ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●河川カメラに不正アクセス…攻撃の踏み台の可能性、被害は300台以上に

https://www.sankei.com/article/20230302-XGKIZ6F5JFPLVDMNGCYWW4S7RY/
https://www3.nhk.or.jp/kansai-news/20230303/2000071532.html
https://www3.nhk.or.jp/news/html/20230304/k10013998191000.html

このニュースをザックリ言うと･･･

- 3月2日(日本時間)以降、産経新聞やNHK等により、国土交通省近畿地方整備局等が設置した河川監視カメラが不正アクセスを受けている疑いがあると報じられています。

- 不正アクセスを受けたとされるのは、関西を中心とする2府6県に設置された河川監視カメラ261台で、1月中旬にこのうち199台について通常と異なる通信量が確認されたことから、問題がみられなかったものを含む261台について停止したとのことです。

- 中国・四国地方に設置した同様のカメラ約70台についても不具合の恐れから停止されており、被害の疑いがあるのは合わせて300台以上に上るとされています。

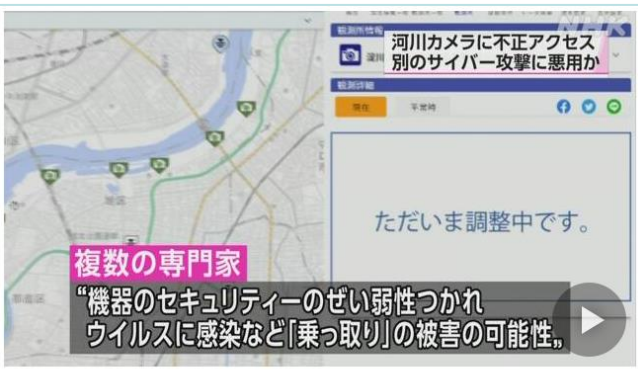
AUS便りからの所感等

- 被害を受けたカメラは、2020年度以降に設置が発表された「簡易型河川監視カメラ」とされ、インターネットを経由して国土交通省のWebサイトに定期的に静止画を提供しているものとされています(専用線を使うカメラについては影響は出ていないとのことです)。

- 2016年にはインターネットに接続する監視カメラを含む多数のIoT機器に感染してDDoSボットネットを構築したマルウェア「Mirai」が猛威を奮っており、また2021年3月には、群馬県で設置された同様のカメラにランサムウェアが感染し、カメラのIPアドレスや職員のメールアドレス情報等が流出した事案も発生しています(AUS便り 2021/03/22号参照)。

- カメラへの侵入経路は不明ですが、カメラを含むIoT機器のファームウェアが脆弱性を突かれることのないよう確実に更新を行うこと、管理機能等に外部の第三者が直接アクセスされたり、あるいは管理者がいる組織内ネットワークからマルウェアを介して侵入されたりしないようUTM等を用いた適切な隔離を行うこと、また管理機能にアクセスするためのパスワードについても第三者に安易に破られない複雑なものを設定すること、等の各種対策を確実にとることが肝要です。

NHK



河川カメラ不正アクセス 別のサイバー攻撃の踏み台に悪用か

2023年3月4日 5時32分　サイバー攻撃

国土交通省の河川カメラ、300台以上が不正アクセスを受けた疑いで運用を休止している問題で、複数の専門家はカメラが別のサイバー攻撃の踏み台として悪用された可能性を指摘しています。

これは、国土交通省近畿地方整備局が各地に設置している河川カメラのおよそ260台が外部から不正にアクセスされた疑いがあるもので、中国地方や四国などあわせておよそ70台にも不具合のおそれが見つかり、いずれも運用を休止しています。

● Chrome拡張機能「Get cookies.txt」にスパイウェア化指摘、Webアクセス情報を外部に送信する仕様に

https://forest.watch.impress.co.jp/docs/news/1482079.html
https://togetter.com/li/2090793

このニュースをザックリ言うと･･･

- 2月28日(日本時間)、あるTwitterユーザーより、Chromeブラウザー用拡張「Get cookies.txt」がスパイウェア的挙動を示しているとしてアンインストールを行うよう注意喚起が出されています。

