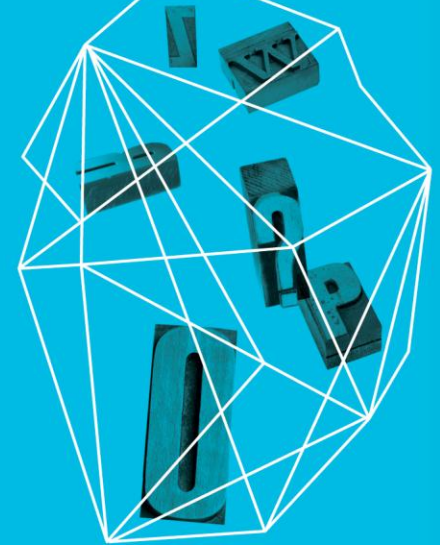


THE CYBER THREAT LANDSCAPE: NEW THEMES IN PREVENTION, DETECTION, RESPONSE

Kimberly Peretti
Partner, Alston & Bird, LLP

Security in
knowledge



— AGENDA

- ▶ Cyber Threat Landscape
 - ▶ Nation States
 - ▶ Organized criminal groups
 - ▶ Hacktivists
 - ▶ Lessons learned
- ▶ New Themes
 - ▶ Response
 - ▶ Detect
 - ▶ Protect
- ▶ Take-aways

**THREAT
LANDSCAPE –
NATION STATES**





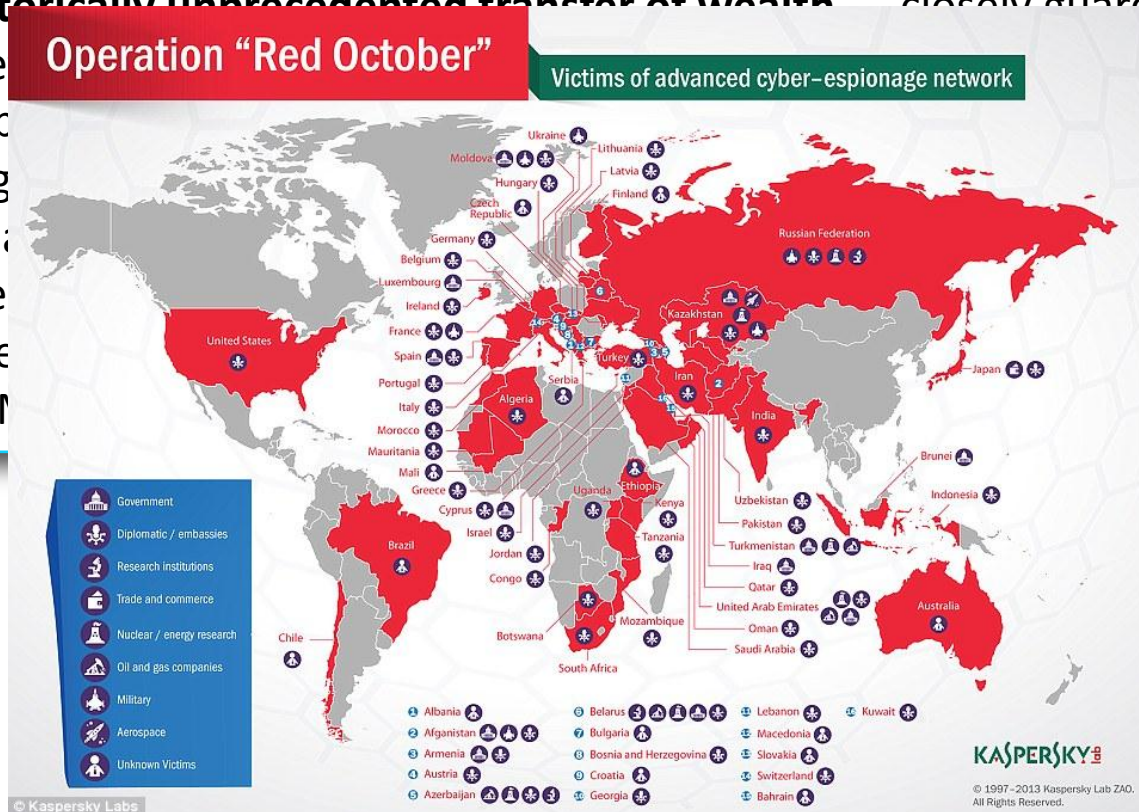
... the constant electronic theft of intellectual property that has silently occurred over the past several years has already **caused significant harm to**

