

security is not an island
HILTONMALTA

24th Annual **FIRST**
Conference
MALTA
17 - 22 June 2012



Incident Response in Large Complex Business Environments

Ramses Martinez
Ismail Guneydas
Yahoo!

The Yahoo! logo is displayed in a purple, serif font with a registered trademark symbol.

24th Annual
FIRST
Conference

MALTA

17 - 22 June 2012

Agenda

1. Definitions
2. Challenges
3. Solutions
4. Case Studies

Definition of 'Large & Complex'

1. Scale:
 - >100k Production Systems.
 - > 1 Petabyte of data generated per week
2. Diversity:
 - > 4 Major Business Lines.
 - Business lines must 'interact' with each other.
 - Business lines must be have internal/external dependencies.
 - Heterogeneous technology environment.
3. Geographical Distribution:
 - Employee base in at least 10 different countries.
 - Providing services globally.

Challenges: Scalability, Cost & Resources

1. System Forensic Tools
 - Per-node approach is not cost effective.
 - Speed of traditional acquisition not adequate.
 - Resources required may not be available.
2. Network Forensic Tools
 - Bandwidth/cost limitations.
 - Geographical distribution constraints.
3. Detection, Alerting, and Correlation
 - Per byte log analysis model not cost effective.
 - High false positive rate.
 - Linear searches simply break down at this scale.
4. Resources

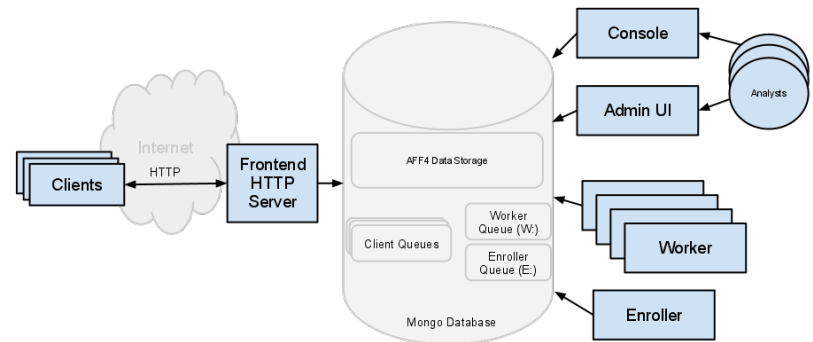
However, what ever alternatives to traditional methods we decide to use must always preserve the integrity of the investigative process, comply with the law and obviously yield good results.

Solutions: Scalability & Cost

System Forensic Tools

GRR Live Forensic Framework:

- Lightweight and very fast
- Accessible anywhere
- Open source
- Secure communications channel
- Memory and disk forensics
- Multiple platform support
- Supports multiple system sequential analysis
- Great detective control, can be configured to do ongoing analysis of processes, registry keys and other system artifacts to detect infections at early stages.



<http://code.google.com/p/grr/downloads/detail?name=GRRArchitecture.png&can=2&q=>

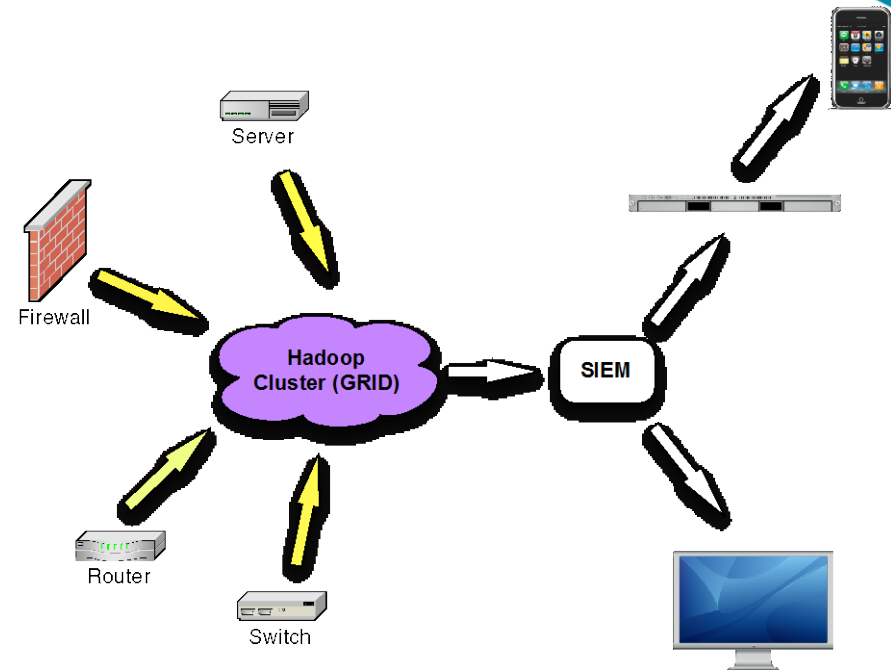
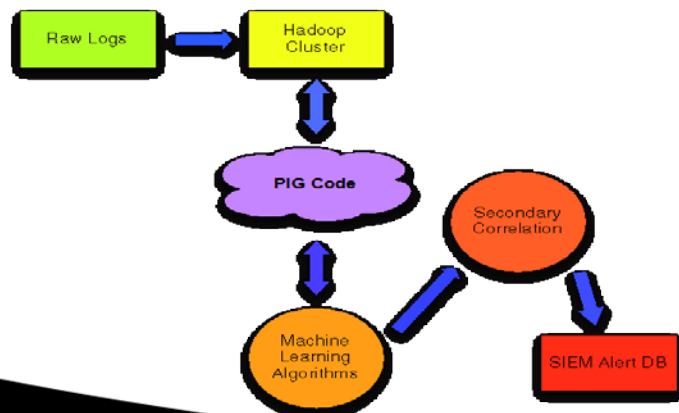
Solutions: Scalability & Cost

