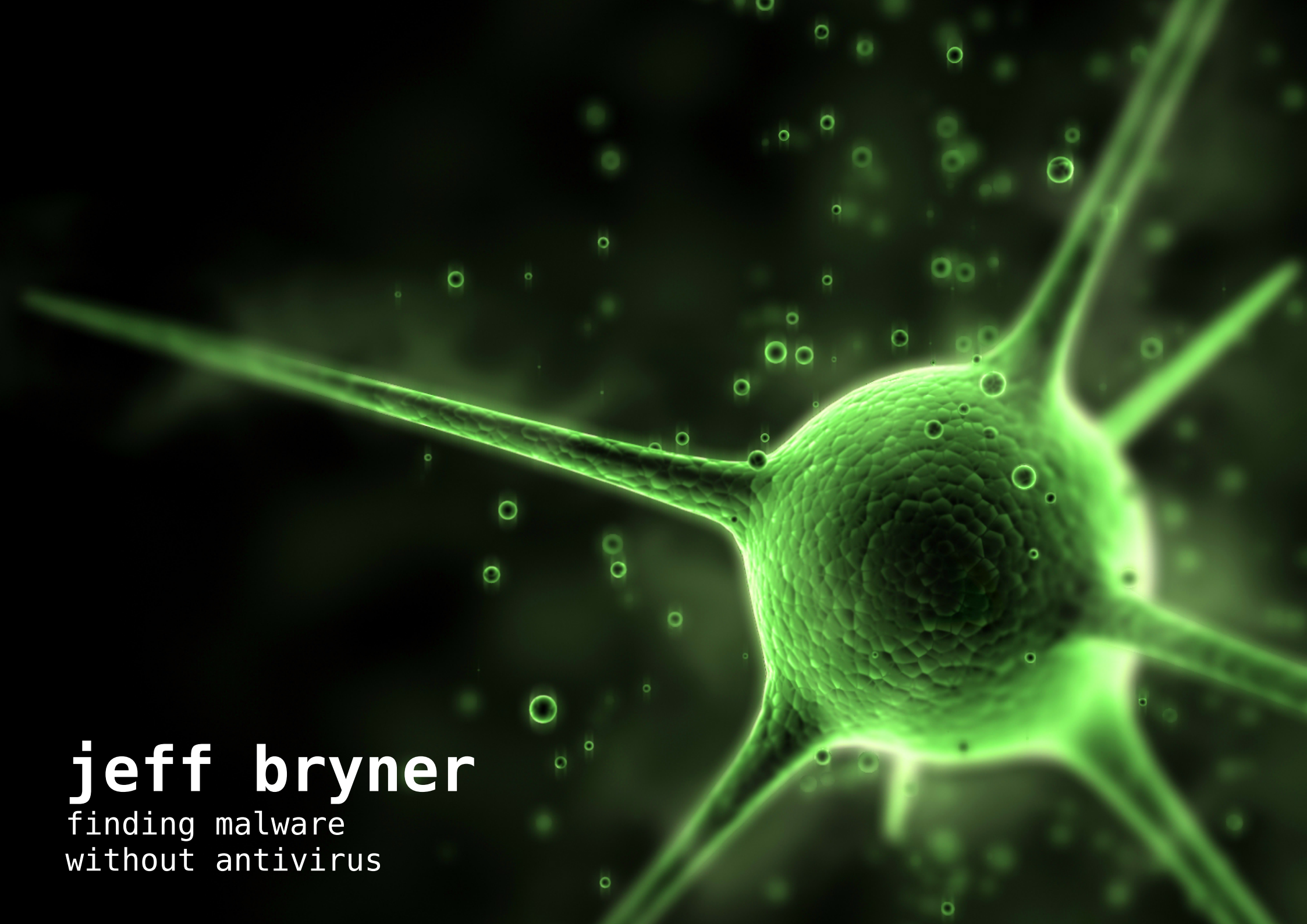
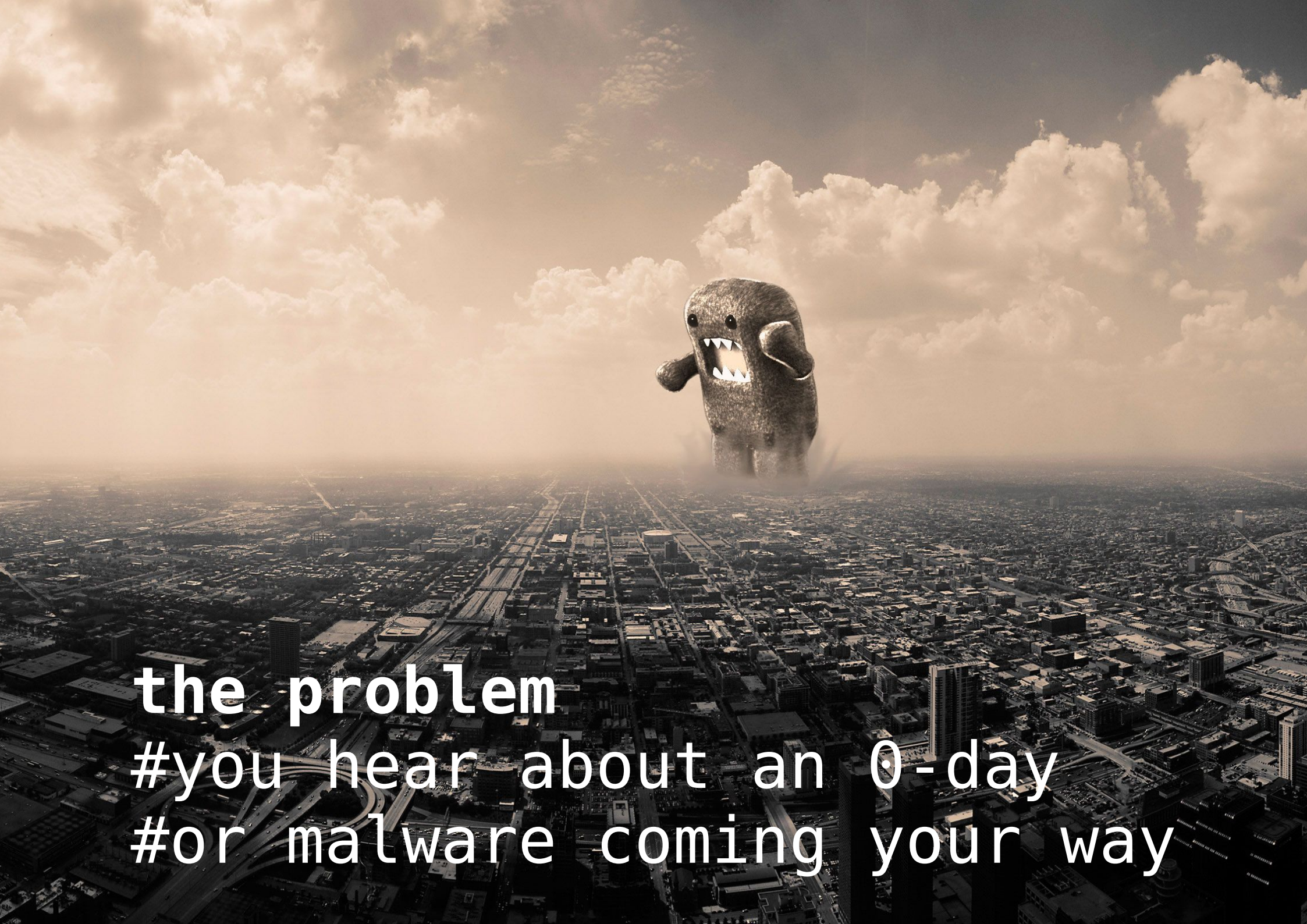
