


**BLUE COAT**  
Security  
Empowers  
Business

# FROM FOG COMPUTING TO ROP GADGETS

FELIX LEDER

Felix.leder@bluecoat.com



**BLUE COAT**


## OVERVIEW

- **Threat Landscape**
  - Adversary
  - Cyber-
  - 0-day,
  - APT
  - HVT
- **Targets**
  - BYOD
  - Internet of Things
  - Cloud
  - Fog
  - aaS
- **Preparation**
  - MSSP
  - MDM, MAM, MIM
- **Protection**
  - Crowd-....
  - AED (advanced evasion detection)
  - NGFW
  - AV, HIDS, HIPS
- **Detection**
  - SIEM
  - Real Time Data Analytics (Big Data)
  - Threat Intelligence, OSINT
  - C2
  - G2
- **Exploitation**
  - ROP Gadgets, ASLR, DEP
- **Post-Breach**
  - DLP, Extrusion Prevention/Detection
  - eDiscovery

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved.

**BLUE COAT**

## THREAT LANDSCAPE



Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved.

**BLUE COAT**

## ADVERSARY

- “Guns don’t kill people, people kill people” [NRA]  
→ Tools don’t break into your systems, organizations do
- Who has an interest in breaking into your system?



Hacktivists



State Sponsored




Cyber Criminals

http://redsoosecurity.com/tag/pay-per-install

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved.

**BLUE COAT**

## STATE SPONSORED



https://www.liquidmatrix.org/blog/2011/01/06/estonian-computer-security-expert-army/




http://redsoosecurity.com/tag/pay-per-install

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved.

**BLUE COAT**

## CYBER...

- Origin: “controlling well” but lost meaning
- ... space ~ Internet
- ... crime
  - Banking, click-fraud, DDoS, spam, break-in
- ... war / warfare
  - DDoS, espionage, sabotage
- ... terrorism
  - Same as warfare but non-state (depends on view)
- -hate, -pilgrimage, -sex, -security

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved.

**BLUE COAT** CYBERWAR / CYBERTERRORISM

## Russia-Ukraine Standoff Going Online as Hackers Attack

By Cornelius Rahn, Ilya Khrennikov and Aaron Egliis Mar 6, 2014 4:21 PM GMT+0100 2 Comments Email Print

Cyberspace is fast becoming a battlefield for Ukrainian and Russian partisans even as ground troops from the two countries continue their military standoff.

Hackers have launched attacks on the websites of state agencies and publications on both sides. A Russian government watchdog has ordered a shutdown of the social-network pages of Ukrainian nationalist groups. And a Ukrainian phone company said its network in parts of the Crimean peninsula was damaged as unidentified men took over communication centers.



Photographer: Filipo Monteforte/AP via Getty Images

A Russian soldier stands guard near a Ukrainian navy ship in the harbor of the Crimean peninsula.

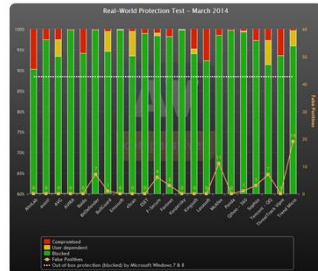
[Read More](#)

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 7

**BLUE COAT** 0-DAY

- 0-day vulnerability: vendor not yet notified
- 0-day malware: No antivirus detection

vendor	detected	total	percent
Avira (Windows)	1,963,327	2,180,597	89.5835
Avast (Windows)	1,785,403	2,180,597	81.8860
BitDefender (Windows)	1,773,526	2,180,597	81.3321
BitDefender (Linux)	1,765,767	2,180,597	80.9763
AVG (Windows)	1,762,446	2,180,597	80.8240
McAfee (Windows)	1,695,681	2,180,597	77.7624
BitDefender (Mac OS X)	1,673,114	2,180,597	76.7273
VirusBlink (Linux)	1,663,147	2,180,597	76.2723
K7 (Windows)	1,642,301	2,180,597	75.3315
... ..	...	...	...
FileSecure (Linux)	1,133,524	2,180,597	51.9823
Clam (Linux)	1,123,923	2,180,597	51.5420
Secure (Windows)	1,077,722	2,180,597	49.4290
TrendMicro (Windows)	1,040,978	2,180,597	47.7382
QuickHeal (Windows)	1,027,214	2,180,597	47.1070
Fortinet (Windows)	783,437	2,180,597	35.9286
TrendMicro (Linux)	758,813	2,180,597	34.7984
Sophos (Windows)	730,673	2,180,597	33.5079
Panda (Linux)	310,835	2,180,597	14.2546



