



Criminal Use of Machine to Machine Communication

Network Security Turned Inside Out

Industry Innovator

- Pioneering cyber threat research, analysis and detection since 2006
- Six patents-pending
- Notable Research Backers



World-Class Customers

- **Over 125 million assets** protected worldwide
- Global enterprise, ISP/Telco, Higher Education, Government

Premier Integration Partners

- SIEM, Web Gateway, Netflow

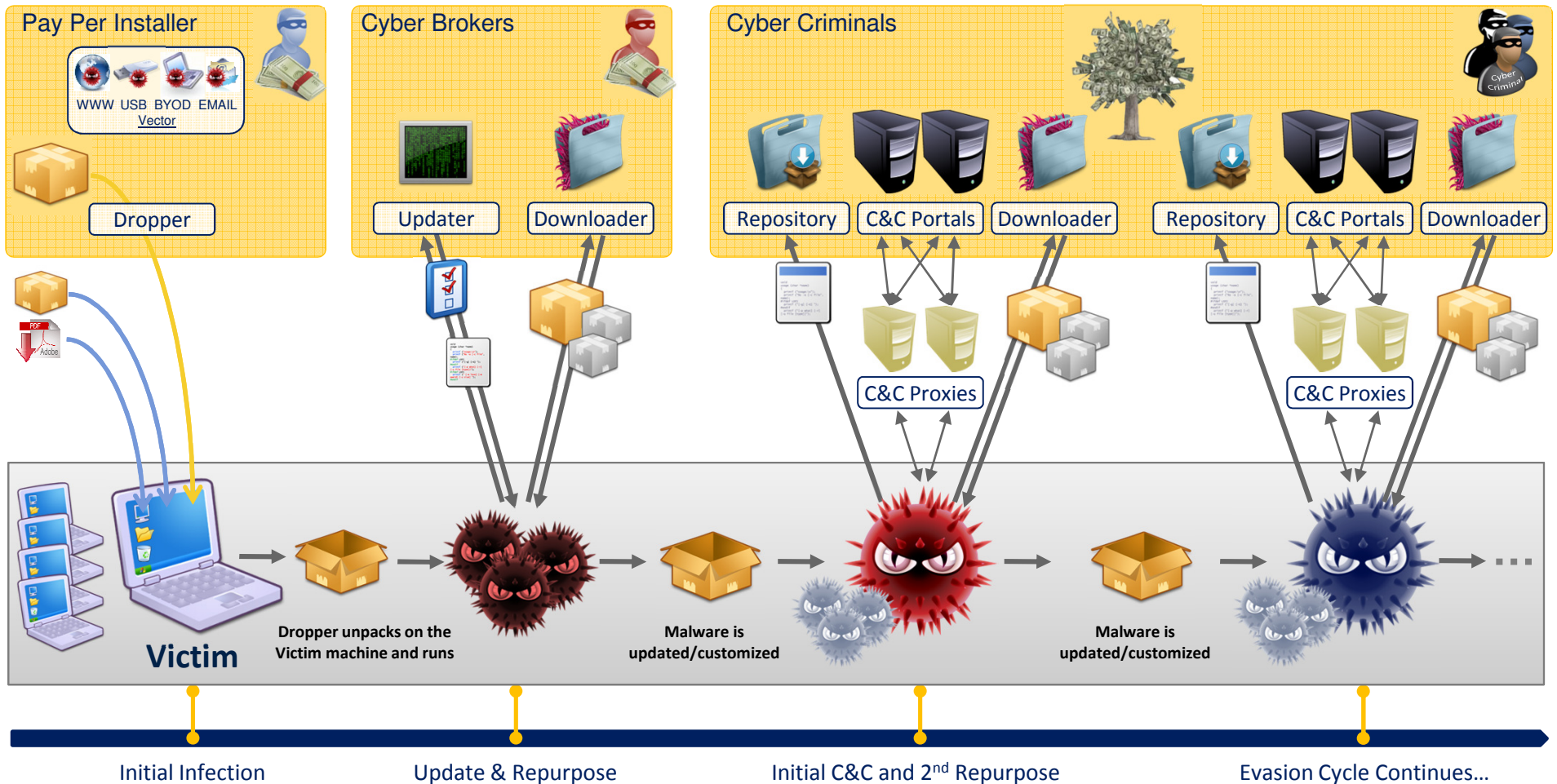


Solutions Delivery Partners

- Network Security “Health Check”, Post-Breach Investigation, Managed Service



The Business Behind Infections



Types of Uses: State Sponsored, Money Transfers, Intellectual Property Theft, Credentials, etc...

