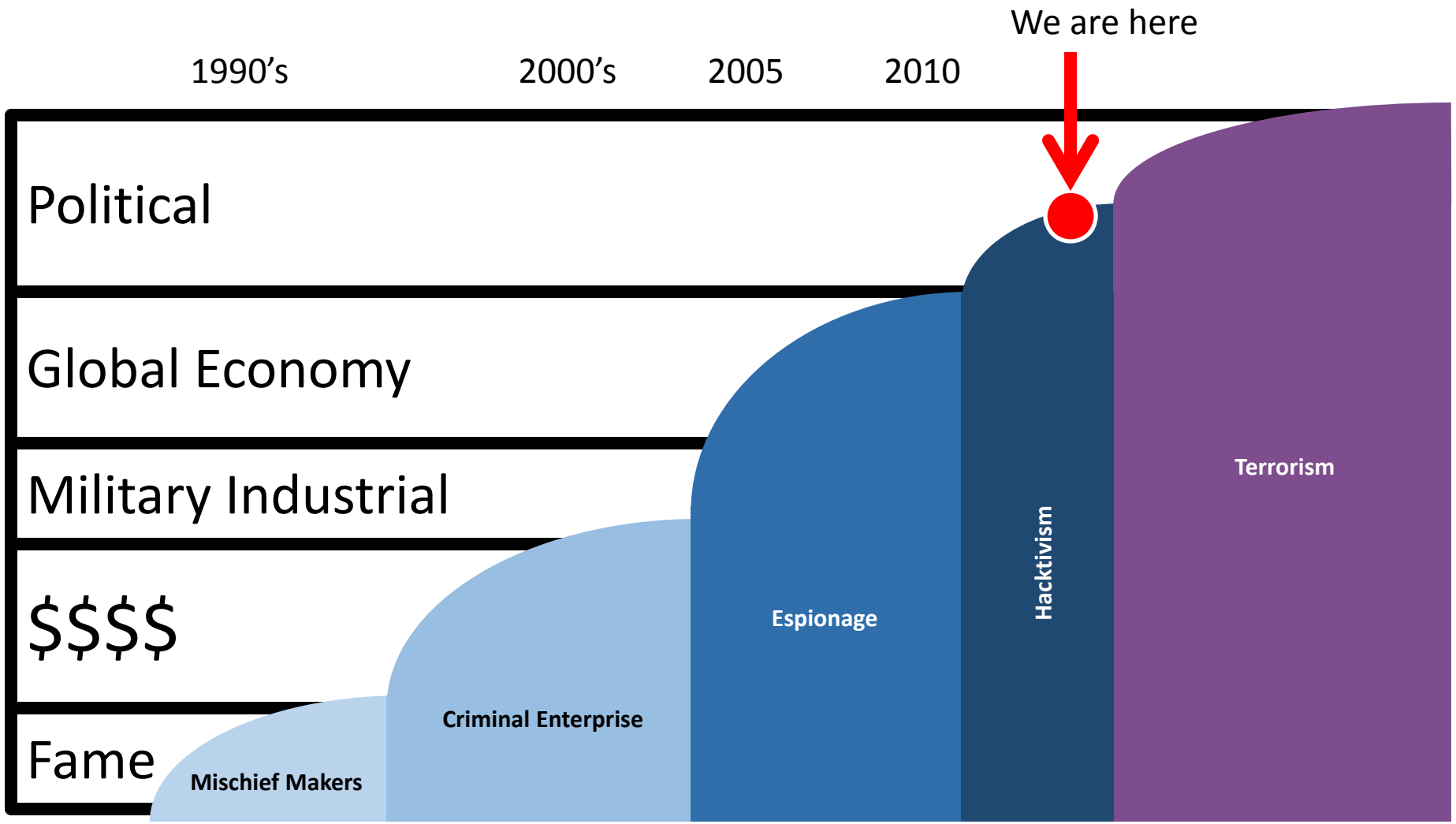
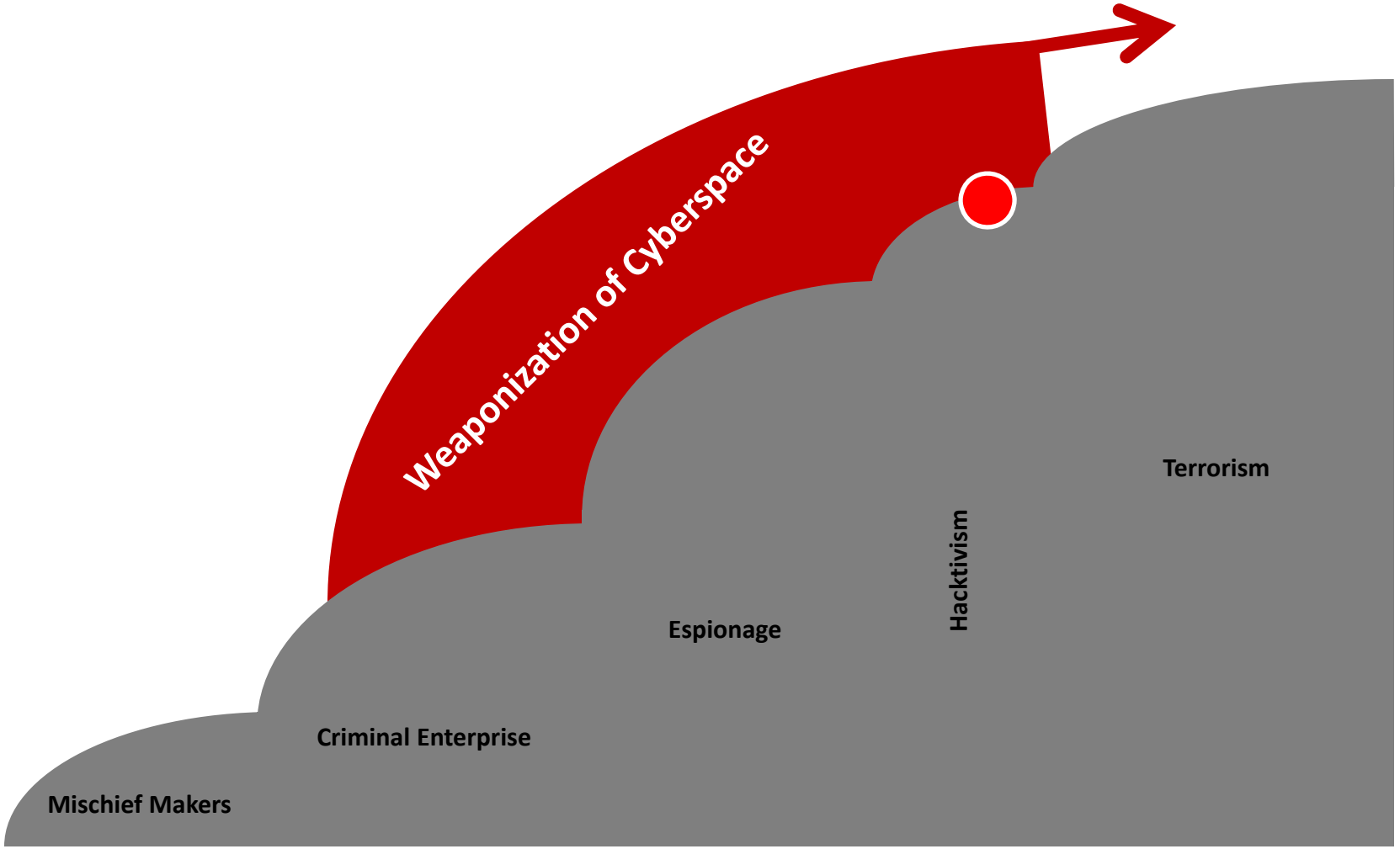
Modern Cyberthreats: The Changing Face Behind the Keyboard

Greg Hoglund
HBGary, Inc.

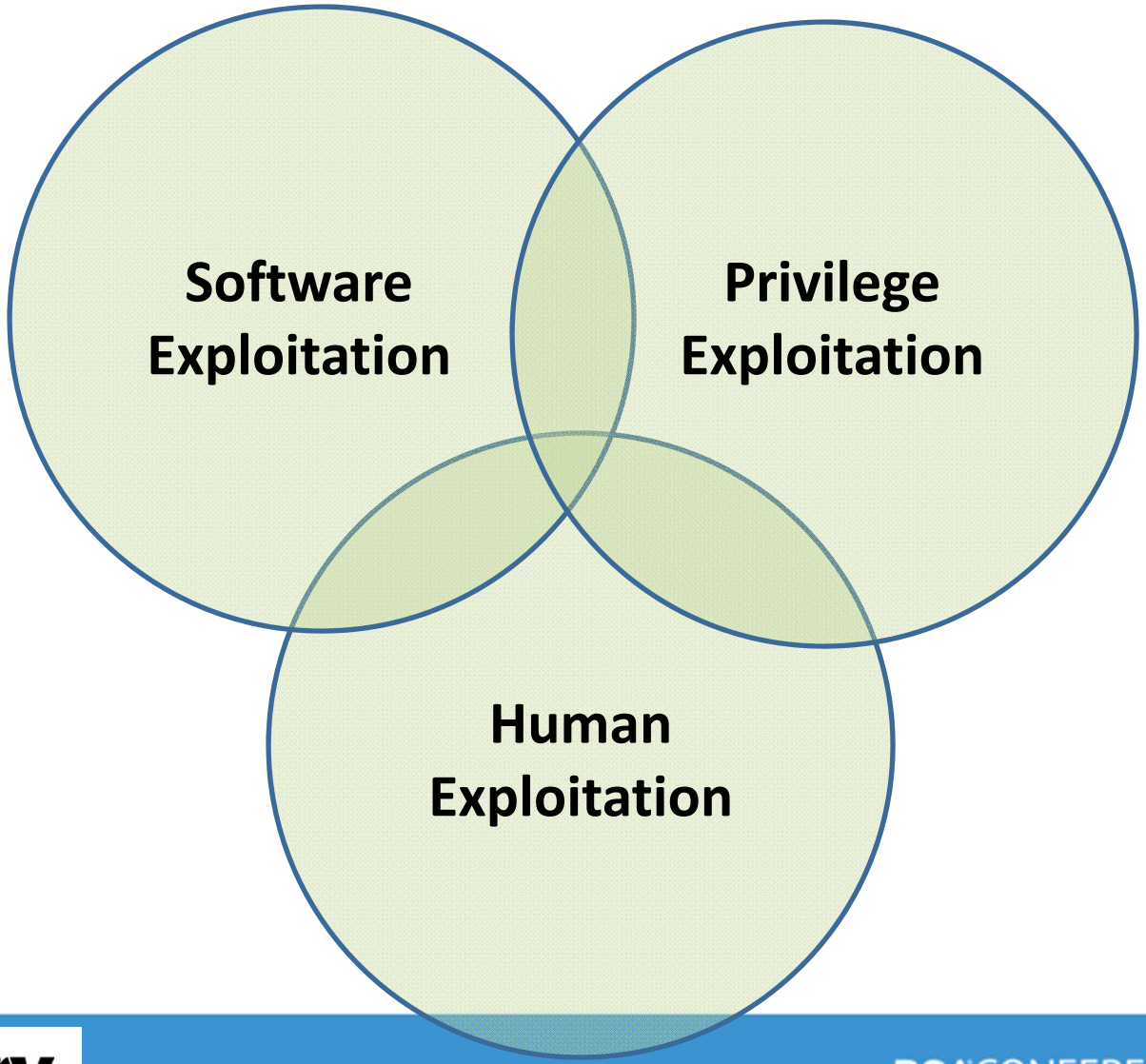
Session ID: EXP-202
Session Classification: Intermediate