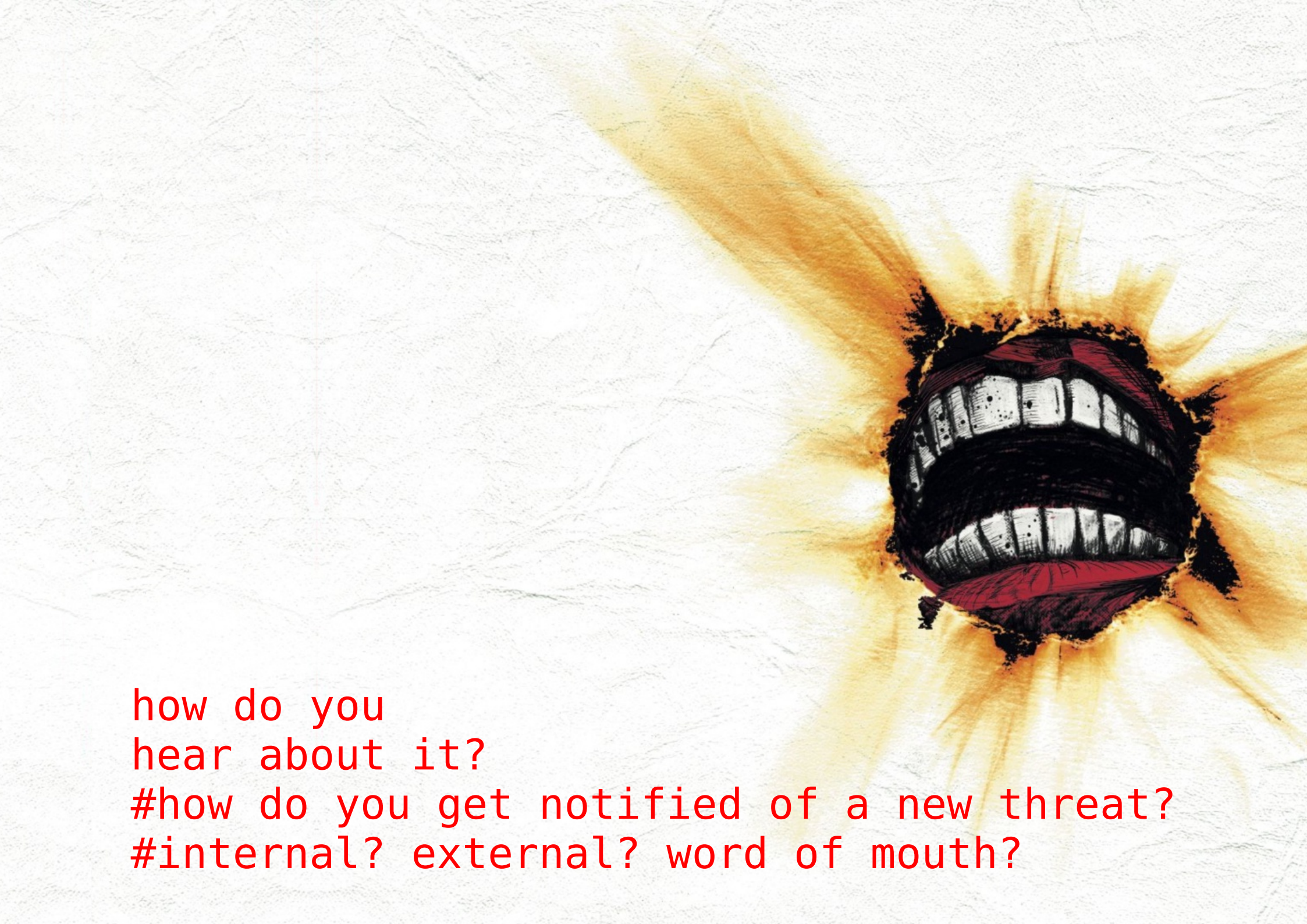


