DNS FIREWALL

Charles Griffin

Systems Engineer

CISSP

INFOSEC THROUGH THE AGES…

World War 1

World War II

Today

THE DEATH OF CRYPTOGRAPHY?

- *Prepare for 'post-crypto world', warns godfather of encryption*
-
- ~Shamir (as in RSA)

- By John Leyden
- Posted in Security, 1st March 2013 12:47 GMT

- *Cryptography is 'becoming less important' because of state-sponsored malware, according to one of the founding fathers of public-key…*

WHAT ARE AGGRESSIVE CONTENT THREATS?

- Security Threats:
- Botnets
- Phishing
- Spyware
- Trojans & exploits

WHAT ARE AGGRESSIVE CONTENT THREATS?

- Most Web filters do not reliably detect much less stop malware based on:
- Observed behavior of executing or downloading malware.
- Malware tied to innocuous content (such as celebrity photographs)
- Fast changing URLs or domains (FastFlux)
- IP addresses not tied to a URL
- Call homes using DNS
- Backdoor data uploads using DNS, SIP, and IRC

NEW YORK TIMES ATTACK


HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | U.S. Edition

The New York Times

Business Day
Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Hackers in China Attacked The Times for Last 4 Months

A Cyberattack From China: TimesCast: Chinese hackers infiltrated The New York Times's computer systems, getting passwords for its reporters and others.

By NICOLE PERLROTH
Published: January 30, 2013 | 383 Comments

SAN FRANCISCO — For the last four months, Chinese hackers have persistently attacked The New York Times, infiltrating its computer systems and getting passwords for its reporters and other employees.

FACEBOOK
TWITTER
GOOGLE+

On 1/30/13 the NYT announced that they had been the victim of hacker attacks for over 4 months originating in China

- How the attack developed:
  - Source: Phishing / Spear Phishing likely but other approaches are suspected as well
  - Botnet: The botnet / attackers changed IP addresses and used compromised US University machines as proxies
  - Deepening: Utilized over 45 types of malware, only 1 which was caught by antivirus

NYT ATTACK CONTINUED…

- Why attack was difficult to detect?
- - The malware and attack vectors were designed to circumvent firewalls, web filtering, and anti-virus defenses

