The major cyberattacks on the telecommunications sector in 2023

Kyivstar, Orange España, 'Sea Turle' campaigns, T-Mobile US – what is known?

January 2024

Authors: Inna Serdiuk, Olga Nasibullina

Contents

Introduction

Recently, there has been an increase in the number of cyberattacks aimed specifically at companies that provide telecommunication services. Controlling the vast majority of countries' complex and critical infrastructure, used for data sharing, and storing vast amounts of sensitive data, the impact of a successful cyberattack on the telecommunications sector can be significant and sometimes catastrophic.

By keeping confidential information about all their customers, telecommunications companies are tempting targets for cybercriminals or insiders trying to trick customers and steal money.

While ransomware remained a serious threat to organizations, in 2023, cyber threat actors focused on data theft and destruction, system disruption, and espionage. Let's talk about Kyivstar, Orange España, 'Sea Turle' campaigns, T-Mobile US and what is known about it.

About CyberPeople

CyberPeople is a skills-based cybersecurity job-marching platform.
Test our beta https://cyberpeople.tech - help to break cyber workforce gap!

Follow us here: in

Read blog CyberPeople here.

Ukrainian “Kyivstar”

On the morning of December 12, 2023, subscribers of “Kyivstar” throughout Ukraine were unable to use mobile communication services and internet access due to a massive outage. The cause of the technical failure in the operator's system was a hacker attack.

CEO of “Kyivstar”, Alexander Komarov, noted that the cyberattack was highly powerful. According to him, there was a “penetration into the IT infrastructure and its destruction”. The primary goal of the attack, as explained by the company's leader, was the maximum destruction of the operator's intellectual infrastructure.

Key events.

- On December 12, 2023, at 5:26 am, “Kyivstar's” specialists identified unusual behavior in their computer network.
- At 6:30 am, “Kyivstar” employees realized that the company was under a powerful hacker attack. The target of the attack was the core network, responsible for processing and routing traffic between users and services.
- At 8:04 am, “Kyivstar” publicly announced the technical failure in its operations and warned of possible service limitations for its subscribers.

Ilya Vityuk, the head of the Cyber Security department of the Security Service of Ukraine (SBU), reported that the attack caused “catastrophic” destruction and aimed to deliver a psychological blow while obtaining intelligence information.

“This attack is a significant warning not only for Ukraine but for the entire Western world to understand that no one is immune”, - Ilya Vityuk

The attack destroyed “almost everything”, including thousands of virtual servers and PCs, according to Vityuk, describing it as possibly the first instance of a destructive cyberattack that “completely annihilated the core of the telecommunications operator”.

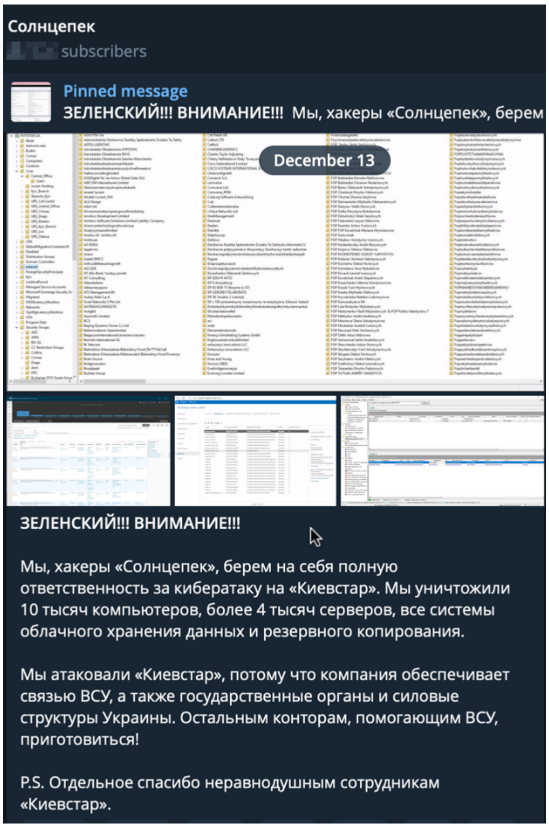
How the hackers compromised “Kyivstar”?

During the investigation, the SBU found that hackers may have attempted to penetrate “Kyivstar” in March 2023 or earlier.

On December 13, 2023, the responsibility for the attack was claimed by the Russian hacker group "Sontsepok" ("Солнцепьок"). On their Telegram channel, they declared that they had destroyed "10 thousand computers, over 4 thousand servers, all cloud data storage systems, and backup systems". They stated that they targeted "Kyivstar" because the company "provides communication for the Armed Forces of Ukraine, as well as state bodies and law enforcement agencies of Ukraine". They also issued threats to other Ukrainian companies supporting the Ukrainian army.

On the same day, the SBU stated, "Responsibility for the attack has already been claimed by one of the Russian pseudo-hacking groups. It is a hacking unit of the main intelligence directorate of the Armed Forces of Russia", specifying that they were referring to "Sontsepok".

The Telegram channel "Sontsepok" published four screenshots intended to confirm their involvement in the attack on "Kyivstar". Former Deputy Head of the Ukrainian State Special Communications Service, Victor Zhora, noted, "If the published screenshots are genuine, then the enemy was present in the network for quite a long time, thoroughly studied the topology and infrastructure of the services".



Солнцепек

[redacted] subscribers

Pinned message

ЗЕЛЕНСКИЙ!!! ВНИМАНИЕ!!! Мы, хакеры «Солнцепек», берем

December 13

ЗЕЛЕНСКИЙ!!! ВНИМАНИЕ!!!

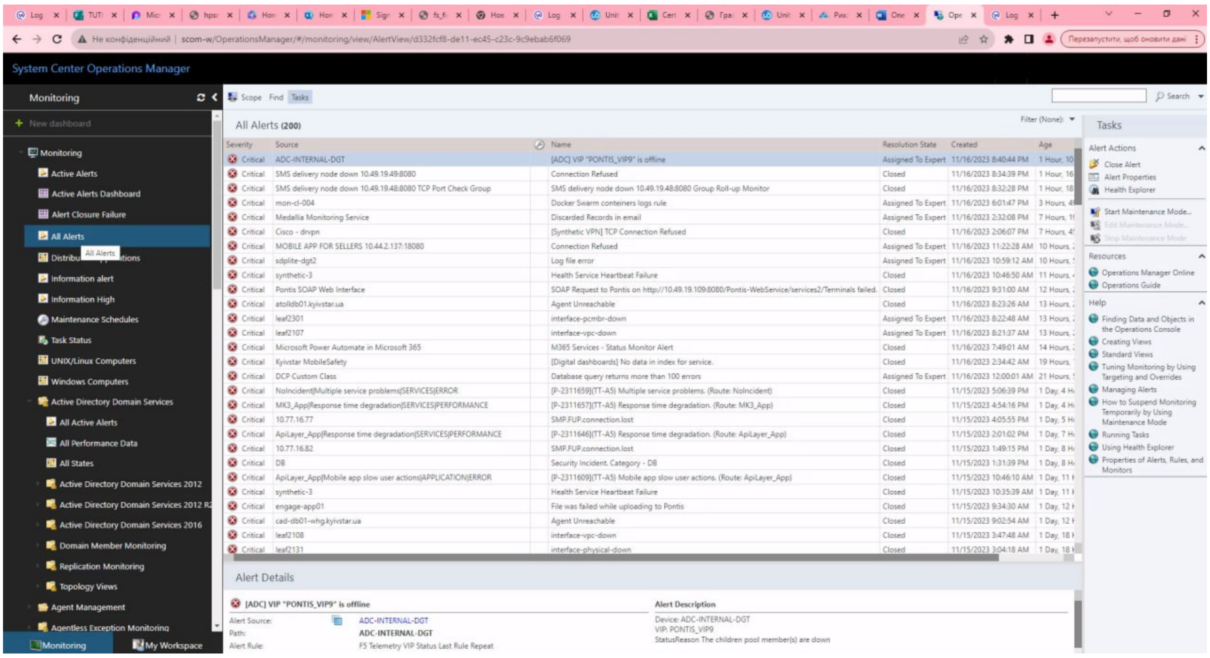
Мы, хакеры «Солнцепек», берем на себя полную ответственность за кибератаку на «Киевстар». Мы уничтожили 10 тысяч компьютеров, более 4 тысяч серверов, все системы облачного хранения данных и резервного копирования.

