
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

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”.

Wake Up Call – Part II



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

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

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



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.

APT – Who is it?

State-Sponsored APT (SSAPT)



Criminal APT (CAPT)



SSAPT – Motivation?

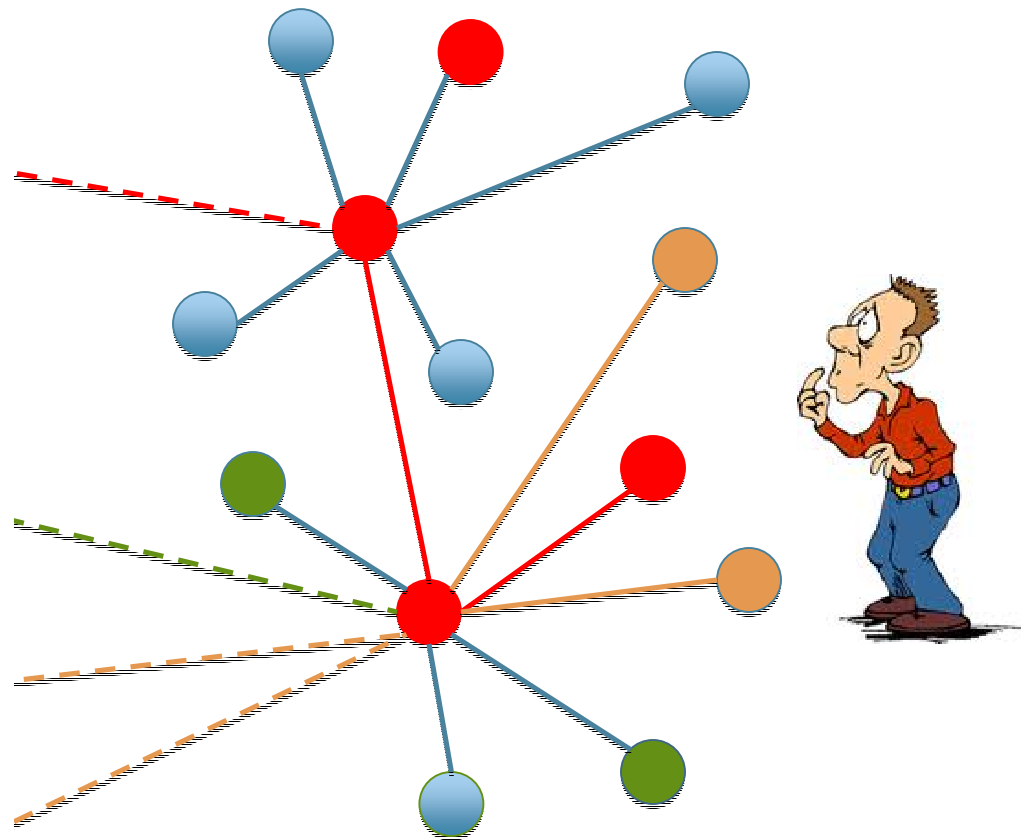
- Military
 - Land, Air, Sea, Space, and Cyberspace dominance
 - Asymmetric Warfare
- Intelligence
 - A good defense requires a good offense
 - Intelligence, Surveillance, and Reconnaissance
- Business
 - Intellectual Property



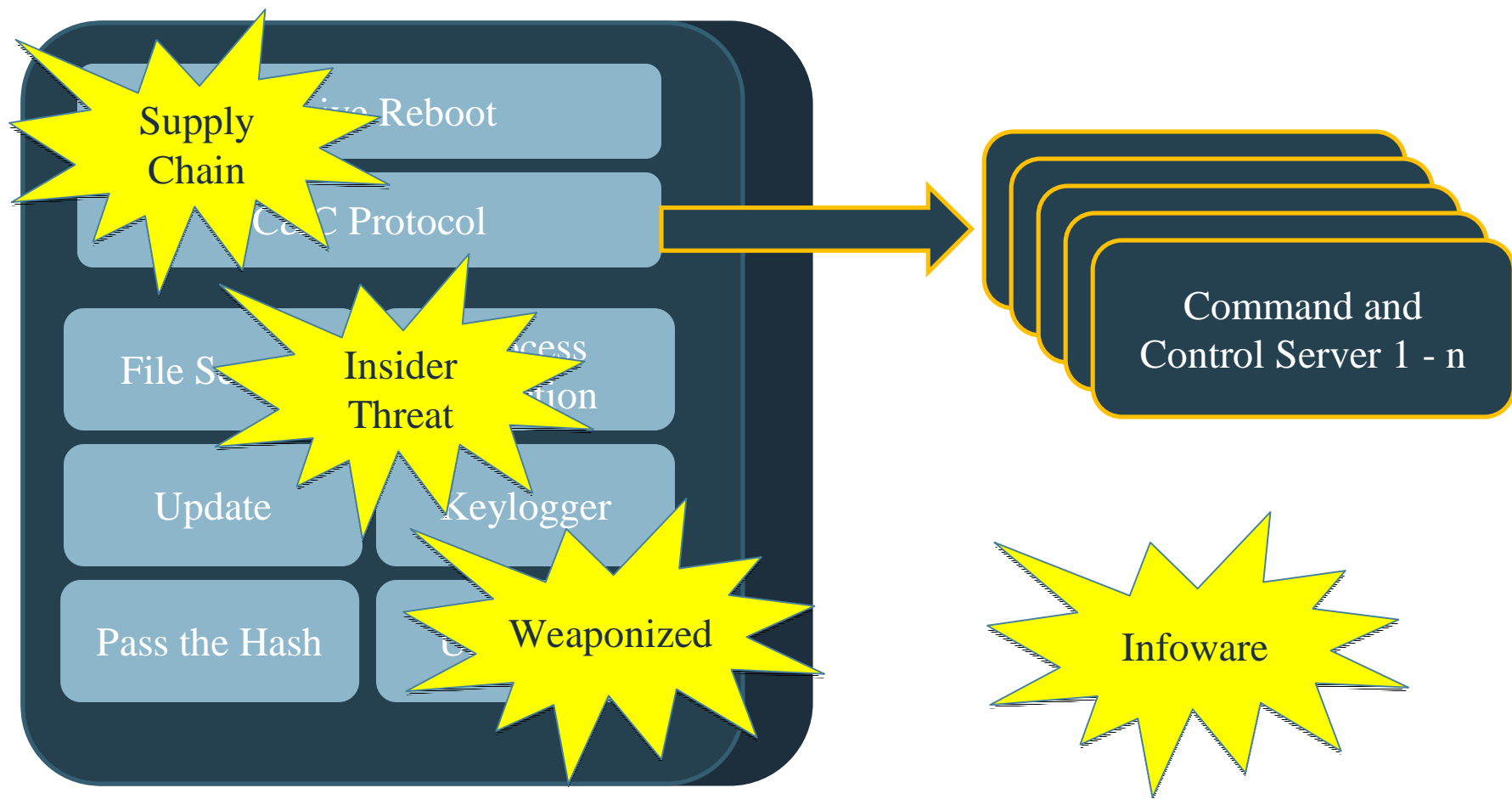
CAPT – Motivation?

- 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.

Its All Very Confusing



Anatomy of APT Malware





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

Social Media Guy

facebook

Likes Redskins
Friends with ...
Lives in Columbia, MD



Linked in

Acme Contractor
Navy Cryptologist
Member Intelligence Group

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>

foursquare

Checked in at
NSA Visitor Parking

...thank you, thank you very much

HB Gary
Federal



Future Landscape

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



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



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.



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.



