



DDoS & Modern Threat Motives

Dan Holden
Director, ASERT



IS YOUR CSO SHAKING IN HIS BOOTS?



What Does This Advanced Threat
Landscape Look Like?

Advanced Threat Landscape



- ✓ More defenses
- ✓ Network change
- ✓ Modern Employee

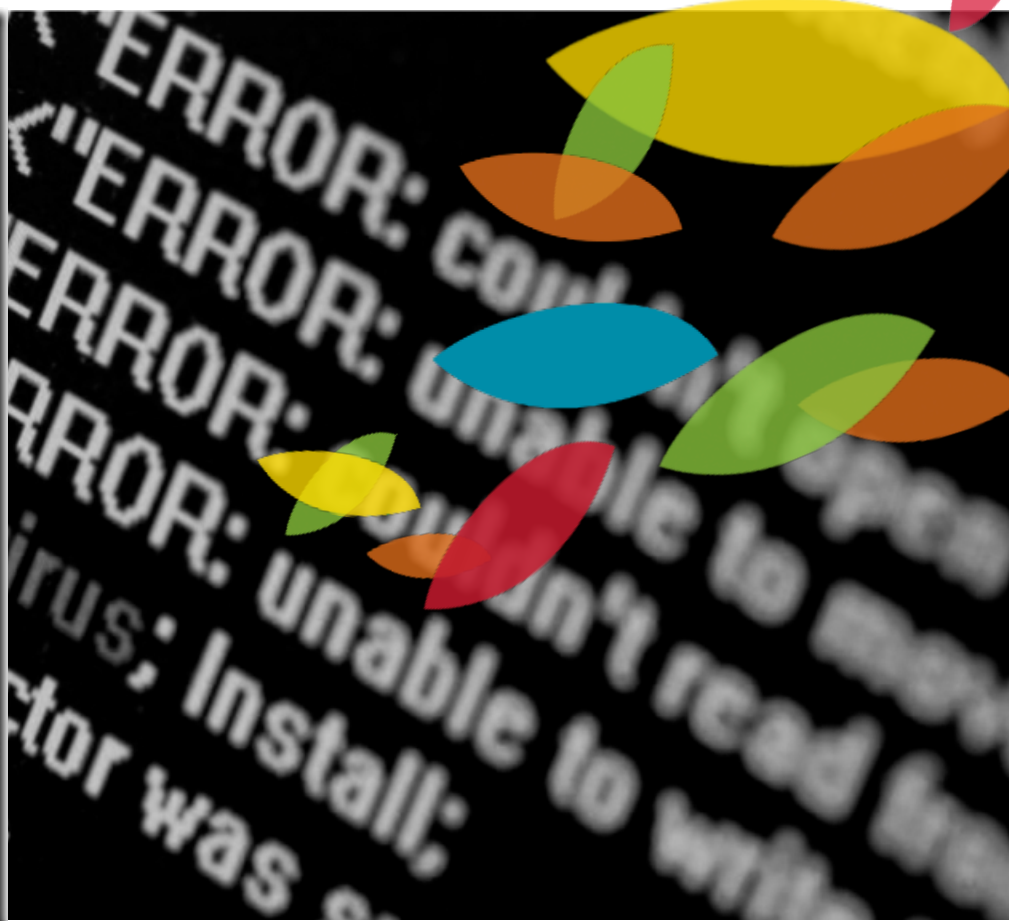
- ✓ Geo-political
- ✓ App/Content
- ✓ Legacy infrastructure

- ✓ DDos
- ✓ Botnets
- ✓ Malware

- ✓ Phishing/SPAM
- ✓ Vulnerabilities
- ✓ Web App

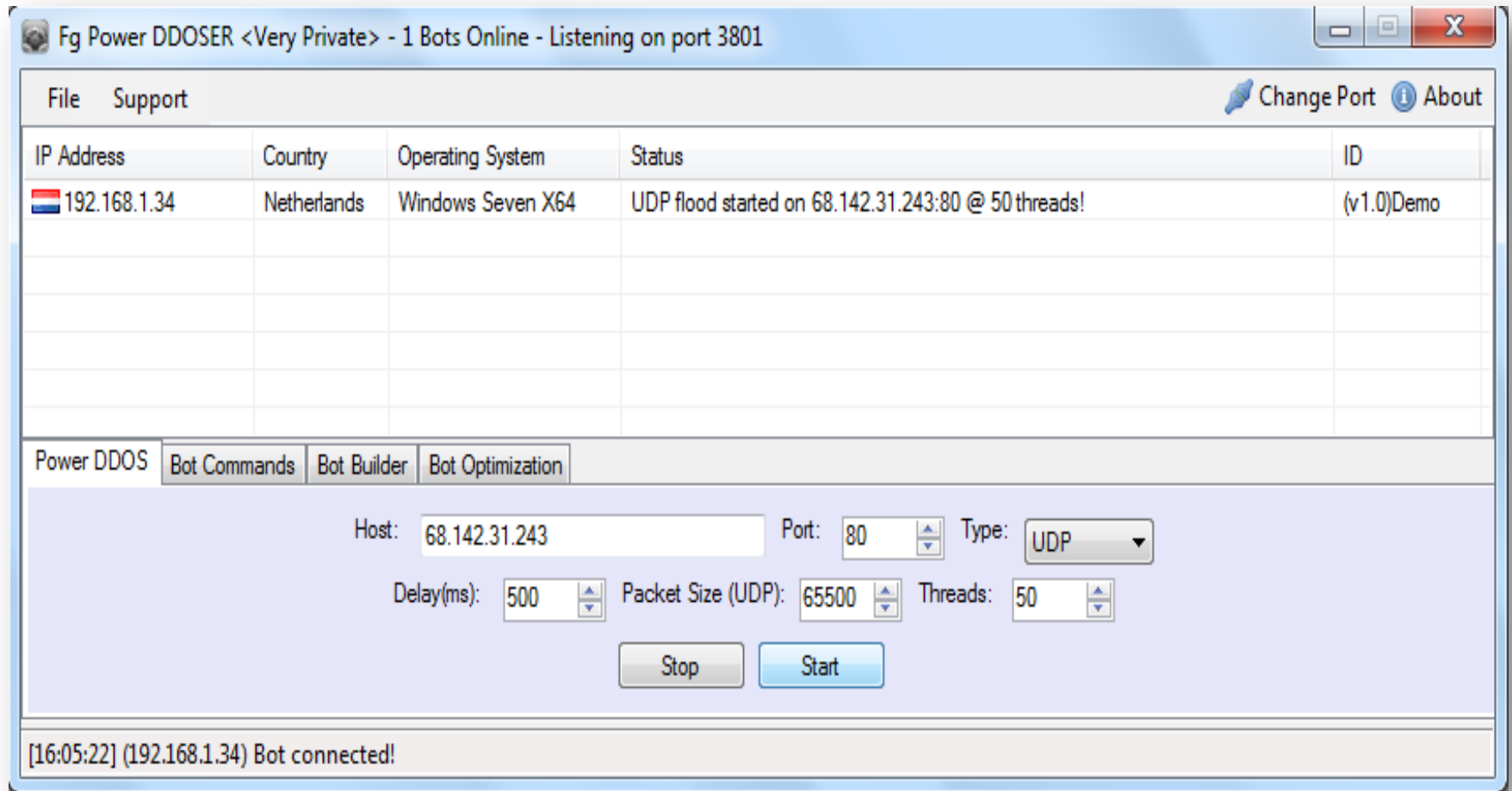
- ✓ Cyber Crime
- ✓ Hacktivism
- ✓ Competitive

