Coincheck

ドメインハイジャック時のインシデント対応と外部機関との連携の重要性について

コインチェック株式会社
サイバーセキュリティ推進部長
喜屋武 慶大

全体像

Coincheck

1. 概要
2. 発覚までの経緯
3. 初動対応
4. ２日目以降の対応
5. 振り返り

自己紹介

Coincheck

喜屋武 慶大

コインチェック株式会社

サイバーセキュリティ推進部長

セキュリティベンダの SOC（Security Operation Center） でセキュリティアナリストとしてセキュリティ機器やサーバーのログからサイバー攻撃を分析する業務に従事。

2018年8月にコインチェック株式会社に転職。セキュリティ監視の設計、実装、運用及びサービスの設計、実装、運用のレビューなどを主にやりつつインシデント対応もやっていたりします。

1. 概要

Coincheck

2020年6月に発覚したコインチェック株式会社におけるドメイン名ハイジャックのインシデント時の対応についてお話します。

当社利用のドメイン登録サービスにおける不正アクセスについて（第一報）

2020.6.2

1. 概要

Coincheck

正しいNSレコード

ns-1515.awsdns-61.org
ns-1985.awsdns-56.co.uk
ns-650.awsdns-17.net
ns-405.awsdns-50.com

改竄後のNSレコード

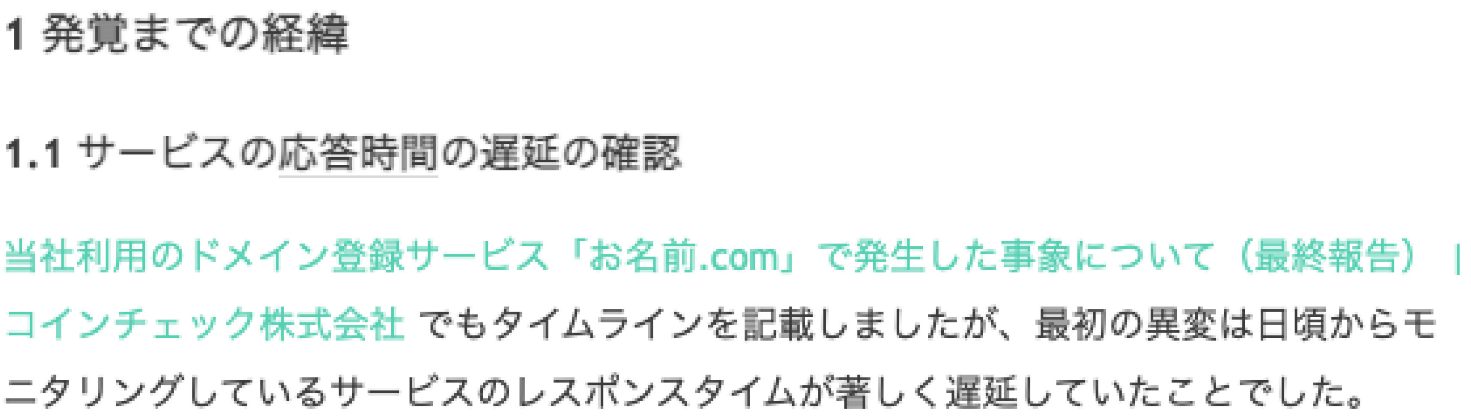
ns-1515.awsdns-061.org
ns-1985.awsdns-056.co.uk
ns-650.awsdns-017.net

