ThreatGRID

Malware Analysis & Threat Intelligence

Threats, Content and Context

(What a year in the life of a MD5 taught us)

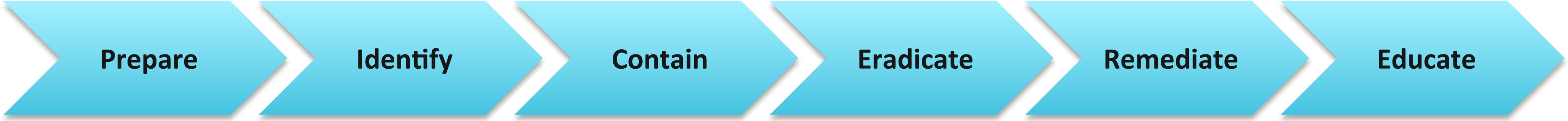
Stuff about me

- Co-founder and CTO at ThreatGRID
  - Platform for Malware Analysis and Correlation
  - Provider of Actionable Threat Content & Threat Telemetry
- Background in:
  - Incident Response
  - Malware Analysis
  - Campaign Intelligence
- Instructor for:
  - Incident Response
  - Network Forensics, etc…

Agenda

- Methodology: Everyone has one
- Threat Content: Everyone needs it
- Threat Content: What is it?
- Threat Content: How do you select it?
- Threat Content: How do you use it?
- A Year in the life of an MD5

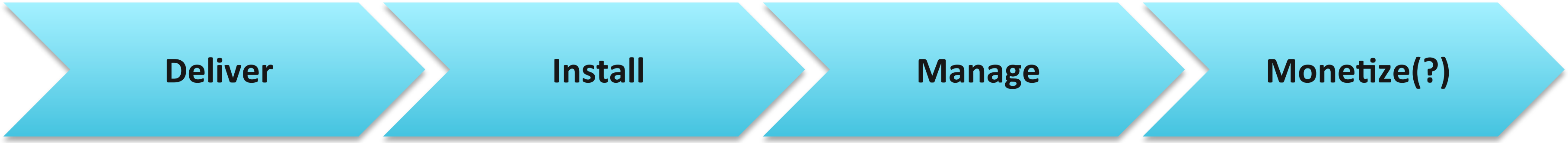
Our (the good guys) Methodology


Prepare
Identify
Contain
Eradicate
Remediate
Educate

- Drives our Incident Response procedures
- Creates repeatable processes for the CIRC/CIRT
- Improves our defenses
- Is time consuming
- Resource intensive
- Scaling issues

We found a needle!

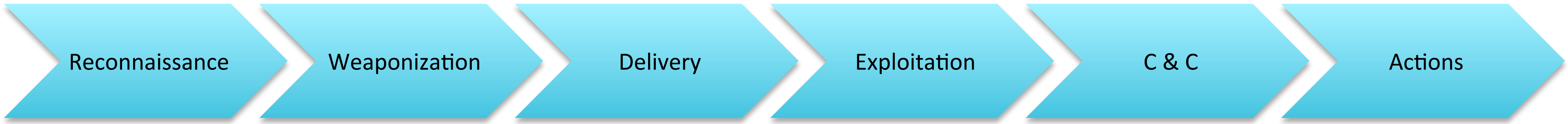
Their (the bad guys) Methodology


Deliver
Install
Manage
Monetize(?)

- Scales pretty damn well
- High success rate regardless of motivation
  - Nation State Driven
  - Politic, Economic and/or Military Advantage
  - Monetization (Crimeware)
  - Hacktivism

They produce a lot of these ->

A little more Specific (targeted) Methodology

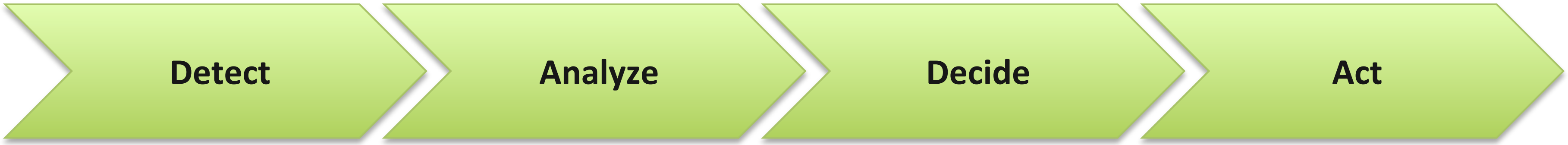


- Reconnaissance
  - Mapping Organization Structure – employees, networks, relationships, vendors, partners
- Weaponization
  - Placing payload into delivery mechanism – PDF, CDF, Website
- Delivery
  - Delivery of Payload – spear phish, watering-hole attack, usb
- Exploitation
  - Targeting a vulnerability, a user or a combination of the two
  - Single phase or multi-phase
- Command & Control
  - Check-in, automated & manual control of assets
- Actions
  - Lateral movement, establishing drop points, exfiltration

http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

It's good to have goals

- Find Anomalies
- Generate Indicators of Compromise
- Apply them where we can
- Reduce the TTL of incidents
- Determine Root Cause
- Retire to somewhere warm

