RE: Volexity Alert - Suspicious Outbound SSH Traffic.

Hanner, Karl <Karl.Hanner@Teledyne.com>

Thu 15 Aug 2024 14:34

To:Jerry Jacobs <JJacobs@Adimec.com>;Patrick Kilian <pkilian@adimec.com>

Hi Jerry,

Many thanks for your response, for taking action on this and for your understanding of the controls that are necessary in larger organisations.

Regards,

Karl

From: Jerry Jacobs <JJacobs@Adimec.com>
Sent: Thursday, August 15, 2024 12:39 PM
To: Hanner, Karl <Karl.Hanner@Teledyne.com>; Patrick Kilian <pkilian@adimec.com>
Subject: Re: Volexity Alert - Suspicious Outbound SSH Traffic.

External Email

Hi Karl,

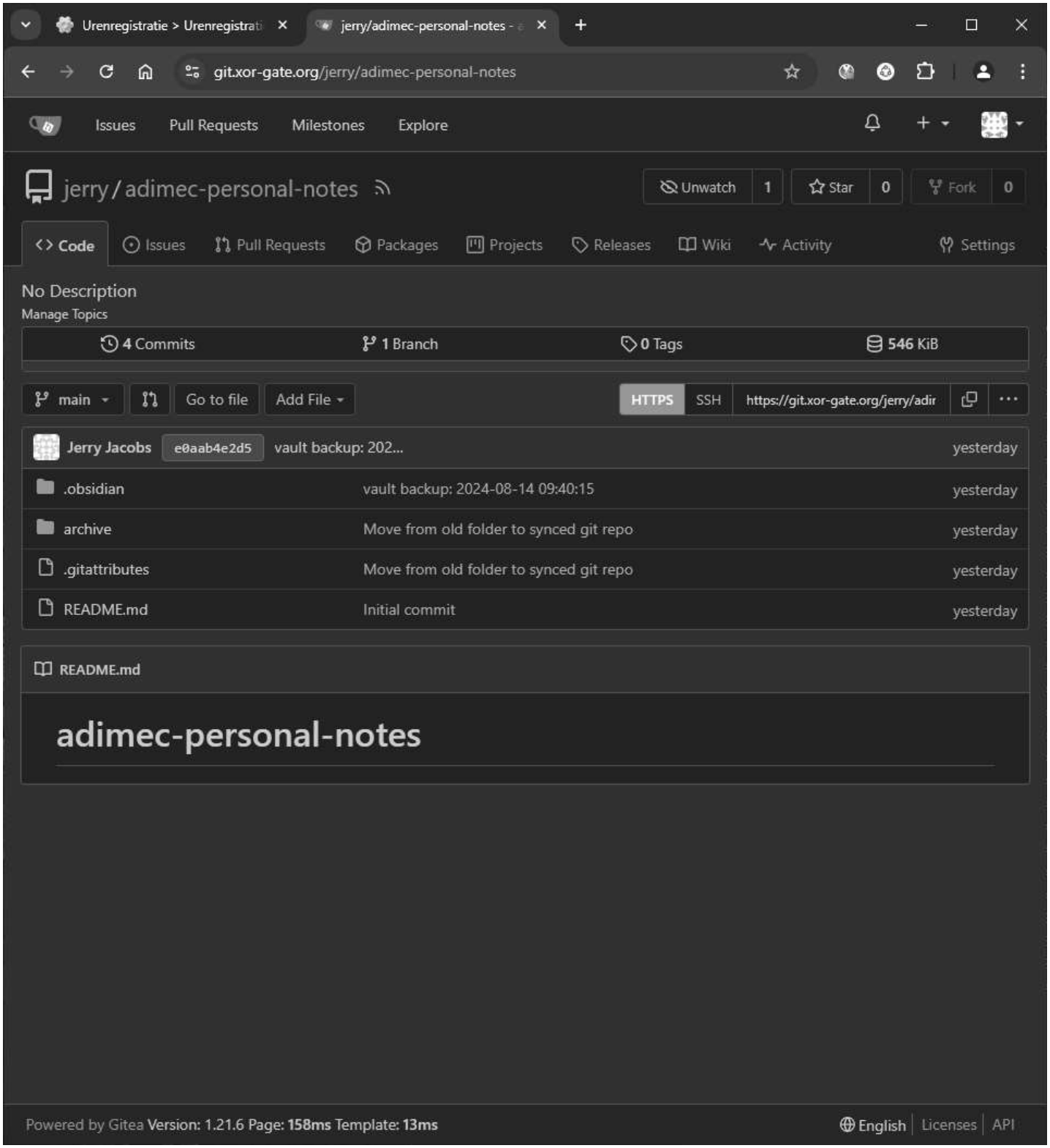
Recently this week I setup syncing some personal notes to my own server at home over git with Obsidian. I found it handy to have some of my Adimec notes at home. As I was also using this setup for my personal home notes.

