**From:** "Aaron Barr" <aaron@hbgary.com>
**To:** "Ted Vera" <ted@hbgary.com>; "Rich Cummings" <rich@hbgary.com>
**Sent:** Wednesday, October 20, 2010 10:08 AM
**Attach:** TSA Cyber Security.pptx
**Subject:** TSA Presentation

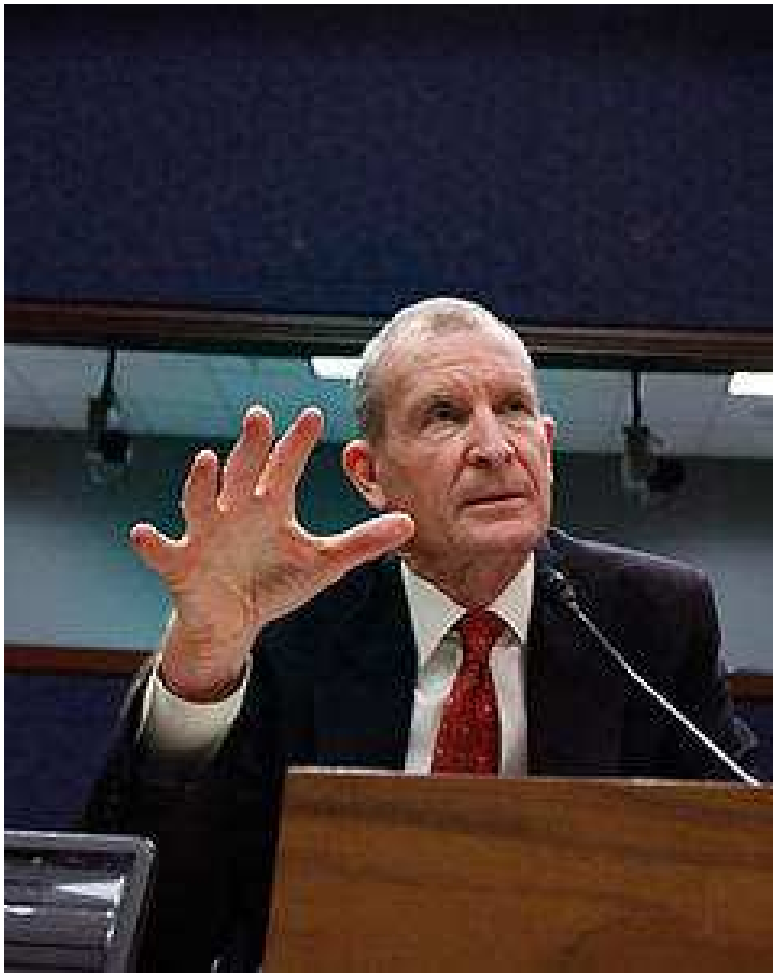
Aaron Barr
CEO
HBGary Federal, LLC
719.510.8478

HB Gary Federal

# Emerging Threats and Trends 2011

**Aaron Barr**
CEO
Oct 21, 2010

# Wake Up Call: <ring>
# Who is it? Answer: APT



## Google cyber attacks a 'wake-up' call

**-Director of National Intelligence Dennis Blair**

My mom now knows what I do for a living…. “yes mom I worked on some of that stuff”… “wow she said”.

http://www.csmonitor.com/USA/2010/0204/Google-cyber-attacks-a-wake-up-call-for-US-intel-chief-says

HBGary Federal

# Wake Up Call – Part II

**Stuxnet - weaponized malware is real. Nobody panic.**

Physical harm from cyber-based attack is no longer a theory.

HBGary Federal

# Cyber Threats

- “Cyber” has been co-opted by intelligence services and organized crime – it’s no longer a kids playground
  - Significant resources and broad objectives
  - Threats represented by multiple capabilities
- Volume of threats has greatly increased
  - Cyber crime now a bigger business than drug trafficking.
  - 6.4 million computer systems, 230 countries, 18 million+ CPUs

HBGary Federal

# APT – What Does It Mean?

- **Advanced** attack capabilities. This does not mean state-of-the-art abilities, but well planned, coordinated, and executed. 9/11 was advanced.
- **Persistent** attacks to maintain up-to-date and continuous access to information and systems.
- **Threat** to business continuity and national security, compromises our ability operate and maintain control.

HBGary Federal

# APT – Who is it?

State-Sponsored APT (SSAPT)

Criminal APT (CAPT)

HBGary Federal

# SSAPT – Motivation?

- Military
  - Land, Air, Sea, Space, and Cyberspace dominance
  - Asymmetric Warfare
- Intelligence
  - A good defense requires a good offense
  - Intelligence, Surveillance, and Reconnaissance
- Business
  - Intellectual Property

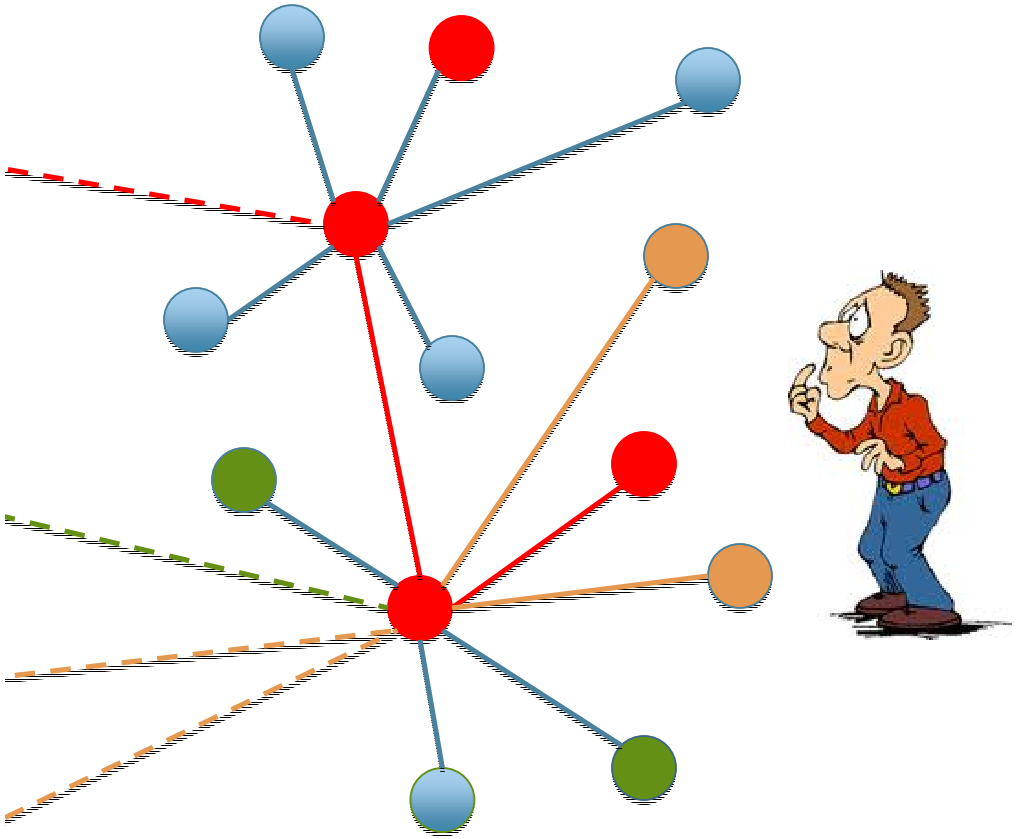
HBGary Federal

# CAPT – Motivation?

- Data = Money
- How do you make more money?
  - Diversify and Automate
- Hackernet
  - Proxy hackers get paid by the infection
  - Master hacker collects all the data
- CAPT will only become more effective.
- Represents a significant threat to national security.

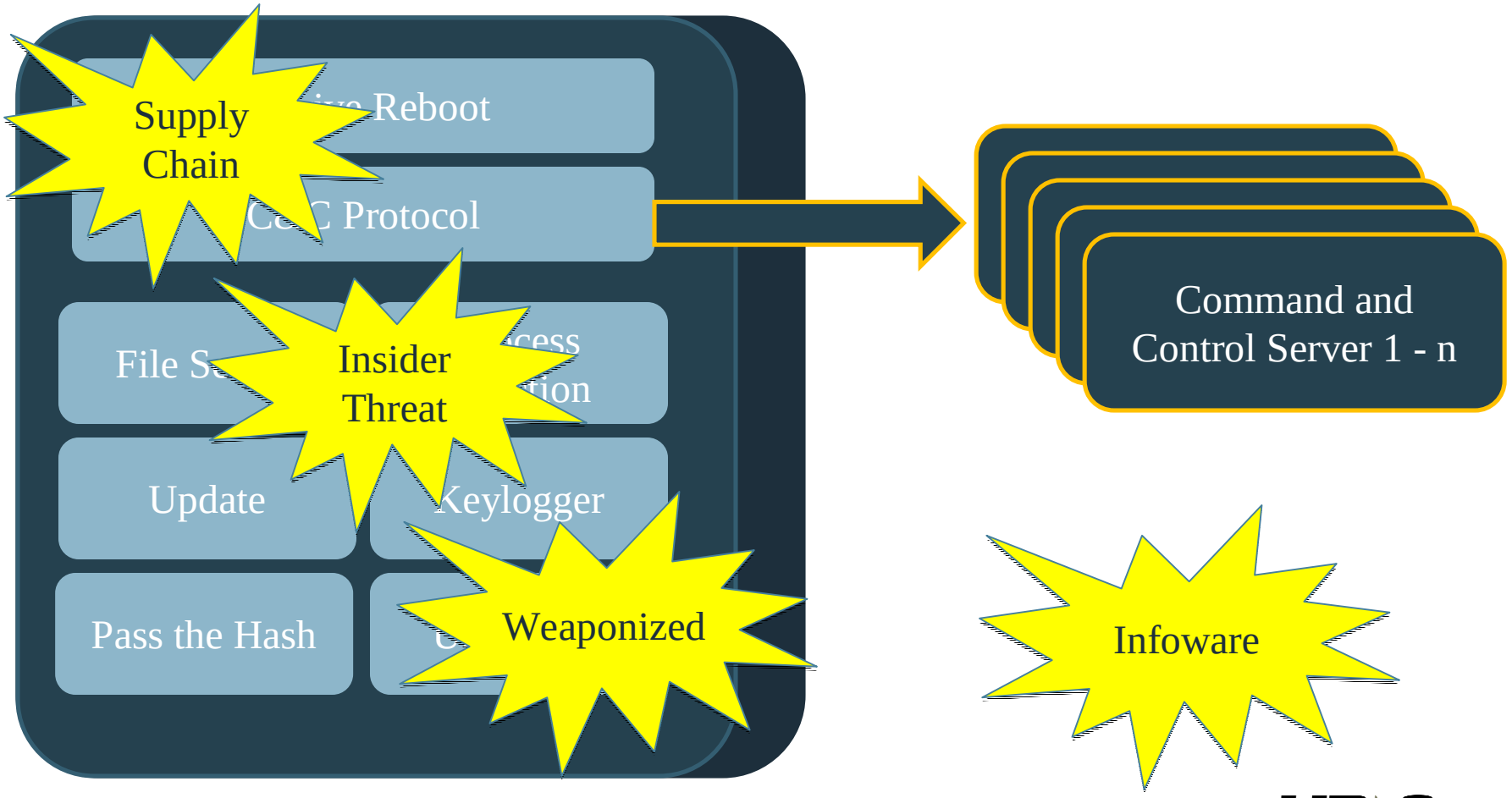
HBGary Federal

# Its All Very Confusing



HBGary Federal

# Anatomy of APT Malware




HBGary Federal

# Social Media

- 1994 all over again…
- Amount of PII is excessive and unmanagable
- Phishing will become much more targeted and effective
- Development of content and services that have the intent to collect information

HBGary Federal

# Social Media Guy

facebook

Likes Redskins
Friends with …
Lives in Columbia, MD

twitter

Securityguru Cyberspace is the new domain of warfare: WASHINGTON: With the creation of the U.S. **Cyber Command in May and last... http://twurl.nl/bgt0xq**

LinkedIn

Acme Contractor
Navy Cryptologist
Member Intelligence Group

foursquare

Checked in at
NSA Visitor Parking

…thank you, thank you very much

HBGary Federal

# Future Landscape

- Technology Evolution
  - Mobile
  - Social Media
  - Convergence
- Security Implications
  - Faded Perimeter
  - Reliance on Commercial Infrastructure
  - Data Access

HBGary Federal

# High Level Observations

- Fact 1: Sophisticated criminal attacks and apparent state sponsored attacks are increasingly becoming the focus of IT security operations and efforts in many vertical markets today – Govt, Energy, Finance, Technology, Critical Infrastructure.
- Fact 2: Existing IT security investments required but ineffective to detect and block the modern attacks and protect enterprise data

HBGary Federal

# High Level Observations

- Fact 3: APT malware is driving demand for new IT Security Solutions – more visibility – scalability – threat correlation & forensics

- Fact 4: The ability to detect and react to new threats and attacks is hampered by a lack of integration and standardization, as well as effective legal and policy guidelines.

HBGary Federal

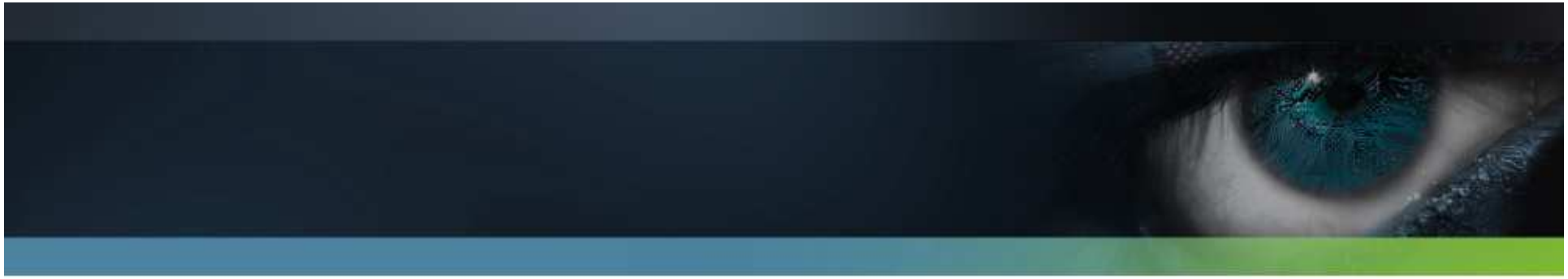
# All Your Base Are Belong to Us

Everybody in this room who manages an Enterprise with more than 10,000 nodes

## YOU ARE ALREADY COMPROMISED

They are STEALING right now, as you sit in that chair.