Why Enterprise Security Products DON'T WORK

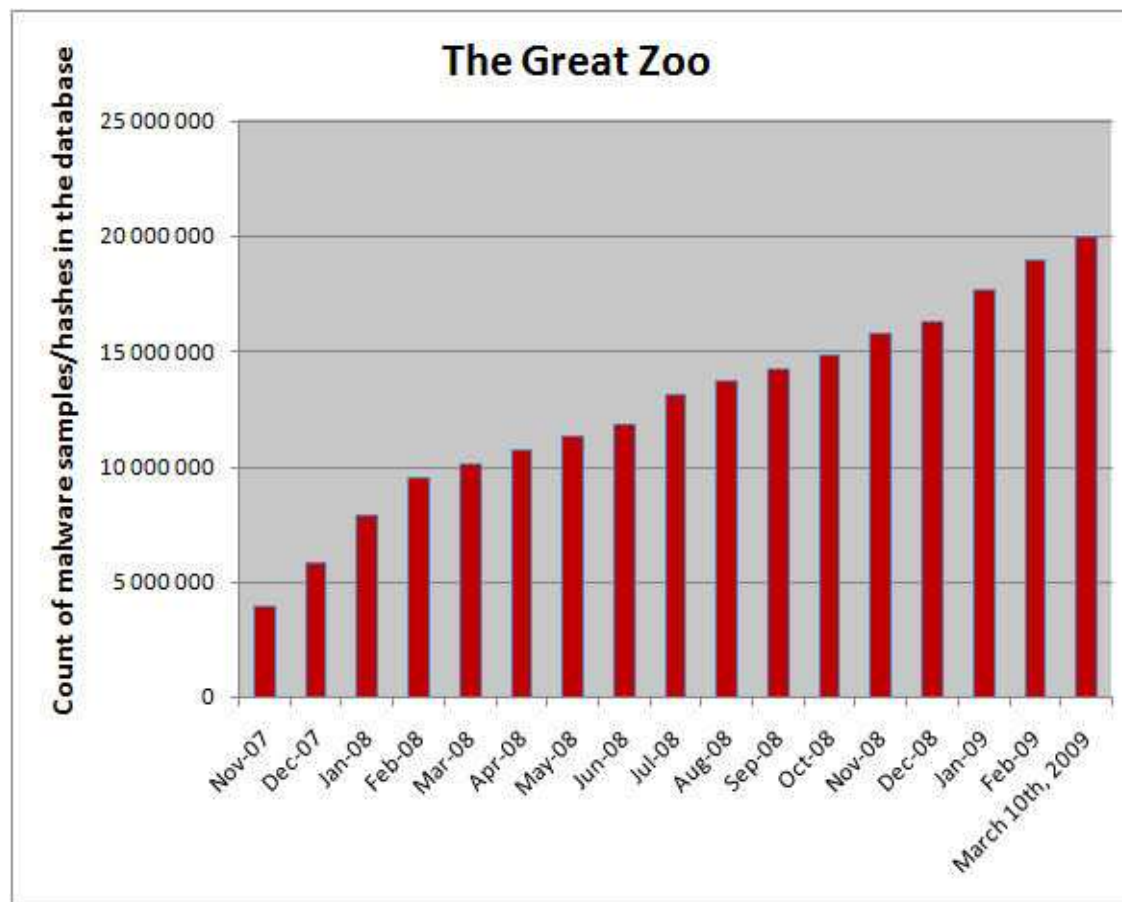


The True Threat

- 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

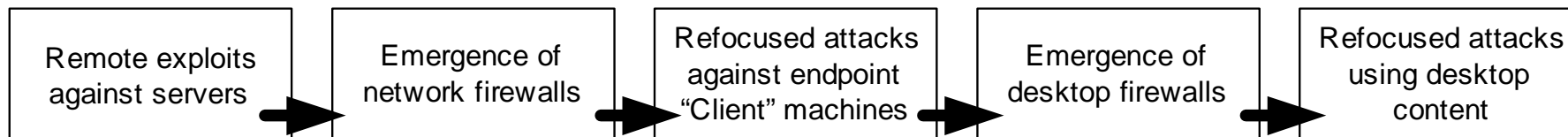
Scale

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



Surface

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



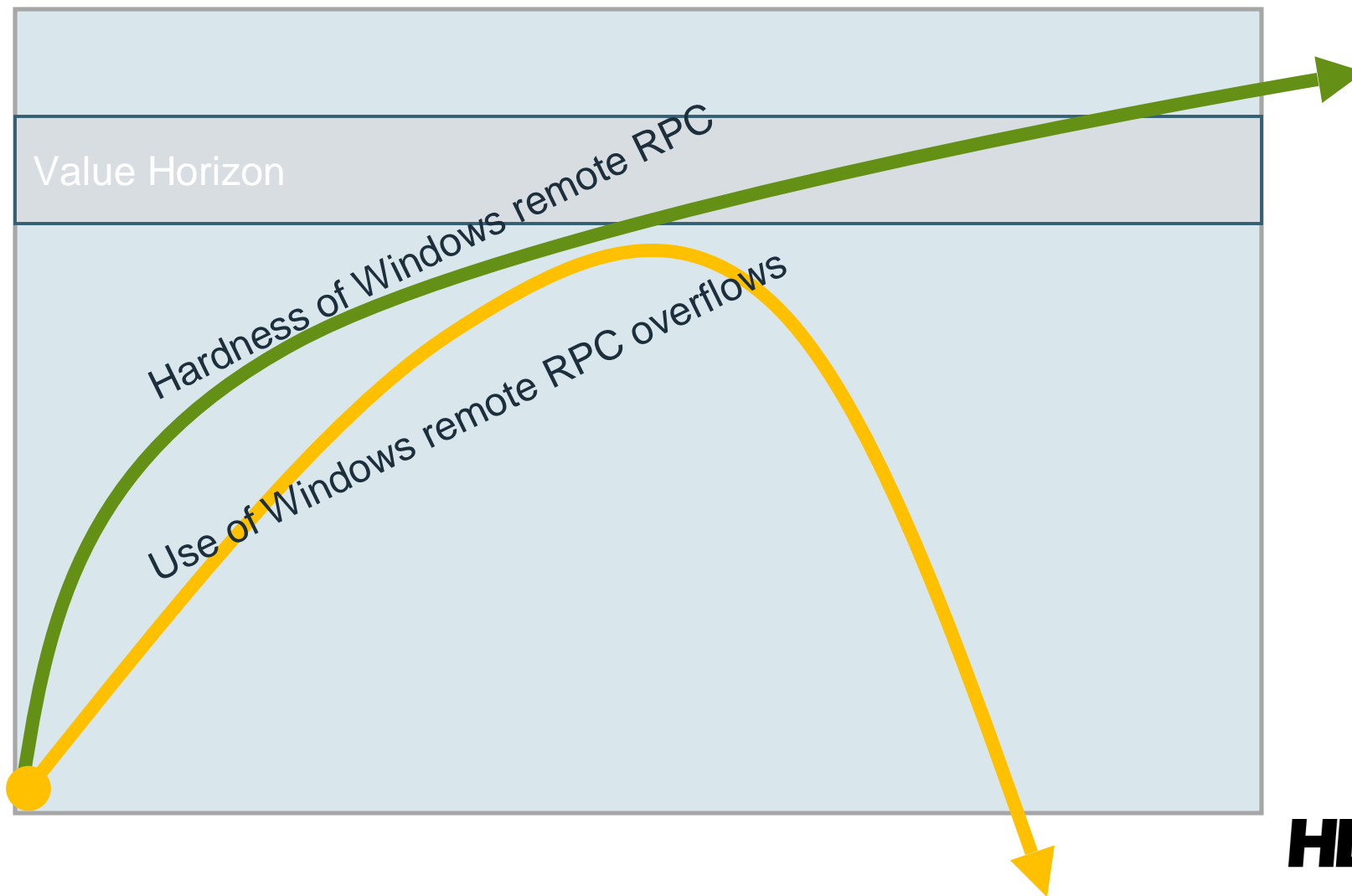
The bad guys STILL HAVE their zero day, STILL HAVE their vectors, and STILL HAVE their malware



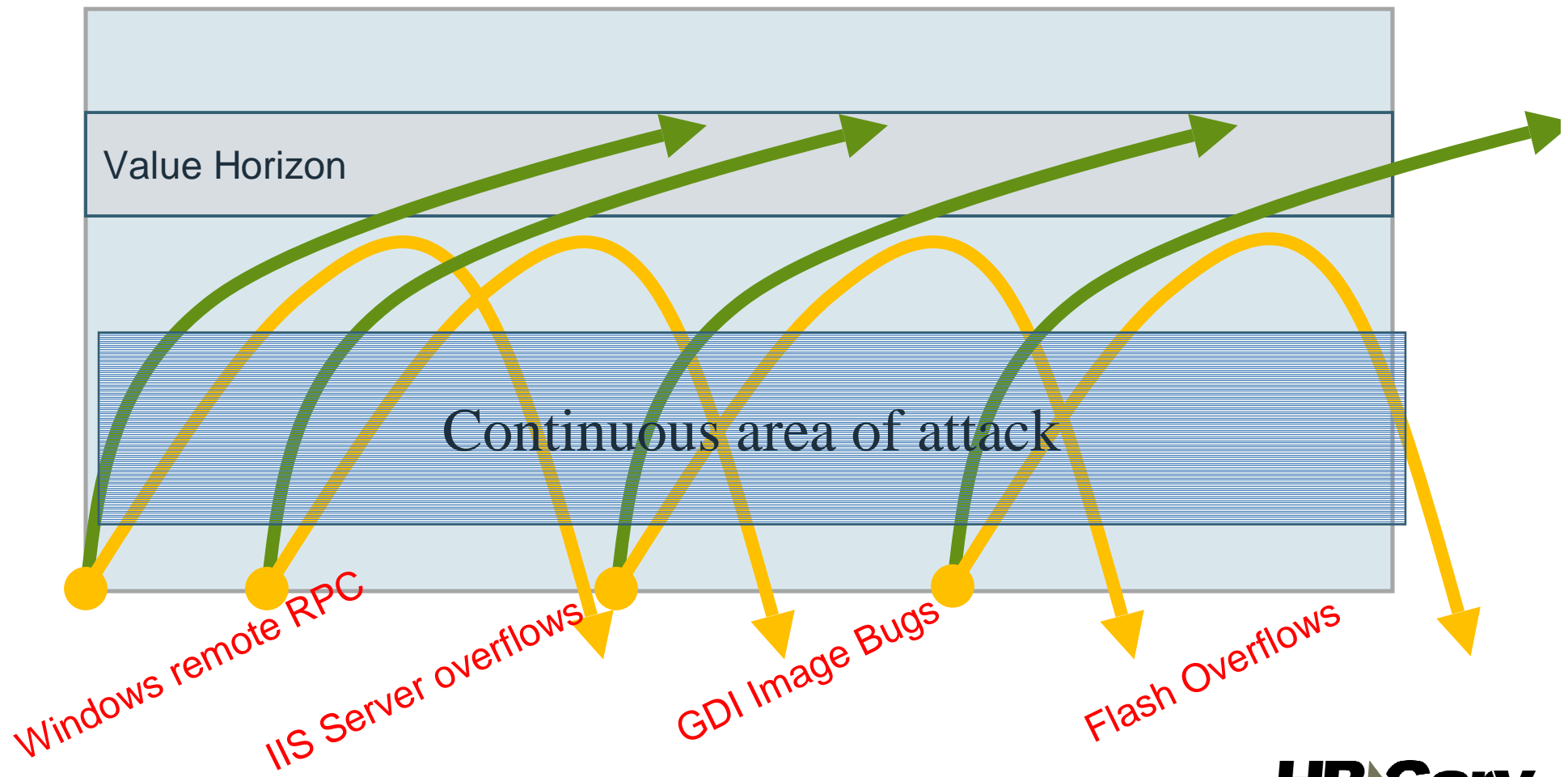
Not an Anti-Virus Problem

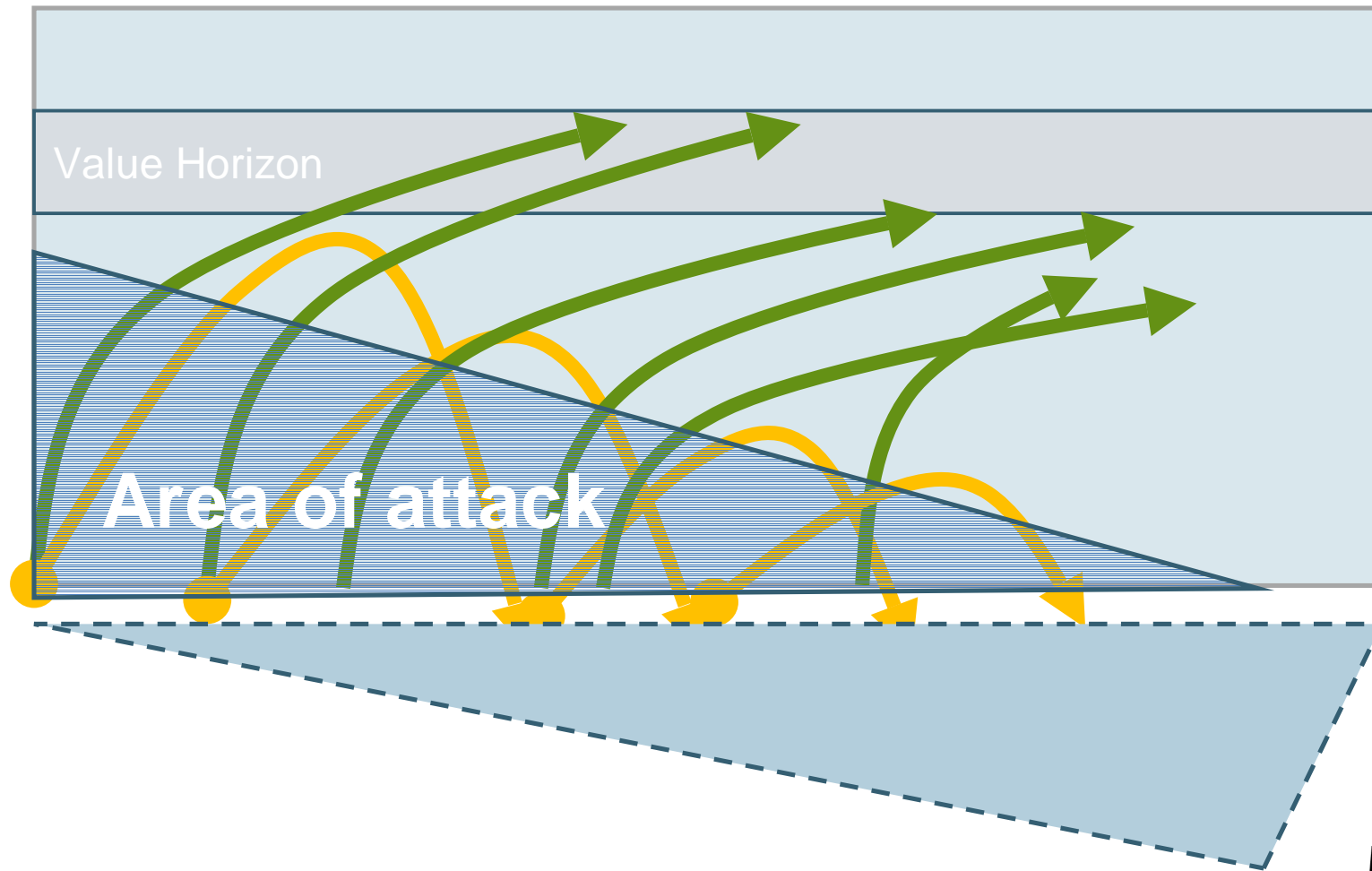
- Malware isn't released until it bypasses AV products
 - Testing against AV is part of the QA process
- AV doesn't address the actual threat – the human who is targeting you
- AV has been shown as nearly useless in stopping the threat
 - AV has been diminished to a regulatory checkbox – it's not even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