our
corp
cont
sens
rese
a ma
Cybe

What we have witnessed over the past five to six years has been nothing short of a **historically unprecedented transfer of wealth** closely guarded national

secret
data
and g
data
"falle
in the
RAT, M

source code, bug
ails for new oil
ory control and
much more has
nd disappeared
Operation Shady



NATION-STATE ATTACKS

The screenshot shows a web page from BankInfoSecurity. The main article is titled "Hacktivists Suspend DDoS Attacks" and is dated January 29, 2013. A large blue circle is overlaid on the page with the text "Cyber Warfare" in the center. To the left of the circle is a red prohibition sign over the text "DDoS". The page includes a navigation menu at the top with categories like Authentication, Compliance, Fraud, Governance, Mobility, Payments, Risk Mgmt, and Technology. There is also a search bar and a "Get Daily Email Updates" sign-up box. A video player for "CAREERS INFO SECURITY" is visible on the right side of the article.

<http://www.bankinfosecurity.com/hacktivists-suspend-ddos-attacks-a-5458?rf=2013-01-29-eb&elq=16d60e649ac743c3bd8642efdef64b87&elqCampaignId=5685>.

**THREAT
LANDSCAPE –
ORGANIZED
CRIMINALS**



THE CARDING



Front Page | Blog Posts | Resources | Media

Dirt Jumper DDoS Botnet Variants Continue to Proliferate

Friday, April 13, 2012

Contributed By:
[Headlines](#)

Researchers at Arbor Networks have identified so many varieties of the RussKill distributed denial of service (DDoS) botnet that they have dubbed the variants collectively as the "Dirt Jumper family".



"Attacks from the Dirt Jumper family of bots continue to target victims all around the world in a robust manner and we will take a look at who is being attacked, although we cannot always determine the motive," writes Arbor Networks' Curt Wilson.

In denial of service attacks, generally a large amount of information is sent to a web server at such high frequency that it overwhelms the processing capacity or causes the system to shut down and reset

altogether.

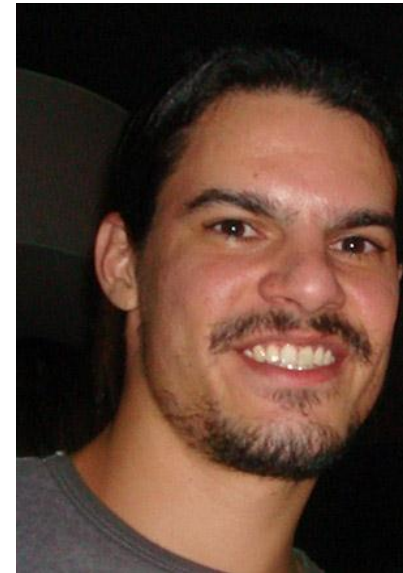
The proliferation of the Dirt Jumper botnets have spawned an underground economy based on DDoS attacks for hire, according to the research.

"While we have collected about 300 malware samples of the Dirt Jumper family, it is likely that other variants are available, as the binaries and back-end PHP for Dirt Jumper has leaked several times. This makes it easy for someone to make slight modifications to the PHP or Delphi binary code and attempt to re-sell the bot, use the bot for their own purposes, or start making money with their own commercial DDoS service," Wilson said.

"Dirt Jumper continues to evolve (version 5 appears to be the newest) and a variety of other associated bots packages have emerged over time to include Simple, September, Khan, Pandora, the Di BoTNet and at least one private version of Dirt Jumper 5 that I am aware of," Wilson continued.