- ✓ APT
- ✓ Cyber Espionage
- ✓ Cyber Warfare



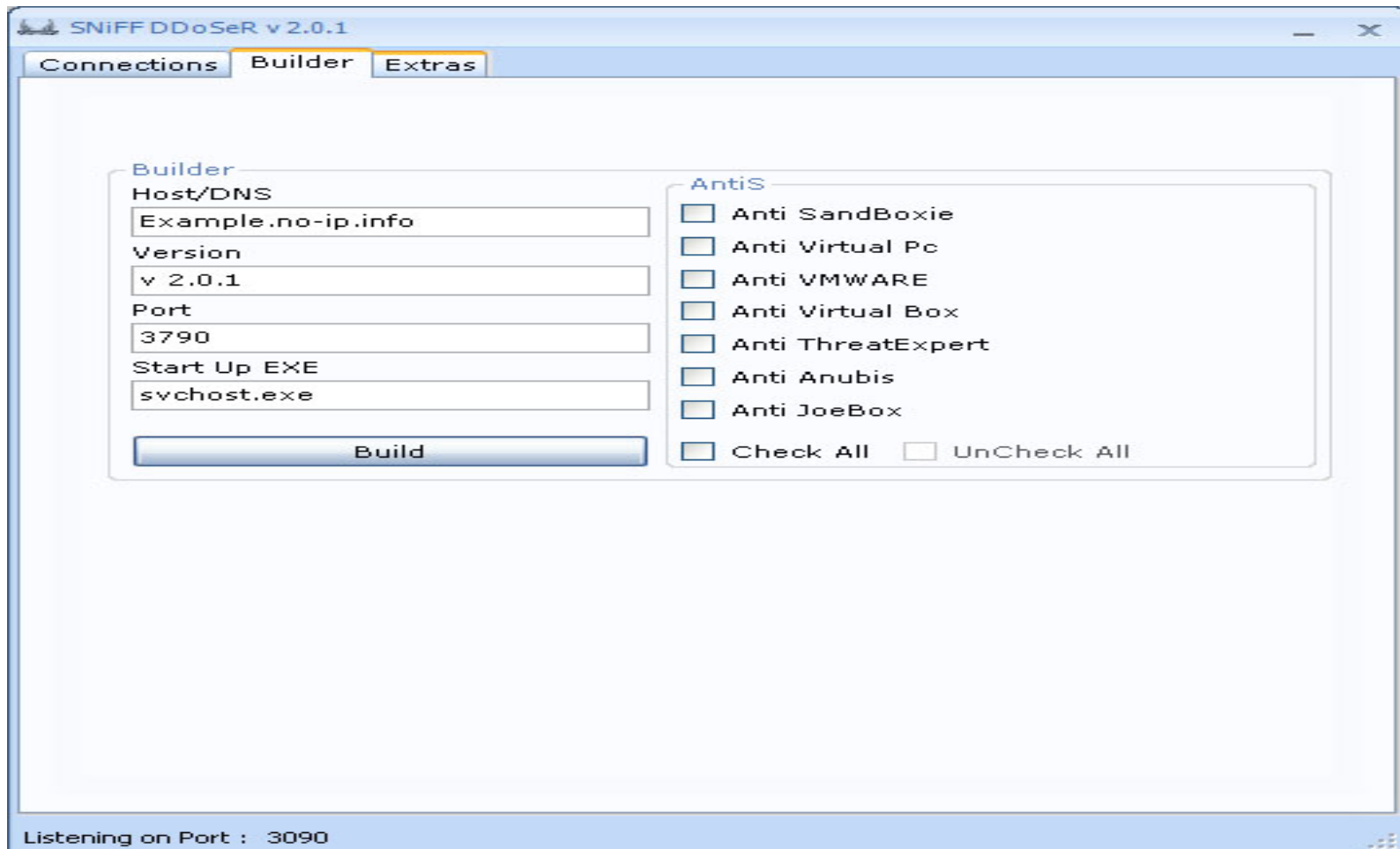
Cyber Crime

Host Booter – Fg Power DDOSER



- Includes Firefox password stealer

Host booter – SniffDDOSER



Host Booter – Fg Power DDOSER

Password Stealing Capability

```
-----  
Program:          Firefox  
Url/Host:         https://my.webmoney.ru  
Login:           [REDACTED]@mail.ru  
Password:      [REDACTED]  
Computer:        admin-ПК  
Date:            2011-05-28 21:20:56  
Ip:              [REDACTED].107.32  
-----
```

- What passwords stored in the browser?
- Firefox password posted to forum
 - My.webmoney.ru

Underground Economy Insight - UFOCrypt

- Crypters bypass anti-malware and other security solutions
- DDoS bots, banking trojans, password stealers, ransomware (“blockers”), etc.
- Crypter service - \$20 per bot, cheap and effective

12/15/2012

1


UFOCRYPT


Windows v.1.01

Register: 15.12.2012

Posts: 4

Thanked total: 1
for this post: 0



 Crypts service "UFOCRYPT". Crypts \$ 20. Payment at least!

We are open! You can contact us for the crypts of their files! TAKE MONEY AFTER YOU ARE test efficiency! always online, and always try to meet our customers! Contact -----
----- ICQ: 647115374 Jabber: 647115374@jabber.org Skype: ufocrypt -----
----- WWW.UFOCRYPT.BLOGSPOT.COM Our service Krypto the following software: - stealer (UFR Stealer, iStealer, HC Stealer and the rest) - **DDos bots (all versions)** - Loader - Zeus (all versions) - Spy-EYE - Blockers - cipher Krypto Price 1 = \$ 20 Individual approach to each client! Get Verified!

Underground Economy Insight – Mr. Worf

- A “load” is access to a compromised system to install software of the attackers choice, typically malware

 **Unread**

Thread Tools ▾

Search this Thread ▾

Rating: ★★★★★ ▾

Display Options ▾

 6 days. back # 1

worf1 ▾

Windows v.1.01

Date: 03/22/2013

Posts: 1

Thanks all: 0
for this post: 0

 Off Line 

 **Loads**

Sale Download
Price:
Price for 1k
-Mix = 25
-Asia = 18
-Without Asia = 50
no-samples
per day to 20k
A regular partner
maximum size of your file should not priveshat - 140kb.
Accept: WM / LR +5% / Yandex money 7%

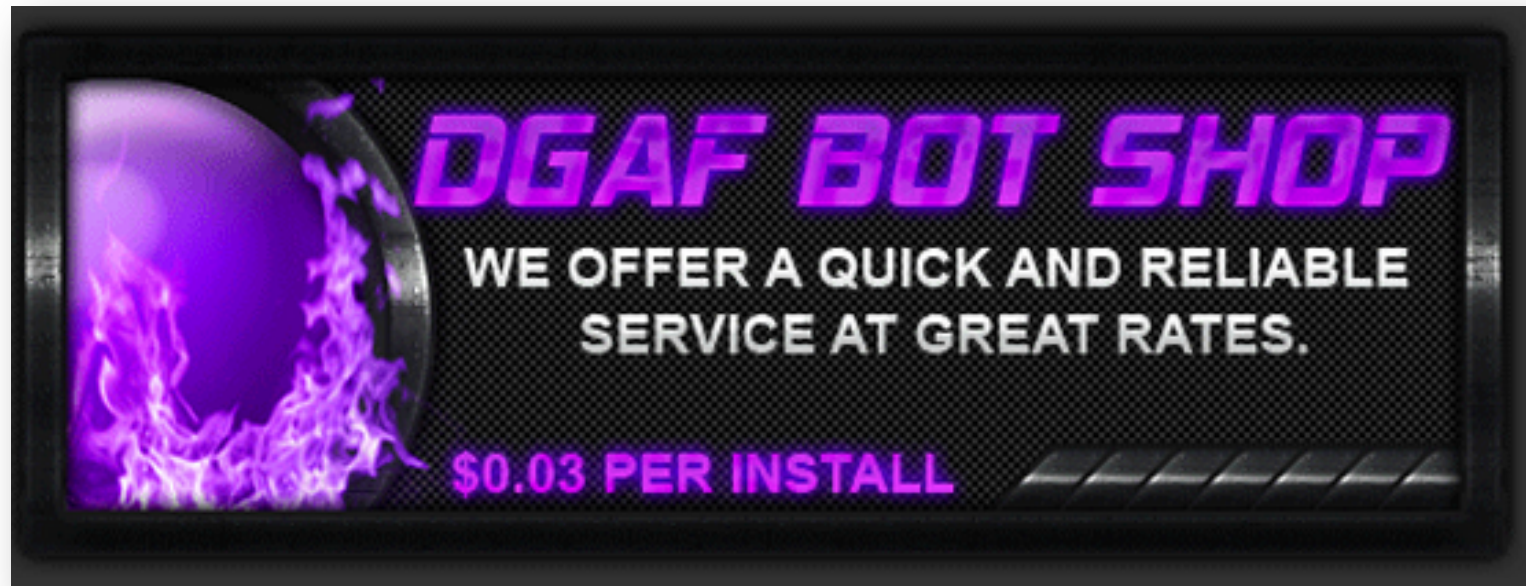
worf1@jabber.ru

Last edited worf1; 4 days. back to 00:50 .