HBGary Federal



# Why Enterprise Security Products DON'T WORK

HBGary Federal

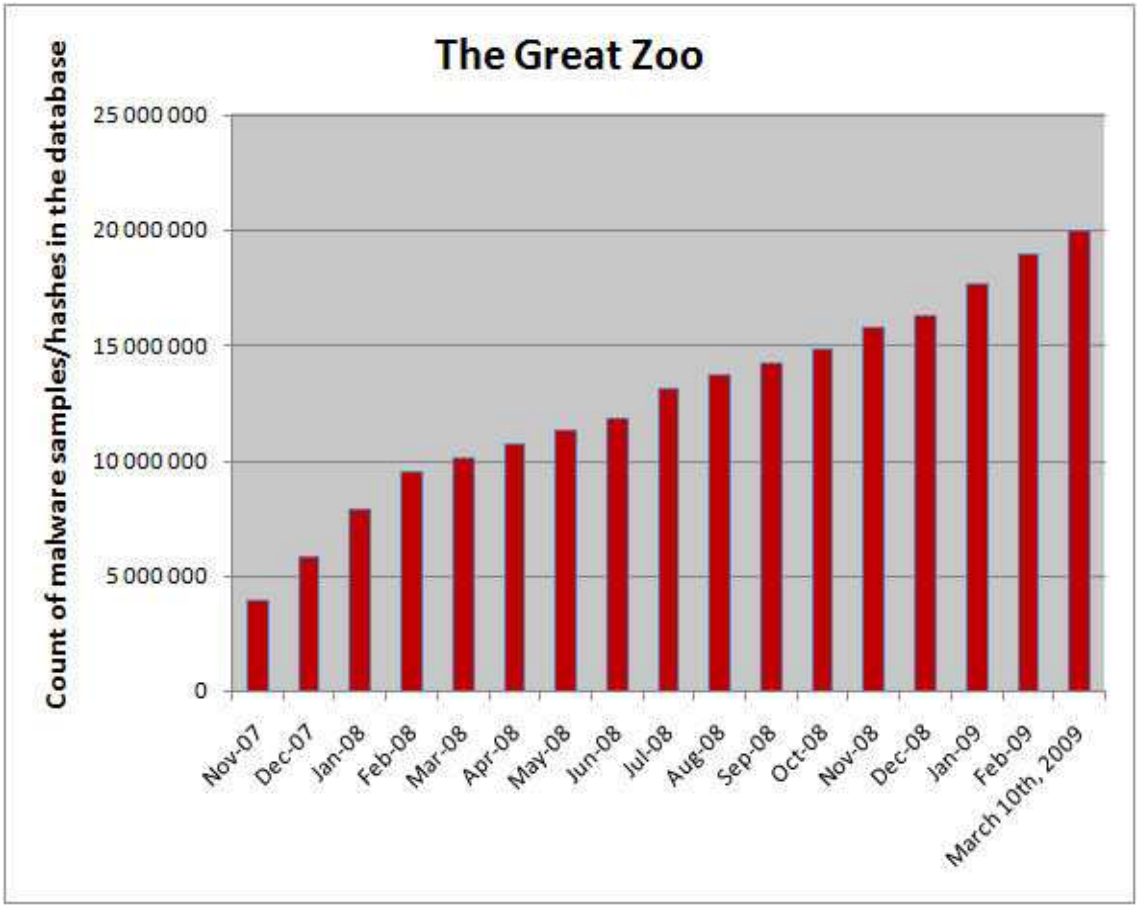
# The True Threat

- Malware is a ***human*** *issue*
  - Bad guys are targeting your systems and information, intellectual property, and personal identity
- Malware is only a vehicle for intent
  - Theft of Intellectual Property
  - Identity Theft for Online Fraud
  - Intelligence Gathering
  - Deny, Degrade, Disrupt

HBGary Federal

# Scale

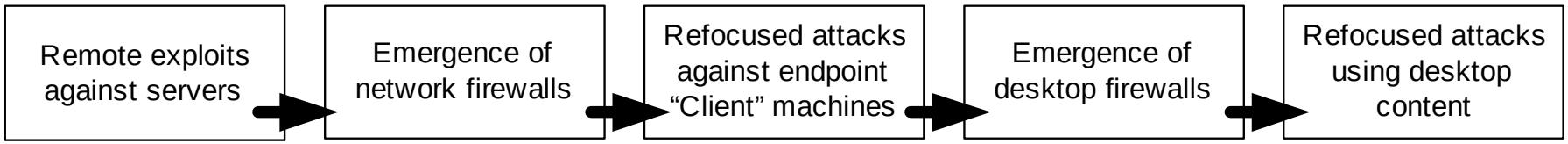
***Over 100,000 malware are automatically generated and released daily. Signature based solutions are tightly coupled to individual malware samples, thus cannot scale.***




HBGary Federal

# Surface

- The attacks today are just as effective as they were in 1999




*The bad guys STILL HAVE their zero day, STILL HAVE their vectors, and STILL HAVE their malware*

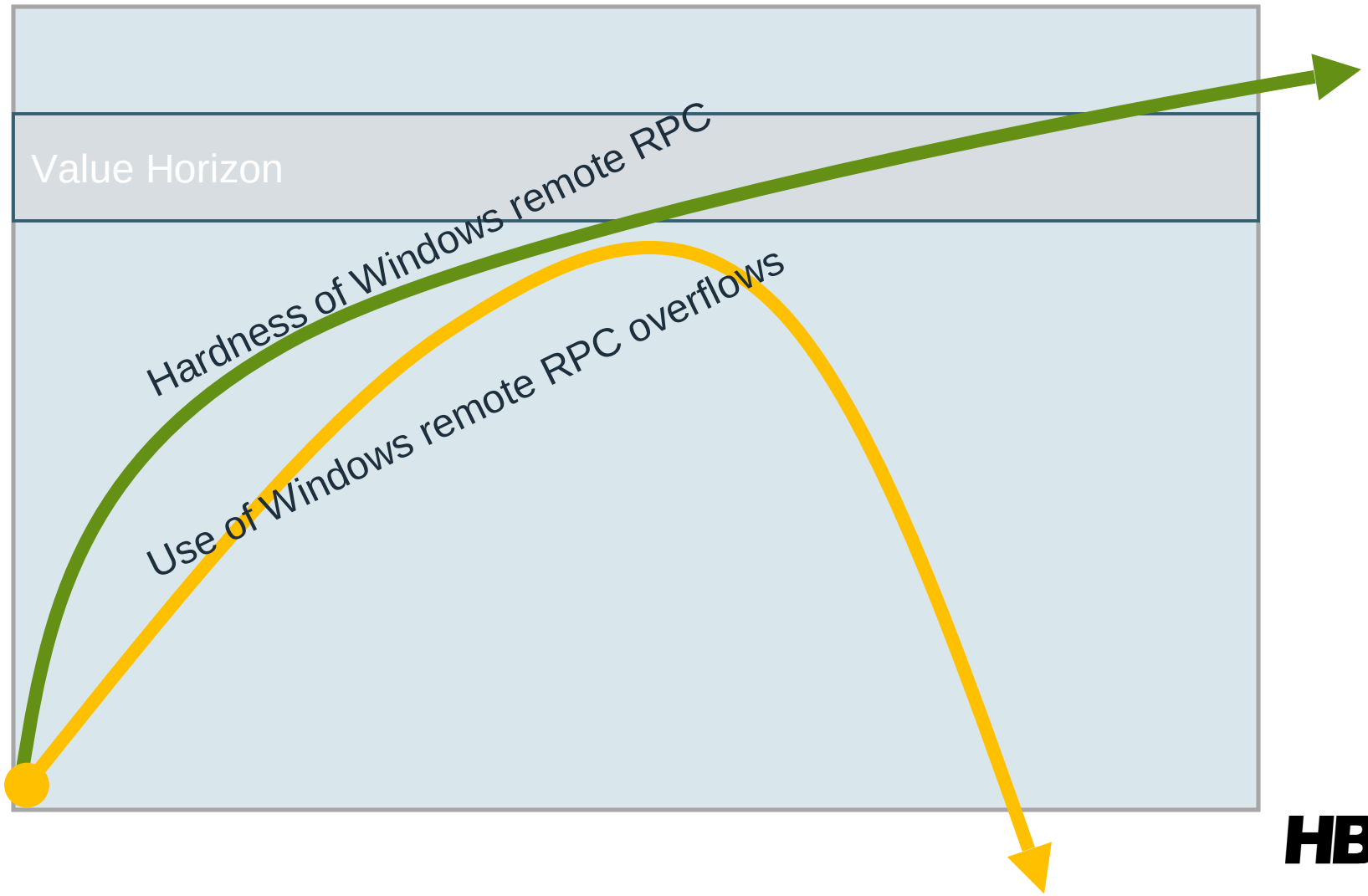
HBGary Federal

# Not an Anti-Virus Problem

- Malware isn't released until it bypasses AV products
  - Testing against AV is part of the QA process
- AV doesn't address the actual threat – the human who is targeting you
- AV has been shown as nearly useless in stopping the threat
  - AV has been diminished to a regulatory checkbox – it's not even managed by the security organization, it's an IT problem

