ICANN MEXICO CITY
MARCH 5TH, 2009

Sizing and Scoping eCrime

Jeffrey R. Bedser
President/COO
The Internet Crimes Group Inc.
*i*Threat Solutions

Criminals 'may overwhelm the web'

By Tim Weber
Business editor, BBC News website, Davos

Criminals controlling millions of personal computers are threatening the internet's future, experts have warned.

Up to a quarter of computers on the net may be used by cyber criminals in so-called botnets, said Vint Cerf, one of the fathers of the internet.

Do you know if your PC has been taken over by cyber-criminals?

Technology writer John Markoff

Sophos:
Downadup May Cause Friday the 13th / Southwest Airlines Problems

Posted by **Keith Ferrell** Monday, Mar 2, 2009, 11:52 AM ET

The Downadup/Conficker infestation may be about wreak a little more havoc. Security firm Sophos says the botnet is gearing up for a Friday the 13th move, with Southwest Airlines among its possible targets. Security firm Sophos has posted a blog entry warning that the Downadup worm (aka Conficker, which is how Sophos refers to it)

The blog entry (here) gives some insight into how Downadup works. The botnet -- which by now includes millions of infected machines worldwide -- receives instructions for contacting a specific domain, chosen from a daily list, on specific dates. That domain in turn is used to contact "Conficker central" -- the server from which further instructions and malware are dispatched.

250 possible domains are generated daily, 250 per day; March, with 31 days, will see Downadup/Conficker generate 7,750 domains.

Knowing which domains the botnet will call has become an important tool in erecting defenses against it, specifically by removing the botnet's target domains from availability. Problem is, as Sophos points out, prowling through the March list of domains reveals some legitimate businesses, Southwest Airlines the most prominent among them. (the domain in question is a Southwest Airlines redirect address, wnsux.com, rather than the airline's main site. If Downadup's millions of computers seek to contact the wnsux address, there is the possibility that the redirects could overload Southwest's system.

TOPICS

1. The e-Crime Ecosystem

2. Emerging efforts that focus on protecting end-users against Internet-based crime

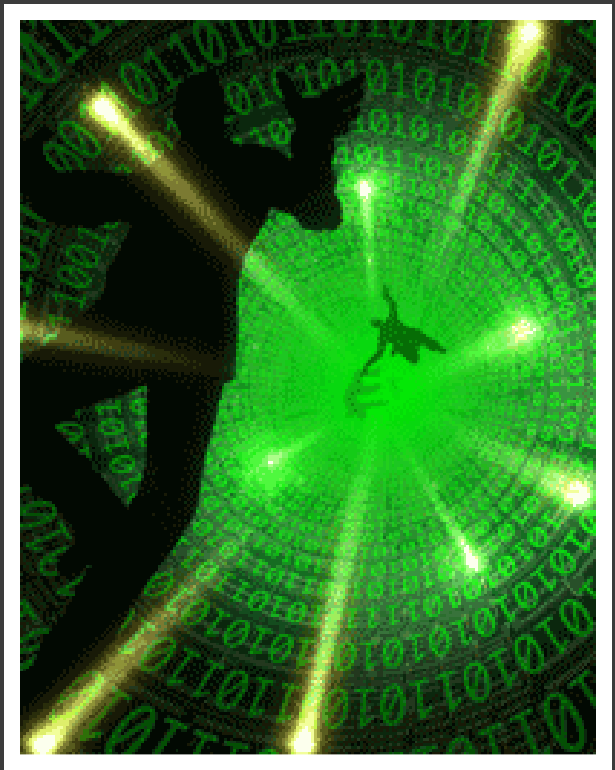
3. Analysis illustrating that e-Crime is able to exploit resources from virtually any user and provider in the global Internet.
4. How criminal attack network activity is distinguished from legitimate (production) traffic.

5. Global hotspots for bot and malware activity.

E-CRIME ECOSYSTEM


CAPITALISM
eCrime = Money

Data Theft and Loss Could Cost Companies $1 Trillion Per Year



Thursday, January 29th, 2009

McAfee released a study today that estimates 2008 losses of intellectual property cost companies **$1 Trillion worldwide**.

Two of the biggest emerging threats are:

1. Targeted crime-ware and malware that steals passwords, credit card numbers and documents.
2. Lax intellectual property laws and enforcement.