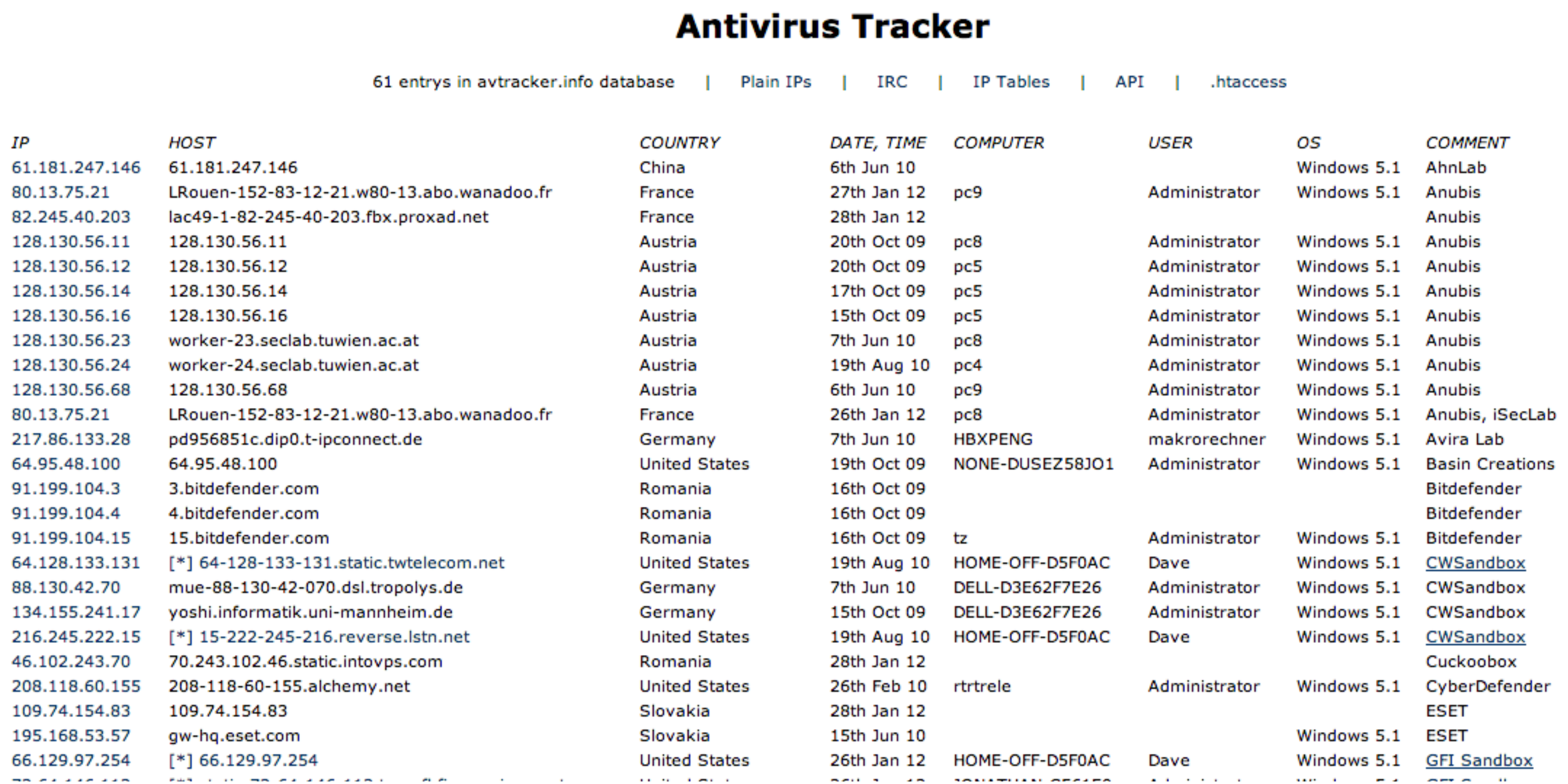


- So how do we speed some of this up?

We need to know more…a lot more

- Event Driven vs. Intelligence Driven Security Programs
- A threat intelligence function is longer a 'nice to have'
- Role
  - Incident Response Function or sub group
  - Researching attacks & potential impact
  - Identify Indicators – tactics, techniques, and procedures (TTP)
  - Produce Actionable Intelligence
  - Collaborate and Share through trusted partnerships
    - ISACs
    - DiB
    - Private Lists & Groups
    - Community Sources

They are gathering intelligence on us



Antivirus Tracker

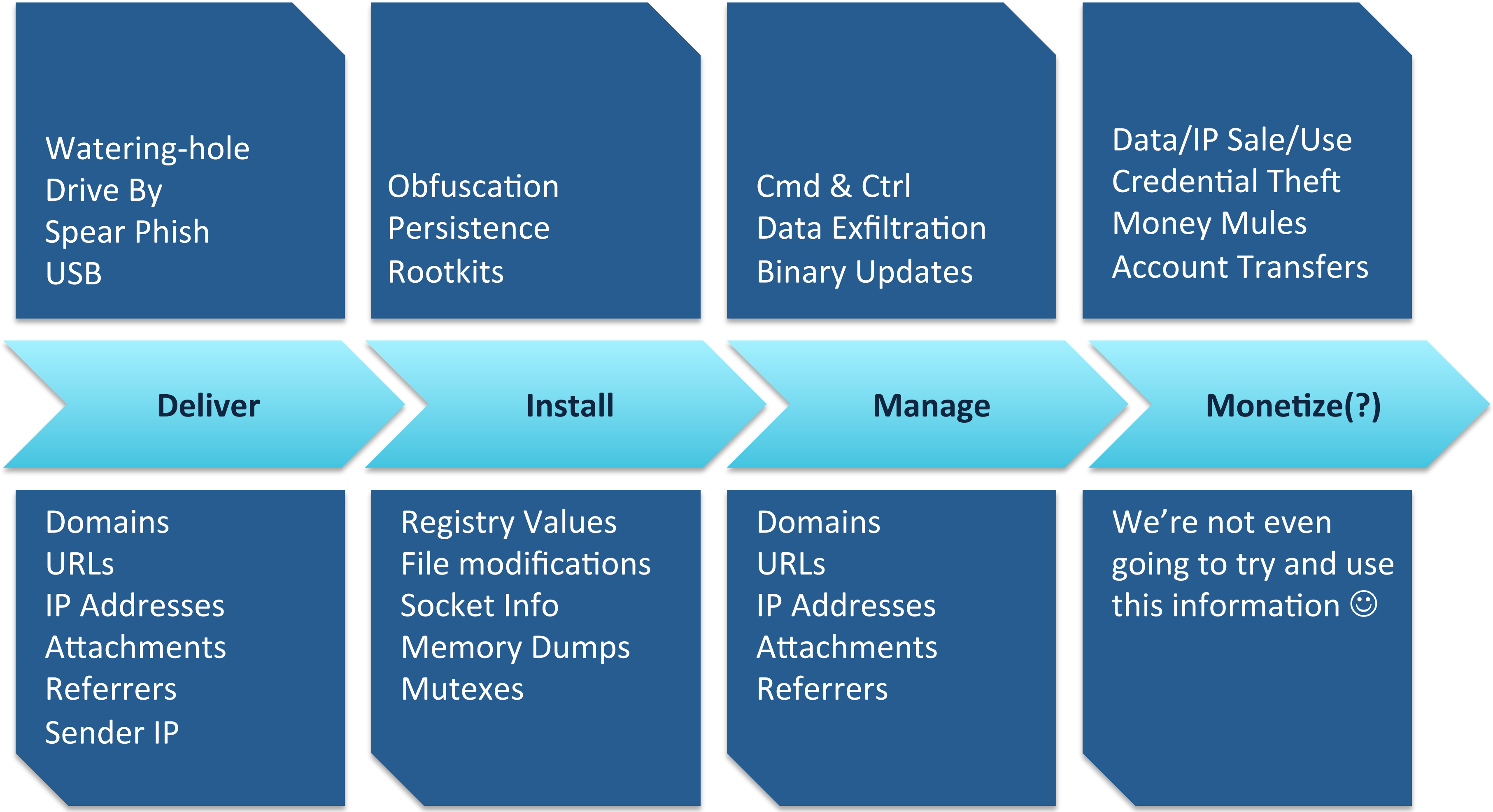
61 entrys in avtracker.info database | Plain IPs | IRC | IP Tables | API | .htaccess

