サイバー攻撃
新たなサイバー脅威に関する考察

Cyber attacks

A few thoughts about emerging cyber threat

JCC Seminar @ KPMG HU

15th May 2024

自己紹介

Kamilló Matek
シニアマネージャー
サイバー研究室長

Kamilló has more than 10 years professional experience in IT Development and in IT Security. He worked as a Lead Software developer and as a Software Architect in Germany and Hungary.

He has participated in several penetration tests and security audits mainly in the financial sector. He has also conducted internal and external penetration testing and ethical hacking assessments for multinational companies and for government related organizations.

Kamilló has broad experience in leading and conducting technical and IT security related assessments, including the following:

- Fat/thin client tests
- Network application tests
- Web application tests
- Wi-Fi network tests
- Operating system related tests
- Database level tests
- Mobile Application tests
- Source code reviews
- Exploit development
- Reverse Engineering

学歴および資格:

- OSWE, Offensive Security Web Expert (2021)
- OSCP, Offensive Security Certified Professional (2020)
- OSWP, Offensive Security Wireless Professional (2019)
- Kürt Certified Ethical Hacker, KCEH, Cyber Institute, 2018
- ELTE, Program Designer E specialization, BA Degree, 2012

主な専門性・スキル:

- Cyber security testing
- Ethical hacking
- Source Code Reviews
- System Programming
- Exploit Development in various programming languages
- Penetration tests
- TCP/IP, network security protocols
- Programming and scripting languages
- Experience in application design and application development
- Auditing security processes, architectures, guidelines, policies and procedures for organizations
- Assessment of several different computer system

CVEの発行実績:

- CVE-2022-29402
- CVE-2021-46122
- CVE-2021-41653
- CVE-2021-36697
- CVE-2021-36698
- CVE-2021-34075
- CVE-2021-35501
- CVE-2021-34074
- CVE-2020-8497
- CVE-2020-7935
- CVE-2020-8511
- CVE-2020-8500
- CVE-2019-20050
- CVE-2019-19968
- CVE-2019-19681

+ 2

- Forcepoint DLP One – Hidden Python Console – Initial access
- Microsoft Autopilot Shift F10 bypass and Privesc

https://k4m1ll0.com

Who am I?

Kamilló Matek

Senior Manager, Head of Cyber Lab

Kamilló has more than 10 years professional experience in IT Development and in IT Security. He worked as a Lead Software developer and as a Software Architect in Germany and Hungary.

He has participated in several penetration tests and security audits mainly in the financial sector. He has also conducted internal and external penetration testing and ethical hacking assessments for multinational companies and for government related organizations.

Kamilló has broad experience in leading and conducting technical and IT security related assessments, including the following:

- Fat/thin client tests
- Network application tests
- Web application tests
- Wi-Fi network tests
- Operating system related tests
- Database level tests
- Mobile Application tests
- Source code reviews
- Exploit development
- Reverse Engineering

Education and qualifications:

- OSWE, Offensive Security Web Expert (2021)
- OSCP, Offensive Security Certified Professional (2020)
- OSWP, Offensive Security Wireless Professional (2019)
- Kürt Certified Ethical Hacker, KCEH, Cyber Institute, 2018
- ELTE, Program Designer E specialization, BA Degree, 2012

Key skills:

- Cyber security testing
- Ethical hacking
- Source Code Reviews
- System Programming
- Exploit Development in various programming languages
- Penetration tests
- TCP/IP, network security protocols
- Programming and scripting languages
- Experience in application design and application development
- Auditing security processes, architectures, guidelines, policies and procedures for organizations
- Assessment of several different computer system

Kamilló published the following CVEs:

- CVE-2022-29402
- CVE-2021-46122
- CVE-2021-41653
- CVE-2021-36697
- CVE-2021-36698
- CVE-2021-34075
- CVE-2021-35501
- CVE-2021-34074
- CVE-2020-8497
- CVE-2020-7935
- CVE-2020-8511
- CVE-2020-8500
- CVE-2019-20050
- CVE-2019-19968
- CVE-2019-19681