Мы атаковали «Киевстар», потому что компания обеспечивает связью ВСУ, а также государственные органы и силовые структуры Украины. Остальным конторам, помогающим ВСУ, приготовиться!

P.S. Отдельное спасибо неравнодушным сотрудникам «Киевстар».

Source by "Sontsepok" (Telegram channel)

American cybersecurity expert Alex Holden mentioned that, according to their findings, the hackers gained access to the Active Directory system, allowing “administrators to manage user access to various resources, establish security rules, grant permissions for the use of various programs and services, and integrate new computers into the network”.



All Alerts (200)

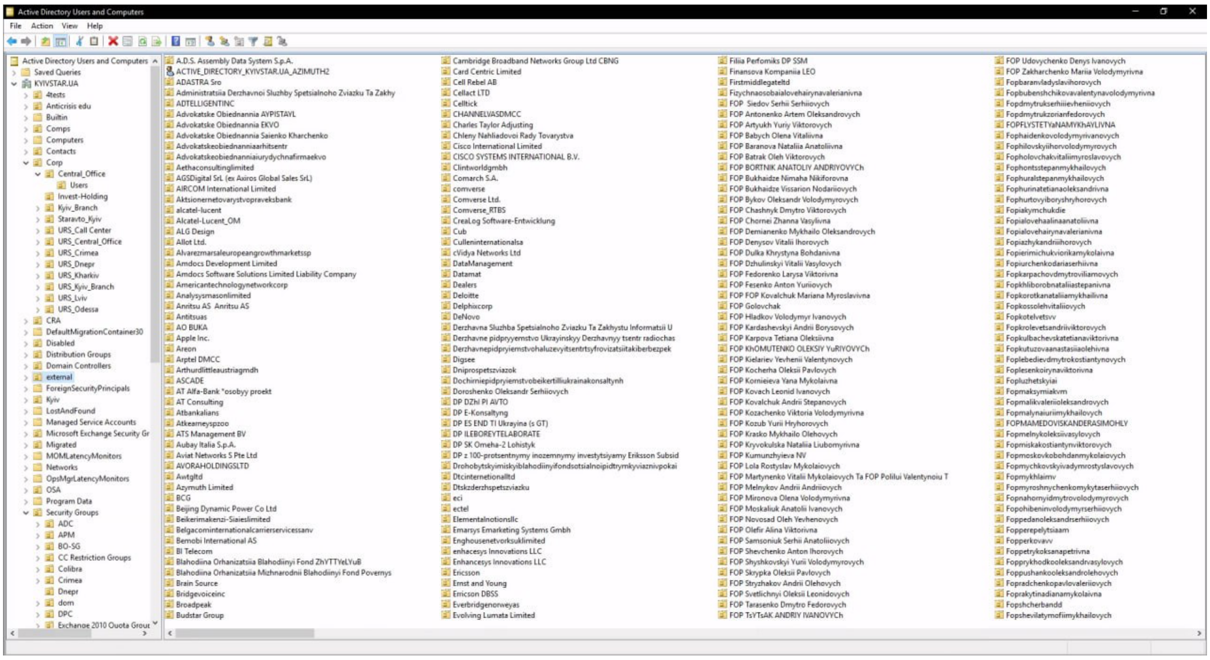
Severity	Source	Name	Resolution State	Created	Age
Critical	ADC-INTERNAL-DGT	[ADC] VIP "PONTIS_VIP9" is offline	Assigned To Expert	11/16/2023 8:40:44 PM	1 Hour, 10
Critical	SMS delivery node down 10.49.19.49:8080	Connection Refused	Closed	11/16/2023 8:34:39 PM	1 Hour, 16
Critical	SMS delivery node down 10.49.19.48:8080 TCP Port Check Group	SMS delivery node down 10.49.19.48:8080 Group Roll-up Monitor	Closed	11/16/2023 8:32:28 PM	1 Hour, 18
Critical	mon-cl-004	Docker Swarm conteiners logs rule	Assigned To Expert	11/16/2023 6:01:47 PM	3 Hours, 4
Critical	Medallia Monitoring Service	Discarded Records in email	Assigned To Expert	11/16/2023 2:32:08 PM	7 Hours, 1
Critical	Cisco - drvpn	[Synthetic VPN] TCP Connection Refused	Closed	11/16/2023 2:06:07 PM	7 Hours, 4
Critical	MOBILE APP FOR SELLERS 10.44.2.137:18080	Connection Refused	Assigned To Expert	11/16/2023 11:22:28 AM	10 Hours,
Critical	sdplite-dgt2	Log file error	Assigned To Expert	11/16/2023 10:59:12 AM	10 Hours,
Critical	synthetic-3	Health Service Heartbeat Failure	Closed	11/16/2023 10:46:50 AM	11 Hours,
Critical	Pontis SOAP Web Interface	SOAP Request to Pontis on http://10.49.19.109:8080/Pontis-WebService/services2/Terminals failed.	Closed	11/16/2023 9:31:00 AM	12 Hours,
Critical	atolldb01.kyivstar.ua	Agent Unreachable	Closed	11/16/2023 8:23:26 AM	13 Hours,
Critical	leaf2301	interface-pcmbr-down	Assigned To Expert	11/16/2023 8:22:48 AM	13 Hours,
Critical	leaf2107	interface-vpc-down	Assigned To Expert	11/16/2023 8:21:37 AM	13 Hours,
Critical	Microsoft Power Automate in Microsoft 365	M365 Services - Status Monitor Alert	Closed	11/16/2023 7:49:01 AM	14 Hours,
Critical	Kyivstar MobileSafety	[Digital dashboards] No data in index for service.	Closed	11/16/2023 2:34:42 AM	19 Hours,
Critical	DCP Custom Class	Database query returns more than 100 errors	Assigned To Expert	11/16/2023 12:00:01 AM	21 Hours,
Critical	NoIncident|Multiple service problems|SERVICES|ERROR	[P-2311659](TT-A5) Multiple service problems. (Route: NoIncident)	Closed	11/15/2023 5:06:39 PM	1 Day, 4 H
Critical	MK3_App|Response time degradation|SERVICES|PERFORMANCE	[P-2311657](TT-A5) Response time degradation. (Route: MK3_App)	Closed	11/15/2023 4:54:16 PM	1 Day, 4 H
Critical	10.77.16.77	SMP.FUP.connection.lost	Closed	11/15/2023 4:05:55 PM	1 Day, 5 H
Critical	ApiLayer_App|Response time degradation|SERVICES|PERFORMANCE	[P-2311646](TT-A5) Response time degradation. (Route: ApiLayer_App)	Closed	11/15/2023 2:01:02 PM	1 Day, 7 H
Critical	10.77.16.82	SMP.FUP.connection.lost	Closed	11/15/2023 1:49:15 PM	1 Day, 8 H
Critical	DB	Security Incident. Category - DB	Closed	11/15/2023 1:31:39 PM	1 Day, 8 H
Critical	ApiLayer_App|Mobile app slow user actions|APPLICATION|ERROR	[P-2311609](TT-A5) Mobile app slow user actions. (Route: ApiLayer_App)	Closed	11/15/2023 10:46:10 AM	1 Day, 11
Critical	synthetic-3	Health Service Heartbeat Failure	Closed	11/15/2023 10:35:39 AM	1 Day, 11
Critical	engage-app01	File was failed while uploading to Pontis	Closed	11/15/2023 9:34:30 AM	1 Day, 12
Critical	cad-db01-whg.kyivstar.ua	Agent Unreachable	Closed	11/15/2023 9:02:54 AM	1 Day, 12
Critical	leaf2108	interface-vpc-down	Closed	11/15/2023 3:47:48 AM	1 Day, 18
Critical	leaf2131	interface-physical-down	Closed	11/15/2023 3:04:18 AM	1 Day, 18