We are here
1990's
2000's
2005
2010
Political
Global Economy
Military Industrial
$$$$
Fame
Mischief Makers
Criminal Enterprise
Espionage
Hacktivism
Terrorism


Weaponization of Cyberspace
Terrorism
Hacktivism
Espionage
Criminal Enterprise
Mischief Makers

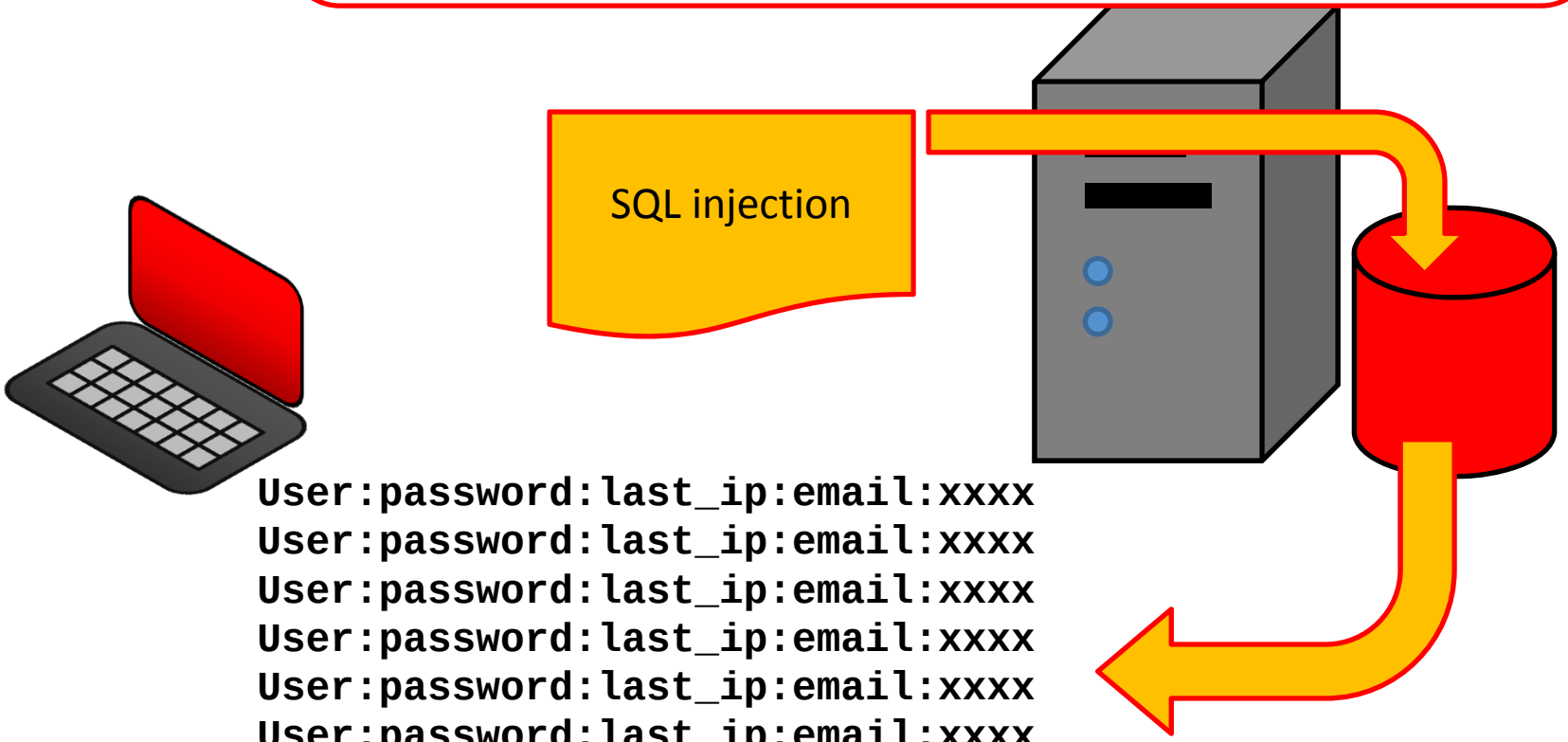

Eleonore Exp
Sql Poizon v1.1 - Sqli Exploit Scanner Tool (By: p0!z0neR)
Search Hunter
Sqli Crawler
Injection Builder
Browser
About
FRAGUS
Low Orbit Ion Cannon
CRUM Cryptor Polymorphic v. 2.6 new!
GeckoCode
TRiAD HTTP Control System
[Set Command] [Statistics Table] [Help]
[Set Command for Machines:]
Bot IP ("all" - to all bots)
all
(yes we are black hat friendly!)
Our Price:
UK, CH $175
DE, AT, ES $160
DK, NO, SE $155
BE, FR, IT $150
CA, USA $130
BR, AR $60
Mix w/o asia $30
Mix $20
Asia $10
Euromix $130
Installs Dealer.com
Support #1: ICQ 556752679 Support #2: ICQ 590674786 Support #3:
EARNING 4 U .com
ENTER STATS
REGISTER TODAY
PoisonIvy Polymorphic Online Builder
YA!BUCKS
LIKE MONEY?
WORK WITH US!
Poison Ivy
Remote Administration Tool

How do they get in?