+ 2

- Forcepoint DLP One – Hidden Python Console – Initial access
- Microsoft Autopilot Shift F10 bypass and Privesc

https://k4m1ll0.com

サイバー攻撃の被害者

01

個人及び組織

- ソーシャルメディアのアカウント：フェイスブック、エックス、インスタグラム、ティックトックなど
- 家庭のコンピューターやネットワーク
- オンラインショッピング
- コロナ禍以降の在宅勤務（在宅勤務とオフィス勤務の垣根がなくなっている。）

など

02

企業

- 業界:
  - ➢ ゲーム制作、テクノロジー、製薬、自動車など
- 会社の規模:
  - ➢ 中小規模企業、大企業、巨大企業
- サイバーセキュリティ対策の予算規模
- **サープライチェーンへの攻撃**

03

国家

- 重要なインフラ:
  - 送電グリッド、輸送インフラなど
- 政治的メッセージ

Cyber victims everywhere...

01

Individuals and Groups

- Social media accounts: Facebook, X, Instagram, TikTok and more social media accounts
- Home computers, and home networks
- Webshop accounts, online Stores
- Covid and Home Office – the border between the home and the corporate environment is not clear anymore.
- Etc.

02

Companies

- Different industries:
  - Gaming, Technology, Pharmaceutical, **Automotive**, etc.
- Different sized companies:
  - small, middle, big and giant companies
- Different budgets
- **Supply Chain Attacks**

03

National-level cyber attacks

- Critical infrastructure:
  - Power grid, transportation infrastructure, etc.
- Political messaging (hacktivists, environmentalists)

攻撃の理由・背景

01 金銭

多くのサイバー犯罪者が既に、フィシング、ランサムウェア、銀行詐欺等により、金銭を得ている。

02 政治的・イデオロギー上の動機

国あるいは組織が、目的達成のために、サイバーツールを活用している。（政治的な扇動やイデオロギー闘争など）

03 データ・情報の窃取、スパイ活動

センシティブ情報、営業機密、政府文書などがターゲットとなり、企業や政府機関が攻撃を受けている。

04 愉快犯罪、名声

世間を騒がせて楽しむ。ハッキングコミュニテーの中での名声を得る。

05 ウィルスやマルウェアの配布

インターネットシステムを混乱あるいはコントロールするようにデザインされたウィルスやマルウェア—の配布のために攻撃者に利用される。

06 サイバーセキュリティ上の弱点の活用

不正なアクセスや損害を与えるために、ソフトウェアやインフラのセキュリティ上の不備を攻撃者に利用される。

07 | その他: 個人的な理由

The possible reasons behind the attacks

01 Financial gain

Many cybercriminals have already made money through attacks such as phishing, ransomware, or bank fraud.

02 Political or ideological motives

States or groups use cyber tools to achieve their goals, including political influence or ideological warfare.

03 Data theft and espionage

Companies or governments target sensitive information, such as trade secrets or government documents.

04 Fun and fame

Some hackers attack just to challenge themselves or gain fame in the hacking community.

05 Cyberspace Distribution

The distribution of viruses and malware designed to disrupt or control Internet systems.

06 Exploiting Cybersecurity Weaknesses

Exploiting security holes in infrastructure or software to gain unauthorized access or cause damage

07 | Other: Personal reasons

What about the automotive industry?

- 金銭支払い能力がある。
- 複雑な IT および運用・制御システム
- ECUレベルまですべてが接続している
- 複雑なサプライヤーシステム
- 古いテクノロジー

What about the automotive industry?

- Perfect targets with notable profit.
- Complex IT and OT systems.
- Everything is connected.
  (ECU level – Flash Over The Air)
- Complex supplier systems.
- Older technologies.

サイバー攻撃の事例

© 2024 KPMG Advisory Ltd., a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

A few examples

© 2024 KPMG Advisory Ltd., a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

セイコー

セイコーは、顧客のセンシティブ情報がランサムウェアの攻撃にさらされたことを発表

2023年7月28日に会社の一部のサーバに対し、第三者による不正アクセスを受けたことを確認した。後に本攻撃はランサムウェアによる攻撃であることが判明した。即座に対策本部を設置し、外部専門家の支援の下、全サーバーの検査を実施するとともに、被害の全容や影響範囲の確認、原因の究明を進めた。また、個人情報保護委員会および警視庁への報告を実施した。

会社および外部専門家による包括的な調査の結果、セイコーグループ株式会社、セイコーウォッチ株式会社、セイコーインスツルメンツ株式会社が保有している約60,000に上る個人情報が危険にさらされたことが確認された。