Alert Details

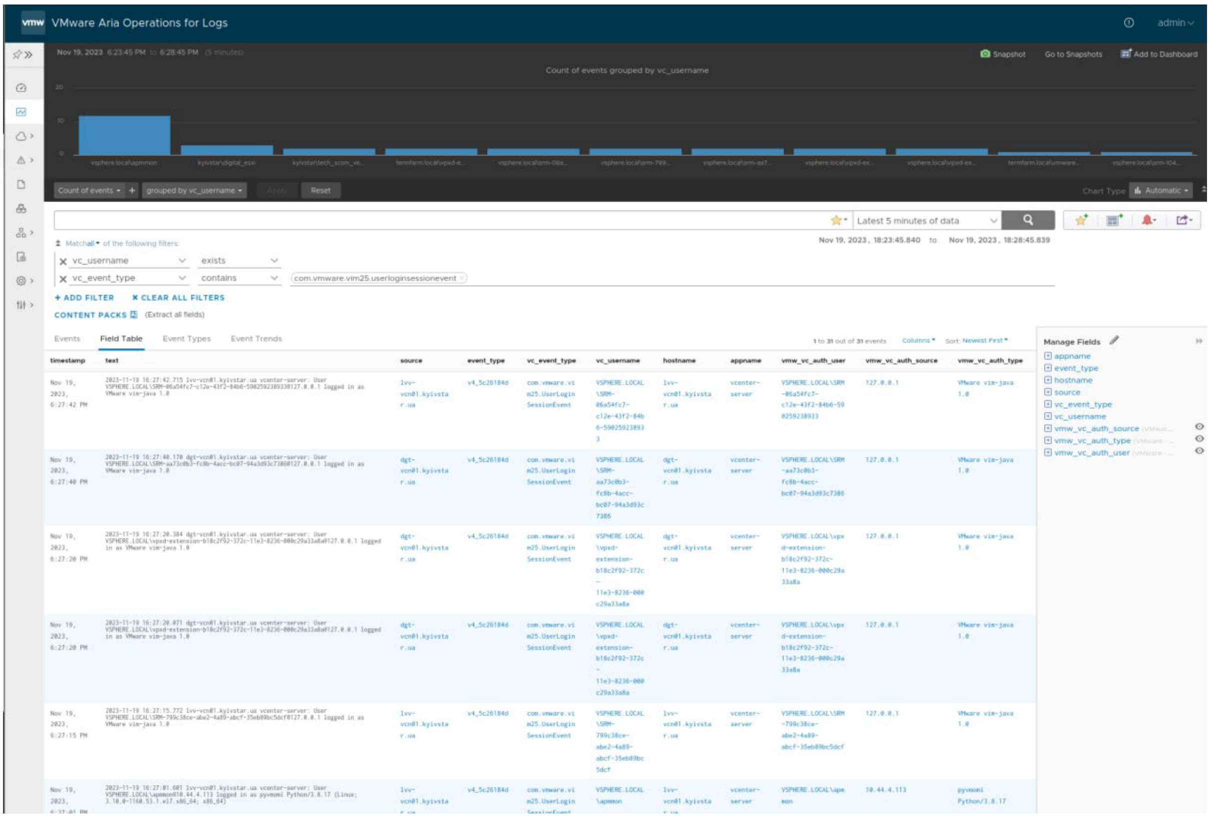
[ADC] VIP "PONTIS_VIP9" is offline

Alert Source: ADC-INTERNAL-DGT
Path: ADC-INTERNAL-DGT
Alert Rule: F5 Telemetry VIP Status Last Rule Repeat

Alert Description
Device: ADC-INTERNAL-DGT
VIP: PONTIS_VIP9
StatusReason The children pool member(s) are down



