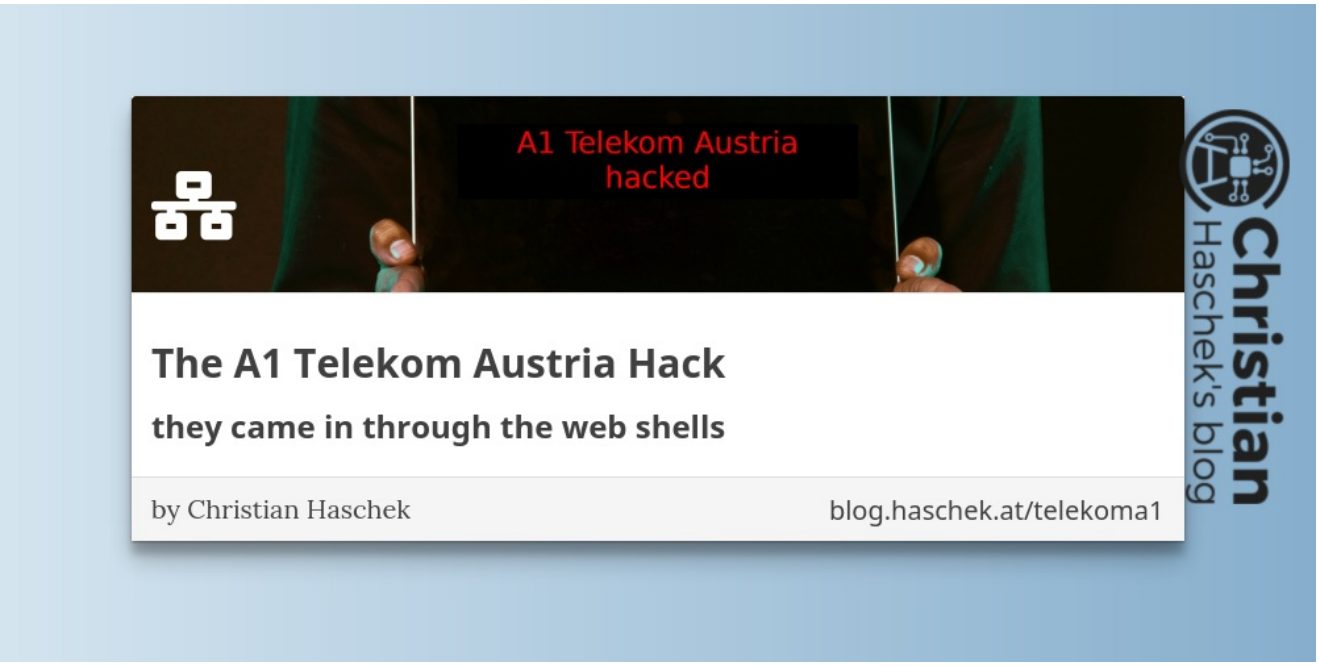
The A1 Telekom Austria Hack

blog.haschek.at/2020/the-a1-telekom-hack.html

Christian



On the 3rd of February 2020 I received an encrypted email on 3 of my email addresses from a person calling themself `"Libertas"` with the subject "Information for the public".

> I am writing to you today because you seem to be a IT security related guy from Austria with a brain. I hope this assumption is correct, otherwise please disregard this message.
>
> I am writing concerning your local telecom company A1 Telekom. -Libertas

At first I thought it's some conspiracy theorist who wants to publish something on my blog `(they always do)` but it was not one of these cases and I wasn't prepared to what they presented me.

Disclaimer:
After confirming the hack with A1 I was asked to postpone the publishing of this post until A1 has kicked the attackers out. I complied with their request so I wouldn't interfere with the ongoing investigation. Since I did not publish this post for months the whistleblower also contacted a journalist from Heise.de and we agreed to release our articles at the same time.

Since I have no way of checking the validity of individual statements made by the whistleblower, they could all be fabricated. I find them very plausible and many details of the email were confirmed by A1 but keep it in the back of your head that the statements of

"Libertas" might be untrue or half-true until confirmed by A1 Telekom. Since I had the opportunity to talk to people from A1 I will add their statements in blue.

First things first: WTF is A1 Telekom?

A1 Telekom is one of the largest telecom companies in Austria. They own a large variety of IT infrastructure including the FTTH connection I am currenlty using for my home office.

They have a yearly revenue of about 2.5 Billion €, over 8,300 employees and in more rural parts of the country they are the only provider of internet and phone connections. They are a big deal here.

Who is Libertas?

Libertas is the `whistleblower` who informed me and a journalist from Heise.de about the A1 hack. Libertas `is not the hacker` who infiltrated A1 but rather someone close to A1 with confirmed insider knowledge.

What about the alleged hack?

The whistleblower stated that around December 2019 the A1 internal CERT (computer emergency response team) (lead by a person the source named in the Email) was informed about problems with their internal EMS system.

Their malware detection systems found several webshells spread around a variety of servers but at this point almost all internal servers were compromised. Including two of their internal domains.

A1 confirmed the timeline and attack vector but stated that not "almost all internal servers" were compromised but only a dozen.

According to the source one of the attacked domains was a managed customer network for a large austrian company.

A1 found this not to be true as the attacker only had access to their office and a few devices, none of the compromised devices were outside of their office network

How did they get in?

The source suspects, that the attackers got in using a vulnerability of an (unspecified) Microsoft product.