Annealing



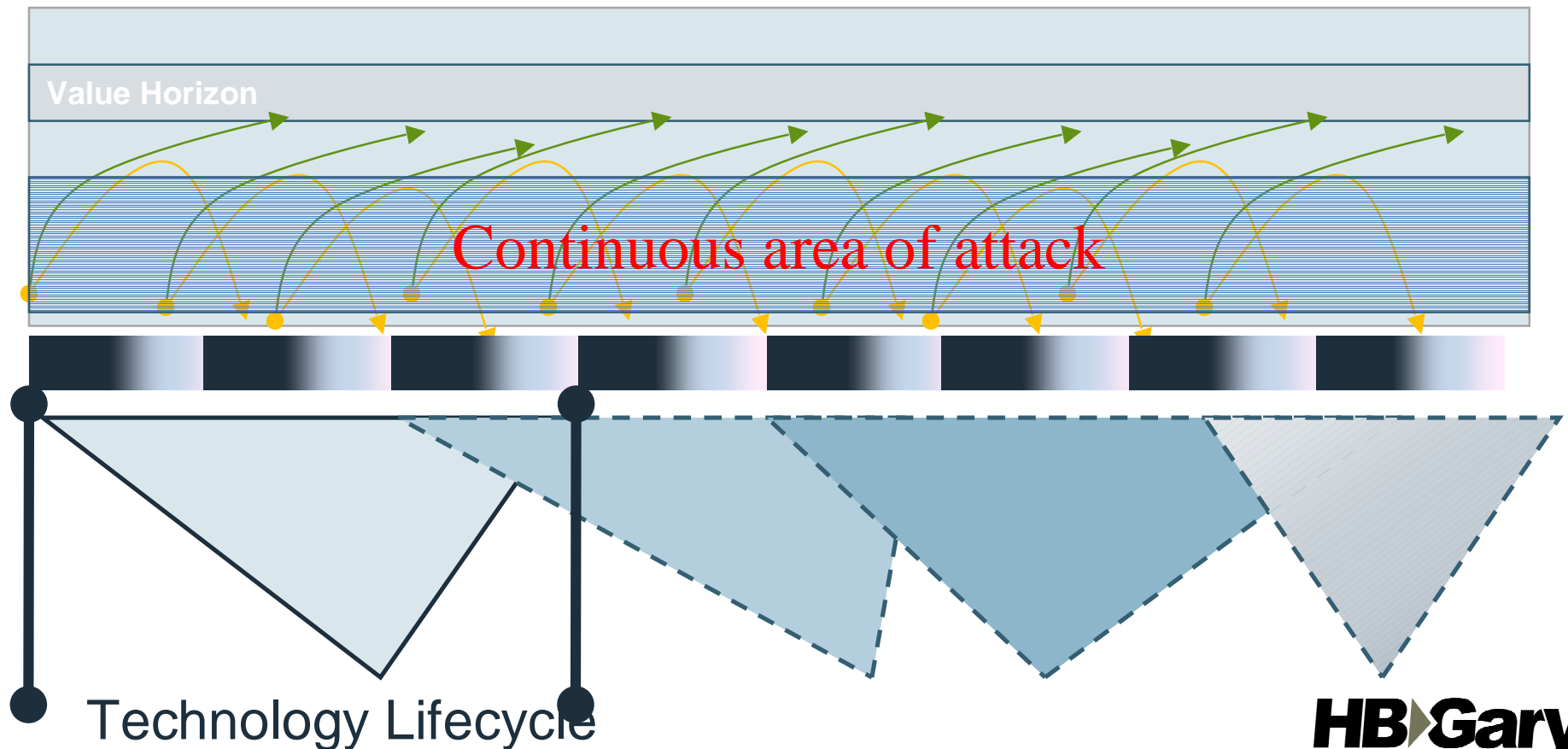
Continuum





Continuous Areas of Attack

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



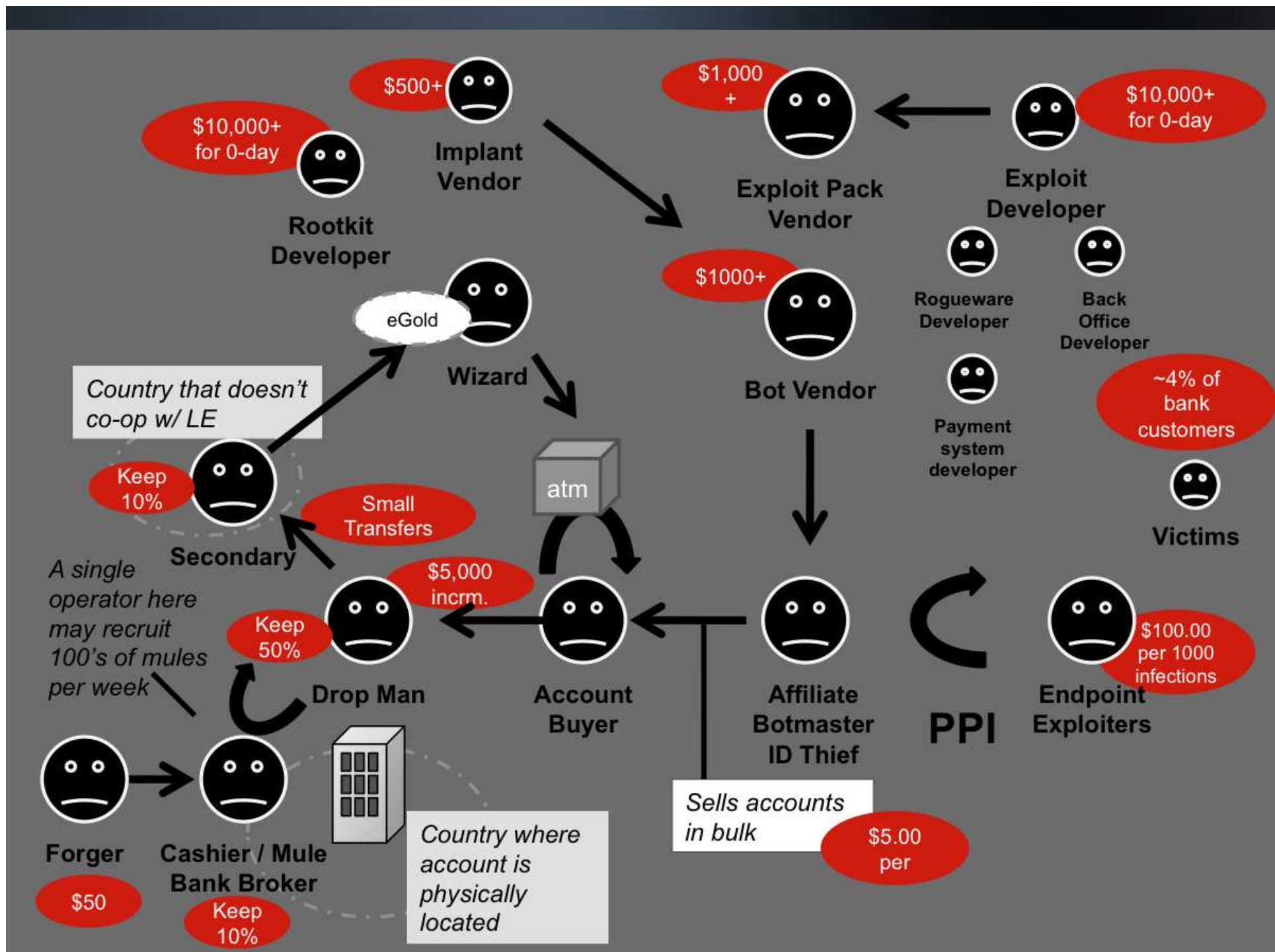


The Global Malware Economy




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



Pay-per-install.org


Pay-Per-Install.org
The Pay Per Install Affiliate Forum

**LIKE MONEY?
WORK WITH US!**

Register | [FAQ](#) | [Members List](#) | [Upgrade / Donate](#) | [Today's Posts](#) | [Search](#)

Pay Per Install Programs [Cashboom](#) [Zangocash](#) [Earning4u](#) [Exerevenue](#) [YA!Bucks](#) [InstallConverter](#)



Zangocash is now Pinball Publisher Network

 **Pay Per Install**

User Name ☐ Remember Me?
Password

Welcome to the Pay Per Install Forums

If this is your first visit, be sure to check out the [FAQ](#) by clicking the link above. You may have to [register](#) before you can post: click the register link above to proceed. To start viewing messages, select the forum that you want to visit from the selection below.

| Forum | Last Post | Threads | Posts |
|--|--|---------|-------|
| Pay-Per-Install.org | | | |
|  Pay Per Install Everything Pay Per Install related |  Donations and JNR VIP by Blademaster Yesterday 07:29 PM » | 623 | 5,461 |

Earning4u



The screenshot shows the Earning4u website. At the top, there's a navigation bar with a logo on the left, the text "EARNING 4 U .COM" in the center, and a "ENTER STATS" button on the right. Below the navigation bar is a large orange banner with a hand cursor pointing to a "REGISTER TODAY" button. To the right of the banner is a cartoon robot. Below the banner is a horizontal menu with links: MAIN, ABOUT US, CONDITIONS, RATES, FAQ, and CONTACTS. The main content area has a light gray background with the following text: "The partnership program «Earning4u» is the easiest way to earn money. All you need to do to start working with us is [register](#)." Below this, it says: "You will earn **from 6\$(Asia) to 140\$(USA)** per 1000 installs. You can view all prices in the [«Rates»](#) section." Below this is a section titled "Key Features" with a list of bullet points. To the right of the list is an illustration of falling money.

EARNING 4 U .COM ENTER STATS

BETTER RATES! NO WIN IN ONLY PER. ONLINE STATISTICS!

REGISTER TODAY

MAIN | ABOUT US | CONDITIONS | RATES | FAQ | CONTACTS

The partnership program «Earning4u» is the easiest way to earn money. All you need to do to start working with us is [register](#).

You will earn **from 6\$(Asia) to 140\$(USA)** per 1000 installs. You can view all prices in the [«Rates»](#) section.

Key Features

- Thanks to an individual approach to each client when you work with our system you have:
- Online statistics updated in real time
- A 24-hour support service ready to answer all your questions
- Absolutely no sharing and total independence of your statistics from other system users
- Stable weekly payments on virtually all payment systems: Fothard, WebMoney, Wire, e-gold, Western Union (WU), MoneyGram, Anelik and ePassports, and PayPal
- For regular clients and for those making more than 5000 installs per day - higher rates for all countries and special working conditions



Custom Crimeware Programming Houses

GeckoCode.com

GeckoCode { Home
Geckocode.com

Services
Contact Us and Get
a Quote For Your
Project

Products
Some of Our Own
Popular Software

Welcome

December 14, 2009 -- Posted by: **Santasack**
GeckoCode is a group of talented software developers who's skills cover a large range of software development, web design and graphics technologies. Our team of developers have extensive expertise in C/C++, legacy visual basic, .NET, Php, database design and implementation, company logo and banner design .. and much much more.

We work with all kinds of clients, from large businesses to individuals, and we believe that custom software and graphic design should be accessible and affordable to anybody that requires such services.

We pride ourself on taking a personal approach to our customers, no matter how small the job our main focus is that on completion our customer is happy and the solutions we provide fit their needs exactly.

We will develop you any kind of software you need, and operate a n (yes we are black hat friendly!)
deployed after project completion (yes we are black hat friendly!)
OUR!!

WE DO NOT CHARGE BY THE HOUR!!

Unlike other companies we will quote you a price that is accepted you will know from the outset as near as possible to the total project cost!

We provide full rights and ownership to the software/graphics over to you on project completion, and will provide you with detailed technical documents, flowcharts and time lines throughout the development period.

NO JOB TOO LARGE OR TOO SMALL

As well as large project development, we accept any kind of software/graphics related jobs, From simple website banner and logo designs right down to trivial technical support.

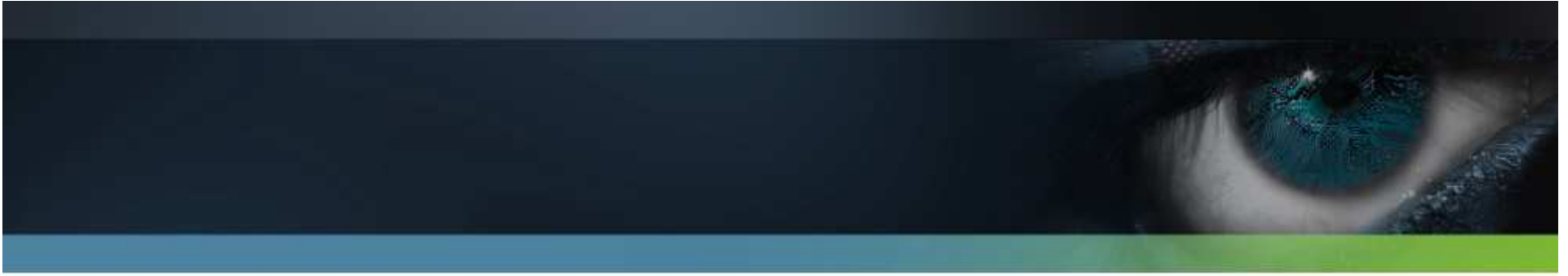
OUR PRICES WON'T BE BEATEN

We believe that our personal approach to customers needs, and the fact we take every customers current situation and overall goals into account before we even consider our quote means that you will not find a cheaper more personal solution to your custom software needs.

INSTANT MESSENGER AND LIVE WEB CHAT SUPPORT

[Read more](#)

