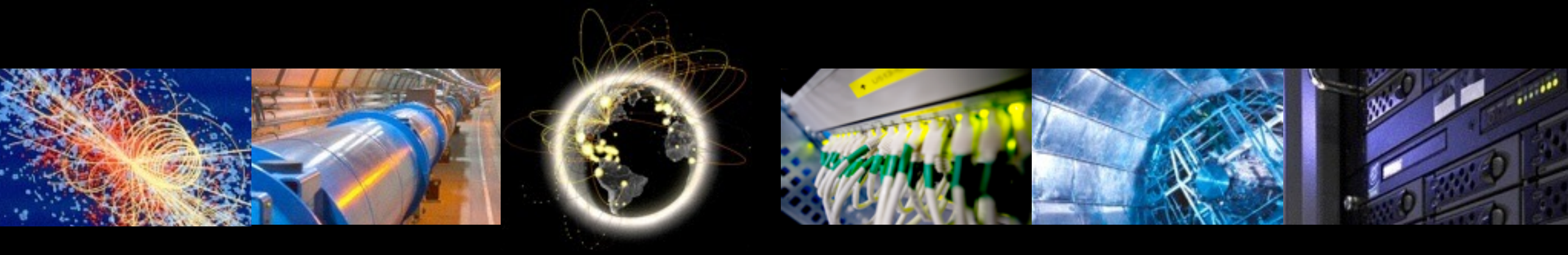
Security update



Romain Wartel, CERN

WLCG Workshop, CHEP 2015, Okinawa

Anecdote

(Source : BBC News)

- Neil Moore is ingenuous
  - Posed as staff from Barclays Bank, Lloyds Bank, etc.
  - Managed to persuade large organisations to give him vast sums of money
  - Sometimes he answered calls from victims using a man's voice and then pretended to transfer the call to a colleague before resuming the conversation in a woman's voice
  - Had previously used four different aliases to commit fraud worth £1,819,000 in total
  - Sent in prison…until…