IP	*HOST*	*COUNTRY*	*DATE, TIME*	*COMPUTER*	*USER*	*OS*	*COMMENT*
61.181.247.146	61.181.247.146	China	6th Jun 10			Windows 5.1	AhnLab
80.13.75.21	LRouen-152-83-12-21.w80-13.abo.wanadoo.fr	France	27th Jan 12	pc9	Administrator	Windows 5.1	Anubis
82.245.40.203	lac49-1-82-245-40-203.fbx.proxad.net	France	28th Jan 12				Anubis
128.130.56.11	128.130.56.11	Austria	20th Oct 09	pc8	Administrator	Windows 5.1	Anubis
128.130.56.12	128.130.56.12	Austria	20th Oct 09	pc5	Administrator	Windows 5.1	Anubis
128.130.56.14	128.130.56.14	Austria	17th Oct 09	pc5	Administrator	Windows 5.1	Anubis
128.130.56.16	128.130.56.16	Austria	15th Oct 09	pc5	Administrator	Windows 5.1	Anubis
128.130.56.23	worker-23.seclab.tuwien.ac.at	Austria	7th Jun 10	pc8	Administrator	Windows 5.1	Anubis
128.130.56.24	worker-24.seclab.tuwien.ac.at	Austria	19th Aug 10	pc4	Administrator	Windows 5.1	Anubis
128.130.56.68	128.130.56.68	Austria	6th Jun 10	pc9	Administrator	Windows 5.1	Anubis
80.13.75.21	LRouen-152-83-12-21.w80-13.abo.wanadoo.fr	France	26th Jan 12	pc8	Administrator	Windows 5.1	Anubis, iSecLab
217.86.133.28	pd956851c.dip0.t-ipconnect.de	Germany	7th Jun 10	HBXPENG	makrorechner	Windows 5.1	Avira Lab
64.95.48.100	64.95.48.100	United States	19th Oct 09	NONE-DUSEZ58JO1	Administrator	Windows 5.1	Basin Creations
91.199.104.3	3.bitdefender.com	Romania	16th Oct 09				Bitdefender
91.199.104.4	4.bitdefender.com	Romania	16th Oct 09				Bitdefender
91.199.104.15	15.bitdefender.com	Romania	16th Oct 09	tz	Administrator	Windows 5.1	Bitdefender
64.128.133.131	[*] 64-128-133-131.static.twtelecom.net	United States	19th Aug 10	HOME-OFF-D5F0AC	Dave	Windows 5.1	CWSandbox
88.130.42.70	mue-88-130-42-070.dsl.tropolys.de	Germany	7th Jun 10	DELL-D3E62F7E26	Administrator	Windows 5.1	CWSandbox
134.155.241.17	yoshi.informatik.uni-mannheim.de	Germany	15th Oct 09	DELL-D3E62F7E26	Administrator	Windows 5.1	CWSandbox
216.245.222.15	[*] 15-222-245-216.reverse.lstn.net	United States	19th Aug 10	HOME-OFF-D5F0AC	Dave	Windows 5.1	CWSandbox
46.102.243.70	70.243.102.46.static.intovps.com	Romania	28th Jan 12				Cuckoobox
208.118.60.155	208-118-60-155.alchemy.net	United States	26th Feb 10	rtrtrele	Administrator	Windows 5.1	CyberDefender
109.74.154.83	109.74.154.83	Slovakia	28th Jan 12				ESET
195.168.53.57	gw-hq.eset.com	Slovakia	15th Jun 10			Windows 5.1	ESET
66.129.97.254	[*] 66.129.97.254	United States	26th Jan 12	HOME-OFF-D5F0AC	Dave	Windows 5.1	GFI Sandbox

Finding the bad guys. A workflow

- Given a potential sample/artifact, determine if it is a threat to the organization
- Determine behavioral and static traits
- Compare the behavioral and static traits against existing content
- Using derived context, make a threat assessment and determine criticality
- Utilize context and sample traits to create actionable intelligence
- Apply actionable intelligence to protect organization

Identify the bad guys (Building Indicators)



Watering-hole
Drive By
Spear Phish
USB

Obfuscation
Persistence
Rootkits

Cmd & Ctrl
Data Exfiltration
Binary Updates

Data/IP Sale/Use
Credential Theft
Money Mules
Account Transfers

Deliver **Install** **Manage** **Monetize(?)**

Domains
URLs
IP Addresses
Attachments
Referrers
Sender IP

Registry Values
File modifications
Socket Info
Memory Dumps
Mutexes

Domains
URLs
IP Addresses
Attachments
Referrers

We’re not even going to try and use this information ☺

Creating Indicators. A Technology Flow

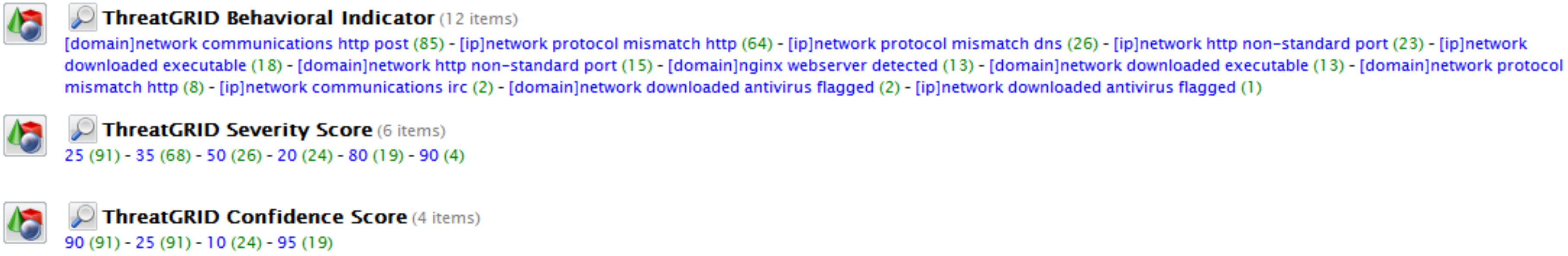
- Threat Content
  - Inbound Information
    - Actionable content/intelligence
    - Raw Malware Samples
      - Obtained from collection points, partners, customers and other feed sources
  - Processing
    - Digestion of inbound information
    - Analysis of Suspected Malware Samples
  - Correlation and Enrichment
    - Using information from multiple sources to enrich
  - Outbound Information
    - Individual Malware Sample Reports
    - Outbound Data Content & Actionable Indicators

How do you select good intelligence sources?

- Buy vs. Build
  - Do you build you own or rely on 3rd Party content? Or is a combination the way to go?
- Quantity vs. Quality
  - How is content produced?
  - What are the sources of the various indicators?
    - Private, Open Source Community
  - What is the % of False Positives in the indicators?
    - When does the data become unusable?
  - How is the data aged out?
  - Whitelisting, Blacklisting, Ranking
- What level of context exists?
  - Why is this Domain bad? Because someone said so….?
- Is the content enriched?
- Are indicators correlated?
  - The analyst needs access to the historical data to determine the threat a sample poses
- Is access automated?
  - REST API, CSV, XML, JSON, Email..?
  - Formats –STIX, CyBox, MAEC, OpenIOC, IODEF, etc…

So I have all these cool indicators…now what?

- Integration points:
  - Network Acquisition & Deep Packet/Session Inspection
  - SIEMs & Network Monitoring
  - Mail Gateways and Mail Spool Analysis
  - DNS & Proxy’s
  - IDS & IPS
  - Host Forensics



ThreatGRID Behavioral Indicator (12 items)
[domain]network communications http post (85) - [ip]network protocol mismatch http (64) - [ip]network protocol mismatch dns (26) - [ip]network http non-standard port (23) - [ip]network downloaded executable (18) - [domain]network http non-standard port (15) - [domain]nginx webserver detected (13) - [domain]network downloaded executable (13) - [domain]network protocol mismatch http (8) - [ip]network communications irc (2) - [domain]network downloaded antivirus flagged (2) - [ip]network downloaded antivirus flagged (1)

ThreatGRID Severity Score (6 items)
25 (91) - 35 (68) - 50 (26) - 20 (24) - 80 (19) - 90 (4)

ThreatGRID Confidence Score (4 items)
90 (91) - 25 (91) - 10 (24) - 95 (19)

ThreatGRID

Malware Analysis & Threat Intelligence

Case Study:

142fd1d9e3e22a1defbf702ec7605192

Why watch a sample for so long?

- Malware is not static
  - Behaviors ~~can~~ do change day to day.
  - A session capture is a **snapshot** of behaviors that day.
  - Many intelligence vendors evaluate whether a given hash is ‘good’ or ‘bad’.
    - The **same hash** can be viewed as **bad** on one day, and trigger indicators of compromise.
    - The **same hash** can be **good** on another day and not trigger indicators of compromise.
    - A **known good** sample can change to a **unknown bad** sample, and if it is whitelisted, it will slip through the cracks.