Motivation: Highly organized business with one goal – **MONEY**.



The Payoff

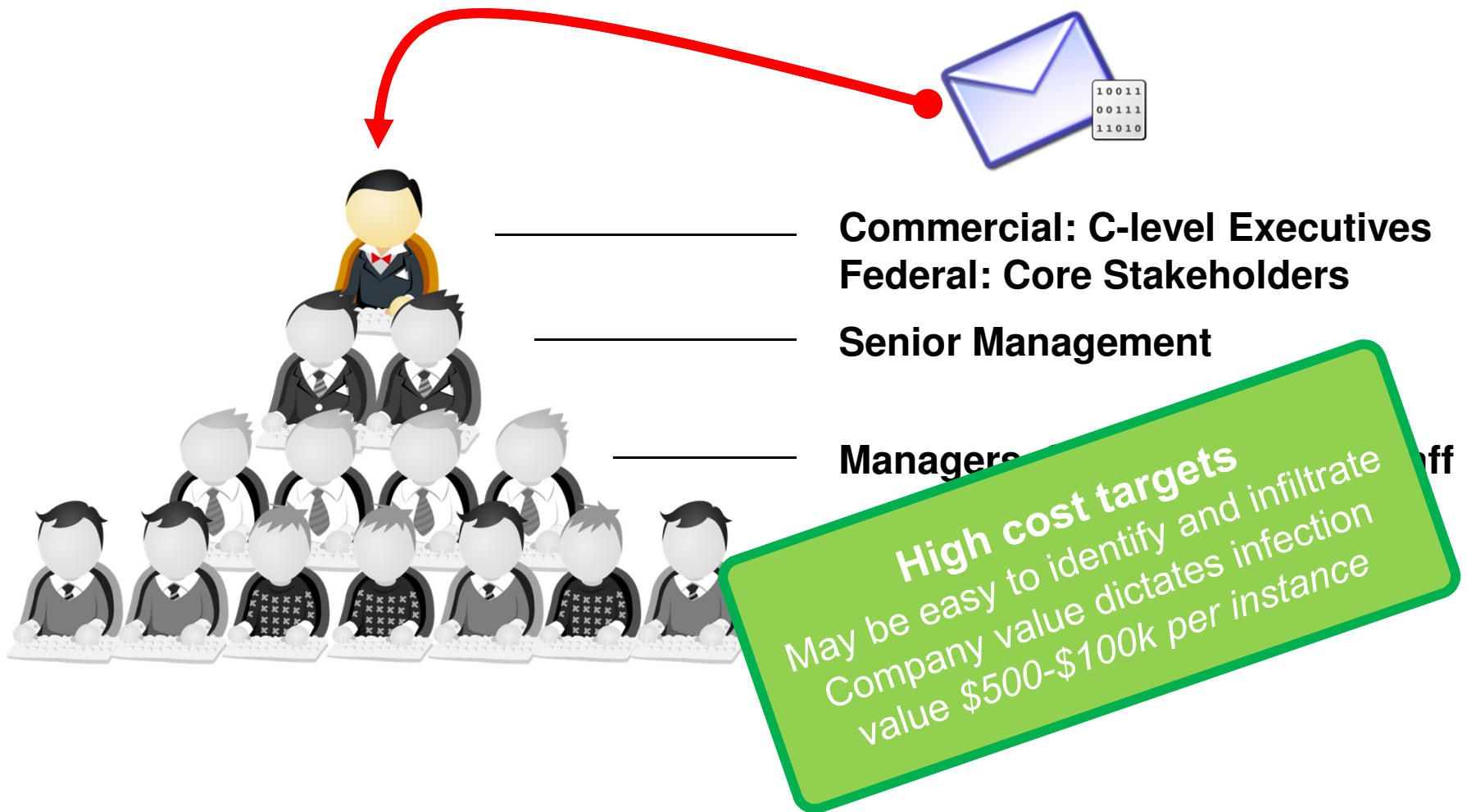
Gold Install

[Main](#)[Sign up](#)[Login](#)[Rates](#)[Contacts](#)[Terms of service](#)[FAQ](#)

Goldinstall Rates for 1K Installs for each Country.