 Спасибо  Цунама  ”  Ответ

Underground Economy Insight – DGAF

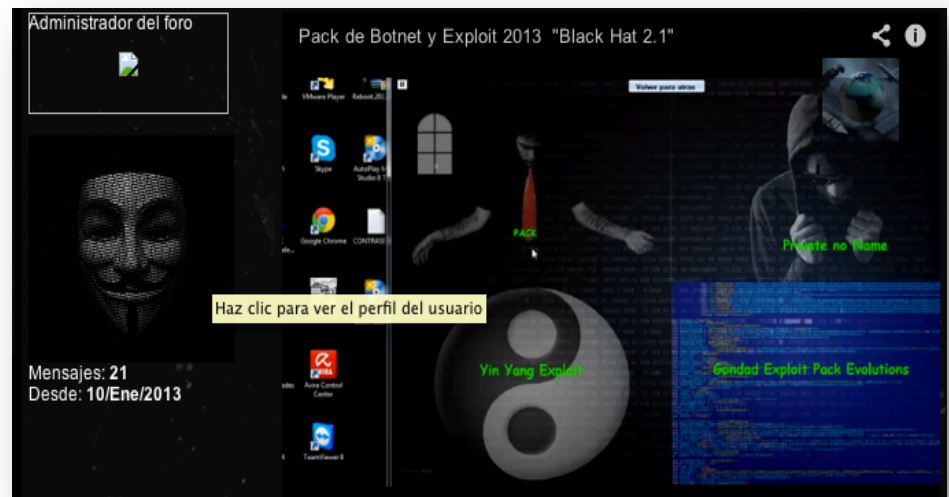
- At only \$30 per 1000 bots, they could purchase 1000 Asian bot loads from worf1 (previous slide) for \$18 & make \$12.



- Eventually the low quality bots would be noticed but many scammers (known as “rippers”) exist in the underground economy. You can’t trust a thief!

Black Hat Botnet and Exploit kit 2.1

- This botnet & exploit kit bundles:
 - Pandora DDoS bot
 - SpyEye banking fraud crimeware
 - Volk botnet
 - Gondad exploit pack
 - Yin Yang exploit
 - a packer “PACK”
 - “Private no Name”
- Bundling in a kit allows for
 - an easy one-stop-shopping crimeware setup
 - or a crimeware service setup

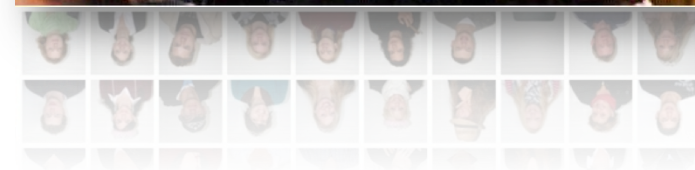
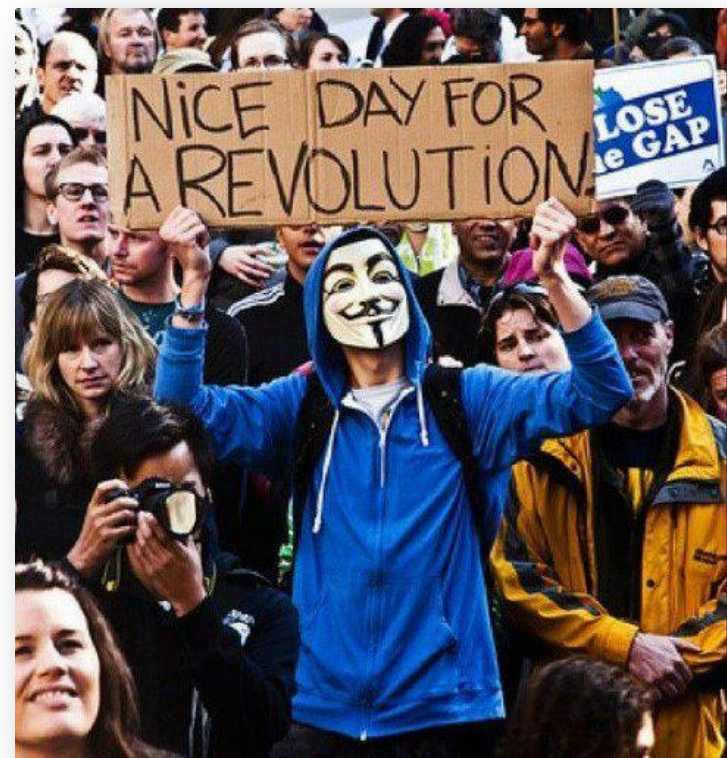




Hacktivism

Know Your Enemy? Good Luck!

- 12 y/o student in Ohio learning computers in middle school
- 13 y/o home-schooled girl getting bored with social networks
- **15 y/o kid in Brazil that joined a defacement group**
- 16 y/o student in Tokyo, learning programming in high school
- **18 y/o high school drop out in the Ukraine**
- 19 y/o college student putting class work into practice
- 20 y/o Taco Bell employee bored with the daily grind
- **21 y/o man in Mali working for an international carding ring**
- 23 y/o mother in Poland, trying to supplement income
- **24 y/o black hat intent on compromising any company encountered**
- 25 y/o soldier in the North Korean army
- **26 y/o military contractor in Iraq**
- 28 y/o Chinese government employee, soon to be mother
- **29 y/o vegan in Oregon who firmly believes in political hacktivism**
- 30 y/o white hat pen tester who has not let go of her black hat origins
- **31 y/o security researcher who finds vulnerabilities on live sites**
- 32 y/o alcoholic in New Zealand, with nothing to lose
- 34 y/o employee who sees a target of opportunity
- 35 y/o officer in MI6
- **36 y/o "consulate attaché" that may be FSB**
- 40 y/o disgruntled admin, passed over for raise 5 years in a row
- 42 y/o private investigator looking for dirt on your CEO
- **43 y/o malware author, paid per compromised host**
- **45 y/o member of a terrorist group**
- 55 y/o corporate intelligence consultant



2008

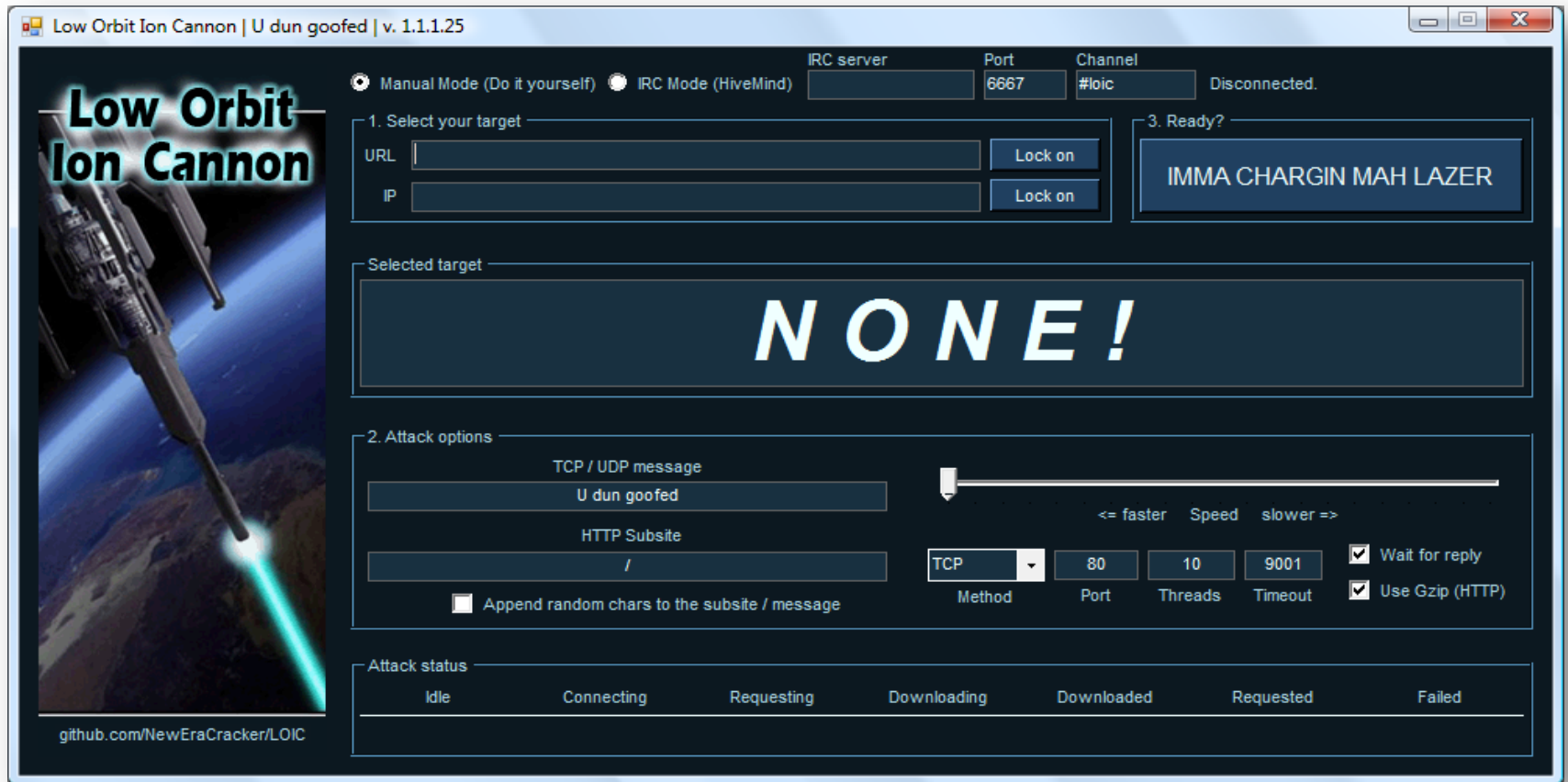
First High-profile Anonymous Attack

January 2008: Anonymous, an Internet hacktivism group, launches the first in a series of high profile DDoS attacks when it floods the *scientology.org* Web site.