About our test subject

- 142fd1d9e3e22a1defbf702ec7605192
  - Analyzed approx. 1200 times in a year
  - Discovered when searching PCAP output files from sandbox for IRC traffic to validate internal network protocol dissection code.
  - Uses IRC for command and control.
  - Originally **not detected** by antivirus.
- Basic Characteristics
  - Simple dropper
  - Uses IRC to obtain URLs to download and execute
  - Likely author is part of Affiliate PPI program

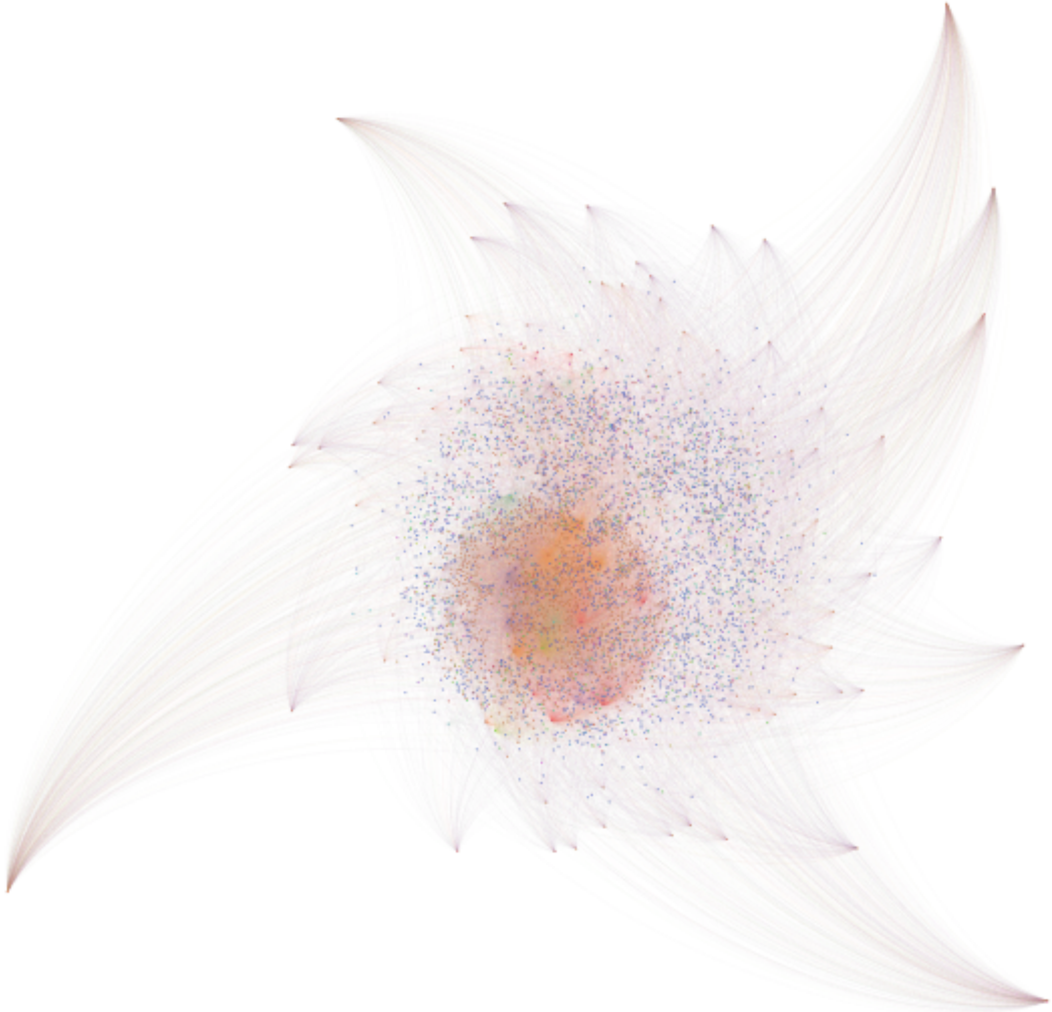
He’s been busy

- Dropper
  - Drops different artifacts almost daily.
    - Zeus, Bredolab, Virut, Cridex, BitcoinMiner, DDoS, etc…
  - Each artifact behaves differently.
    - C&C, Persistence, Weakening, Obfuscation, etc…
  - Uses public IRC networks.
    - Long shelf life
    - Ease of management
- The Gift that Keeps Giving
  - Every run drops different artifacts.
    - Generates new traffic to different networks.
    - Generates new behaviors to analyze.
    - New evasion techniques discovered.
    - New FastFlux botnets discovered.

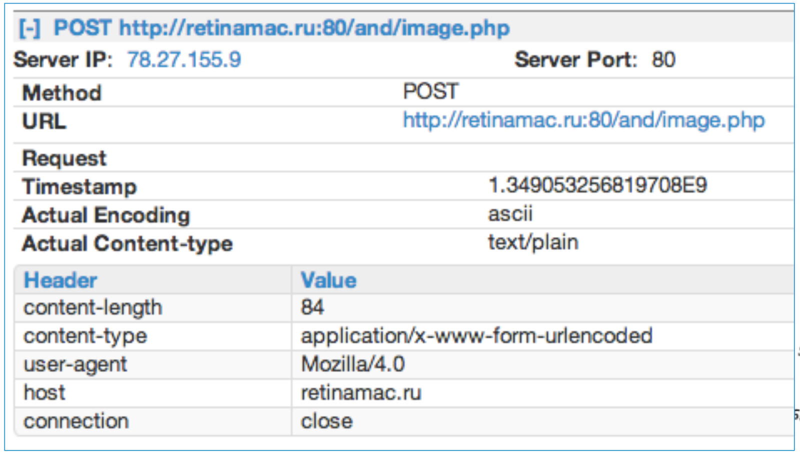
Network Activity

- 3653 Distinct IP Addresses
  - More than 50 Countries
  - Hong Kong, Romania, Russia, Kazakhstan, Ireland, South Korea, United States, China, etc…
- Visualization:
  - Distinct IP Address – Node Circle
  - Country of Origin – Color of Node Circle

Network Activity



Correlation



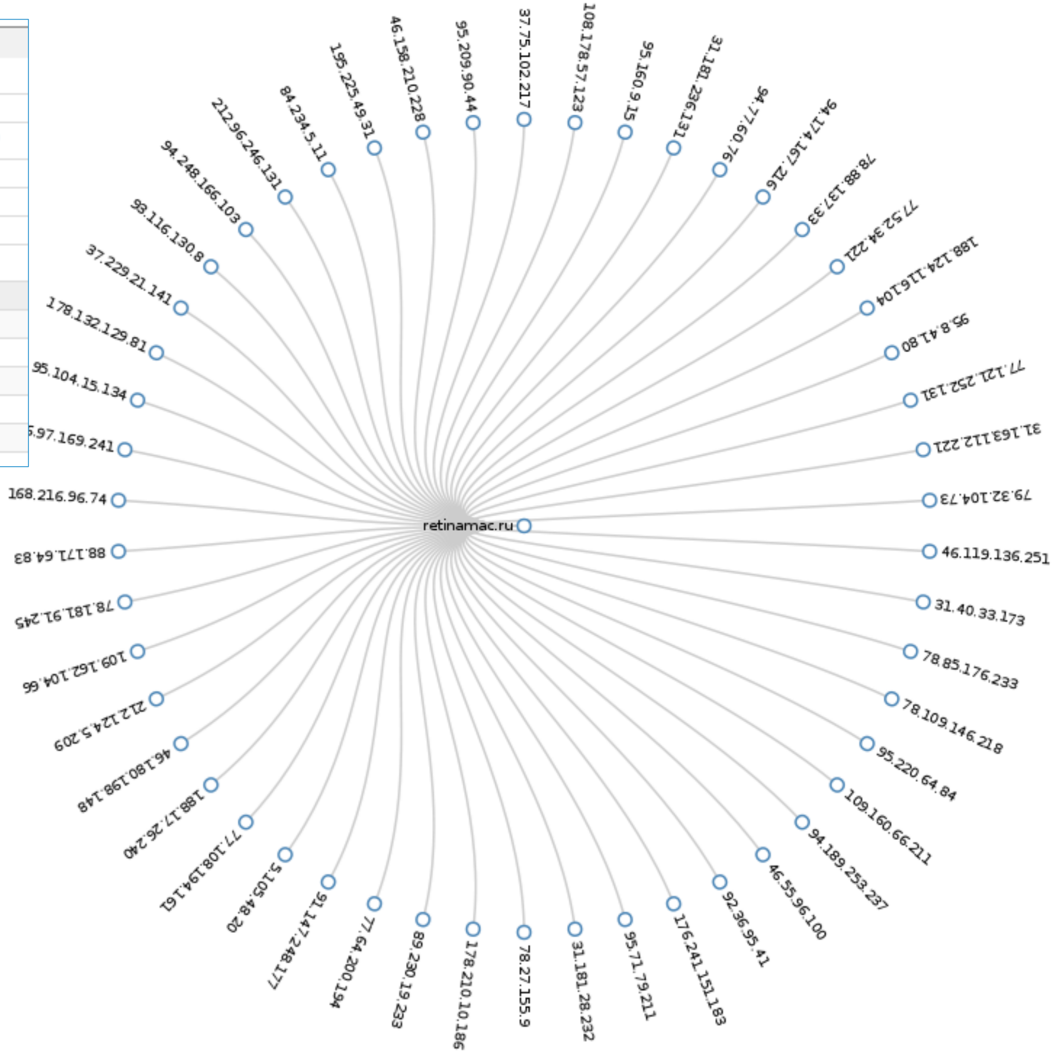
[-] POST http://retinamac.ru:80/and/image.php