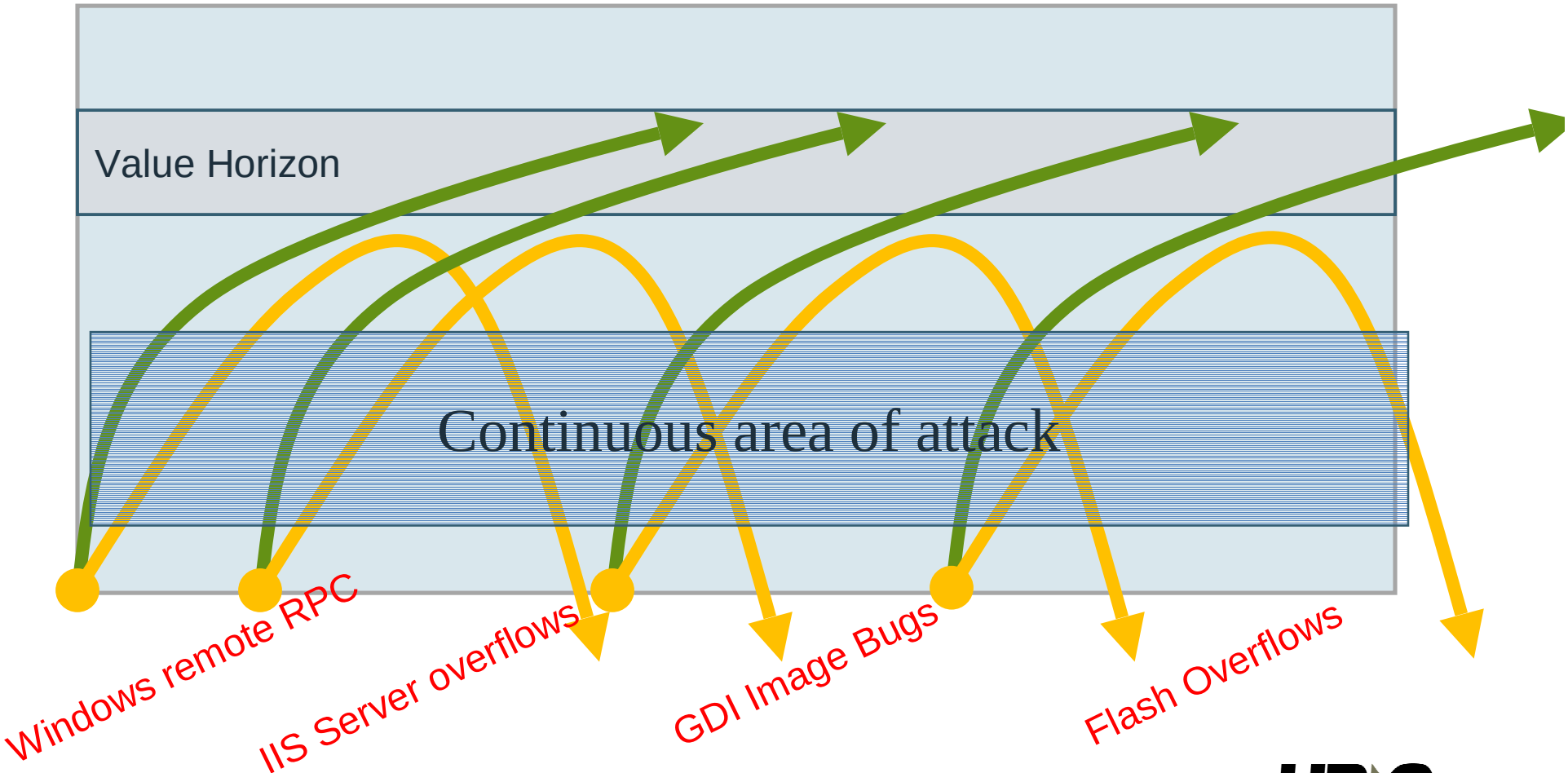
HBGary Federal

# Annealing

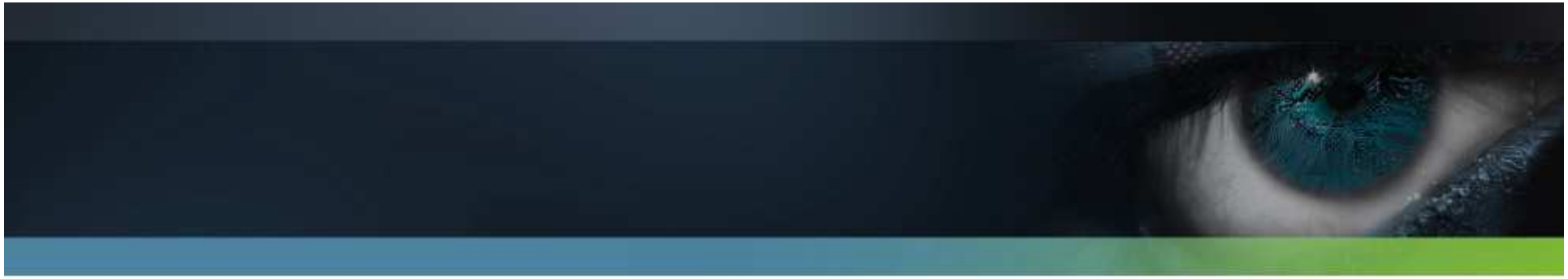


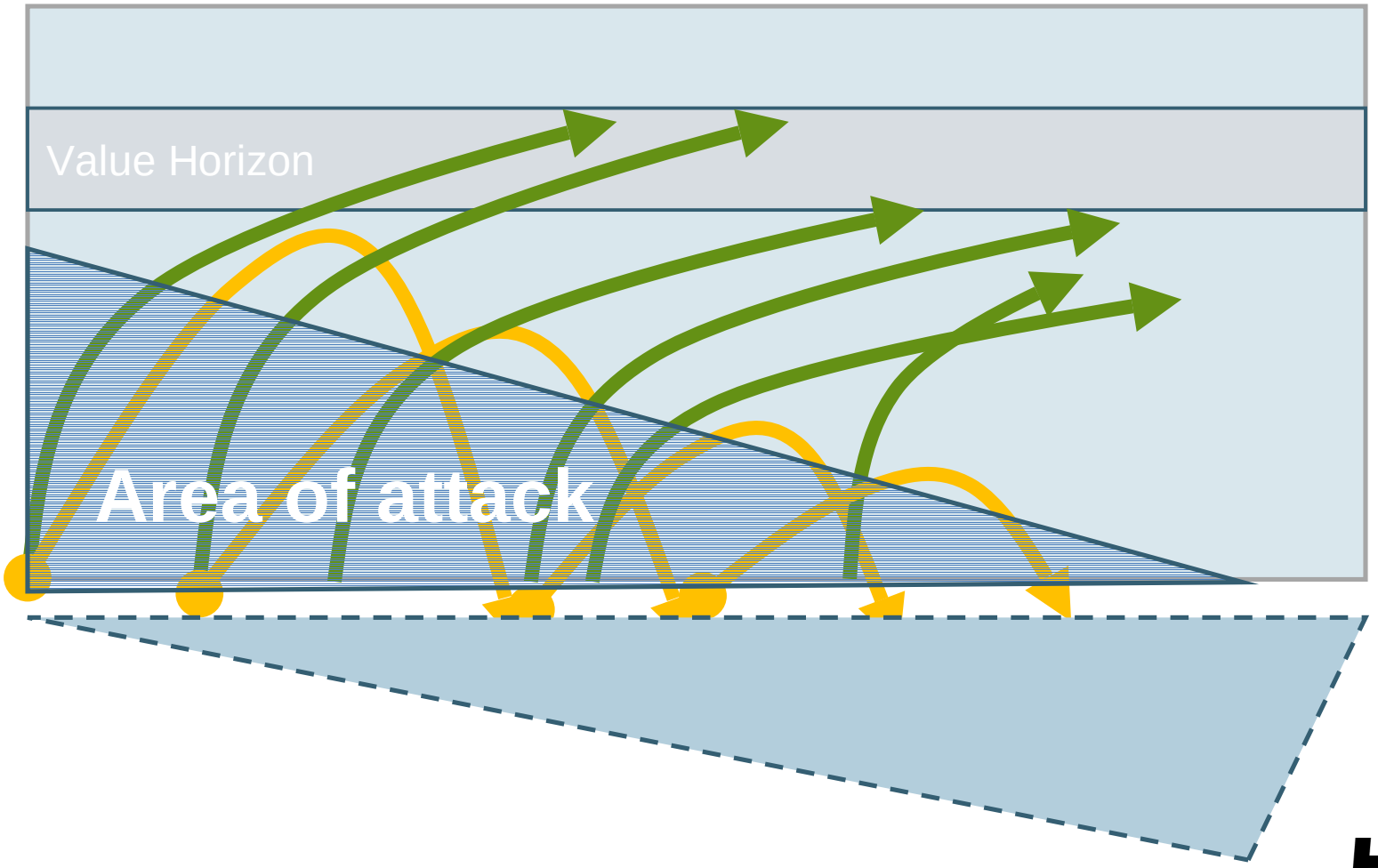

HBGary Federal

# Continuum




HBGary Federal

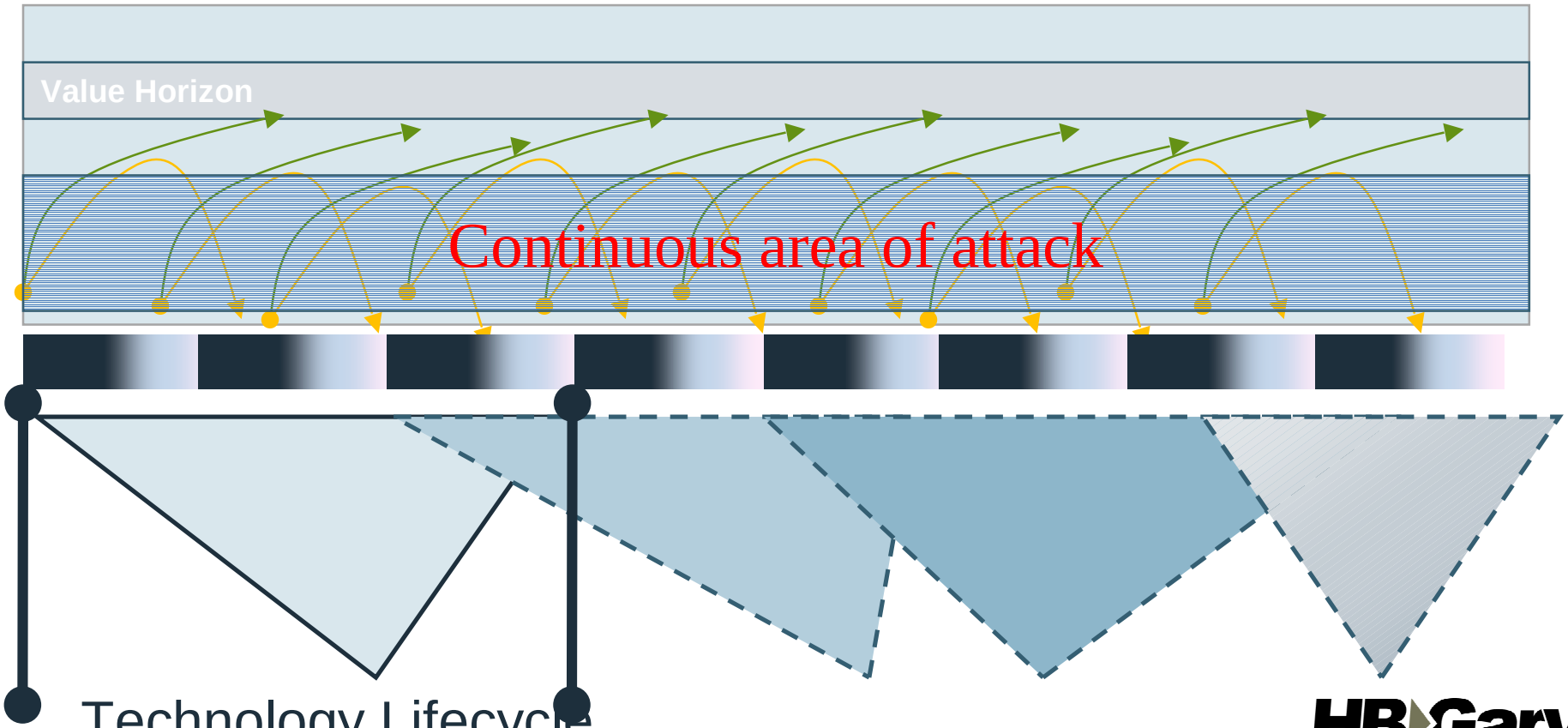




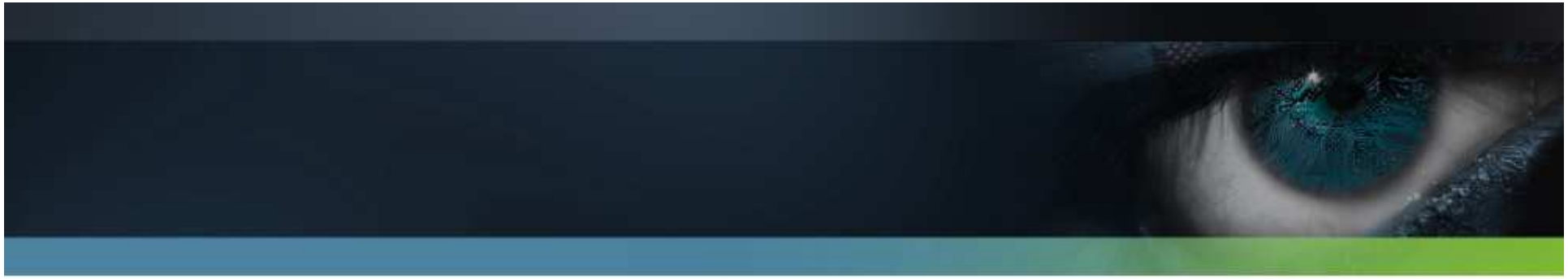

HBGary Federal

# Continuous Areas of Attack

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




HBGary Federal



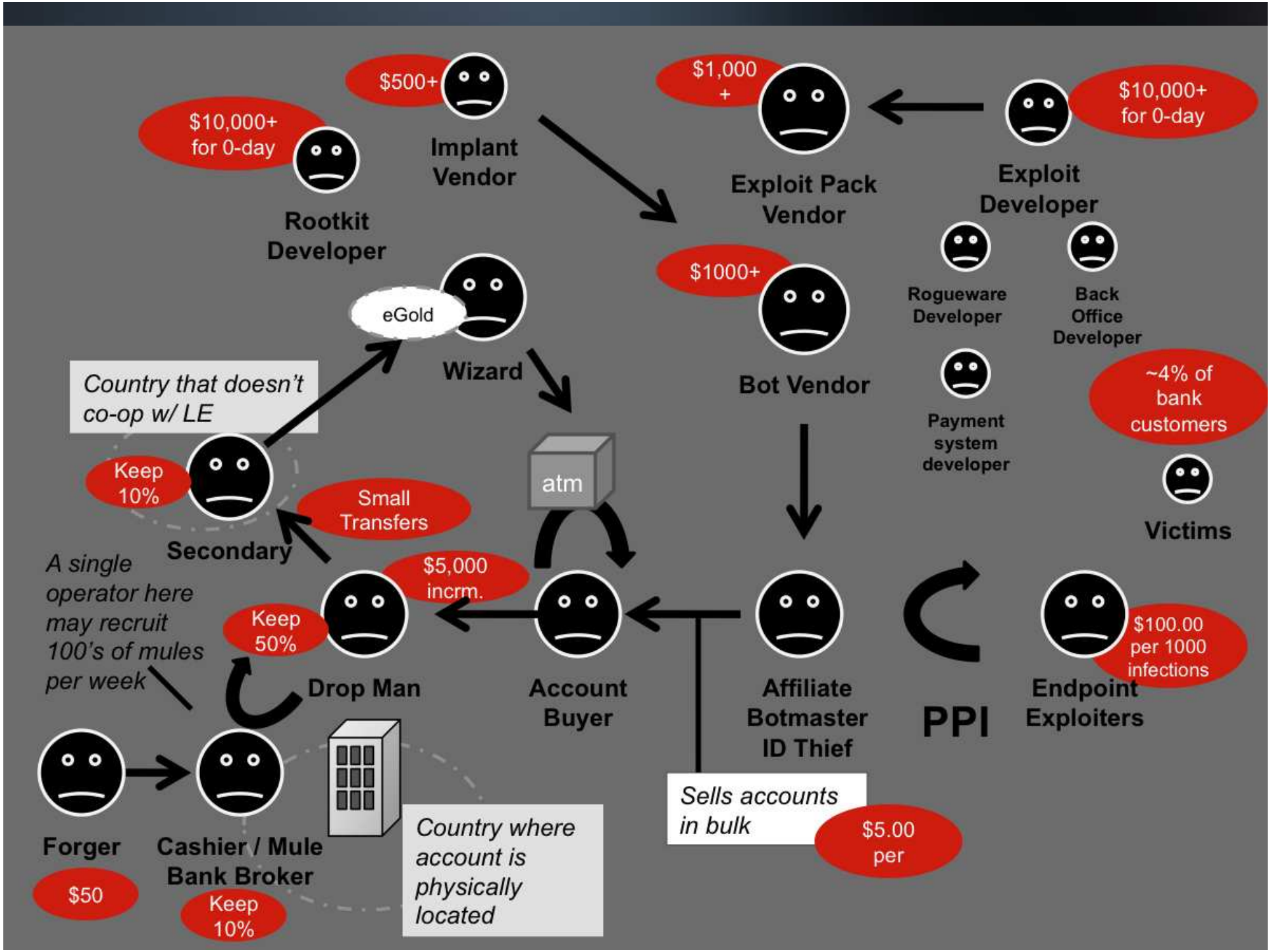
# The Global Malware Economy

HBGary Federal

# A Global Theatre

- There are thousands of actors involved in the theft of information, from technology developers to money launderers
- Over the last decade, an underground economy has grown to support espionage and fraud
- This “malware ecosystem” supports both Crimeware and e-Espionage.  It also likely provides cover for other activities

HBGary Federal


$500+
$10,000+ for 0-day
Implant Vendor
Rootkit Developer
$1,000 +
Exploit Pack Vendor
$10,000+ for 0-day
Exploit Developer
$1000+
Bot Vendor
Rogueware Developer
Back Office Developer
Payment system developer
~4% of bank customers
Victims
eGold
Wizard
Country that doesn't co-op w/ LE
Keep 10%
Secondary
Small Transfers
atm
A single operator here may recruit 100's of mules per week
$5,000 incrm.
Keep 50%
Drop Man
Account Buyer
Affiliate Botmaster ID Thief
PPI
Endpoint Exploiters
$100.00 per 1000 infections
Sells accounts in bulk
$5.00 per
Forger
$50
Cashier / Mule Bank Broker
Keep 10%
Country where account is physically located

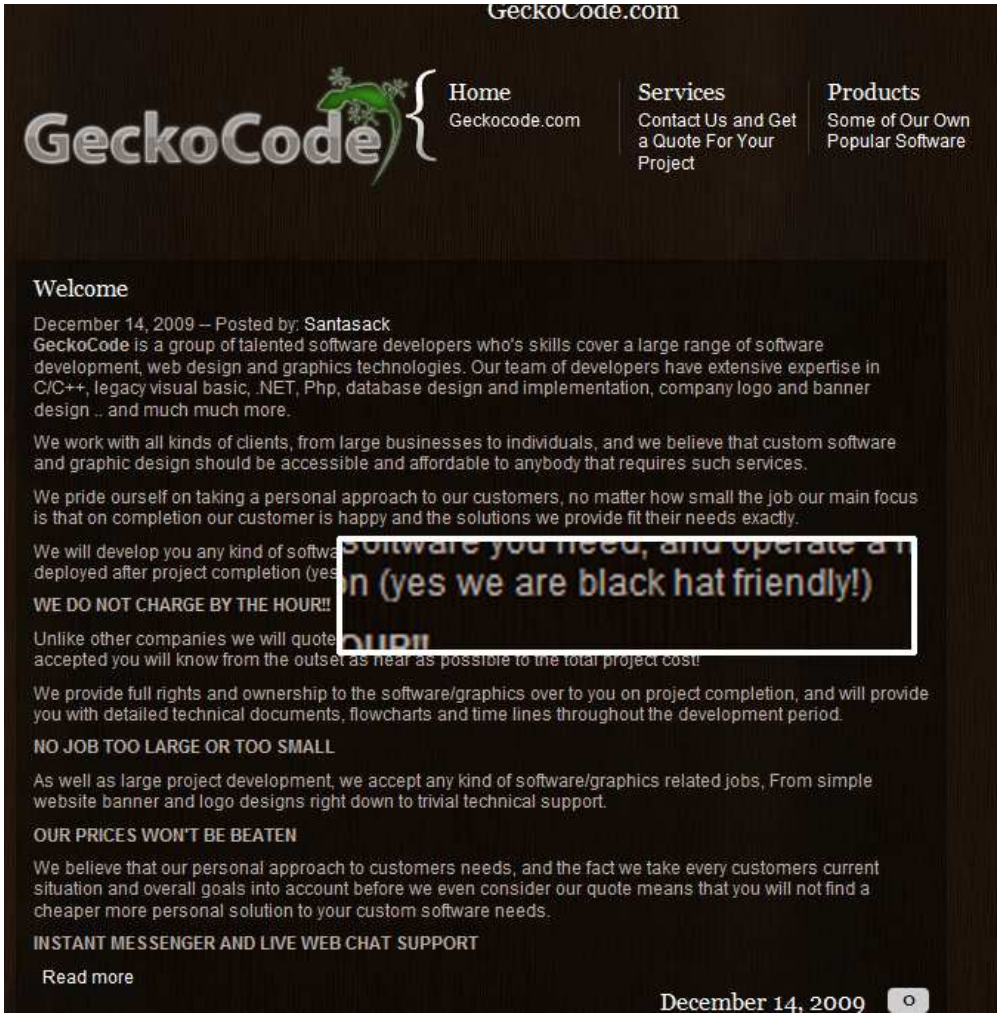
# Pay-per-install.org


HBGary Federal

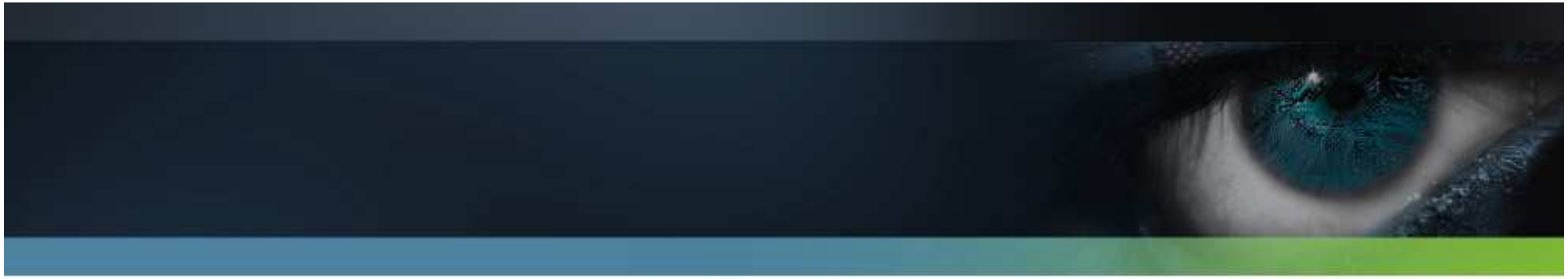
# Earning4u


HBGary Federal

# Custom Crimeware Programming Houses




HBGary Federal



# Anatomy of APT Operations

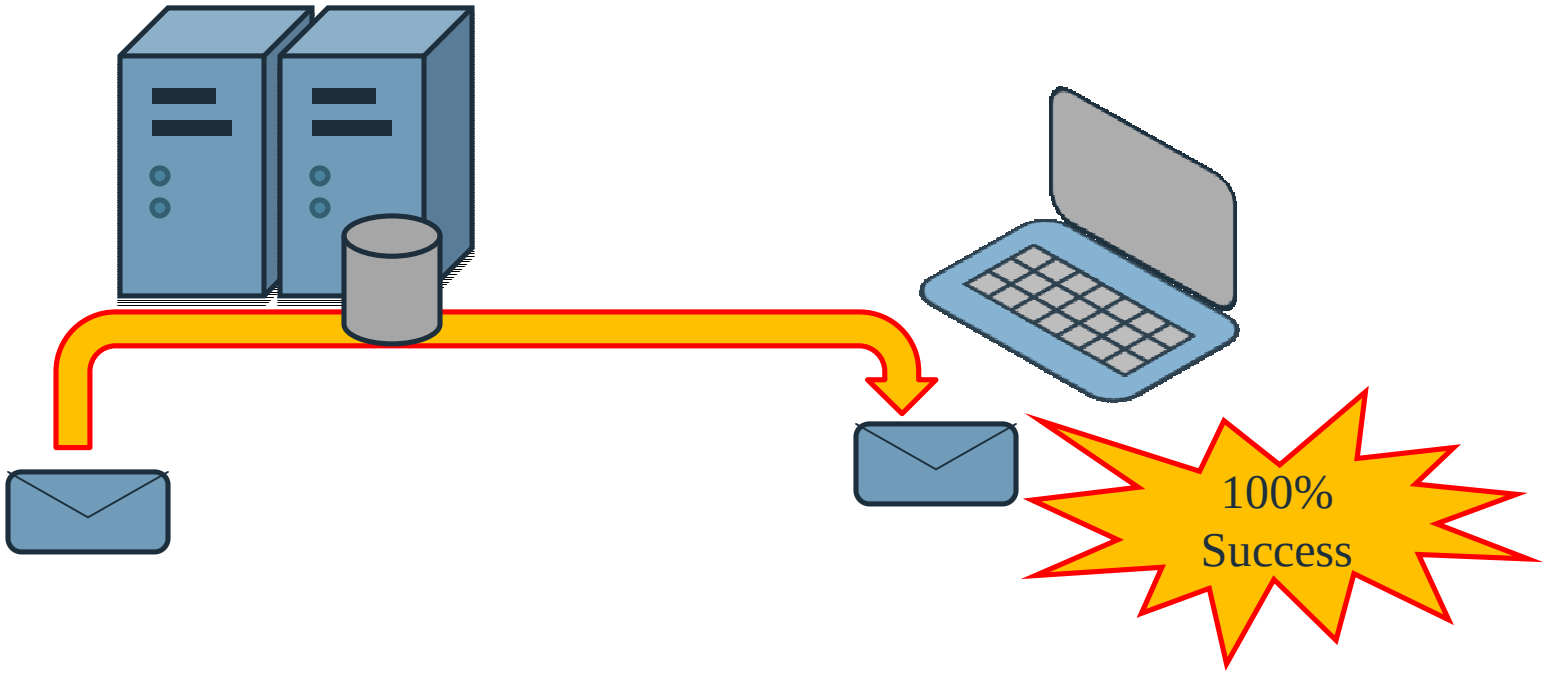
HBGary Federal

# Malware Distribution System

- Many, Many, Attack Vectors
  - Targeted Browser attacks -
  - Spear & Whale Phishing
  - Zero Day or well known exploits
  - Slow and Low & Loud and Proud – they do it all
  - Re-Direction – I expect you to find my first 2 malware infections
- Social Media
  - Intelligence, Surveillance, and Reconnaissance
  - Highly targeted spear-phishing attacks
- Supply Chain
  - IT Hardware with a little extra somethin, somethin…
- Insider Threat
  - Disgruntled employees, or Agents for FIS

