WHOIS: Privacy, Trust, and Public Interest

ICANN APAC-TWNIC Engagement Forum

Alban Kwan, Regional Director, East Asia

16 April, 2019



GDPR and the Expedited Policy Development Process (EPDP)

GDPR - The General Data Protection Regulation (GDPR) replaced the Data Protection Directive 95/46/EC .

- Became enforceable on May 25, 2018
- GDPR was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy
- GDPR in direct conflict with ICANN WHOIS Policy requiring public disclosure of contact data behind a domain registration
- ICANN issued a Temporary Specification regarding WHOIS and initiated an Expedited Policy Development Process (EPDP) to provide community more time to determine long-term WHOIS policy (collection, storage, display, transfer and access)

Expedited Policy Development Process (EPDP) and the Temporary Specification

- The Temporary Specification required significant redaction of the WHOIS Contact Data, eliminating access to name, email address, postal address and phone number
  - This has had significant impact on brand protection, efforts, as well security and fraud investigations

- One of the features of the Temporary Specification is that it is only effective for 1-year under ICANN rules, thus EPDP Team created to help develop new WHOIS consensus policy before expiration

- EPDP Team divided work into 2 Phases:
  - Phase 1 – collection/handling of WHOIS contact data and requests for WHOIS data
    - This is only part that MUST be completed within 1 year under EPDP
  - Phase 2 - access to WHOIS data by registrars, registries, ICANN and other 3rd parties
    - No defined date for completion of this work at this time

EPDP Status

EPDP Team issues Final Report on Phase 1 and GNSO approved Report on March 4, 2019.

- Report now out for Public Comment thru April 17th – see Report & Public Comment here
- ICANN Board expected to adopt 29 Recommendations in the Report after Public Comment period completes

Effort now underway to find chair for Phase 2 – team expected to commence work formally in May/June time frame, but preliminary discussions and planning already underway



EPDP Phase 1 Impact on WHOIS

- WHOIS Contact Data will dramatically change under EPDP Recommendations
- There will still be a public WHOIS data output available under EPDP Recommendations

Contact Data Element	Reccommended by EPDP Team
Reg Name	REDACTED BY DEFAULT/REGISTRAR MAY GIVE OPTION TO PUBLISH
Reg Org	REGISTRY OPTION/REGISTRAR RECONFIRMATION TO PUBLISH REQUIRED
Reg Street Address	REDACTED BY DEFAULT/REGISTRAR MAY GIVE OPTION TO PUBLISH
Reg City	REDACTED BY DEFAULT/REGISTRAR MAY GIVE OPTION TO PUBLISH
Reg State/Province	PUBLISHED
Reg Postal Code	REDACTED BY DEFAULT/REGISTRAR MAY GIVE OPTION TO PUBLISH
Reg Country	PUBLISHED
Reg Phone	REDACTED BY DEFAULT/REGISTRAR MAY GIVE OPTION TO PUBLISH
Reg Fax	REDACTED BY DEFAULT/REGISTRAR MAY GIVE OPTION TO PUBLISH
Reg Email	REDACTED/NO OPTION TO PUBLISH
Admin Name	DELETED/NO LONGER REQUIRED
Admin Org	DELETED/NO LONGER REQUIRED
Admin Street Address	DELETED/NO LONGER REQUIRED
Admin City	DELETED/NO LONGER REQUIRED
Admin State/Province	DELETED/NO LONGER REQUIRED
Admin Postal Code	DELETED/NO LONGER REQUIRED
Admin Country	DELETED/NO LONGER REQUIRED
Admin Phone	DELETED/NO LONGER REQUIRED
Admin Fax	DELETED/NO LONGER REQUIRED
Admin Email	DELETED/NO LONGER REQUIRED
Tech Name	REGISTRAR CHOICE/OPTION
Tech Org	DELETED/NO LONGER REQUIRED
Tech Street Address	DELETED/NO LONGER REQUIRED
Tech City	DELETED/NO LONGER REQUIRED
Tech State/Province	DELETED/NO LONGER REQUIRED
Tech Postal Code	DELETED/NO LONGER REQUIRED
Tech Country	DELETED/NO LONGER REQUIRED
Tech Phone	REGISTRAR CHOICE/OPTION
Tech Fax	DELETED/NO LONGER REQUIRED
Tech Email	REGISTRAR CHOICE/OPTION

IP & Security implications of diminished WHOIS access

VISIBILTY

With no immediate visibility of who owns or controls a domain it will become more difficult to identify and evaluate potential infringing or fraudulent domain name registrations.

