つぶらな瞳で考える、DNSSECの普及に必要な何かは何か？(DNS関連事例紹介)

JPCERTコーディネーションセンター
インシデント レスポンス グループ
中井尚子

JPCERT/CCとIRの紹介

- JPCERT/CCとは
  JaPan Computer Emergency Response Team Coordination Center
  - コンピュータセキュリティインシデントへの対応、国内外にセンサをおいたインターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
  - インシデント対応をはじめとする国際連携が必要なオペレーションや、情報連携に関する我が国の窓口となるCSIRT（窓口CSIRT）

    CSIRT: Computer Security Incident Response Team

    ※各国に同様の窓口となるCSIRTが存在する(米国のUS-CERT、CERT/CC、中国のCNCERT/CC, 韓国のKrCERT/CC 等)
  - 経済産業省からの委託事業として、サイバー攻撃等国際連携対応調整事業を実施
- インシデント レスポンス グループ(IR)とは
  - 国内・国外のセキュリティインシデント報告の受領・分析
  - 内容を理解し技術的な視点でコーディネーション

インシデント レスポンスの流れ

受付
- 第三者からの報告
- 当事者からの報告

調査
- 改ざんサイト、マルウエアサイトの調査
- 外部関連サイトの調査、情報収集

分析
- 証拠の確認(ログ分析、マルウエア分析)
- 状況把握

調整
- 適切な連絡先の特定
- 確認、対処依頼

インシデントレスポンスから見えるDNS

手段　サイバー攻撃の一手段

対象　インターネット利用者

影響　広範囲に影響を及ぼす

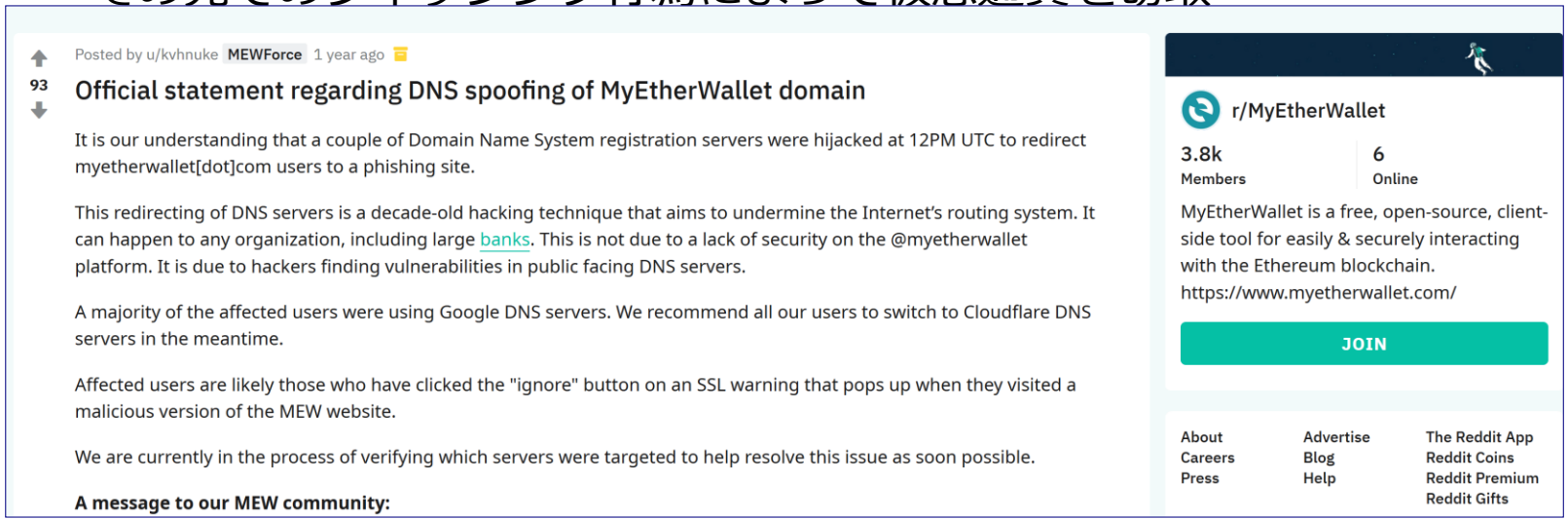
DNSSEC導入を考えるために…

1) DNSSEC未導入で被害にあったケース
~仮想通貨を狙った攻撃~

2) DNSSEC導入により被害を防いだケース
~DNSプロバイダを狙った攻撃~

1) 仮想通貨を狙った攻撃

- **仮想通貨を保管するサービス MyEtherWallet.com の権威DNSサーバが不正に建てられた**
  - 閲覧者を不正サイト(不正IPアドレス)に誘導
  - その先でのフィッシング行為によって仮想通貨を窃取



Posted by u/kvhnuke MEWForce 1 year ago

93

Official statement regarding DNS spoofing of MyEtherWallet domain

It is our understanding that a couple of Domain Name System registration servers were hijacked at 12PM UTC to redirect myetherwallet[dot]com users to a phishing site.