December 14, 2009



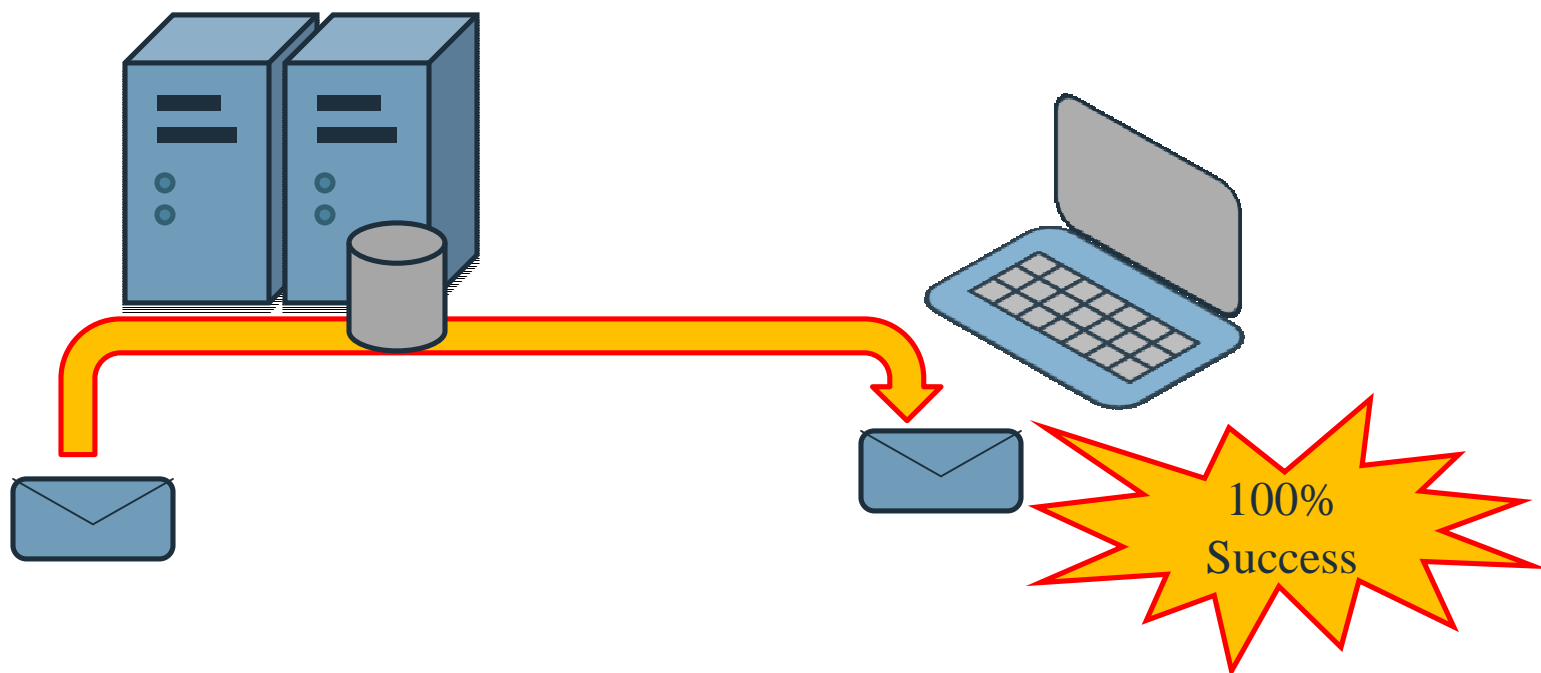
Anatomy of APT Operations



Malware Distribution System

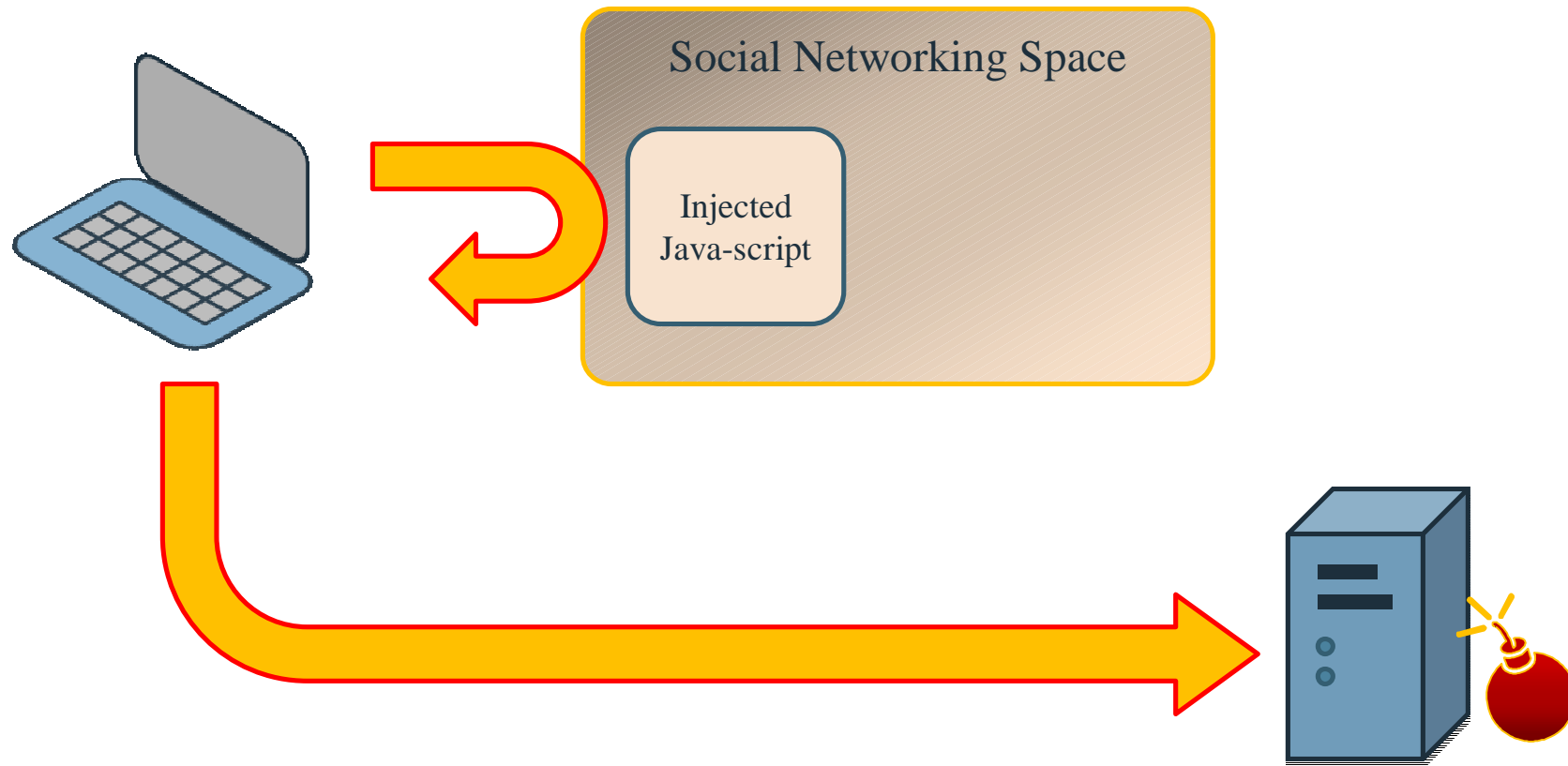
- Many, Many, Attack Vectors
 - Targeted Browser attacks -
 - Spear & Whale Phishing
 - Zero Day or well known exploits
 - Slow and Low & Loud and Proud – they do it all
 - Re-Direction – I expect you to find my first 2 malware infections
- Social Media
 - Intelligence, Surveillance, and Reconnaissance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

Booby Trapped Documents



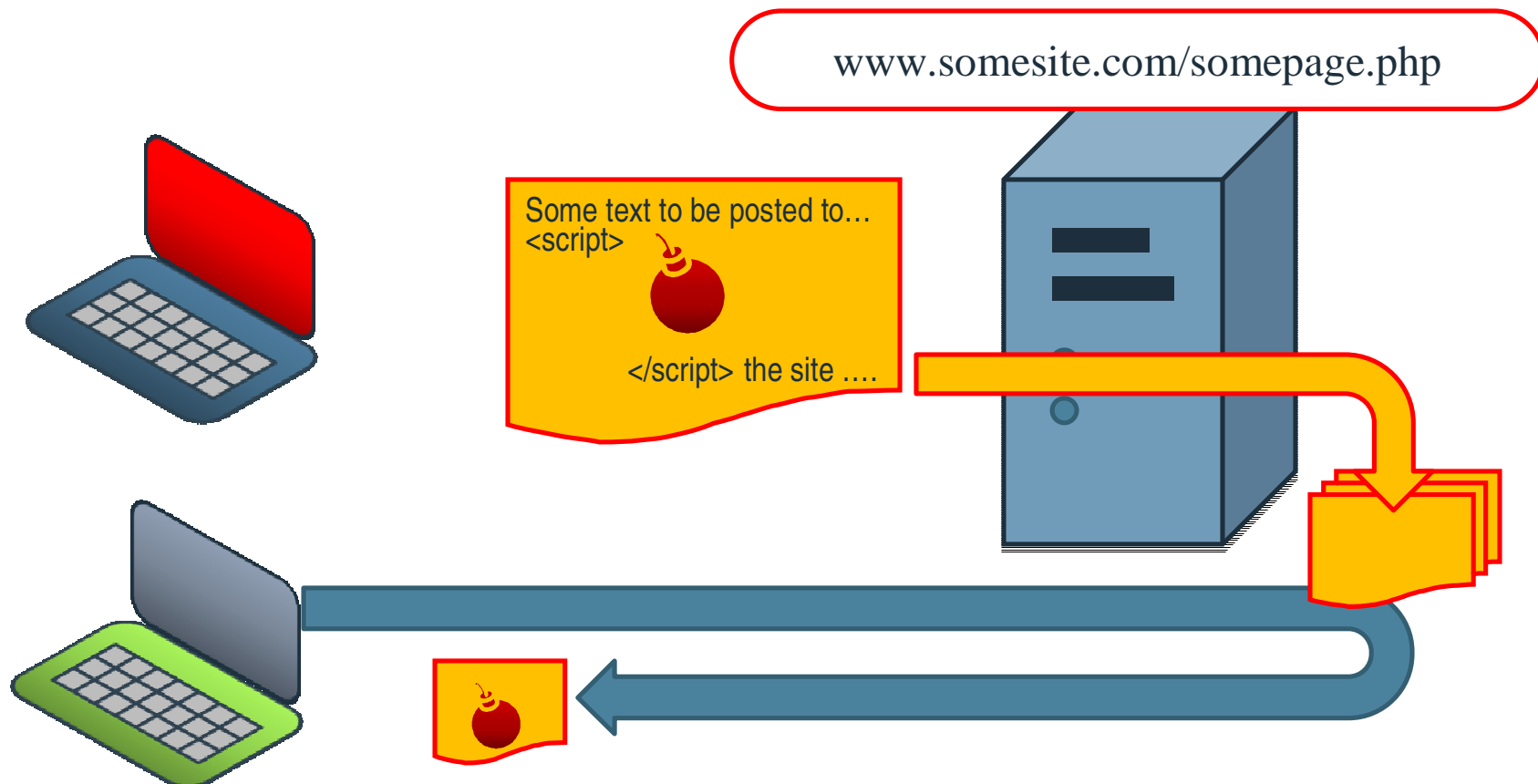
- Single most effective *focused* attack today
- Human crafts text to look legitimate

Web Based Attack

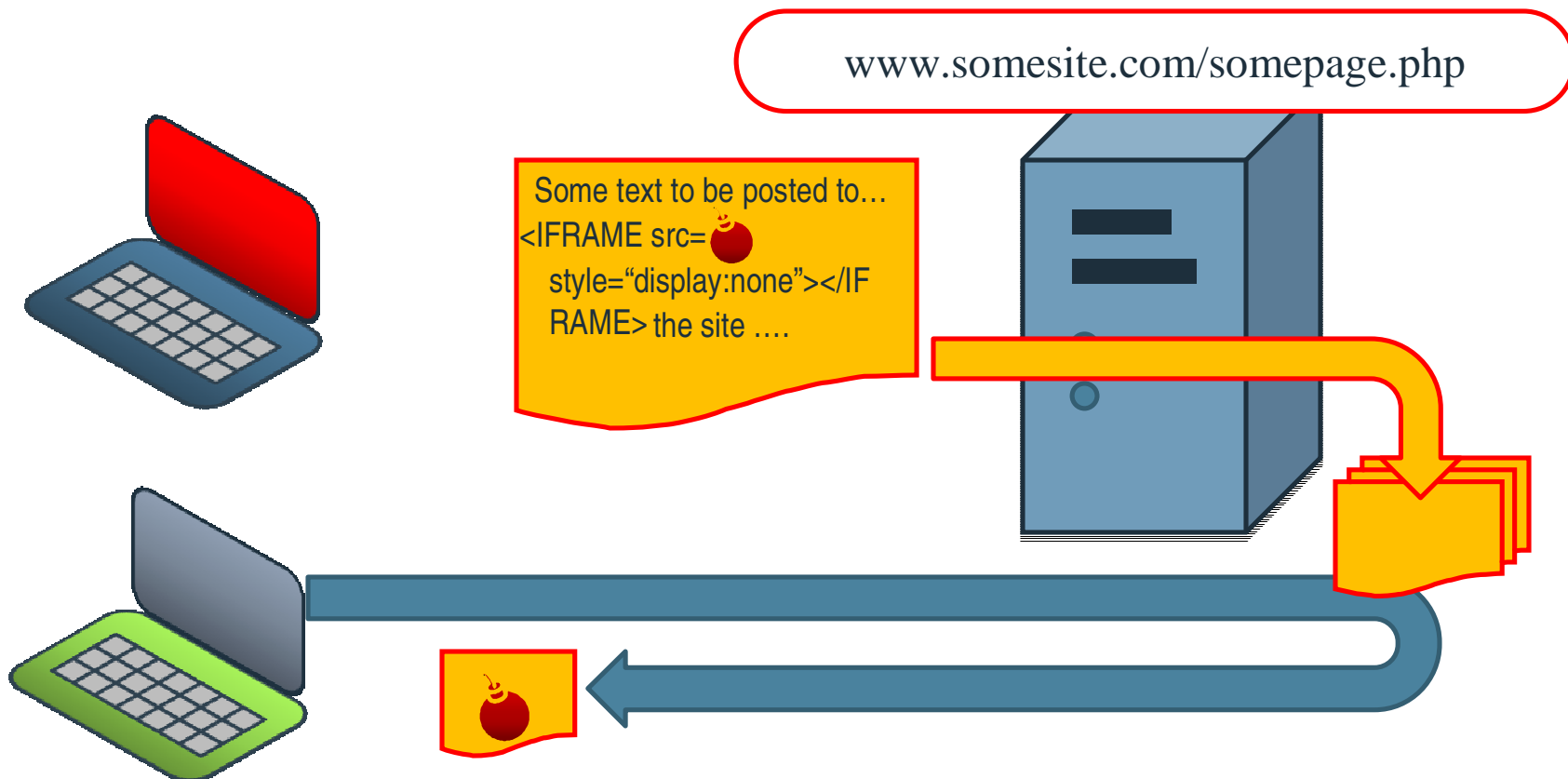


- Used heavily for large scale infections
- & Targeted Operations for specific groups of people....