It is a response to the Church of Scientology trying to remove video of an infamous Tom Cruise interview from the Internet.



Single User+ - LOIC



- Famously used tool by Anonymous
- Also has “HiveMind” mode
- Discloses attacker IP
- Rarely used due to ability to track attacker source

2010

Hacktivism Escalates

December 2010: Paypal is hit with DDoS attacks coordinated by supporters of the Wikileaks website after Paypal suspends money transfers to the site.

A variety of other major financial sites and credit card companies are also hit for their role in blocking payments to the site.

Single User Flooding Tools – JS-LOIC

JS LOIC

No need to download, install or setup anything - just click the button, sit and enjoy the show.



Step 1. Select your target:

URL:

For current target see: <http://anonops.net/>

Step 2. Ready?

Optional. Options

Requests per second:

Append message:

Attack status:

Requested:
0

Succeeded:
0

Failed:
0

We need your help in support of [wikileaks](#) leave this page firing as long as you can. Don't worry if requests show as failed.

- Stand-alone JavaScript version
- Lacks some of the features of regular LOIC
- No need to install tool, just visit Webpage with JS code
- Proliferated delivery simple via URL

2012

Governments Become Prime Target

April 2012: In a protest against “draconian surveillance proposals” and the extradition of suspects from the UK to the US to stand trial, the hacker group Anonymous targets a number of US and UK government sites including the US Department of Justice, the CIA and the UK Home Office.



Single User+ - Binary Cyber Cannon



- Anonymous attack tool used in Brazil
- Not as easy to use as LOIC or HOIC
- Has “packet blaster” for more detailed attacks
- Hacktivist oriented tool with “hive mind”

2012

DDoS Is Very Political

2012: Canada's New Democrat Party sees its leadership election impacted by DDoS attack that delayed voting and reduced turnout.

Mexico and the Dominican Republic have both fended off cyber attacks on their national elections by Anonymous.

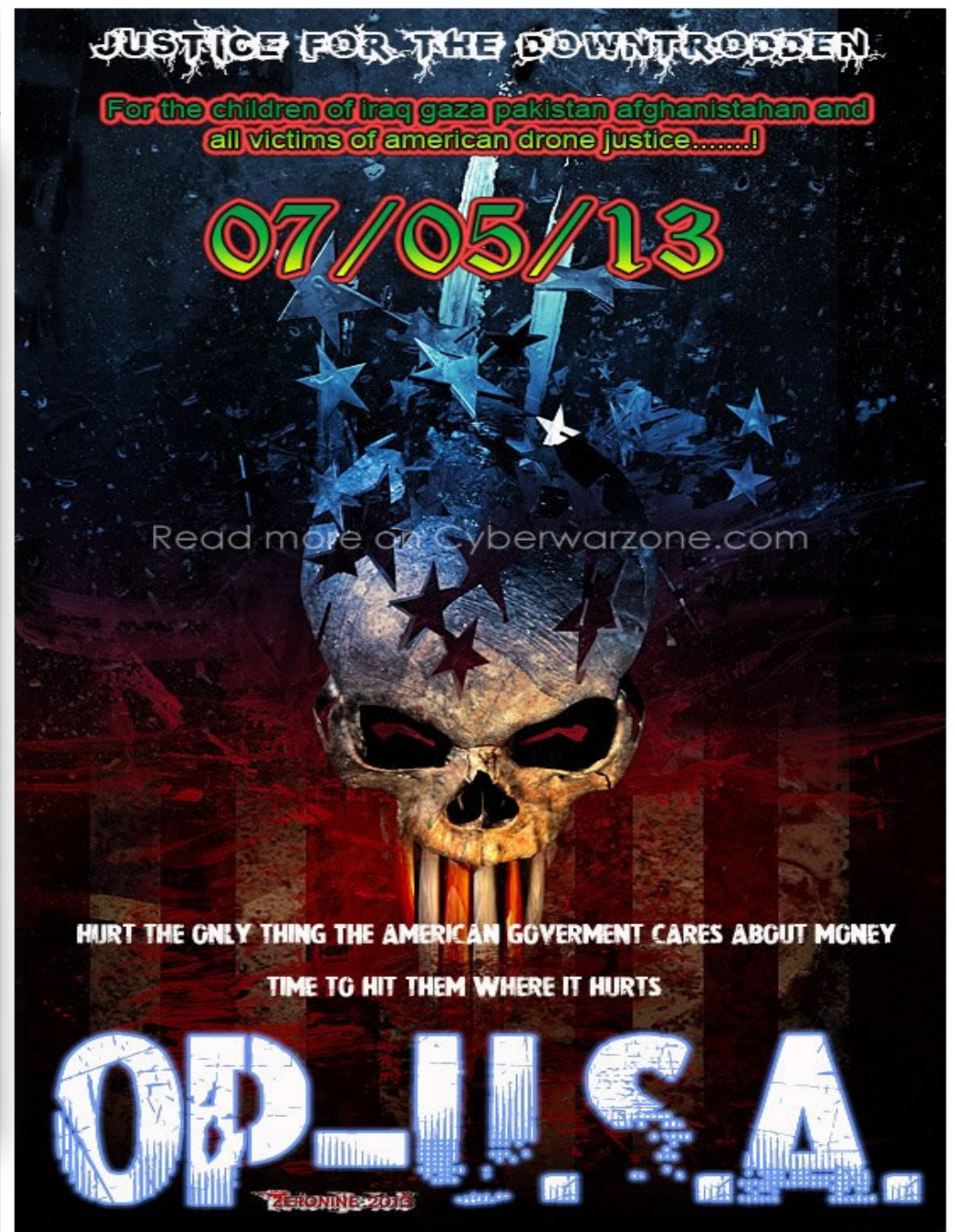
Cyber attacks throughout 2012 also hit national elections in Russia, Ukraine, and South Korea.



#OpIsreal #OpUSA



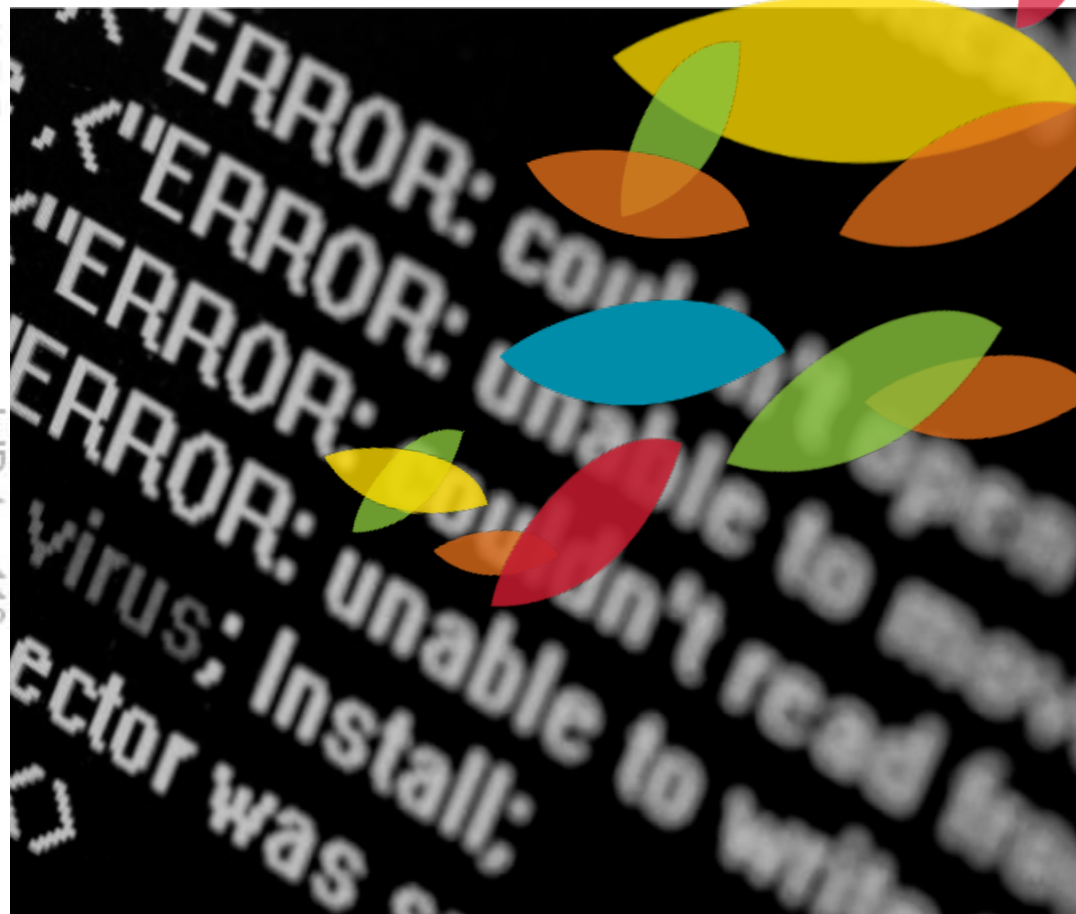
ARBOR[®]
NETWORKS



© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com



search ID: tcm110



Competitive Takeout

Commercial DDoS Services – March 2012

JunaidNoor •

Junior Member



Join Date: Jun 2008

Posts: 8

Professional DDoS Service! free test!