  - Malware used DNS to locate the botnet controller

  How DNS Firewalling (RPZ) would have helped-

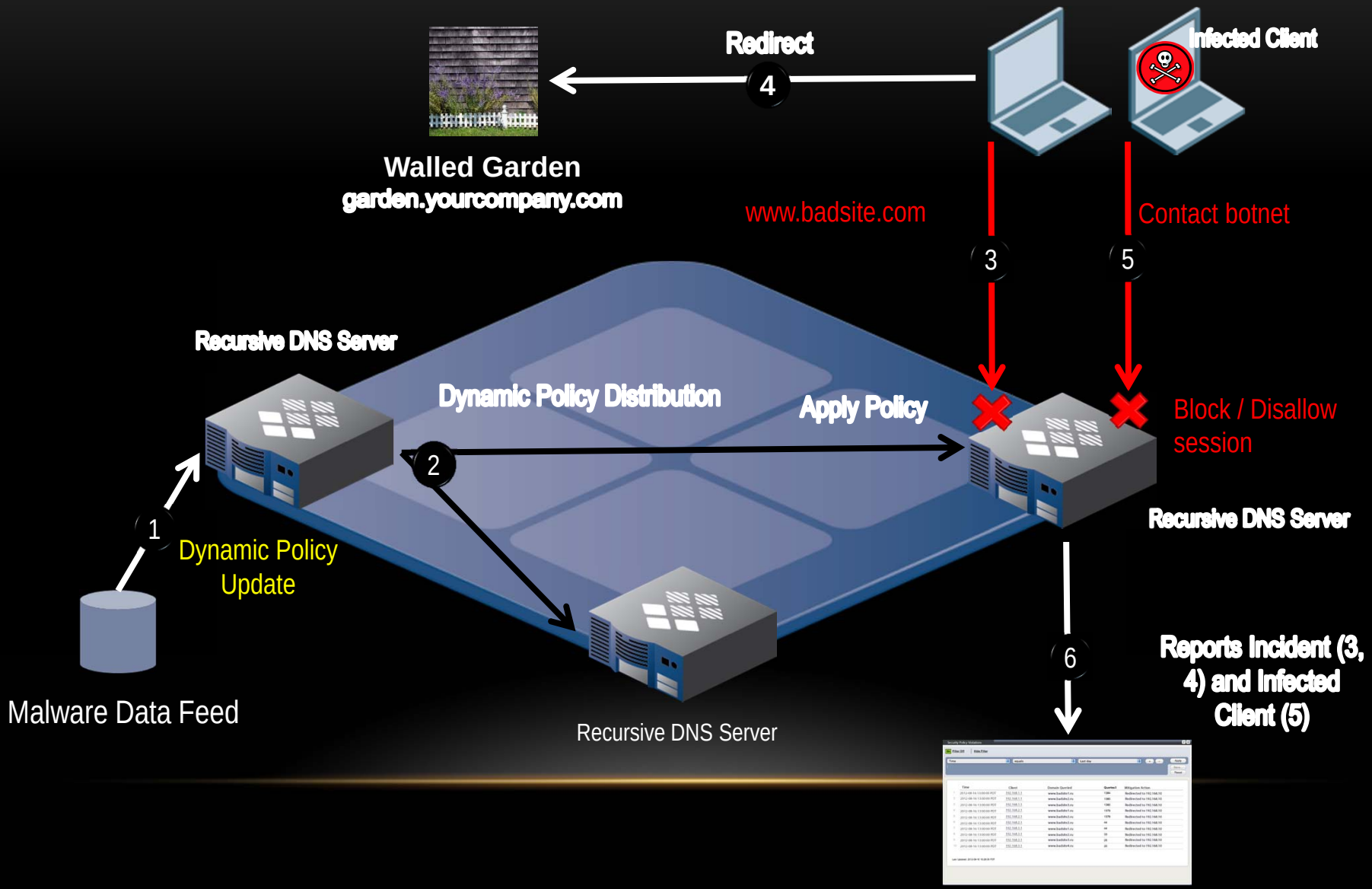
  - The malware data feed targets specific IP locations, *may* have prevented infection via phishing – if first query went to a tagged site

  Would have disrupted botnet communications to China

  A reporting server could have alerted of the attacks - very early in the attack lifecycle – “client X has a lot of traffic hitting the RPZ list”

- *RPZ is a technology developed by ISC which provides DNS recursive resolver operators with a simple way to block certain queries which they wish to or legally must prevent or to redirect them to an alternative location.*
- *RPZ allows a great deal of flexibility and fine-grained selection of resolver policy.*

HOW DOES THE DNS FIREWALL WORK?