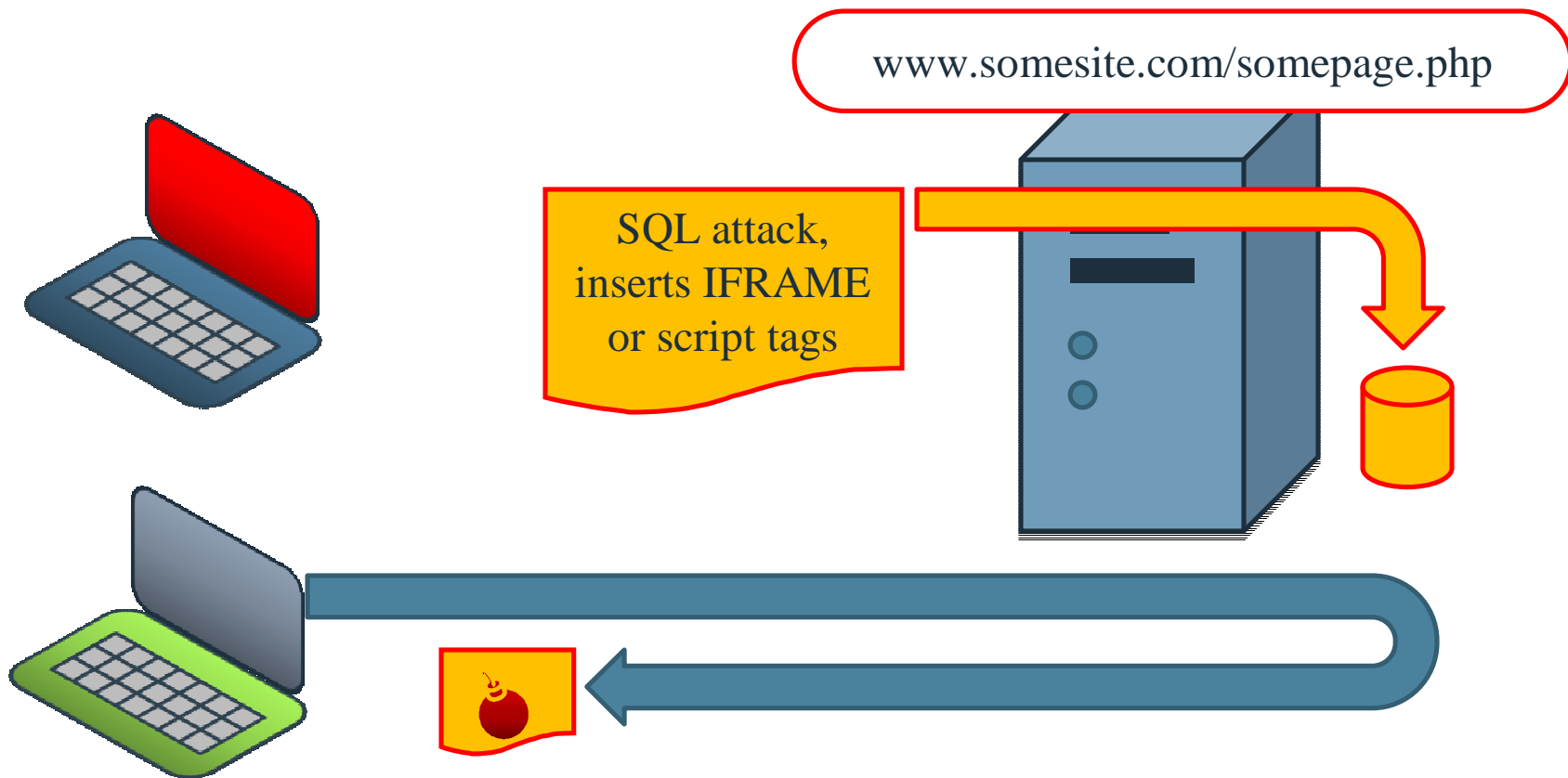
Trap Postings I



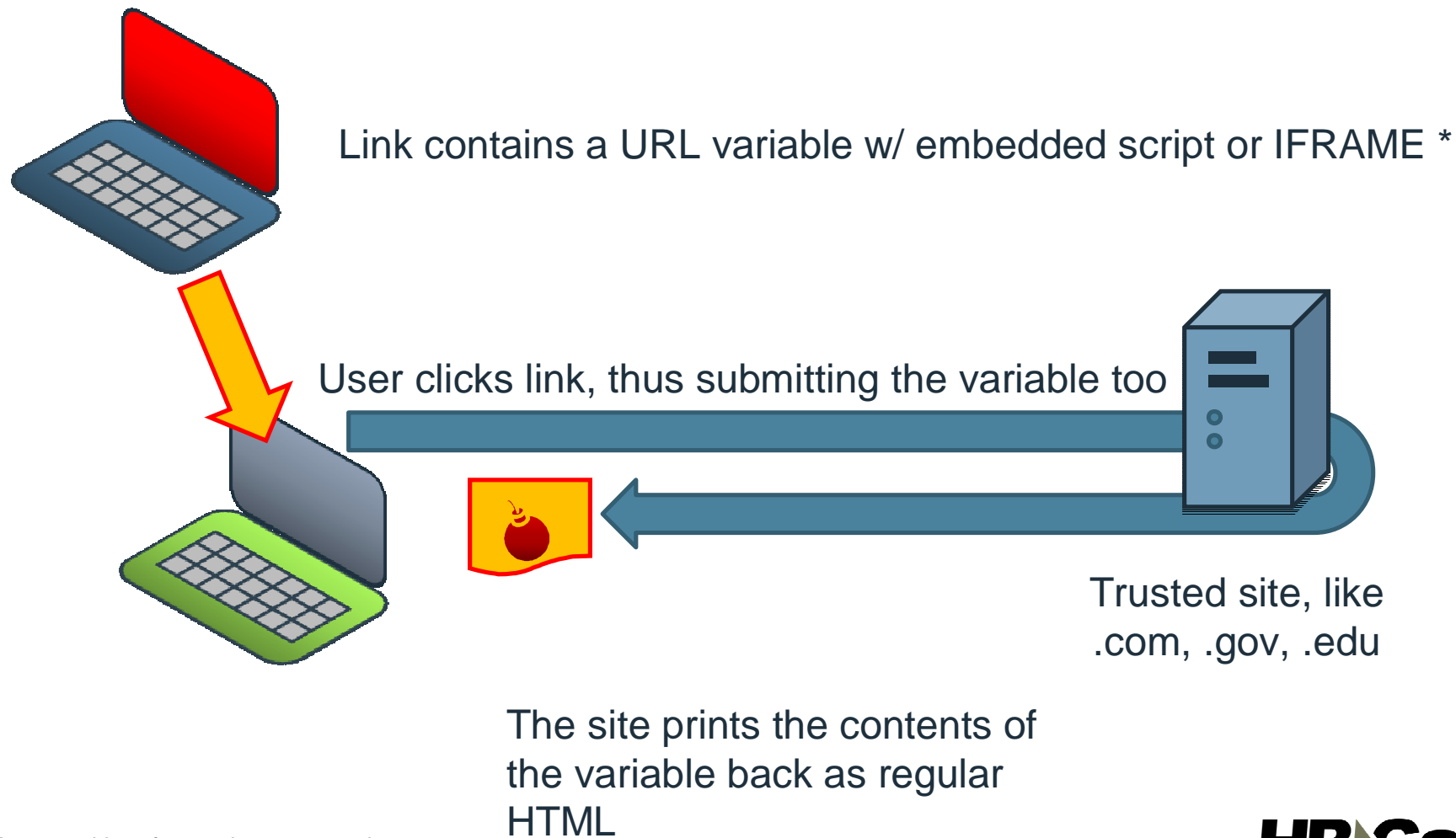
Trap Postings II



SQL Injection

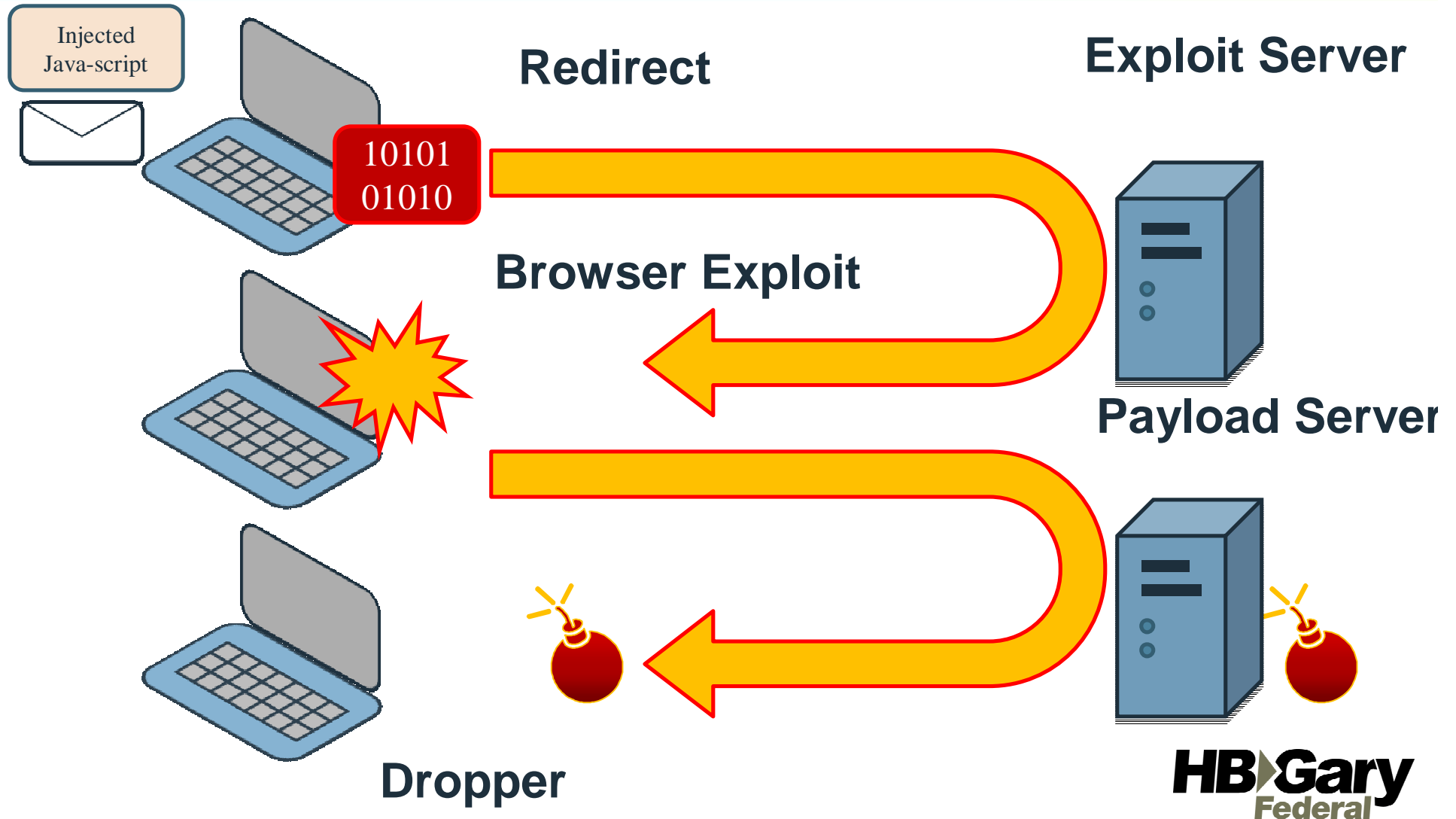


'Reflected' injection




*For an archive of examples, see xssed.com

A three step infection



Phoenix (exploit kit)