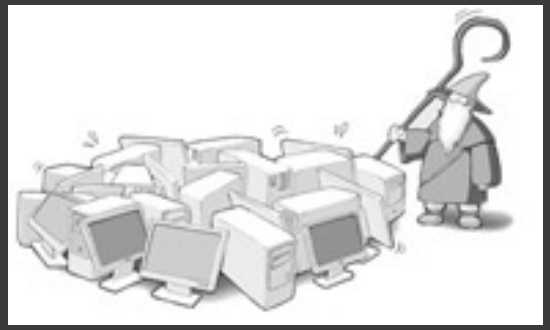
TOOLS

botnet

A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Any such computer is referred to as a zombie - in effect, a computer "robot" or "bot" that serves the wishes of some master spam or virus originator.

According to a report from Russian-based Kaspersky Labs, botnets -- not spam, viruses, or worms -- currently pose the biggest threat to the Internet. A report from Symantec came to a similar conclusion.

BOTNET LIFECYCLE



- Bot-herder creates and configures initial bot parameters (such as infection vectors, payload, stealth, command and control details)
- Register a Dynamic DNS
- Register a static IP
- Bot-herder launches or seeds new bot(s)
- Bots spread

CRIMINAL BENEFITS

- **Shifts the cost of (illegal) business to others, including the costs of being caught engaging in illegal activity**
- **Creates a buffer between a criminal and criminal activity**
- **Provides to criminals a massive information processing resource at minimal cost**

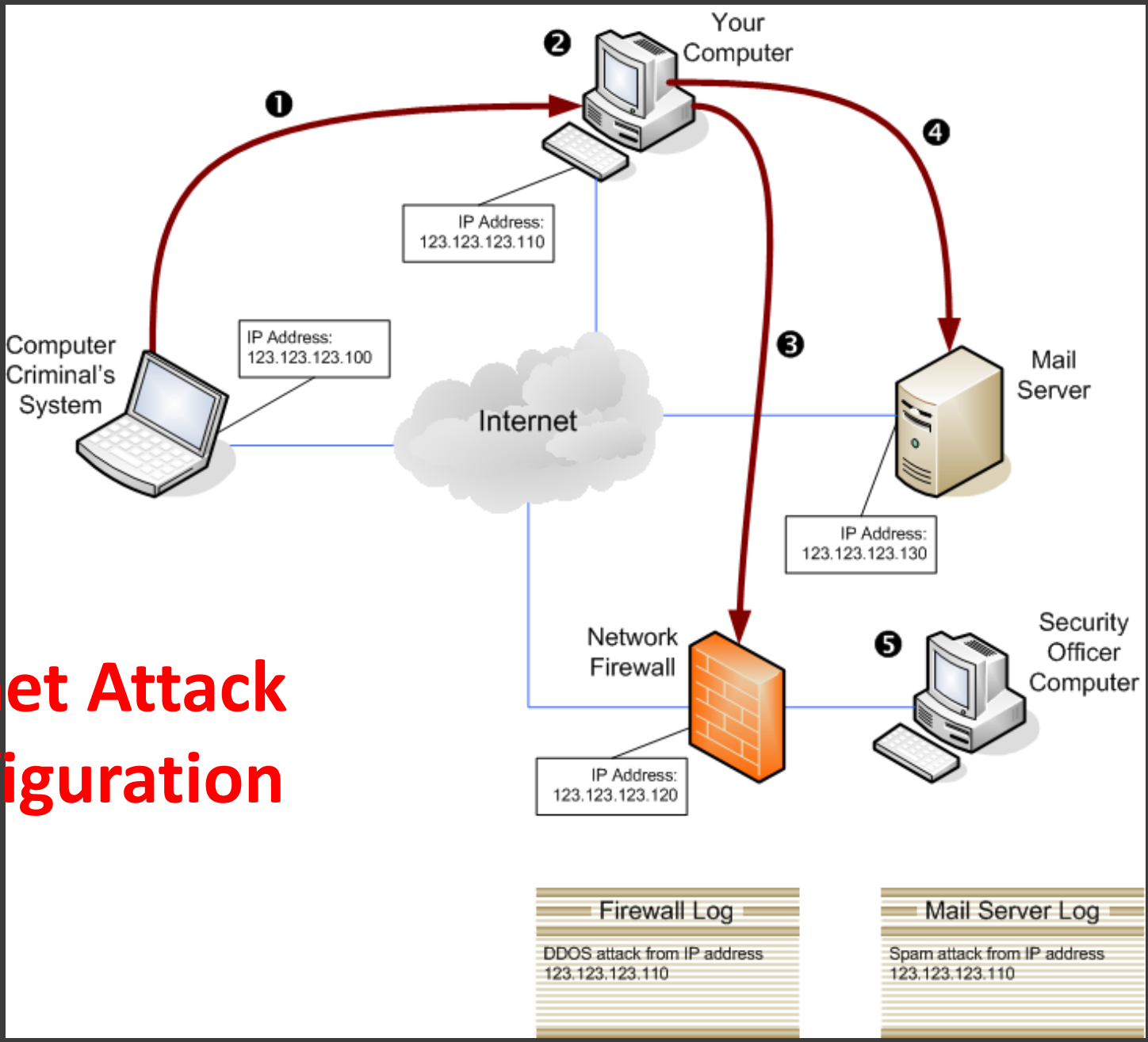
- **Botnets facilitate:**
    1. Bidding to the highest bidder for arbitrary usage
    2. Sale of products and services (often fraudulent or illegal) via spam
    3. Extortion (DoS against governments, financial institutions, etc.)
    4. Identify theft via phishing e-mails