This redirecting of DNS servers is a decade-old hacking technique that aims to undermine the Internet's routing system. It can happen to any organization, including large banks. This is not due to a lack of security on the @myetherwallet platform. It is due to hackers finding vulnerabilities in public facing DNS servers.

A majority of the affected users were using Google DNS servers. We recommend all our users to switch to Cloudflare DNS servers in the meantime.

Affected users are likely those who have clicked the "ignore" button on an SSL warning that pops up when they visited a malicious version of the MEW website.

We are currently in the process of verifying which servers were targeted to help resolve this issue as soon possible.

A message to our MEW community:

r/MyEtherWallet

3.8k Members

6 Online

MyEtherWallet is a free, open-source, client-side tool for easily & securely interacting with the Ethereum blockchain.
https://www.myetherwallet.com/

JOIN

About Careers Press

Advertise Blog Help

The Reddit App Reddit Coins Reddit Premium Reddit Gifts

https://www.reddit.com/r/MyEtherWallet/comments/8eloo9/official_statement_regarding_dns_spoofing_of/ (出典元：Reddit Inc.)

インシデントの詳細

- 2018/4/24 UTC (約11:00 から13:00の2時間)
- 仮想通貨の窃取が目的のフィッシング攻撃
  1) BGP経路ハイジャックによりDNSクエリを偽権威DNSサーバに誘導
  2) 偽権威DNSサーバによってMyEtherWallet.com に対する悪意あるAレコードが返され偽サイトへ誘導

MyEtherWallet が行った対策

攻撃回避

- BGP経路ハイジャックは防げない

被害防止

- 正規な権威DNS応答であることの検証の環境

DNSSEC対応

- DNSSEC対応可能なプロバイダにドメイン移管

2）DNSプロバイダを狙った攻撃

- サイバー攻撃：Sea Turtle 活動の一環
- 攻撃期間： 2018年12月29日～ 2019年1月2日の数時間
- 攻撃対象：DNSプロバイダの内部IMAPサーバ

DNSSECのおかげで被害を防ぐことができた

自身のドメインにDNSSEC導入

DNSSEC検証リゾルバによる名前解決 (Public DNS)