HBGary Federal

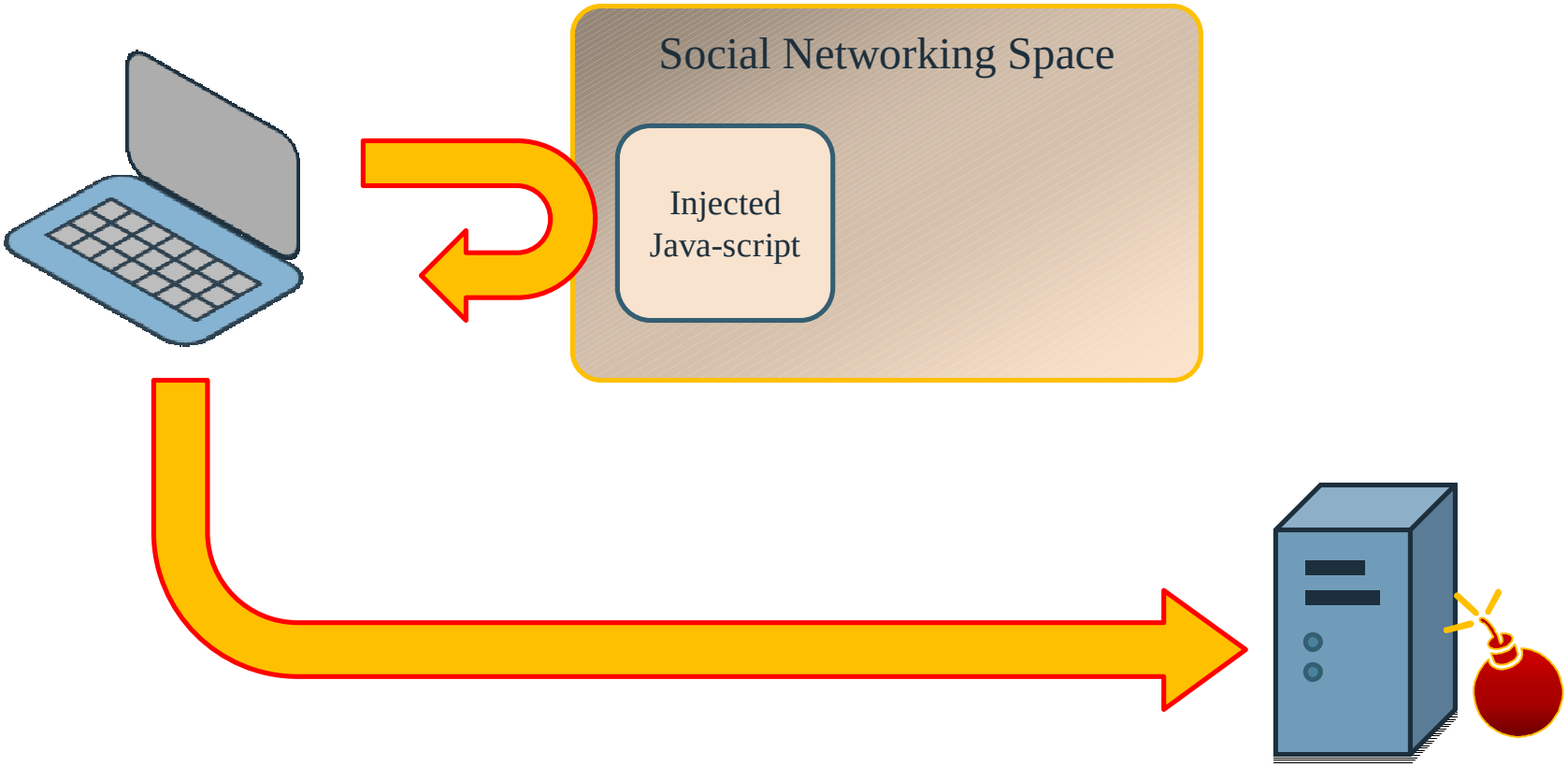
# Booby Trapped Documents




- Single most effective *focused* attack today
- Human crafts text to look legitimate

HBGary Federal

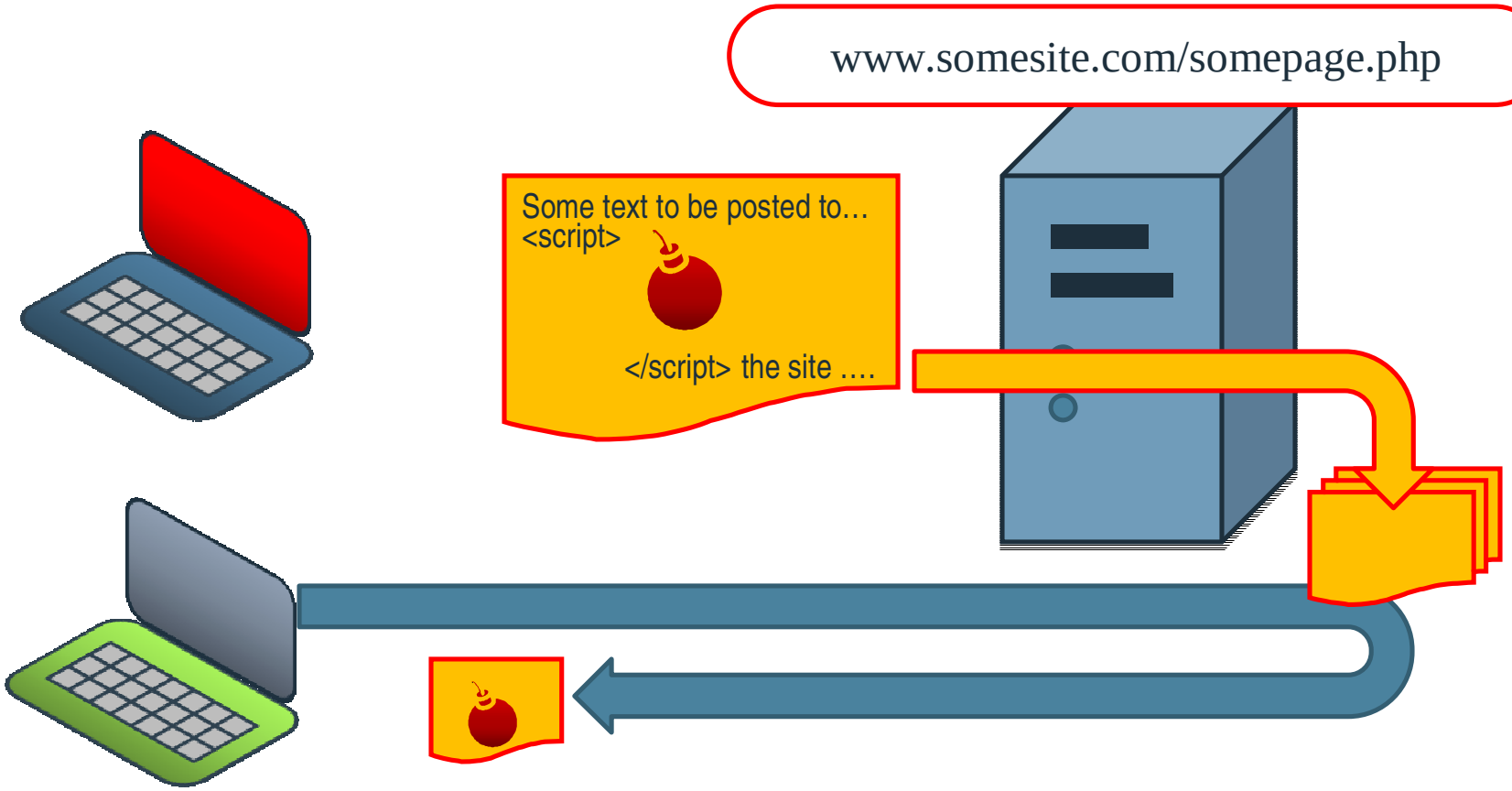
# Web Based Attack




- Used heavily for large scale infections
- & Targeted Operations for specific groups of people….

