Keeping Your Service Secure – Are You Doing Your Diligence?

ccNSO Meeting – ICANN51 - October 14, 2014

Merike Kaeo, CISO

Topics For Today

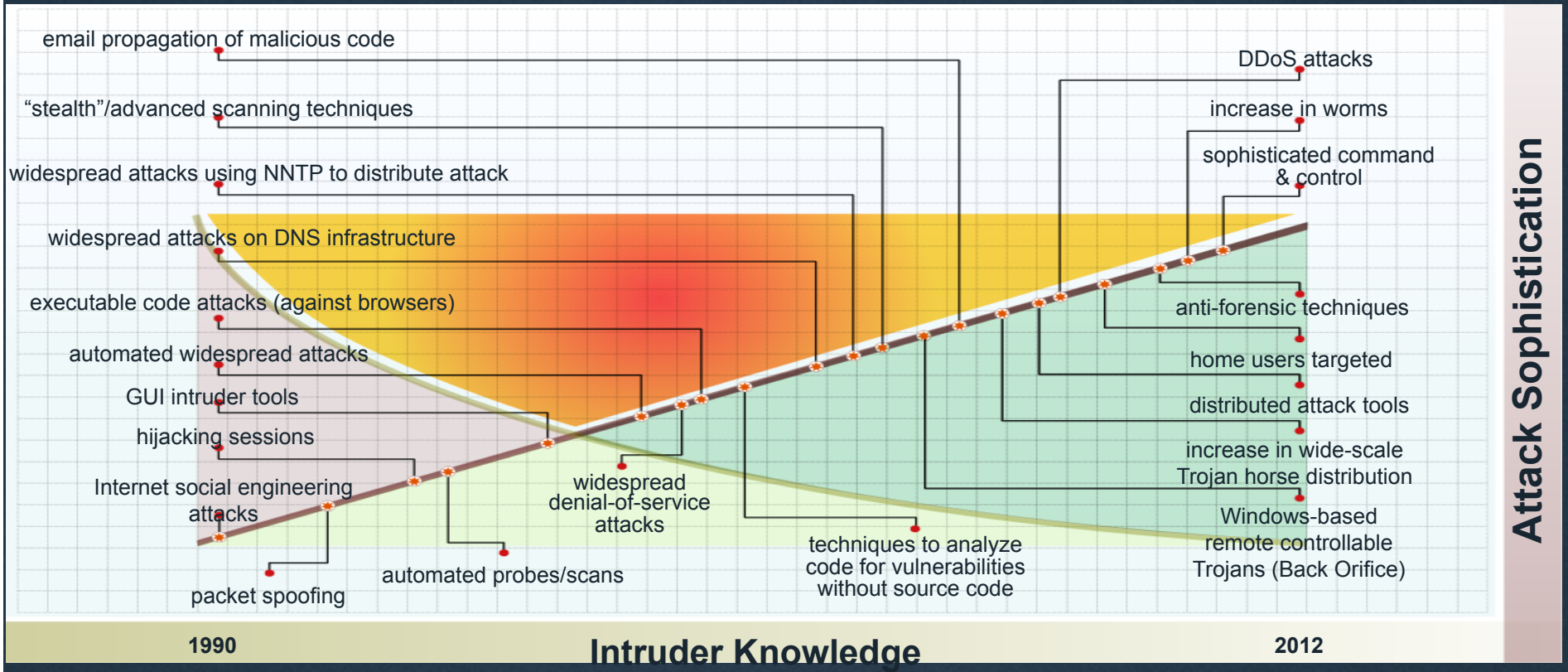
Trends in Attacks

Exploitation and Impacts

Community Responsibility

What You Can Do

Evolution of Attack Landscape



Credential Leakage is a Big Problem

Most often thru re-use of usernames and passwords

- How many registrants use usernames and passwords that they also use for their social media access?

Uncontrolled processes where new passwords are sent in cleartext emails to users

- This happens more often than you'd think

Exploiting vulnerabilities to get unauthorized access to systems where password files may be stored

Critical Vulnerabilities (last 6 months)

SSL/TLS

- Heartbleed followed by more bugs in June
- Be on lookout for more vulnerabilities

Scripts and Shells

- Bash shell issues [Shellshock] still need attention
- Resource for Proof of Concepts and Potential Targets

  https://github.com/mubix/shellshocker-pocs

Keeping Up With Vulnerabilities

Know Your Operating Systems and Application Versions

- For TLS/SSL can use publicly available tests
- https://www.ssllabs.com/ssltest/

Get On Mailing Lists For Vendor Security Announcements

Subscribe to National CERT Alert Lists

- https://www.us-cert.gov/ncas/alerts/

Follow Security Industry Blogs

- http://ccnso.icann.org/resources/cybercrime-resources.htm

Determine Likelihood of Risk

Likelihood	Definition	Description
Low	Unlikely	Working tools or exploits are not readily available. Exploitation requires in-depth knowledge of the system and/or may require strong programming skills. User (or perhaps higher privilege) level access may be one of a number of pre-conditions.
Medium	Likely	Tools and exploits are available but need to be modified to work successfully. Exploitation requires basic knowledge of the system and may require some programming skills. User level access may be a pre-condition.
High	Certain	Tools and exploits are readily available on the Internet or other locations. Exploitation requires no specialized knowledge of the system and little or no programming skills. Anonymous users can exploit the issue.

Assess Impact of Successful Exploitation

Impact	Definition	Description
Low	Negligible	The risk will not substantively impede the achievement of business objectives, causing minimal damage to the organization's reputation.
Medium	Moderate	The risk will cause some business objectives to be delayed or not be achieved, causing potential damage to the organization's reputation. User level access with no disclosure of sensitive information.
High	Critical	The risk will cause damage to systems and the organization's reputation. Administrator level access (for arbitrary code execution through privilege escalation for instance) or disclosure of sensitive information.

Review Credential Lifecycle Management

Creation

- Utilize password cracking tools to check strength of passwords
- https://www.thc.org/thc-hydra/

Distribution

- Look to use cryptographical means for integrity and confidentiality

Storing

- Ensure credentials never stored in publicly accessible systems
- All credentials should be stored using cryptographic protections
- Pass The Hash Attacks

  http://www.microsoft.com/en-gb/download/details.aspx?id=36036

Review Credential Lifecycle Management

Renewal

- Tradeoff between too frequent vs how long a potential credential compromise can go undetected and cause harm

Revocation

- Remember to create a revocation certificate at the time when certificate created.

Recovery

- Scenarios where employee leaves company or forget password

What Are Basic Things Everyone Can Do

Control Physical and Logical Access to your Critical Servers

Credential Management

- Don’t share credentials across systems
- Look at entire lifecycle of how you handle credentials (creation, distribution, storing, renewal, revocation, recovery)
- Test password strength
- Encourage 2-factor authentication

Keep track of operating systems and application versions and apply security patches as they become available