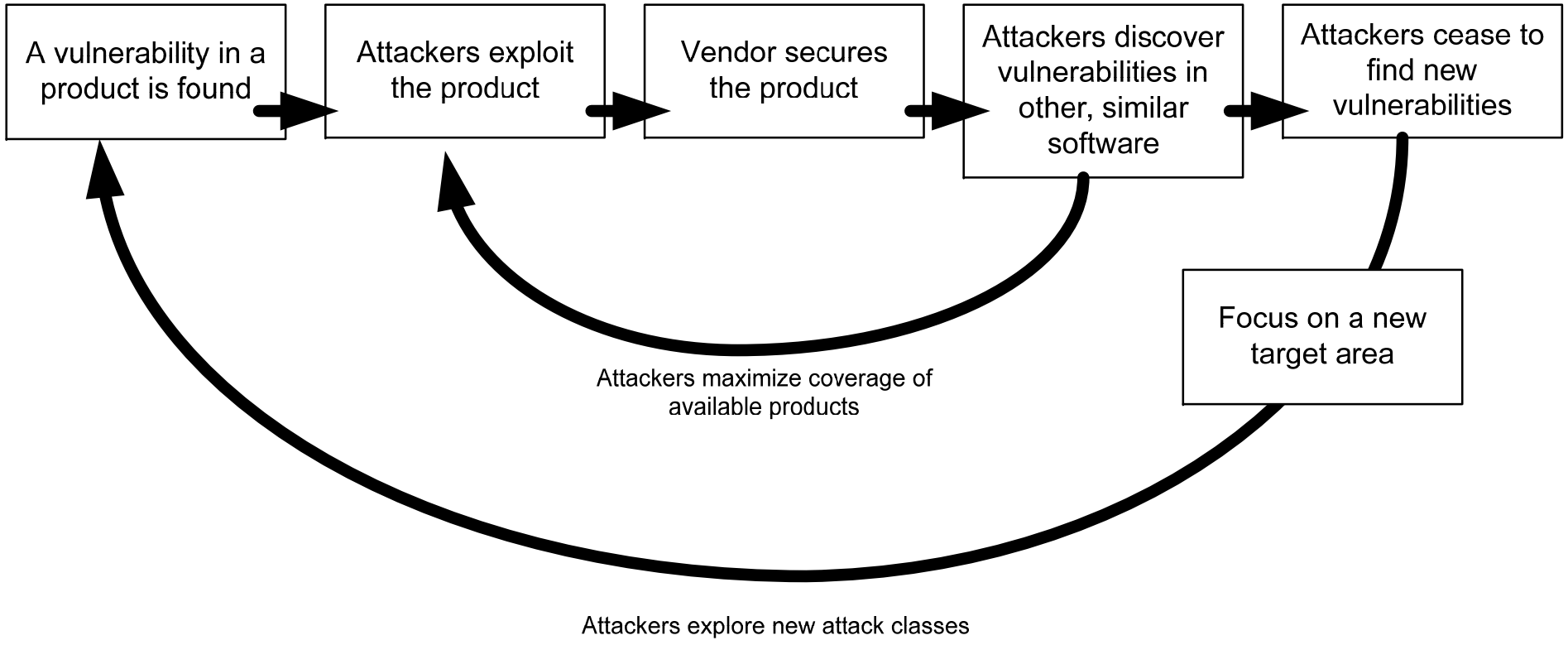
SQL Injection

www.somesite.com/somepage.php?id=1 UNION SELECT 1,2,3…

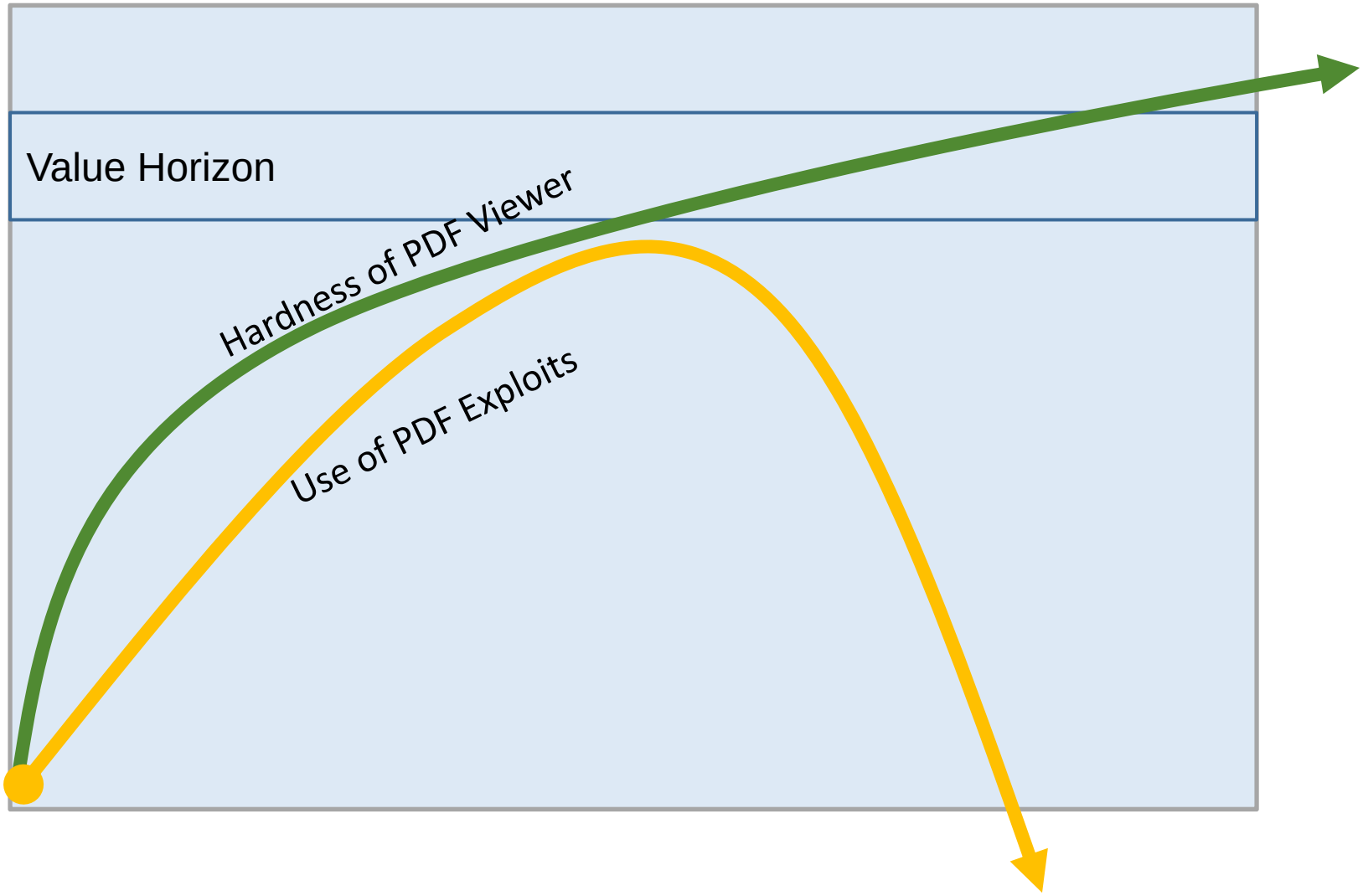



```
User:password:last_ip:email:xxxx
User:password:last_ip:email:xxxx
User:password:last_ip:email:xxxx
User:password:last_ip:email:xxxx
User:password:last_ip:email:xxxx
User:password:last_ip:email:xxxx
```

Attack Evolution Cycle

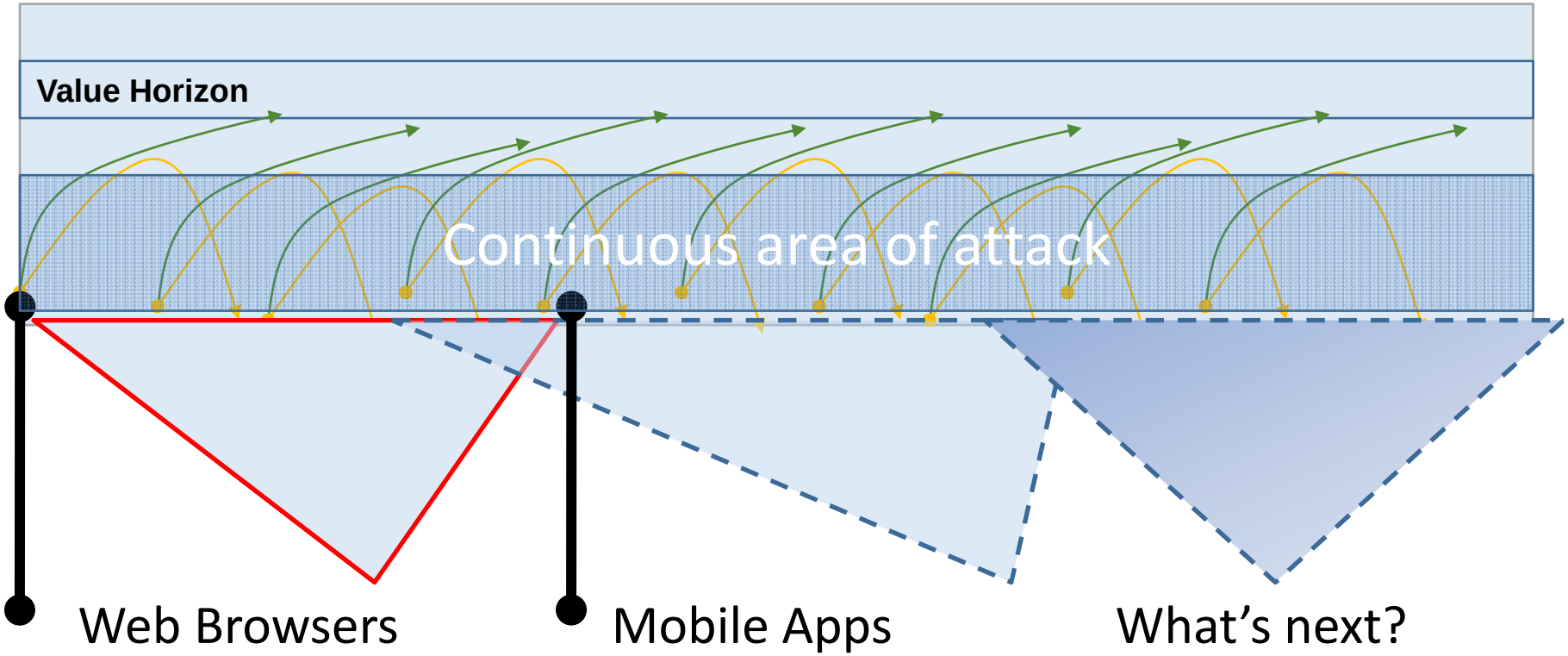


Value Horizon



Continuous Area of Attack

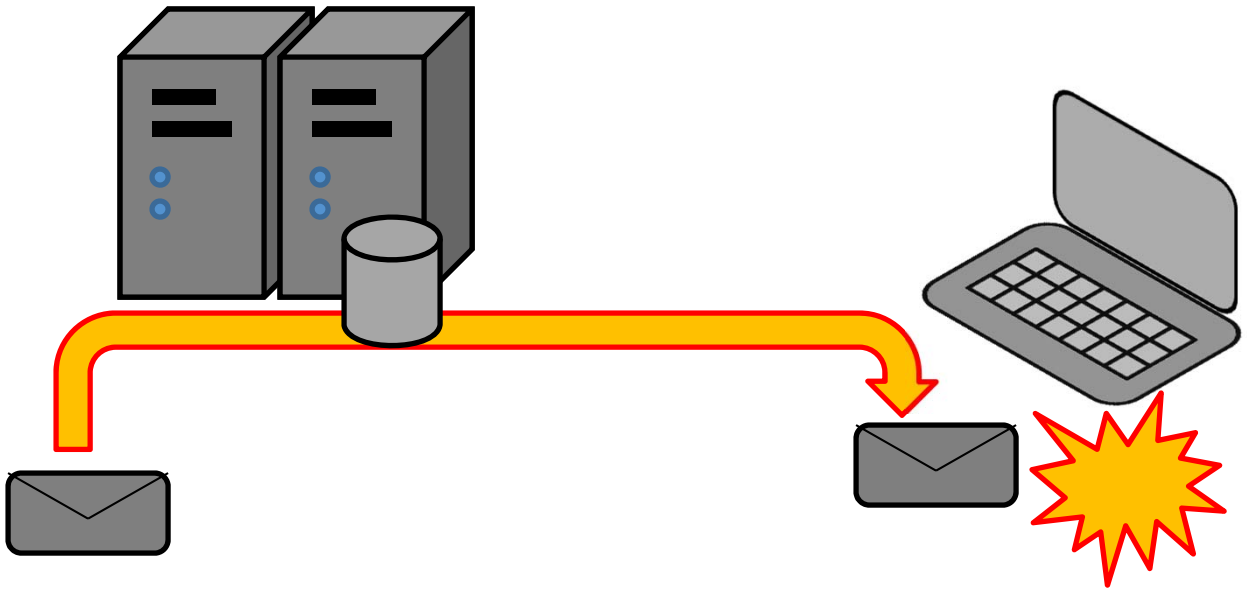
By the time all the surfaces in a given technology are hardened, the technology is obsolete