jeff bryner

finding malware
without antivirus


the problem
#you hear about an 0-day
#or malware coming your way

THE *problem?*
#maybe it's already inside your enterprise?



how do you
hear about it?
#how do you get notified of a new threat?
#internal? external? word of mouth?


how do you fight?
#what tools do you have to fight?

safe?
#antivirus doesn't cover the primary phase of IR: identification
#when antivirus fires, you're already in containment
#preparation,identification,containment,eradication,recovery,lessons learned

ClamAV	0.91.2	2007.08.29	-
DrWeb	4.33	2007.08.30	-
eSafe	7.0.15.0	2007.08.29	-
eTrust-Vet	31.1.5095	2007.08.30	-
Ewido	4.0	2007.08.29	-
FileAdvisor	1	2007.08.30	-
Fortinet	3.11.0.0	2007.08.30	Misc/HideVault
F-Prot	4.3.2.48	2007.08.29	W32/FSM.A@dr
F-Secure	6.70.13030.0	2007.08.30	-
Ikarus	T3.1.1.12	2007.08.30	-
Kaspersky	4.0.2.24	2007.08.30	-
McAfee	5108	2007.08.29	potentially unwanted program HideVault
Microsoft	1.2803	2007.08.30	-
NOD32v2	2491	2007.08.30	-
Norman	5.80.02	2007.08.29	-
Panda	9.0.0.4	2007.08.29	-

PLEASE WAIT

#do you panic?