会社は一時的に影響を受けたサーバーと外部の通信を遮断し、承認されないアクセスを検知するためにEDR (Endpoint Detection and Response) システムを全サーバー、PCにインストールした。会社は多要素認証の導入など、再発防止への措置をとった。

https://therecord.media/seiko-ransomware-attack-leaked-60000-pieces-of-data

WORLD ATHLETICS CHAMPIONSHIPS BUDAPEST 23

SEIKO
OFFICIAL TIMER

Seiko

Seiko says ransomware attack exposed sensitive customer data

On July 28, 2023, we detected unauthorized access to some of our servers, which later turned into a ransomware attack. We immediately started an emergency inspection of all our servers and sought assistance from cyber security experts. We initiated an investigation to clarify the extent of the breach, established an emergency response team to limit the damage, and initiated a clean system restoration. We also reported the incident to the Personal Information Protection Committee and the Tokyo Metropolitan Police.

Following a comprehensive review by both the Company and cybersecurity experts, we confirmed that a total of approximately 60,000 items of personal data held by Seiko Group Corporation (SGC), Seiko Watch Corporation (SWC), and Seiko Instruments Inc. (SII) were compromised.

As part of our ongoing response, we temporarily blocked external communication with the affected servers and have installed EDR (Endpoint Detection and Response) systems on all servers and PCs to detect unauthorized activity. We have also implemented measures such as multi-factor authentication to prevent further breaches.

https://therecord.media/seiko-ransomware-attack-leaked-60000-pieces-of-data

WORLD ATHLETICS CHAMPIONSHIPS BUDAPEST 23

SEIKO
OFFICIAL TIMER

フォルクスワーゲン

中国のハッカーによるフォルクスワーゲンのシステムへの複数年に渡る侵入

攻撃者はドイツ自動車巨大企業フォルクスワーゲンに対して少なくとも5年間にわたり侵入に成功していたとZDF（ドイツのテレビ局）が報じた。

ジャーナリストが閲覧した内部文書によると、2010年から2015年にかけて、悪意のある者が同社のシステムに侵入し、数回にわたり、知的財産を盗み出したとのこと。

攻撃者は、ガソリンエンジン、トランスミッション、デュアルクラッチトランスミッションの研究・開発また、電気自動車の研究に関する情報窃取に注力した。

報告によると少なくとも19,000点の文書が窃取された。同社の情報セキュリティーチームは窃取された文書を復元することに成功したが、実際にはさらに申告な攻撃が行われていた可能性を示唆する証跡があった。

専門家によると攻撃者のIPアドレス、使用されたソフトウェア、ハッキングが試みられた時間帯などを総合すると、ハッキングが組織された場所は中国である可能性がある。

https://cybernews.com/news/volkswagen-breach-china-hackers/

Volkswagen

Multi-year Volkswagen breach points to Chinese hackers

Attackers successfully targeted the German automotive giant Volkswagen, for at least five years, ZDF reports. Internal documents seen by journalists show that between 2010 and 2015, malicious actors infiltrated Volkswagen's systems, exfiltrating intellectual property several times over the period.

Attackers mostly focused on the company's development of gasoline engines, transmission development, and dual-clutch transmission research. Additionally, attackers focused a lot of effort on Volkswagen's electric vehicle research.

According to the German report, at least 19,000 documents were stolen from the automaker. The company's security team successfully recovered files exfiltrated from Volkswagen, which means that the true extent of the attack could be more significant.

Experts to whom journalists discussed the hack mention that attackers' IP addresses, the software they used, and the time zone they operate in point to the hack originating from China.