Server IP: 78.27.155.9 Server Port: 80

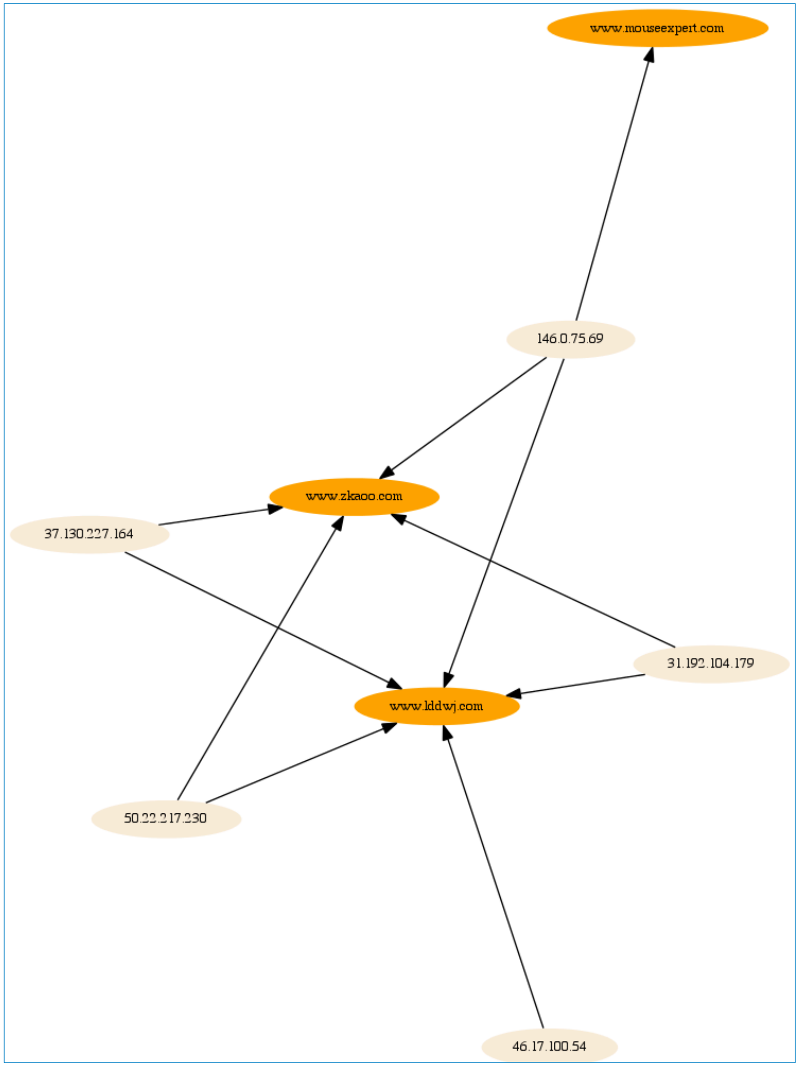
Method	POST
URL	http://retinamac.ru:80/and/image.php
Request	
Timestamp	1.349053256819708E9
Actual Encoding	ascii
Actual Content-type	text/plain

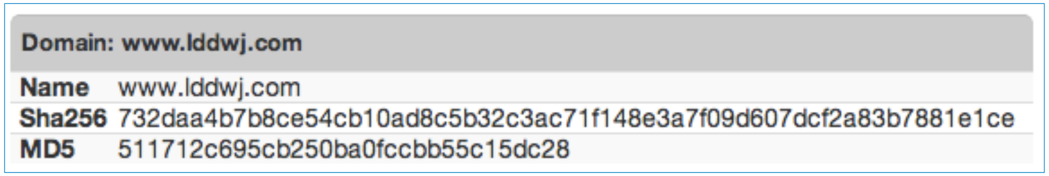
Header	Value
content-length	84
content-type	application/x-www-form-urlencoded
user-agent	Mozilla/4.0
host	retinamac.ru
connection	close

retinamac.ru



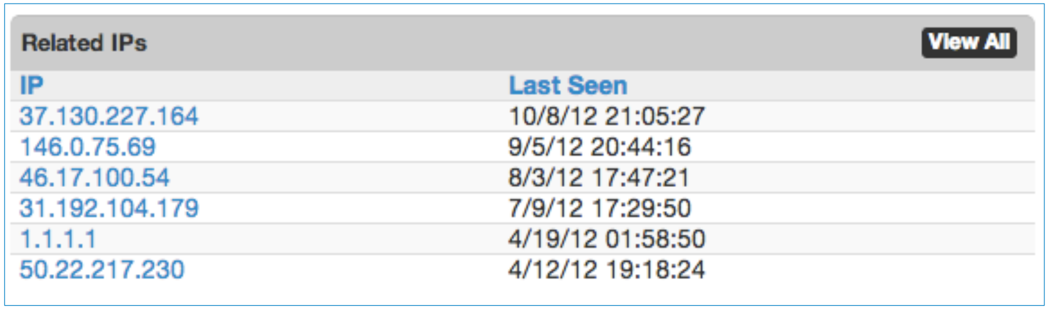
Relationships





Domain: www.lddwj.com

Name	www.lddwj.com
Sha256	732daa4b7b8ce54cb10ad8c5b32c3ac71f148e3a7f09d607dcf2a83b7881e1ce
MD5	511712c695cb250ba0fccbb55c15dc28