Real-World Protection Test - March 2014

Legend: Green: detected, Yellow: not detected, Red: false positive, Blue: not tested

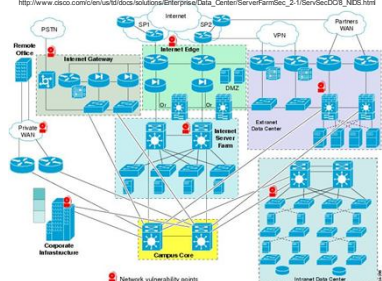
http://www.shodanranger.org/0day/0day.php?chart1.php

http://www.shodanranger.org/0day/0day.php?chart1.php

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 8

**BLUE COAT** ADVANCED PERSISTENT THREAT - APT

- Advanced?
  - naw (~"stealthy")
- Persistent?
  - yep (long-term)
- Threat—uh oh




http://www.cisco.com/en/us/sd/docs/solutions/Enterprise/Data\_Center/ServerFarmSec\_2-1/ServiceCOP\_NIDS.html

→ There is no 100% security ("just need firewall + AV" is long ago)

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 9

**BLUE COAT** HIGH VALUE TARGET - HVT

- STADA
- ICS




http://www.fox.com/article/index/215962/lyskashtrns-likely-death-a-bigger-deal-than-bin-laden

http://www.ngrounstitution.ca/boast2/viewtopic.php?h=295405&h=stunet

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 10

**BLUE COAT** TARGETS



Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 11

**BLUE COAT** BYOD

- Tablets
- Smartphones
- Laptops


**Bring Your Own Device**

- Full mobility → agility
- (Company) cost saving
- Productivity through familiarity (+spare time)

**Challenges:**

- Easy to get lost/stolen
- Full data access
- No control outside work infrastructure
- locked down (hard to add security monitoring)
- Policy enforcement

**Last but not least: Privacy**



Tomorrow never dies - James Bond - 1997

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 12

BLUE  
COAT

INTERNET OF THINGS

- **Locked devices**
  - No patch
  - No modifications possible
- **Full Internet Connectivity**
  - Attackers can exploit
  - Multi-platform attacks

The Honeynet  
PROJECT®

- **Every product has bugs**
  - ➔ Depend on 3rd party?



<http://linuxgizmos.com/2012/05/04/emerges-in-an-ii-system-and-in-a-refrigerator/>

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 13


BLUE  
COAT

CLOUD

**Cloud = The Internet**

I don't care where the service is...  
... as long as it works seamlessly  
... scalable to multiple users  
... access from (almost) everywhere

- IaaS, PaaS are usually "the cloud"




[http://en.wikipedia.org/wiki/File:Cloud\\_computing.svg](http://en.wikipedia.org/wiki/File:Cloud_computing.svg)

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 14

BLUE  
COAT

FOG COMPUTING

- **Local "cloud"** (used to be called data center)
- **or service close endpoints** (edge computing)
- **Reduced latency**
- **Local data transfer**
- **Process locally** instead of sending to the cloud
- **Local availability** of typical cloud services
- **Using closest/"own" infrastructure**




Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 15

BLUE  
COAT

AAS

- **... as a Service (aaS)**
  - Cost efficient
  - Leave domain to experts (hopefully)
  - Leave your data to somebody else
- **Infrastructure as a Service IaaS**
  - Routers, VMs, IP addresses, SAN
- **Platform as a Service - PaaS**
  - Full platform (LAMP, Hadoop clusters, Elasticsearch, Tomcat, Django, SQL server)
- **Software as a Service (SaaS)**
  - Office 365, Google docs

/dev/null as a Service




Plan	Traffic	Features	Price
Personal	10GB/Month	-	\$9
Economy	10GB/Month	SSL, Encryption	\$15
Business	50GB/Month	Dedicated IP, 24/7 Support	\$299
Enterprise	UNLIMITED	High Availability, 24/7 Support	\$499

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 16

BLUE  
COAT

PREPARE

...your defenses




Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 17

BLUE  
COAT

MSSP / UTM

- **Managed Security Service Providers**  
Manages security for you
- **Another aaS: Security as a Service**
- **A.k.a. Unified Threat Management**
  - Firewalls, Web-Filtering, NGFW, IPS, IDS
  - Endpoint security, AV
  - VPN, WAN, WiFi, Patch Management
  - Incident handling
- **Sometimes PaaS**




Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 18



BLUE COAT

MDM, MAM, MIM



**Mad Madam Mim**  
CHARACTER • Mad Madam Mim appears in 194 issues.  
 A powerful but eccentric sorceress. Introduced in "Sword in the Stone" as an opponent to Merlin. Has since been featured as friend or foe, often both, of almost all Disney characters and Magica DeSpell's housemate.