AUDIT

Some customers may wish to advance their plans to identify and consolidate their portfolios of domains as historical methods of identification will likely be less useful or full of stale data.



DISPUTE

As visibility decreases there will more complexity & cost in dispute cases either through direct action or dispute channels.

OWNERSHIP

Now is the time to simplify domain ownership across your own portfolio by selecting generic contacts and addresses. Maintaining correct ownership details remains extremely important for SSL issuance & the next phase of the community work.

ICANN Security Alert



Search ICANN.org | Log In | Sign Up

ICANN | GET STARTED | NEWS & MEDIA | POLICY | PUBLIC COMMENT | RESOURCES | COMMUNITY | IANA STEWARDSHIP & ACCOUNTABILITY

Details

ICANN Announcements

15 Feb 2019

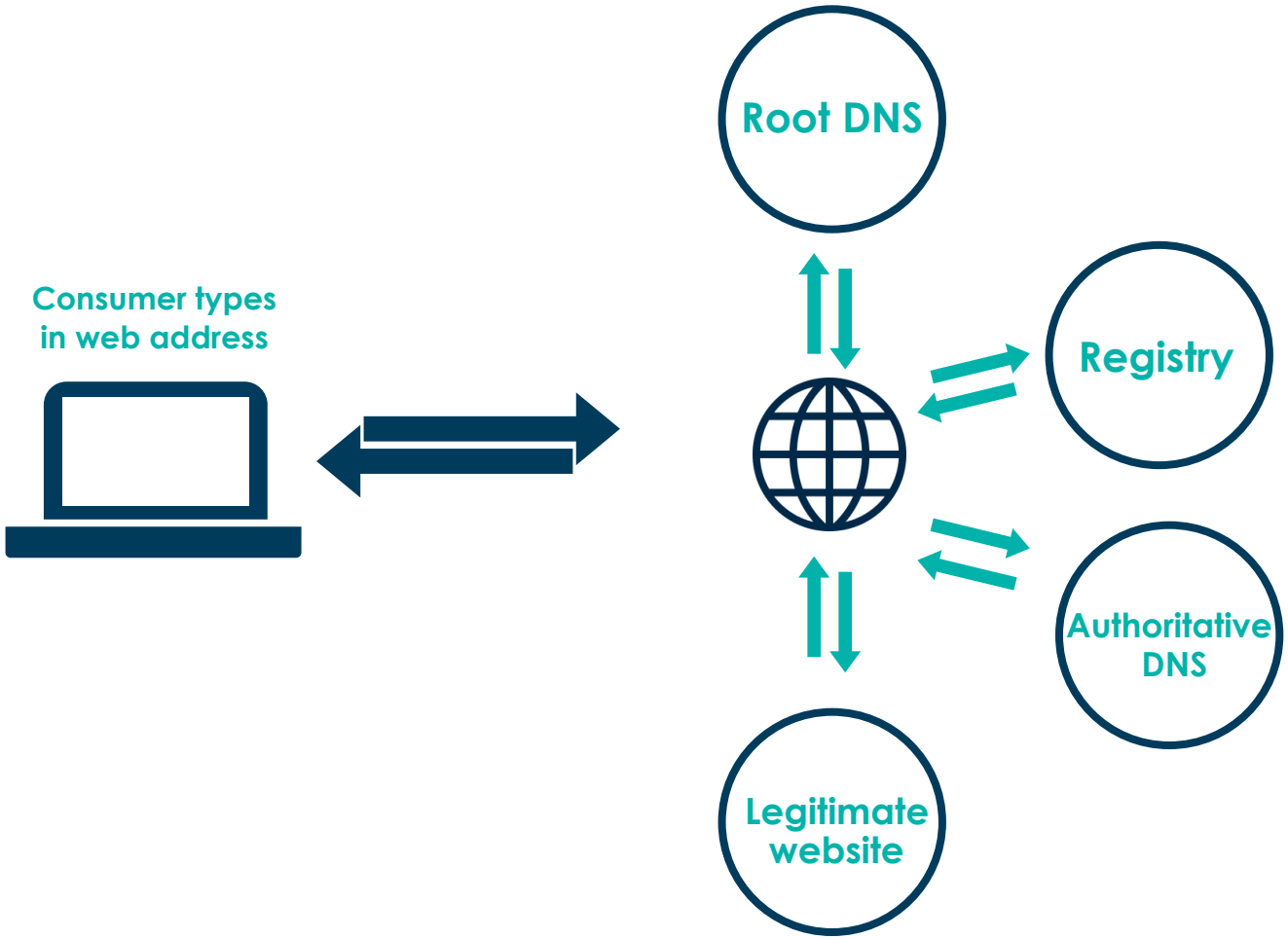
Alert Regarding Published Reports of Attacks on the Domain Name System