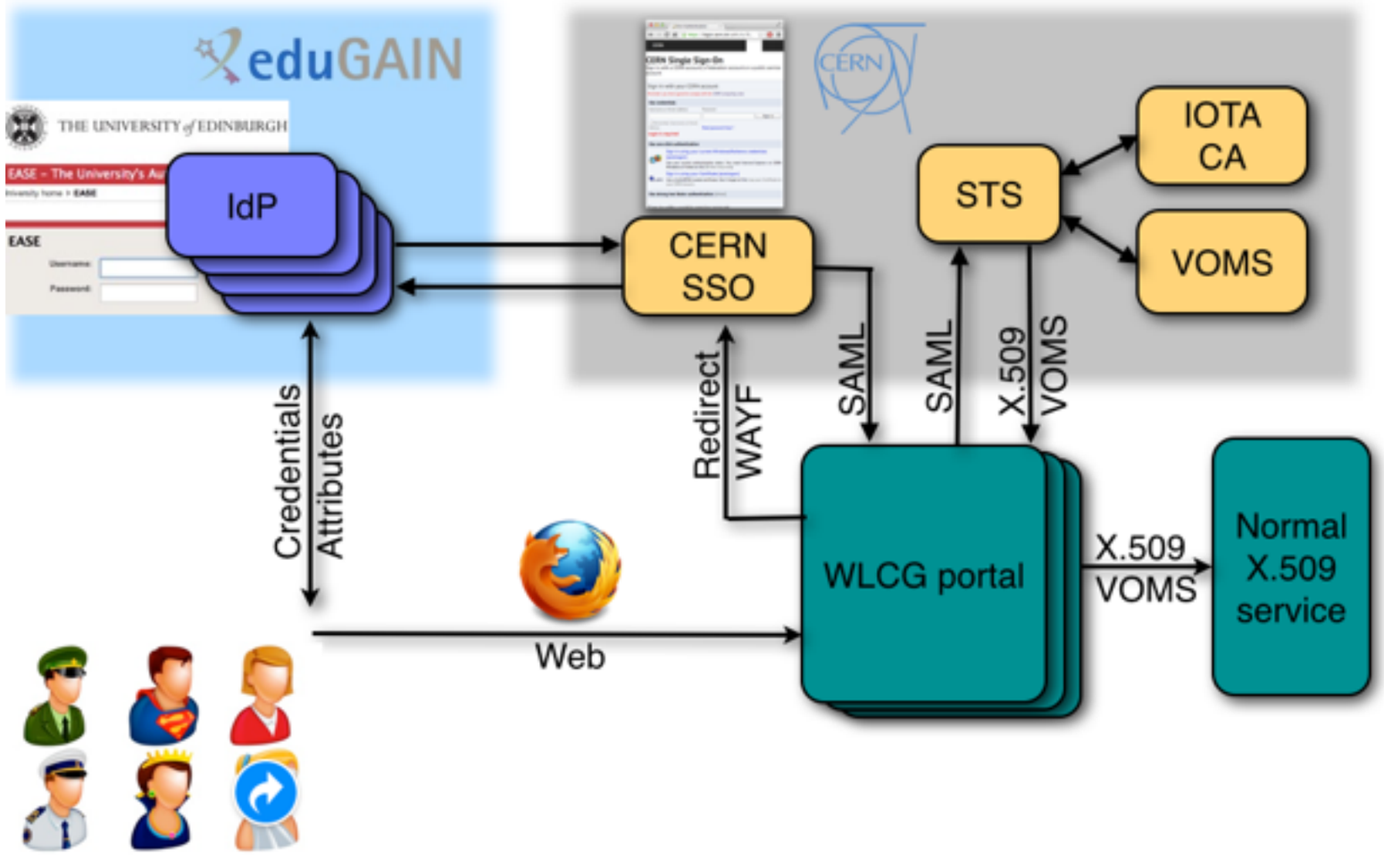
Anecdote

- How did Neil Moore escape from a UK prison?
  - Obtained access to a smartphone from cell
  - Searched public information,
  - Set up a fake domain and related email accounts
    - Similar to the court service's official URL
    - Used the name of an investigating officer, giving the address and contact details for the Royal Courts of Justice.
  - Posed as a court clerk and sent instructions for his release to custody inbox
  - Staff prison released him
  - Had 3 days head-start before somebody noticed…

Identity federation

- Identity management basic building block
- Expected in every future computing e-infrastructure services
- No longer one account per service ; Just one global identity

- (now hopefully) familiar goal:

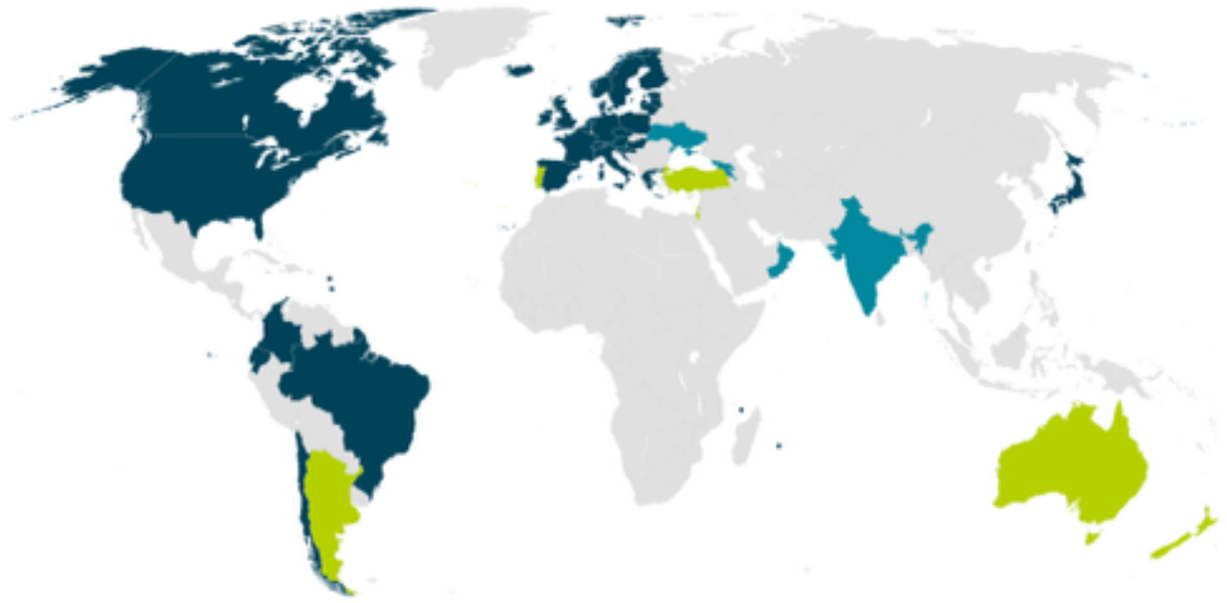


Identity federation

- Status
  - Slowly implementing the missing components
  - A lot of application-specific changes need to be made
    - Vidyo, plugins for online CAs, VOMS, etc.
  - One-by-one troubleshooting generally needed for inter-federation
- Issues
  - The amount of technical work is really significant
  - Trust, policy and data protection issues non-trivial
  - No obligation or agreement, moral or legal for operational security
  - Hitting a number of technical, legal and cultural barriers
  - Global issue, not just HEP
  - Negotiating and agreeing with more people globally means more time

Identity federation

- Progress
  - Communities, projects and people are now better organised
  - International Code of Conduct being worked on
    - Should help improving trust between participants
  - Policy work very well received, more documents to come
    - e.g. incident response
  - AARC, the H2020 EU project, bringing some hope
    - However, we have to manage expectations - 24 months project!



AARC?

GÉANT ASSOCIATION

Authentication and Authorisation for Research and Collaboration

- support the collaboration model across institutional and sector borders
- advance mechanisms that will improve the experience for users
- guarantee their privacy and security

- build on the very many existing and evolving components
  ESFRI clusters, eduGAIN, national AAI federations, NGIs, IGTF, SCI, SirTFi, …
- design, test and pilot any missing components
- **integrate them** with existing working flows

AARC – Authentication and Authorisation for Research and Collaboration

- Two-year project
- 19 funded plus 2 unfunded
  - Coordinated by the Amsterdam Office
  - NRENs, e-Infrastructure providers and Libraries as equal partners
- About 3M euro budget
- Starting date 1 May, 2015

AARC - Goals

- OUTREACH and TRAINING
  - To lower entry barriers for organisations to join national federations
  - To improve penetration of federated access

- TECHNICAL and POLICY Work
  - To develop an integrated AAI built on production services (i.e. eduGAIN)
  - To define an incident response framework to work in a federated context
  - To agree on a LoA baseline for the R&E community
  - To pilot new components and best practices guidelines in existing production services