MxM:


- Mobile DEVICE Management
- Mobile APPLICATION Management
- Mobile INFORMATION Management

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 19


BLUE COAT

WORKING WITH BYOD

- **Mobile DEVICE Management**
  - Rollout of policies, settings
  - Monitoring / device portfolio / rooted devices
  - "Remote wipe" / lock
  - Backup



- **Mobile APPLICATION Management**
  - Trusted apps
  - Installed apps
  - "Wrapped" apps to limit data access




<http://www.netelive.org/communitiy/blog/iam-gang-knox-should-have-apple-worried-about-enterprise>

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 20

BLUE COAT

MOBILE INFORMATION MANAGEMENT




<http://www.sudcamp.com/best-free-dropbox-alternatives/>

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 21

BLUE COAT

PROTECTION



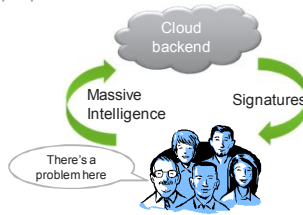
Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 22

BLUE COAT

CROWD

- **Power to of the people**
  - Exploit existing client base (there is nothing like a free lunch App)
  - Pay small money to a lot of people to do a lot of work

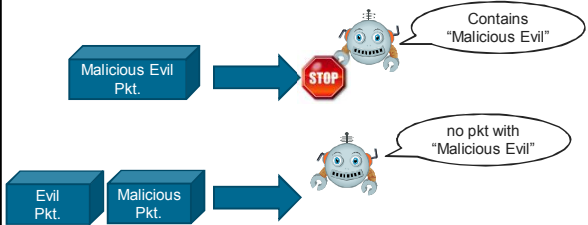
- Crowd Intelligence
- Crowd AV
- Crowd Testing
- (Crowd Funding)



Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 23

BLUE COAT

ADVANCED EVASION DETECTION



- Stream reassembly is not trivial
- And not rocket science

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 24

## BLUE COAT NGFW – NEXT GENERATION FIREWALLS

← Features

- **Application identification by protocol details**
  - Usually http based protocols
  - Extend traditional IP, port, protocol, fields, ... model
- **Application level IPS**
- **User identification**

→ Security

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 25

## BLUE COAT AV - ANTI-VIRUS

- **Most misunderstood**
- **Common perception: Something that applied signatures to files**
- **Most AV suites have more:**
  - (Browser) exploit detection
  - On-access scanning
  - Clean-up
  - Firewall
  - HIDS, HIPS

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 26

## BLUE COAT DETECTION

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 29

## BLUE COAT SIEM

### ▪ Security Information and Event Management

- Collect
- Aggregate
- Correlate
- Alert
- Keep data for future (forensic) analysis

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 29

## BLUE COAT REAL TIME DATA ANALYTICS

- **Previously known as BIG DATA**
- **Research and solutions around for 50 years**
  - Divide and conquer (now known as map-reduce)
  - Data indexing
  - Multi-processing
- **Problem now: “Store everything”-mantra**
- **Now there are easy-to-use tools**
  - Hadoop
  - Elastic Search
  - Solr
  - Logstash / Kibana

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 30

## BLUE COAT THREAT INTELLIGENCE

- **Threat Intelligence**
  - Black lists, white lists, reputation scores
  - Spam templates
  - Intelligence as a Service (whois, detection history and correlation)
- **OSINT – Open Source INtelligence**
  - Public Sandbox reports
  - CIA world fact book
  - Open directory listings on C2 server

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 31

US • KOREA INSTITUTE AT SAIS

## 38 NORTH

HOME  
ABOUT  
CONTACT  
SUBSCRIBE  
DIGITAL ATLAS

TOPICS  
Leadership Watch  
WMD  
Domestic Affairs  
Foreign Affairs  
Human Security