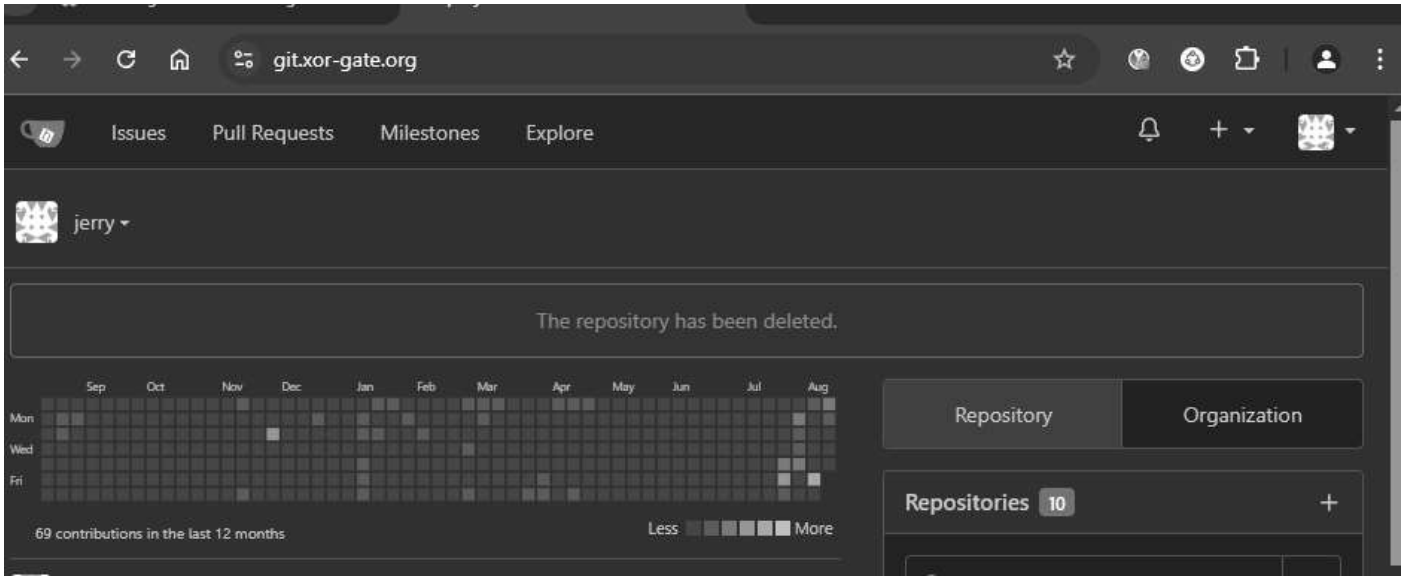
I have attached a tree list of the Obsidian notes git repository I synced. And screenshots of my git server.

At time of writing I removed this from my server. And will use our internal git server to backup the notes in a private repository. So possible Teledyne Adimec related information is not on non-Teledyne hardware.

It's also a wakeup call for me to be aware about data confidentiality.

If any more information is necessary, let me know.