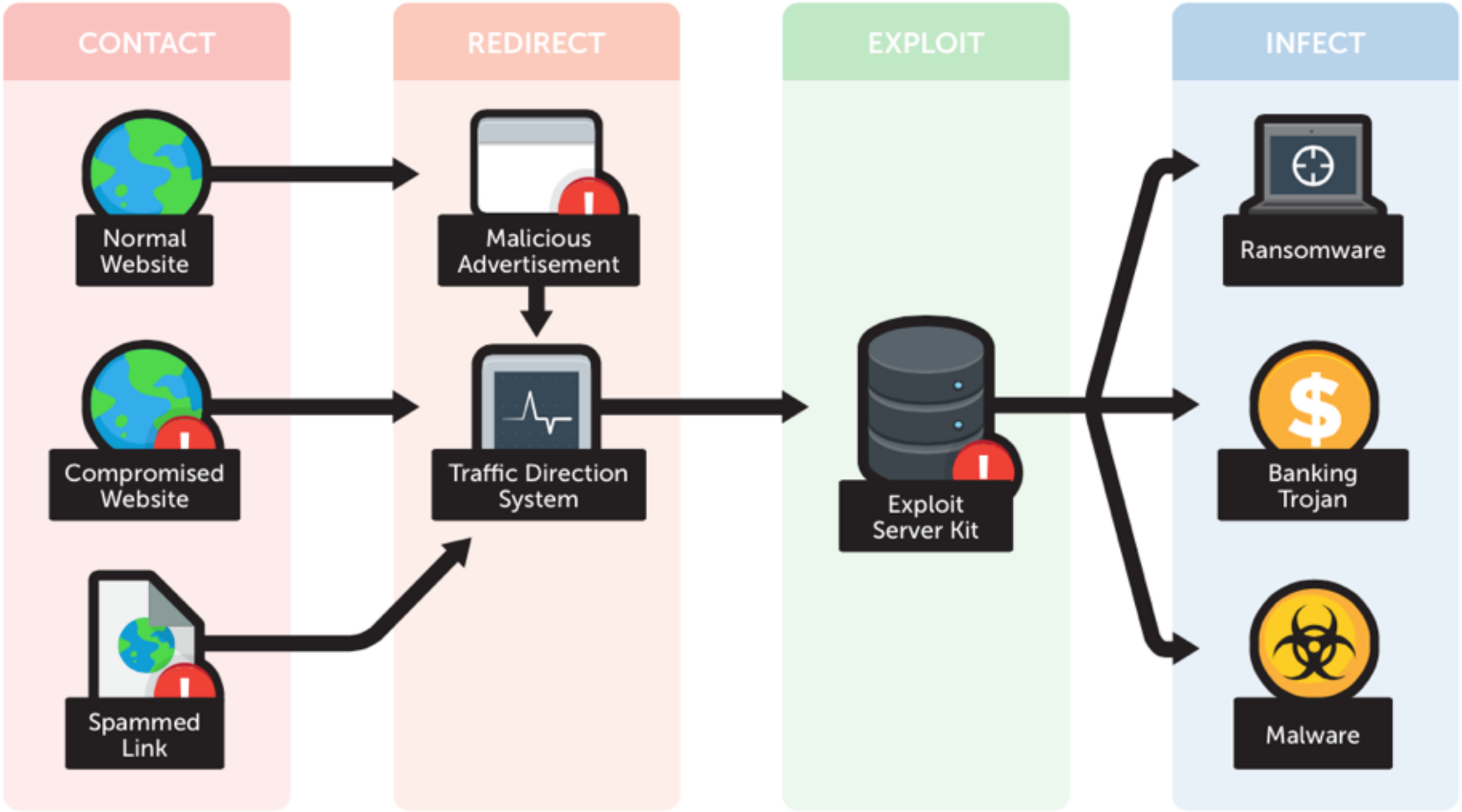
Identity federation

- Priorities for the research communities in AARC:
  - International AuthN
  - Attribute harmonization
  - Unique, non-reusable identifier for each user
  - Attribute management for AuthZ
  - Wider adoption of the CoC
  - Outreach, training material for SPs
  - Clearer contact points in eduGAIN
  - Non-web use case

Global computing

- While the communities built global services…
  …criminal organisation think alike
- Profound changes in the underground economy and organised crime in the last years
  - Cybercrime highly profitable
  - Profits can be earned globally
  - Risks are minimum
  - Malware-as-a-service
  - Specialised markets, new areas of expertise: new opportunities
- Interpol:
  - Cybercrime is bigger than cocaine, heroin and marijuana trafficking put together
  - 80% online crime connected to international organised gangs
- This has significant impacts for our community

Exploitation chain



Source: Trend Micro

Commercial EK

- Strong consolidation of the underground market/economy
  - Severe competition between a handful of exploit kits (EK)
  - Huge progress on time-to-market for exploits
    - Only hours/days before vulnerabilities available in EK
    - CVE-2015-0311 discovered as a Flash "0-day" in Angler EK

	Nuclear Exploit Kit	Sweet Orange Exploit Kit	FlashPack Exploit Kit	Rig Exploit Kit	Angler Exploit Kit	Magnitude Exploit Kit	Fiesta Exploit Kit	Styx Exploit Kit
Internet Explorer	CVE-2013-2551	CVE-2013-2551 CVE-2014-0322 CVE-2014-6332	CVE-2013-2551 CVE-2013-3918 CVE-2014-0322	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551	CVE-2013-2551
Microsoft Silverlight	CVE-2013-0074			CVE-2013-0074	CVE-2013-0074		CVE-2013-0074	CVE-2013-0074
Adobe Flash	CVE-2014-0515 CVE-2014-0569	CVE-2014-0515 CVE-2014-0569	CVE-2013-0634 CVE-2014-0497 CVE-2014-0515 CVE-2014-0569	CVE-2014-0569	CVE-2014-0515 CVE-2014-0569	CVE-2014-0515	CVE-2014-0497 CVE-2014-0569	CVE-2014-0515
Adobe Acrobat/ Reader	CVE-2010-0188						CVE-2010-0188	
Oracle Java	CVE-2012-0507		CVE-2013-2460 CVE-2013-2471		CVE-2013-2465		CVE-2012-0507	
XMLDOM ActiveX	CVE-2013-7331			CVE-2013-7331	CVE-2013-7331			CVE-2013-7331