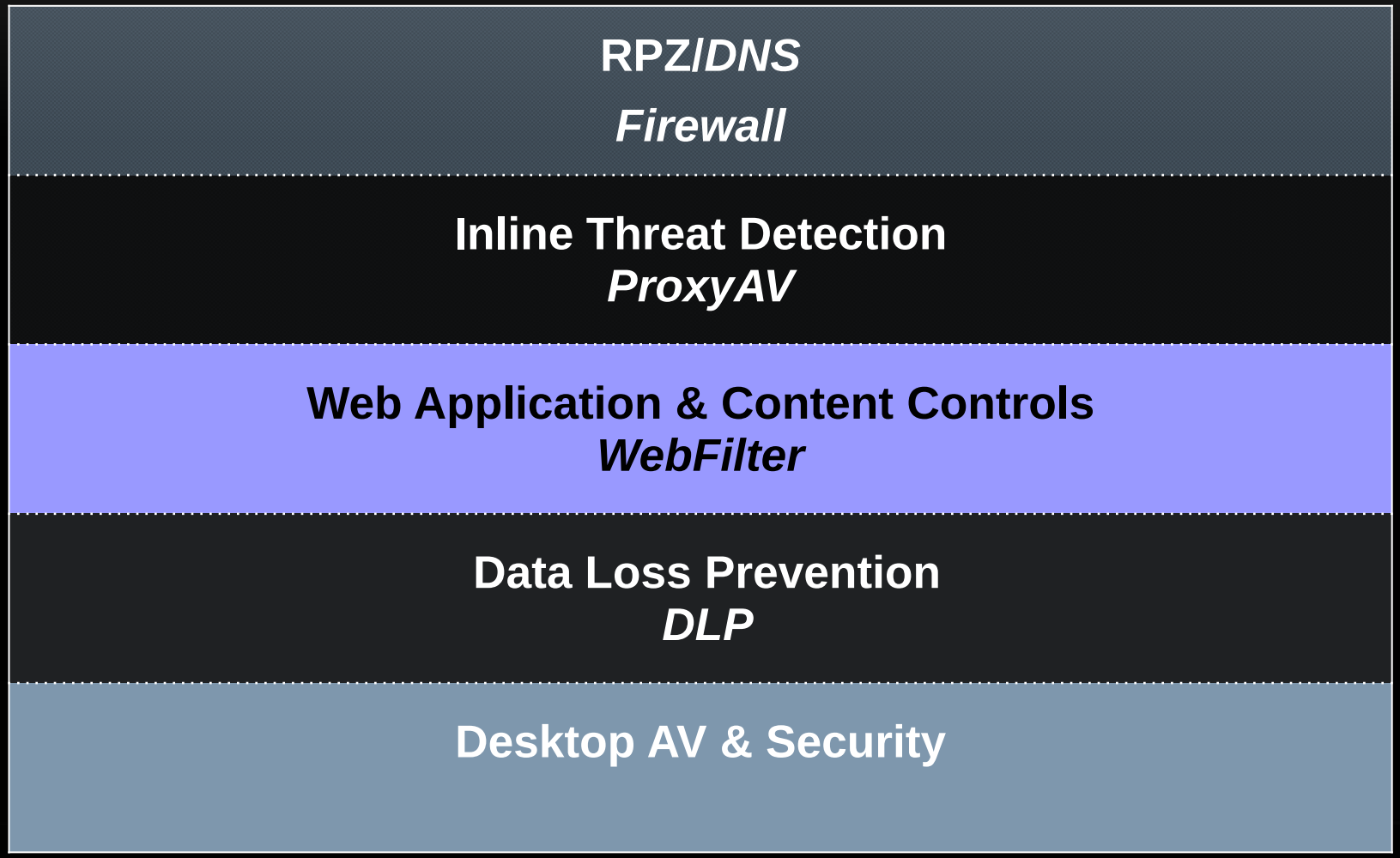
TRADITIONAL URL FILTERING HAS MANY HOLES

- Poor coverage leaves holes in protection
- Slow rating lets new malware outflank defense
- Uses one category per site, which leads to inaccurate categorization and ineffective security
- Crude options: Blocks whole page instead of just malware. Leads to complex policy mgmt.
- Average Phishing site exists for only 5.5 days. Most of that time it will be uncategorized.

CHALLENGES FOR TRADITIONAL FILTERING RPZ ADDRESSES…

- All it can do is Block URLs it knows have spyware and allow all the rest.
- Bad News 16 Billion + Web pages, You can never know what's on every site at every moment.
- Hundreds of thousands of new URL each week
- Existing sites may add spyware adding to the problem.
- Simple fact is the web has become too dynamic.
- Some vendors do use Dynamic Categorization. But this technology has proven to create many false positives.
- Content Filtering was designed to RATE, CATEGORIZE and BLOCK url's

Layered Defenses



THANK-YOU