Hello all. i present to you professional DDoS service!

free test 5 minutes, only for serious clients!

i use private ddos bot - dirt jumper v5 (special edition for me).

supported methods of attack:

- TCP SYN Flood
- HTTP GET Flood
- HTTP POST Flood
- HTTP Downloading Flood
- HTTP Synchronous Flood

prices for attack:

- 4\$ / hour
- 35\$ / day
- 200\$ / week

* prices may change, if target have Anti-DDoS protection!

payment:

- WMZ
- Liberty reserve

Commercial DDoS Services – Late 2012

Good day, our service offers DDOS services to address sites (any subject), servers, and other Internet resources.



conditions our server:

- * Complete anonymity
- * Service without mediation
- * Reasonable prices for excellent quality
- * Garntirovany monitor to 10:00 to 00:00 (GMT)

* Test 10 minutes before booking and consultation with our specialist!

* We return the remainder of the funds if conditions of the order are not met! **Prices of our**

service: * 6 \$ - per hour * \$ 60 - per day * from \$ 380 - per week * from \$ 900 - per month (Prices may change Depends on the time of order and the complexity of the attacked site) **Payment**

Methods: * WebMoney * Liberty Reserve * Also can receive payment via other systems +% on the exchange WM **Contact our Saporta:** ICQ: 429149 Jabber: psycho@kaddafi.me

Competitive Takeout

- The Russian security service FSB arrested Pavel Vrublevsky, the CEO of ChronoPay, the country's largest processor of online payments, for allegedly hiring an attacker to DDoS his company's rivals



Commercial DDoS Product – Dirt Jumper v5

27-02-2012

Stanislav •

Senior Member



Join Date: Dec 2011

Posts: 278

[Leaked] Dirt Jumper v5 [Strongest bot in the world] new!

Thanks to TORTURER for finding Leaked builder!

My comment on bot :

This is the strongest bot i have ever used, it crashes everything with minimum amount of bots.

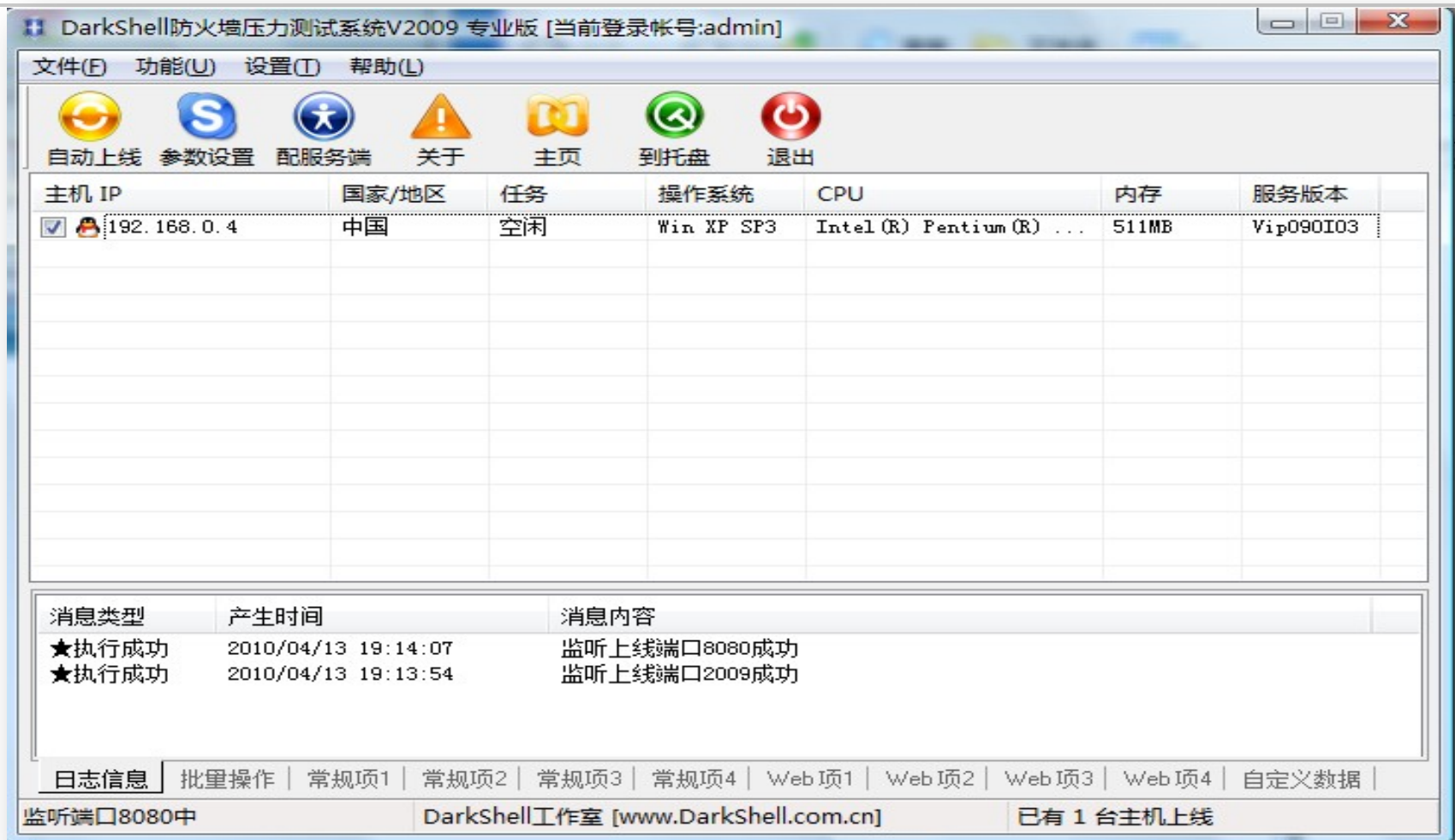
Tested :

1. Hostbooter.com - 5 bots with HTTP Flood , 25 Flows. After 2 minutes site is "DOWN"
2. Nilus.org - 5 bots HTTP Flood , 35 flows. Down.
3. HackForums.net - 250 bots , 35 flows . Synchronous flood , DOWN.
4. Prolexic.com - 500 bots , HTTP Flood.

I have really never seen such amazing power , it is like "HAMMER" .

Bot is very fast to responses, ddos starts momentarily after giving a command.

Bot – “DarkShell”



- In 2010, this bot was seen to attack industrial food processor equipment vendors

Competitive DDoS

- Co-founder & former YouSendIt CEO Pleads Guilty to DoS Attacks
- In March 2009, Shaikh founded a new company called FlyUpload which offered the same content distribution services as YouSendIt



Commercial DDoS Services – March 2013

2 hour (s) ago

1

Stelios ▾

Windows v.1.01



Date: 28/03/2013

Posts: 1

Thanks all: 0
for this post: 0



DDoS Service 911

DDoS Service 911

DoS-attack (from the English. Denial of Service, Denial of Service) and **DDoS-attack** (from the English. Distributed Denial of Service, Distributed Denial of Service) - a kind of attack on the computer system, the aim of which is to bring the system up to overload condition in which it can not access legitimate users, or that access is difficult. Our **DDoS service** - the best way of pesky competitors that prevent you from working.