Security is a human problem

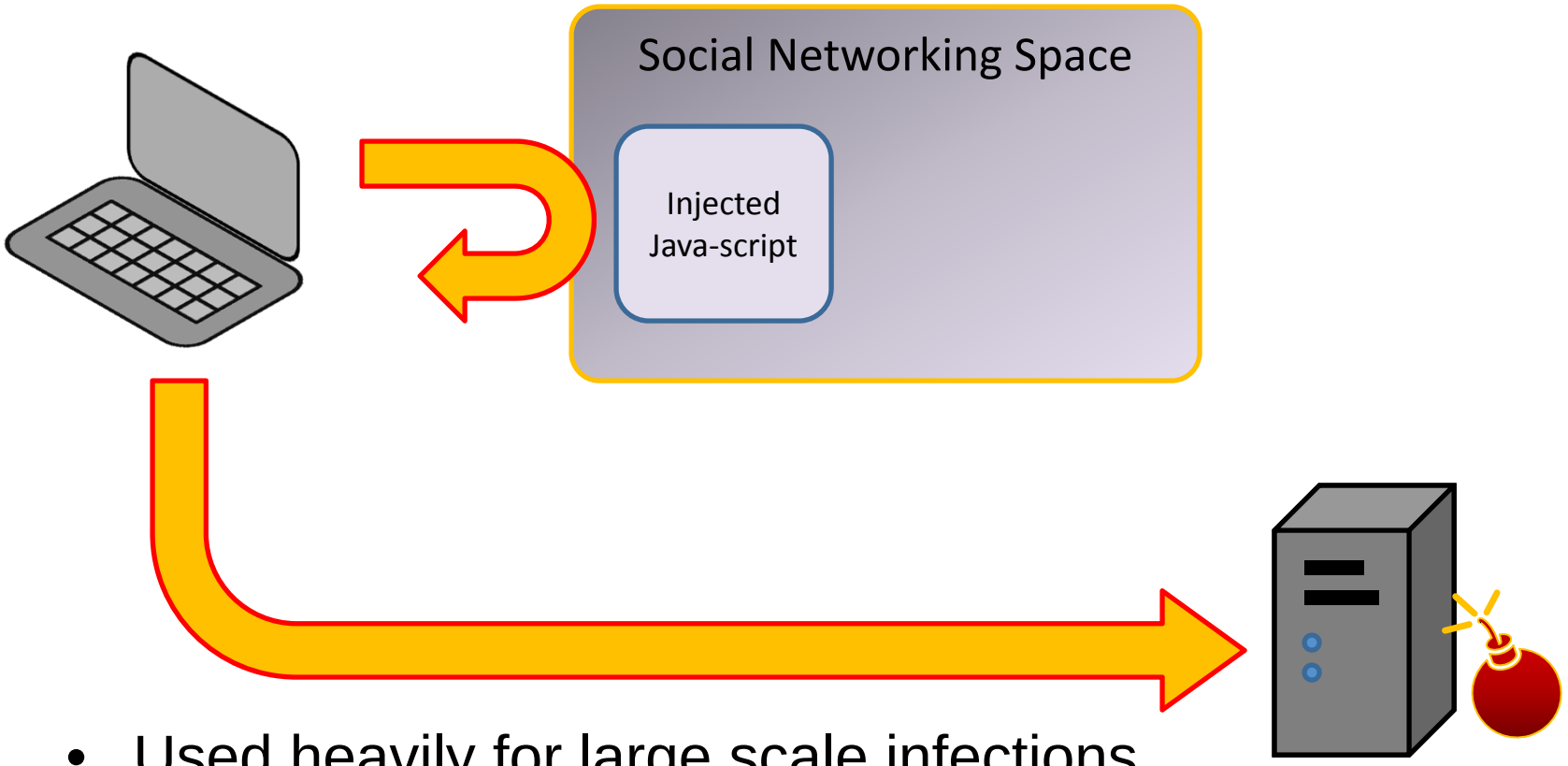
bit.ly ? You can't even tell what you are clicking on…

Boobytrapped Documents



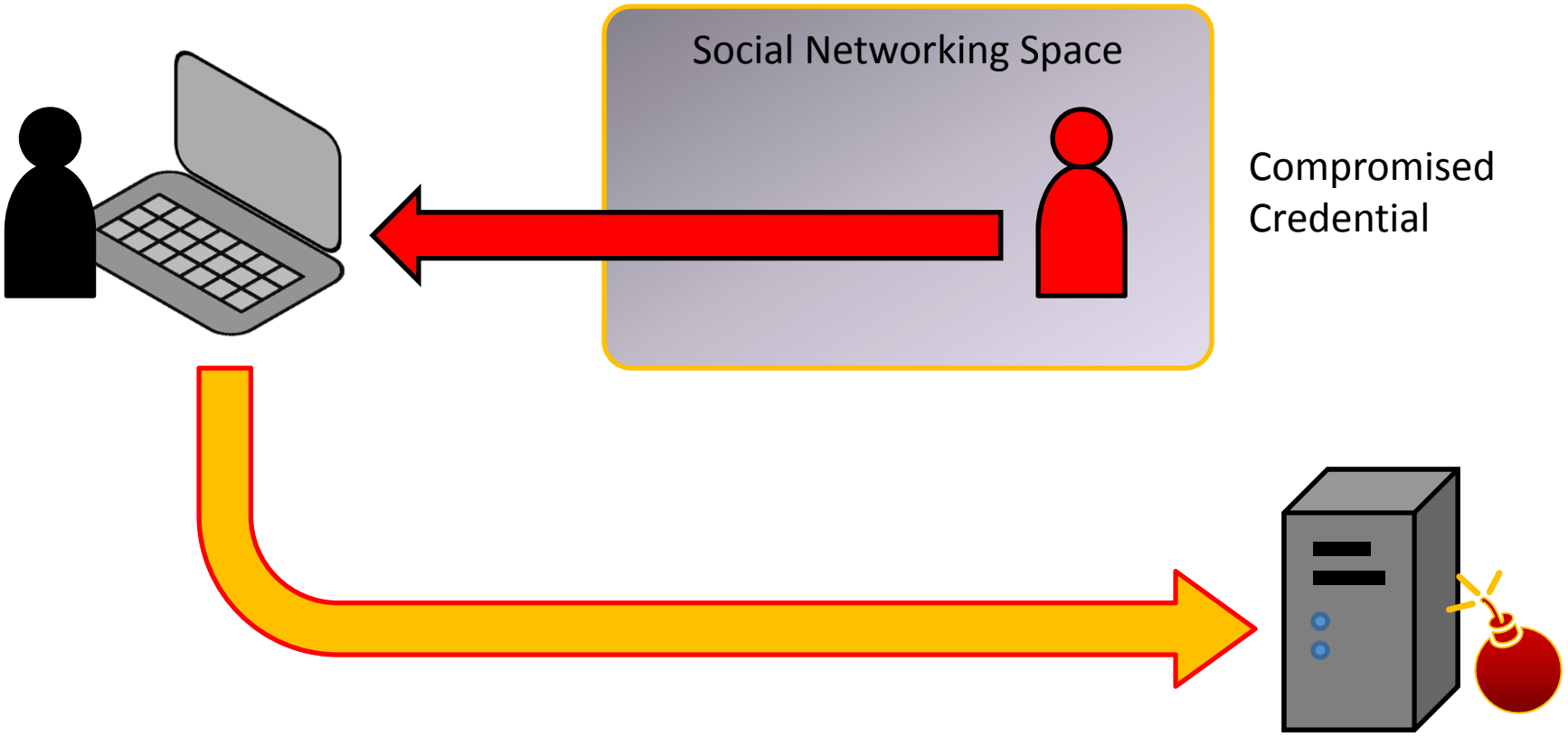
- Single most effective *focused* attack today
- Human crafts text

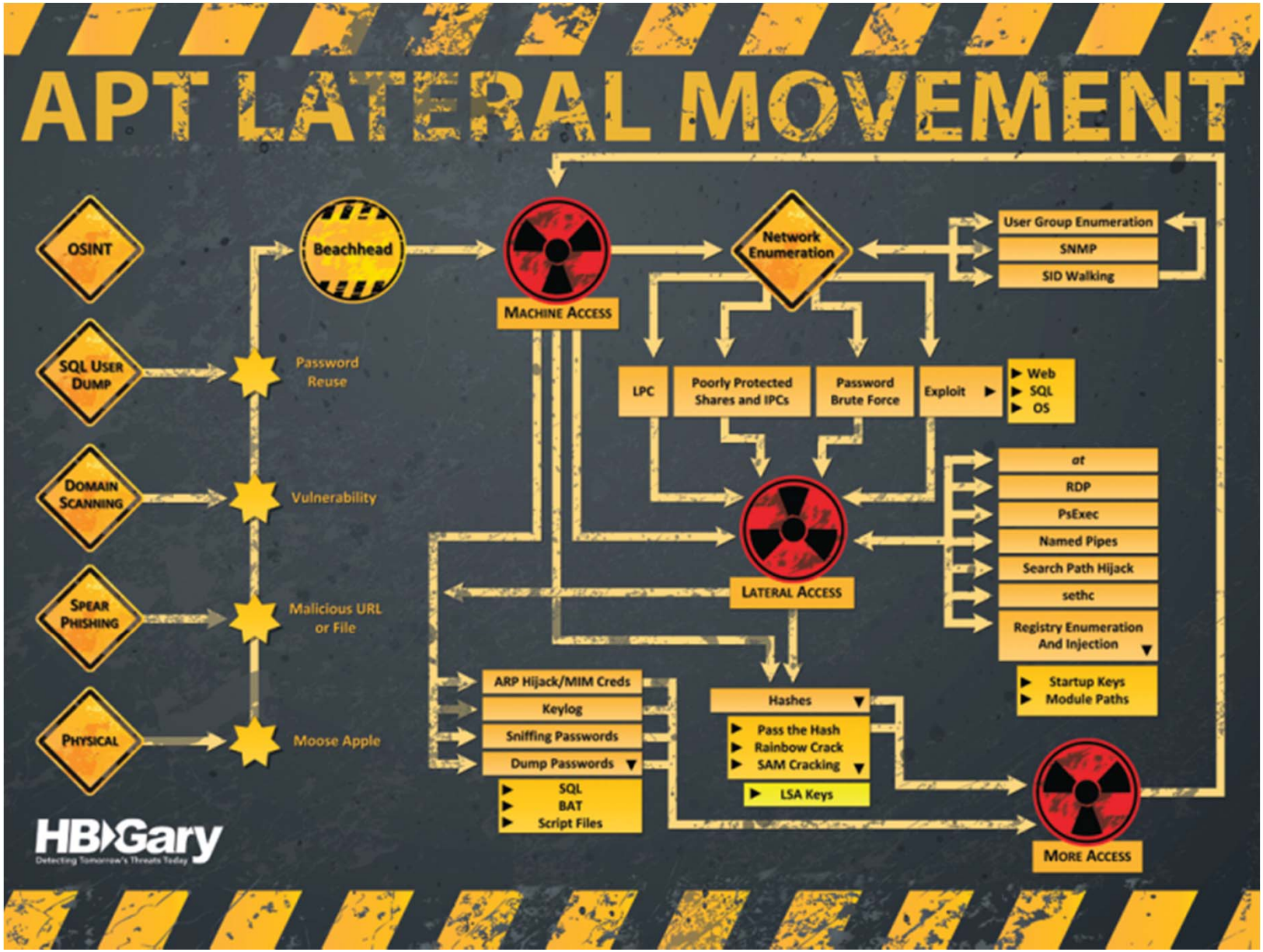
Social Networking Attack (I)