A.D.S. Assembly Data System S.p.A.
ACTIVE_DIRECTORY_KYIVSTAR.UA_AZIMUTH2
ADASTRA Sro
Administratsiia Derzhavnoi Sluzhby Spetsialnoho Zviazku Ta Zakhy
ADTELLIGENTINC
Advokatske Obiednannia AYPISTAYL
Advokatske Obiednannia EKVO
Advokatske Obiednannia Saienko Kharchenko
Advokatskeobiednanniaarhitsentr
Advokatskeobiednanniaiurydychnafirmaekvo
Aethaconsultinglimited
AGSDigital SrL (ex Axiros Global Sales SrL)
AIRCOM International Limited
Aktsionernetovarystvopraveksbank
alcatel-lucent
Alcatel-Lucent_OM
ALG Design
Allot Ltd.
Alvarezmarsaleuropeangrowthmarketssp
Amdocs Development Limited
Amdocs Software Solutions Limited Liability Company
Americantechnologynetworkcorp
Analysysmasonlimited
Anritsu AS Anritsu AS
Antitsuas
AO BUKA
Apple Inc.
Areon
Arptel DMCC
Arthurdlittleaustriagmdh
ASCADE
AT Alfa-Bank "osobyy proekt
AT Consulting
Atbankalians
Atkearneyspzoo
ATS Management BV
Aubay Italia S.p.A.
Aviat Networks S Pte Ltd
AVORAHOLDINGSLTD
Awtgltd
Azymuth Limited
BCG
Beijing Dynamic Power Co Ltd
Beikerimakenzi-Siaieslimited
Belgacominternationalcarrierservicessanv
Bemobi International AS
BI Telecom
Blahodiina Orhanizatsiia Blahodiinyi Fond ZhYTTYeLYuB
Blahodiina Orhanizatsiia Mizhnarodnii Blahodiinyi Fond Povernys
Brain Source
Bridgevoiceinc
Broadpeak
Budstar Group
Cambridge Broadband Networks Group Ltd CBNG
Card Centric Limited
Cell Rebel AB
Cellact LTD
Celltick
CHANNELVASDMCC
Charles Taylor Adjusting
Chleny Nahliadovoi Rady Tovarystva
Cisco International Limited
CISCO SYSTEMS INTERNATIONAL B.V.
Clintworldgmbh
Comarch S.A.
comverse
Comverse Ltd.
Comverse_RTBS
CreaLog Software-Entwicklung
Cub
Culleninternationalsa
cVidya Networks Ltd
DataManagement
Datamat
Dealers
Deloitte
Delphixcorp
DeNovo
Derzhavna Sluzhba Spetsialnoho Zviazku Ta Zakhystu Informatsii U
Derzhavne pidpryyemstvo Ukrayinskyy Derzhavnyy tsentr radiochas
Derzhavnepidpryiemstvohaluzevyitsentrtsyfrovizatsiitakiberbezpek
Digsee
Dniprospetszviazok
Dochirniepidpryiemstvobeikertilliukrainakonsaltynh
Doroshenko Oleksandr Serhiiovych
DP DZhI PI AVTO
DP E-Konsaltyng
DP ES END TI Ukrayina (s GT)
DP ILEBOREYTELABORATE
DP SK Omeha-2 Lohistyk
DP z 100-protsentnymy inozemnymy investytsiyamy Eriksson Subsid
Drohobytskyimiskyiblahodiinyifondsotsialnoipidtrymkyviaznivpokai
Dtcinternetionalltd
Dtskzderzhspetszviazku
eci
ectel
Elementalnotionsllc
Emarsys Emarketing Systems Gmbh
Enghousenetvorksuklimited
enhacesys Innovations LLC
Enhancesys Innovations LLC
Ericsson
Ernst and Young
Erricson DBSS
Everbridgenorweyas
Evolving Lumata Limited
Filiia Perfomiks DP SSM
Finansova Kompaniia LEO
Firstmiddlegateltd
Fizychnaosobaialovehairynavalerianivna
FOP Siedov Serhii Serhiiovych
FOP Antonenko Artem Oleksandrovych
FOP Artyukh Yuriy Viktorovych
FOP Babych Olena Vitaliivna
FOP Baranova Nataliia Anatoliivna
FOP Batrak Oleh Viktorovych
FOP BORTNIK ANATOLIY ANDRIYOVYCh
FOP Bukhaidze Nimaha Nikiforovna
FOP Bukhaidze Vissarion Nodariiovych
FOP Bykov Oleksandr Volodymyrovych
FOP Chashnyk Dmytro Viktorovych
FOP Chornei Zhanna Vasylivna
FOP Demianenko Mykhailo Oleksandrovych
FOP Denysov Vitalii Ihorovych
FOP Dulka Khrystyna Bohdanivna
FOP Dzhulinskyi Vitalii Vasylovych
FOP Fedorenko Larysa Viktorivna
FOP Fesenko Anton Yuriiovych
FOP FOP Kovalchuk Mariana Myroslavivna
FOP Golovchak
FOP Hladkov Volodymyr Ivanovych
FOP Kardashevskyi Andrii Borysovych
FOP Karpova Tetiana Oleksiivna
FOP KhOMUTENKO OLEKSIY YuRIYOVYCh
FOP Kielariev Yevhenii Valentynovych
FOP Kocherha Oleksii Pavlovych
FOP Kornieieva Yana Mykolaivna
FOP Kovach Leonid Ivanovych
FOP Kovalchuk Andrii Stepanovych
FOP Kozachenko Viktoria Volodymyrivna
FOP Kozub Yurii Hryhorovych
FOP Krasko Mykhailo Olehovych
FOP Kryvokulska Nataliia Liubomyrivna
FOP Kumunzhyieva NV
FOP Lola Rostyslav Mykolaiovych
FOP Martynenko Vitalii Mykolaiovych Ta FOP Polilui Valentynoiu T
FOP Melnykov Andrii Andriiovych
FOP Mironova Olena Volodymyrivna
FOP Moskaliuk Anatolii Ivanovych
FOP Novosad Oleh Yevhenovych
FOP Olefir Alina Viktorivna
FOP Samsoniuk Serhii Anatoliiovych
FOP Shevchenko Anton Ihorovych
FOP Shyshkovskyi Yurii Volodymyrovych
FOP Skrypka Oleksii Pavlovych
FOP Stryzhakov Andrii Olehovych
FOP Svetlichnyi Oleksii Leonidovych
FOP Tarasenko Dmytro Fedorovych
FOP TsYTsAK ANDRIY IVANOVYCh
FOP Udovychenko Denys Ivanovych
FOP Zakharchenko Mariia Volodymyrivna
Fopbaranvladyslavihorovych
Fopbubenshchikovavalentynavolodymyrivna
Fopdmytrukserhiiievheniiovych
Fopdmytrukzorianfedorovych
FOPFLYSTETYaNAMYKhAYLIVNA
Fophaidenkovolodymyrivanovych
Fophilovskyiihorvolodymyrovych
Fopholovchakvitaliimyroslavovych
Fophontsstepanmykhailovych
Fophuralstepanmykhailovych
Fophurinatetianaoleksandrivna
Fophurtovyiboryshryhorovych
Fopiakymchukdie
Fopialovehaalinaanatoliivna
Fopialovehairynavalerianivna
Fopiazhykandriiihorovych
Fopierimichukviorikamykolaivna
Fopiurchenkodariaserhiivna
Fopkarpachovdmytroviliamovych
Fopkhliborobnataliiastepanivna
Fopkorotkanataliiamykhailivna
Fopkossolehvitaliiovych
Fopkotelvetsvv
Fopkrolevetsandriiviktorovych
Fopkulbachevskatetianaviktorivna
Fopkutuzovaanastasiiaolehivna
Foplebedievdmytrokostiantynovych
Foplesenkoirynaviktorivna
Fopluzhetskyiai
Fopmaksymiakvm
Fopmalikvaleriioleksandrovych
Fopmalynaiuriimykhailovych
FOPMAMEDOVISKANDERASIMOHLY
Fopmelnykoleksiivasylovych
Fopmiskakostiantynviktorovych
Fopmoskovkobohdanmykolaiovych
Fopmychkovskyivadymrostyslavovych
Fopmykhlaimv
Fopmyroshnychenkomykytaserhiiovych
Fopnahornyidmytrovolodymyrovych
Fopohibeninvolodymyrserhiiovych
Foppedanoleksandrserhiiovych
Fopperepelytsiaam
Fopperkovavv
Foppetrykoksanapetrivna
Fopprykhodkooleksandrvasylovych
Foppushankooleksandrolehovych
Fopradchenkopavlovaleriiovych
Foprakytinadianamykolaivna
Fopshcherbandd
Fopshevilatymofiimykhailovych



Nov 19, 2023 , 18:23:45.840 to Nov 19, 2023 , 18:28:45.839

Match all of the following filters:

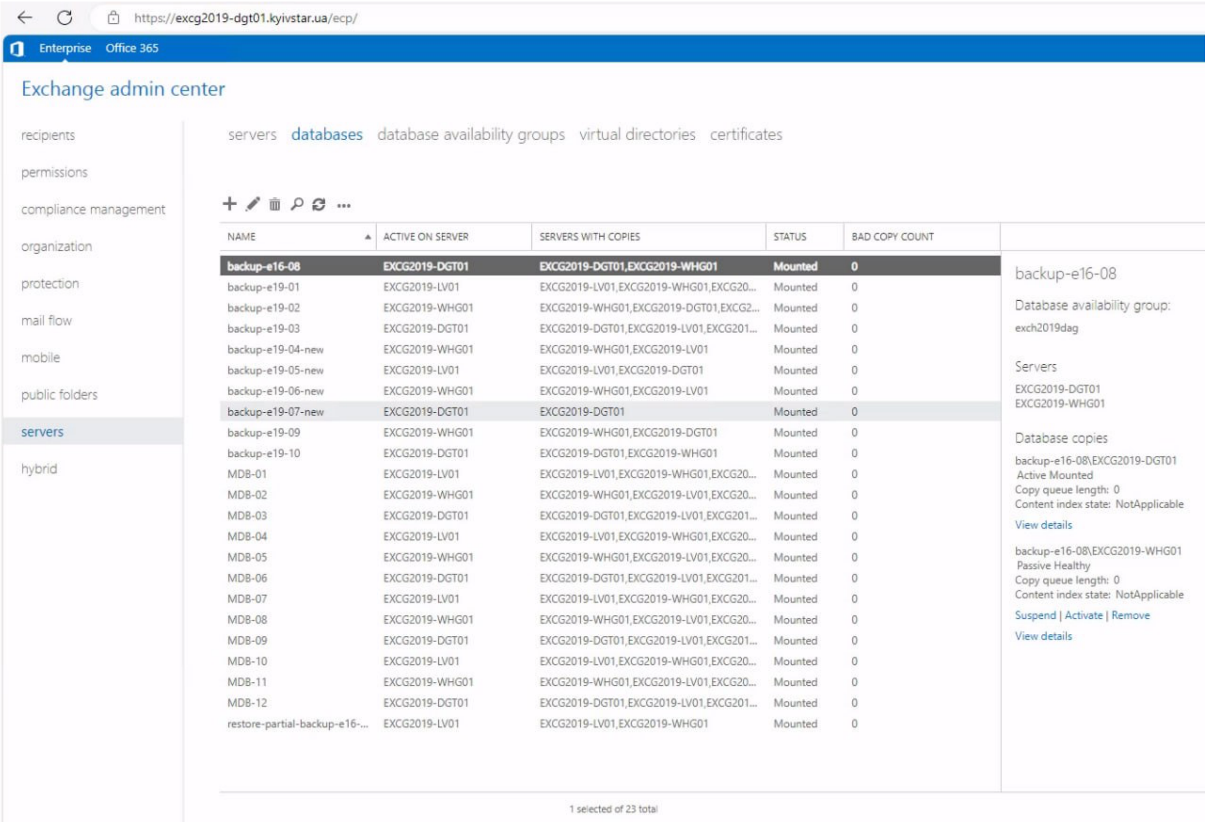
- vc_username exists
- vc_event_type contains com.vmware.vim25.userloginsessionevent

+ ADD FILTER ✕ CLEAR ALL FILTERS

CONTENT PACKS (Extract all fields)