Urgent assistance in solving your problems - a support network round the clock ! We present to you **Ddos-service service** that helps you eliminate business rivals, etc. We will help you to test the **anti-ddos** protection for your server site. In our Ddos-service, you can order a **DDoS attack** on almost any website or server! Conduct DDoS attacks on the game servers, online shopping, political sites! Our prices are available in the market **ddos service** . Average price is only \$ 50 per night . The final price may kolebatsya in greater and down. Wholesale customers and regular customers individual circumstances! **Attention!** In view of the widespread fraud in Ddos-orders DDoS service tests are only after the money transfer under the protection code, to fight with resellers and Kidal. **Payment** : WebMoney Liberty Reserve are also other ways of payment on request. **Communications / Contact** : **ICQ : 332212 Jabber :**

stelios@jabber.se tags for google: **order a ddos attack , ddos order , DDoS attacks , ddos service, ddos attack, ddos service, ddos server, ddos service, ddos a site, ddos to the server, ddos service, ddos site ddos server attack on the site, the attack nA server, kill site, kill the server, put the site, put the server, flood the site, flood the server, bring down a site, print server fails, how much harm the site, how much harm server, stop the site, stop the server, disable / remove competitor's site, disable / remove server competitor, as to fill up the site as fill up the server, ddos attack on order, ddos attack on order, hacking, powerful DDoS-attack.**

Gwapo's Professional DDOS Service

YouTube



Browse | Movies

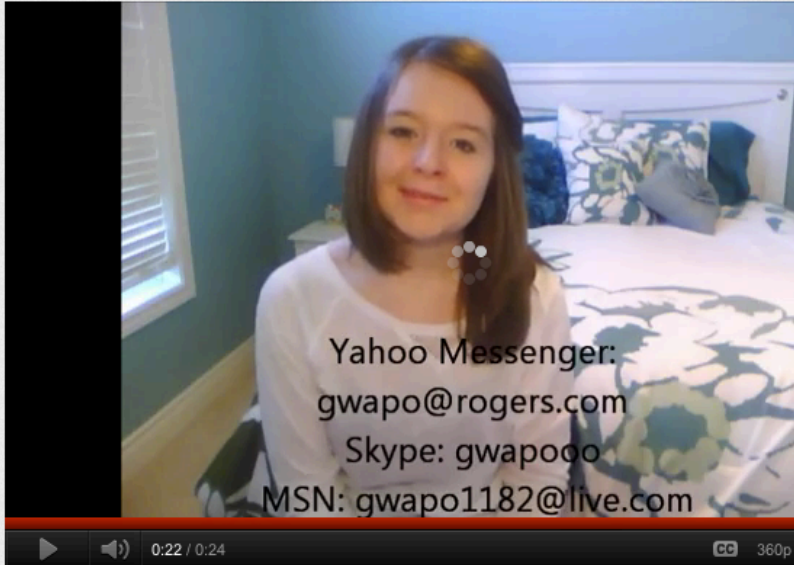
Gwapo's Professional DDOS Service

Gwapologist

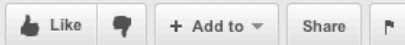


Subscribe

2 videos



0:22 / 0:24 CC 360p



Uploaded by Gwapologist on Jan 4, 2012

Please visit our thread posted here :

<http://www.hackforums.net/showthread.php?tid=1971939>

22 likes, 73 disl

As Seen O
/g/ - Techn

ARBOR[®]
NETWORKS

YouTube



Browse | Mov

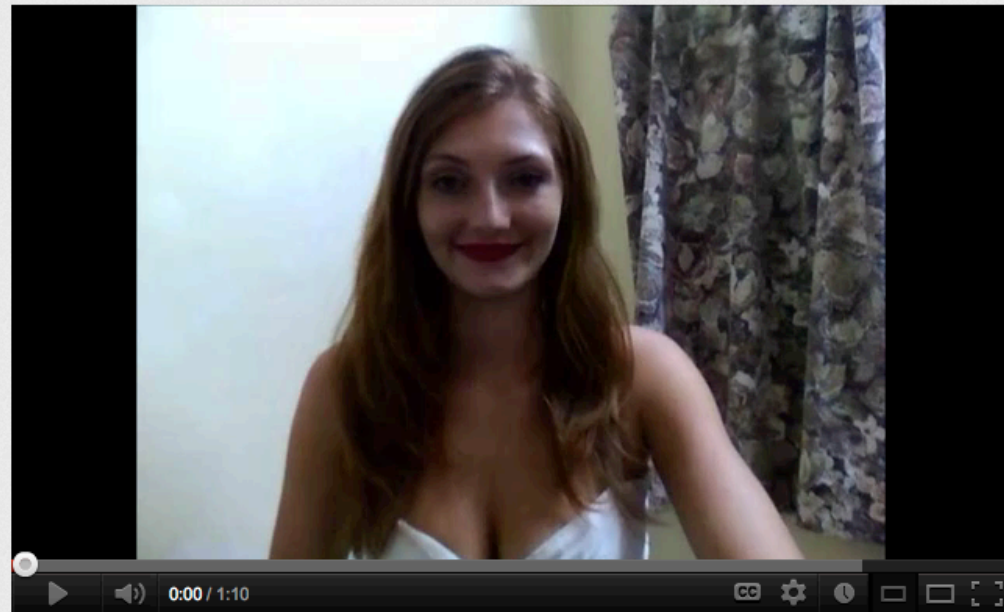
Gwapo's Professional DDOS Service

Gwapologist



Subscribe

5 videos



0:00 / 1:10 CC



Published on Mar 12, 2012 by Gwapologist

Service Website : <http://www.ddosservice.org/>

Email Us : gwapo@hackforums.net

Yahoo Messenger : gwapologisthf

4,816

6 likes, 28 dislikes

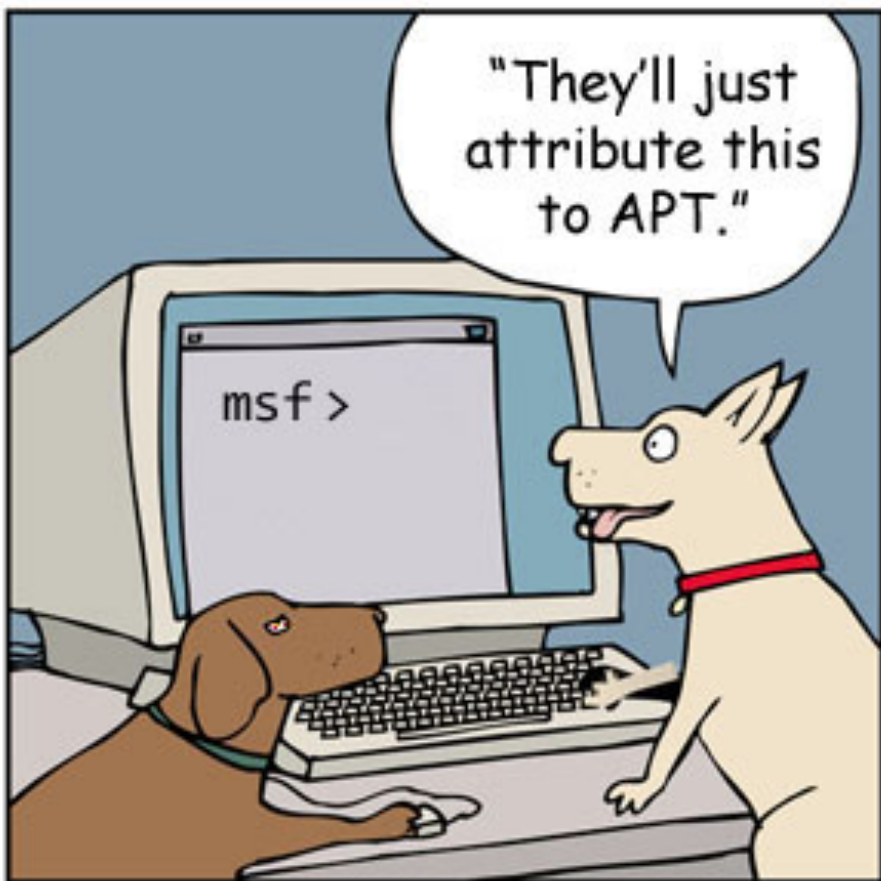
As Seen On:
[Hacking Forum- Home O...](#)

Asylumstresser.com Featured By Krebs

Asylumstresser.com also features a youtube.com ad that highlights the service's ability to "take down your competitors' servers or Web site."



"Do you get annoyed all the time because of skids on xBox Live? Do you want to take down your competitors' servers or Web site?," reads the site's ad, apparently recorded by **this paid actor at Fiverr.com**. "Well, boy, do we have the product for you! Now, with asylumstresser, you can take your enemies offline for just 30 cents for a 10 minute time period. Sounds awesome, right? Well, it gets even better: For only \$18 per month, you can have an unlimited number of attacks with an increased boot time. We also offer Skype and tiny chat IP resolvers."