Coincheck

2. 発覚の経緯について

2. 発覚までの経緯

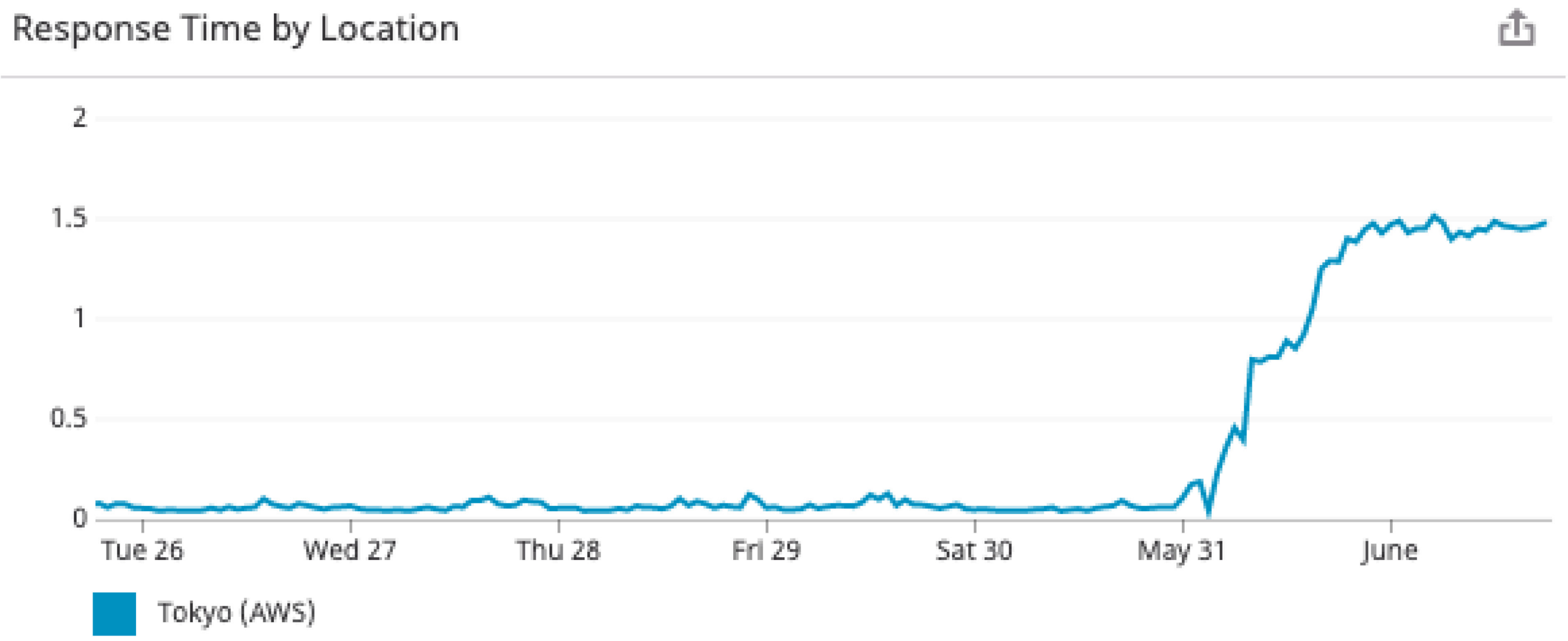
Blogの内容の振り返り



2. 発覚までの経緯

Coincheck

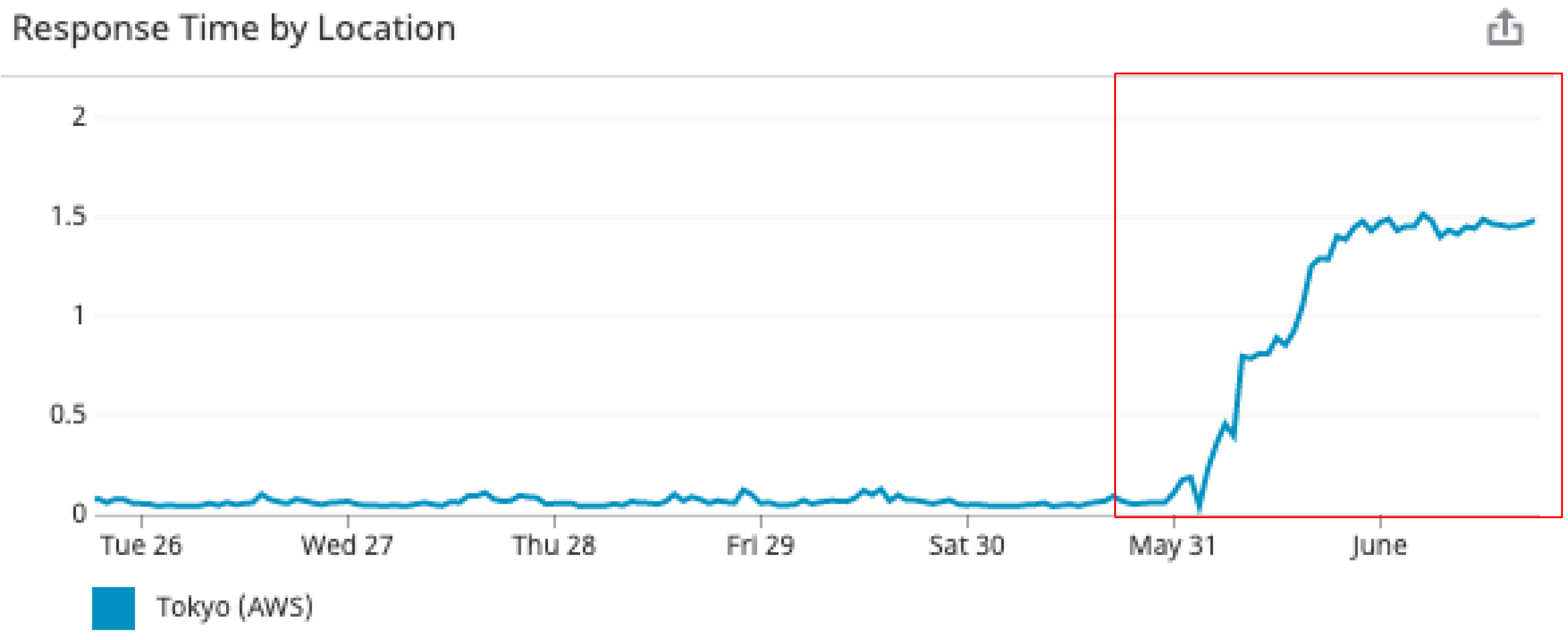
きっかけはレスポンスタイムの遅延から



2. 発覚までの経緯

Coincheck

きっかけはレスポンスタイムの遅延から



2. 発覚までの経緯

この時点では、ネームサーバーが書き換えられているなんて思いもしなかった

2. 発覚までの経緯

Coincheck

人によって遅延の有無が変わるため経路がおかしいのではと調査したところ何故かオランダを経由

```
[~]$ traceroute coincheck.com
traceroute to coincheck.com (*.*.*.*), 64 hops max, 52 byte packets
 1 *.*.*.* (*.*.*.*) 8.848 ms 1.440 ms 1.231 ms
 2 * * *
 3 *.jp (*.*.*.*) 39.671 ms 31.535 ms 48.041 ms
 4 *.jp (*.*.*.*) 49.228 ms 30.629 ms 40.791 ms
 5 *.jp (*.*.*.*) 39.525 ms 66.073 ms 32.224 ms
 6 * * *
 7 *.net (*.*.*.*) 349.044 ms 323.057 ms
   *.net (*.*.*.*) 347.276 ms
 8 *.net (*.*.*.*) 3.641 ms
   *.net (*.*.*.*) 49.727 ms
   *.net (*.*.*.*) 51.372 ms
 9 *.net (*.*.*.*) 151.669 ms 150.529 ms
   *.net (*.*.*.*) 204.721 ms
10 *.net (*.*.*.*) 209.535 ms
   *.net (*.*.*.*) 248.627 ms 150.673 ms
11 *.us.bb.gin.ntt.net (*.*.*.*) 213.621 ms
   *.us.bb.gin.ntt.net (*.*.*.*) 209.251 ms 212.087 ms
12 *.nl.bb.gin.ntt.net (*.*.*.*) 309.269 ms 312.889 ms 314.210 ms
13 *.nl.bb.gin.ntt.net (*.*.*.*) 306.177 ms 323.874 ms 306.553 ms
14 *.nl.bb.gin.ntt.net (*.*.*.*) 307.962 ms
   *.nl.bb.gin.ntt.net (*.*.*.*) 306.440 ms 295.733 ms
```