MORE REASONS FOR BOTNETS

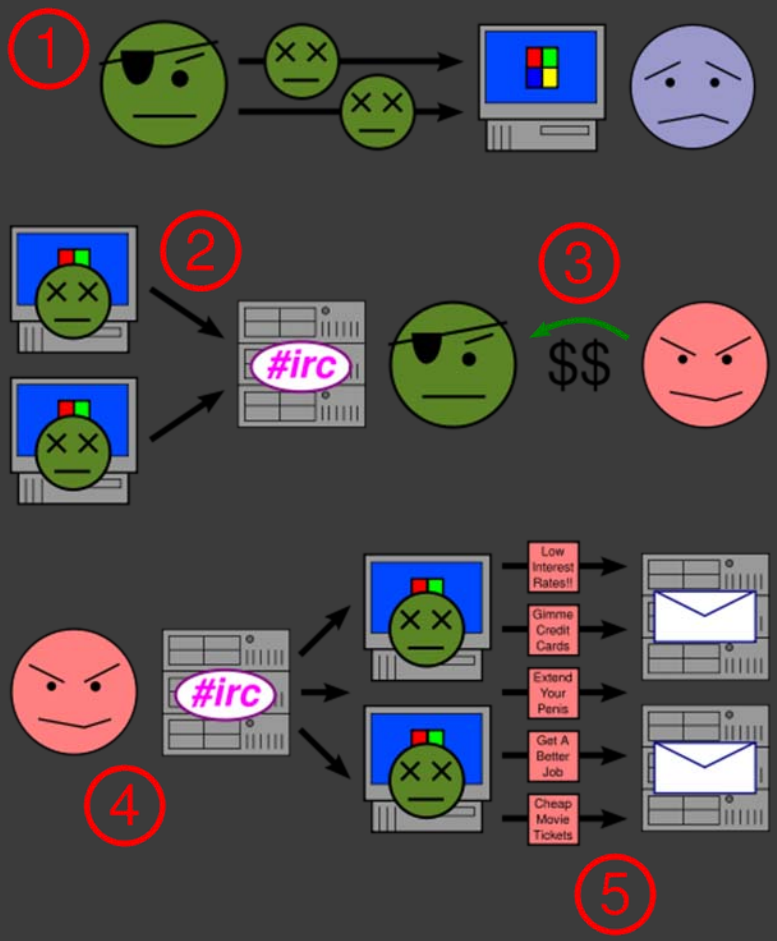
- People will pay for untraceable servers
  - Spammers, scammers, DDoSers
- People will pay for stolen information
  - CD keys, bank account info, passwords to sites
- Rent out time on your botnet

- Adware companies will pay per installed system

Botnet Attack Configuration



BOTNET CREATION WORKFLOW



TYPES OF ATTACKS

- Denial-of-service attacks where multiple systems autonomously access a single Internet system or service in a way that appears legitimate, but much more frequently than normal use and cause the system to become busy.
- Click fraud is the user's computer visiting websites without the user's awareness to create false web traffic for the purpose of personal or commercial gain.
- Access number replacements are where the botnet operator replaces the access numbers of a group of dial-up bots to that of a victim's phone number. Given enough bots partake in this attack, the victim is consistently bombarded with phone calls attempting to connect to the internet. Having very little to defend against this attack, most are forced into changing their phone numbers (land line, cell phone, etc).
- Fast flux is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.