Urenregistratie > Urenregistrati
jerry/adimec-personal-notes -
git.xor-gate.org/jerry/adimec-personal-notes
Issues
Pull Requests
Milestones
Explore
jerry / adimec-personal-notes
Unwatch 1
Star 0
Fork 0
Code
Issues
Pull Requests
Packages
Projects
Releases
Wiki
Activity
Settings
No Description
Manage Topics
4 Commits
1 Branch
0 Tags
546 KiB
main
Go to file
Add File
HTTPS
SSH
https://git.xor-gate.org/jerry/adir
Jerry Jacobs
e0aab4e2d5
vault backup: 202...
yesterday
.obsidian
vault backup: 2024-08-14 09:40:15
yesterday
archive
Move from old folder to synced git repo
yesterday
.gitattributes
Move from old folder to synced git repo
yesterday
README.md
Initial commit
yesterday
README.md
adimec-personal-notes
Powered by Gitea Version: 1.21.6 Page: 158ms Template: 13ms
English
Licenses
API



With kind regards/Met vriendelijke groet,

Jerry Jacobs

Development Engineer Firmware

Teledyne Adimec

From: Hanner, Karl <Karl.Hanner@Teledyne.com>
Sent: Thursday, 15 August 2024 13:13
To: Jerry Jacobs <JJacobs@Adimec.com>; Patrick Kilian <pkilian@adimec.com>
Subject: RE: Volexity Alert - Suspicious Outbound SSH Traffic.

Caution: This is an external email and is mentioning a password change or reset. Please take care when actioning anything within this email. If you are in doubt please contact the IT Department.

Hi Jerry,

Many thanks for the explanation.

We are also seeing activity as detailed in the attached file. The activity looks like notes made in Obsidian running on a virtual machine being routinely synced with your personal (blog) domain. Can you please explain the purpose of this activity as well and the content of the notes?

Regards,

Karl

From: Jerry Jacobs <JJacobs@Adimec.com>
Sent: Thursday, August 15, 2024 12:00 PM
To: Patrick Kilian <pkilian@adimec.com>; Hanner, Karl <Karl.Hanner@Teledyne.com>
Subject: Re: Volexity Alert - Suspicious Outbound SSH Traffic.

External Email

Hi Patrick and Karl,

I was using an SSH tunnel with my personal google profile chrome session to listen to music on youtube. The server is located at home and indeed it is hosted at my personal (blog) domain. Then it was marked as suspicious traffic because streaming is high volume traffic.

I understand for security reasons personal accounts may not be used on teledyne adimec hardware to prevent potential malware/virus infection.

The Teledyne Adimec firewall SSL filter also sniffs passwords, browser session keys etcetera. That is why I was using it for my personal youtube session.

Hope this clears things up, and no malicious activity has happened. It will not happen again.

With kind regards/Met vriendelijke groet,

Jerry Jacobs

Development Engineer Firmware

Teledyne Adimec

From: Patrick Kilian <pkilian@adimec.com>
Sent: Thursday, 15 August 2024 09:43
To: Hanner, Karl <Karl.Hanner@Teledyne.com>; Jerry Jacobs <JJacobs@Adimec.com>
Subject: Re: Volexity Alert - Suspicious Outbound SSH Traffic.

Hi Jerry,

Could you please explain the traffic that was detected?

With kind regards,

Patrick Kilian

IT Manager

Teledyne Adimec

Luchthavenweg 91, 5657 EA | P.O.Box 7909, 5605 SH

Eindhoven The Netherlands

Phone: +31 40 235 3900

E-mail: pkilian@adimec.com

www.adimec.com

Join us here: LinkedIn - Blog

Van: Hanner, Karl <Karl.Hanner@Teledyne.com>
Verzonden: donderdag 15 augustus 2024 09:38
Aan: Patrick Kilian <pkilian@adimec.com>
Onderwerp: Volexity Alert - Suspicious Outbound SSH Traffic.

Hi Patrick,

I hope that you are well.

Please see below an alert we have received from Volexity regarding suspicious outbound SSH traffic from a particular PC seemingly owned by Jerry Jacobs. We need to understand the purpose of this activity and whether it is related to Adimec business activities, if it is not then we need to understand if there are any security concerns related to this activity.

Many thanks for looking into this.

Volexity Alert:-

We have received some alerts about high volume of outbound SSH connections at Adimec from the IP address 10.10.104.145. We usually review these to make sure it is not mass scanning of different destination IP addresses. However, in examining the activity, we saw this system is making numerous ongoing session back to 143.178.7.101 (git.xor-gate[.]org). The website xor-gate[.]org looks to be run by someone in the Netherlands named Jerry Jacobs, which looks to be someone at Adimec. We can see older connections of the 143.178.7.101 IP also connecting into vpn.adimec.com. We also saw some connections to the same remote IP from 10.10.104.168 as well.