This page is available in: English | العربية | Español | Français | Русский | 中文

LOS ANGELES – 15 February 2019 – The Internet Corporation for Assigned Names and Numbers (ICANN) today announced that it is aware of several recent public reports regarding malicious activity targeting the Domain Name System (DNS). We have no indication that any ICANN organization systems have been compromised, and we are working with relevant community members to investigate reports of attacks against top-level domains (TLDs). For some reporting on this issue, please refer to these sources:

- United States Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA) Emergency Directive 19-01: "Mitigate DNS Internet Tampering", 22 January 2019.

How the DNS Works



CSC

DNS Hijacking



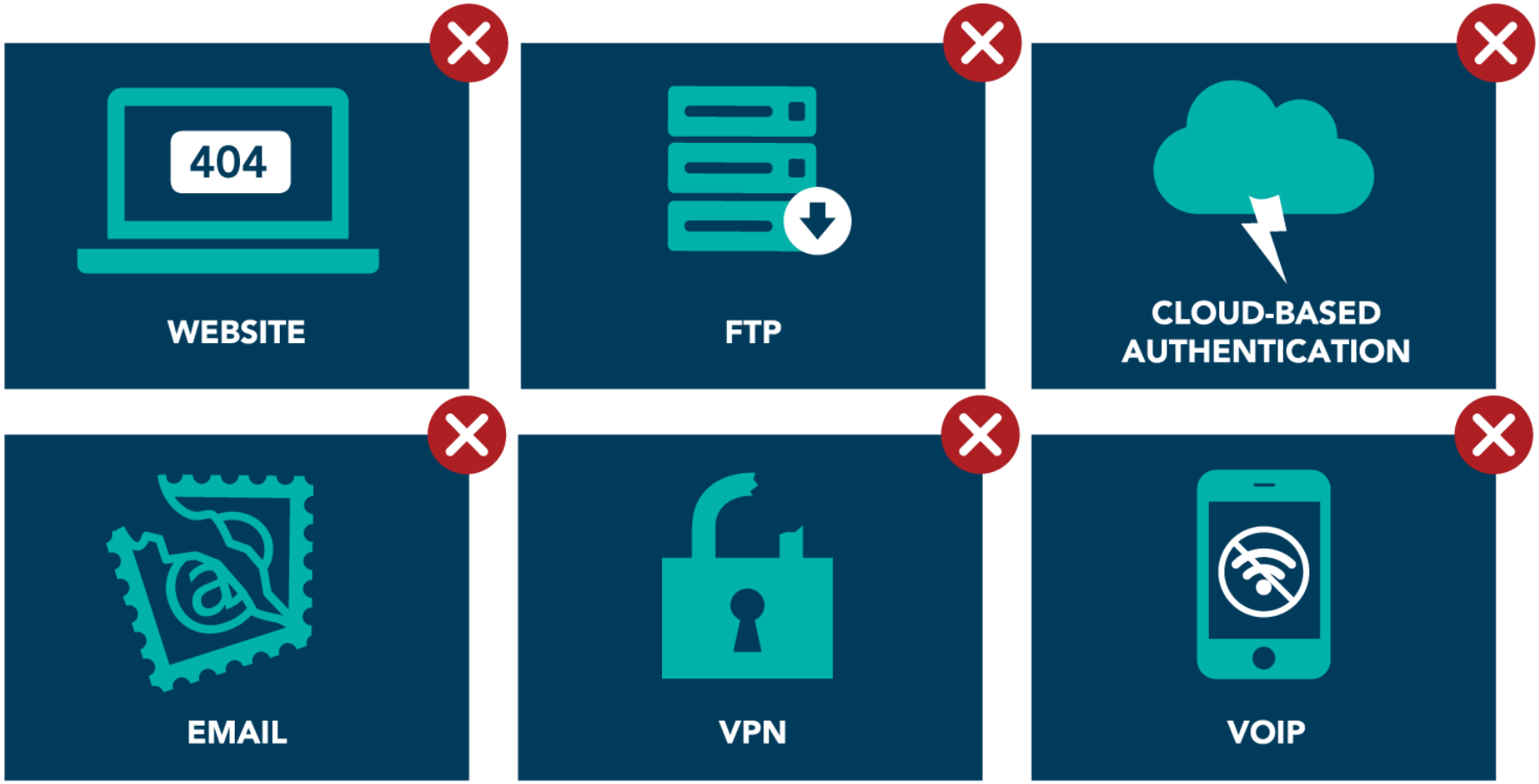


Cyber-criminal changes either:

- The domain name servers
- The zone file

CSC

What Happens When a Domain or DNS Fails?



CSC

CSC Resources



CSC

digital asset SECURITY CHECKLIST

DIGITAL ASSET *vendor management*

- You have a FULL accounting of all your domains, domain name systems (DNS), and secure sockets layer (SSL) providers.
- All your digital asset providers deliver enterprise-level support 24/7/365.
- All your digital asset providers have invested heavily in protecting their systems, e.g., ISO 27001 accredited data centers, SOC 2® compliant, third-party penetration, vulnerability testing, and security tests, including SQL injection and XSS, etc.
- All your digital asset providers have invested heavily in training their staff, e.g., security training, phishing awareness, including regular phishing email testing, two-factor authentication for outside network (remote) access, etc.
- All your digital asset providers have invested heavily in protecting their customers, e.g., IP validation, two-factor authentication, authorized contact policy, always in writing and never via phone (orders/requests), and federated identity, etc.
- None of your providers have a track record of succumbing to phishing, social engineering, DNS hijacking, or distributed denial of service (DDoS) attacks.
