DAKOTA STATE UNIVERSITY

# Dynamic Resolution

## A Deeper Look

Thomas Williams

CSC 840 - Final

# Dynamic Resolution – Why Care?

- Implications for past attacks – what if the WannaCry kill switch (*iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com)* in had been generated periodically by a DGA?[1]
- Prevalence of techniques in current botnets, C2 attacks, and even phishing [2]
- Difficult to reliably detect[2]
  - Constantly changing
  - Masked by similarity legitimate traffic
- Understanding helps detection and prevention

[1] “The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet”, *Wired Magazine,* https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/
[2] “What is DNS Fast Flux?”, *Cloudflare*, https://www.cloudflare.com/learning/dns/dns-fast-flux/

# Dynamic Resolution - What?

- Family of techniques containing…
  - **Domain Generating Algorithms (DGAs)** – Dynamically creates new domains for Command and Control (C2) attacks
  - **Fast Flux DNS** – Rapidly rotate IP addresses for DNS URLs
  - **DNS Calculation** – Dynamically generate port and IP numbers to use based on DNS URL
- Takes advantage of **legitimate uses** of technology (primarily load-balancing) to hide malicious activity

"Dynamic Resolution", *MITRE ATT&CK Framework,* https://attack.mitre.org/techniques/T1568/

# Methods – DGAs

- Reasonable use – load balancing, disaster recovery[1]
- Generation
  - Gibberish strings
  - Dictionary word compilation
  - Deterministic vs Non-deterministic
- Why is detection hard?
  - Sheer volume – thousands of DNS entries can be created and registered in a short amount of time

[1] “Understanding domain generation algorithms (DGAs)”, *Zscaler, https://www.zscaler.com/cxorevolutionaries/insights/understanding-domain-generation-algorithms-dgas*
[2] “What is DNS Fast Flux?”, *Cloudflare*, https://www.cloudflare.com/learning/dns/dns-fast-flux/

# Methods – Fast Flux DNS

- Reasonable use – load balancing, redundancy[1]
- Methodology
  - Uses round robin DNS plus very short TTL values
  - Single fast-flux – IP address changes for URL frequently
  - Double fast flux – also changes the authoritative nameserver for the URL
- Why is detection hard?
  - Frequent changes to multiple layers makes tracking difficult
  - Again, sheer volume

[1] “What is DNS Fast Flux?”, *Cloudflare*, https://www.cloudflare.com/learning/dns/dns-fast-flux/

# Methods – DNS Calculation

- Reasonable use
  - Dynamic DNS for connectivity into home environments that may not have a static IP[1]
  - For ports, no legitimate cases documented
- Generation
  - IP – Not well documented
  - Port – Can use octets of returned IP from DNS query to generate port value, typically (A * B) + C[2]
- Why is detection hard?
  - For ports, real IP addresses of blogs are often used, masking the generation process. If non-well-known ports are used, detection can be easier

[1] “What Is DDNS (Dynamic DNS) and How Does It Work?”, *WhatIsMyIP, https://www.whatismyip.com/ddns/*
[2] “Whois Numbered Panda”, *Crowdstrike*, https://www.crowdstrike.com/en-us/blog/whois-numbered-panda/

# DEMO - ialabs

# Dynamic Resolution – What Next?

- Explore ways to get common ports from well-known IPs or URLs.
- Explore detection methods further.
- Examine ways to generate IP addresses (and see if valid reasons for this exist)
- Examine detection statistics for DGAs that reach out to the internet for sources compared with those that do not, such as word list or dictionary DGAs.