Volkswagen Group is one of the world's largest automakers, with last year's revenue exceeding $322 billion and employees over 667,000. The group's brands include Audi, Lamborghini, MAN, Porsche, Skoda, Bentley, and others.

https://cybernews.com/news/volkswagen-breach-china-hackers/

トヨタ

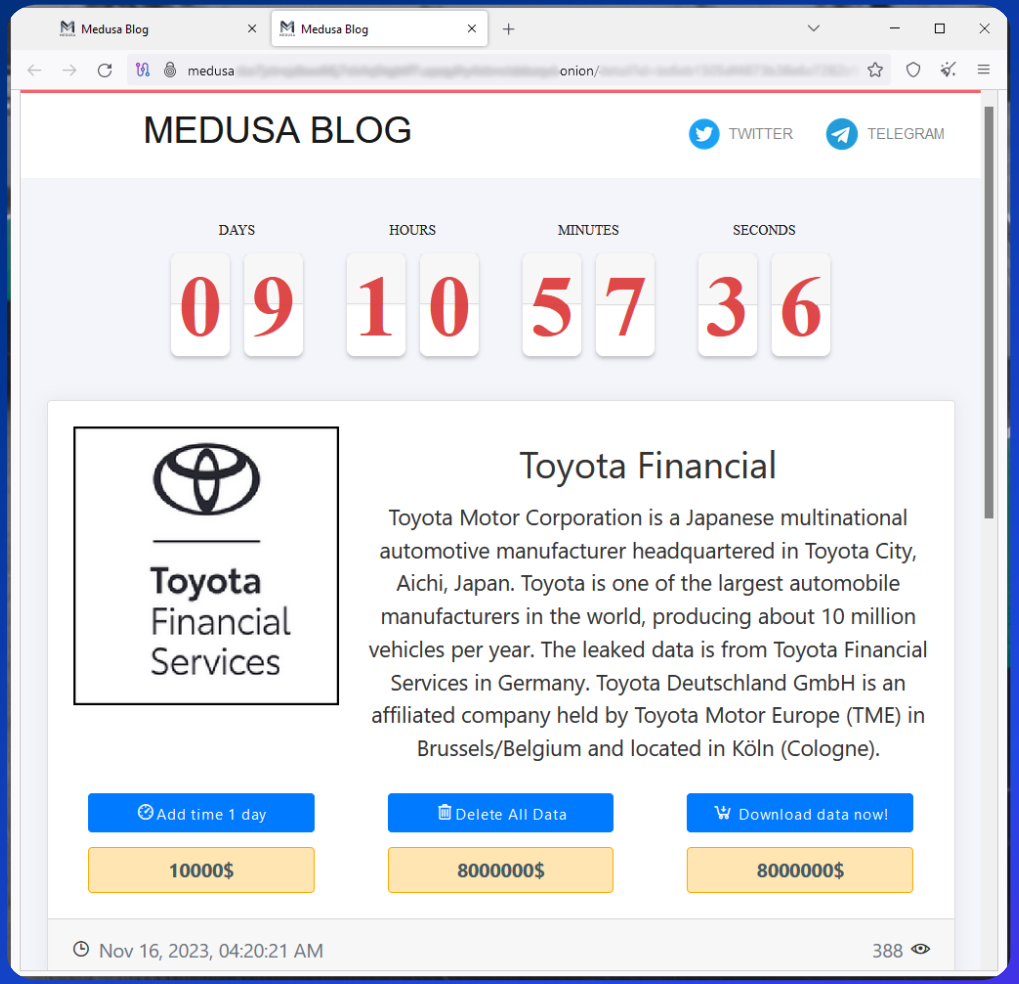
ランサムウェアのメドゥーサが欧州、アフリカのトヨタファイナンスサービスに攻撃を仕掛け、800万ドルの身代金を要求

トヨタファイナンシャルサービスは、ランサムウェアのメドゥーサが身代金を要求した後、同社のシステムが不正なアクセスを受けたことを確認した。

トヨタファイナンシャルサービスは、トヨタ自動車が販売する市場において、同社関連の自動車金融の90%を担う重要子会社。

メドゥーサランサムフェアの犯罪組織は、同組織のダークウェブサイトに、窃取したとするデータの削除に対して、トヨタファイナンシャルサービスに800万ドルの身代金を要求すると掲載した。