Phoenix Exploit's Kit v2.0

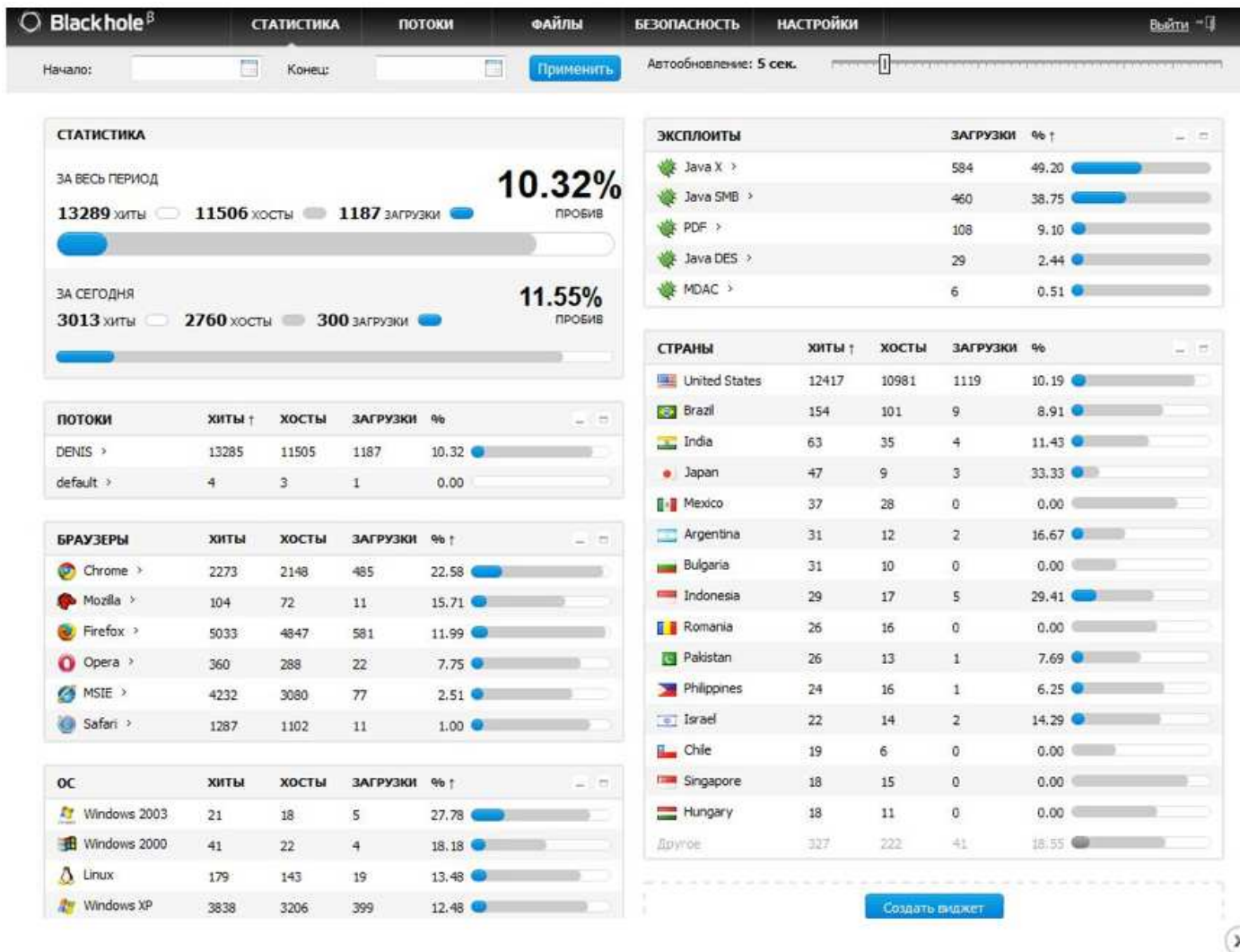
COMES WITH TRIPPLE SYSTEM

| Referers statistics | | | |
|------------------------------|----------|-----------|---------|
| Referer | Visitors | Exploited | Percent |
| ad10em.eu | 5613 | 786 | 14% |
| cr1.easyfranchiselessons.net | 6284 | 538 | 8.56% |
| ad1.movieslist.biz | 5216 | 357 | 6.84% |
| cr1.guideeasylessons.net | 1860 | 127 | 6.83% |
| --- | 493 | 97 | 19.68% |
| www.columbiadrove.de | 214 | 19 | 8.88% |
| www.meine-gewinnseite.de | 217 | 17 | 7.83% |
| ad1.guide-pro.com | 186 | 17 | 9.14% |
| ad1.movieslist.in | 84 | 7 | 8.33% |
| ad1.streamdirectgate.net | 62 | 7 | 11.29% |
| columbiadrove.de | 40 | 7 | 17.5% |
| www2.bestfranchise24.net | 86 | 6 | 6.98% |
| www.columbiadrove.de | 72 | 5 | 6.94% |

Menu

- [Simple statistics](#)
- [Advanced statistics](#)
- [Countries statistics](#)
- [Referers statistics](#)
- [Clear statistics](#)
- [Upload .exe](#)
- [Exit](#)

Blackhole (exploit kit)



Payload Server

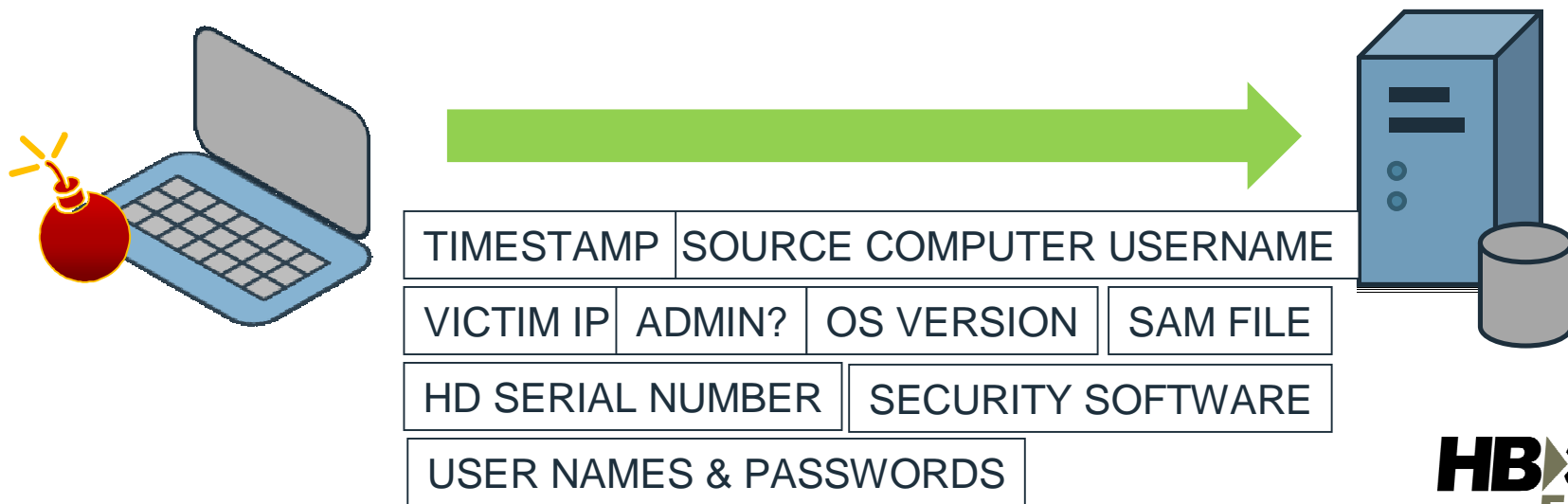
- A machine that has the actual malware dropper ready for download.
- The exploit server will redirect the victim to download a binary from this location



Command and Control



Once installed, the malware phones home...





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

Triad (botnet)

TRIAD HTTP Control System
[Set Command] [Statistics Table] [Help]

[Set Command for Machines:]

Bot IP ("all" - to all bots)

Command

ARGV[1]:

ARGV[3]:

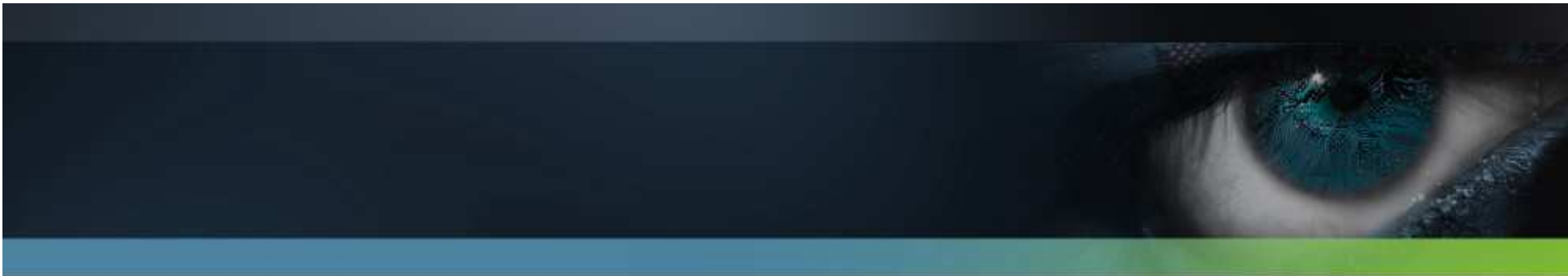
- [Sleep]-[time(in secs)]
- [AckStorm]-[Host]-[Port]-[Nr of Packets]
- [Reverse Shell]-[Host]-[Port]
- [Bind Shell]-[Port]
- [Delete Bot from remote machine]
- [Shutdown Remote Machine]
- [Reboot Remote Machine]

Zeus (botnet)

Zeus :: Options

| | |
|---|--|
| Information: Profile: admin GMT date: 26.04.2009 GMT time: 16:06:08 | Screenshots Format: <input type="text" value="jpeg"/> Quality: <input type="text" value="80"/> % |
| Statistics: Summary | Local paths Reports: <input type="text" value="_reports"/> |
| Botnet: Online bots Remote commands | Other <input checked="" type="checkbox"/> Enable log write to database. <input checked="" type="checkbox"/> Enable log write to local path. Online bot timeout: <input type="text" value="30"/> Encryption key: <input type="text" value="2222"/> |
| Logs: Search Uploaded files | <input type="button" value="Update"/> |
| System: Profile → Options | |
| Logout | |

Copyright © 2006-2009 Zeus Group



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:

Botnets:

IP-addresses:

Countries:

ru

NAT status:

Outsi

Online status:

Onlin

Install status:

-

Used status:

-

Comments status:

-

R.

Result (31):

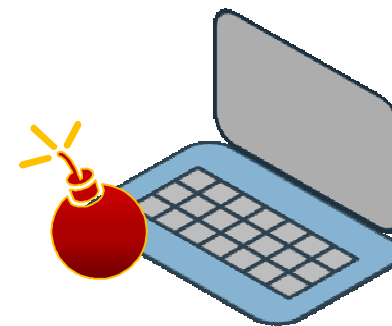
Bots action: Check socks

>>>

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

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



Poison Ivy (implant)

PoisonIvy Polymorphic Online Builder

Poison Ivy Server (binary) :

Parcourir...

Upload

Binary name: shellcode.bin

Binary size: 6215 bytes

Binary hexa: 558bec81c430f0fff6033c08dbd84...

[OK] Binary uploaded.

[OK] Binary modified

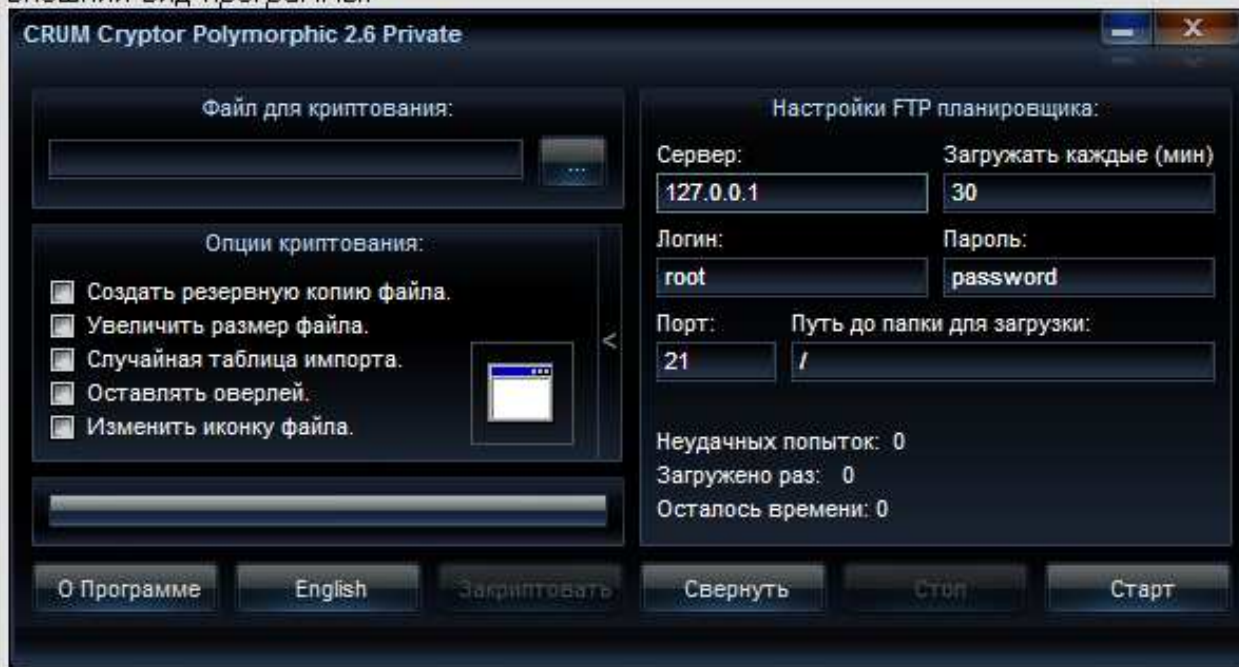
Features:

- Polymorphic encryption
- Polymorphic decryption routine
- Add junk code (not a block with a jmp)
- Add a unique trick to bypass Sandbox and Memory Scan on VT (found by me) (the server is slow to start)
- Add junk API call

CRUM (protector)

CRUM Cryptor Polymorphic v. 2.6 new!