<http://www.infosecisland.com/blogview/20997-Dirt-Jumper-DDoS-Botnet-Variants-Continue-to-Proliferate.html>

<http://www.bankinfosecurity.com/visa-issues-atm-cash-out-warning-a-5438?rf=2013-01-22-eb&elq=2bf2a633e97640b5937654d8af58ee66&elqCampaignId=5619>



PROFILES OF CYBERCRIMINALS



http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?pagewanted=all&_r=0

**THREAT
LANDSCAPE –
HACKTIVISTS**



► News for **anonymous** hacker



Kansas City Star

3 Sec
Inform:
As BA
expert
455 re

[Anony](#)
PCWo
[Anony](#)
eWeel

Anonymous bre

[www.infoworld.com/...](http://www.infoworld.com/)

3 days ago – The grou
service on Thursday n

Anonymous bre

www.computerworld.c

4 days ago – The hac



onymous, its security
reaches, ...



[Network](#)



ed
tting off phone



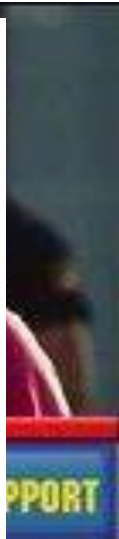
Sunday" belonging

July 10, 2011. FBI agents executed a search warrant at the Long Island, N.Y., home of a suspected member of notorious hacking group Anonymous.

investigative recon... Island, N.Y., home and one in Brooklyn, N.Y., sources told EngNews.com

The agents spent an hour and 40 minutes at Jordan's house; other agen

at
cter
ip
l.
the
dar
rant
d



LESSONS LEARNED

- ▶ Era of targeted intrusions
- ▶ Same methods (or modus operandi) occur time and time again
- ▶ Blending of methods, tactics, and techniques among groups
- ▶ Containment / eradication may take months not days
- ▶ Number of systems compromised may well reach into the hundreds
- ▶ Somewhere along the way, PII will probably come into play

RESPONSE



NEW THEMES: RESPONSE

- ▶ Enterprise impact investigations
- ▶ Crisis management
- ▶ Active Defense

— ENTERPRISE IMPACT INVESTIGATIONS

- ▶ Three common breach response scenarios
- ▶ Inherent limitations
 - ▶ Lack of privilege
 - ▶ Incomplete understanding of scope of breach

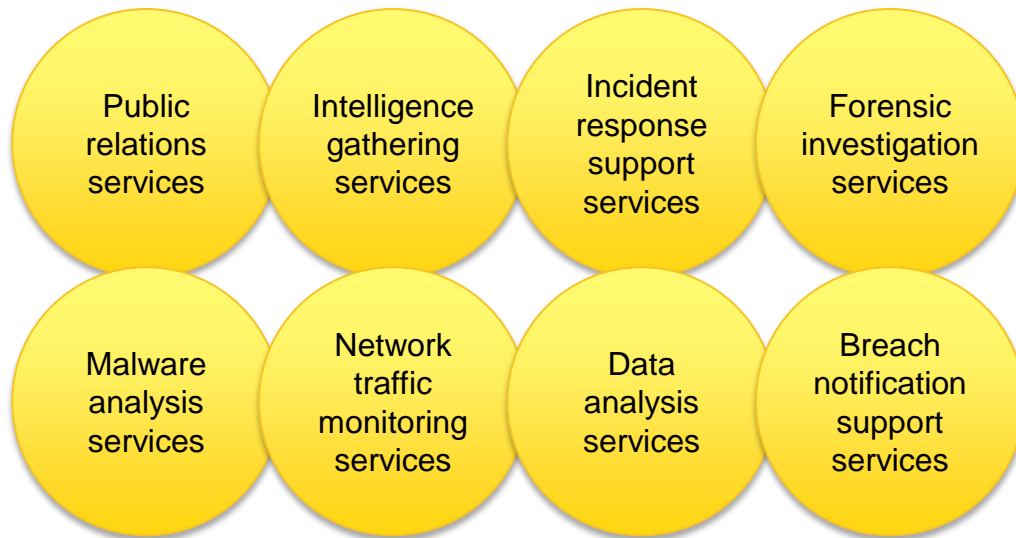
ENTERPRISE IMPACT INVESTIGATIONS

- ▶ Hallmarks of an enterprise impact investigation
- ▶ Are enterprise impact investigations necessary? And, when?