脅迫者は、10日以内の支払いを要求しており、1日遅延するごとに追加で1万ドルを要求するとしている。



Toyota

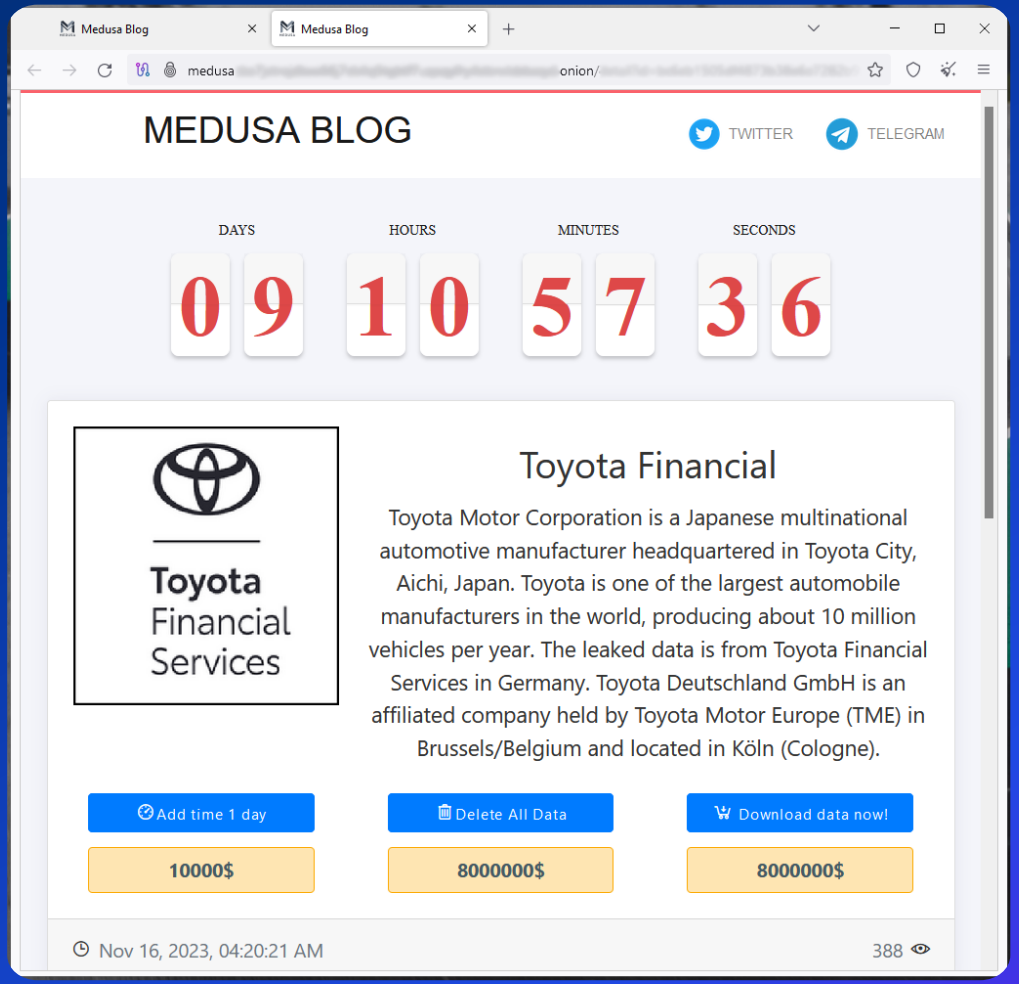
Medusa Ransomware Targets Toyota Financial Services in Europe and Africa, Demands $8 Million Ransom

Toyota Financial Services (TFS) has confirmed that it detected unauthorized access on some of its systems in Europe and Africa after Medusa ransomware claimed an attack on the company.

Toyota Financial Services, a subsidiary of Toyota Motor Corporation, is a global entity with a presence in 90% of the markets where Toyota sells its cars, providing auto financing to its customers.

Earlier today, the Medusa ransomware gang listed TFS to its data leak site on the dark web, demanding a payment of $8,000,000 to delete data allegedly stolen from the Japanese company.

The threat actors gave Toyota 10 days to respond, with the option to extend the deadline for $10,000 per day



自動車会社

自動車会社は、ウェブ上の脆弱性にさらされている

調査によると自動車会社の異なる多くのシステムにおける脆弱性が指摘されている。例えばBMWとロールスロイスのウェブポータルでワンタイムパスワードを生成するためのAPIエンドポイントの設定の脆弱性により従業員あるいは取引業者等のアカウント、さらには、センシティブな顧客や車両情報へのアクセスを許す可能性が指摘されている。

メルセデスベンツのシングルサインオンシステムの設定不備は、調査員による個人のギットハブや内部コミュニケーションツール等のいくつかの情報へのアクセスが可能であった。