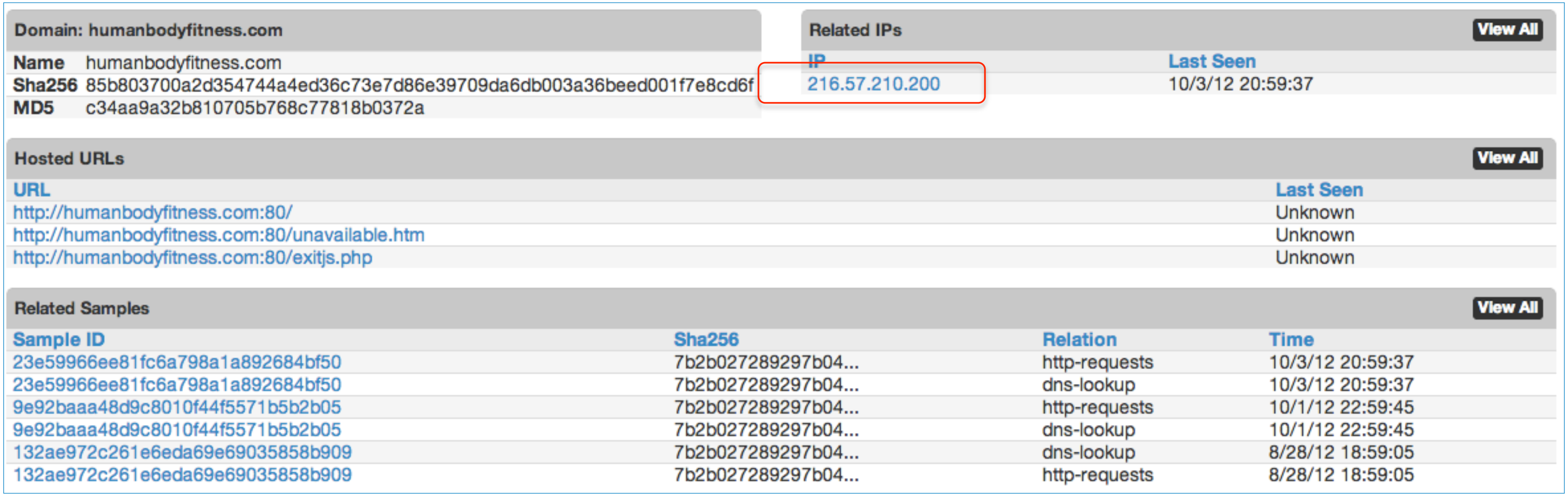


Related IPs View All

IP	Last Seen
37.130.227.164	10/8/12 21:05:27
146.0.75.69	9/5/12 20:44:16
46.17.100.54	8/3/12 17:47:21
31.192.104.179	7/9/12 17:29:50
1.1.1.1	4/19/12 01:58:50
50.22.217.230	4/12/12 19:18:24

www.lddwj.com

Drilling Down



Domain: humanbodyfitness.com

Name	humanbodyfitness.com
Sha256	85b803700a2d354744a4ed36c73e7d86e39709da6db003a36beed001f7e8cd6f
MD5	c34aa9a32b810705b768c77818b0372a

Related IPs

IP	Last Seen
216.57.210.200	10/3/12 20:59:37

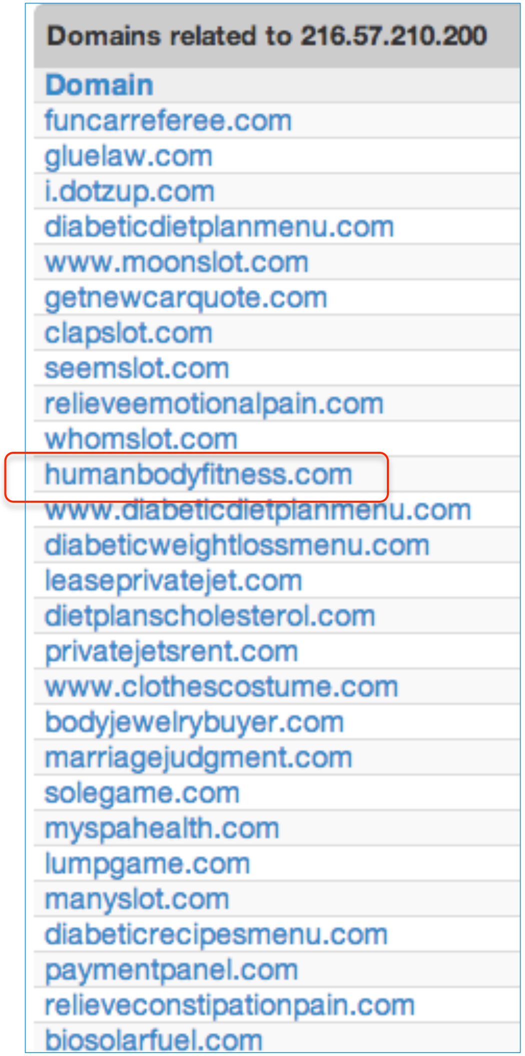
Hosted URLs

URL	Last Seen
http://humanbodyfitness.com:80/	Unknown
http://humanbodyfitness.com:80/unavailable.htm	Unknown
http://humanbodyfitness.com:80/exitjs.php	Unknown

Related Samples

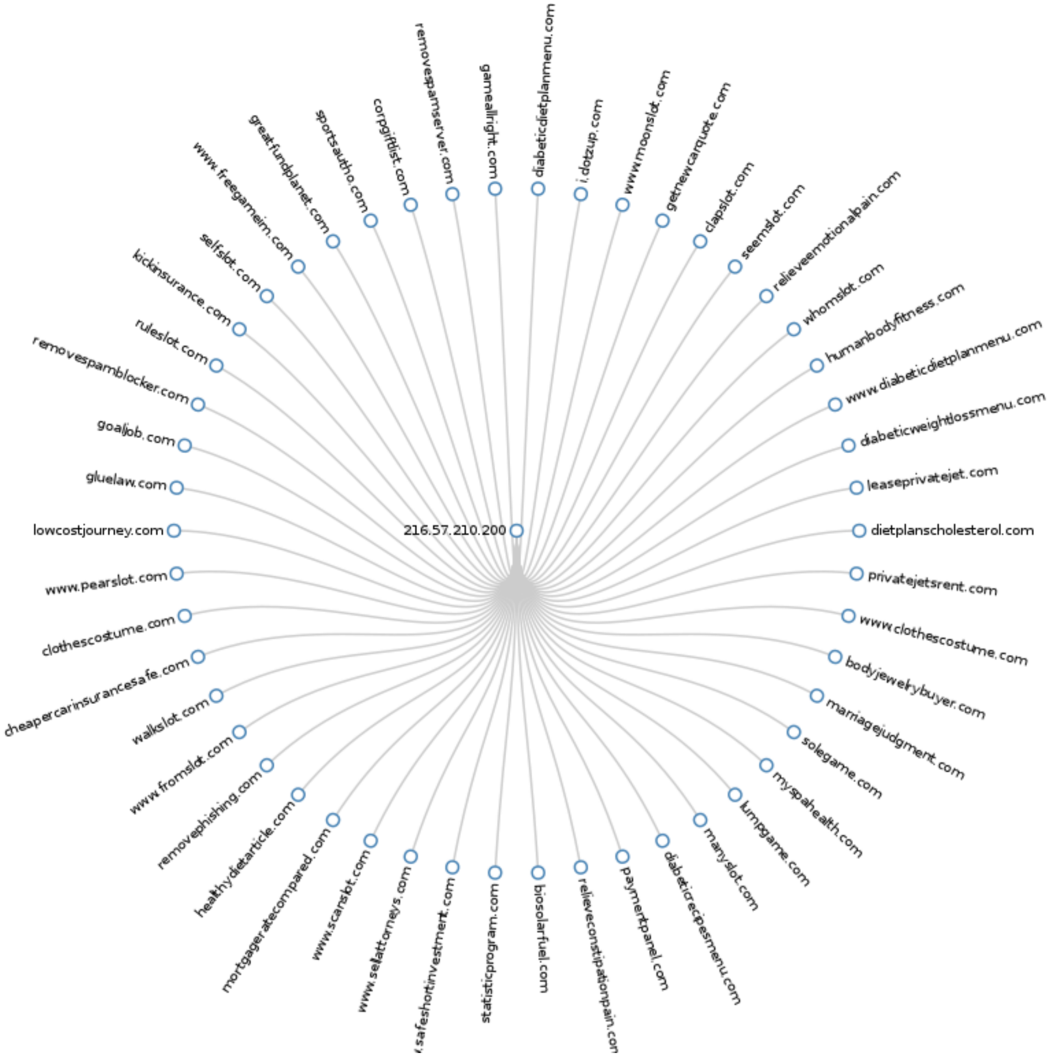
Sample ID	Sha256	Relation	Time
23e59966ee81fc6a798a1a892684bf50	7b2b027289297b04...	http-requests	10/3/12 20:59:37
23e59966ee81fc6a798a1a892684bf50	7b2b027289297b04...	dns-lookup	10/3/12 20:59:37
9e92baaa48d9c8010f44f5571b5b2b05	7b2b027289297b04...	http-requests	10/1/12 22:59:45
9e92baaa48d9c8010f44f5571b5b2b05	7b2b027289297b04...	dns-lookup	10/1/12 22:59:45
132ae972c261e6eda69e69035858b909	7b2b027289297b04...	dns-lookup	8/28/12 18:59:05
132ae972c261e6eda69e69035858b909	7b2b027289297b04...	http-requests	8/28/12 18:59:05