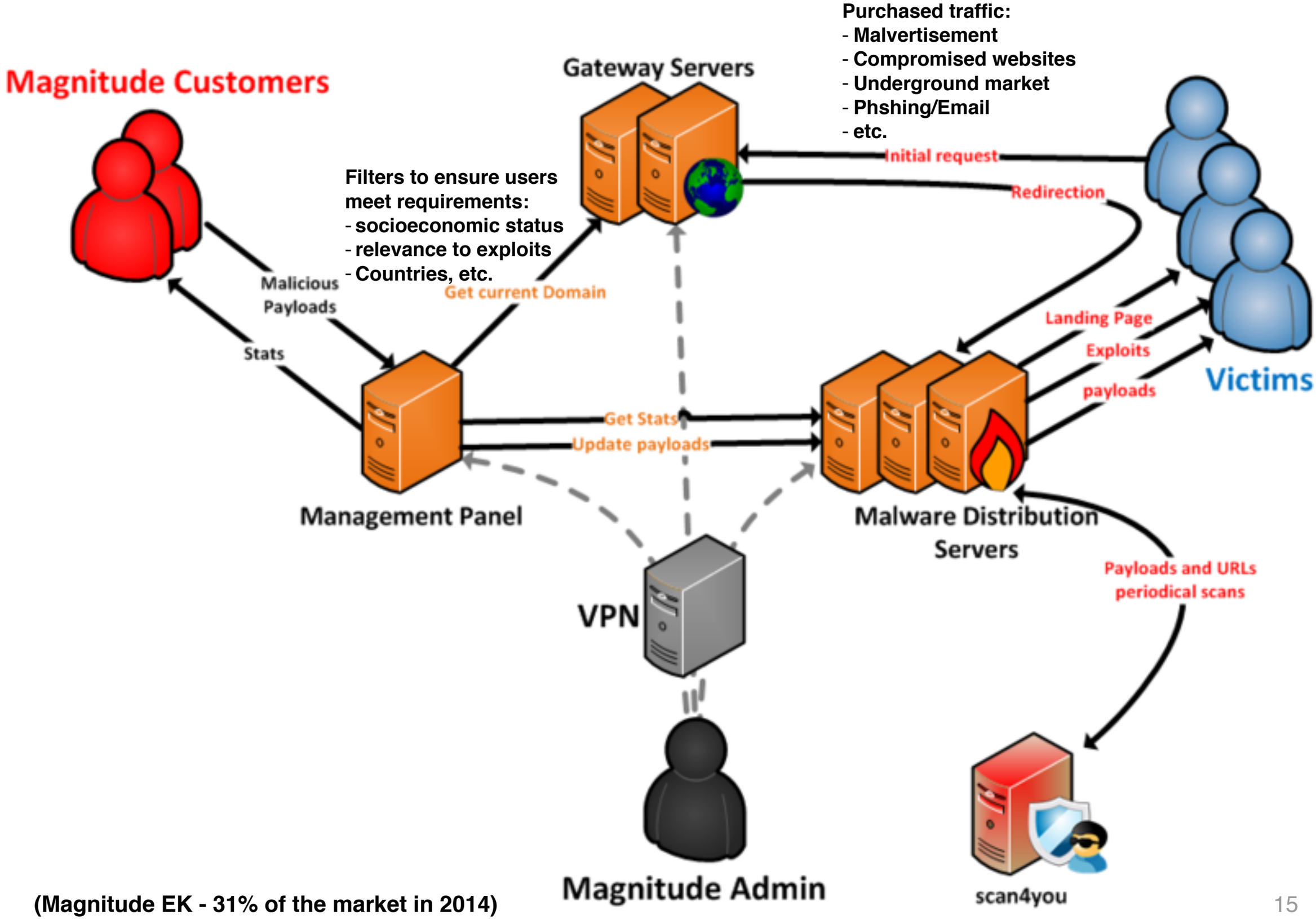
http://blog.trendmicro.com/trendlabs-security-intelligence/whats-new-in-exploit-kits-in-2014/

Commercial EK

Antivirus Products Detected in Exploit Kits				
Exploit Kit	**Angler**	**Nuclear**	**Rig**	**Styx**
Evasion target (antivirus or virtualization software)	Kaspersky	Kaspersky	Kaspersky	Kaspersky
	Trend Micro	Trend Micro	Trend Micro	ESET
	VMWare			
	VirtualBox			
	Parallels Desktop			