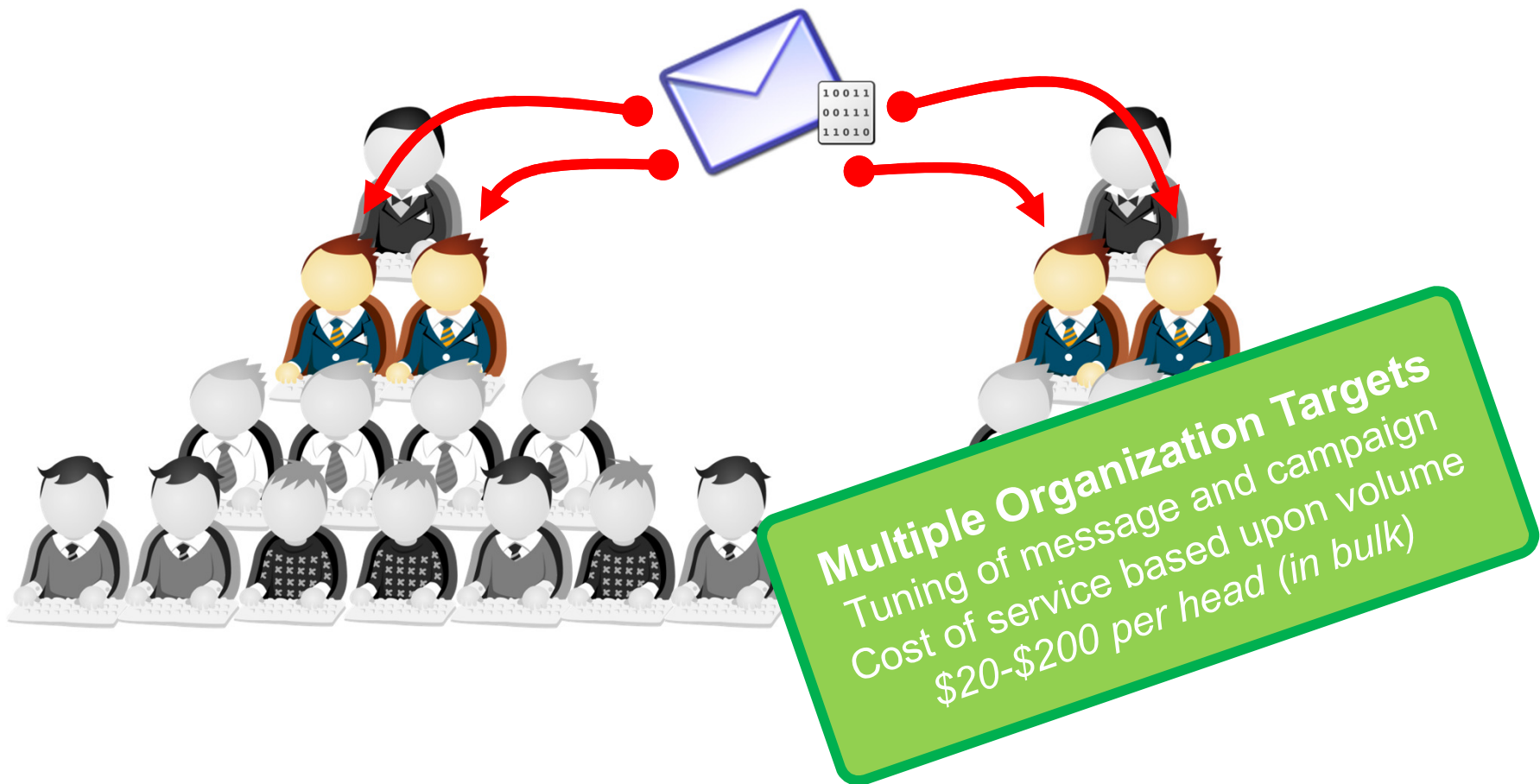
Country	Price
OTH	13\$
US	150\$
GB	110\$
CA	110\$
DE	30\$
BE	20\$
IT	65\$
CH	20\$