1 to 31 out of 31 events Sort: Newest First

timestamp	text	source	event_type	vc_event_type	vc_username	hostname	appname	vmw_vc_auth_user	vmw_vc_auth_source	vmw_vc_auth_type
Nov 19, 2023, 6:27:42 PM	2023-11-19 16:27:42.715 lvv-vcn01.kyivstar.ua vcenter-server: User VSPHERE.LOCAL\SRM-06a54fc7-c12e-43f2-84b6-59025923893 3@127.0.0.1 logged in as VMware vim-java 1.0	lvv-vcn01.kyivstar.ua	v4_5c26184d	com.vmware.vim25.UserLoginSessionEvent	VSPHERE.LOCAL\SRM-06a54fc7-c12e-43f2-84b6-590259238933	lvv-vcn01.kyivstar.ua	vcenter-server	VSPHERE.LOCAL\SRM-06a54fc7-c12e-43f2-84b6-590259238933	127.0.0.1	VMware vim-java 1.0
Nov 19, 2023, 6:27:40 PM	2023-11-19 16:27:40.170 dgt-vcn01.kyivstar.ua vcenter-server: User VSPHERE.LOCAL\SRM-aa73c0b3-fc8b-4acc-bc07-94a3d93c7386@127.0.0.1 logged in as VMware vim-java 1.0	dgt-vcn01.kyivstar.ua	v4_5c26184d	com.vmware.vim25.UserLoginSessionEvent	VSPHERE.LOCAL\SRM-aa73c0b3-fc8b-4acc-bc07-94a3d93c7386	dgt-vcn01.kyivstar.ua	vcenter-server	VSPHERE.LOCAL\SRM-aa73c0b3-fc8b-4acc-bc07-94a3d93c7386	127.0.0.1	VMware vim-java 1.0
Nov 19, 2023, 6:27:20 PM	2023-11-19 16:27:20.384 dgt-vcn01.kyivstar.ua vcenter-server: User VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a@127.0.0.1 logged in as VMware vim-java 1.0	dgt-vcn01.kyivstar.ua	v4_5c26184d	com.vmware.vim25.UserLoginSessionEvent	VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a	dgt-vcn01.kyivstar.ua	vcenter-server	VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a	127.0.0.1	VMware vim-java 1.0
Nov 19, 2023, 6:27:20 PM	2023-11-19 16:27:20.071 dgt-vcn01.kyivstar.ua vcenter-server: User VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a@127.0.0.1 logged in as VMware vim-java 1.0	dgt-vcn01.kyivstar.ua	v4_5c26184d	com.vmware.vim25.UserLoginSessionEvent	VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a	dgt-vcn01.kyivstar.ua	vcenter-server	VSPHERE.LOCAL\vpxd-extension-b18c2f92-372c-11e3-8236-000c29a33a8a	127.0.0.1	VMware vim-java 1.0
Nov 19, 2023, 6:27:15 PM	2023-11-19 16:27:15.772 lvv-vcn01.kyivstar.ua vcenter-server: User VSPHERE.LOCAL\SRM-799c38ce-abe2-4a89-abcf-35eb89bc5dcf@127.0.0.1 logged in as VMware vim-java 1.0	lvv-vcn01.kyivstar.ua	v4_5c26184d	com.vmware.vim25.UserLoginSessionEvent	VSPHERE.LOCAL\SRM-799c38ce-abe2-4a89-abcf-35eb89bc5dcf	lvv-vcn01.kyivstar.ua	vcenter-server	VSPHERE.LOCAL\SRM-799c38ce-abe2-4a89-abcf-35eb89bc5dcf	127.0.0.1	VMware vim-java 1.0
Nov 19, 2023, 6:27:01 PM	2023-11-19 16:27:01.601 lvv-vcn01.kyivstar.ua vcenter-server: User VSPHERE.LOCAL\apmmon@10.44.4.113 logged in as pyvmomi Python/3.8.17 (Linux; 3.10.0-1160.53.1.el7.x86_64; x86_64)	lvv-vcn01.kyivstar.ua	v4_5c26184d	com.vmware.vim25.UserLoginSessionEvent	VSPHERE.LOCAL\apmmon	lvv-vcn01.kyivstar.ua	vcenter-server	VSPHERE.LOCAL\apmmon	10.44.4.113	pyvmomi Python/3.8.17



https://excg2019-dgt01.kyivstar.ua/ecp/

Exchange admin center

NAME	ACTIVE ON SERVER	SERVERS WITH COPIES	STATUS	BAD COPY COUNT
backup-e16-08	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-WHG01	Mounted	0
backup-e19-01	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
backup-e19-02	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-DGT01,EXCG2...	Mounted	0
backup-e19-03	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
backup-e19-04-new	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01	Mounted	0
backup-e19-05-new	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-DGT01	Mounted	0
backup-e19-06-new	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01	Mounted	0
backup-e19-07-new	EXCG2019-DGT01	EXCG2019-DGT01	Mounted	0
backup-e19-09	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-DGT01	Mounted	0
backup-e19-10	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-WHG01	Mounted	0
MDB-01	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-02	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-03	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
MDB-04	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-05	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-06	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
MDB-07	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-08	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-09	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
MDB-10	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01,EXCG20...	Mounted	0
MDB-11	EXCG2019-WHG01	EXCG2019-WHG01,EXCG2019-LV01,EXCG20...	Mounted	0
MDB-12	EXCG2019-DGT01	EXCG2019-DGT01,EXCG2019-LV01,EXCG201...	Mounted	0
restore-partial-backup-e16-...	EXCG2019-LV01	EXCG2019-LV01,EXCG2019-WHG01	Mounted	0

1 selected of 23 total

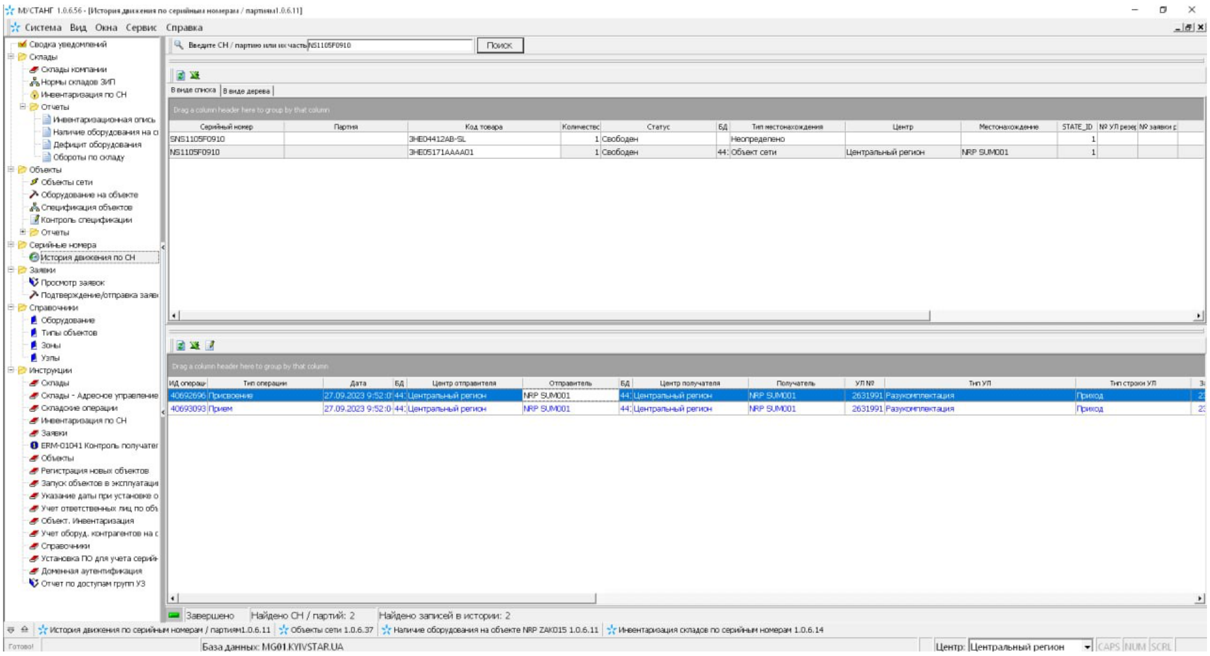
backup-e16-08

Database availability group:
exch2019dag

Servers
EXCG2019-DGT01
EXCG2019-WHG01

Database copies
backup-e16-08\EXCG2019-DGT01
Active Mounted
Copy queue length: 0
Content index state: NotApplicable
View details

backup-e16-08\EXCG2019-WHG01
Passive Healthy
Copy queue length: 0
Content index state: NotApplicable
Suspend | Activate | Remove
View details