2. 発覚までの経緯

Coincheck

名前解決の結果を確認するとアムステルダムの CloudFront(AWS) の IP が返ってきている

```
[~]$ dig coincheck.com.

; <<>> DiG 9.10.6 <<>> coincheck.com.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53814
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;coincheck.com.                 IN      A

;; ANSWER SECTION:
coincheck.com.          286     IN      A   54.192.85.80

;; Query time: 162 msec
;; SERVER: *.*.*.*#53(*.*.*.*)
;; WHEN: Mon Jun 01 18:42:03 JST 2020
;; MSG SIZE  rcvd: 58
```

2. 発覚までの経緯

Coincheck

AWS のチケットを起票してサポートに調査を依頼
ここから AWS のサポートとのやりとりが始まる

発生している事象としてはレスポンスの遅延でいいですか？

直近でどういった変更を加えましたか？

DNS がおかしいというのはどういう点からですか？

2.発覚までの経緯

Coincheck

これ DNS 本当に正しいか確認してもらえますか？

これ AWS じゃないです、めちゃくちゃ怪しいですね

ネームサーバー改竄発覚

この後 AWS の方は終日対応に付き合ってくださいました

2.発覚までの経緯

Coincheck

WHOIS を確認するとなぜか 5月30日 15時11分(UTC) に更新されている

```
   Domain Name: COINCHECK.COM
   Registry Domain ID: 80933535_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.discount-domain.com
   Registrar URL:
   Updated Date: 2020-05-30T15:11:38Z
   Creation Date: 2001-12-10T11:05:42Z
   Registry Expiry Date: 2020-12-10T11:05:42Z
   Registrar:
   Registrar IANA
   Registrar Abuse Contact Email:
   Registrar Abuse Contact Phone:
   Domain Status: ok https://icann.org/epp#ok
   Name Server: NS-1515.AWSDNS-061.ORG
   Name Server: NS-1985.AWSDNS-056.CO.UK
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-06-01T11:10:35Z <<<
```

2.発覚までの経緯

Coincheck

正しいNSレコード

ns-1515.awsdns-61.org
ns-1985.awsdns-56.co.uk
ns-650.awsdns-17.net
ns-405.awsdns-50.com

改竄後のNSレコード

ns-1515.awsdns-061.org
ns-1985.awsdns-056.co.uk
ns-650.awsdns-017.net

3. 初動対応

3. 初動対応

Coincheck

レジストラのサポートにコンタクトを取る

From coincheck

Subject 不正利用の申告

To ドメインレジストラ

アカウントが乗っ取られて ネームサーバーが書き換えられました。

イメージです

約１時間２０分後に復旧

3. 初動対応

Coincheck

緊急事態対策本部設置

- まだアカウント乗っ取りの原因が不明
- 原因が不明なのでまた書き換えられるかもしれない
- 影響範囲も未知数
- ユーザーへの影響も無いとは言い切れない

3. 初動対応

Coincheck

変な MX レコードが登録されています

```
;; ANSWER SECTION:
coincheck.com.      33000   IN   SOA ns-1985.awsdns-056.co.uk. ns-
1515.awsdns-061.org. 2020050775 864000 72000 1209600 360000
coincheck.com.      360000  IN   NS   ns-1515.awsdns-061.org.
coincheck.com.      360000  IN   NS   ns-1985.awsdns-056.co.uk.
coincheck.com.      360000  IN   NS   ns-650.awsdns-017.net.
coincheck.com.      300 IN   A    54.192.85.80
coincheck.com.      60   IN   MX   5 mail.coincheck.com.
coincheck.com.      300 IN   TXT "atlassian-domain-
verification=tTCWNrSNtNaqGqVPgZWhLMryhgrJD+iSmpgHI61+3D1Qv/zqWlrXgHJRWYy
mh+KT"
coincheck.com.      300 IN   TXT "apple-domain-
verification=HYRwkB7d1bV30n6U"
coincheck.com.      300 IN   TXT "facebook-domain-
verification=la8geuy2tp70oh91bzf9qv80norcko"
coincheck.com.      300 IN   TXT "v=spf1 +include:servers.mcsv.net
+include:amazonses.com +include:_spf.google.com ~all"
coincheck.com.      300 IN   TXT "MS=ms23516971"
coincheck.com.      300 IN   TXT "google-site-
verification=9Vdf1PUnTUg7DQpW_amjVI_CLQAzBs4KpH58W1EBgew"

;; ADDITIONAL SECTION:
mail.coincheck.com. 300 IN   A    45.77.24.250
```