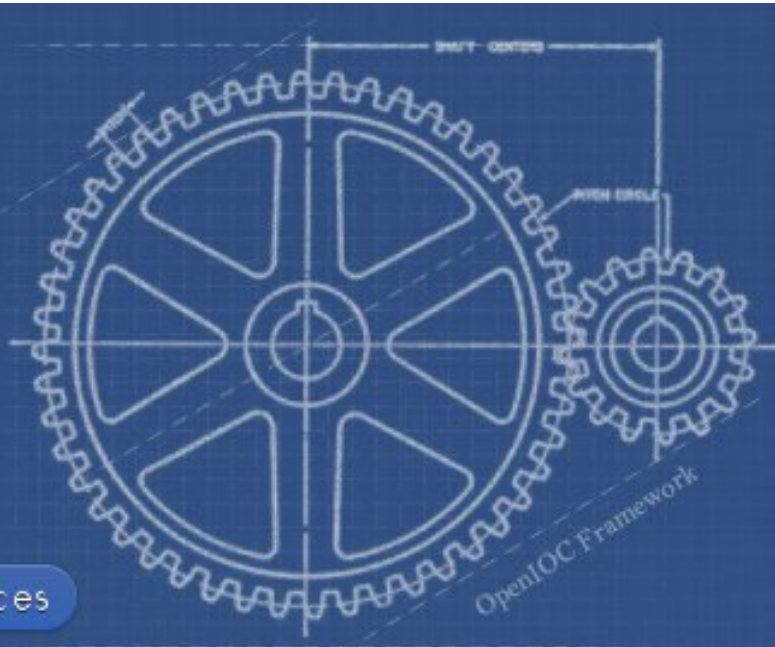

help!
#what if folks want to help and share info?


sharing=hard
#email is too informal, may not reach everyone?
#logs only hold what they were told to log
#pen/paper?
#every security tool has it's own unique format

OpenIOC

An **Open Framework** for **Sharing Threat Intelligence**

Sophisticated Threats Require Sophisticated Indicators



```
<ioc >
  <short_description>firefox running</short_description>
  <description>Is firefox in the list of running processes</description>
  <authored_by>jab</authored_by>
  <authored_date>2012-08-14T21:46:51</authored_date>
  <links />
  <definition>
    <Indicator operator="OR">
      <IndicatorItem condition="contains">
        <Context document="ProcessItem" search="ProcessItem/name" />
        <Content type="string">firefox</Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
#ioc is just xml
```


```
xml + malware=two problems?
#I know..now we have two problems: a compromise and an xml format.
#       IOC format is a reasonable approach, but not many tools support it.
#       IOC too complex to do by hand (see flame.ioc)
#       IOC collection and analysis toolset is limited:
```

```
<ioc >
  <short_description>firefox running</short_description>
  <description>Is firefox in the list of running processes</description>
  <authored_by>jab</authored_by>
  <authored_date>2012-08-14T21:46:51</authored_date>
  <links />
  <definition>
    <Indicator operator="OR">
      <IndicatorItem condition="contains">
        <Context document="ProcessItem" search="ProcessItem/name" />
        <Content type="string">firefox</Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
#sample ioc to see if firefox is running..could be svch0st.exe, etc.
```

```
automation advantages:
Flame filename IOCs:
                FileItem/FileName is ~a28.tmp or
                FileItem/FileName is ~DFL542.tmp or
                FileItem/FileName is ~DFL543.tmp or
                FileItem/FileName is ~DFL544.tmp or
                FileItem/FileName is ~DFL545.tmp or
                FileItem/FileName is ~DFL546.tmp or
                FileItem/FileName is ~dra51.tmp or
                FileItem/FileName is ~dra52.tmp or
                FileItem/FileName is ~fghz.tmp or
                FileItem/FileName is ~rei524.tmp or
                FileItem/FileName is ~rei525.tmp or
                FileItem/FileName is ~TFL848.tmp or
                FileItem/FileName is ~TFL842.tmp or
                FileItem/FileName is GRb2M2.bat or
                FileItem/FileName is indsvc32.ocx or
                FileItem/FileName is scaud32.exe or
                FileItem/FileName is scsec32.exe or
                FileItem/FileName is sdclt32.exe or
                FileItem/FileName is sstab.dat or
                FileItem/FileName is sstab15.dat or
                FileItem/FileName is winrt32.dll or
                FileItem/FileName is winrt32.ocx or
                FileItem/FileName is wpab32.bat or
                FileItem/FileName is commgr32.dll or
                FileItem/FileName is comspol32.dll or
                FileItem/FileName is comspol32.ocx or...
73 different filenames!
125 different IOC items total!
#malware is way beyond the point where we can hope to discover it
#by just poking around a system
```

