

Future Work

- Raspberry Pi Model 3?
- Integrations with firewalls
  - External/Third-Party
  - IPTables
- Security Onion
- Kali Linux for Pi
  - https://www.offensive-security.com/kali-linux-arm-images/

Thank You

Travis Smith

tsmith@tripwire.com

Twitter: @mrtrav