- All your digital asset providers primarily utilize their own accreditations rather than solely replying on third parties, e.g., your domain provider primarily utilizes their own accreditations directly with the registries and your certificate provider is an accredited Certificate Authority in their own right.

DOMAIN *management*

- You have a FULL accounting of your entire domain name portfolio.
- You have an auto-renewal policy in place with your providers that is supported by credit on account.
- All staff members are trained in, and adhering to, a centralized process for registering new domains.
- There are clear guidelines on the WHOIS template and user defined fields that must be provided at point of registration.
- You follow a procedure to identify company registrations that fall outside the centralized policy.

DNS *management*

- You have a FULL accounting of your entire DNS provider portfolio.
- You follow a procedure to identify domains not on enterprise-level DNS with a credible 100% uptime guarantee.
- All staff members are trained in, and adhering to, placing all new vital domains on enterprise-level DNS.

SSL *management*

- You have a FULL accounting of your SSL providers.
- All staff members are trained in, and adhering to, a centralized process for purchasing new and replacing old certificates.
- You follow a procedure to identify any SSL certificates purchased outside of your centralized policy.

VITAL (BUSINESS-CRITICAL) DOMAIN *management*

- You can immediately identify all vital domains and demonstrate they are secure.
- All DNS providers for your vital domains have a credible 100% uptime guarantee and co
- All vital domains use a su
- All vital domains are utili extensions to protect aga
- All vital domains are em DNS hijacking.
- All vital domains are emp

THREAT MIT *continued*

- You use additional DDoS servers beyond DNS.
- You use email authentica monitoring and takedow phishing attacks.

CSC Security Center enables your organization to protect your vital domains.



Understand security best practices with our checklist.

CSC