攻撃者は従業員になりすますことで、センシティブ情報にアクセスしたり、顧客の車両に対して指令を送ったり、RCE 攻撃を実施したり、同社のインフラにおいてソーシャルエンジニアリングを試みたりすることができる。

https://portswigger.net/daily-swig/car-companies-massively-exposed-to-web-vulnerabilities/volkswagen-breach-china-hackers/

Car companies

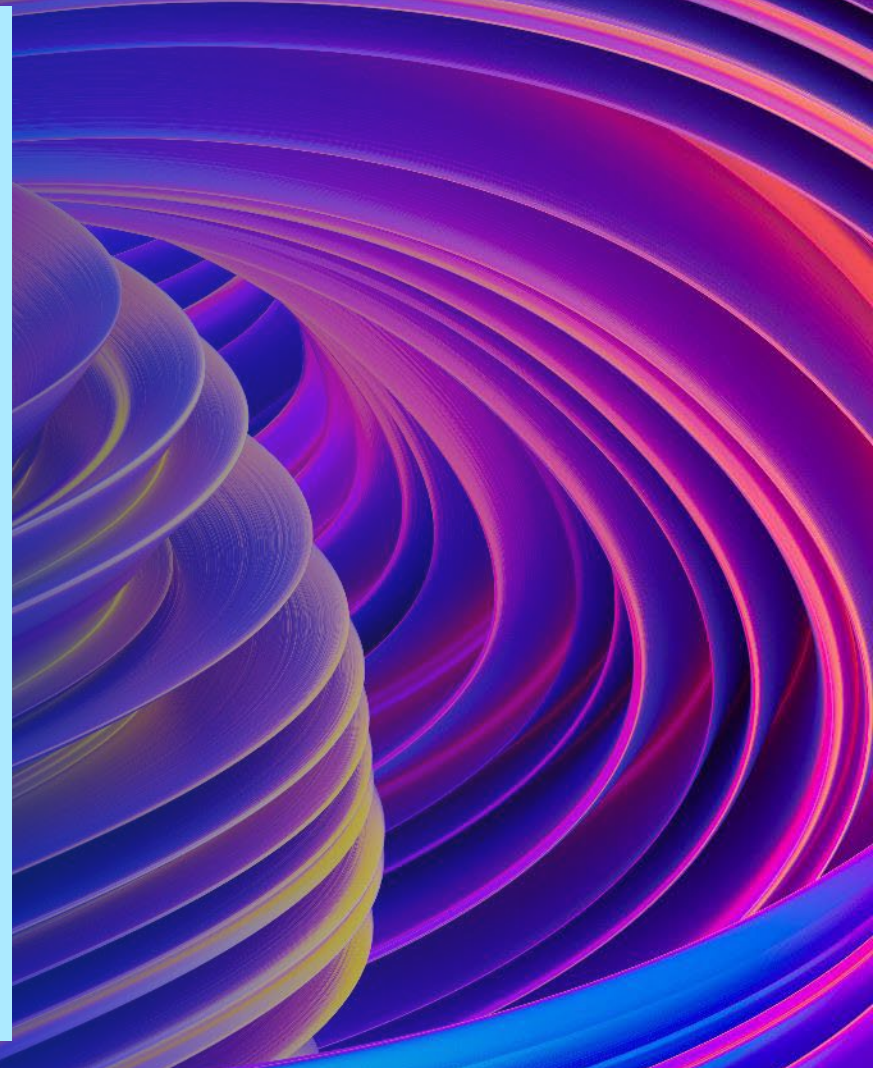
Car companies massively exposed to web vulnerabilities

The researchers' findings, detailed on Curry's blog, highlight an alarming number of critical vulnerabilities across different systems. For example, a poorly configured API endpoint for generating one-time passwords for the web portals of BMW and Rolls Royce potentially enabled attackers to take over the accounts of any employee and contractor, thereby gaining access to sensitive customer and vehicle information.

A misconfiguration in the Mercedes-Benz single sign-on (SSO) system enabled the researchers to gain access to several internal company assets, including private GitHub repositories and internal communication tools. Attackers could pose as employees, allowing them to access sensitive information, send commands to customer vehicles, perform RCE attacks, and use social engineering to escalate their privileges across the Mercedes-Benz infrastructure.

https://portswigger.net/daily-swig/car-companies-massively-exposed-to-web-vulnerabilities/volkswagen-breach-china-hackers/

解決策



Solution?