- Used heavily for large scale infections
- Social network targeting is possible

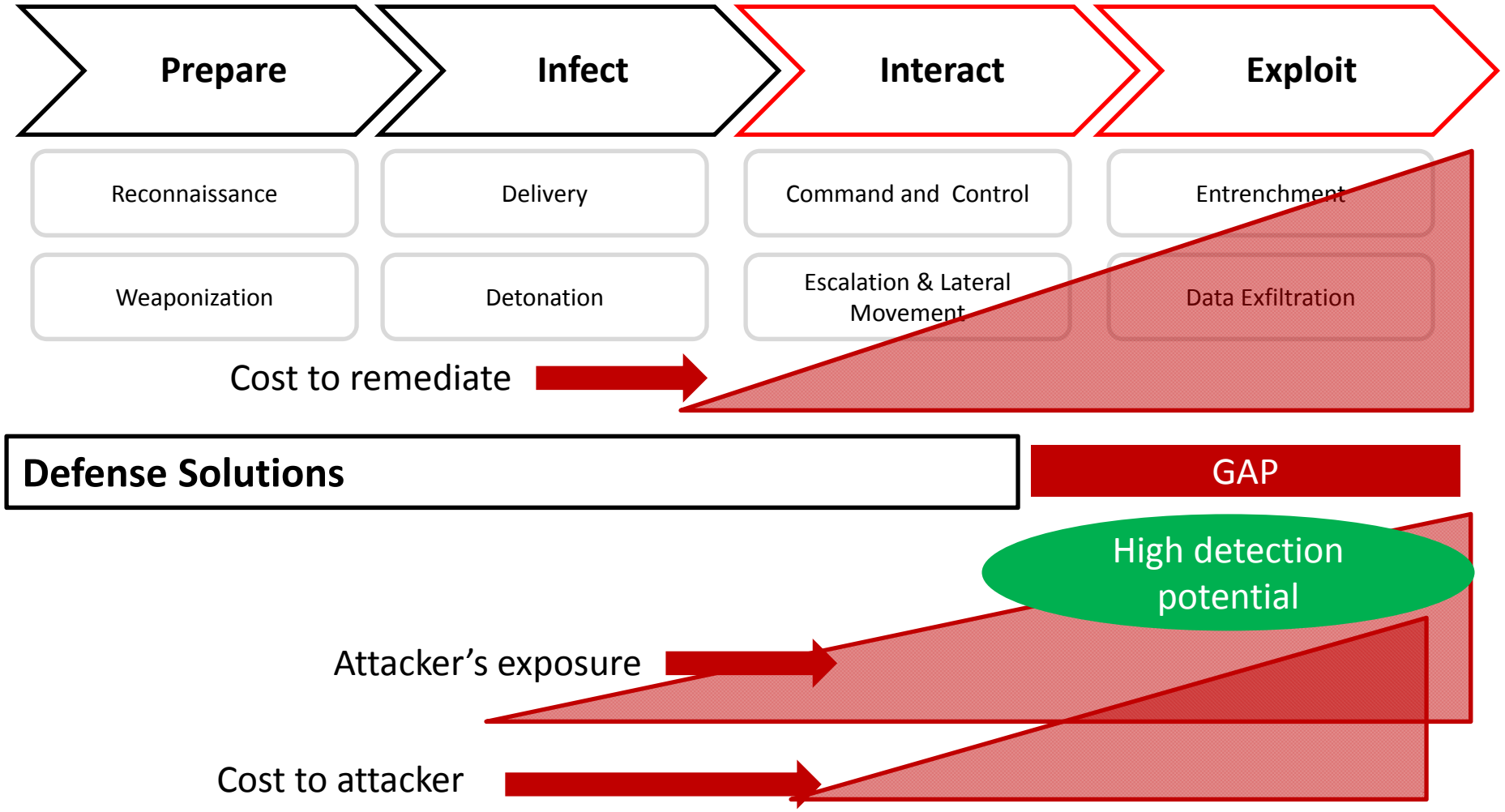
Social Network Attack (II)



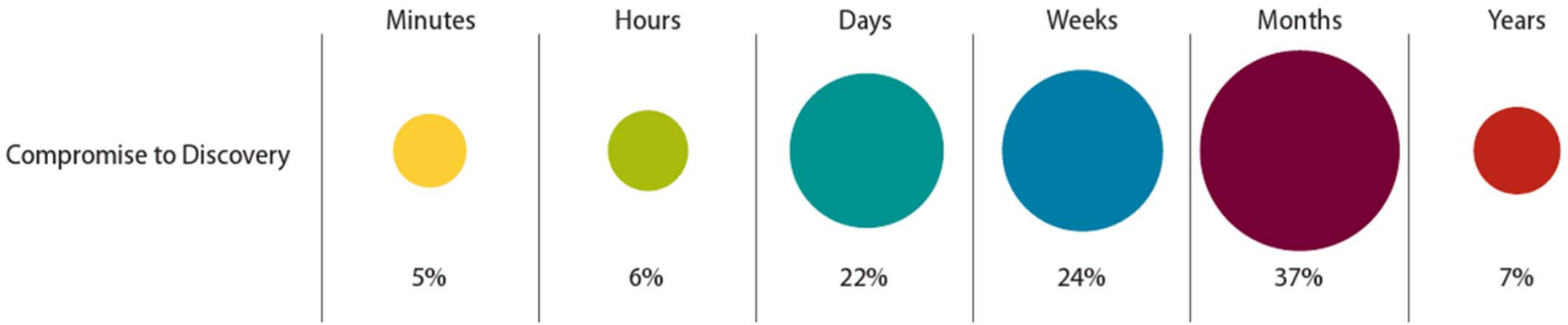

APT LATERAL MOVEMENT
OSINT
SQL User Dump
Domain Scanning
Spear Phishing
Physical
Beachhead
Password Reuse
Vulnerability
Malicious URL or File
Moose Apple
Machine Access
Network Enumeration
User Group Enumeration
SNMP
SID Walking
LPC
Poorly Protected Shares and IPCs
Password Brute Force
Exploit
Web
SQL
OS
Lateral Access
at
RDP
PsExec
Named Pipes
Search Path Hijack
sethc
Registry Enumeration And Injection
Startup Keys
Module Paths
ARP Hijack/MIM Creds
Keylog
Sniffing Passwords
Dump Passwords
SQL
BAT
Script Files
Hashes
Pass the Hash
Rainbow Crack
SAM Cracking
LSA Keys
More Access
HBGary
Detecting Tomorrow's Threats Today

Resiliency post intrusion

APT Attack Progression



Internal Network Exploitation

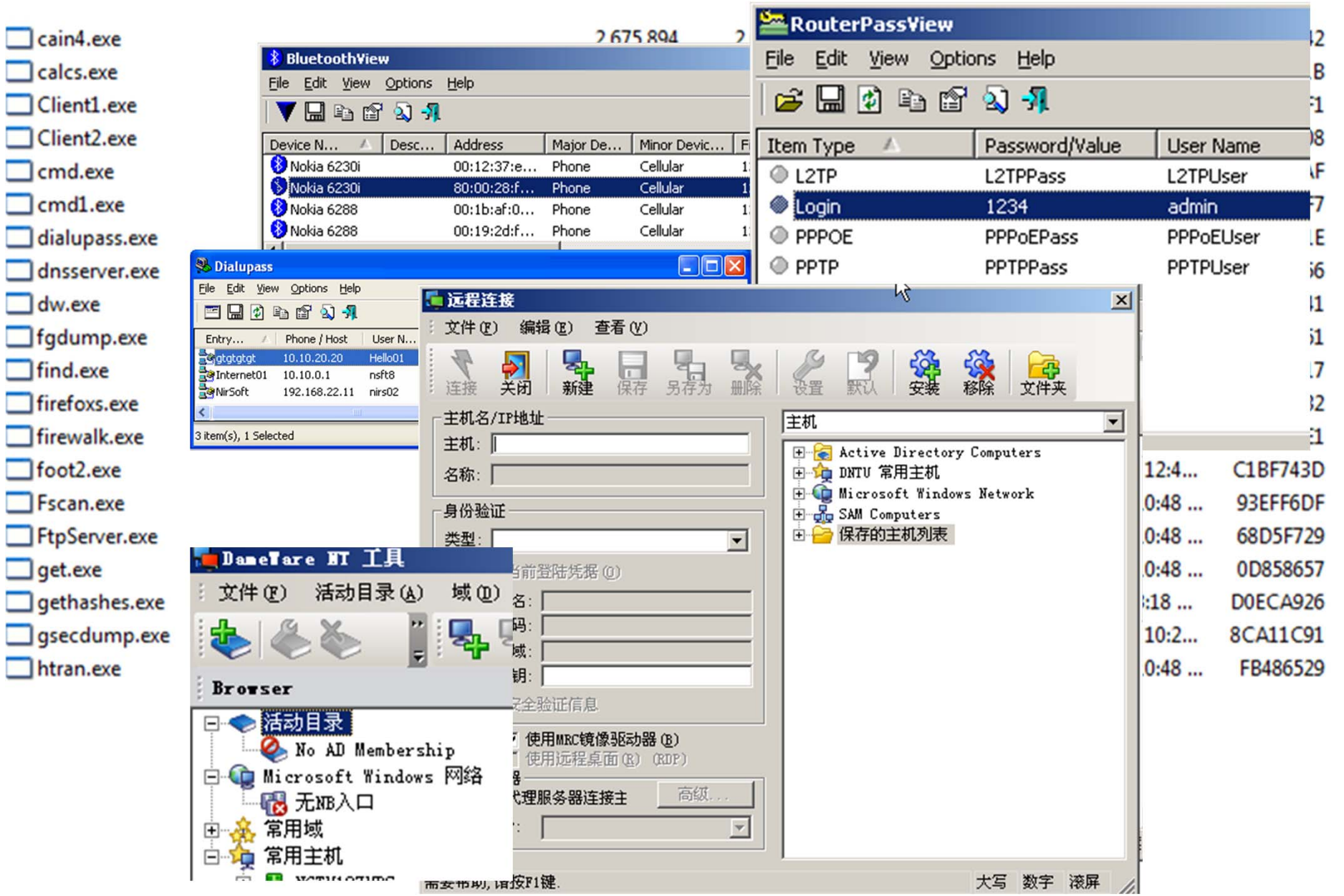


Length of time from “Compromise to Discovery” in 2010*

Also..