サイバー攻撃：Sea Turtle

Sea Turtle の目的：国家情報、軍事関連情報の窃取

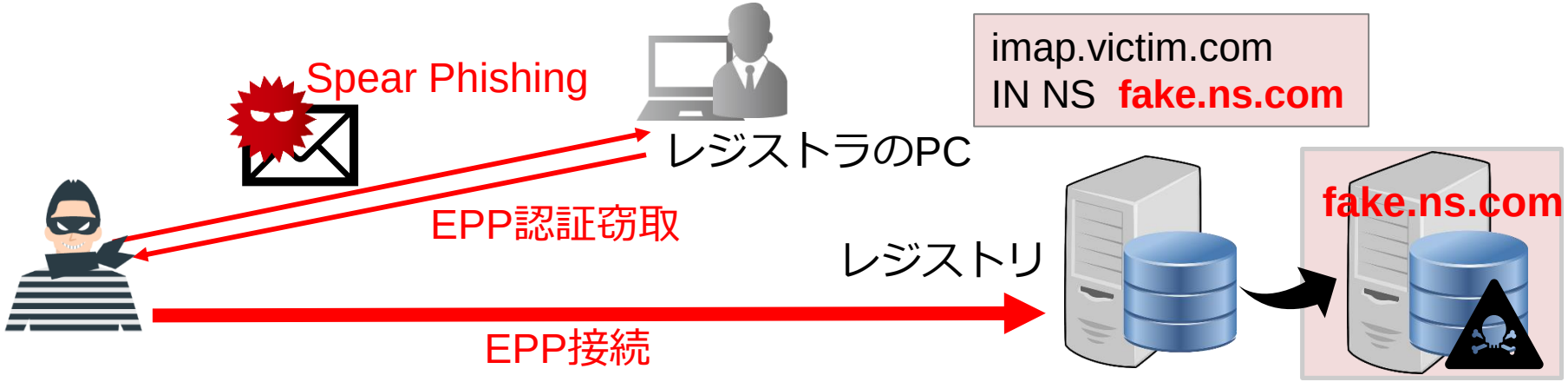
DNSプロバイダのネットワークに侵入しレコード改ざん

目的の情報にリーチするため潜伏し準備

標的DNSハイジャック

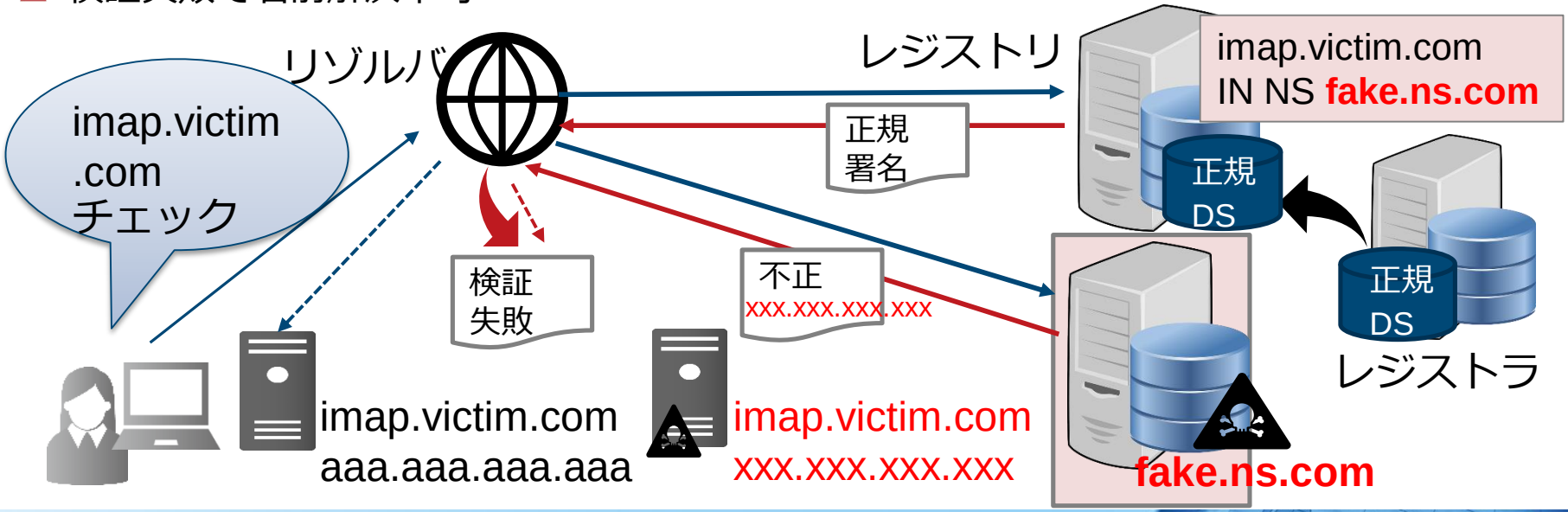
攻撃の準備：EPP経由でレジストリ台帳改ざん

- 攻撃者は Spear Phishing 攻撃によりEPP認証情報を窃取
  ※ EPP(Extensible Provisioning Protocol:レジストリデータの登録・更新のためのプロトコル)
- 窃取したEPP認証を使用し、レジストリの台帳に悪意あるNSレコードを登録、NSレコードは攻撃者が準備したDNSサーバを指名



攻撃の全貌：IMAPサーバを狙った攻撃

- 攻撃者はレジストリに偽のNSレコードを登録するが、DNSSEC導入済み対象ドメインのDSレコードの削除や改ざんはせず
  - DNSSEC仕組み理解不足の可能性
- 偽の権威DNSサーバが応答、正規署名なし
- 検証失敗で名前解決不可



まとめ

- 監視ツールではDNSの攻撃は気づけない
- 数時間の攻撃でも影響が大きい
- 被害に遭うのはインターネット利用者
- DNSSECはすべての攻撃は防げないが防御ゼロよりは良い
- 今、出来ることから始めませんか

参考情報

- Reddit/Official statement regarding DNS spoofing of MyEtherWallet domain
https://www.reddit.com/r/MyEtherWallet/comments/8eloo9/official_statement_regarding_dns_spoofing_of/

- Cisco/Talos
https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html
https://blog.talosintelligence.com/2019/04/seaturtle.html

- Fireeye
https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

- Ars Tech
https://arstechnica.com/information-technology/2019/01/multiple-us-gov-domains-hit-in-serious-dns-hijacking-wave-dhs-warns/
https://arstechnica.com/information-technology/2019/01/a-dns-hijacking-wave-is-targeting-companies-at-an-almost-unprecedented-scale

- Netnod
https://www.netnod.se/news/statement-on-man-in-the-middle-attack-against-netnod

- Packet Clearing House (PCH)
https://www.icann.org/en/system/files/files/11-woodcock-icann-2019-dns-imap-hijack-11may19-en.pdf

お問合せ、インシデント対応のご依頼は

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html

Thank you