Whaling = Targeting the biggest & most visible targets



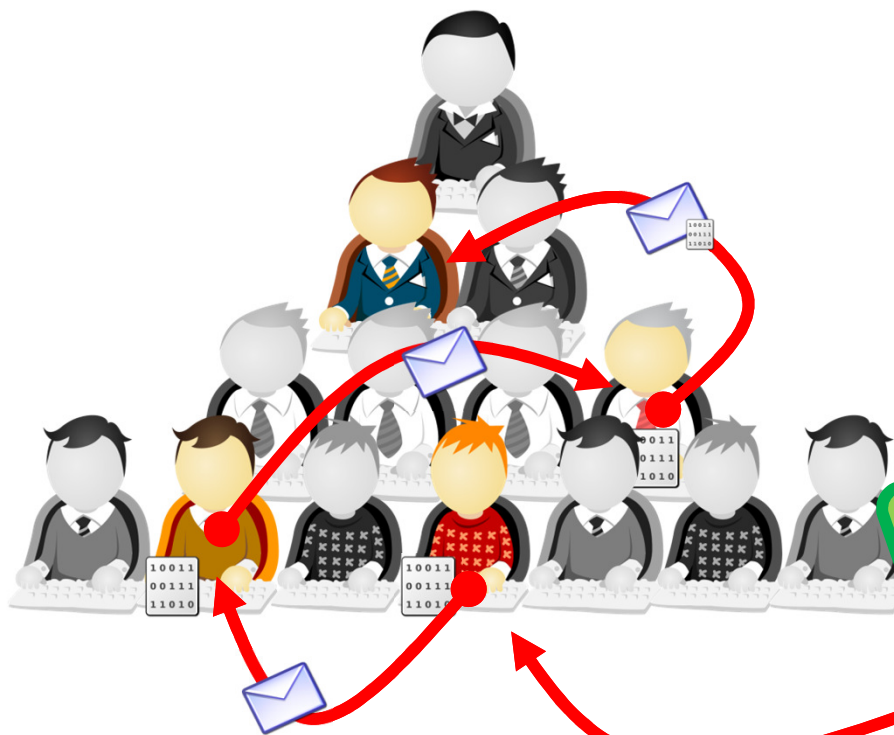
Horizontal Spear Phishing

Horizontal Spear = Targeting a specific role across similar industries using field-specific terminology.



Vertical Spear = Exploiting relationships and hierarchy within the targeted organization

- Messages reference people within the organization
- Each victim helps illuminate more of the hierarchy
- Exploitation of trust relationships
- Copy/Paste of real internal email content for e



Single Organization Target
Costly to perform – manual work
Cost of service based upon time
\$ unknown