Advanced Threats

2011

Consequences are Damaging

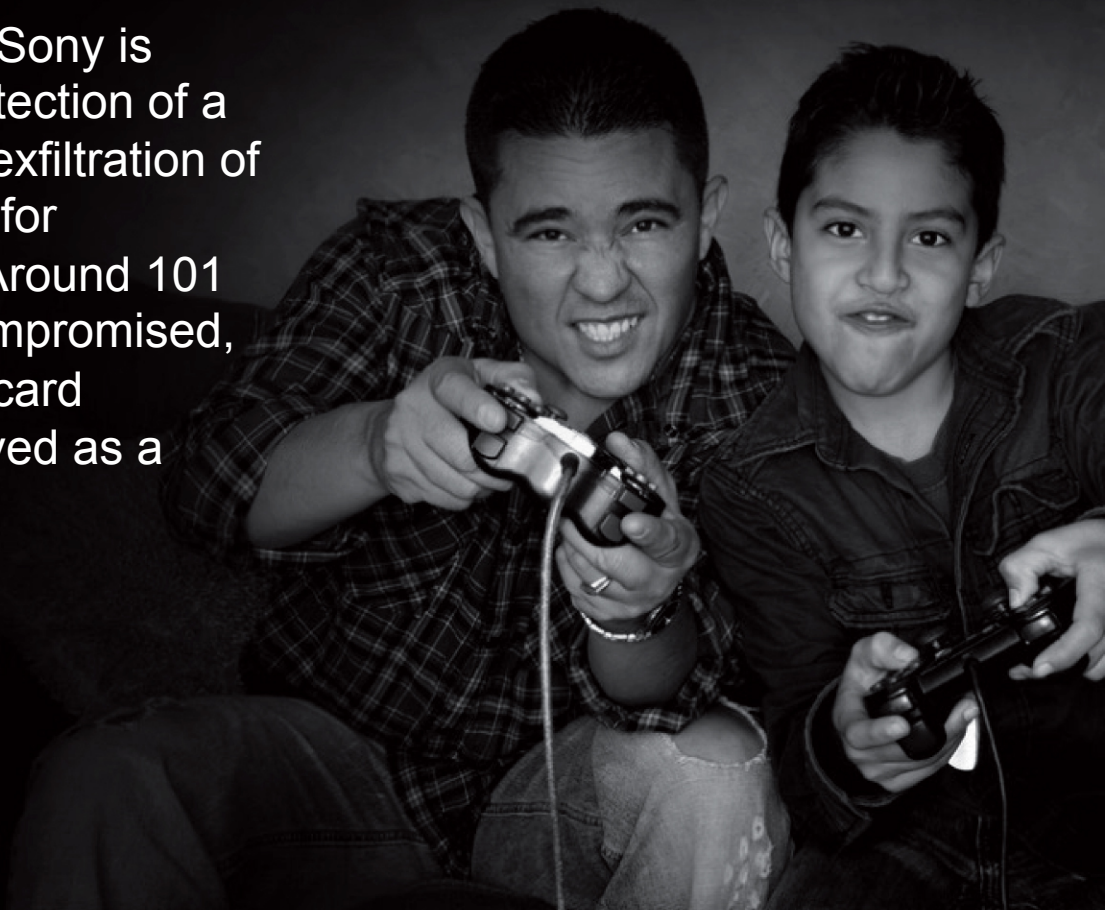
April 2011: DDoS attack on Sony is purportedly used to block detection of a data breach that lead to the exfiltration of millions of customer records for PlayStation Network users. Around 101 million user accounts are compromised, although Sony claims credit card information was securely saved as a cryptographic code.