Network Forensic Tools

Hadoop cluster & Machine Learning:

- Average of 900% gain in speed vs. linear searches
- Open source.
- Multiple platform support.
- Supports multiple system parallel queries.
- Highly customizable.
- Can be configured to do ongoing analysis.

<http://hadoop.apache.org/>



Case Study: Fraudulent Ticket Sales

- Set of 1962 potentially fraudulent yahoo e-mails with passwords along with other information was reported to us by an external resources to us on December 02, 2011.
- Extracted account ID's and possible passwords from the file
- Run a grid script to match e-mail addresses to user ids.
- Run a grid script to check if the reported passwords were real
- Run a grid script to check for associations to unreported accounts

Before:

- [2358|Maria|Surrova|mariasurrova@yahoo.com|c0deb4910|GWTG56](#)

After

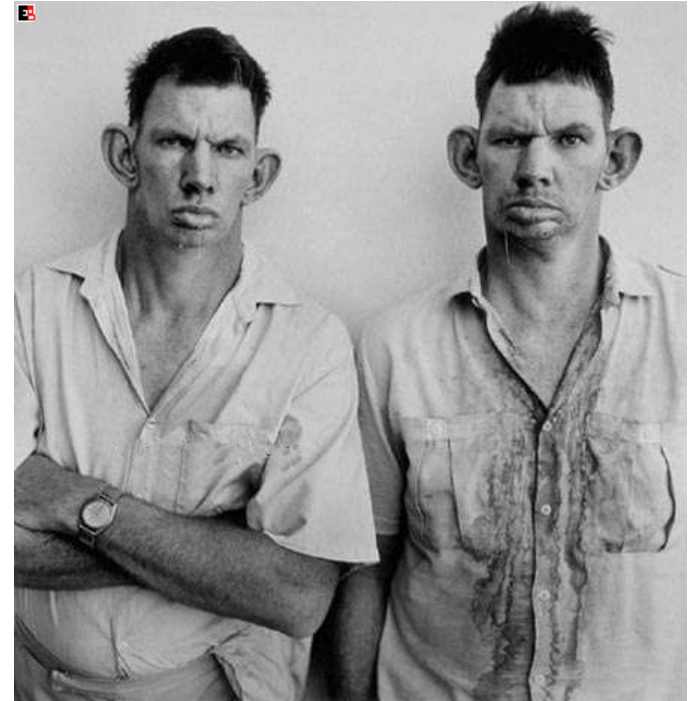
- One file with all e-mails , one file with all passwords
- [mariasurrova@yahoo.com](#)
- [c0deb4910](#)

Case Study: Initial Data Analysis

- All of them has a unique characteristic:
 - 9 characters with all lower cases and numbers
:c0deb4910
- Accounts have same verification questions
 - What is the first name of your favorite uncle?
 - What was your favorite food as a child?
- All of the answers were
33 character lower case combined with numbers.
 - Ahsdufkdoplsjdk3jd7j8ks8d6hr64jks

100% Match

- Not compromised users but machine registrations. But for what? What were attackers' goals?