If the number of connections was not so high/frequent we would not have otherwise flagged this activity. However, since we did look into it and noticed a lot of connections and byte transfer over SSH (possibly git) we just wanted to make sure this was authorized/expected. Again, we have no specific evidence or reason to believe this is malicious or unauthorized but after review believe it is worth raising and validating.

Sample flows with larger byte counts:

StartTime	Proto	SrcAddr	Sport	Dir	DstAddr	Dport	SrcPkts	DstPkts	SrcBytes	DstBytes	State
2024-08-14 08:35:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	13697	11845	8868386	1666194	CON
2024-08-14 08:40:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	8751	7266	5087220	1073931	CON
2024-08-14 08:45:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	17585	14910	12239745	2028447	CON
2024-08-14 08:50:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	15631	12636	11171724	1747975	CON
2024-08-14 08:55:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	9751	8202	5813889	1186146	CON
2024-08-14 09:00:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	11111	8662	7391742	1224078	CON
2024-08-14 09:05:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	13226	9688	9538717	1354074	CON
2024-08-14 09:10:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	12417	9499	8985125	1306897	CON
2024-08-14 09:15:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	12221	9348	8580008	1314130	CON
2024-08-14 09:20:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	20150	13847	17968548	1743393	CON
2024-08-14 09:25:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	13006	9872	8966795	1388003	CON
2024-08-14 09:30:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	15906	11362	12724700	1507325	CON
2024-08-14 09:35:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	17682	12777	13801002	1704409	CON
2024-08-14 09:40:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	17849	13641	13828766	1837933	CON
2024-08-14 09:45:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	19910	16432	14659327	2253206	CON
2024-08-14 09:50:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	5638	4572	3645441	637798	CON
2024-08-14 09:55:00.072163	6	10.10.104.145	53176	->	143.178.7.101	22	1816	1340	1446668	169664	CON
2024-08-14 10:00:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	6052	4745	4277252	654470	CON
2024-08-14 10:05:00.000000	6	10.10.104.145	53176	->	143.178.7.101	22	8633	6213	6075935	868983	CON
2024-08-14 10:06:40.569535	17	10.10.104.168	50012	<->	143.178.7.101	50010	10267	10118	1607394	1647608	CON
2024-08-14 10:06:55.261602	17	10.10.104.168	50048	<->	143.178.7.101	50049	2302	299	1927604	50402	CON
2024-08-14 10:10:00.000000	17	10.10.104.168	50012	<->	143.178.7.101	50010	16105	15802	2448408	2425432	CON
2024-08-14 10:10:00.000000	17	10.10.104.168	50048	<->	143.178.7.101	50049	2298	374	1793595	56104	CON
2024-08-14 10:15:00.000000	17	10.10.104.168	50012	<->	143.178.7.101	50010	16117	15862	2456141	2574469	CON
2024-08-14 10:15:00.000000	17	10.10.104.168	50048	<->	143.178.7.101	50049	3458	382	3220477	57372	CON
2024-08-14 10:20:00.000000	17	10.10.104.168	50012	<->	143.178.7.101	50010	5984	5887	1015748	1016656	CON

Regards,

Karl

Useful Cybersecurity links

DISCLAIMER This e-mail message may contain legally privileged or confidential information. If you are not the intended recipient and received this e-mail message in error, you may not disclose, use, disseminate, distribute, copy or forward this message or attachment in any way. Please return the message including its attachments to the sender and delete this e-mail message from your systems. For control of technical data, Adimec has implemented an effective and rigorous compliance program under corporate procedure. In the event this e-mail message contains technical data within the definition of the International Traffic in Arms Regulations or European export legislation of strategic goods, it is subject to Governmental export control laws. Transfer of this data by any means to anyone who is not a US citizen or Adimec employee, without an official Governmental export license or other approval, is prohibited. For complete regulations, please contact Compliance Manager at Adimec advanced image systems bv, Eindhoven, the Netherlands. T: +31 40 2353 900, E: compliance@adimec.com; website: https://www.adimec.com). Adimec does not accept liability for any errors, omissions, corruption or virus in the contents of this message or any attachments.