DNS FLAW

Security researcher Dan Kaminsky had uncovered a major DNS flaw which enables hackers to easily perform cache poisoning attacks on any nameserver . Security experts worldwide hurried to patch the problem immediately.

Kaminsky says :
“Recently, a significant threat to DNS was discovered that would allow malicious people to impersonate almost any website on the Internet. Software companies across the industry have quietly collaborated to simultaneously release fixes for all affected name servers.”

However, this fundamental vulnerability is in a design flaw in the DNS protocol itself, and there has been no complete patch or solution for it yet.

An attack of that nature would cause a corruption on a DNS server, so that, for example a user who types Google.com in his browser, would end up at a location of the attacker's choice.

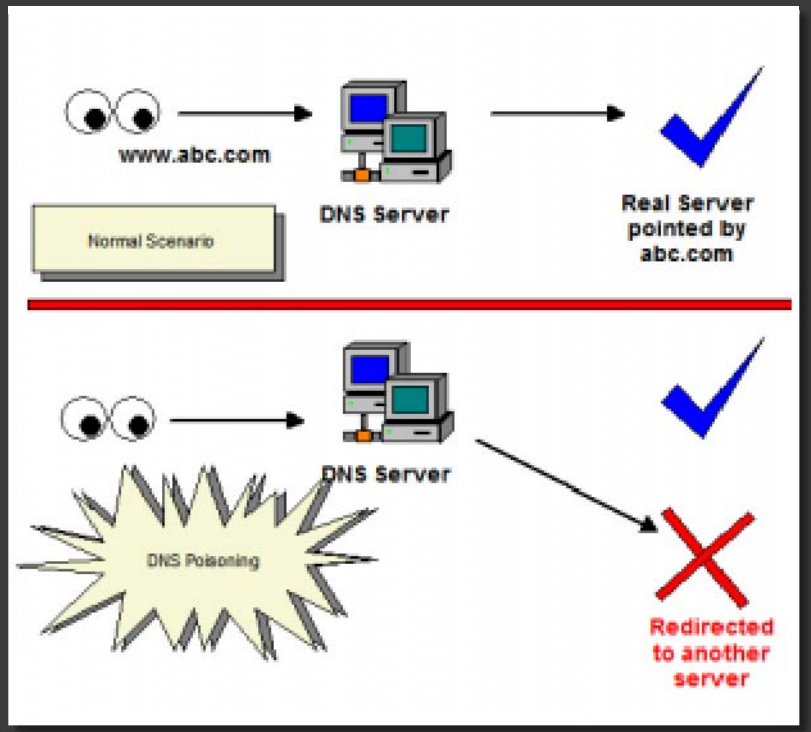
Profiting from the DNS Flaw

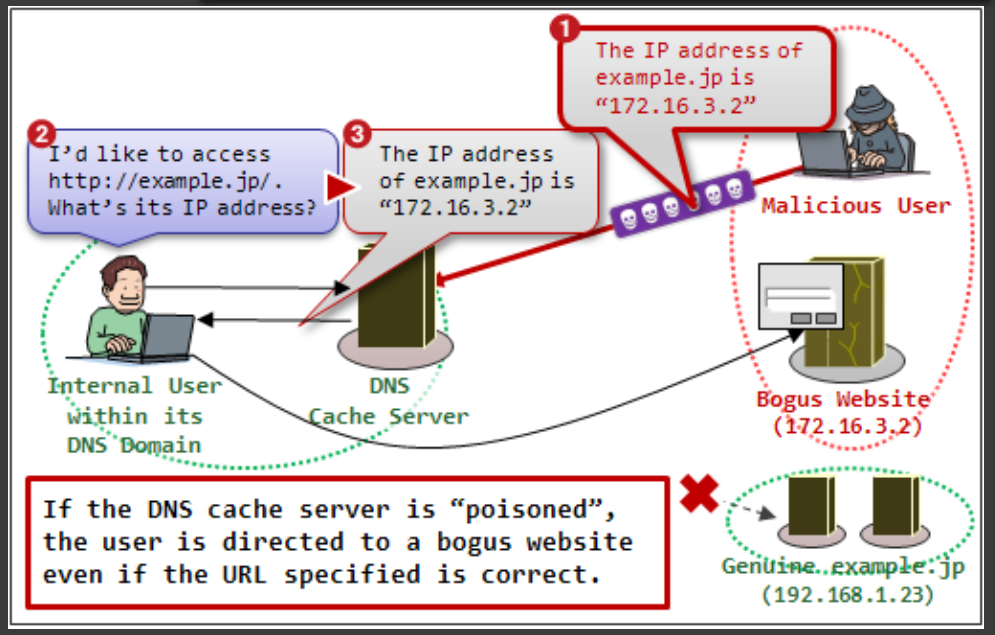
- An attacker can set up a website that looks enough like the original so as to not raise any suspicion.