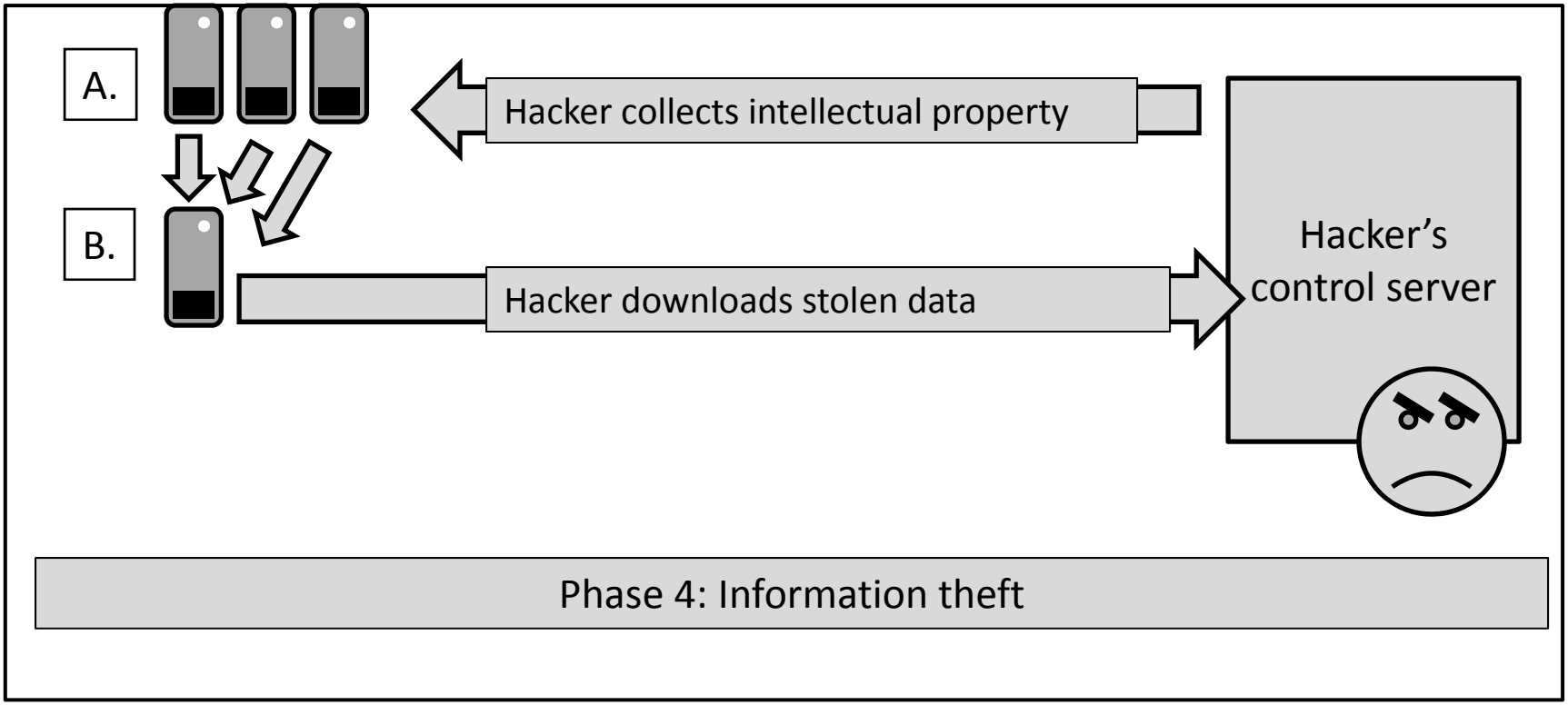
Average length of time before Shady RAT was discovered: 8 ½ months

*Source for graph: Verizon Data Breach Report 2010


cain4.exe
calcs.exe
Client1.exe
Client2.exe
cmd.exe
cmd1.exe
dialupass.exe
dnsserver.exe
dw.exe
fgdump.exe
find.exe
firefoxs.exe
firewalk.exe
foot2.exe
Fscan.exe
FtpServer.exe
get.exe
gethashes.exe
gsecdump.exe
htran.exe
BluetoothView
File Edit View Options Help
Device N... Desc... Address Major De... Minor Devic...
Nokia 6230i 00:12:37:e... Phone Cellular
Nokia 6230i 80:00:28:f... Phone Cellular
Nokia 6288 00:1b:af:0... Phone Cellular
Nokia 6288 00:19:2d:f... Phone Cellular
RouterPassView
File Edit View Options Help
Item Type Password/Value User Name
L2TP L2TPPass L2TPUser
Login 1234 admin
PPPOE PPPoEPass PPPoEUser
PPTP PPTPPass PPTPUser
Dialupass
File Edit View Options Help
Entry... Phone / Host User N...
gtgtgtgt 10.10.20.20 Hello01
Internet01 10.10.0.1 nsft8
NirSoft 192.168.22.11 nirs02
3 item(s), 1 Selected
远程连接
文件(F) 编辑(E) 查看(V)
连接 关闭 新建 保存 另存为 删除 设置 默认 安装 移除 文件夹
主机名/IP地址
主机:
名称:
身份验证
类型:
主机
Active Directory Computers
DNTU 常用主机
Microsoft Windows Network
SAM Computers
保存的主机列表
使用MRC镜像驱动器(B)
使用远程桌面(R) (RDP)
高级...
大写 数字 滚屏
DameWare NT 工具
文件(F) 活动目录(A) 域(D)
Browser
活动目录
No AD Membership
Microsoft Windows 网络
无NB入口
常用域
常用主机
12:4... C1BF743D
0:48 ... 93EFF6DF
0:48 ... 68D5F729
0:48 ... 0D858657
:18 ... D0ECA926
10:2... 8CA11C91
0:48 ... FB486529

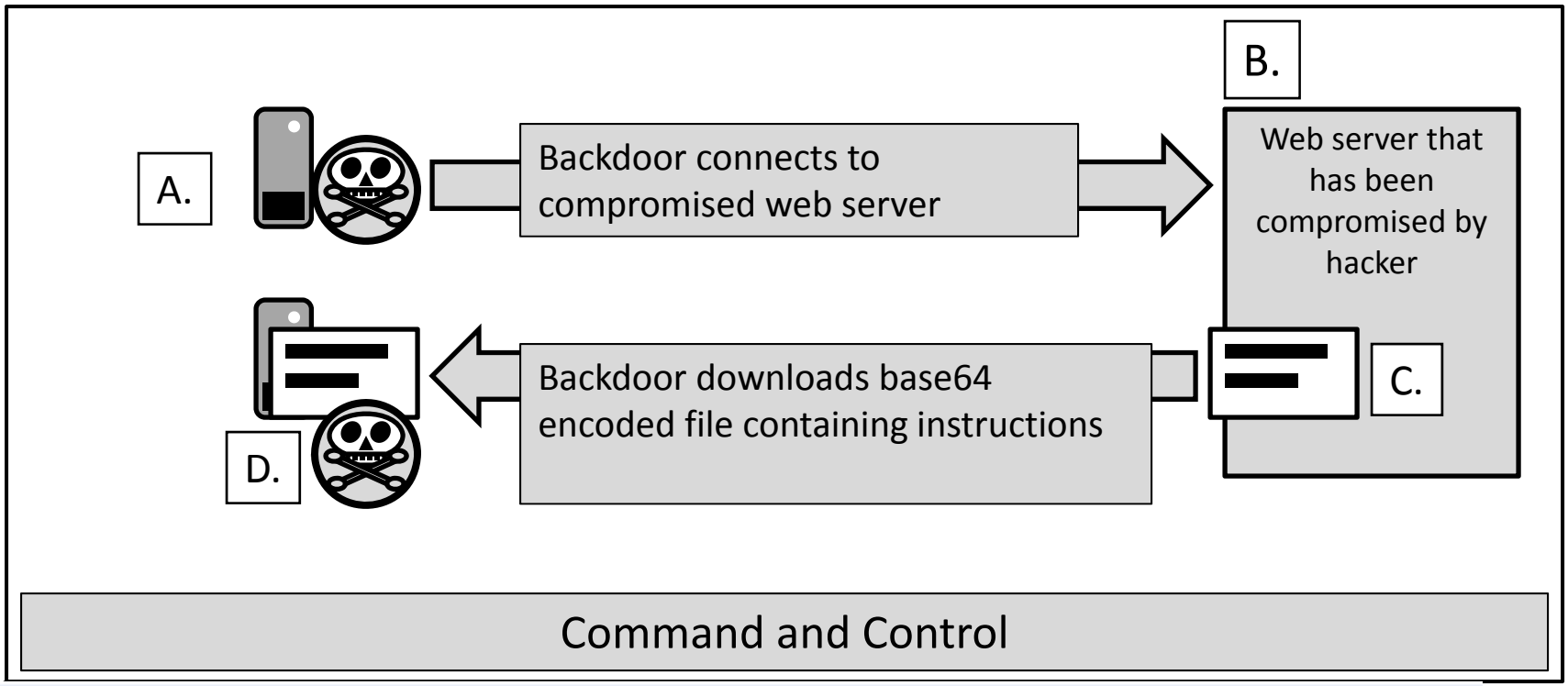
Attack vectors and strategies (TTP's)

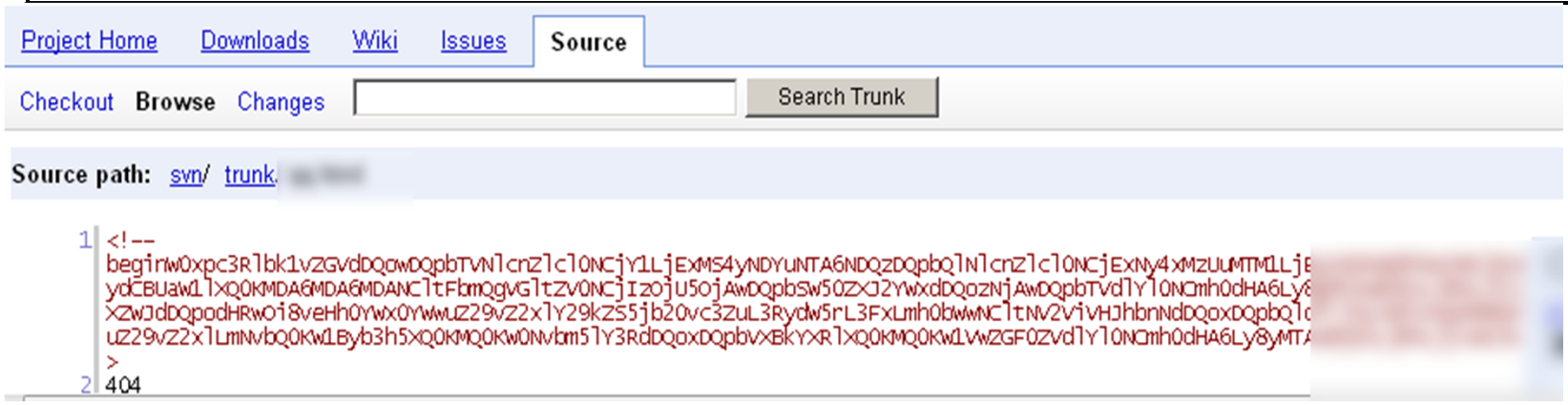
- Extensive use of hash cracking, rainbow tables
  - PTH toolkit and friends
- Entrenchment strategy
  - Multiple backup plans, backup CNC protocol & servers both
- Avoidance of packing, rootkits, etc.
- Staging data for exfil
  - Watch out for 3-day weekends



Files.part1.rar
Files.part2.rar
Files.part3.rar
Files.part4.rar
Files.part5.rar
Etc…