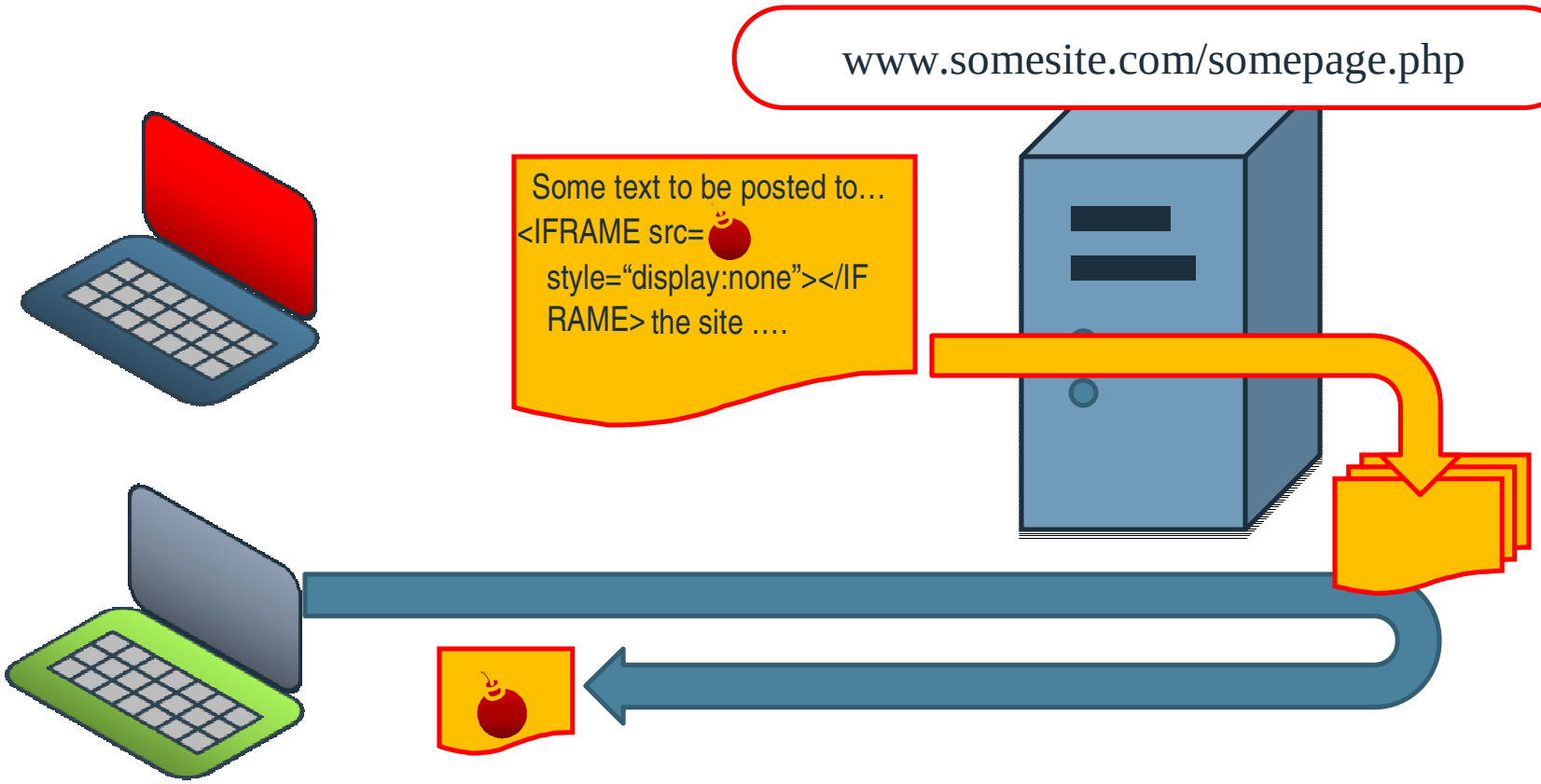
HBGary Federal

# Trap Postings I



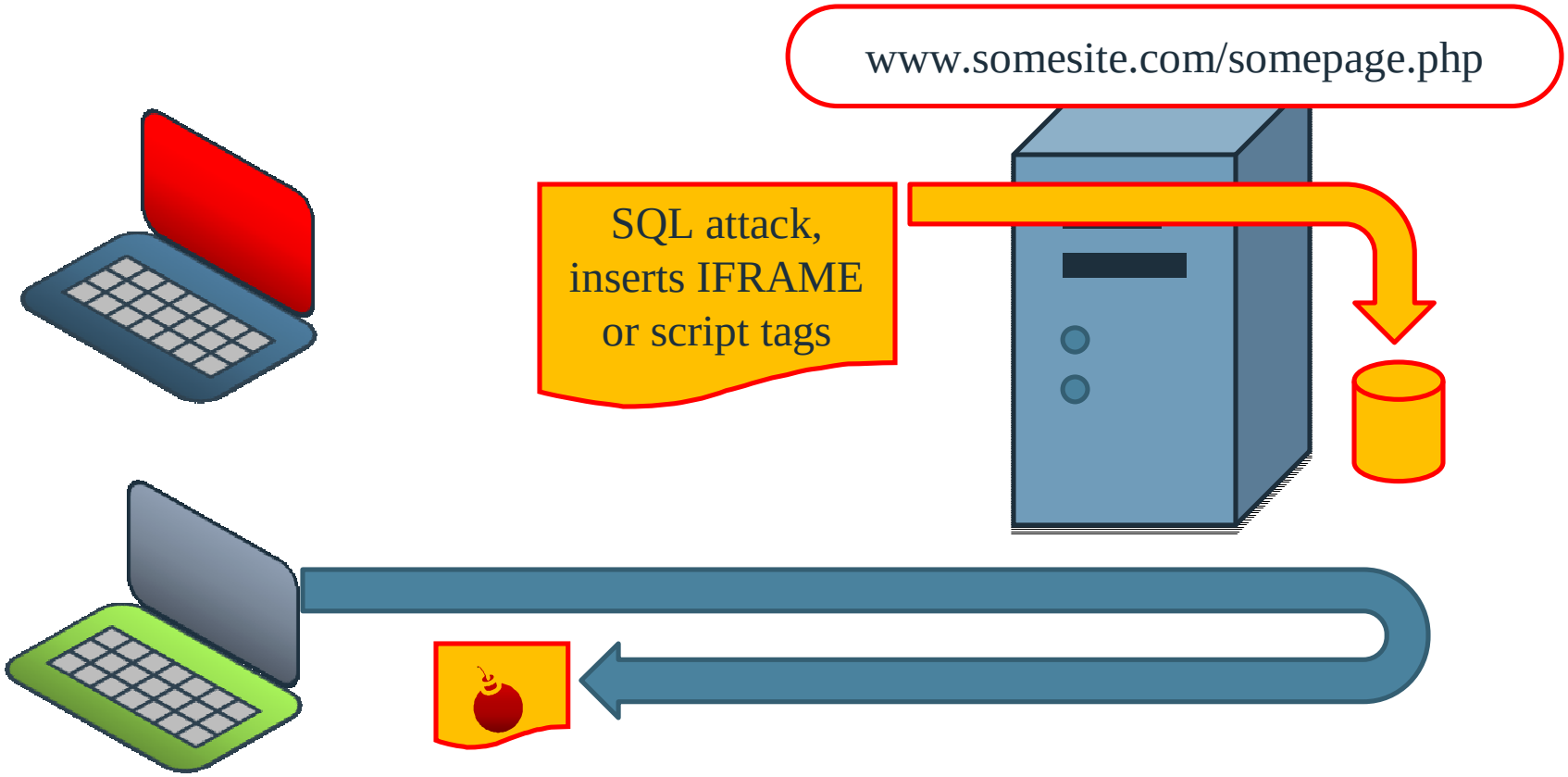

HBGary Federal

# Trap Postings II



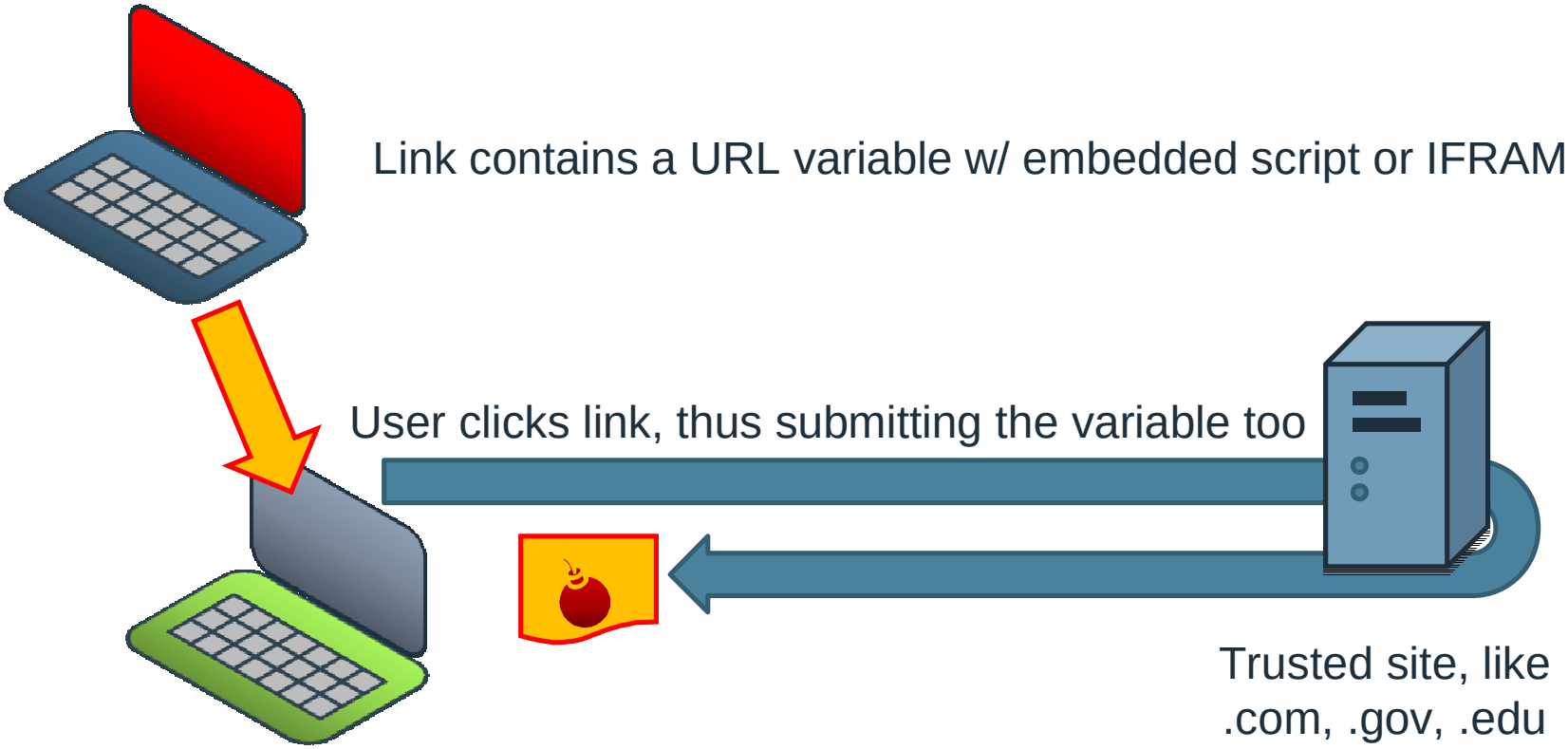

HBGary Federal

# SQL Injection




HBGary Federal

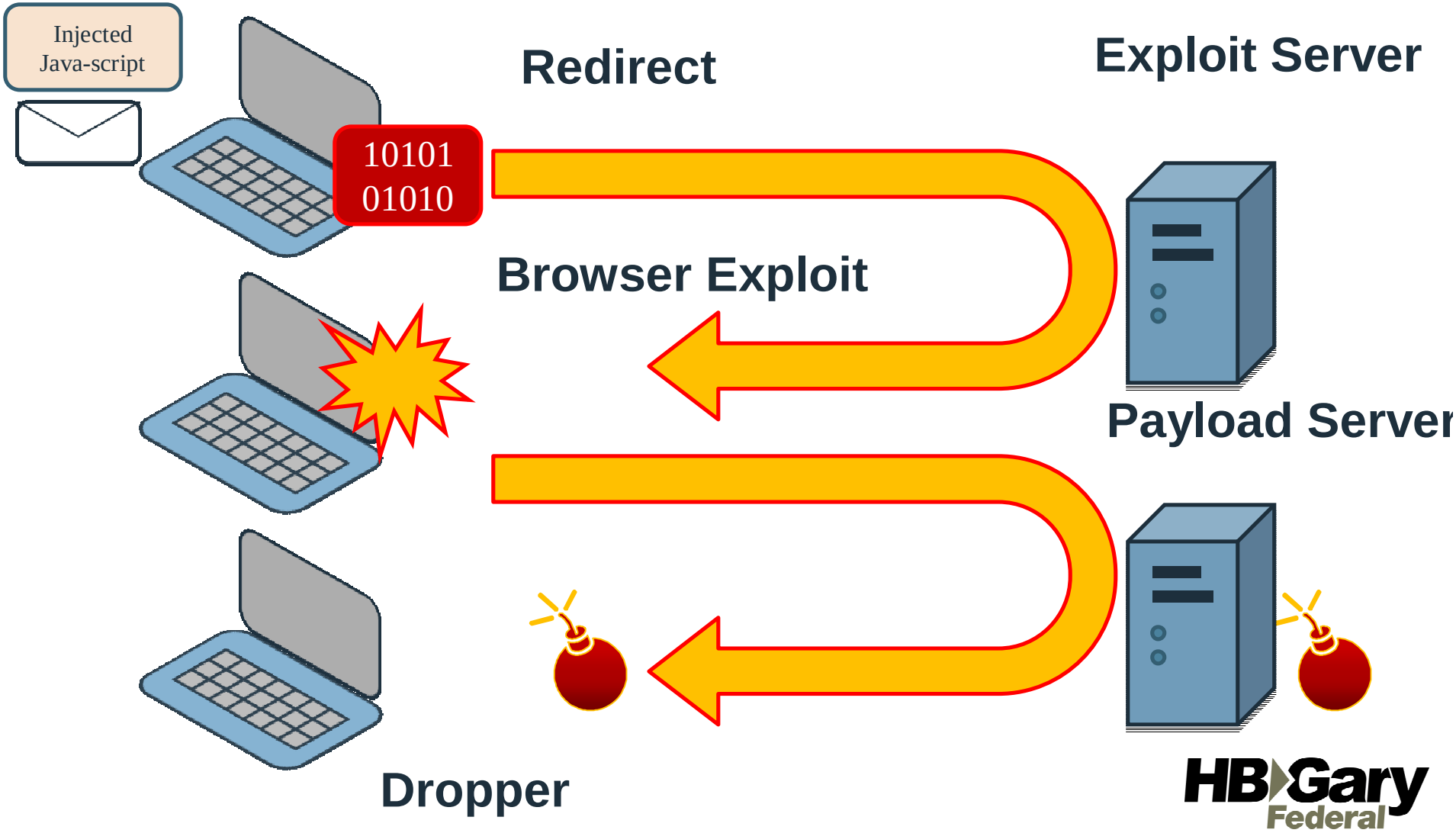
# ‘Reflected’ injection



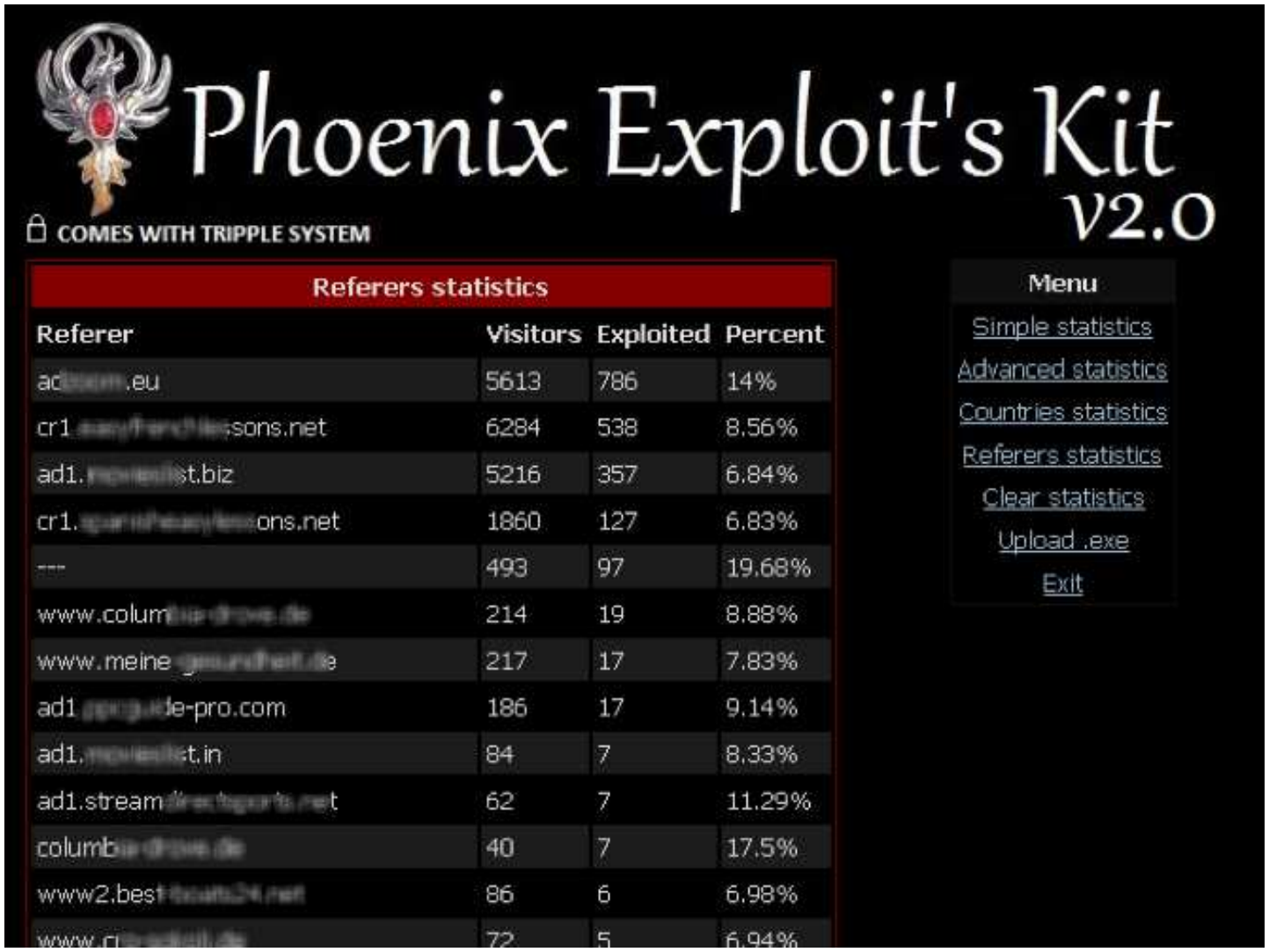

*For an archive of examples, see xssed.com

HBGary Federal

# A three step infection

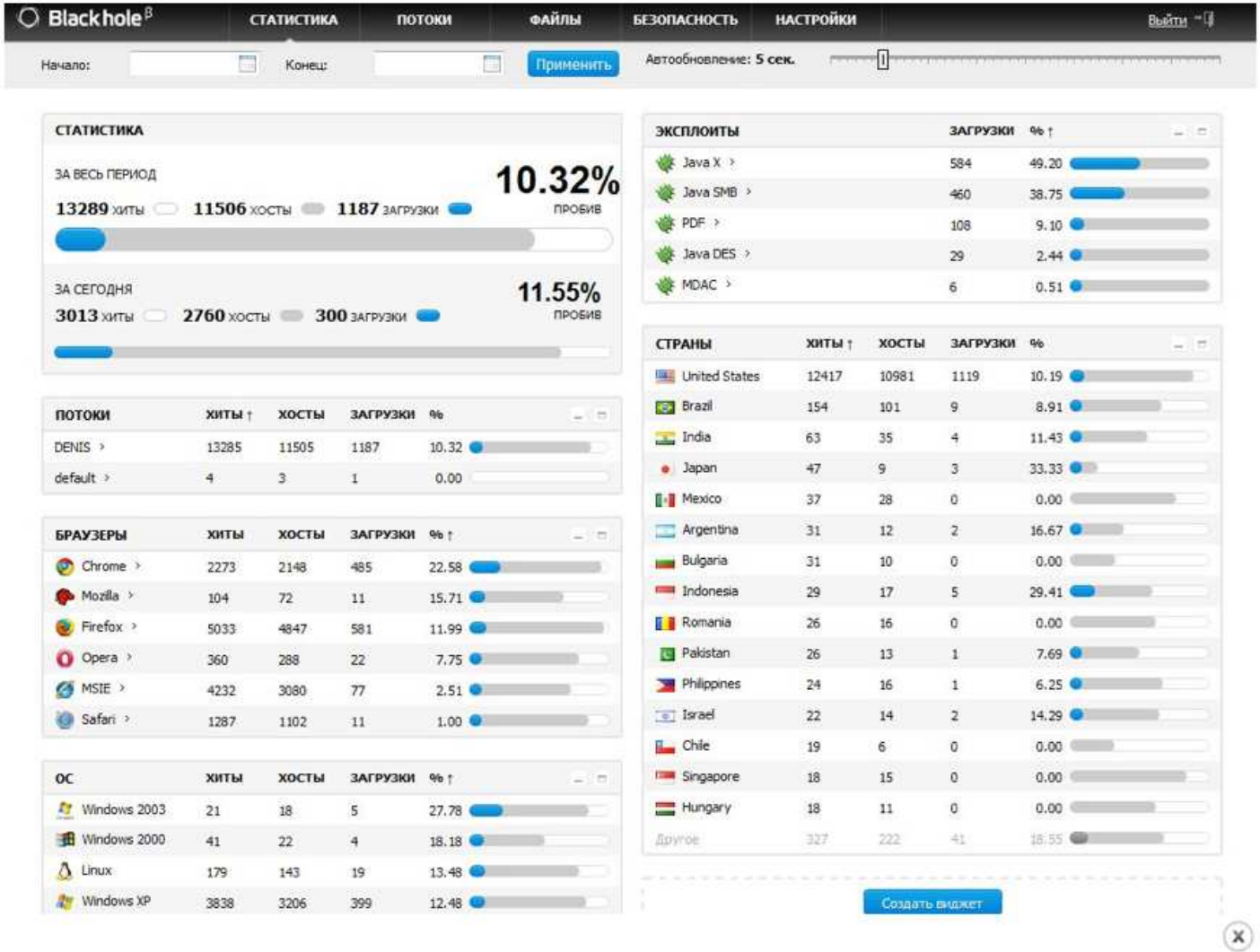


# Phoenix (exploit kit)




HBGary Federal

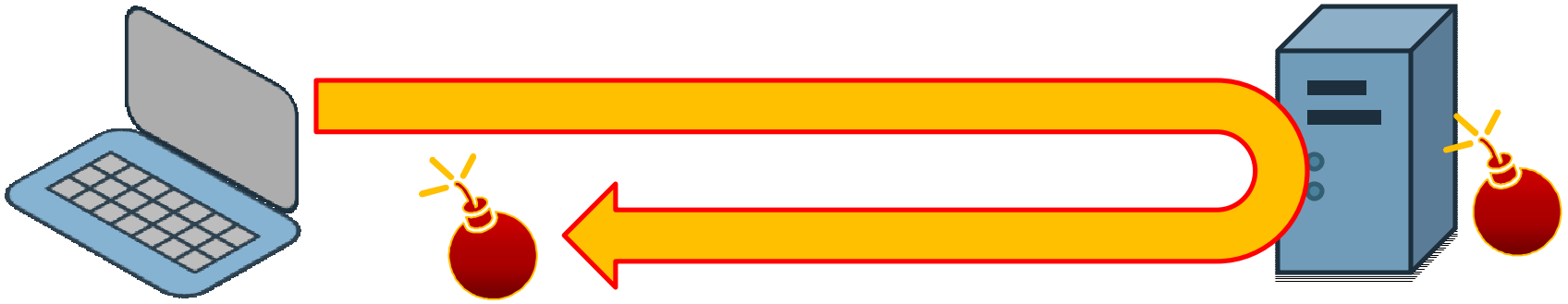
# Blackhole (exploit kit)




HBGary Federal

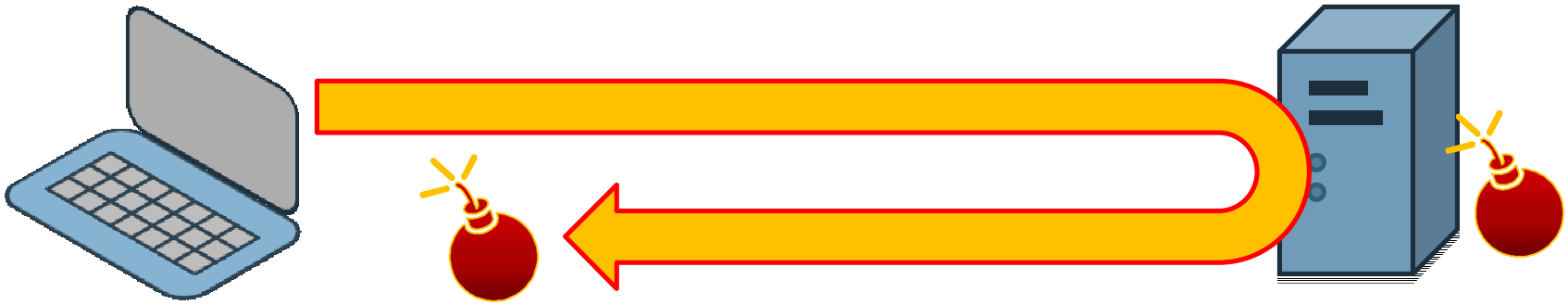
# Payload Server

- A machine that has the actual malware dropper ready for download.
- The exploit server will redirect the victim to download a binary from this location