Payload Evasion Summary		
	Payload (PE) Encryption	**Fileless Infection**
FlashPack	×	×
Rig	✓	×
Magnitude	✓	×
Nuclear	✓	×
Fiesta	✓	×
Angler	✓	✓
SweetOrange	×	×
GongDa	×	×
Styx	×	×
HanJuan	✓	✓

Malware-as-a-service



(Magnitude EK - 31% of the market in 2014)

Getting to the victims

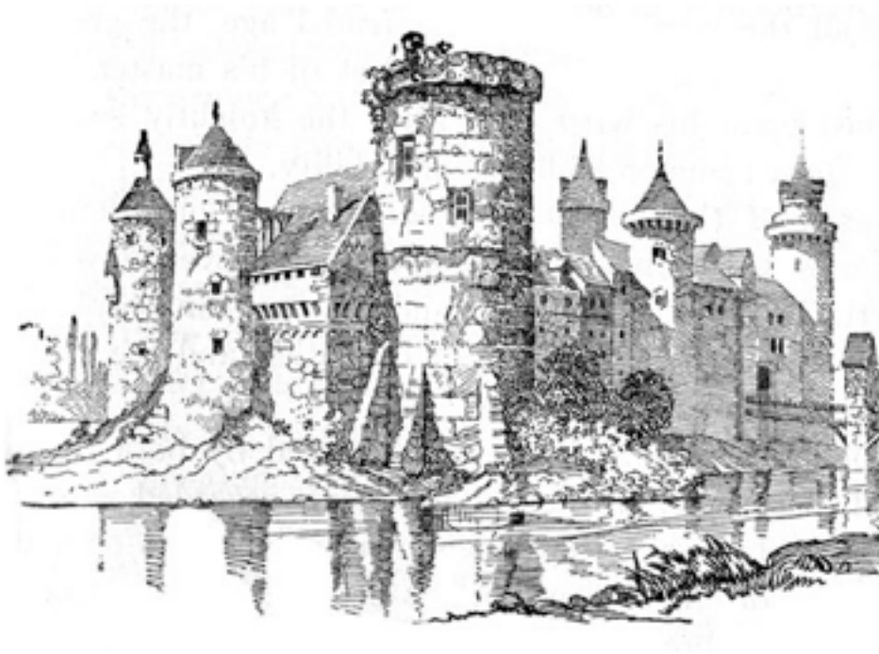
- Email: leading source of compromise
  - 90%+ of breaches caused by spear phishing
  - Extremely effective ("shooting phish in a barrel"):
    - 10 emails = 1 click guaranteed
    - Targeted phishing: ~70% success rate
    - HEPiX 2015: 9% click rate (good + technical audience!)
  - Since Dec 2014 CERN is victim of a targeted phishing campaign
    - ~20 variants of the Geodo malware, not detected/blocked by any major antivirus
    - Constant evolution: Cridex, Feodo, Geodo, Dridex, etc.
    - Short email campaign ~6-8h maximum
    - Antivirus vendor need ~9-24h to detect

Extracting marketable data

- Personal data
  - Credit card, accounts, personal details, contacts, billing information, etc.
- Medical data
  - Names, birth dates, and policy numbers
  - Buy medical equipment or drugs, make-up insurance claims
  - Worth 10-20x more than credit card details! (and harder to cancel)
- Corporate data
  - Intellectual property, espionage, payroll system
- Computing resources
  - CPU, bandwidth, storage, Web hosting, Mail servers
- Everything centrally harvested, then filtered and split for sale to different buyers

Security: the old vs the new

- Very “medieval” approach
- Sites usually build their security architecture around:
  - Well defined security perimeters



- Priorities:
  - Reinforce center perimeters (services)
  - Concentrate resources and expertise on data center security (linux)

- Goal : keep the attackers outside of the data center

- While this worked will in the 90s and early 2000s, this model is clearly no longer working

Linux = Windows

- The landscape has changed:
  - Data center security = laptop security
  - Linux = Windows

- Most large attacks now target both platforms
  - Attackers needs both data and computing services
  - Relying solely on “multi layers” security is bound to fail

- Data center compromises occur via admin credentials theft

- Web, mail and mobile platforms are a primary battlefields
  - And a firewall will not help