IOC collection and analysis toolset is limited:

IOCFinder,IOCEditor are free but:
- Windows only, no unix/linux/mac
- time consuming
  - (45 mins to collect data on a win2k8r2 vanilla install)
- manual process:
  - run iocfinder
  - collect xml data (lots)
  - process iocs on data

#OK, if it's so great why aren't we using it
#existing IOC tools have some gaps

No support for IOCs in common agents:

- BigFix
- ncircle
- tripwire
- SCCM
- nessus
- ...

#you probably have one of these agents
#in addition to AV running on your hosts
#no love for IOCs...

open source to the rescue?
#maybe we can ease the burden with some open source tools?

What if we could create
a system for centrally
issuing indicators
of compromise?

What if hosts we suspect
as being compromised
used this system
to check themselves
for compromise?

Lets find out...


python

Copy

Paste

zero-install; copy and paste a single .exe
#simple zero-install python client
#compiled to native executable on linux/windows. 32 and 64bit.


simple server for issuing IOCs
in realtime
#simple python server to dish out IOCs and receive results


demos

simple IOC client/server examples

small server

```
$ wc -l pyiocServer.py
141 pyiocServer.py
```

small-ish client

```
$ wc -l *.py */*.py
  249 pyiocClient.py
  118 iocItems/FileItem.py
   47 iocItems/PortItem.py
   82 iocItems/ProcessItem.py
   77 iocItems/RegistryItem.py
    0 iocItems/__init__.py
    0 lib/__init__.py
   55 lib/log.py
   18 lib/settings.py
   37 lib/util.py
  683 total
#client is fairly small with support for
#common
files, processes and registry IOCs.
```

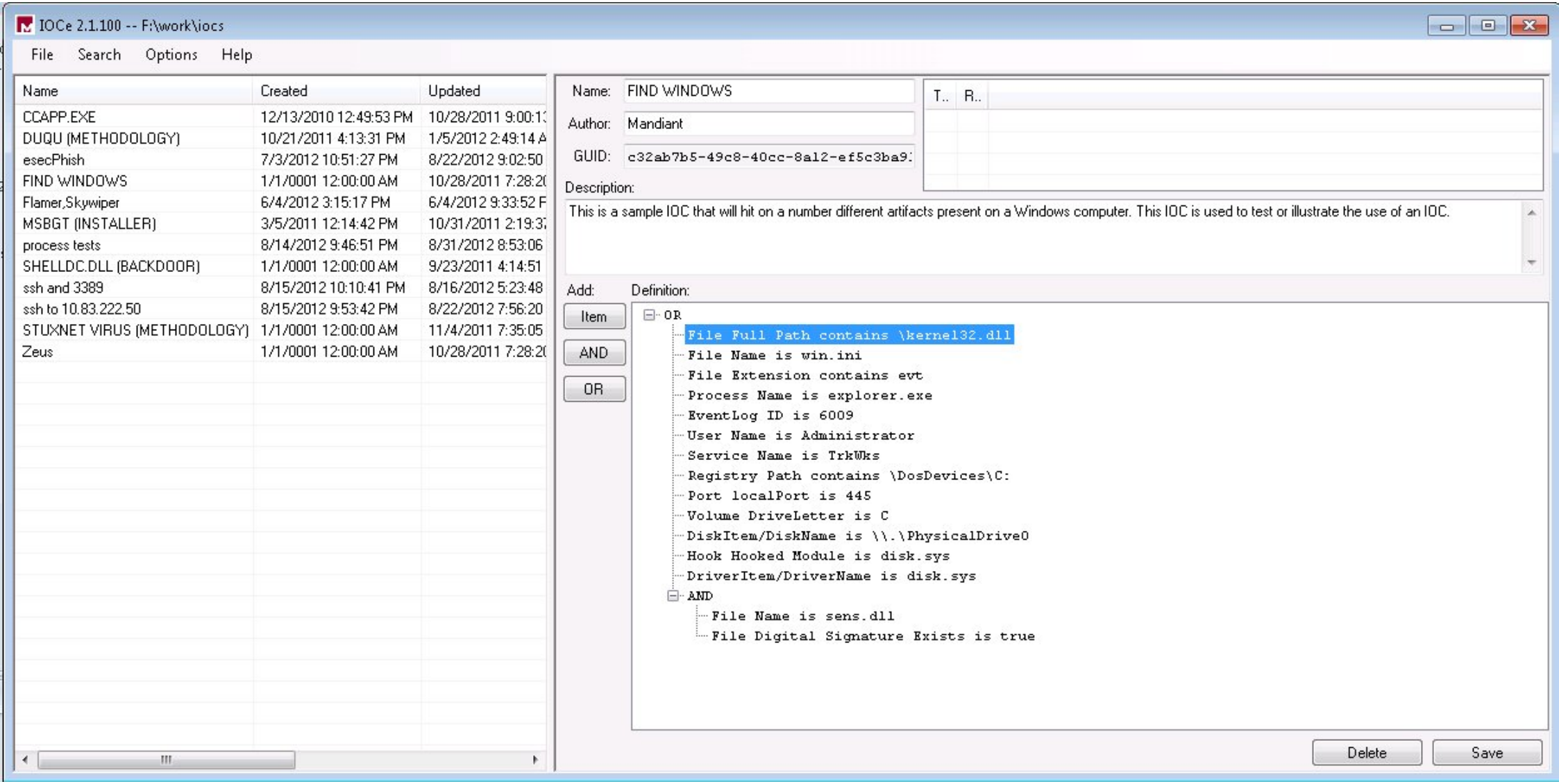
```
server folder structure:
$ find iocs/
iocs/
iocs/172.16.0.0-16
iocs/172.18.6.0-24
iocs/172.18.6.0-24/pybackdoor.ioc
iocs/10.83-16
iocs/10.83-16/sshto10.83.222.50.ioc
iocs/10.83-16/windows.ioc
iocs/10.83-16/duqu.ioc
iocs/172.21-16
iocs/172.21-16/firefox.ioc
iocs/10.200-16
iocs/10.200-16/firefox.ioc
iocs/10.200-16/windows.ioc
iocs/10.200-16/duqu.ioc
#uses netblock cidr masks as folders to determine
#what iocs to send to what clients
```