APRIL 20, 2011

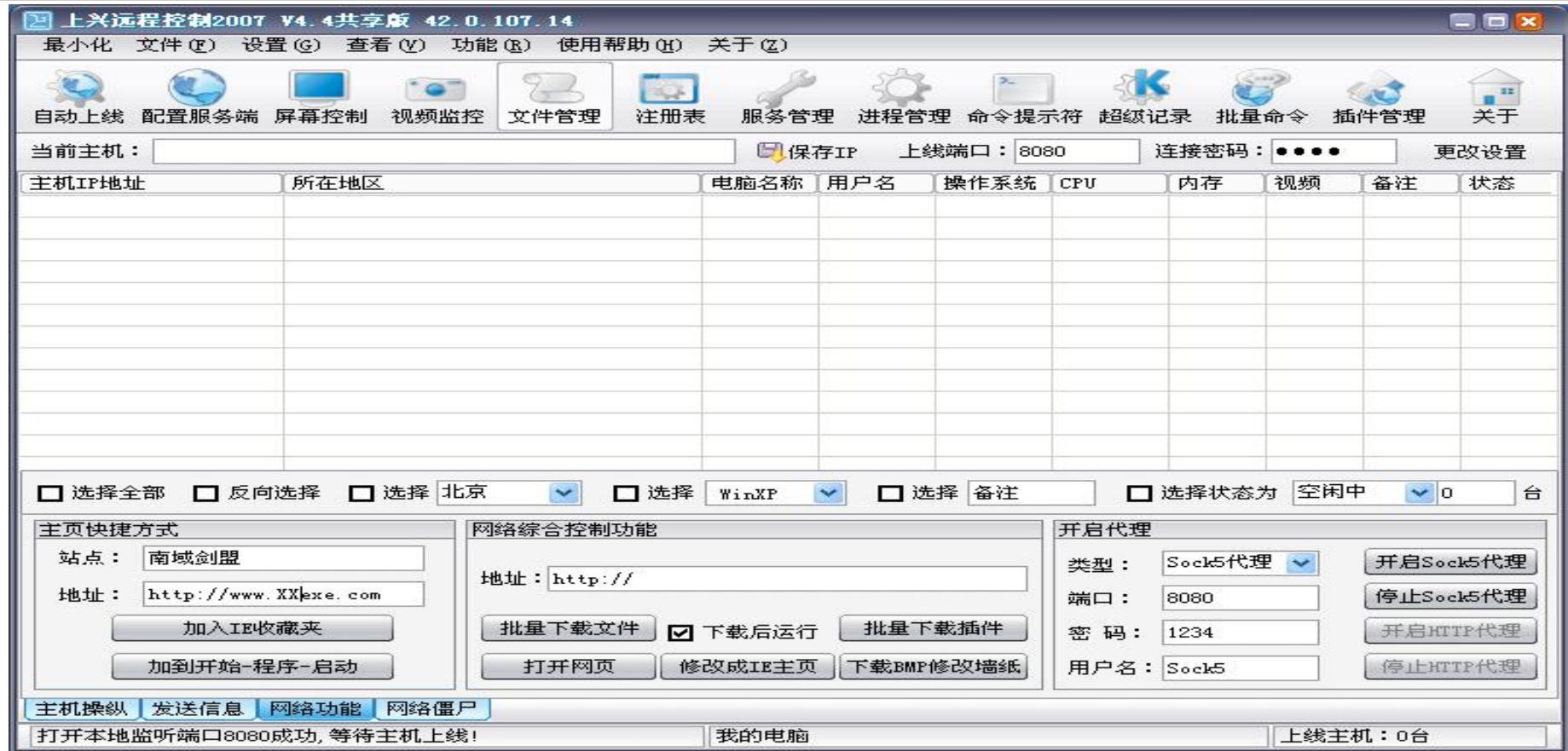
INTRUSION DETECTED

APRIL 26, 2011

CUSTOMERS INFORMED



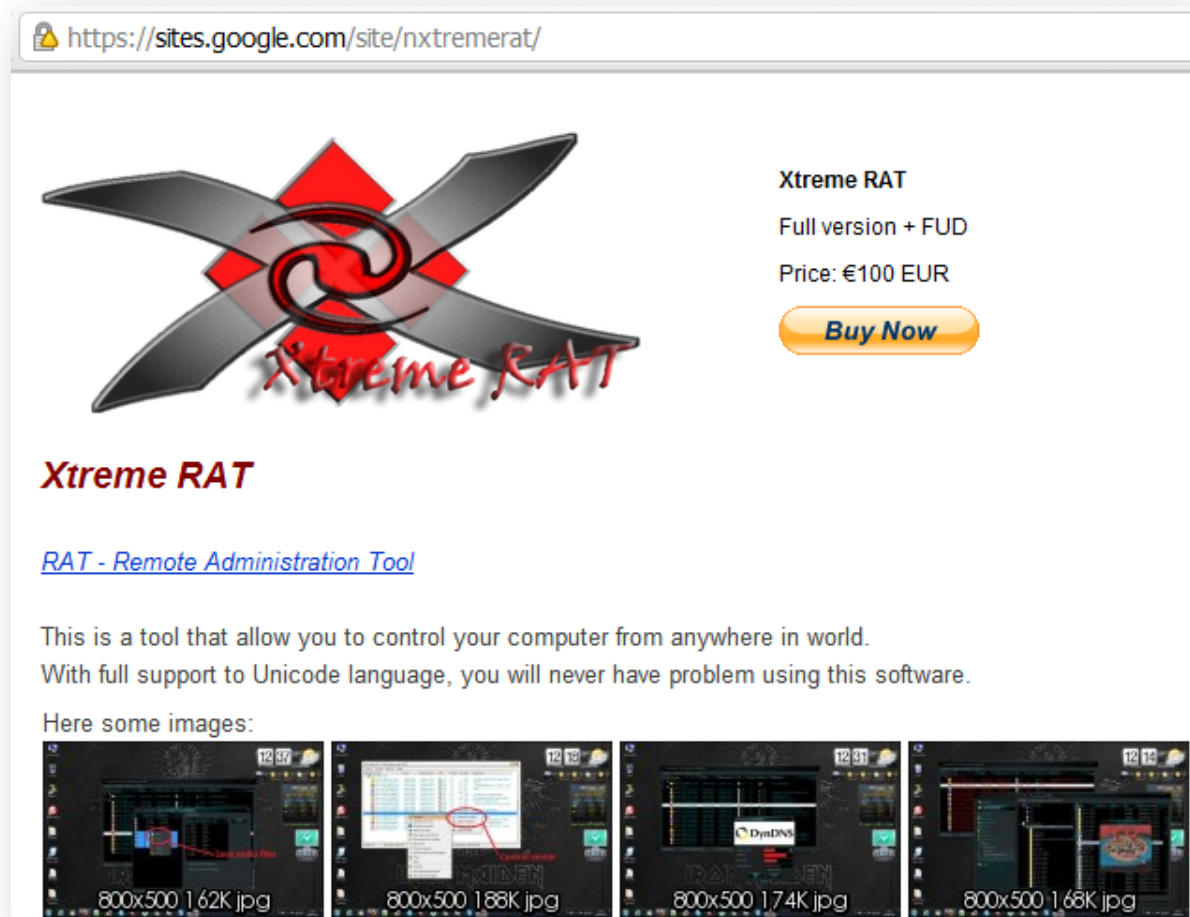
RAT + DDoS – Gray Pigeon aka Hupigon



- Chinese RAT with DDoS capabilities
- Used in espionage style attacks

Xtreme RAT

- Remote Access Trojan (RAT) that allow remote users to steal data from malware-infected machines
 - Spear phishing e-mails targeted US and Israeli government institutions
 - Also used to target Syrian activists





Cyber Warfare

Cyber Warfare Thinking

Russia Alleges Arms Race in Cyberspace

4. (C) Russia (Sherstyuk) believed that "an arms race in cyberspace" was at hand. Sherstyuk said that it was the U.S. who first recognized that cyber capabilities could be more destructive than WMD. He stressed that Russia considered

USOSCE 00000066 002 OF 003

cybersecurity a "political-military" issue. He also agreed that the U.S. and Russia had made little progress in moving forward on this issue bilaterally.

U.S. Concerns with Russian Approach

2. (SBU) U.S. head of del (Markoff) reviewed her guidance, explaining that cyber security was high on the Obama administration's agenda and that a 60-day review of national cyber security policy was currently ongoing. Markoff gave a detailed account of U.S. concerns regarding the RF approach, as it was outlined in Sherstyuk's published remarks. She underscored the key theme that the U.S. did not think that the threats of cyber attack could be usefully addressed by traditional arms control-type constraints. She noted that constraining state capabilities were meaningless when governments have no particular monopoly on attack tools and attacks could be carried out by proxies. She noted that layered "dynamic defenses" are the best way to handle any attack, whatever the source.



2007

DDoS Becomes a Weapon of Conflict

April 2007: The formerly Soviet occupied Republic of Estonia is taken offline by sustained DDoS attacks following diplomatic tension with Russia.

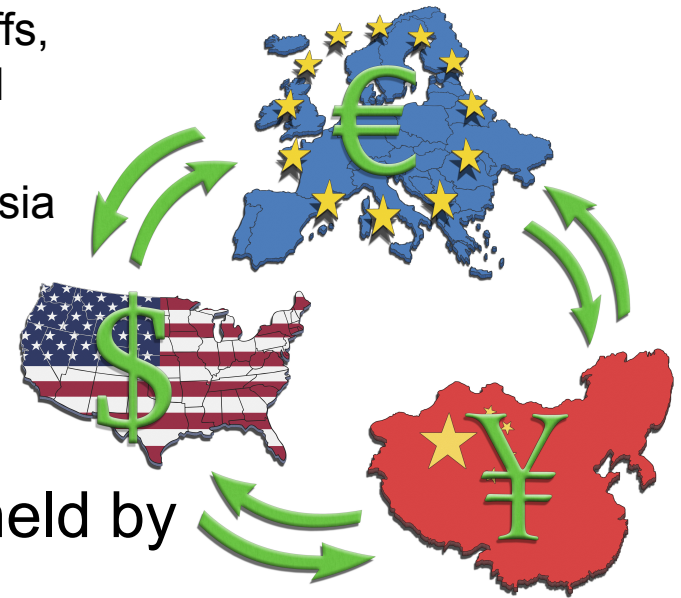
Just over a year later, attacks on Russian and Georgia websites are co-ordinated with ground offenses against Georgia territories by Russian forces. The attack effectively isolates Georgia from the Internet at large.



Russia & China Have Too Much To Lose!

- Obama removes Jackson-Vanik amendment

- Allows US business the benefit of trade with Russia as a full member of the World Trade Organization
- US firms can now benefit from lower import tariffs, intellectual property protection and greater legal transparency
- Exports could double in the next 5 years to Russia

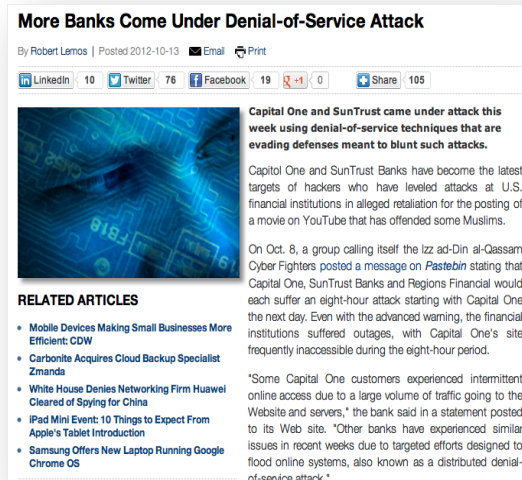


- Approximately 7.5% of U.S. debt is held by China, the largest foreign holder

- China wants the U.S. economy to prosper because that means China will be able to continue exporting here – DUH
- Obama & Xi Jinping to hold regular high level talks around commercial espionage tensions

Focused Multi-Stage & Multi-Vector DDoS

- Longest running public attack campaign in history
- Izz ad-Din al-Qassam Cyber Fighters Attacks on U.S. financial sector ongoing since September 2012
- "There is no doubt within the U.S. government that Iran is behind these attacks,"
 - former U.S. official James A. Lewis



Chase, NYSE Websites Targeted in Cyber Attacks

By Matt Egan, Adam Samson / Published September 19, 2012 / FOXBusiness



Print
Email
Share

Like 143
Tweet 36
Share 14

J.P. Morgan Chase ([JPM](#)) and NYSE Euronext ([NYSE](#)) experienced website trouble Wednesday after being targeted by apparent cyber attacks. The problems came a day after Bank of America experienced prolonged issues following a separate attack.

Flashpoint Partners, an intelligence gathering network specializing in cyber threats, said it believes the Chase outage is "likely due to a sustained denial of service attack." A Flashpoint analyst told FOX Business the attack was probably caused by "a large botnet," a tactic commonly used by hacking group Anonymous. Generally, botnets function by controlling a large number of computers that have been

- Unique characteristics of the attacks
 - Very high packet per second rates per individual source
 - Attacks on multiple companies in same vertical
 - Real-time monitoring of effectiveness
 - Agility in modifying attack vectors when mitigated

North Korea Attacks South Korea

- South Korean television broadcasters & financial institutions attacked on March 20-26
 - Infiltration
 - Monitoring
 - Data deletion
- It is said that N. Korea has over **3000** cyber warfare experts



Project X & Plan X



Added Risks if Nation States are Involved

- Virtually unlimited funding
 - Accelerated development of attack tools
- More precise and persistent than other cyber criminals or hactivists
- High risk that DDoS activity is only part of a much broader cyber campaign
- The 'rules' are uncertain
 - Few want to cross the cyber/physical world boundary





ARBOR SERT
Security Engineering & Response Team

Thank You!



Follow Dan Holden on Twitter: [@desmondholden](#)



Follow Arbor Networks on Twitter: [@arbornetworks](#)



Read the ASERT blog: <http://ddos.arbornetworks.com>