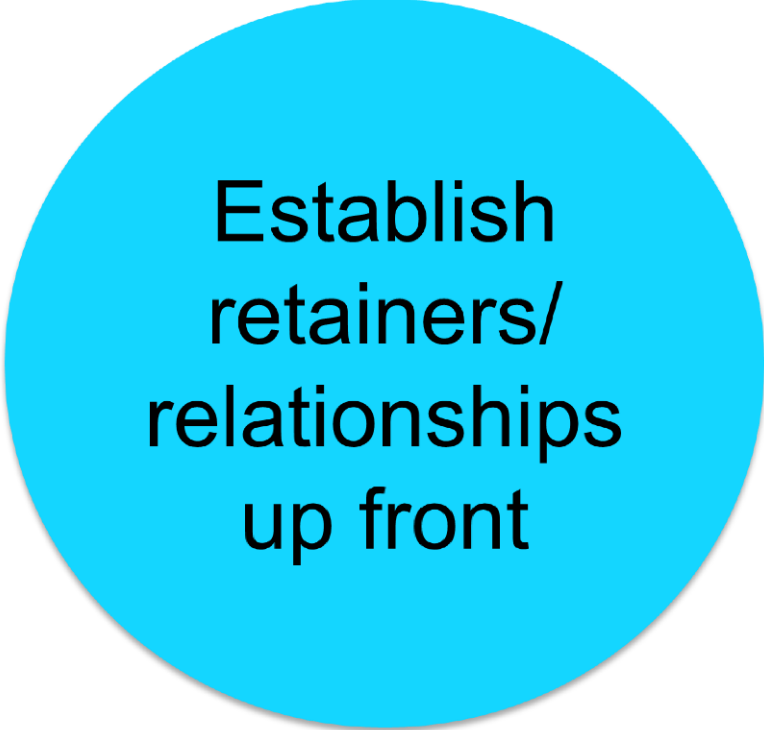
CRISIS MANAGEMENT

- ▶ What types of services may be relevant in a cyber response / data breach incident?



- ▶ Not all of the services can be handled internally or even with one vendor

— CRISIS MANAGEMENT



Establish
retainers/
relationships
up front

ACTIVE DEFENSE

ZDNet White Papers Hot Topics Downloads Reviews Newsletters

US Edition M2M Windows 8 Big Data Social Enterprise Cloud Networking

New Protect America Offer
www.ProtectAmerica.com
Free Security System Plus 2 Free Keychain Remotes. Limited time offer.

MUST READ: *It's BlackBerry 10; RIM changes name*

Topic: Security Follow via: RSS Email

Singapore's cybersecurity amendments opens questions on compliance

Summary: The government is proposing the word "cybersecurity" be included in the country's Computer Misuse Act. It will also harden the legislation to include pre-emptive actions.

By Bryan Tan for Tech Legal | November 19, 2012 -- 02:45 GMT (18:45 PST)
Follow @zdnetasia

In a bid to harden Singapore's cyberdefense, the government has proposed upgrades to its Computer Misuse Act.

<http://www.zdnet.com/sg/singapores-cybersecurity-amendments-opens-questions-on-compliance-7000007565/>

ALSTON & BIRD LLP
CYBER ALERT
A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM JANUARY 11, 2013

<http://www.alstonprivacy.com/?entry=4793>

Los Angeles Times

LOCAL U.S. WORLD BUSINESS SPORTS ENTERTAINMENT HEALTH LIVING TRAVEL OPINION DEALS

MONEY & CO. TECHNOLOGY HIGHWAY 1 COMPANY TOWN PERSONAL FINANCE JOBS REAL ESTATE CARS

Search

YOU ARE HERE: LAT Home → Collections → Business

Ads by Google

A new brand of cyber security: hacking the hackers

Irvine start-up CrowdStrike is pioneering a confrontational approach to cyber security. It identifies hackers and uses their own techniques to prevent theft.