Cyber Brokers

Buy Specific Infections



Offers Services Proofs Free Logins Payment Method Runescape

Yes – we already handed this over to the NSA. *It isn't around any more!*

Site	Details	Level of Control	Traffic	Price
http://mel.org/	The United States - Michigan eLibrary: MEL	Full SiteAdmin Control/SSH Root access	4262	\$99
http://gs.mil.al/	ARMY Forces of republic of albania	Full SiteAdmin Control + High value informations	unknown	\$499
http://www.scguard.army.mil/	Souce Carolina National Guard	MySQL root access + High value informations	unknown	\$499
http://cecom.army.mil/	The United States Army CECOM	Full SiteAdmin Control/SSH Root access	unknown	\$499
http://pec.ha.osd.mil/	The Department of defense pharmaco-economic Center	Full SiteAdmin Control/Root access, High value informations!	unknown	\$399
http://www.woodlands.edu.uy/	Woodlands School Uruguay.	Full SiteAdmin Control!	5200	\$33
http://s-u.edu.in/	Singhania University	Full SiteAdmin Control.	unknown	\$55
http://www.nccu.edu.tw/	National Chengchi University.	Students/Exams user/pass and full admin access!	56093	\$99
http://www.terc.tp.edu.tw/	Taipei City East Special Education Resource Center	Full SiteAdmin Control.	74188	\$88
http://itcpantaleo.gov.it/	Italian Official Government Website.	Full SiteAdmin Control.	292942	\$99
http://donmilaninapoli.gov.it/	Istituto Statale Don Lorenzo Milani	Full SiteAdmin Control.	292942	\$99
http://itcgcesaro.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	\$99
http://itimarconi.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	\$99
http://primocircolovico.gov.it/	Official Italian gov website.	Full SiteAdmin Control.	292942	\$99
http://www.utah.gov/	American State of Utah Official Website.	Full SiteAdmin Control.	173146	\$99
http://www.uscb.edu/	University of South Carolina Beaufort.	Full SiteAdmin Control.	1123	\$88
http://michigan.gov/	American State of Michigan Official Website.	MySQL root access/Valuable information.	205070	\$55



- Everyday access to 100k-2M Infections
 - Price range from \$200 (24hr use) to \$50k (to own)
- Self-build botnet provisioning
 - Off-the-shelf tools
 - Avg. 20k bot installs within a week (500k if optimized)
- Commissioned building of botnet
 - Target centric pricing

Buying Infections

Home




















Price

Stats

Sign Up

- Октябрь 26/2007
Налетай на ES IT DE , идёт хороший подлив.
- Октябрь 23/2007
Введена принудительная проверка грузимых файлов на предмет полноты , если файл галится более чем 30% из тестируемых 11 антивирусов , то загрузка данной задачи прекращается и рядом с ней появляется уведомление. Проверка файлов производится через приватный сервис.
- Октябрь 16/2007
Налетай не скупись покупай живопишь) а точнее мис и юсу.
- Август 30/2007
Введена проверка файлов



Country	Price for 1k	
 AU	300\$	Order now
 DE	220\$	Order now
 GB	210\$	Order now
 IT	200\$	Order now
 NZ	200\$	Order now
 ES	200\$	Order now
 US	110\$	Order now
 BG	100\$	Order now
 DK	100\$	Order now
 FR	100\$	Order now
 PT	100\$	Order now
 NL	100\$	Order now
 CA	80\$	Order now
 JP	80\$	Order now
 SE	70\$	Order now
 BR	60\$	Order now
 TR	60\$	Order now
 NO	50\$	Order now
 RU	50\$	Order now

Lease an existing botnet



Global stats Rap. per time stats

Bot traffic Statistics for [redacted] generated on 2008/08/09

Top 10 Countries		Top 10 new countries today		Top 10 Countries order by bot's reports	
Country	Rating	Country	Rating	Country	Rating
Russia	7099 56%			Russia	626089 59%
United States	1641 13%			United States	163156 15%
Germany	1504 12%			Germany	63896 6%
Netherlands	492 4%			Brazil	24697 2%
Ukraine	237 2%			Ukraine	20728 2%
Brazil	196 2%			Spain	19229 2%
United Kingdom	152 1%			Netherlands	13215 1%
Spain	138 1%			United Kingdom	11816 1%
Belgium	126 1%			Taiwan	11541 1%
Turkey	101 1%			Turkey	10173 1%
Totally: 80		Country Rating totally: 0		Totally bot's reports: 1061892	

Web-based portal bot-management

For a small fee, attackers can rent/purchase members of a larger botnet. Online tools enable remote management and configuration of the botnet agents. Portals include performance monitoring tools – how fast is the spam being sent, DDoS throughput, etc.