simple ioc detection demo

windows.ioc

firefox.ioc

```
our malware
#what good is a malware finding tool without malware? Lets create some
#create python back-door
```


IOCe 2.1.100 -- F:\work\iocs
File
Search
Options
Help
Name
Created
Updated
CCAPP.EXE
12/13/2010 12:49:53 PM
DUQU (METHODOLOGY)
10/21/2011 4:13:31 PM
1/5/2012 2:49:14 A
esecPhish
7/3/2012 10:51:27 PM
8/22/2012 9:02:50
FIND WINDOWS
1/1/0001 12:00:00 AM
Flamer,Skywiper
6/4/2012 3:15:17 PM
6/4/2012 9:33:52 F
MSBGT (INSTALLER)
3/5/2011 12:14:42 PM
process tests
8/14/2012 9:46:51 PM
8/31/2012 8:53:06
SHELLDC.DLL (BACKDOOR)
1/1/0001 12:00:00 AM
9/23/2011 4:14:51
ssh and 3389
8/15/2012 10:10:41 PM
8/16/2012 5:23:48
ssh to 10.83.222.50
8/15/2012 9:53:42 PM
8/22/2012 7:56:20
STUXNET VIRUS (METHODOLOGY)
1/1/0001 12:00:00 AM
11/4/2011 7:35:05
Zeus
1/1/0001 12:00:00 AM
10/28/2011 7:28:2
Name:
FIND WINDOWS
Author:
Mandiant
GUID:
c32ab7b5-49c8-40cc-8a12-ef5c3ba9
T..
R..
Description:
This is a sample IOC that will hit on a number different artifacts present on a Windows computer. This IOC is used to test or illustrate the use of an IOC.
Add:
Item
AND
OR
Definition:
OR
File Full Path contains \kernel32.dll
File Name is win.ini
File Extension contains evt
Process Name is explorer.exe
EventLog ID is 6009
User Name is Administrator
Service Name is TrkWks
Registry Path contains \DosDevices\C:
Port localPort is 445
Volume DriveLetter is C
DiskItem/DiskName is \\.\PhysicalDrive0
Hook Hooked Module is disk.sys
DriverItem/DriverName is disk.sys
AND
File Name is sens.dll
File Digital Signature Exists is true
Delete
Save