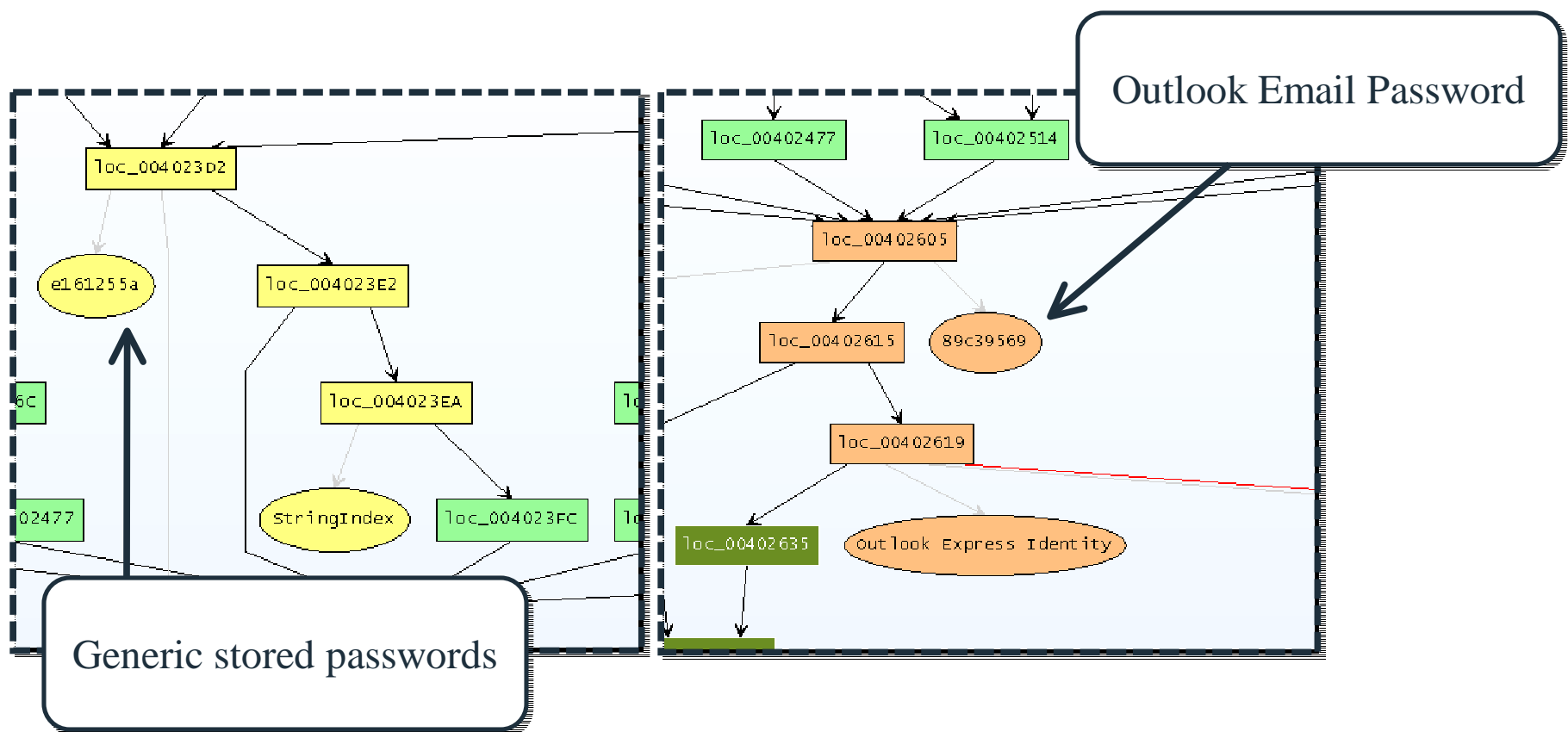
Внешний вид программы:



Цена: 200\$



Steal Credentials



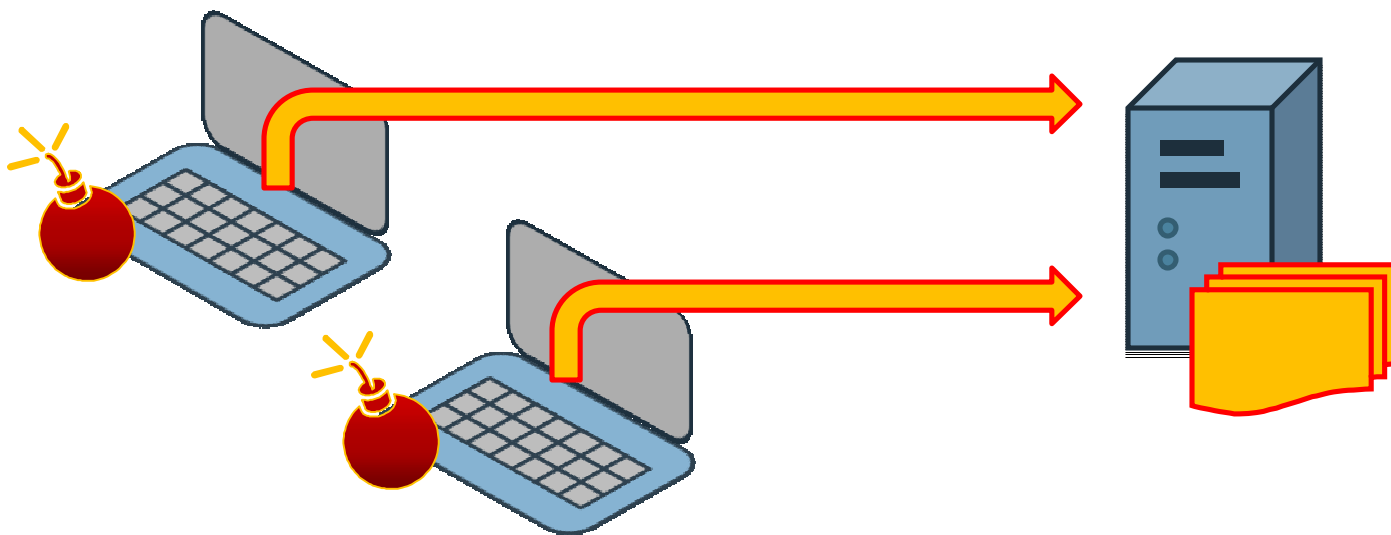
Steal Files

Diagram illustrating a network connection and file exfiltration:

- Call graph nodes: `loc_71004294`, `207.43.230.21` (highlighted in red), `__imp_ws2_32.dll!inet_addr`, `loc_71004298`, `data_71008348`.
- Binary View window showing a list of file types (all in red text):
 - `regsvr.dll`
 - `207.43.230.21...`
 - `\\.\%s..\drivers`
 - `\\own\...\...xls`
 - `....XLS.....rar`
 - `....RAR.....ZIP`
 - `....PPT.....PDF`
 - `....doc.....`
 - `*...List domain`
 - `server ok!#..Ent`
 - `ries enumerated:`
 - `%d....Total en`
 - `tries: %d....Mor`
- Callout box: "All the file types that are exfiltrated"

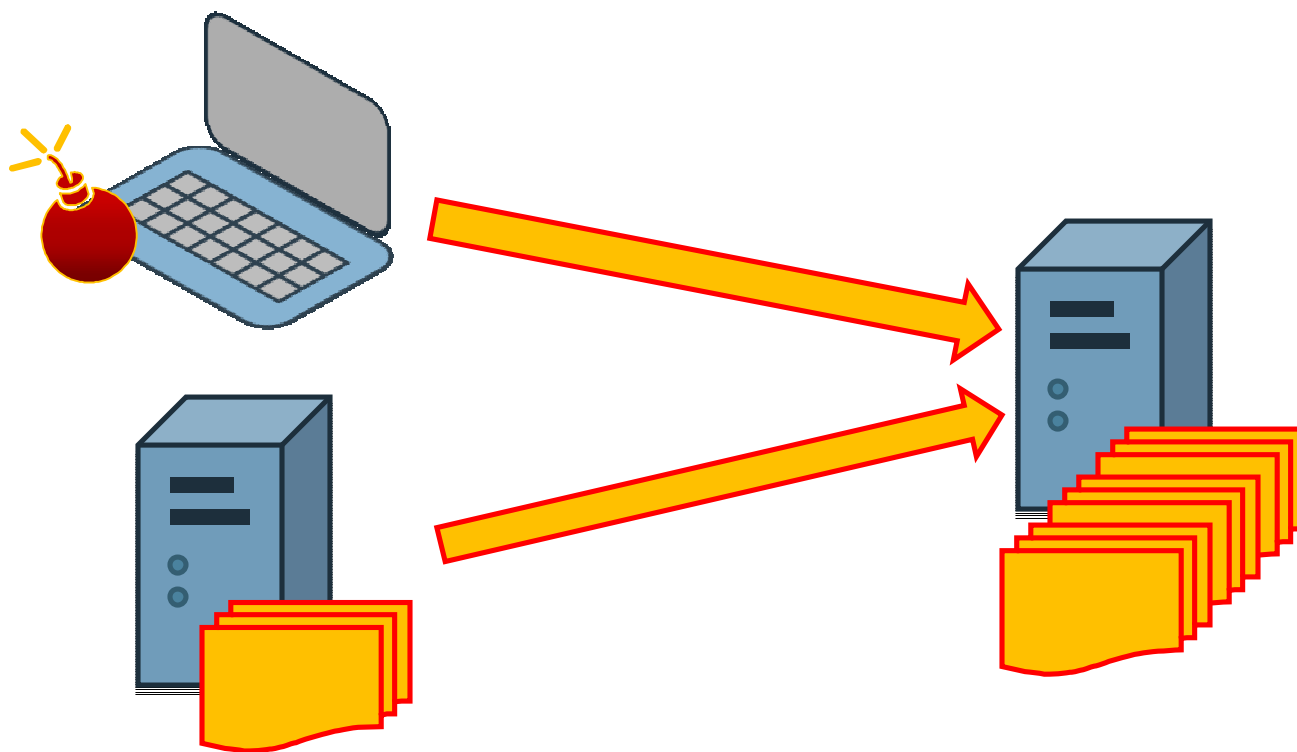
Staging Server

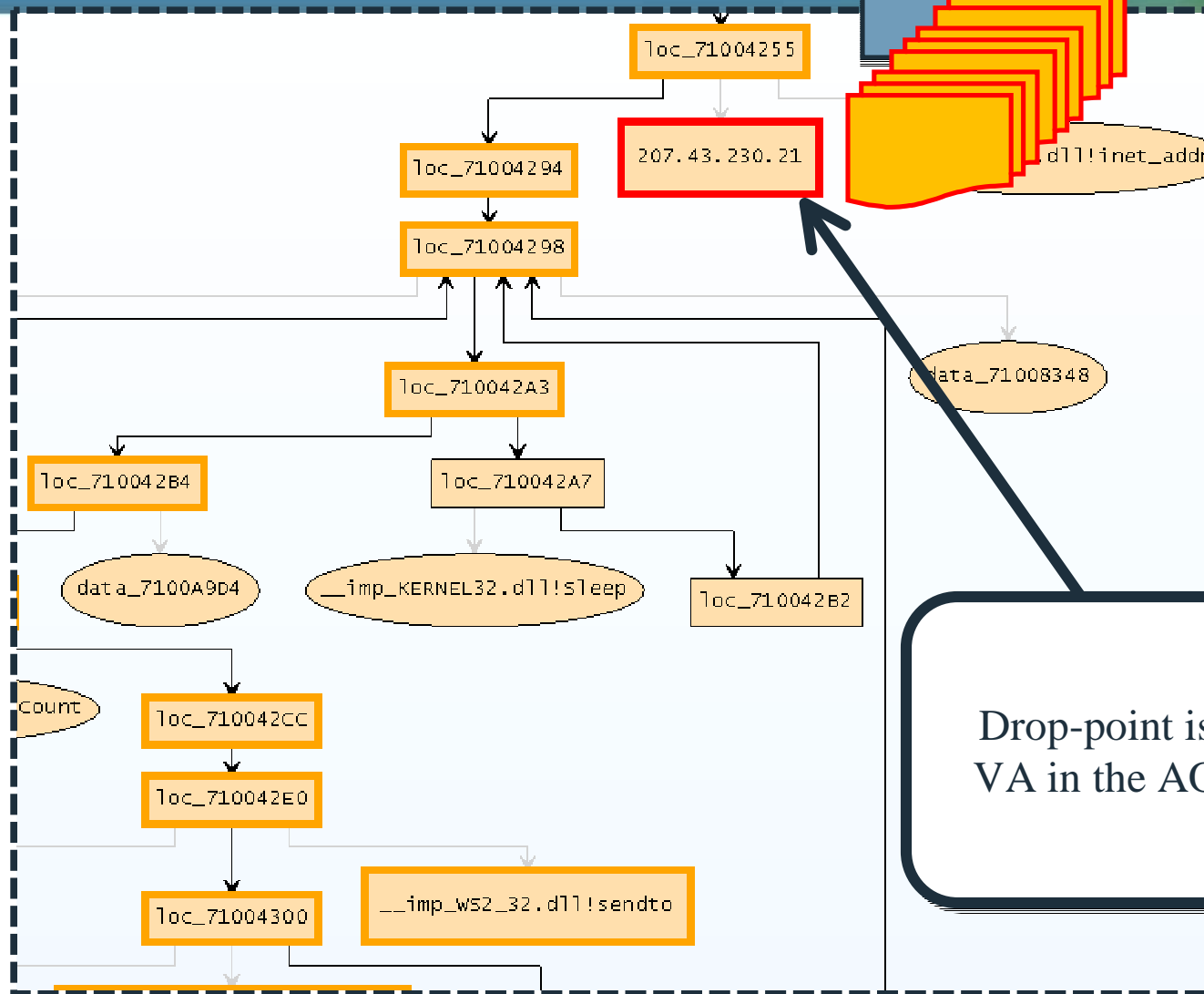
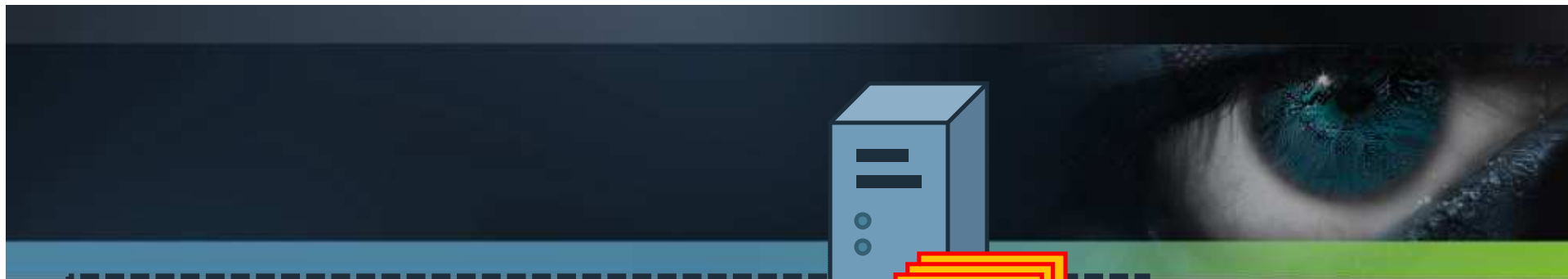
- A place to store all the stolen goods before it gets 'exfiltrated'
- Data is moved off the network in a variety of ways – 'Hacking Exposed' level behavior



Drop Site

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





Drop-point is in Reston,
VA in the AOL netblock



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.