December 04, 2012 | By Ken Dilanian, Los Angeles Times

<http://articles.latimes.com/2012/dec/04/business/la-fi-cyber-defense-20121204>

DETECT



— NEW THEMES - DETECT

- ▶ Preventative forensics
- ▶ “Big Data” forensics (detect/respond)

— PREVENTATIVE FORENSICS

- ▶ Periodic scanning for breach indicators
 - ▶ Key systems
 - ▶ Assortment of endpoints
 - ▶ Updated list of indicators
- ▶ Component of cyber risk assessment

BIG DATA FORENSICS

Training big data's eye on cybersecurity threats

Summary: *The data explosion is upon us. Big data analytics is supposed to help us sift through it all. Can it also help keep enterprise hackers at bay? We talk to the founders of Seculert.*

<http://www.zdnet.com/training-big-datas-eye-on-cybersecurity-threats-7000008357/>

PROTECT



— NEW THEMES: PROTECT

- ▶ Use of threat intelligence
- ▶ Threat modeling / assessment

THREAT INTELLIGENCE

Upcoming Events
Wednesday, January 23, 2013
1:00pm ET
How To Complete Your Patch

Financial Services ISAC
HOME ABOUT FS-ISAC

FS-ISAC 8th Annual Summit 2013

InfraGard
a collaboration for infrastructure protection

Cyveillance
a QinetiQ Company
World Leader in Cyber Intelligence
Home | Contact Us

PASTEBIN | #1 paste tool since 2002
create new paste | tools | api | archive | faq | search...
Follow @pastebin Like 19k
create new paste trending pastes sign up | login | my alerts | my settings | my profile

We Recommend: Boost Your PC Speed 216% in 2 Mins?
Don't like ads? PRO users don't see any ads ;-)

3.0% No Closing Cost Refi
GreenlightLoans.com/866.557.6024
No Closing Cost APR Refi. Quote As Seen on CNN News. Call Today!

Public Pastes

- Untitled 4 sec ago
- TBS Draft 0: Epis... 10 sec ago
- Untitled 7 sec ago
- Untitled 8 sec ago
- Untitled 14 sec ago
- Untitled 11 sec ago
- Untitled 16 sec ago
- Untitled 17 sec ago

Optional Paste Settings

Syntax Highlighting: None
Paste Expiration: Never

Hello Guest
Sign Up or Login
Sign in with Facebook

New Social Media Guidebook
Provides social media policy best practices and more.
Download »

Nationwide Insurance
IN THE NATION, SAFE DRIVING IS REWARDED.

— THREAT INTELLIGENCE

- ▶ Use threat data points gathered in real-time from the criminal underground to analyze and understand
 - ▶ The specific threat actors targeting your network
 - ▶ The assets within your organization they are targeting
 - ▶ The methods by which they are entering your networks/systems
- ▶ Aggregate/analyze this content in order to:
 - ▶ Drive formation of a security strategy
 - ▶ Determine security spending
 - ▶ Implementation of, or changes to, security controls and capabilities
- ▶ Risk-based approach to security, not compliance-based

— THREAT MODELING / ASSESSMENT

- ▶ Threat models/assessment
 - ▶ Understanding current defenses in place to protect against most likely threat vectors
 - ▶ Should be part of cyber risk assessment

**FINAL
THOUGHTS /
LESSONS
LEARNED**



— 5 TIPS TO TAKE HOME

- ▶ Invest in information sharing
 - ▶ Real-time mechanisms are the key to threat intelligence
- ▶ Don't get caught in trap of narrowly-tailored investigations
 - ▶ The sooner you uncover the scope, the better
- ▶ Use Big Data concepts to manage investigations
 - ▶ The technology is there, use it
- ▶ Explore creative solutions in active defense space
 - ▶ But this is especially an area to include counsel
- ▶ Hail to the Board
 - ▶ Board involvement necessary in protect, detect, and respond

QUESTIONS?

Kimberly.peretti@alston.com
202.251.8118

For additional information, please see:
www.alstonprivacy.com
www.alstoncyber.com
www.alstonsecurity.com