МУСТАНГ 1.0.6.56 - [История движения по серийным номерам / партиям1.0.6.11]

Введите СН / партию или их часть: NS1105F0910

Серийный номер	Партия	Код товара	Количестс	Статус	БД	Тип местонахождения	Центр	Местонахождение	STATE_ID	№ УЛ резер	№ заявки р
SNS1105F0910		3HE04412AB-SL	1	Свободен		Неопределено			1		
NS1105F0910		3HE05171AAAA01	1	Свободен	44:	Объект сети	Центральный регион	NRP SUM001	1		

ИД операц	Тип операции	Дата	БД	Центр отправителя	Отправитель	БД	Центр получателя	Получатель	УЛ №	Тип УЛ	Тип строки УЛ	З
40692696	Присвоение	27.09.2023 9:52:0	44:	Центральный регион	NRP SUM001	44:	Центральный регион	NRP SUM001	2631991	Разукомплектация	Приход	2
40693093	Прием	27.09.2023 9:52:0	44:	Центральный регион	NRP SUM001	44:	Центральный регион	NRP SUM001	2631991	Разукомплектация	Приход	2

Завершено | Найдено СН / партий: 2 | Найдено записей в истории: 2

История движения по серийным номерам / партиям1.0.6.11 | Объекты сети 1.0.6.37 | Наличие оборудования на объекте NRP ZAK015 1.0.6.11 | Инвентаризация складов по серийным номерам 1.0.6.14

Готово! | База данных: MG01.KYIVSTAR.UA | Центр: Центральный регион | CAPS | NUM | SCRL

Source by "Sontsepok"

According to Victor Zhora, the Telegram channel "Sontsepok" is a "dumping ground" for the GRU, where groups like APT28 and Sandworm deposit the results of their activities.

Vityuk confirmed that there is a high likelihood that the Sandworm hacking group, a unit of Russian military intelligence, was behind it. Sandworm has previously carried out cyberattacks on Ukrainian targets, including telecommunication operators and internet service providers.

Vityuk revealed that SBU investigators are still working to determine how the breach of "Kyivstar" occurred and what type of malware was used for the intrusion. He added that it could have been phishing, assistance from within, or something else.

Cybersecurity experts speculate that even if it was an inside job, an insider assisting the hackers did not have a high level of access within the company. This is because the hackers utilized software designed for stealing password hashes. Samples of this malicious software have been collected and are undergoing analysis, Vityuk added.

Recovery.

- On December 12, 2023, "Kyivstar" began restoring access to fixed-line communication services and gradually started restoring mobile communication. Meanwhile, the Ministry of Internal Affairs of Ukraine warned about scammers exploiting phishing links with fake messages purportedly from "Kyivstar" regarding the restoration timeline and compensation to subscribers.

- On December 14, 2023, “Kyivstar” enabled voice calls and restored home internet service to 93%.
- On December 15, 2023, “Kyivstar” activated mobile internet across the entire controlled territory of Ukraine, including 4G standard.
- On December 21, 2023, “Kyivstar” announced the complete restoration of all essential services affected by the hacker attack. Earlier, the company assured that subscriber information and personal data remained secure. After recovering from the cyberattack, the company decided to waive the scheduled tariff payments for all its users.

Consequences.

Due to the extensive disruption caused by the cyberattack, “Kyivstar” filed a lawsuit against the interference in the network's operation. The estimated damages are in the “billions of hryvnias”.

Orange España

One of the largest mobile operators in Spain has officially announced the restoration of its services after a cyberattack that caused a failure in the company's internet infrastructure.

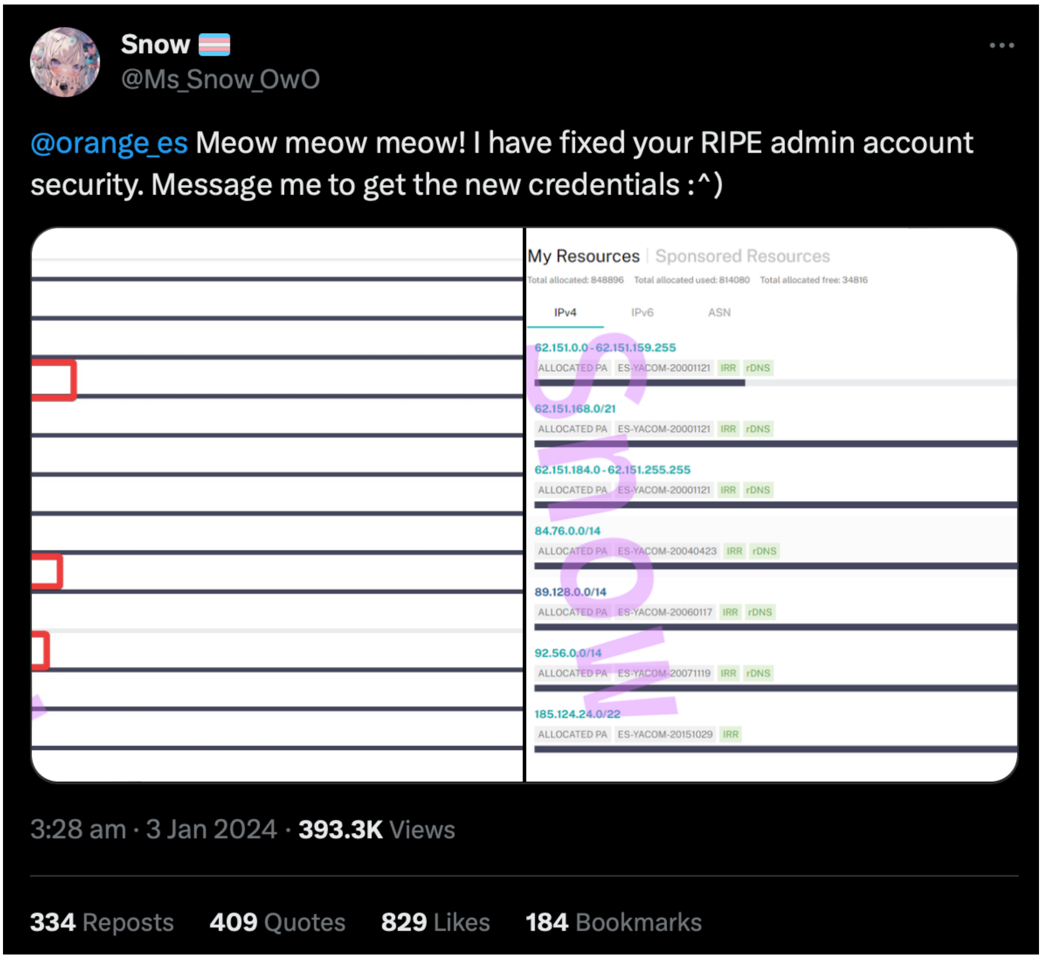
Through its social media account, on January 3, 2024, Orange España spoke about the incident that occurred and its impact on customers. There was no official comment on whether the internet outage directly affected the Madrid-based company's mobile service, but the outage lasted about three hours in total.

What is known?

An attacker made some changes to the RIPE Orange España account, causing Border Gateway Protocol (BGP) routing to fail and significant traffic loss.

Additionally.
RIPE is a Regional Internet Registry (RIR) that oversees the allocation and registration of IP addresses and Autonomous System (AS) numbers in Europe, Central Asia, Russia and West Asia.

A hacker on X with a newly created account called “Ms_Snow_OwO” posted screenshots showing how they hacked the Orange RIPE NCC (Network Coordination Center) account using the password ‘ripeadmin’.