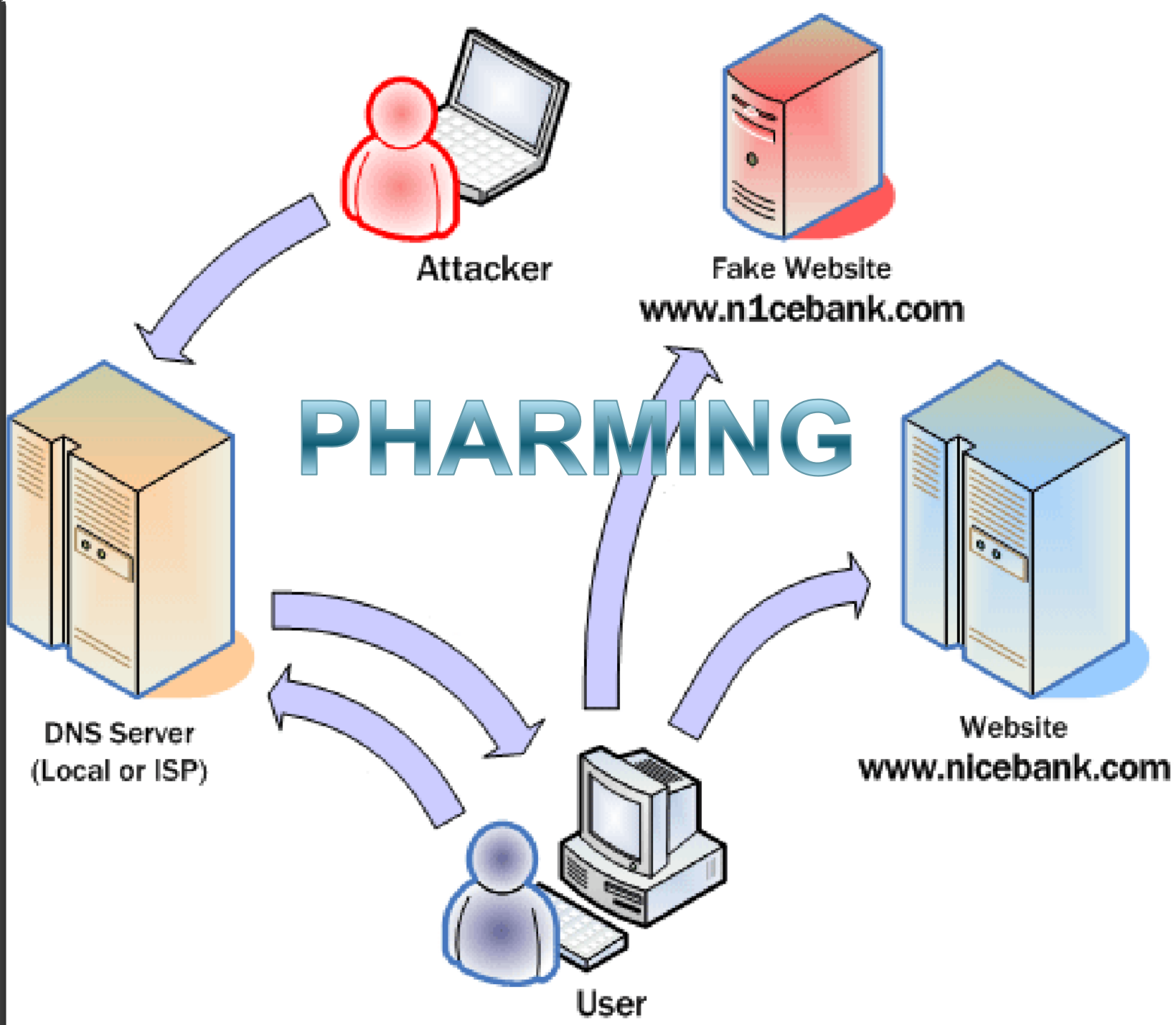
- Redirecting a popular search engine to a malicious domain or redirecting a bank website to gain access to user account credentials.