The header of the slide features a dark, textured background. On the right side, there is a close-up, high-contrast image of a human eye with a greenish-blue iris. The title 'Stuxnet FAQ' is written in a white, serif font on the left side of the header.

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.



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.



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



Detect and Respond

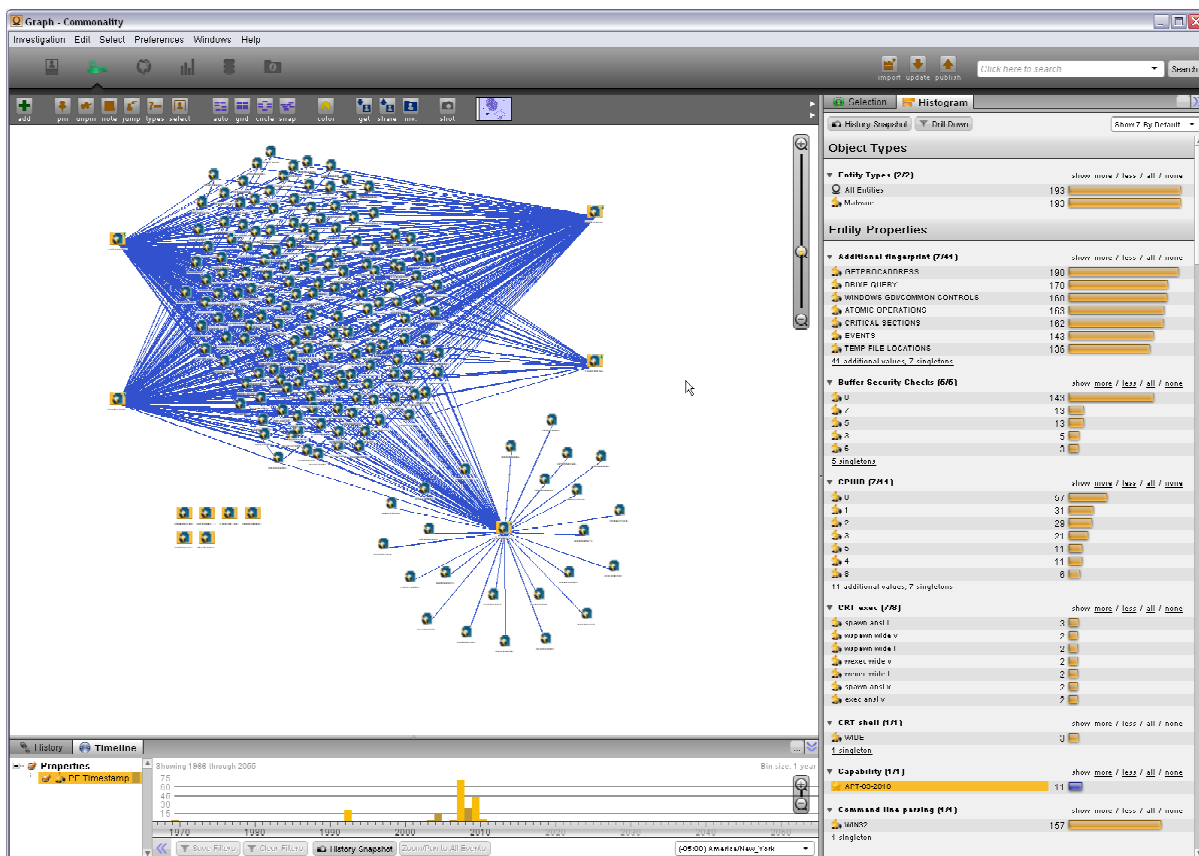




Detect and Respond

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

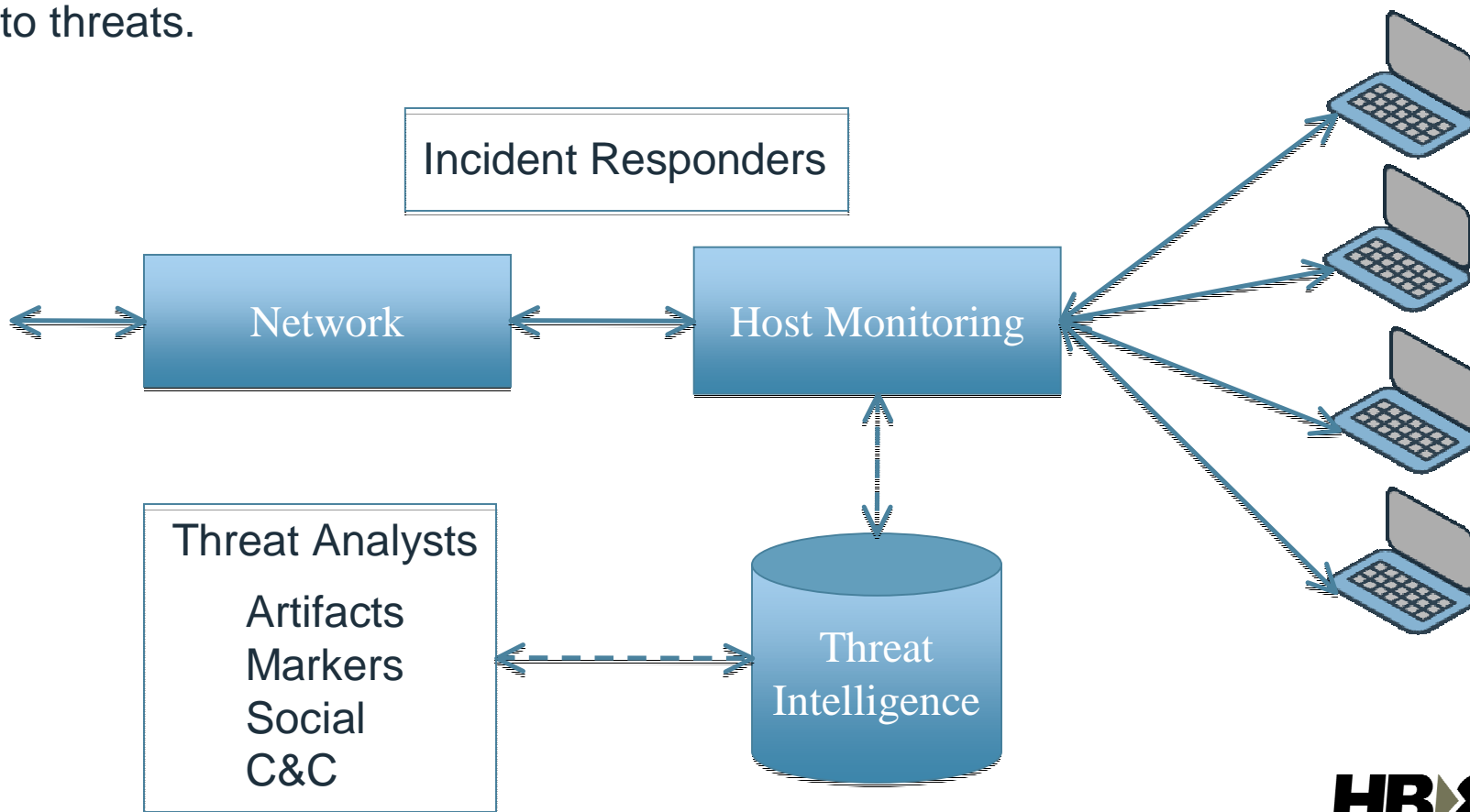
Threat Intelligence



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

Incident Response

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





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.



Threat Analysis

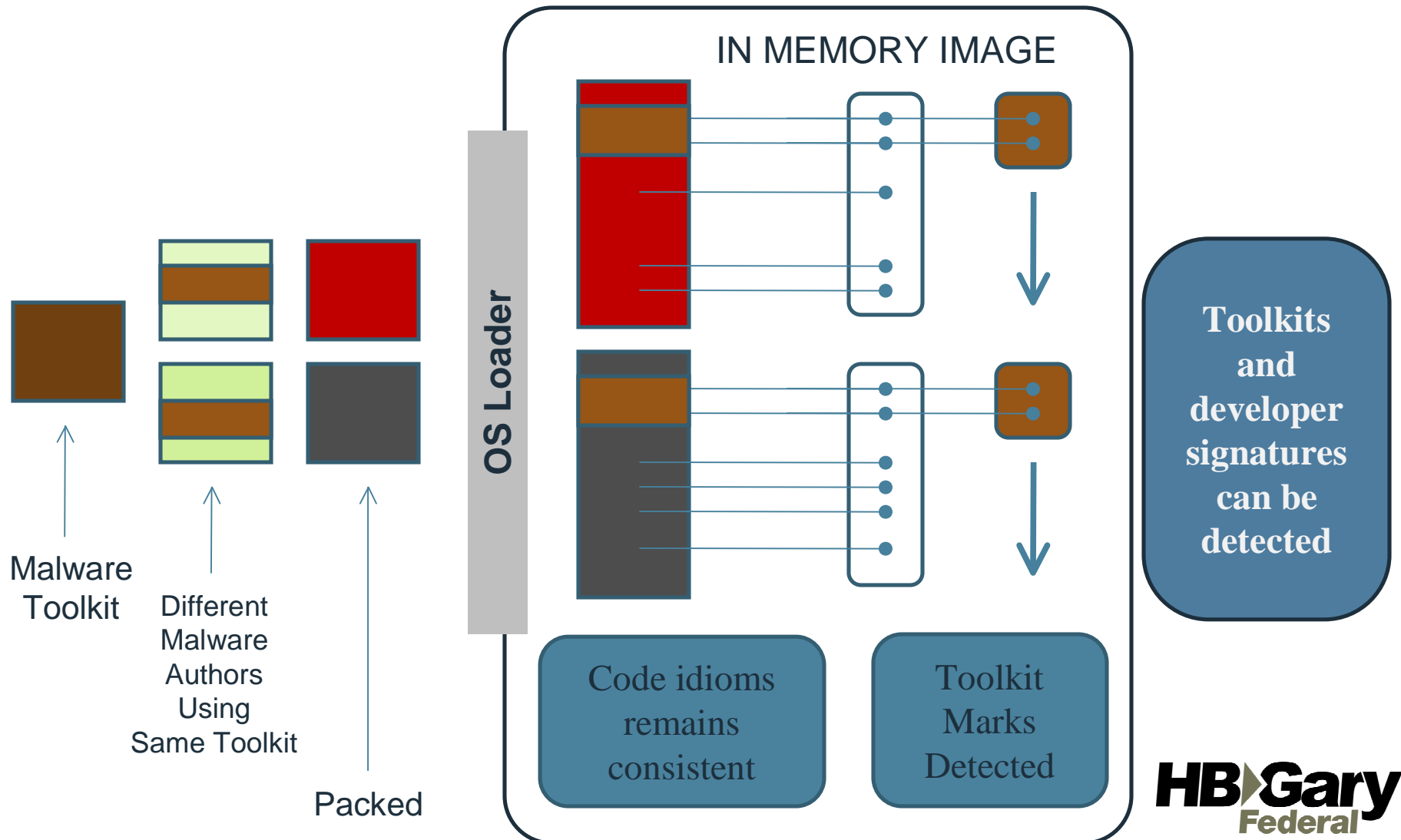
- Integrate cyber verticals into single data set.
- Develop larger sets of quantified artifacts and markers
 - Fingerprints
- Correlate Malware based on fingerprints
 - Statistical probabilities based on % matching fingerprints
- Develop threat maps using associated intelligence around correlated malware

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.

Fingerprints



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



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



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