Linux = Windows

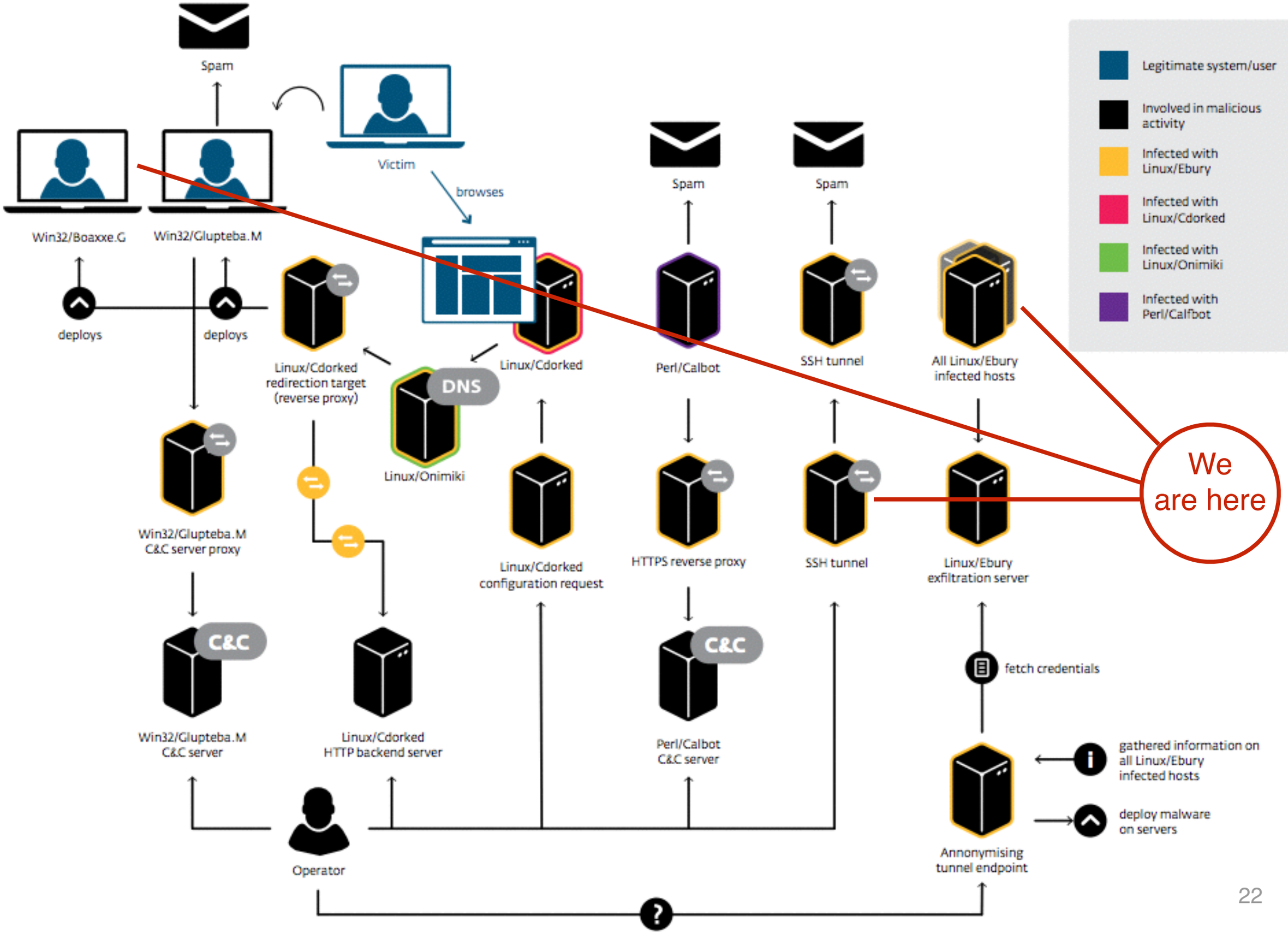
- Modern strategy
  - Treat all platforms and devices as equally risky for your services
  - Focus on people and procedures instead
    - e.g: what is the password reset procedure of the people in charge of your domain settings?
  - Treat security incidents as part of normal operations
  - Protect both services… and people

Operation Windigo (2011 - now)

- 30,000+ unique servers compromised in the last two years
  - kernel.org, Linux Foundation, CPanel, many universities and research lab, public and private sector organisations
- A full ecosystem of advanced malware
  - Ebury: SSH backdoor. Controls servers + steals credentials