3. 初動対応

攻撃者はMX レコードを書き換えて何をしようとしたのか？

- TXT レコードが改竄されていた形跡はない
- つまり coincheck.com を送信元として偽のメールをばら撒こうとした訳ではない
- となると他には・・・

3. 初動対応

Coincheck

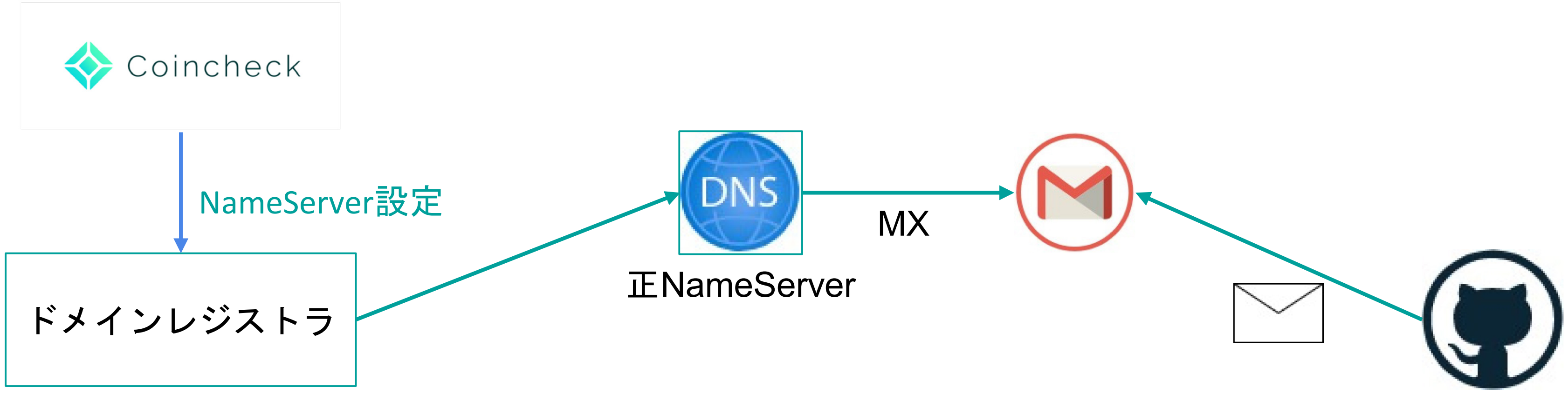
Yoshihiro Kyan 3ヶ月前
お疲れ様です、6月1日1時35分に[redacted]さんのメールアドレス宛に
`[GitHub] Please reset your password` というメールが届いている
かと思うのですがこちら心当たりありますでしょうか？
それとGitHubにログインできるかご確認いただき、一度パスワードを
違うものに再設定をお願いします。
@[redacted]