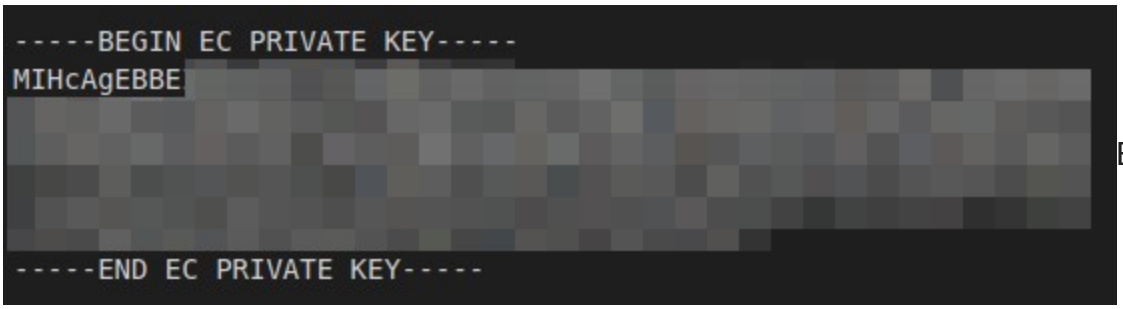
> here are several reasons why they where able to move around so comfortably. While A1 spent lots of resources to protect their systems from external threats, internal threats where not really cared about. Meaning it is pretty easy for an authorized user to take control over systems he normally would not have control over. And unfortunately, as this example shows, it happens that unauthorized people take over the role of such authorized users. -Libertas

The source names two internal admin accounts called `"VIPRegionen"` and `"ITSolution"` and also added the passwords of these accounts to the email they sent me. The passwords to these accounts started with `"Y_2"` and `"X_7"` and were (according to the source) unchanged since 2013 and were well known to a few generations of technicians at the company.

`Note: This fact has nothing to do with the hack, it was just meant for me to confirm the validity of the whistleblowers insights into the company.`

They state these logins were used by the "Core team" which operate Windows Systems for A1 customers and interal ones. There's also the "NTOS team" which manage most A1 internal Windows Servers and the "UXOS team" manages all linux based systems. The latter one allegedly manages over 2500 systems.

The whistleblower also sent me the (uncensored) ECDSA private key for the root user:



ECDSA key

A1 confirmed the existence of webshells and the validity of the passwords, although they were old and most of them not used anymore.

What about the databases?

Glad you asked.

The source states that the database systems were also compromised and the password of the Database Administration Team sarted with `"Gfr"`. A1 also manages some external corporate customer database systems and the root password for them is the same as the one above with a single symbol added at the end.

The source also claimed the DBA team rotates this master password and has changed it 8 times since 2014.

A1 confirmed that the attackers had access to a SQL database and did various queries although they said no customer data was in those databases and no customer info was transferred out of the system.

How widespread was the breach?

According to the whistleblower attackers gained access to more than 12,000 client systems which were all operated by A1. A1 said this was not true and just about a dozen devices were compromised and these were all in the Office space. The number 12,000 systems was confirmed by A1 to be the whole number of devices they manage, not the number of compromised computers.

> My source tells me that he doubts that this is the first huge successful infiltration of A1, but much more likely just the first one detected. A1 brought in `-REDACTED COMPANY NAME-` and `-REDACTED COMPANY NAME-` in early January to investigate and launched an internal project (`"Project Alcatraz"`) to increase security awareness and procedures all around A1. -Libertas

The source also states that A1 did not only not make it public, they even let the attackers roam in their systems and let them download "massive amounts" of customer data to find out more about them without alarming them.

> However, it seems that one of their main concerns is keeping all of this under wraps and not really acting because that could "alarm the attackers that we are watching" and even ordering certain security features not yet to be implemented on certain systems where activity of the attackers was noted or suspected. So they implemented all kind of additional monitoring (like running Sysmon on many internal Windows systems and centrally analyzing the data) while they let the attackers pull all kind of data from their systems including massive amounts of customer data. -Libertas

They also state that the attackers were watched making very specific queries of location, phone numbers and other customer data for certain private A1 customers. the source did not disclose who these people were.

A1 stated that the attackers did not have access to any client systems, only a few devices in their corporate office were infected and no customer data was stolen. They confirmed that external IT security professionals were flown in in January

When did the attack stop?

A1 told me that the attackers were successfully kicked out of the system on May 22nd 2020 by closing all remaining backdoors. The aftermath for A1 was a painful one as any sysadmin can imagine:

- New Passwords for all 8000+ employees
- New keys and passwords for all servers and services
- IT security training

Who were the attackers?

The source thinks it was the Gallium group who are notorious for using bugs in Windows web servers and specifically targetting telecom companies which might have ties to the Chinese Ministry of State Security according to the source.

> There are quite some hints that a state power or similar is at work here, but honestly you know attribution is hard and these could probably be all kind of three-letter agency weasels from god knows where. -Libertas

A1 stated that they had no clues who the attackers were only that they used multiple VPN servers from multiple countries.

Why is the source telling me this?

The person says "The public should be informed about this"

> The public should know and A1 should act here and condemn these constant network infiltrations coming from god alone knows what state agencies. Also they should publicate what they improve now in order to also help others to secure them against these threats. -Libertas

The email ended with

```
Please understand that i cannot keep in touch with you, this will be my only
communication.

best regards,
concerned third party
```

When I tried to write back I got an error message from their email provider stating the account no longer exists.

Let's recap

The anonymous source states that

- A1 was owned on a massive scale (over 12000 Servers)
- The attack was known internally but not stopped (to learn more about the attackers)
- It is unclear who the attackers were or if they were state sponsored but it seems to be a very sophisticated attack

A1 corrected it

- Only a dozen devices were compromised and no customer or corporate data was stolen
- The attackers were discovered and kicked off their network on May 22 2020
- A1 was not blackmailed and it was not a cryptolocker