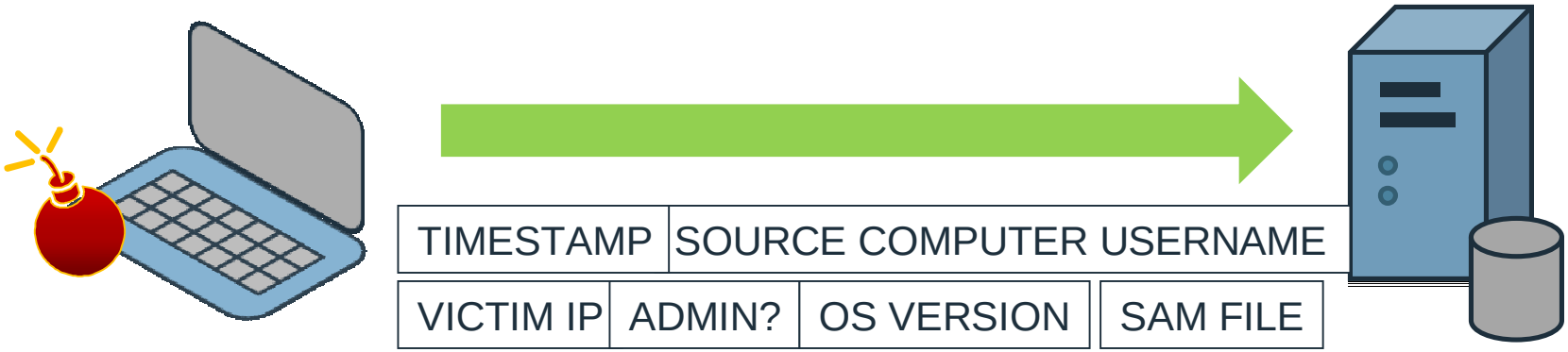


HBGary Federal

# Command and Control



Once installed, the malware phones home…



| | | | |
|---|---|---|---|
| TIMESTAMP | SOURCE COMPUTER USERNAME | | |
| VICTIM IP | ADMIN? | OS VERSION | SAM FILE |
| HD SERIAL NUMBER | SECURITY SOFTWARE | | |
| USER NAMES & PASSWORDS | | | |

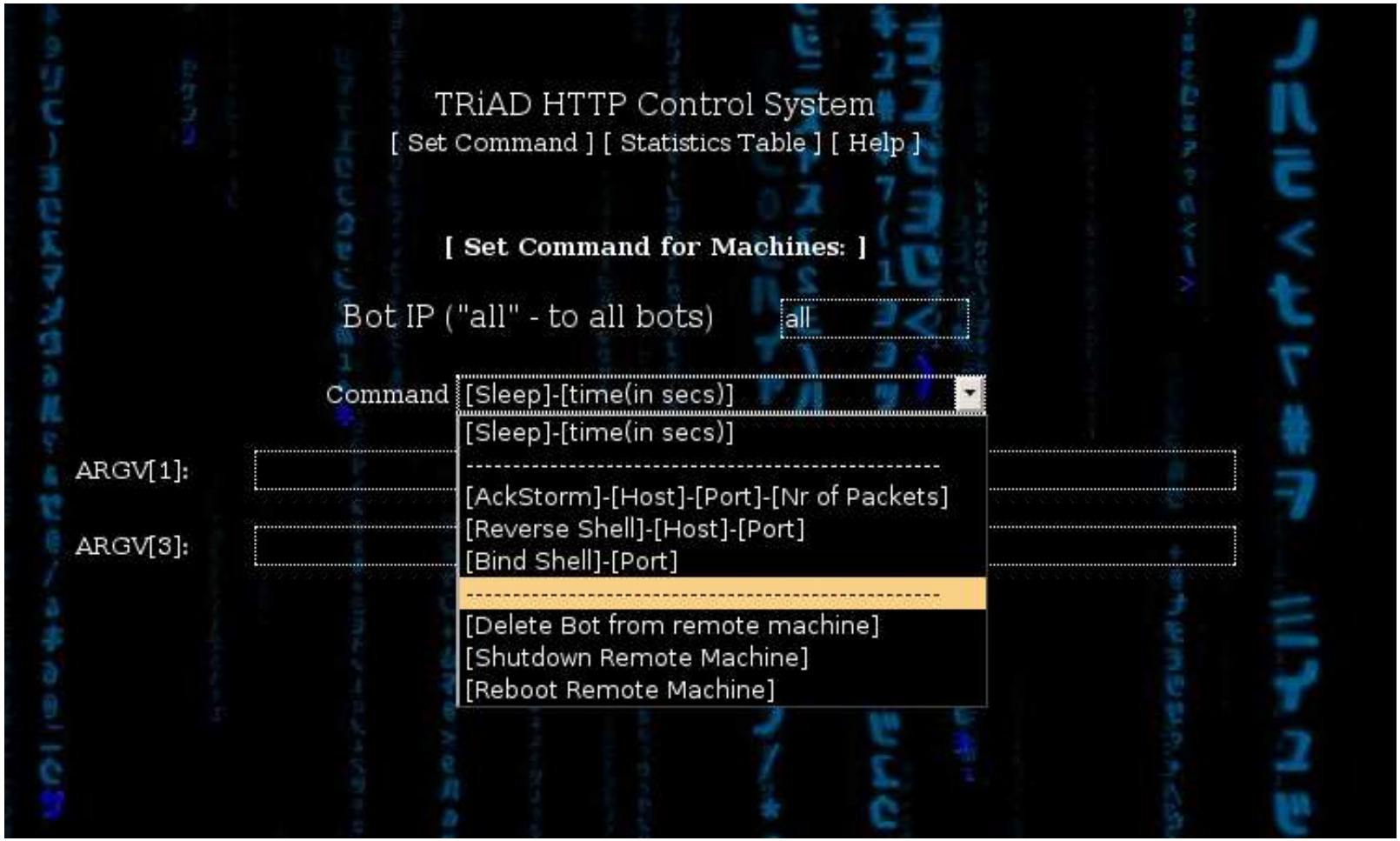
HBGary Federal

# C&C Server

- The C&C system may vary
  - Custom protocol (Aurora-like)
  - Plain Old Url's – Very Hard to Identify
  - IRC (not as common today)
  - Stealth / embedded in legitimate traffic
  - Automation
  - DynDNS
- Machine identification
  - Stored infections in a back end SQL database

HBGary Federal

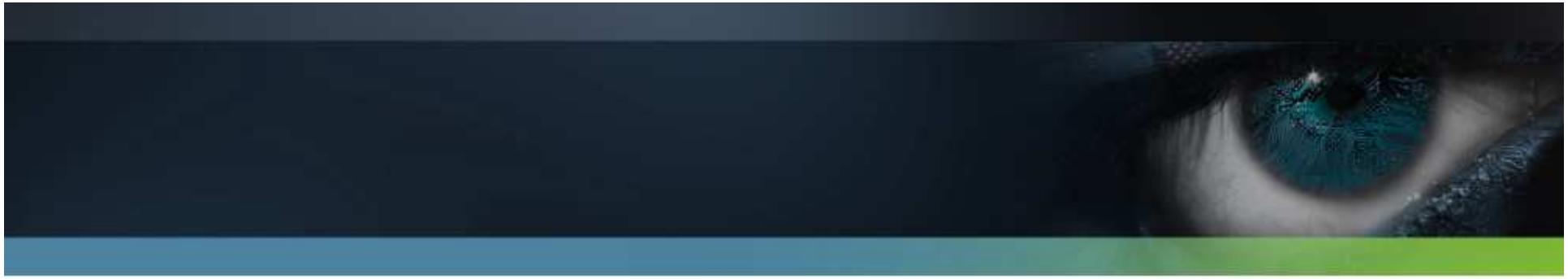
# Triad (botnet)




HBGary Federal

# ZeuS (botnet)


HBGary Federal



CP :: Bots

**Information:**

Current user: russian
GMT date: 15.10.2009
GMT time: 19:16:17

**Statistics:**

Summary
OS

**Botnet:**

→ Bots

**Reports:**

Search in database
Search in files

Logout

**Filter**

| | | | |
|---|---|---|---|
| Bots: | | NAT status: | Outsi |
| Botnets: | | Online status: | Onlin |
| IP-addresses: | | Install status: | - |
| Countries: | ru | Used status: | - |
| | | Comments status: | - |

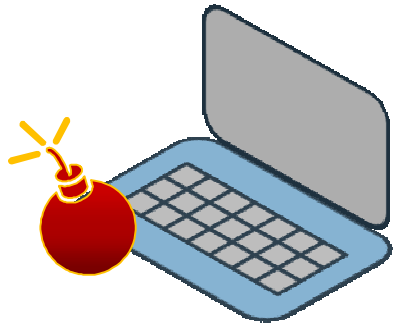
**Result (31):**

Bots action: Check socks >>

| # | Bot ID | Botnet | Version | IPv4 | Country | ↑ Online |
|---|---|---|---|---|---|---|
| 1 | server_01df59ed | tch | 1.3.1.1 | 92.61.24.60 | RU | 81:2 |
| 2 | microsof_f007b4_02660862 | tch | 1.3.1.1 | 77.245.119.153 | RU | 57:1 |
| 3 | athlon_011fee44 | tch | 1.3.1.1 | 94.181.102.60 | RU | 38:5 |
| 4 | microsof_ad86f1_00038ee3 | tch | 1.3.1.1 | 94.181.125.33 | RU | 16:0 |
| 5 | dom_5404f68e72f_00036775 | tch | 1.3.1.1 | 95.78.86.81 | RU | 13:0 |
| 6 | loner_xp_0001e25c | tch | 1.3.1.1 | 88.80.39.164 | RU | 11:1 |
| 7 | tycoon_ada54ca2_0001bf92 | tch | 1.3.1.1 | 81.20.174.80 | RU | 10:1 |
| 8 | alexiz6_014408f1 | tch | 1.3.1.1 | 94.181.119.193 | RU | 10:1 |
| 9 | microsof_1b0ea1_00026ff6 | tch | 1.3.1.1 | 94.181.111.163 | RU | 08:5 |
| 10 | microsof_01fb7c_002d12a2 | tch | 1.3.1.1 | 92.241.227.220 | RU | 06:3 |
| 11 | microsof_beb7c0_0001e867 | tch | 1.3.1.1 | 92.241.254.170 | RU | 06:3 |
| 12 | microsof_658578_00006b7b | tch | 1.3.1.1 | 78.85.109.72 | RU | 06:0 |
| 13 | krasnoar_46e2cb_0040cb67 | tch | 1.3.1.1 | 92.241.251.131 | RU | 05:4 |

HBGary Federal

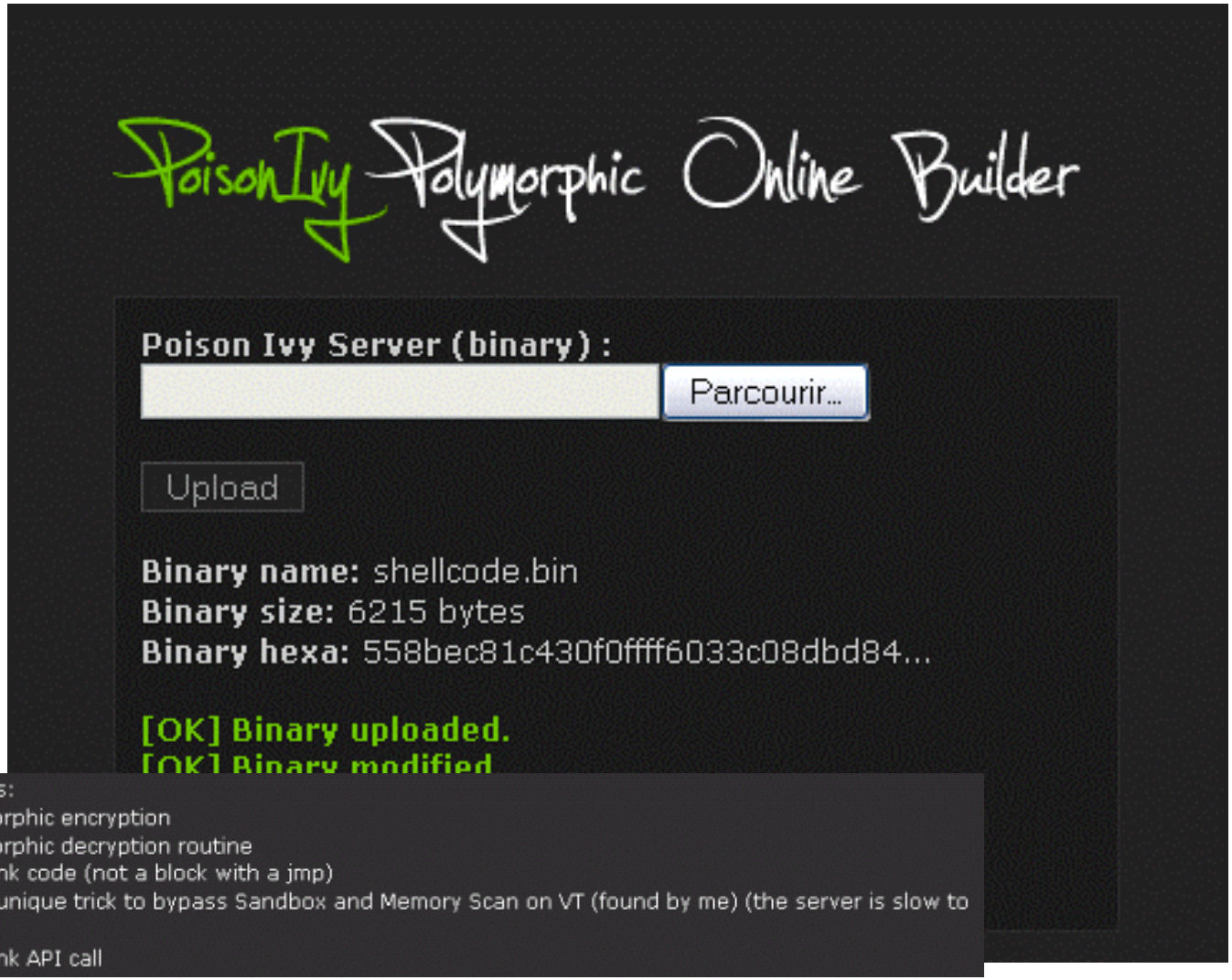
# Implants & Persistence



- The ‘persistent’ backdoor program
- Hide in plain sight strategy
  - Some DLL that to the trained eye looks normal
- General purpose hacking tool
- Stealth capabilities
- In-field update capabilities