[redacted] 3ヶ月前
@Yoshihiro Kyan
了解しました、パスワードを変更します！
メールには心当たりがありません。。

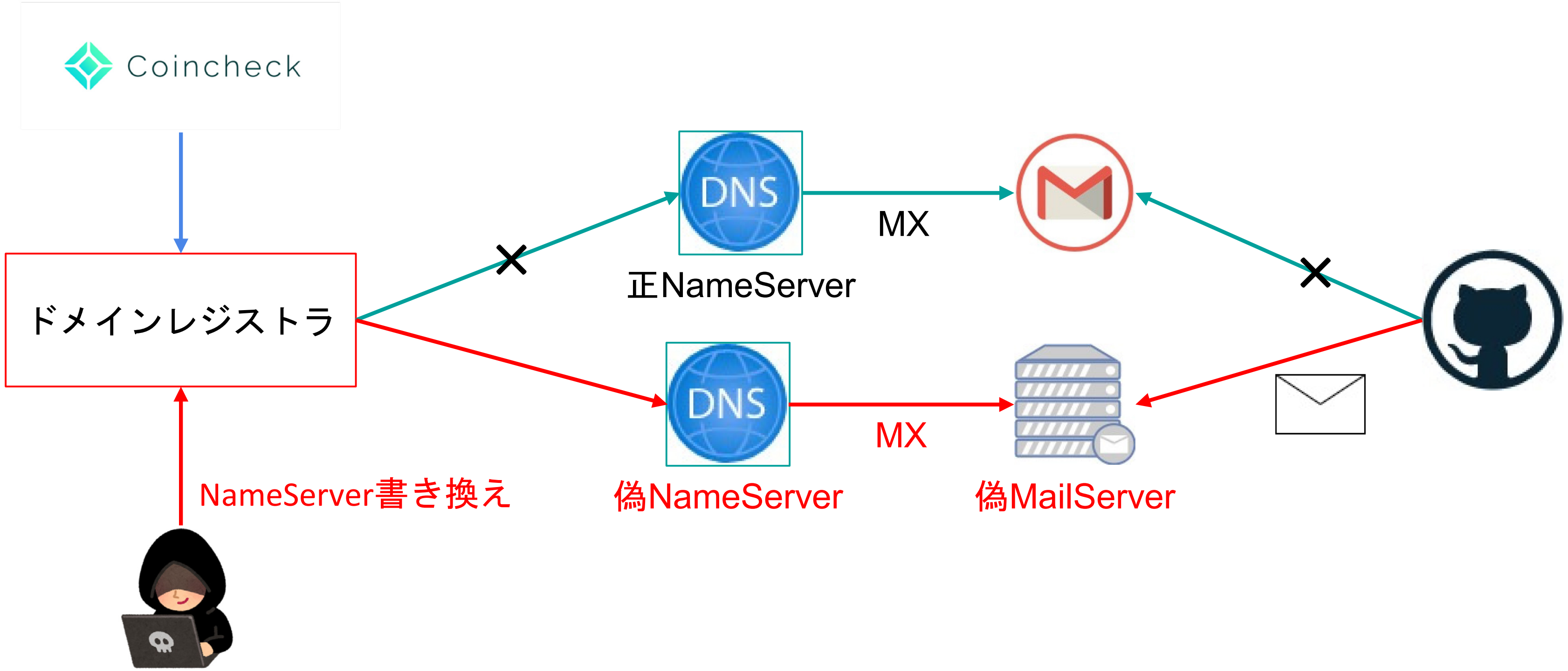
[redacted] 3ヶ月前
横からすみません、リセットメールはなかったのですが、自分も確認
してみたところ、攻撃者がリセットを試みようとした形跡がありまし
た。

[redacted] 3ヶ月前
横から失礼します
私のgithubアカウントにも同様の形跡があったため念のため共有致し
ます

攻撃の全体像



攻撃の全体像



Coincheck
ドメインレジストラ
DNS
正NameServer
MX
DNS
偽NameServer
MX
偽MailServer
NameServer書き換え

4. 2日目以降の対応

4. ２日目以降の対応

Coincheck

- 朝、昼、夕方に定期ミーティング実施
- その他必要に応じて臨時召集
- コロナ禍でリモートワーク状態だったので Zoom の常設部屋を設置
- 代わりに使用するドメインの策定、当局や関連団体への報告、関連作業や原因調査の進捗報告