CHOOSE YOUR PROJECT

MAIN

- [Manage projects](#)
- [Add project](#)
- [Change info](#)

PROJECT

- [Search by host](#)
- [Search by URI](#)
- [Global searching](#)
- [Online bots](#)

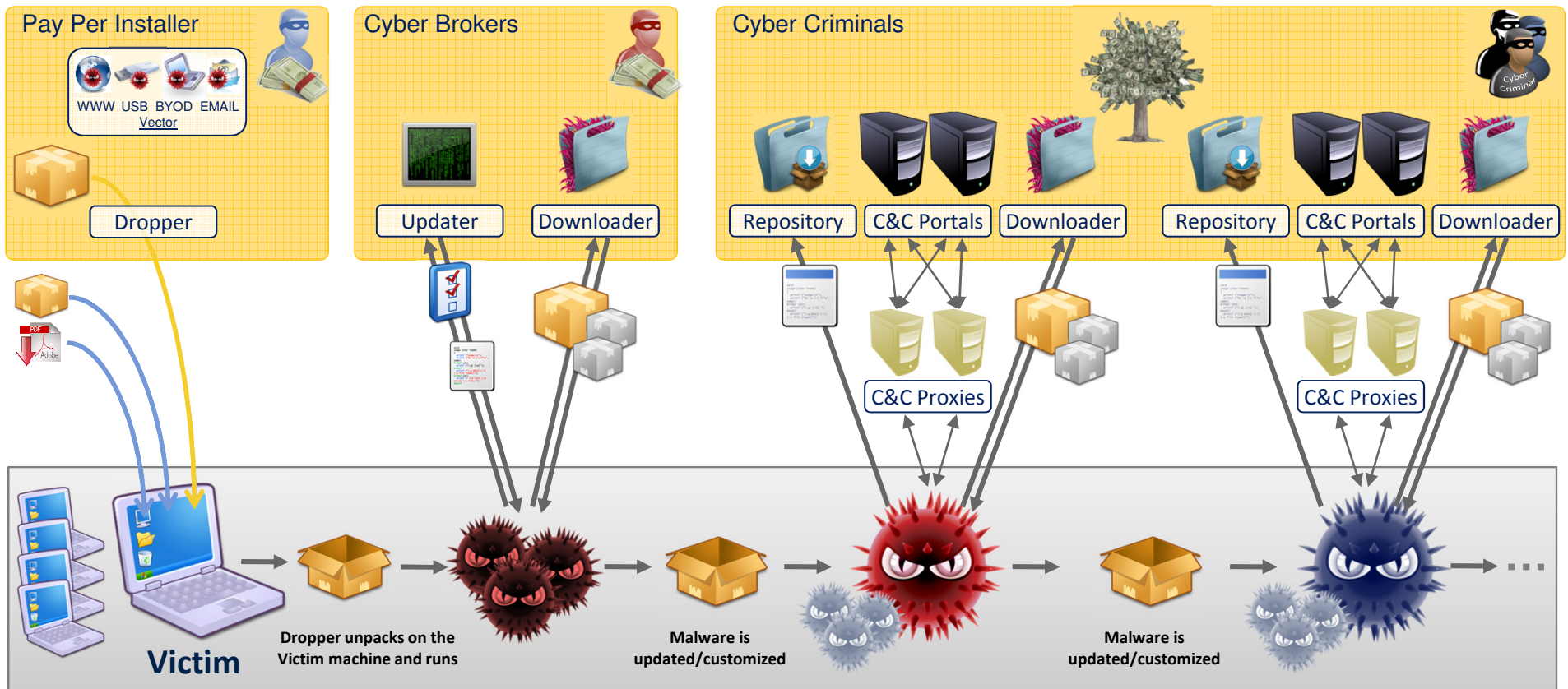
Hello,

Your last session: Tue Aug 5 06:16:31 2008

Active projects:

project	time end	price	bots	index time	size (mb)	action
[redacted]	14/1/2008	1	48 / 1	Tue May 13 00:18:43 2008	0.00	index
[redacted]	6/8/2008	1	1048 / 10000	Tue Aug 5 17:00:52 2008	0.00	index

How can corporations combat the threat!



- Accept You Will Be Infected (traditional defenses don't stop everything)
- Develop a Plan to Rapidly Discover Hidden Threats
 - Use Technologies that combine Threat Intelligence, Content Inspection & Behavioral Based Communication Discovery
 - Use Technologies that provide context and risk based on your network
- Arm your Incident Responders so they can take action