Case Study: Account Analysis

- Accounts created in last two months and registration IP's geographically distributed across the US.
- Moreover, IP addresses are from both residential (right pic.) businesses (i.e. hosting companies) as well as proxy servers (Left pic.).
- There was no failed login activity on those accounts.
- There was no e-mails sent from those e-mail boxes.
- All accounts used to registered with a particular VOIP company .

General IP Information

IP: 69.116.173.219
Decimal: 1165274587
Hostname: ool-4574addb.dyn.optonline.net
ISP: Optimum Online
Organization: Optimum Online
Services: [Suspected network sharing device](#)
Type: [Broadband](#)
Assignment: [Dynamic IP](#)
Blacklist:


Geolocation Information

Country: United States 
State/Region: New Jersey
City: Lodi
Latitude: 40.8783
Longitude: -74.0813
Area Code: 973
Postal Code: 07644

General IP Information

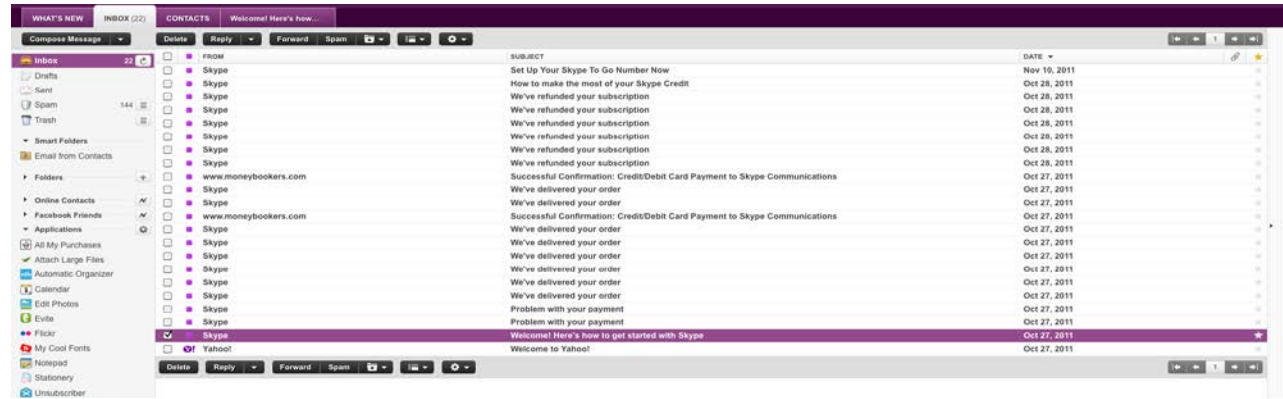
IP: 97.104.122.78
Decimal: 1634237006
Hostname: cpe-97-104-122-78.cfl.res.rr.com
ISP: Road Runner
Organization: Road Runner
Services: None detected
Type: [Broadband](#)
Assignment: [Dynamic IP](#)
Blacklist:

Geolocation Information

Country: United States 
State/Region: Florida
City: Winter Park
Latitude: 28.6051
Longitude: -81.3322
Area Code: 407

The other commonality between those accounts, there were tickets were purchased using those e-mails from a company ticket sales and distribution company based.

Case Study: IP → Geolocation Correlation



You purchased 2 tickets to:

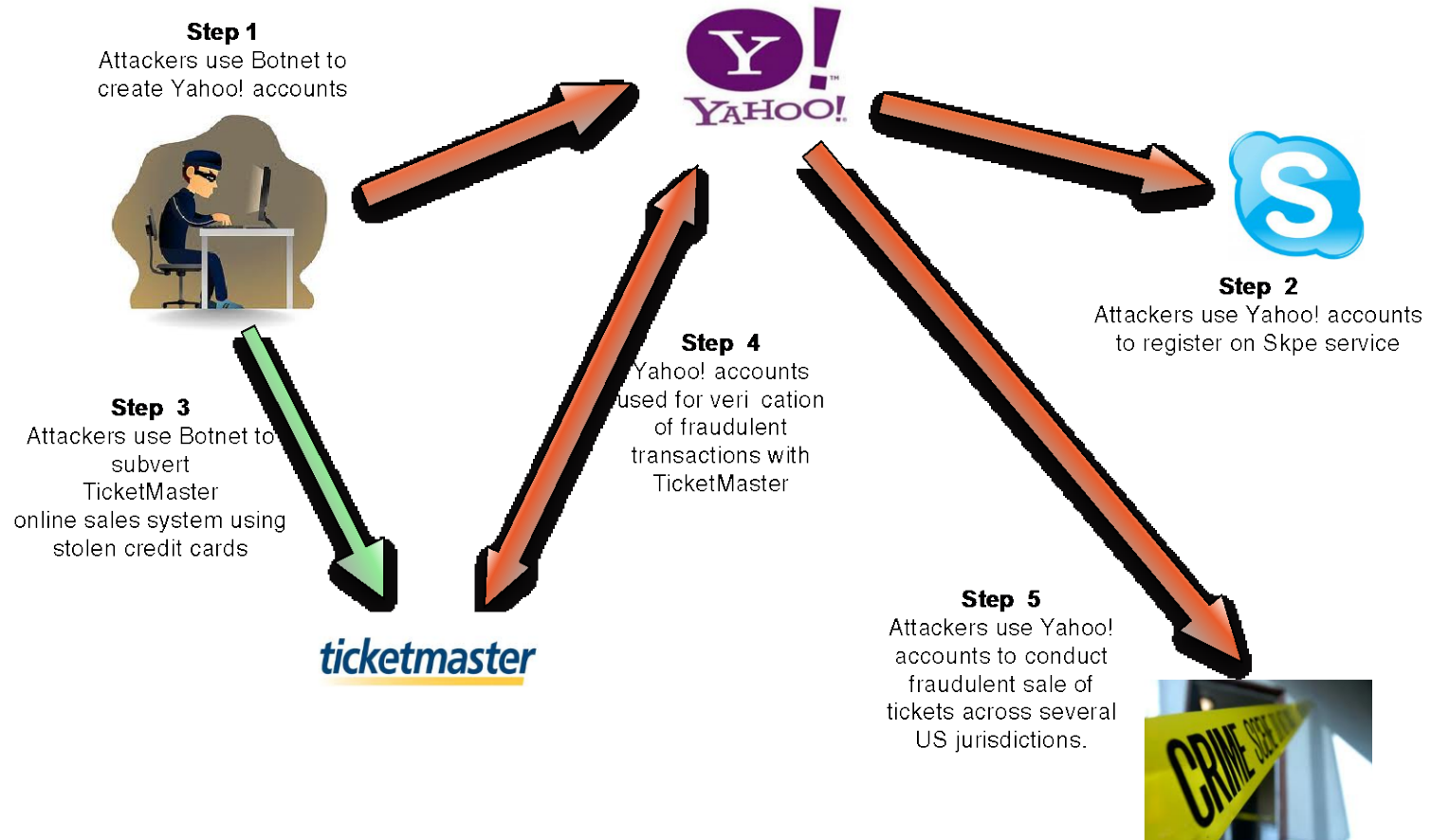
Denver Broncos vs. Detroit Lions
Sprint's Authority Field At Mile High, Denver, CO
Sun, Oct 30, 2011 02:05 PM

Order for: Michael Harris
Seat location: section 306, row 10, seats 11-12
Total Charge: US \$ 647.95

AMERICAN EXPRESS® CARDMEMBERS have access to advanced tickets, preferred seating and great savings on select Ticketmaster events. Visit Ticketmaster.com/AmericanExpress to learn more about these exclusive benefits!
Thanks again for using Ticketmaster.

