BACKDOORS TO THE KINGDOM:
CHANGING THE WAY YOU THINK ABOUT ORGANIZATIONAL RECONNAISSANCE

David Westcott
Security Principal
iDefense, Accenture security

SANS OSINT SUMMIT 2019
WHOAMI

David Westcott:

- Finder of things
- Attack surface aficionado
- Android RE
- OSINT/ HUMINT
- iDefense THOR TAA Team
AGENDA

• Why?
• Certificate Transparency (CT)
• Start of Authority (SOA)
• Sender Policy Framework (SPF)
• Border Gateway Protocol (BGP)
• Q/A
WHY?

- DNS Enumeration is **LOUD**
- GDPR **COMPLICATED** WHOIS
- The “Cloud” (aka: off-prem) is **MASSIVE**
CERTIFICATE
TRANSPARENCY
 Doesn’t capture (most) **self-signed**

- Visibility gap without **scan data**
- Supplementary data is needed to show where the certs are used
(CT) CAVEAT?

32,581,124 (Self-Signed)
26,109,510 (^ & Unexpired)

Source: shodan.io
CT CAVEAT?

238,694,349 (Unexpired, not Pre-Cert)
166,355,708 (Unexpired, Pre-cert)

13,642,992 not in CT logs, but in scans

Source: censys.io
(CT) TERMS

- **OID**: Object identifier
- **Pre-certificate**: OID 1.3.6.1.4.1.11129.2.4.3
  - AKA Certificate Poison AKA Pre-Cert
- **SCT**: Signed Certificate Timestamp
- **CRL**: Certificate Revocation List
- **AIA Path**: Authority Information Access Path
- **CN**: Common Name
- **SAN**: Subject Alternative Name
- **CA**: Certificate Authority
Operators:

- Google, Cloudflare, DigiCert, CNNIC, Sectigo (Comodo), Certly, Izenpe, WoSign, Venafi, StartCom, Wang Shengnan, GDCA, Beijing PuChuangSiDa Technology Ltd., NORDUnet, SHECA, Akamai, Matt Palmer, Let's Encrypt, Up In The Air Consulting
(CT) CONTENTS

- AIA/CRL Paths!
- IP Addresses
- Email Addresses
- Domains
- SANs
- Certificate Authorities
- Serial Numbers
- Issuers
- Fingerprint
- Pre-Cert!
AIA/CRL PATH

- Issuer AIA: CN, DC, LDAP String
- Issuer AIA =~ "ldap", Not Expired, Not Pre-Cert == ~444,000+
  - Source: Censys
Current CT entry count: ~2,924,366,030 (as of Feb. 12, 19)

- Google:

- Cloudflare:
  - Nimbus2018, 2019, 2020, 2021

~571 GB*
++: Email Addresses, Names, CAs, Internal Naming Syntax, IPs
(CT)
AND....ACTION!
(CT) GETTING STARTED

- Censys
- Binaryedge
- Shodan
- crt.sh (Sectigo)
- Google Transparency Report
- Facebook CT
- Axeman (Cali Dog Security; Ryan Sears)
- CertStream (Cali Dog Security; Ryan Sears)
- Rapid7 Open Data
- scans.io (Censys)
(SOA)

- MNAME (Primary Master NS)
- RNAME (Email Address)
- SERIAL
- REFRESH
- RETRY
- EXPIRE
- MINIMUM
- $TTL
(SOA) AND...ACTION!
SENDER POLICY FRAMEWORK
SPF

- ALL
- A
- IP4 -> ASN/pDNS/Certs -> Off-Prem, Friends, Providers
- IP6 -> ASN/pDNS/Certs -> Off-Prem, Friends, Providers
- MX -> ReverseMX -> Sibling Domain(s)
- PTR
- EXISTS
- INCLUDE -> Off-Prem, Friends, Providers
(SPF)
AND...ACTION!
BORDER GATEWAY PROTOCOL
(BGP) ASN/RANGES

bgpview.io (indexed by Google, has API)

rdap.arin.net/registry/entity/ID-ARIN (not indexed)
  • Name, Email, Address, Phone # (vcard)
  • Status of PoC (w/ dates)
BGP) CLIENTS

- RDAP (Registration Data Access Protocol)
  - nicinfo (client | Ruby)
  - DNSBelgium (client | Java)
  - CNNIC (client | Java)
  - CentralNIC “rdapper” (client | Perl)
(BGP)
AND...ACTION!

[REDACTED]