Snow
@Ms_Snow_OwO

@orange_es Meow meow meow! I have fixed your RIPE admin account security. Message me to get the new credentials :^)

My Resources | Sponsored Resources
Total allocated: 848896 Total allocated used: 814080 Total allocated free: 34816

IPv4 IPv6 ASN

62.151.0.0 - 62.151.159.255
ALLOCATED PA ES-YACOM-20001121 IRR rDNS

62.151.168.0/21
ALLOCATED PA ES-YACOM-20001121 IRR rDNS

62.151.184.0 - 62.151.255.255
ALLOCATED PA ES-YACOM-20001121 IRR rDNS

84.76.0.0/14
ALLOCATED PA ES-YACOM-20040423 IRR rDNS

89.128.0.0/14
ALLOCATED PA ES-YACOM-20060117 IRR rDNS

92.56.0.0/14
ALLOCATED PA ES-YACOM-20071119 IRR rDNS

185.124.24.0/22
ALLOCATED PA ES-YACOM-20151029 IRR

3:28 am · 3 Jan 2024 · **393.3K** Views

334 Reposts **409** Quotes **829** Likes **184** Bookmarks

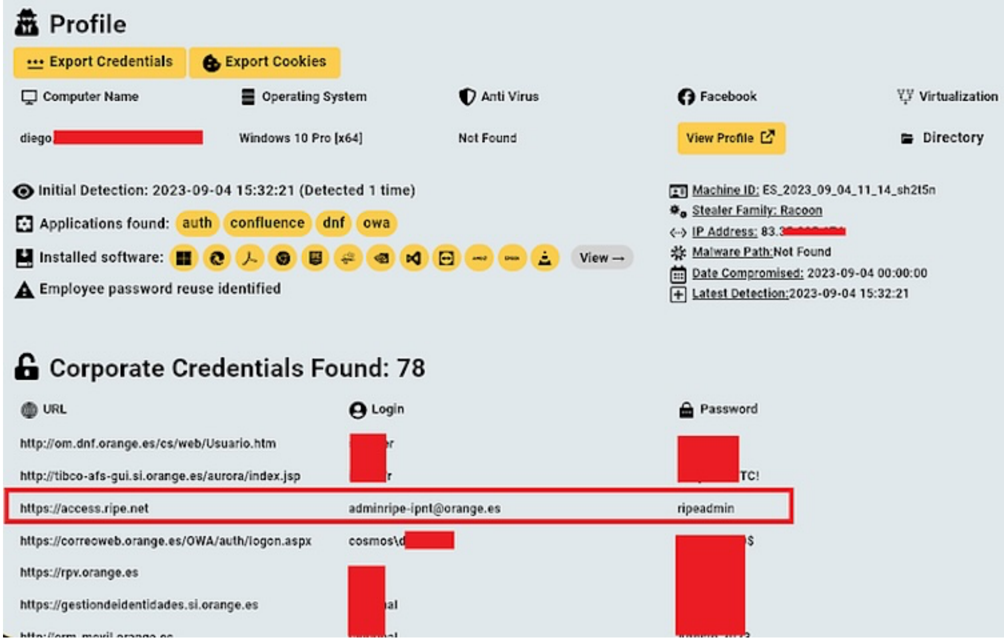
Source by "Snow"

"I've fixed the security of your RIPE administrator account. Send me a message to get the new credentials", they said. "I was just looking into public leaks of bot data and came across the ripe account with the password 'ripeadmin' and no 2FA, no SE (social engineering) at all". The attacker even shared a video detailing how he managed to access and compromise the network.

Threat intelligence company Hudson Rock, after analyzing the images sent, traced the hack to a computer belonging to an employee of Orange España, which was infected with Raccoon type Infostealer since September 4, 2023. Among the corporate credentials identified on the machine, the employee had certain credentials for 'https://access.ripe[.]net' using the email address that was compromised (adminripe-ipnt@orange.es).

"It is also worth noting that the password that was used on Orange's RIPE administrator account was 'ripeadmin' which is ridiculously weak" – "Snow"

The attacker later confirmed Hudson Rock's findings by tweeting that they had found the account in a public leak of stolen data.



Profile

Computer Name	Operating System	Anti Virus	Facebook	Virtualization
diego[redacted]	Windows 10 Pro [x64]	Not Found	View Profile	Directory

Initial Detection: 2023-09-04 15:32:21 (Detected 1 time)
Applications found: auth confluence dnf owa
Installed software:
Employee password reuse identified

Machine ID: ES_2023_09_04_11_14_sh2t5n
Stealer Family: Racoon
IP Address: 83.3[redacted]
Malware Path:Not Found
Date Compromised: 2023-09-04 00:00:00
Latest Detection:2023-09-04 15:32:21

Corporate Credentials Found: 78

URL	Login	Password
http://om.dnf.orange.es/cs/web/Usuario.htm	[redacted]r	[redacted]
http://tibco-afs-gui.si.orange.es/aurora/index.jsp	r	TC!
https://access.ripe.net	adminripe-ipnt@orange.es	ripeadmin
https://correoweb.orange.es/OWA/auth/logon.aspx	cosmos\d[redacted]	[redacted]$
https://rpv.orange.es	[redacted]	
https://gestiondeidentidades.si.orange.es	al	

Image by Hudson Rock

“I was just looking into public leaks of bot data and came across the ripe account with the password ‘ripeadmin’ and no 2FA, No SE at all”

When asked why they hacked the account, the attacker said they did it for the “lulz”, or in other words, for laughs.

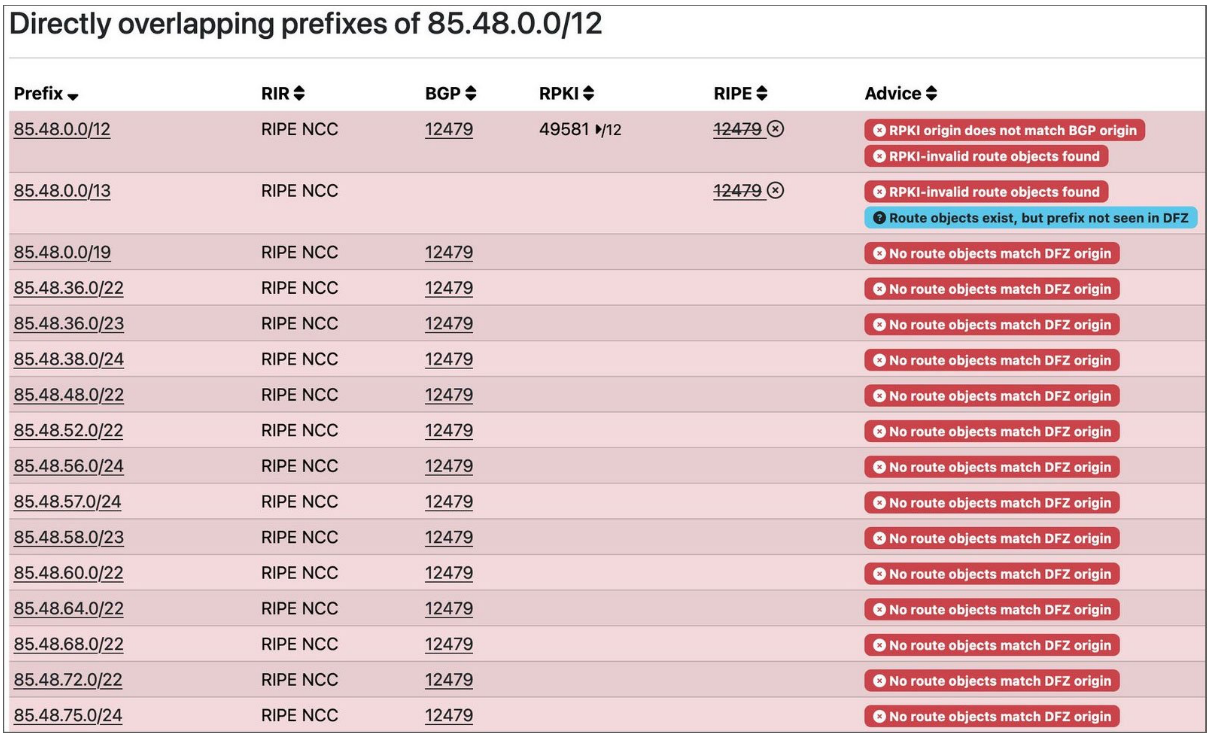
Key events.