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
000000000	52	61	72	21	1A	07	00	19	7A	73	11	00	0D	00	00	00	Rar! zs
000000016	00	00	00	00	84	D4	74	C3	90	30	00	A8	77	FC	05	00	▮ÔtÃ 0 ¨wü
000000032	00	00	20	02	88	22	79	94	C0	63	A7	3C	14	30	0B	00	▮"y▮Àc§< 0
000000048	20	00	00	00	6D	65	6D	64	75	6D	70	2E	62	69	6E	00	memdump.bin
000000064	B0	E0	85	30	89	99	0B	00	00	8D	64	24	FC	89	0C	24	°à▮0▮▮ d$ü▮ $
000000080	8B	4C	24	04	C2	04	00	E4	74	50	50	8D	05	D8	79	49	▮L$ Â ätPP Øy I
000000096	00	8D	80	11	0A	00	00	89	44	24	04	8D	05	74	DC	50	▮ ▮D$ tÜP
000000112	00	8D	80	99	0F	00	00	8D	64	24	FC	89	04	24	8B	44	▮▮ d$ü▮ $▮D
000000128	24	04	C2	04	00	4A	CE	8D	64	24	FC	89	3C	24	57	8D	$ Â JÎ d$ü▮<$W
000000144	3D	B0	7D	49	00	8D	BF	6D	06	00	00	89	7C	24	04	8D	=°}I ¿m ▮|$





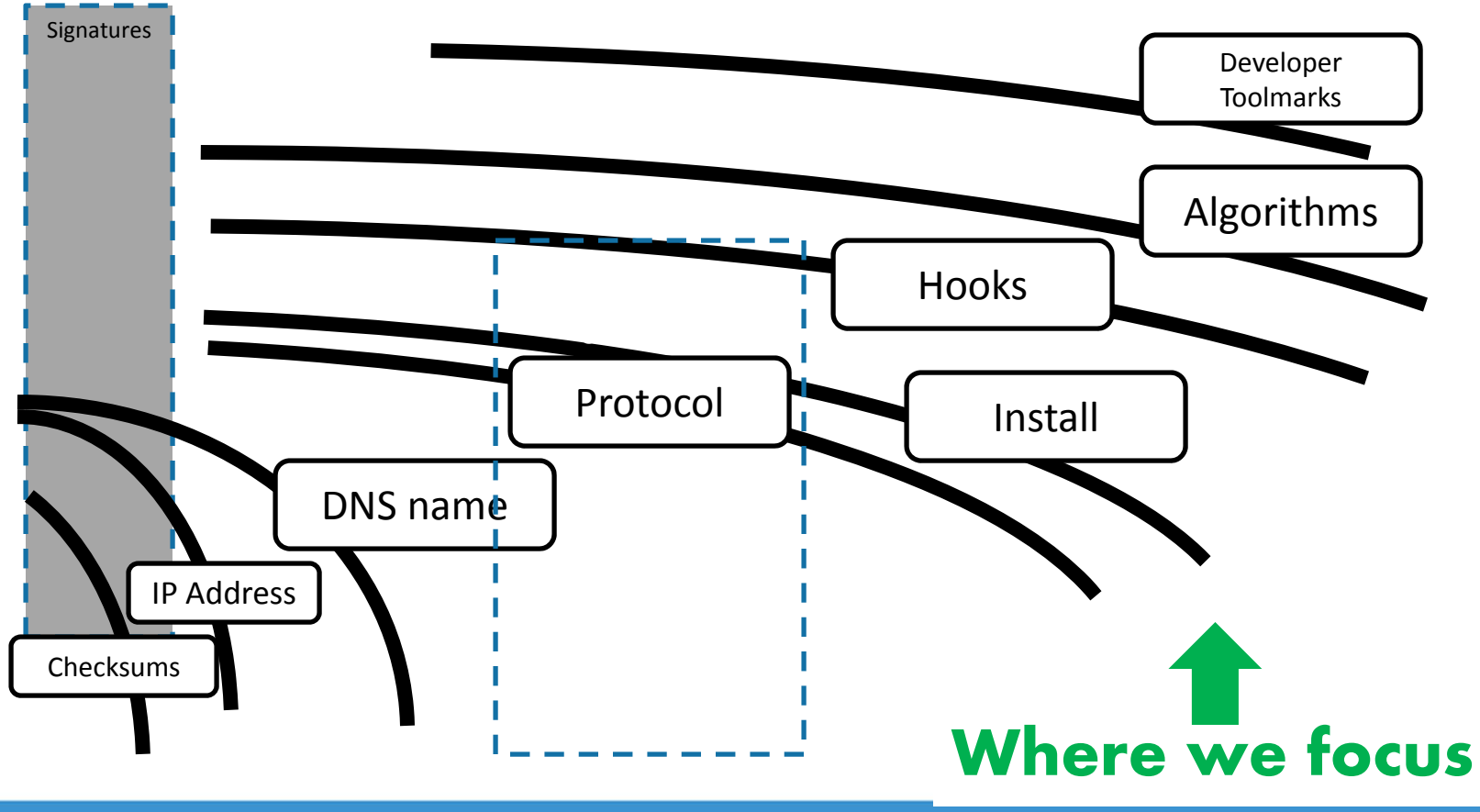
HTML to make this look like a 404 error page.

```
[ListenMode]
0
[MServer]
[redacted]:443
[BServer]
[redacted]
[Day]
1,2,3,4,5,6,7
[Start Time]
00:00:00
[End Time]
23:59:00
[Interval]
3600
[MWeb]
http://[redacted]
[BWeb]
http://[redacted]
[MWebTrans]
0
[BWebTrans]
1
[FakeDomain]
www.[redacted]
[Proxy]
1
[Connect]
1
[Update]
0
[UpdateWeb]
http://[redacted].bmp
```