HBGary Federal

# Poison Ivy (implant)

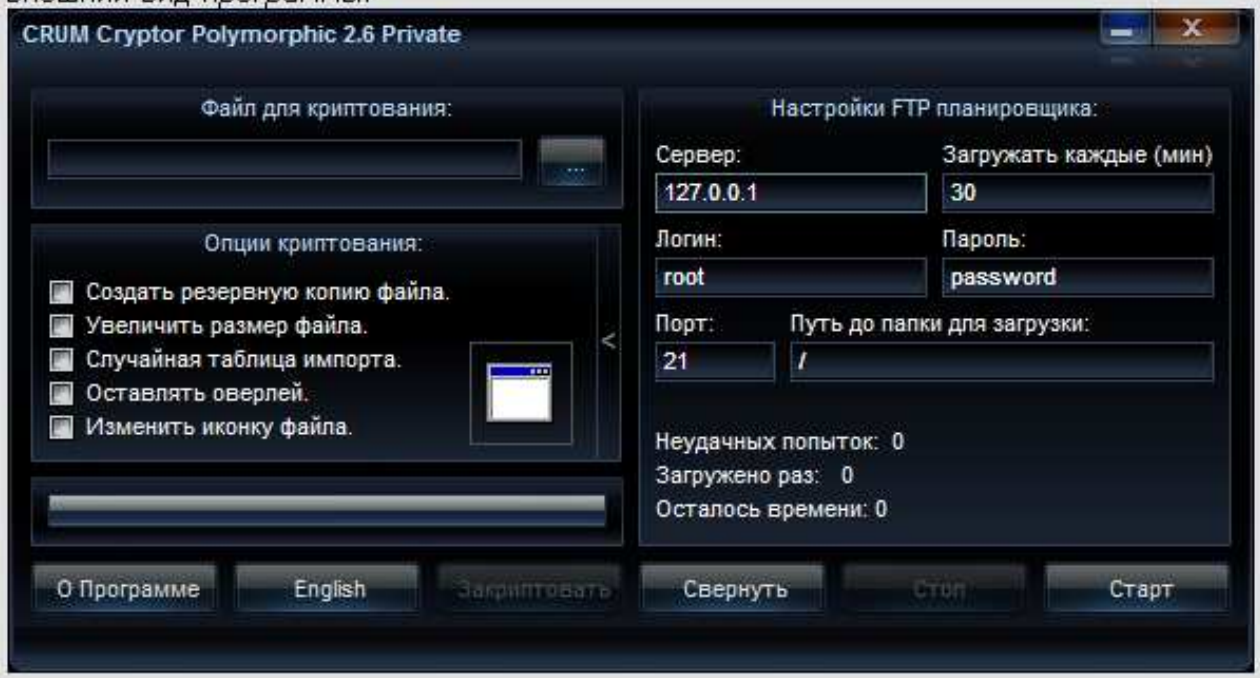



HBGary Federal

# CRUM (protector)

**CRUM Cryptor Polymorphic v. 2.6** new!

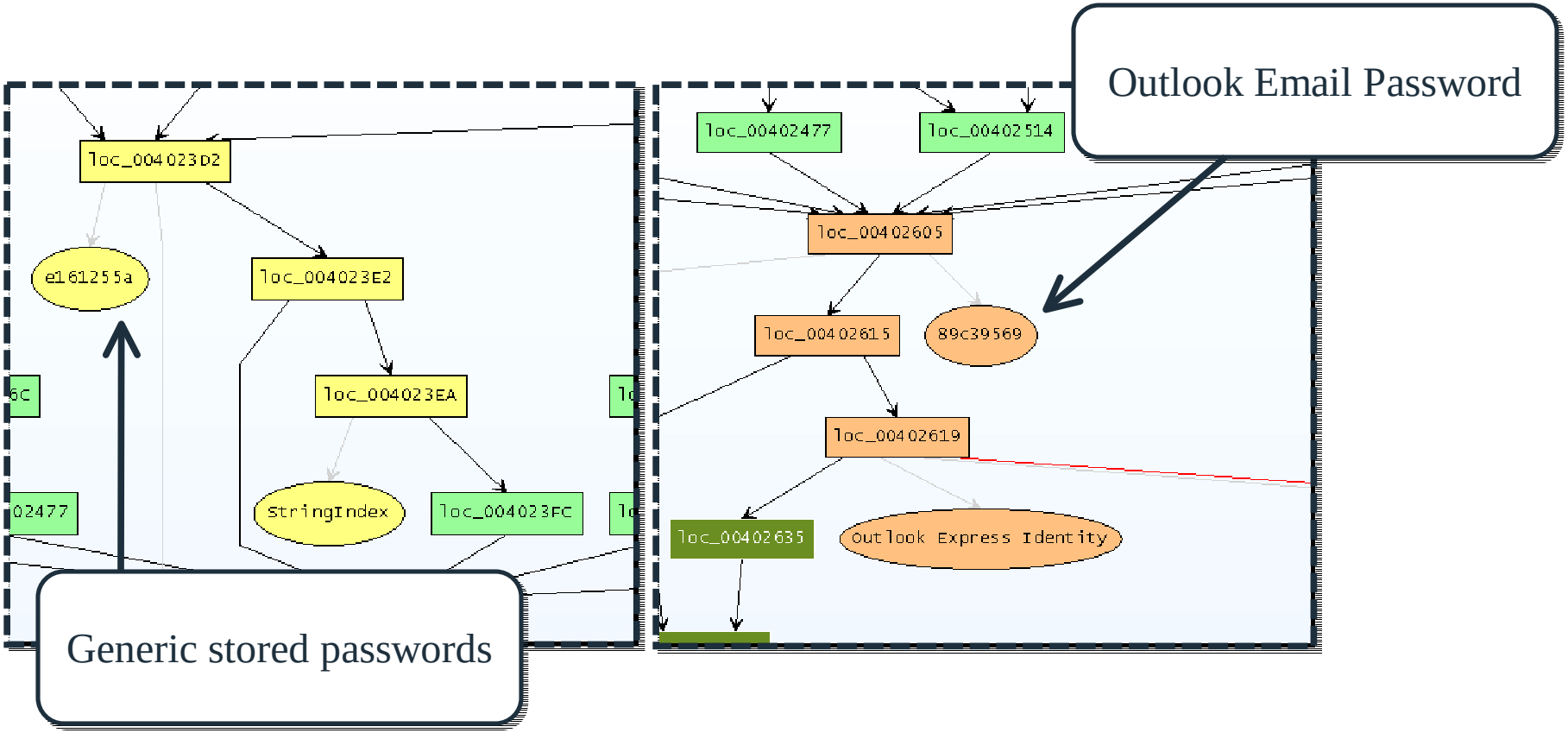
*Внешний вид программы:*




**Цена:** 200$

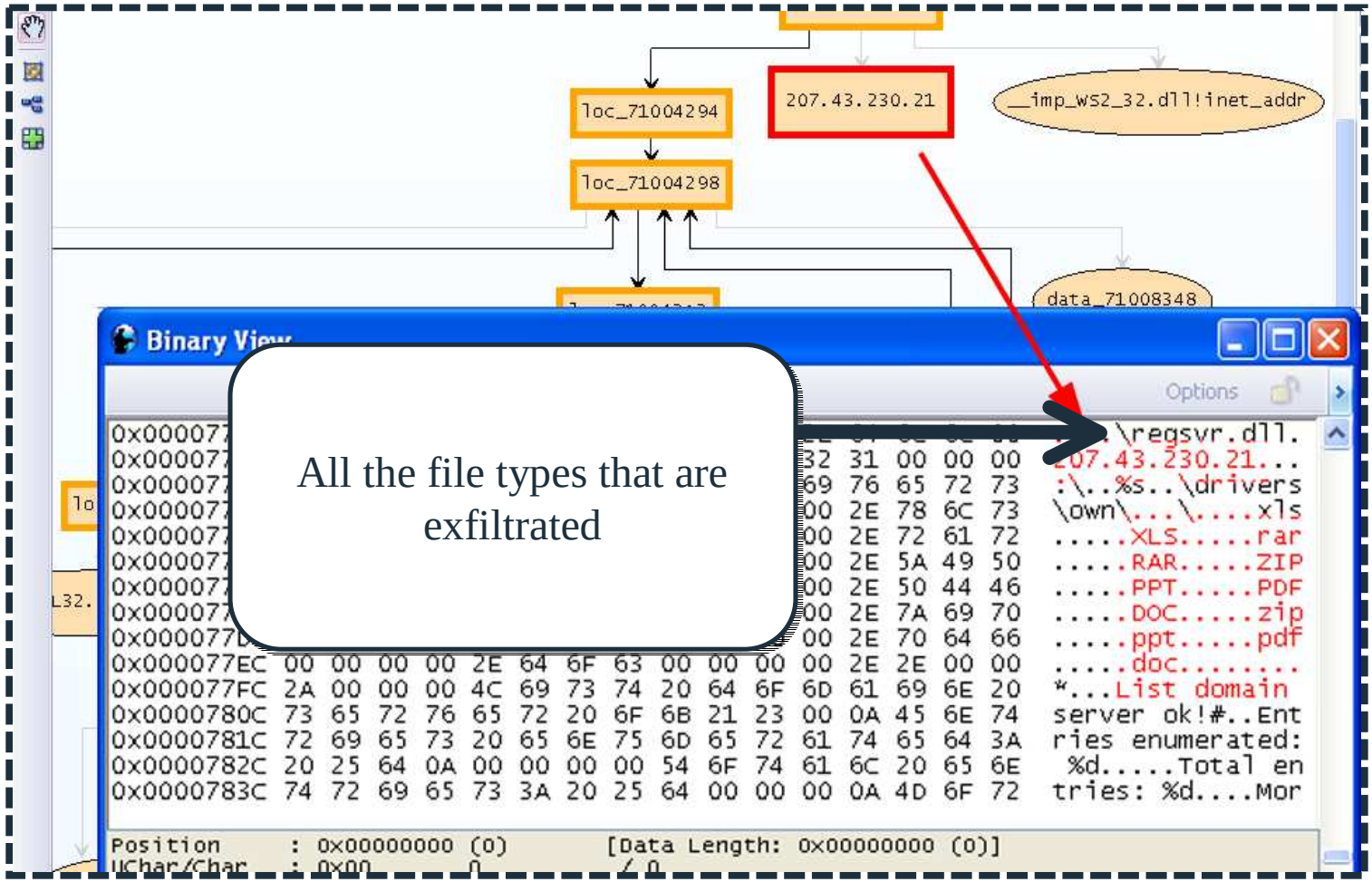
HBGary Federal

# Steal Credentials




HBGary Federal

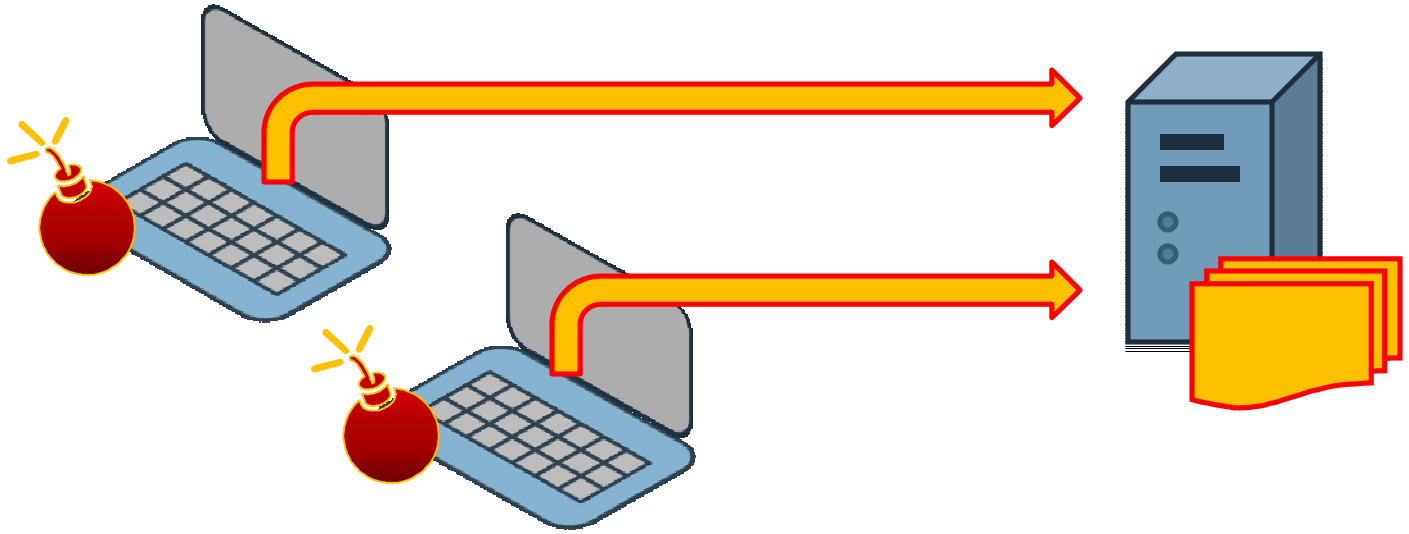
# Steal Files




HBGary Federal

# Staging Server

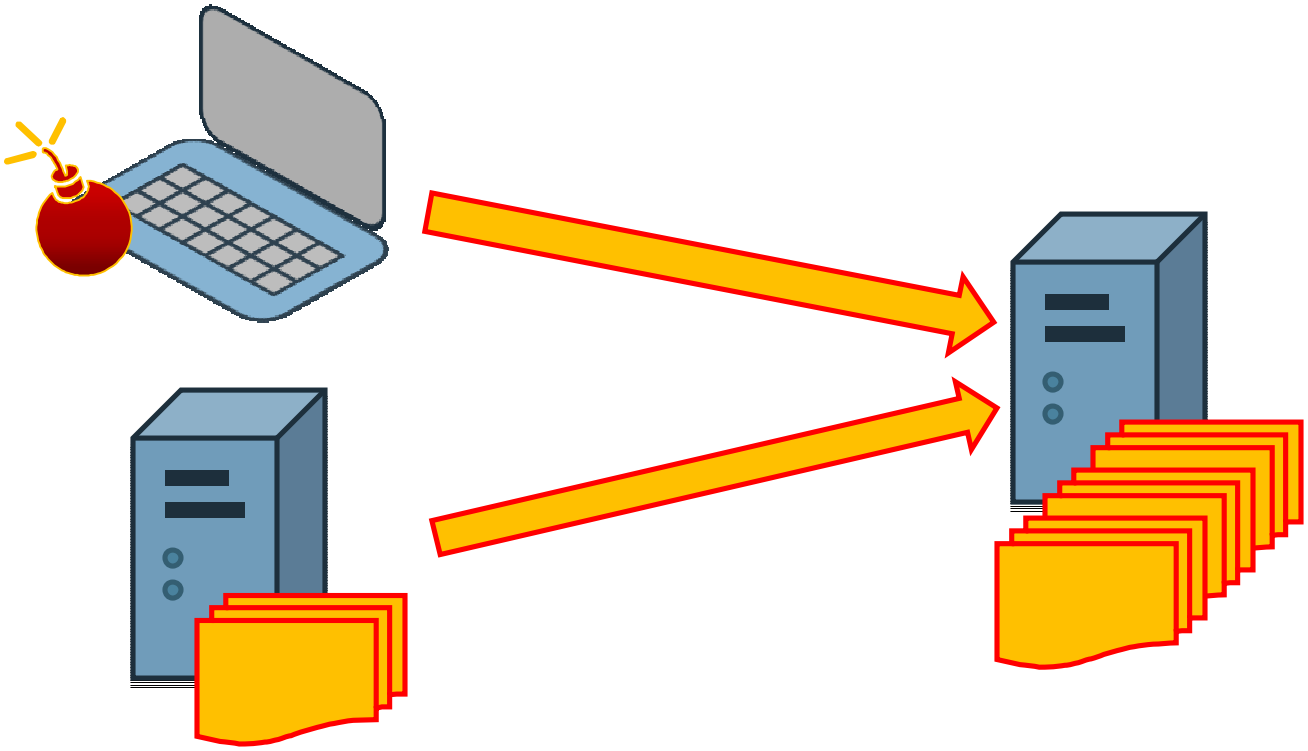
- A place to store all the stolen goods before it gets ‘exfiltrated’
  - Data is moved off the network in a variety of ways – ‘Hacking Exposed’ level behavior



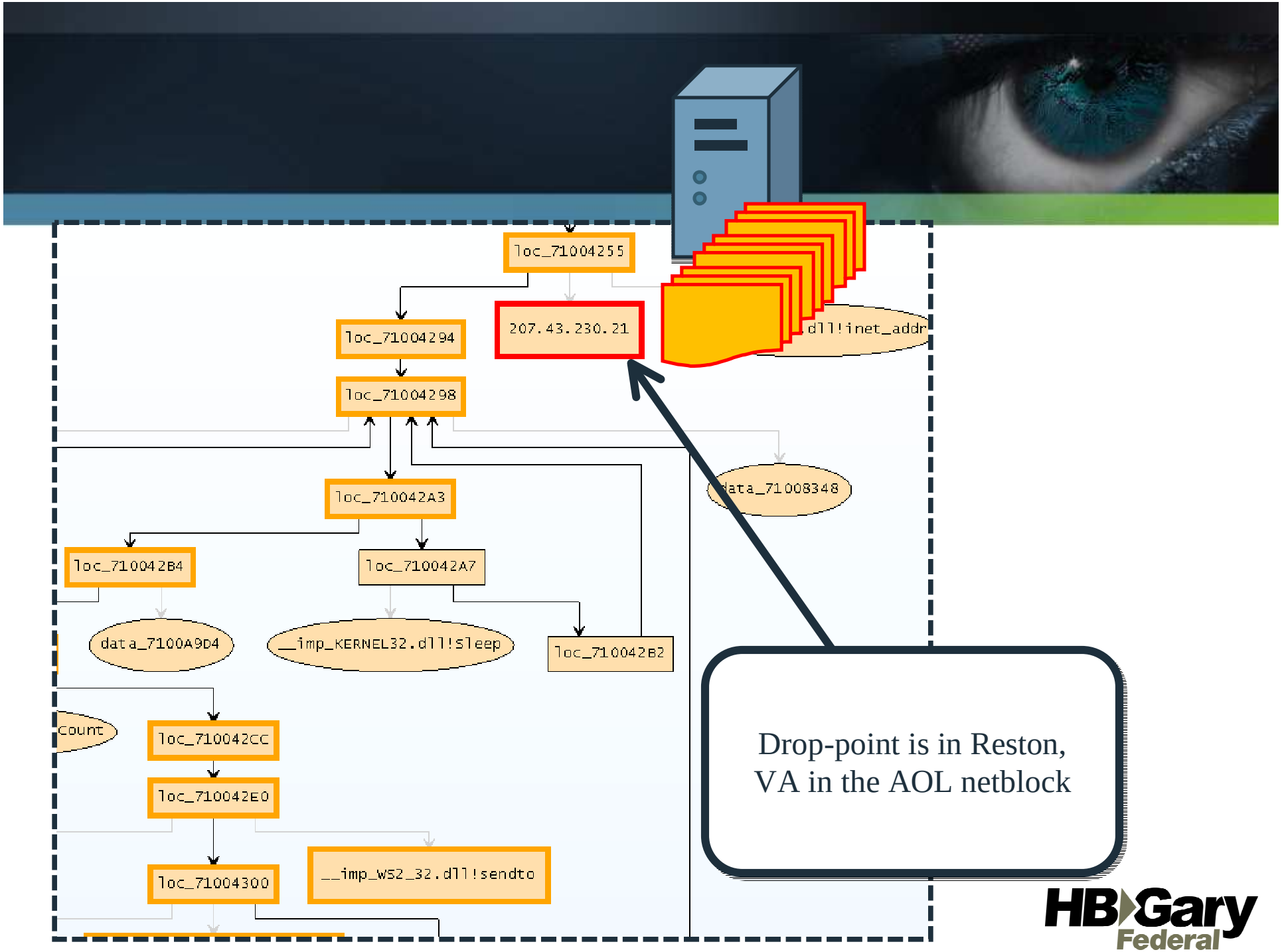
HBGary Federal

# Drop Site

- Sometimes the stolen data is moved to a tertiary system, *not the same as the C&C*



HBGary Federal




HBGary Federal

# A New Age in Malware

- In July 2010 a Belarus-based security company discovered a new worm on computers belonging to an Iranian client.
- Targets the Siemens WinCC/PCS 7 SCADA system.
- Many unique features
- Most sophisticated malware ever discovered.

