Defence Intelligence.

Mariposa Botnet Briefing
Three arrests have been made...

Over 1,000,000 personal credentials recovered thus far during investigation

Since March 3rd - 903 international news stories have been published about Mariposa

From Dec 23rd 2009 through March 7 2010 there have been 15,550,850 unique IPs connecting with the exact Mariposa connection string to the sinkhole
What Does it Do?

Whatever it wants. The software behind Mariposa is engineered to gain access to and maintain control over the victim machine. The most lucrative use of the botnet is of course, data theft. Over 1 million stolen usernames, passwords, and banking details have been recovered from the machines of the botmasters.

*In 2008, data breaches led to the theft of 85 million personal records.* - DataLoss DB
Who is responsible?

Currently there have been three arrests in relation to Mariposa.

How does it spread?

By default, the malware is designed to spread across instant messenger programs, USB keys, and P2P networks. It will also exploit older versions of IE6 to install the latest Mariposa binary without user interaction.

In the last year, 70 of the top 100 most visited websites served malicious software or redirected users to malicious sites. - Websense
Why Mariposa?

The primary kit behind the creation of Mariposa is called bfbot or the butterfly bot kit. We determined that the primary botmaster was in Spain, and Mariposa is Spanish for butterfly. As a bonus, calling someone a Mariposa is apparently an insult.

What companies/organizations are compromised?

While we will not disclose any compromised parties publicly, we can see all systems compromised by Mariposa. Of the Fortune 500, it would be easier for us to say who isn’t compromised.

3 out of 4 enterprises have undetected, compromised computers within their network.
- Gartner Research Products
The biggest ever? - 15.5 million unique IP addresses
How we detected Mariposa

97% of malware uses DNS to locate its command and control

- We use DNS to detect malware.
- Strategically placed sensors on the Internet provide DNS visibility into more than a dozen countries.
- Ground breaking behaviour analysis engine allows us to determine human vs. automated behaviour.
January 2009

• Reports concerning the butterfly kit start hitting the web.

“This thing...is one bad-mother.” - Rafal Los SPI Dynamics/HP

May 2009

• Defence Intelligence notices the formation of a new botnet and starts to track it.

June - July 2009

• Tracking establishes the growth of the botnet, little information on victims or perpetrators is known. The butterfly kit is not yet known to be the main compromise mechanism.
August - September 2009

• The size of the botnet warrants in-depth investigation. Critical/sensitive networks are identified. The butterfly kit is determined to be the main payload used to spread and maintain control of victims.

• Defence Intelligence begins notifying organizations compromised by Mariposa.

*Notification was not as well received as we had hoped.*
“You hacked my network!!
- This is blackmail!!”

“You’re lying! We use Symantec/McAfee/Trend/etc.”

“Who is this? You’re socially engineering me!”

“What are you selling?”

And a few times:

“Thanks for the info, we found the machines and took care of them.”
• Only 6 of 41 AV Vendors detected it according to VirusTotal

• The Canadian Bankers Association confirms presence within banks

• The World Bank releases emerging threat snort signature based upon our binary analysis

• Palo Alto Networks releases Wireshark plugins for detection based upon the same analysis
October - December 2009

- Start taking over command and control domains
- In retaliation, C&C changes to defintelsucks.com, net, org
- Track the bad guys (domain registrations, logins, email addresses)
- Identify and enumerate victims through sink-holing of C&C channels
- Information and evidence gathering for law enforcement
December 23, 2009

- MWG executes worldwide takedown of all remaining botnet C&C domains
January 22, 2010

- An entry level employee of a European domain registrar working with the MWG accepts a bribe from the botmaster to re-establish control of the botnet.

January 25, 2010

- Guilty employee terminated, MWG regains control

- DDoS against Defence Intelligence - over 900MB/sec (seen) sustained traffic sent to our network
January 26, 2010 - Now

- Guardia Civil and the FBI execute search warrants and arrest primary botmaster.
- Computing devices are seized and examined, additional participants are arrested by local law enforcement in their countries.
- Binaries are distributed to AV companies to create signatures for complete (hopefully) remediation.

March 3, 2010

- Spanish LE Hold press conference.
- A complete technical analysis is completed.
Why didn’t the big guys detect this?

- Modern malware is designed specifically to avoid detection. This is big business, usually funded by international criminal organizations.

- Modern malware updates on average, every 24 hours - AV signatures often take weeks.

- The security industry is trying to apply outdated technology and methodology to a threat which has evolved.
“Less sophisticated cybercriminals still use attacks that AV vendors can catch, but signature-based AV tools are becoming ineffective as fine targeting and one-time packing techniques now dominate commercial malware activities. Traditional tools will be even less relevant as the threatscape shifts.”

- McAfee

Infected files which one or more anti-virus engines failed to detect
Infected files detected by all anti-virus engines

* virustotal.com January 5, 2010
Anti-Virus

• Malicious software generally employs AV detection or evasion. Advanced forms of these techniques disable AV protection entirely.

• The amount of malware to process has become overwhelming for every anti-virus company - 50,000 binaries/day - Shadowserver

• Modern malware updates on average every 24 hours - Perpetual 0 Day

• The major AV vendors have a combined proactive detection rate of 45% - AV Comparatives

“The most popular brands of anti-virus have an 80% miss rate. That is not a detection rate, that is a miss rate.” - Australian Computer Emergency Response Team
Fighting Malware is all ours responsibility!

- If we have to wait for a court order, the bad guys will win. Every time.
- As long as Malware uses DNS, we should use DNS to fight Malware.
- CyberCriminals make more money than drug traffickers. Every country is losing money to these guys.

Domain ReDirection

- Sinkholes enable remediation and damage control.
- Sinkholes allow us to truly understand a given botnet. You can’t prevent something you don’t understand.