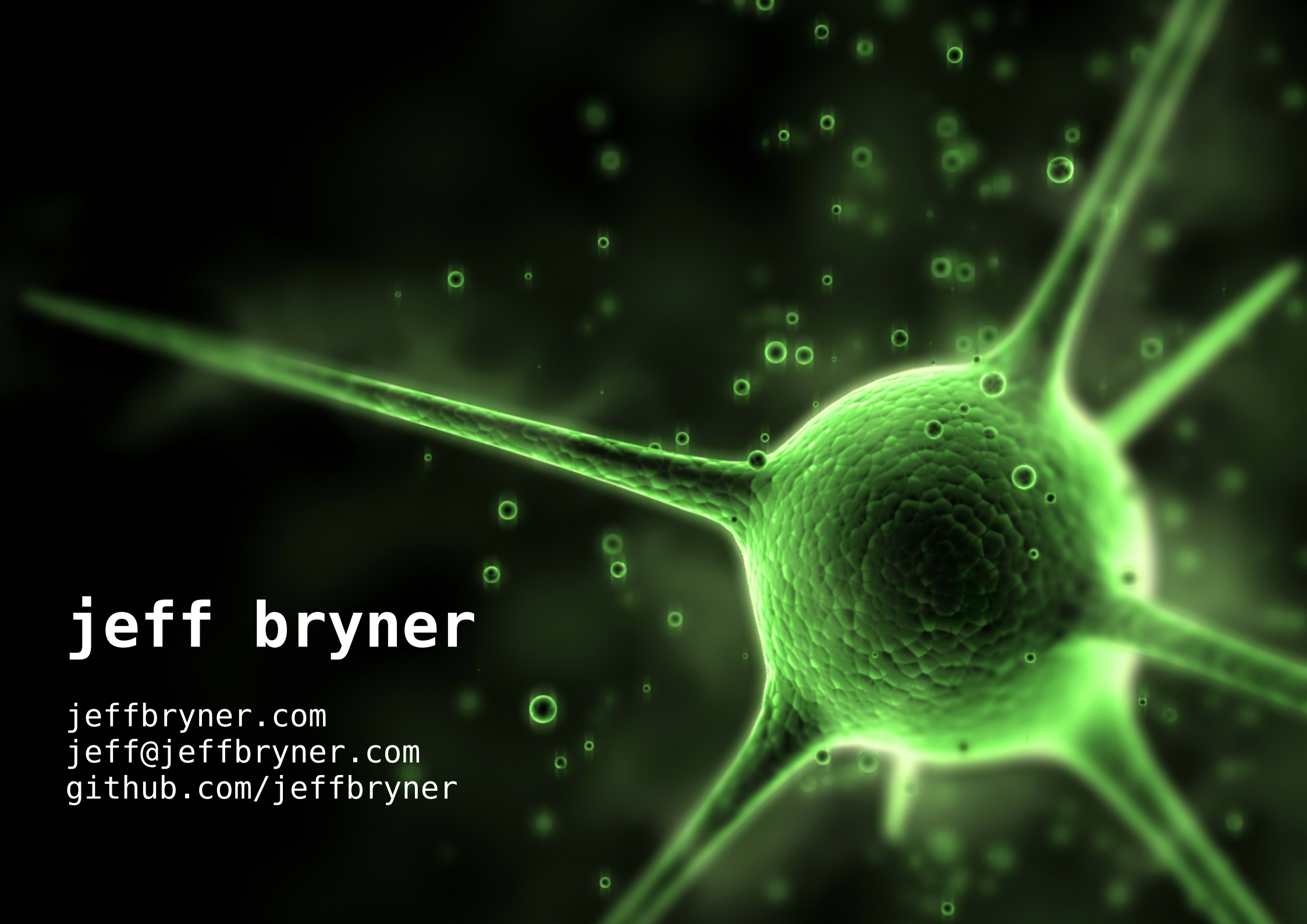
ioc distribution via the ioc server
#CIDR mask directory names to control what IOCs go to what servers

ioc client push
#simple xcopy installation
#wmiFileTransfer demo

```
ioc client run
#run once or run via at job for recurring checks.
```

next steps:

- Publish: github.com/jeffbryner
- Is it useful?
- Will it be used?
- What's missing?
- Vendor support in their tools?



jeff bryner

jeffbryner.com
jeff@jeffbryner.com
github.com/jeffbryner