HBGary Federal

# Stuxnet FAQ

- 4 Zero Days
- 2 Acquired Digital Certificates
- First PLC rootkit.
- Self-propagation and direction (AI).

- This took a team of developers months.
- But the technical details are not the important part.

HBGary Federal

# Stuxnet Deconstructed

- Political/national security likely motivation.
- Lots of moving parts from planning, ISR, hardware acquisition, development, and human assets used for deployment.
- Malware that bridges the gap between logical and physical control and manipulation.
- Destroying power facilities, water treatment, emergency services – no longer a theory.

HBGary Federal

# Changes Everything

- In this new environment traditional capabilities are useless.
  - Designed for 100% chance of initial success
  - No C&C
  - Bypass existing security mechanisms
  - Incorporated with other resources.
    - Supply Chain
    - Human Asset

HBGary Federal

# Detect and Respond

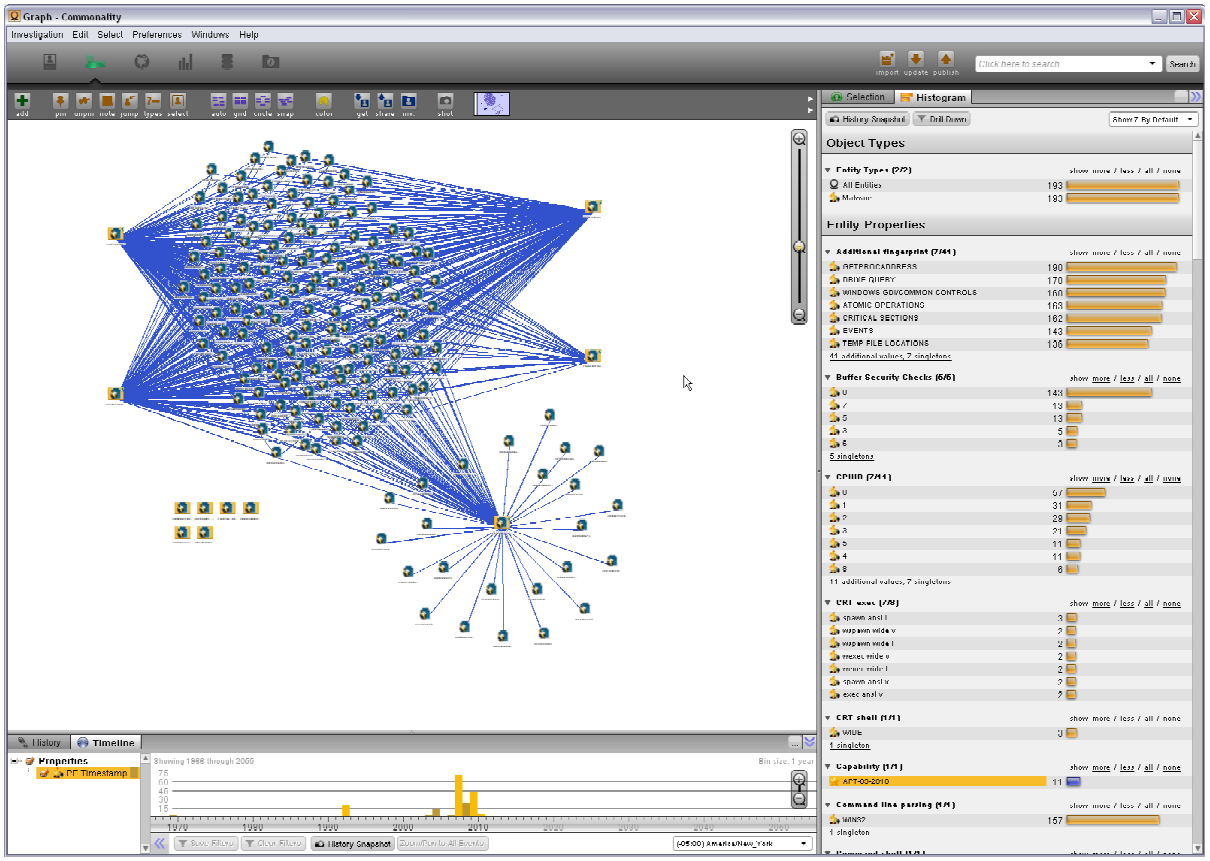
HBGary Federal

# Detect and Respond

- Compromise is inevitable and continual.
- Detect threats and respond rapidly.
  - Threat Intelligence
    - Artifacts
    - Markers
    - Social
  - Continuous Incident Response
    - Technology
    - Process

HBGary Federal

# Threat Intelligence

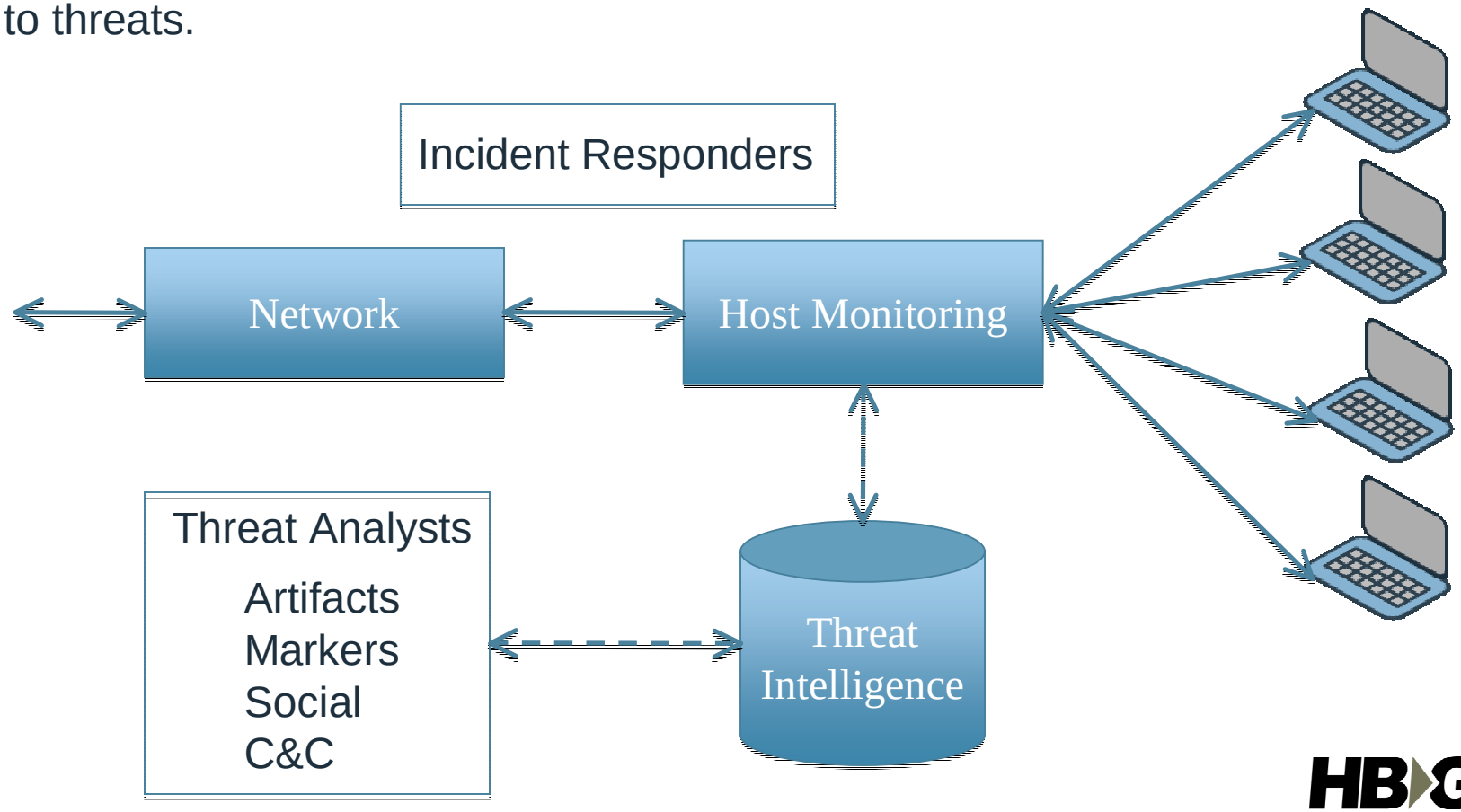



- End Point
  - Physical Memory
  - Physical Disk
  - Live-OS
- Network
- C&C
- Open Source

HBGary Federal

# Incident Response

Continuous IR. Real-time correlation of information related to threats.




HBGary Federal

# Is Attribution Possible?

# Yes

While we believe attribution to be measurably achievable this comes with some caveats, mileage may vary, not all experiences will be equal and we can not be held responsible or liable for any deviations in experiences hitherto experienced by stated security professionals.

HBGary Federal

# Threat Analysis

- Integrate cyber verticals into single data set.
- Develop larger sets of quantified artifacts and markers
  - Fingerprints
- Correlate Malware based on fingerprints
  - Statistical probabilities based on % matching fingerprints
- Develop threat maps using associated intelligence around correlated malware

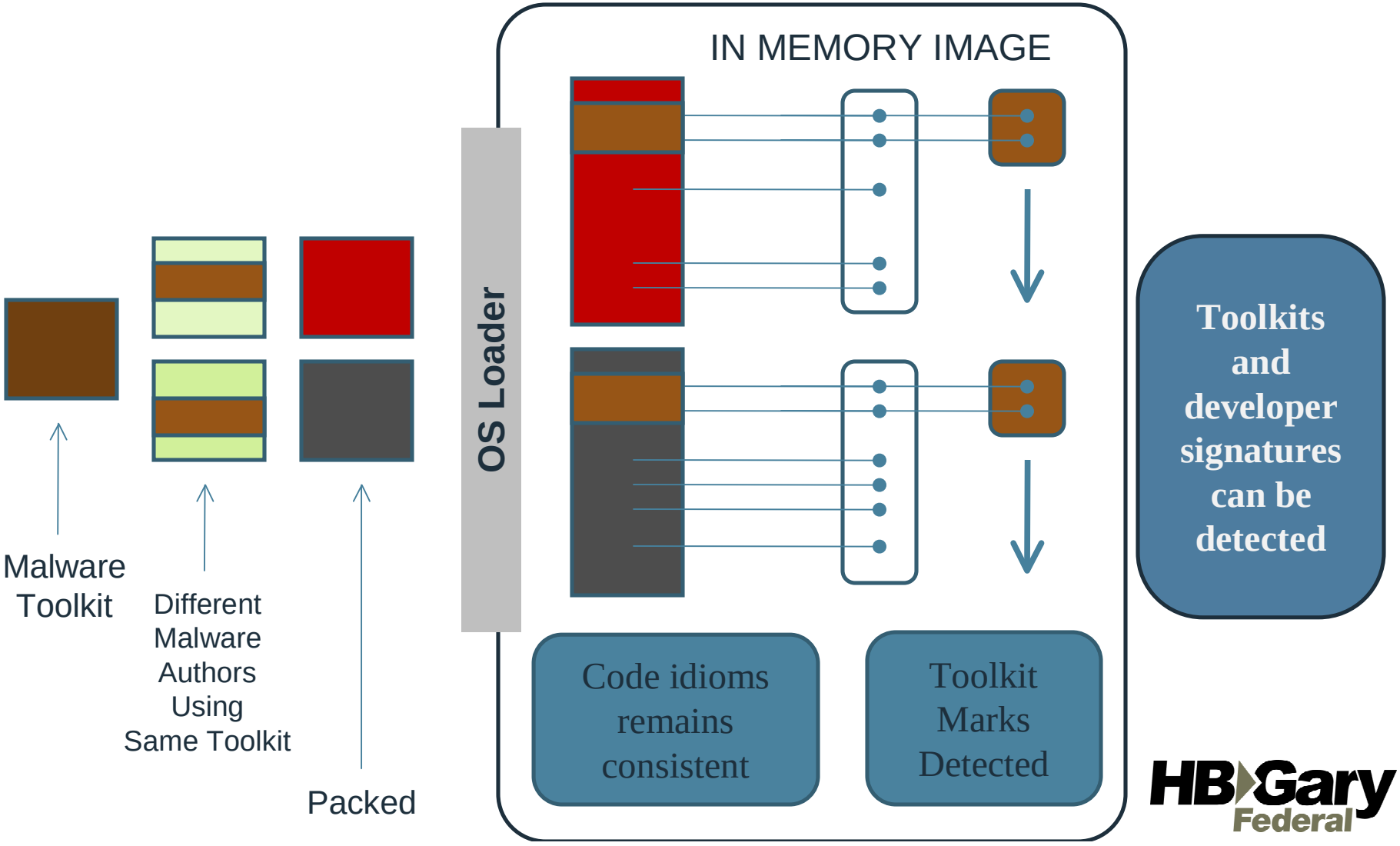
HBGary Federal

# Threat Artifacts and Forensics Markers

- People are habitual and lazy.
- Threat Artifacts are observable characteristics of specific threats.
- Forensic markers exist where software development occurs
- Threat Artifacts and Forensic markers are a good starting point to correlate malware and classify threats.

HBGary Federal

# Fingerprints



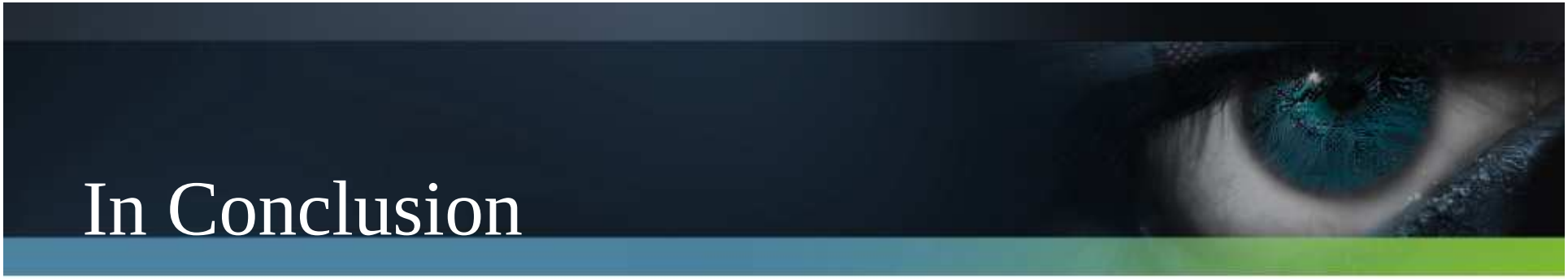

HBGary Federal

# Soft linking into the Social Space

- Where is it sold, does that location have a social space?
  - If it has a social space, then this can be targeted
  - Forum, IRC, instant messaging
- Using link-analysis, a softlink can be created between the developer of a malware product and anyone else in the social space
  - Slightly harder link if the two have communicated directly
  - If someone asks for tech support, indicates they have purchased
  - If someone queries price, etc, then possibly they have purchased

HBGary Federal

# In Conclusion



- Threats are significant and have lots of room to grow
  - This is an entrenched problem that will not go away.
  - No Magic bullets
- Can’t rely on protection, need to think beyond compliance
- Better Education – Immersive and Realistic
- Invest in intelligence and response.
  - Integrate cyber data
  - Understand threats not just vehicles of attack
  - Implement IR into daily practice - Limit Loss and Exposure

HBGary Federal

# Thank You

- Cyber Security for the Enterprise
  - Active Defense with Digital DNA – Enterprise Malware Detection, Continuous Monitoring and Response System
  - Digital DNA™ - codified detection of zero day malware
    - Integrated into several Enterprise products, McAfee ePO, Guidance EnCase, more to be announced
  - Threat Management Center – Malware processing, threat correlation and analysis.
  - Responder™ – malware analysis and physical memory forensics
  - Social Media Pen testing and Training

HBGary Federal