セキュリティ対策

KPMGハンガリーサイバー研究所のアプローチ

01

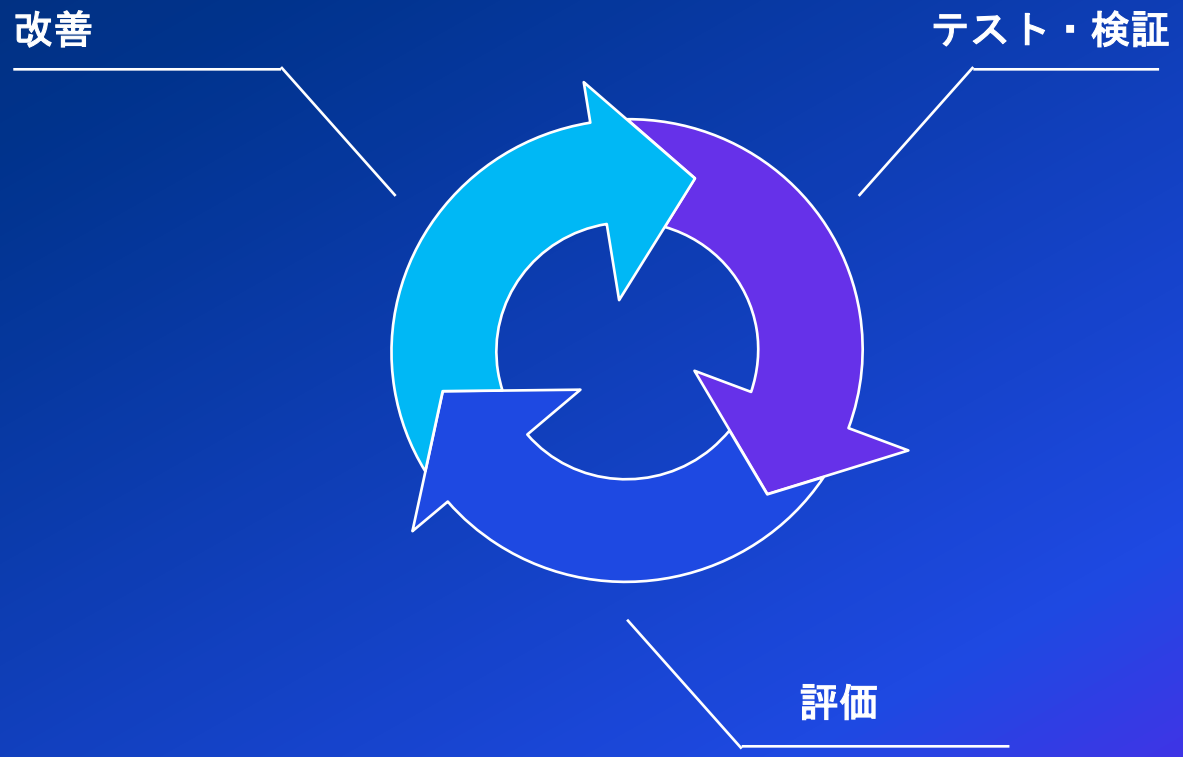
人

- 内部セキュリティトレーニング
- 継続的なソーシャルエンジニアリングテスト
- IT 知識向上のためのトレーニング

02

システム

- IT 監査
- IT セキュリティー検査
- 定期的な侵入テスト
- レッドチーミング演習



Security consciousness

KPMG Hungary CyberLab is here to help!

01

People

- Internal security trainings
- Continuous social engineering tests
- IT awareness trainings

02

System

- IT audits
- IT security reviews
- Regular penetration tests
- Red Teaming and adversary emulation

Contacts

Kornél Lukács
Partner,
Head of Cyber

kornel.lukacs@kpmg.hu

Kamilló Matek
Senior Manager,
Head of Cyber Lab

kamillo.matek@kpmg.hu

Judit Körmendy
Senior Cyber Project Manager

judit.kormendy@kpmg.hu

Masashi Nomura
野村　雅士

Director, Japanese Desk

ディレクター
ジャパンデスク

+48 604 496 342

mnomura1@kpmg.pl

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

Kpmg.hu