- この拡張はブラウザーがアクセスしているWebサイトで使用されるCookieの情報を出力するためのものでしたが、サイトアクセス時のリクエスト情報(URLとリクエストヘッダー)を外部のサイトに送信する仕様となっていることが指摘されています。

- 3月7日現在、当該拡張はChromeウェブストアから削除されています。

AUS便りからの所感

- 少なくとも1月の時点でスパイウェア化の指摘が海外フォーラムに投稿され、Googleにも複数の報告がありましたが、3月に入った時点でしばらくはインストールが可能な状態でした。

- この挙動については拡張機能のプライバシーポリシーに明記されており、拡張の開発ルールの改訂に伴う変更であるという開発者の主張もあったとされる一方、外部に情報を送信しない安全な挙動をとる代替拡張もリリースされています。

- Chrome拡張はマルウェアがPCに侵入するために使われる典型的な侵入経路の一つともされ(AUS便り 2022/10/18号参照)、インストールにより、理論上Webブラウザーのあらゆる機能を拡張機能に許可することになります(前述した開発ルールの改定は拡張が使用できる機能を制限する意味合いもあります)ので、必要最低限の拡張機能のみインストール・有効化すること、身に覚えのない拡張機能が入っていたり、有効にしている拡張についてSNS等で問題が報告された場合は速やかに無効化・アンインストールすることを心掛けてください。

Impress Watch

Googleの「おすすめ」バッジ付きChrome拡張がマルウェアに、ユーザー情報が外へダダ漏れ

「Get cookies.txt」は今すぐアンインストールを

樽井 秀人　2023年2月28日 17:13

「Google Chrome」用の拡張機能「Get cookies.txt」が、ユーザー情報を無断で外部サーバーへ送信しているようだ。編集部でも、デバイスの情報やCookieなどがPOST送信されていることを確認しており、警戒が必要だ。

● 2月フィッシング報告件数は59,044件…昨年の水準に戻る可能性

https://www.antiphishing.jp/report/monthly/202302.html

このニュースをザックリ言うと･･･

- 3月6日(日本時間)、フィッシング対策協議会より、2月に寄せられたフィッシング報告状況が発表されました。

- 2月度の報告件数は59,044件で、1月度(https://www.antiphishing.jp/report/monthly/202301.html)の38,269件から20,775件増加しています。

- フィッシングサイトのURL件数は9,994件で1月度(7,704件)から2,290件増加、フィッシングに悪用されたブランド数は89件で1月度(76件)から13件増加となっています。

- フィッシングサイトで使用されるTLD(トップレベルドメイン)の割合は、.lyが約28.9%でトップ、次いで.com(約24.5%)、.top(約15.0%)、以下 .cn、.orgが上位に挙げられています。

- Amazonを騙るフィッシングは全体の約28.0%と割合は減少(1月度44.6%)、以下イオンカード・ヤマト運輸・ソニー銀行・セゾンカード・ETC利用照会サービス・えきねっとを騙るものと合わせて全体の約74.5%を占めたとのことです。

AUS便りからの所感

- 同協議会の調査用メールアドレスへ配信されたフィッシングメールの約85.9%が中国の通信事業者からの配信とされ、他にもアメリカの大手クラウドサービス、日本国内のホスティング事業者からの配信も多く確認されているとしています。

- 同協議会では1月度の報告件数減少を旧正月だったためと分析しており、一貫して6万件台以上を維持してきた2022年の水準に戻る可能性は十分に考えられます。

- フィッシングメールやスパムメールを排除するための機構として既に採用が広く進んでいるSPFについて、自組織からのメール配信に外部サービスを利用することに伴いDNSレコードにエントリーを追加した結果、DNS参照回数制限を超過したり、include先がなくなったりしてエラーが発生するケースが散見されているとしており、SPFが正常に機能するため、エントリーのチェック・監視を行うことは重要です。

フィッシング対策協議会
Council of Anti-Phishing Japan