James Church  
Commentary  
Spotlight  
Media/Issues  
Flashpoints

Media Analysis  
Book Reviews  
Satellite Imagery  
Videos

SUNDAY MAY 11TH 2014

*Informed analysis of events in and around the DPRK.*

**Foreign Affairs**

**Is Russia-North Korea Cooperation at a New Stage?**

Deputy Prime Minister of the Russian Federation, the Plenipotentiary Representative of the Russian Federation, and the President in the Far Eastern Federal District of the Russian Federation, Yuri Trutnev's three day long visit to the DPRK (April 28-30, 2014) symbolized the culmination of a new phase in Russian-North Korean relations taking shape—a sort of renaissance if you will. Indeed it was the first time in the last 30 years—since [Read More]

**NEW! DPRK DIGITAL ATLAS**

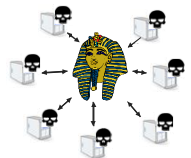
Roam through North Korean provinces, cities, towns and villages on the new 3d North DPRK Digital Atlas.

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 32

BLUE COAT

C2 / G2


- **G2**
  - Military grade intelligence
  - Related to military units
- **C2 a.k.a. Command & Control**
  - Controlling instance of botnets
  - Also: Drop zone



Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 33

BLUE COAT


EXPLOITATION



Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 34

BLUE COAT

EXPLOITATION

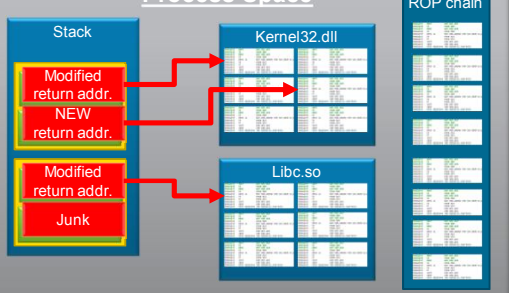


Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 35

BLUE COAT

RETURN ORIENTED PROGRAMMING

**Process Space**

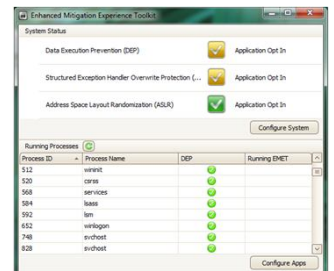


Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 36

BLUE COAT


ADDRESS SPACE LAYOUT RANDOMIZATION

- **ASLR**
- **DEP & ASLR active in most modern OS**
  - Latest Windows (limited)
  - iOS 4.3 +
  - Android 4.0 +
  - OS X 10.5 +



Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved. 37


**BLUE COAT** POST BREACH



Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved 38

**BLUE COAT** DLP / EPS / EDS


- Data Leakage/Loss Prevention
- Extrusion Detection/Prevention System **NEW**
- Possible monitoring points
  - Endpoint
  - Network
  - Storage
- Sophistication varies widely
  - Log access, transfer
  - Signatures for content
  - Digital signatures / watermarks
  - DRM



Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved 39

**BLUE COAT** E-DISCOVERY

- E-Discovery
  - Network forensics
  - Host forensics
  - G2 + OSINT



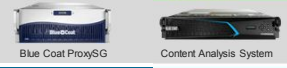




Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved 40

**BLUE COAT** Security Empowers Business

1 Minute Advertisement

**BLUE COAT** INTEGRATED

**A Complete and Integrated Portfolio of Modern Advanced Threat Protection Solutions**

<p><b>Blocking and Prevention</b></p>  <p>Blue Coat ProxySG Content Analysis System</p>	<p><b>SSL Visibility</b></p>  <p>Blue Coat SSL Visibility Appliance</p>
<p><b>Security Analytics Platform by Solera</b></p>  <p>Security Analytics Appliances Security Analytics Storage Security Analytics Central Manager</p>	<p><b>Malware Analysis Appliance</b></p>  <p>Blue Coat Malware Analysis Appliance</p>
<p><b>ThreatBLADES</b></p>  <p>WebThreat BLADE MailThreat BLADE FileThreat BLADE</p>	

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved 42

**BLUE COAT** SUMMARY

- There is a lot of hype
- Who is your "adversary"?
- Have tools to protect and to detect
- Breaches will happen – be prepared for the incident

Copyright © 2013 Blue Coat Systems Inc. All Rights Reserved 43