    (signed RPM installed "in the past". Infects libkeyutils.so)
  - LinuxCdorked: stealth, file-less, multi-platform HTTP backdoor
  - Perl/Calfbot: manages the payload, 35 million spams/day
  - Linux/Onimiki: supporting Linux DNS malware
  - Win32/Boaxxe.G: Click fraud malware
  - Win32/Glupteba.M: Generic proxy/downloader malware
- Not just software: large-scale malicious infrastructure
  - Fully distributed, complex infrastructure, using multi-tiered proxies, lots of obfuscation and encryption
- International gang, highly profitable activity - still ongoing

Operation Windigo (2011 - now)



Ransomware

- Plenty of schemes

- ESET Case study: http://www.welivesecurity.com/wp-content/uploads/2014/12/torrent_locker.pdf
- Torrent Locker (~9 months study)
  - Out of 39,670 infected systems, 570 or 1.45% have paid the ransom to the criminals
    These 570 payments made to the gang tell us they made between US$292,700 and US$585,401 in Bitcoins.
  - According to data from the C&C servers, at least 284,716,813 documents have been encrypted so far.
  - TorrentLocker actors have been reacting to online reports by defeating indicators of compromise (IOCs) used for detection and changing the way they use AES from CTR to CBC mode after a method for extracting the keystream was disclosed.

Doxing

- Doxing: searching and exposing personal information
  - Home address, pictures, kids information and school location, etc.
  - Initially for personal revenge
  - Now tied to identity theft, corporate activity

- This is a HEP problem as well
  - Happened recently in our community
  - Multiple HEP staff targeted, including death threats

- Difficult to deal with this in a very open community
  - Most research public, lots of articles, papers and presentations…
  - Large amount of personal information handled and disseminated
  - Data protection policies are essential

Learn & adapt

- Defend your organisation or (Linux) data center
  - Must start defending Windows/Web/mobile realms too
  - Ultimately, must defend people
- International collaboration is our main asset
  - Main intrusion detection system at CERN in the last 5 years
- International community: sharing and trusting
  - Strong knowledge on attack methods and tools
  - Report about actual compromises or data leaks in our community
  - Invaluable intelligence
  - Engage & participate!
- Work on connections with industry and law enforcement
  - Attackers arrested on a regular basis for attacking HEP organisations

Learn & adapt

- Protect your people:
  - Raise awareness
  - Organise training events (tools, methods)
  - Write and advertise clear policies
  - Do not overlook personal use and devices

- Protect your organisation
  - Understand your adversaries
  - Invest resources to have sufficient in-house capabilities
  - Contribute to global efforts against cybercrime (botnet takedown…)
  - Build your network of contacts in the security community
  - Invest in threat intelligence and technical means to use it
  - Treat security incidents as part of normal operations

Future of academic security

- Main trends for the medium/long term
  - Security as a global issue
    - Including: operations, traceability, incident handling, policies
    - Increased costs likely (traceability, expertise)
  - Global adversaries
    - Impossible to defend without dedicated (WLCG) experts
      - Distributed security models unlikely to work
      - Most sites will most likely deal with “traceability” requests
    - Security vendors will likely participate in incidents/forensics
    - Government-induces threats will continue to increase
    - Global response, from a global public/private community
      - Threat intelligence will be a key aspect
  - Target switching
    - Services will no longer be the main targets
    - Users and service managers will be

Future of academic security

- Key areas to work on:
  - Design our infrastructure(s) to deal with global incident response
    - Have appropriate legal, policy and technical tools
    - Remove concept of community/organisation/academic/public-private boundaries
  - Participate/invest in global trust framework
  - Contribute to global internet security issues
  - Establish a solid network of security contacts (intelligence)
  - Liaise with security vendors and law enforcement
  - Improve data protection and our usage of personal information
  - Educate the community to protect its people

Conclusions

- Both identity federation and security operations are:
  - Global issues
  - Put the emphasis on people
- Data center security is depending on external factors
  - Mobile devices, laptops, etc.
  - Ultimately, people are the target
- Adversaries are now too sophisticated to deal with alone
  - Commercial and government adversaries will continue to rise
  - Critical to liaise with other experts, in and outside the community
- It is important to invest time & effort wisely, and now
  - Joining late or ignoring these issues will be very costly