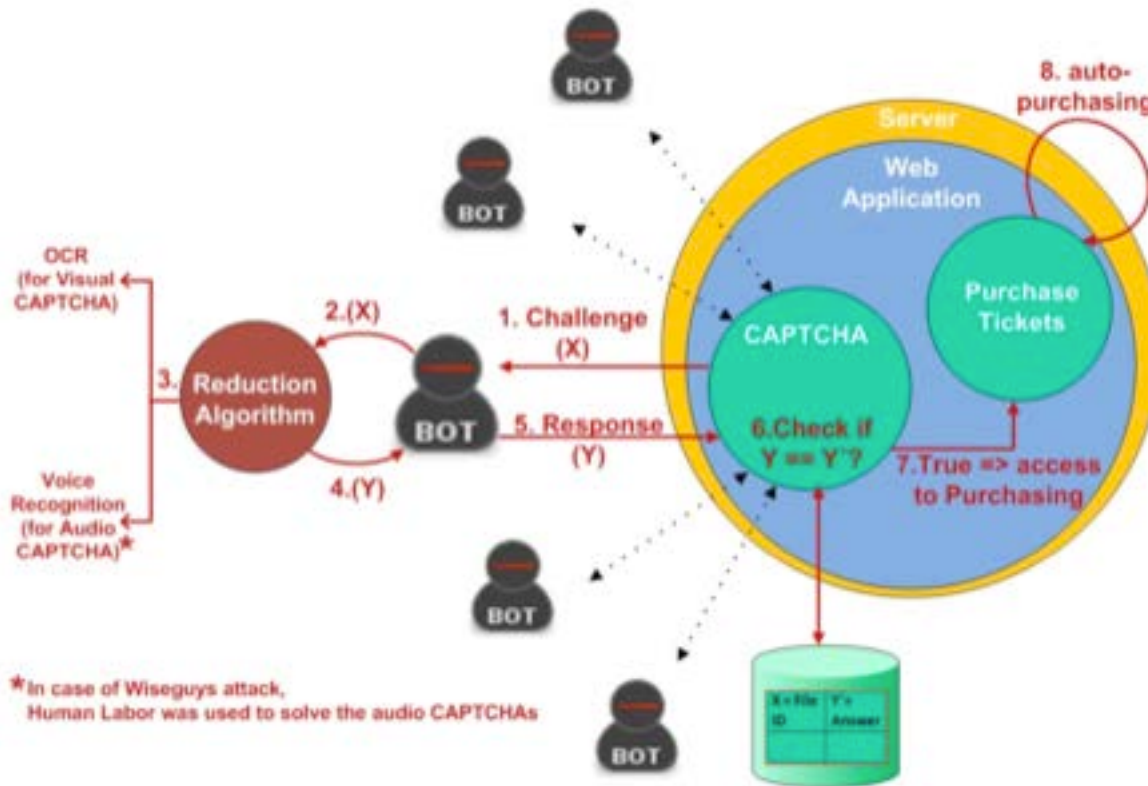
Direct correlation between the registration IP of each account and the state where sporting events tickets were being purchased.

Case Study: How the Attack Works



* Red arrows indicate points where Yahoo! infrastructure is abused
The FBI investigated a similar case of defrauding ticket vendors last year:
<http://www.fbi.gov/newark/press-releases/2010/nk030110.htm>

Case Study: FBI Wiseguy Operation



Case Study: Conclusions

- Attackers use some clever techniques to beat CAPTCHA mechanisms
- Attackers had access a botnet or compromised systems across to USA (literally every single state in US)
- They focused on high-end expensive seats at events.
- They purchase a ticket in a state where they had compromised systems.
- They have enough people to go through all e-mail accounts to respond any verification mechanisms
- After initial attack the accounts were used for other fraudulent schemes like targeting jewelry stores and online banking.
- The attack involved a strong physical (human) component and was likely conducted by an organized criminal group.

Order Confirmation

Thank you for shopping with Helzberg.

You should be feeling pretty good right now - you just bought something from one of the nation's most established, trusted jewelers. If you registered during the checkout process, or are an existing registered user and would like to track your order online, your order confirmation number is: **ORDER CONFIRMATION NUMBER: ML_2609801**

When your order ships we will send you an email containing the shipper tracking number and your credit card will be charged the total amount (personalized jewelry is charged 2 days from the date of purchase), which includes merchandise, any applicable shipping charges and sales tax. For all the details, please [click here](#) to read about our order processing and shipping times. If you have any questions or comments, please contact our Customer Service Department at 800.435.9237 , or email us at customerservice@helzberg.com. It's a good idea to have your order confirmation number available when you call, or include it in your email message. Operator hours are Monday through Friday 8am-5pm Central Time.

Thanks again for your order!

Sincerely,
Helzberg

ORDER CONFIRMATION NUMBER: ML_2609801

Billing Info		Payment Method		
Jaymes Allen 10 W Crook Lane Bella Vista, AR 72714 US 479-852-1239		MC *****8992 for \$1098.53		
Shipping Info		Shipping Method		
Jaymes Allen 160 Antrim Rd. Coventry, CT 06238 US 860-521-4589		Saturday Delivery: \$32.95 (We use UPS or Fedex for all deliveries.)		
Item #	Product	Qty	Price Each	Total Price
1675850	2ct TW* Moissanite Three-Stone Ring Size: 7.0	1	\$999.99	\$999.99
Clearance items do not qualify for discount offers and is excluded from discount calculations.				

Order Subtotal: \$999.99
Shipping Total: \$32.95
Tax Total: \$65.50