会社全体として見ると２日目が一番忙しかった

4. ２日目以降の対応

Coincheck

指揮官（システム担当の執行役員）が Zoom に常駐

作業で詰まったこと、相談、緊急で報告が必要なことが発生した場合はとりあえずZoom に入って報告

4. ２日目以降の体制

Coincheck

２日目夜にプレスリリース第一弾発表

当社利用のドメイン登録サービスにおける不正アクセスについて（第一報）

2020.6.2

プレスリリースと同時に新しいアドレスへ問い合わせるよう案内を出さないと攻撃を受けたcoincheck.com宛にメールを出してしまうユーザーが出る可能性があったため、メールアドレスの設定変更作業が終わるのを待って発表

4. ２日目以降の体制

Coincheck

６月１日（月）
ドメイン名ハイジャック発覚及び復旧
緊急事態対策本部設置

６月２日（火）
メールアドレス変更作業実施
プレスリリース第一弾発表

６月３日（水）
ドメインレジストラより問題を修正した連絡を受ける

６月４日（木）
プレスリリース最終報発表
止めていた一部サービスを再開

Coincheck

5. 振り返り

5. 振り返り

我々が今回のインシデントの気づくことができたのはモニタリングをやっていたおかげ

5. 振り返り

Coincheck

モニタリング項目

- レスポンスタイム（サイト/API 間）
- リクエスト数
- 各サーバー毎のメモリとCPUの使用率
- エラー率
- トラフィック量
- Queue に溜まっている Job の数

etc...

モニタリングのおかげで今回のインシデントに気づけた

5. 振り返り

日本コンピュータセキュリティインシデント対応チーム協議会のサイトよりレジストラのCSIRTチーム連絡先を調べ、CSIRT にも協力を依頼

https://www.nca.gr.jp/member/index.html

5. 振り返り

レジストラの CSIRT にも連絡した結果として早急に対応してもらうことができた

5/31(日) 0:05 NSレコード書き換え

6/1(月) 19:10 NSレコード改竄発覚

6/1(月) 19:36 ドメインレジストラへ協力依頼

6/1(月) 20:52 NSレコード復旧

連絡を取ってから１時間半程で復旧と迅速に対応してもらえた

5. 振り返り

今回のような社外のシステム（SaaS等）が攻撃を受けてしまった場合にはサービスプロバイダーとの協力が必要になってくる

5. 振り返り

Coincheck → JPCERT/CC

テイクダウンの依頼

JPCERT/CC に不正なネームサーバー及びメールサーバーのテイクダウンを依頼

↓ コンタクト

偽NameServer　偽MailServer

6月2日0時ごろに依頼のメール

テイクダウンの依頼

ネームサーバーを書き換えられて不正なネームサーバを指すようになってしまったのでテイクダウンの依頼を出したいです。
MXもやられてるので返事は電話でお願いします。

5. 振り返り

Coincheck

翌朝に返事が来る

Coincheck

JPCERT CC

受信できました。

試しにメールを一通送ってみますので受信できるか確認をお願いします。

5. 振り返り

JPCERT/CC とのやりとり

Coincheck

改竄当時のNSレコードとMXレコードです。

```
coincheck.com. 315 IN NS ns-1985.awsdns-056.co.uk.
coincheck.com. 315 IN NS ns-650.awsdns-017.net.
coincheck.com. 315 IN NS ns-1515.awsdns-061.org.
coincheck.com.      60  IN  MX  5 mail.coincheck.com.
```

モニタリングでレスポンスの遅延を検知し、調査したところNSレコードの改竄に気付きました。

5. 振り返り

６月４日(木)

不正なネームサーバー

- ns-1515.awsdns-061.org
  - FQDN停止
- ns-1985.awsdns-056.co.uk
  - 名前解決不可
- ns-650.awsdns-017.net
  - 名前解決不可

5. 振り返り

Coincheck

JPCERT/CC さんよりテイクダウンに関するお話

最後に

- 各クラウドサービス事業者のインシデント時のサポート窓口の確認をしましょう

- 外部に不正なサーバーを設置されてしまった場合はJPCERT/CC さんを頼りましょう

- DNS はとても重要、皆さんも是非レジストラや権威サーバーに使っている DNS 関連サービスのアカウント管理やレコードの監視を実施しましょう！