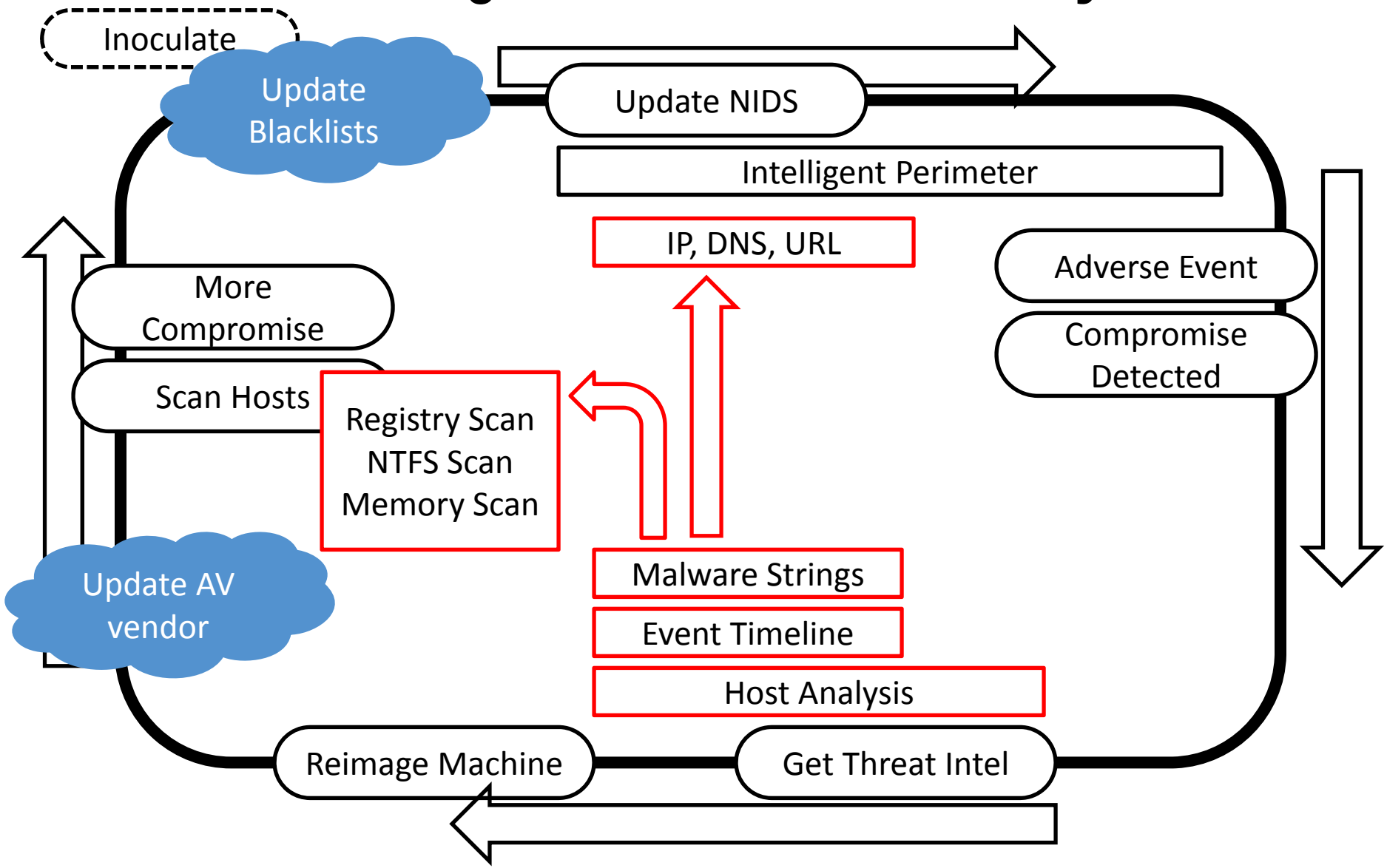
Intelligence Value Window

Lifetime →

Minutes Hours Days Weeks Months Years



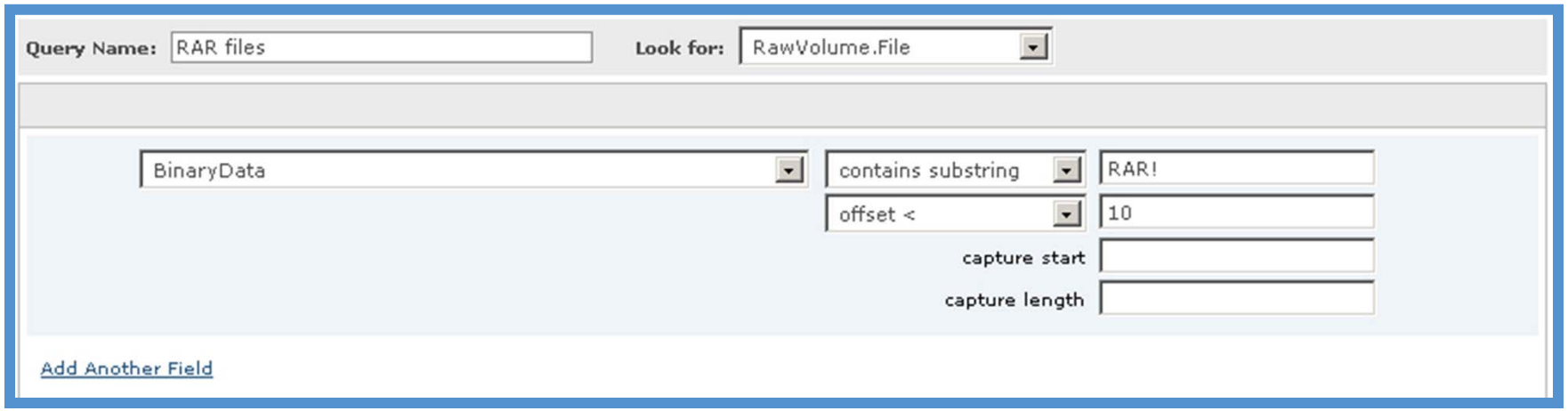
Intelligence-driven security



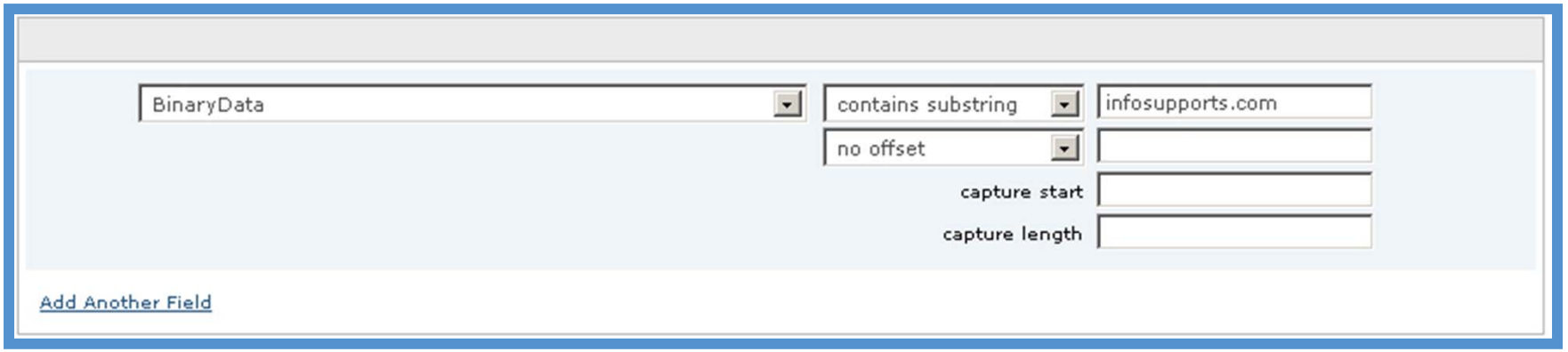
Searching for Indicators

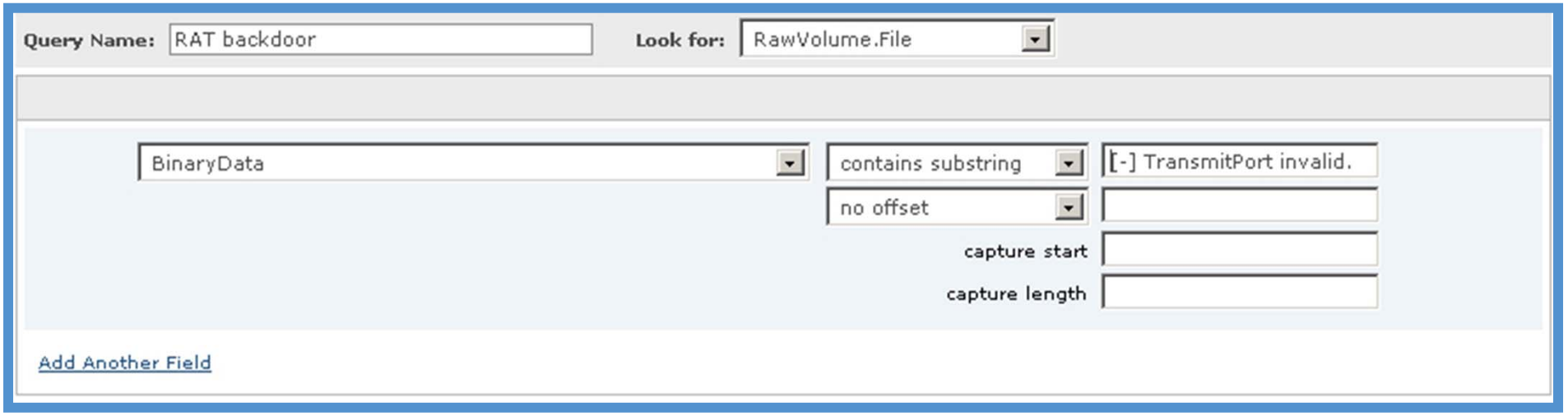
Files.part1.rar
Files.part2.rar
Files.part3.rar
Files.part4.rar
Files.part5.rar
Etc…

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
000000000	52	61	72	21	1A	07	00	19	7A	73	11	00	0D	00	00	00	Rar! zs
000000016	00	00	00	00	84	D4	74	C3	90	30	00	A8	77	FC	05	00	▮ÔtÃ 0 ¨wü
000000032	00	00	20	02	88	22	79	94	C0	63	A7	3C	14	30	0B	00	▮"y▮Àc§< 0
000000048	20	00	00	00	6D	65	6D	64	75	6D	70	2E	62	69	6E	00	memdump.bin
000000064	B0	E0	85	30	89	99	0B	00	00	8D	64	24	FC	89	0C	24	°à▮0▮▮ d$ü▮ $
000000080	8B	4C	24	04	C2	04	00	E4	74	50	50	8D	05	D8	79	49	▮L$ Â ätPP Øy I
000000096	00	8D	80	11	0A	00	00	89	44	24	04	8D	05	74	DC	50	▮ ▮D$ tÜP
000000112	00	8D	80	99	0F	00	00	8D	64	24	FC	89	04	24	8B	44	▮▮ d$ü▮ $▮D
000000128	24	04	C2	04	00	4A	CE	8D	64	24	FC	89	3C	24	57	8D	$ Â JÎ d$ü▮<$W
000000144	3D	B0	7D	49	00	8D	BF	6D	06	00	00	89	7C	24	04	8D	=°}I ¿m ▮|$

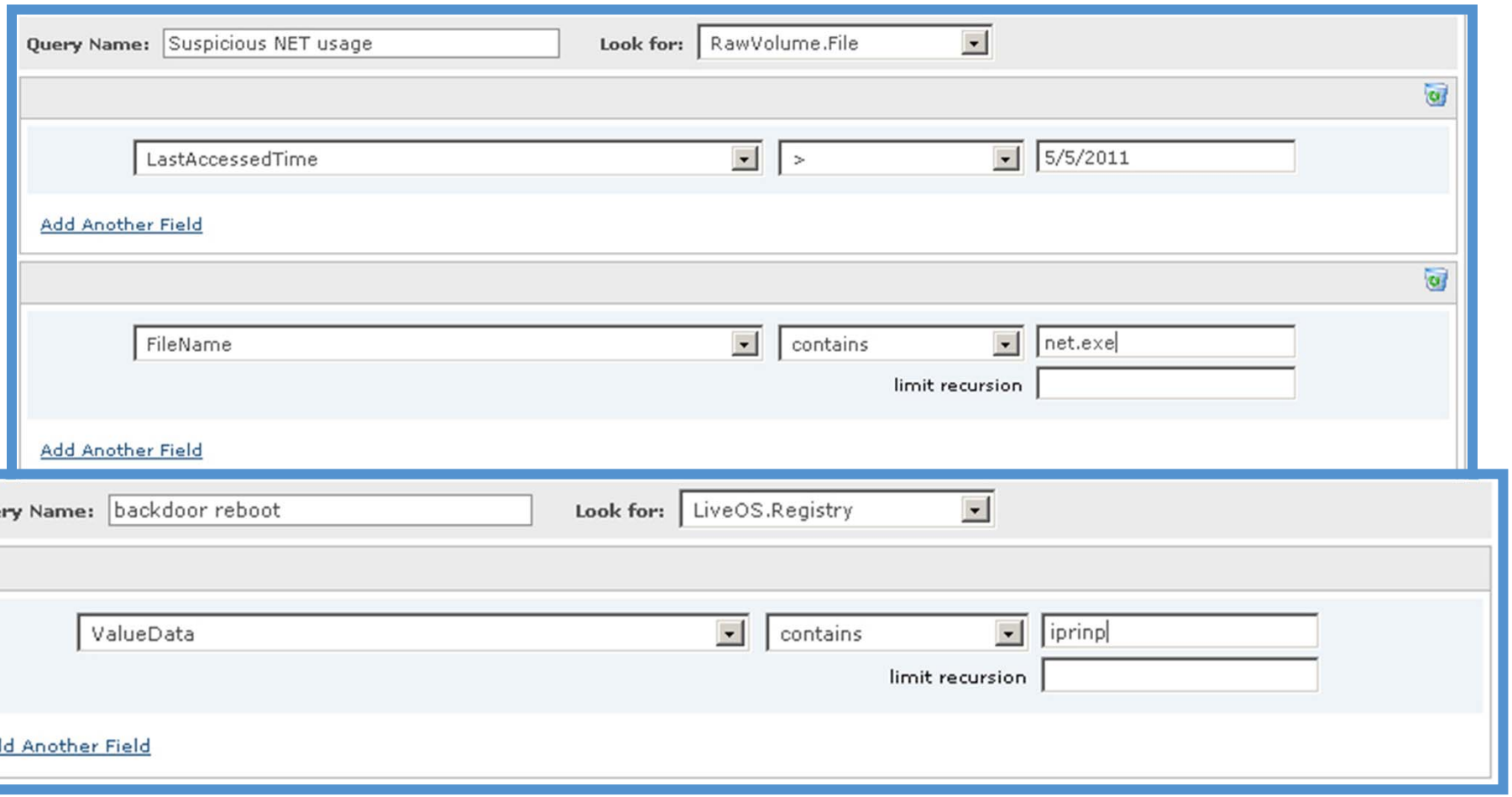


Searching for Indicators





Searching for Indicators



Apply

- Use your threat intelligence
- You need endpoint visibility
- The perimeter is vanishing
- Security is a counter intelligence problem, not a technology
  - Security will not be provided solely by blinking appliances in the rack

HBGary Active Defense dramatically reduced the time between network intrusion and discovery.

- U.S. Government Contractor

We can't live without it. Active Defense is saving us major money.

- Top 10 Financial Institution

Digital DNA is a game changer.

- Big Consulting Company

Responder with Digital DNA is definitely a need-to-have item in our toolbox.

- VP eCrime Unit, Fortune 50 Bank

HBGary

DEFEATING TOMORROW'S THREAT TODAY