Further Correlation

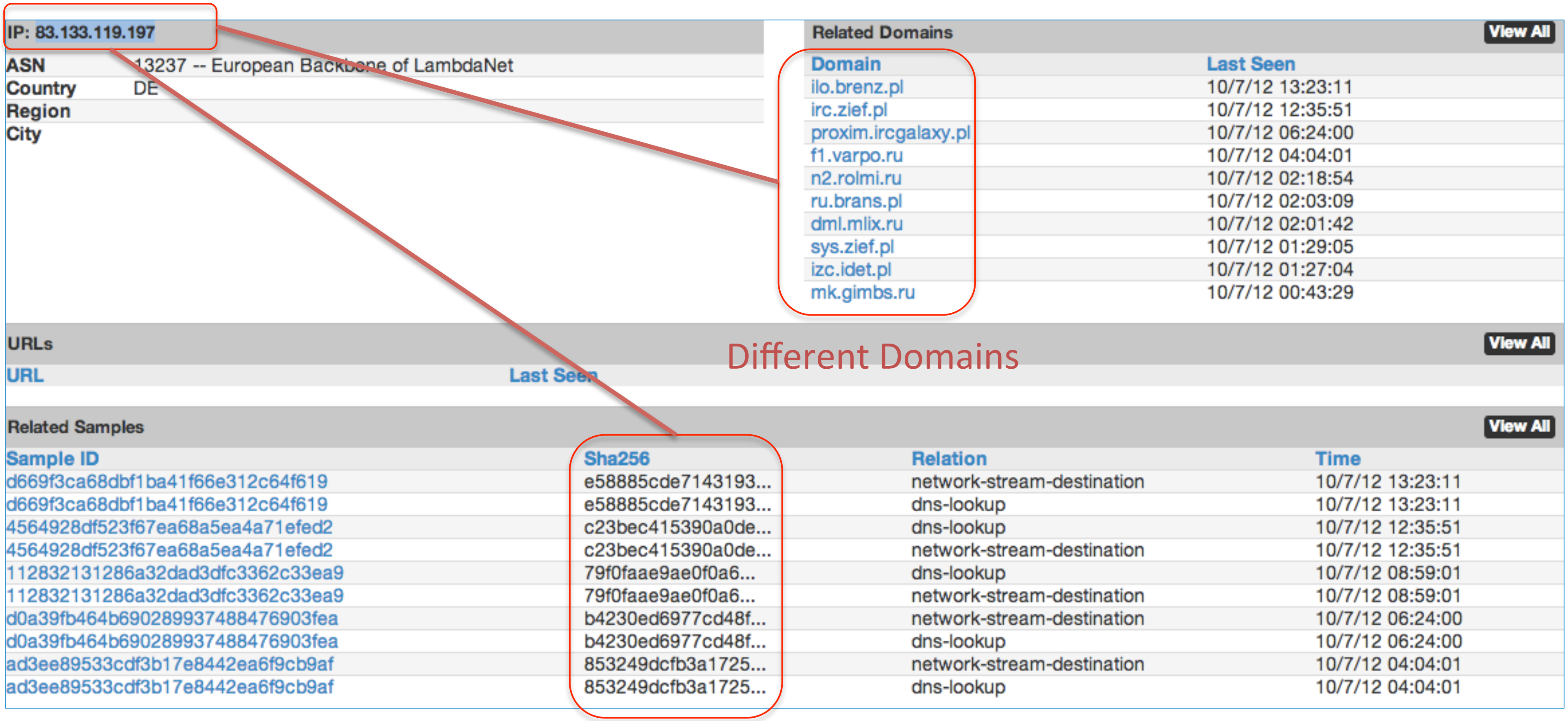


Domains related to 216.57.210.200

Domain
funcarreferee.com
gluelaw.com
i.dotzup.com
diabeticdietplanmenu.com
www.moonslot.com
getnewcarquote.com
clapslot.com
seemslot.com
relieveemotionalpain.com
whomslot.com
humanbodyfitness.com
www.diabeticdietplanmenu.com
diabeticweightlossmenu.com
leaseprivatejet.com
dietplanscholesterol.com
privatejetsrent.com
www.clothescostume.com
bodyjewelrybuyer.com
marriagejudgment.com
solegame.com
myspahealth.com
lumpgame.com
manyslot.com
diabeticrecipesmenu.com
paymentpanel.com
relieveconstipationpain.com
biosolarfuel.com



A Year In the Life of a MD5: Drilling Down



IP: 83.133.119.197

ASN	13237 -- European Backbone of LambdaNet
Country	DE
Region	
City	

Related Domains

Domain	Last Seen
ilo.brenz.pl	10/7/12 13:23:11
irc.zief.pl	10/7/12 12:35:51
proxim.ircgalaxy.pl	10/7/12 06:24:00
f1.varpo.ru	10/7/12 04:04:01
n2.rolmi.ru	10/7/12 02:18:54
ru.brans.pl	10/7/12 02:03:09
dml.mlix.ru	10/7/12 02:01:42
sys.zief.pl	10/7/12 01:29:05
izc.idet.pl	10/7/12 01:27:04
mk.gimbs.ru	10/7/12 00:43:29