- Zero-day attacks will occur between the time security vendors release patches and DNS servers get patched.

- URL filtering based products will prove insufficient in dealing with this type of attacks.
    - URL filtering products do not inspect the IP address so a hijacked website may pass the URL filtering because of the fact that the domain is still trusted, although the IP addresses is untrusted.






Attacker
Fake Website
www.n1cebank.com
PHARMING
DNS Server
(Local or ISP)
Website
www.nicebank.com
User

Pharming: (pronounced farming)

is a hacker's attack aiming to redirect a website's traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.

The term *pharming* is a neologism based on *farming* and *phishing*. Phishing is a type of social engineering attack to obtain access credentials such as user names and passwords. In recent years both pharming and phishing have been used for online identity theft information. Pharming has become of major concern to businesses hosting ecommerce and online banking websites. Sophisticated measures known as anti-pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming.

Source: http://en.wikipedia.org/wiki/Pharming

Methods for Dealing with Criminal Attack Network Activity

Honeypots/Honeynets Are used to detect communication attempts toward unused IP addresses. In that case an alarm is triggered, warning that someone is trying to compromise or attack the network.

Blackhole routing and sinkhole routing, can be used when the network is under attack. These techniques try to temporarily mitigate the impact of the attack. They direct routing traffic to a null interface, where it is finally dropped.

Filtering on the service. This tactic presupposes that we know the attack mechanism. In this case, we can filter traffic toward a specific UDP port or a TCP connection or ICMP messages. But what if the attack is directed toward a very common port or service? Then we must either reject every packet (even if it is legitimate) or suffer the attack.

Filtering on the destination address. Attacks are usually addressed to a restricted number of victims, so it seems to be easy to reject all traffic toward them. But this means that legitimate traffic is also rejected. In case of a large-scale attack, this should not be a problem because the victims will soon break down and the ISP will not be able to serve anyone. So filtering prevents victims from breaking down by simply keeping them isolated.

Hybrid Methods and Guidelines

Currently researchers try to combine the advantages from all the methods stated previously in order to minimize their disadvantages.

Further Thoughts

The Internet is not a stable environment — It reforms itself rapidly. This means that countermeasures quickly become obsolete. New services are offered through the Internet, and new attacks are deployed to prevent clients from accessing these services.

Obviously, it appears that both network and individual hosts constitute the problem. Consequently, countermeasures should be taken from both sides. Because attackers cooperate in order to build the perfect attack methods, legitimate users and security developers should also cooperate against the threat.

EFFORTS to Combat

1. International Cooperation:
    1. IMPACT: International Multilateral Partnership Against Cyber Threats (www.impact-alliance.org

        1. Goes online March 20, 2009
        2. Agreements with the United Nations and Interpol and others

    1. Honeynet Project – combined efforts of a large number of analysts and researchers


Global Hotspots of
Malicious Activity

Global Hotspots – Activity Snapshots

BY COUNTRY

Key	Country	Attacks per subnet	Percentage
	US (United States)	0.09	37.7%
	TW (Taiwan)	0.03	12.2%
	ES (Spain)	0.03	12.1%
	BR (Brazil)	0.03	11.3%
	GR (Greece)	0.02	7.2%
	DE (Germany)	0.01	4.7%

BOT NETS connecting to a command and control iRC channel over a five (5) day period

Sum it all up…

…and some thoughts to leave with…

1. eCrime is for profit.

2. Any component of infrastructure that can be compromised to enable these ill gotten profits will be utilized.

3. Today botnets and pharming are part of organized crime. Tomorrow… state sponsored cyber terrorism? Same infrastructure can be tasked to either objective.

4. Don’t expect the researchers and technology companies to solve this.

5. International cooperation between the entities that run the infrastructure, policy makers and law enforcement will facilitate a means to an end.