Different Domains

URLs

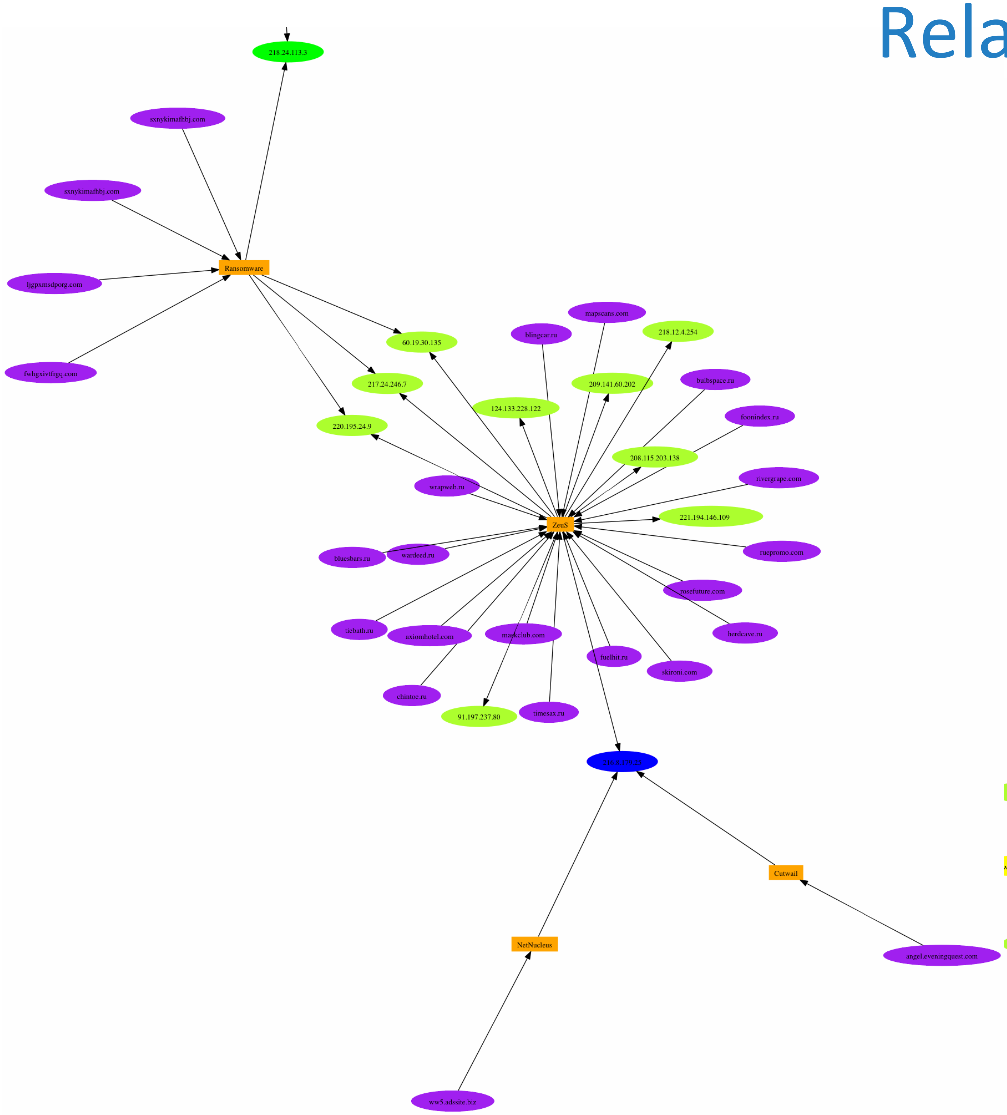
URL	Last Seen

Related Samples

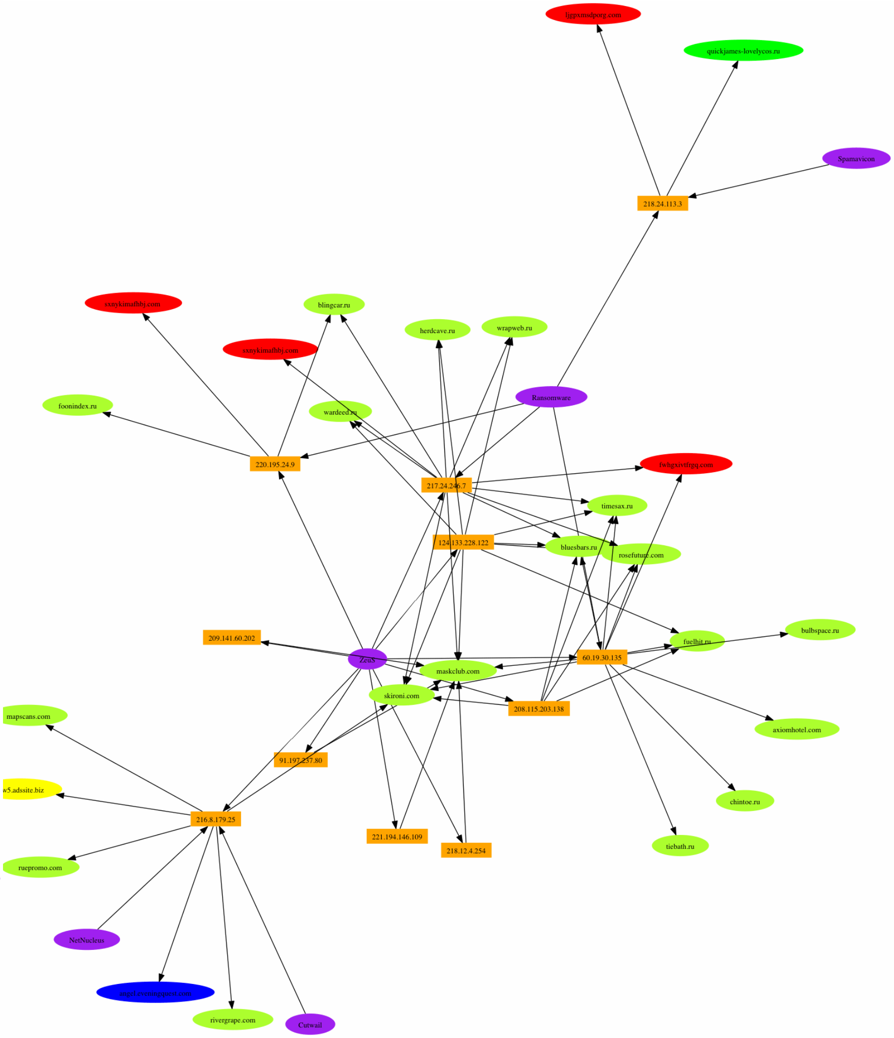
Sample ID	Sha256	Relation	Time
d669f3ca68dbf1ba41f66e312c64f619	e58885cde7143193...	network-stream-destination	10/7/12 13:23:11
d669f3ca68dbf1ba41f66e312c64f619	e58885cde7143193...	dns-lookup	10/7/12 13:23:11
4564928df523f67ea68a5ea4a71efed2	c23bec415390a0de...	dns-lookup	10/7/12 12:35:51
4564928df523f67ea68a5ea4a71efed2	c23bec415390a0de...	network-stream-destination	10/7/12 12:35:51
112832131286a32dad3dfc3362c33ea9	79f0faae9ae0f0a6...	dns-lookup	10/7/12 08:59:01
112832131286a32dad3dfc3362c33ea9	79f0faae9ae0f0a6...	network-stream-destination	10/7/12 08:59:01
d0a39fb464b690289937488476903fea	b4230ed6977cd48f...	network-stream-destination	10/7/12 06:24:00
d0a39fb464b690289937488476903fea	b4230ed6977cd48f...	dns-lookup	10/7/12 06:24:00
ad3ee89533cdf3b17e8442ea6f9cb9af	853249dcfb3a1725...	network-stream-destination	10/7/12 04:04:01
ad3ee89533cdf3b17e8442ea6f9cb9af	853249dcfb3a1725...	dns-lookup	10/7/12 04:04:01

Different Samples

Relationships are important



AfterGlow 1.6.2 - Property File: color.properties



AfterGlow 1.6.2 - Property File: color.properties

Takeways

- De-duplication can reduce quality of content produced
- Rich content is a requirement to successful correlation
- Correlation is essential in understanding the threat
- Context is necessary for effective Threat Intelligence

Finis

Questions?

- Dean De Beer
- CTO, ThreatGRID, Inc.
- dean@threatgrid.com