With access to the RIPE account, the hacker manipulated the way Orange's Internet addresses were perceived by the Border Gateway Protocol (BGP), a key component for managing global digital traffic.

Additionally.
BGP serves as a set of rules that define optimal data routes.

In addition, the hacker changed the AS number associated with Orange IP addresses. When properly assigned, AS numbers allow networks to exchange information on the Internet.

The attacker created an invalid Resource Public Key Infrastructure (RPKI) configuration for Orange España. RPKI is supposed to help secure BGP routing, but in this incident the hacker used it to ensure that switching to an AS number would cause problems.

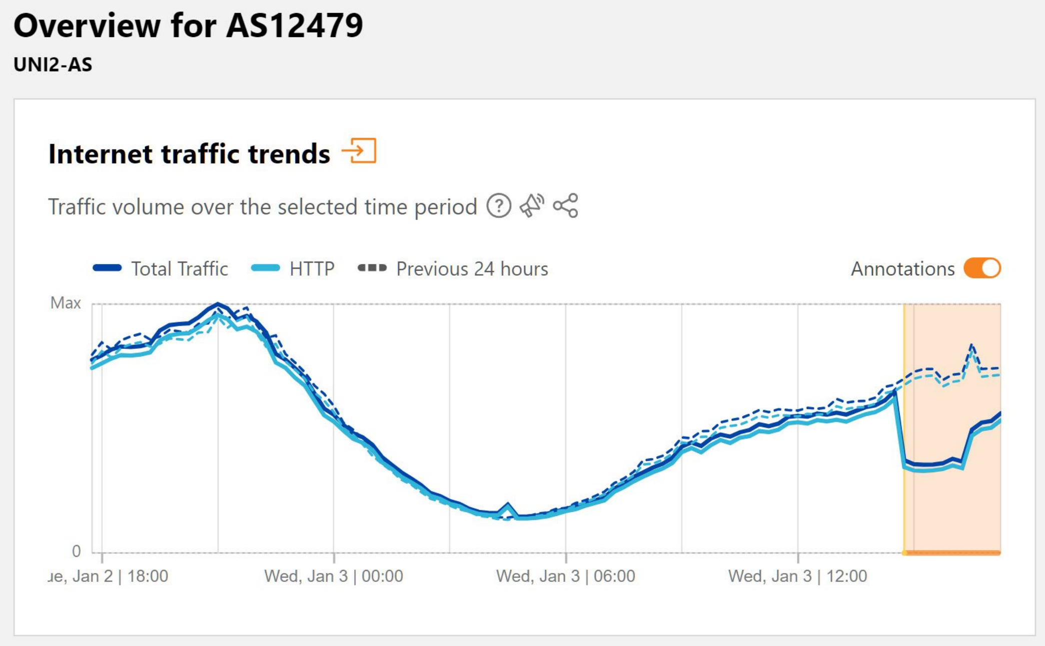


Directly overlapping prefixes of 85.48.0.0/12

Prefix ▾	RIR ⇕	BGP ⇕	RPKI ⇕	RIPE ⇕	Advice ⇕
85.48.0.0/12	RIPE NCC	12479	49581 ▸/12	~~12479~~ ⊗	⊗ RPKI origin does not match BGP origin ⊗ RPKI-invalid route objects found
85.48.0.0/13	RIPE NCC			~~12479~~ ⊗	⊗ RPKI-invalid route objects found ? Route objects exist, but prefix not seen in DFZ
85.48.0.0/19	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.36.0/22	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.36.0/23	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.38.0/24	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.48.0/22	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.52.0/22	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.56.0/24	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.57.0/24	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.58.0/23	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.60.0/22	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.64.0/22	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.68.0/22	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.72.0/22	RIPE NCC	12479			⊗ No route objects match DFZ origin
85.48.75.0/24	RIPE NCC	12479			⊗ No route objects match DFZ origin

Source by Cañizares

This resulted in a performance issue on the Orange España network between 14:45 and 16:15 UTC, which can be seen in the Cloudflare traffic graph for AS12479.



Overview for AS12479

UNI2-AS

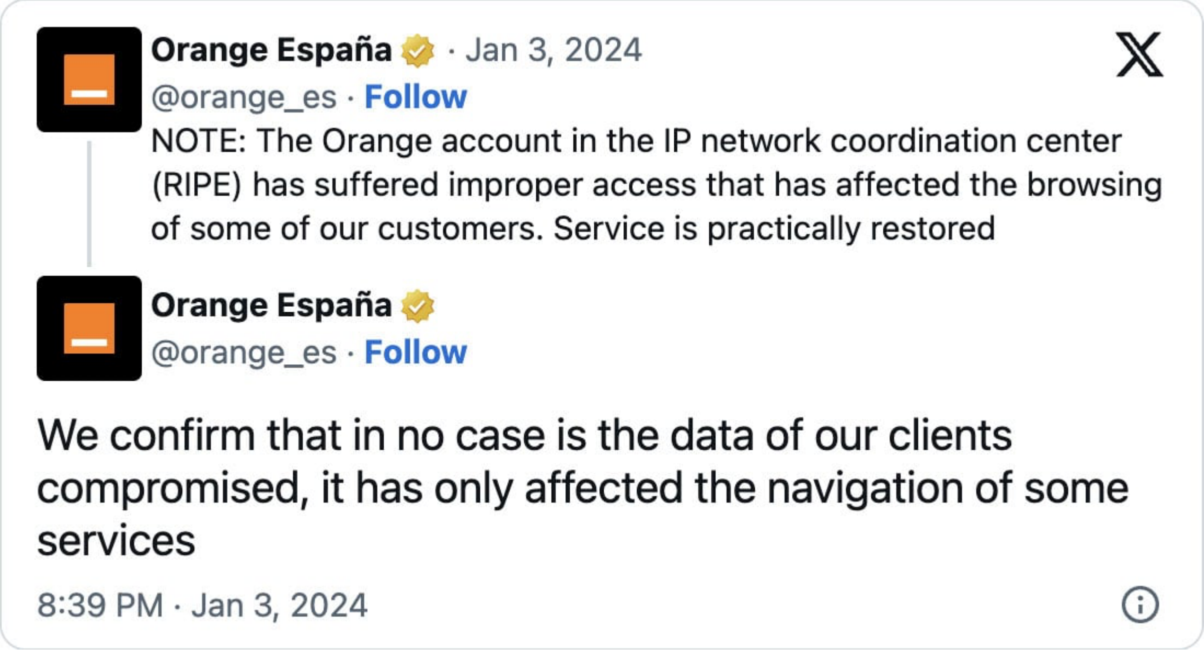
Internet traffic trends

Traffic volume over the selected time period

Source by Cloudflare

Recovery.

Orange España said on X that there was no compromise of customer data and clarified that the incident only affected the navigation of some services.



Orange España · Jan 3, 2024
@orange_es · Follow
NOTE: The Orange account in the IP network coordination center (RIPE) has suffered improper access that has affected the browsing of some of our customers. Service is practically restored

Orange España
@orange_es · Follow

We confirm that in no case is the data of our clients compromised, it has only affected the navigation of some services

8:39 PM · Jan 3, 2024

Source by Orange España

In response to the situation, RIPE released a statement acknowledging the investigation into the compromised account resulted in temporary disruption to the account owner.

RIPE has assured that access has been restored to the rightful owner of the account, and they are actively working together to ensure the integrity of the account. The information security team is conducting ongoing investigations to determine if other accounts were affected.

RIPE emphasized its commitment to contacting affected account holders directly, urging them to update their passwords and enable multi-factor authentication.

In response to inquiries regarding the lack of mandatory two-factor authentication, RIPE stated that they are accelerating the implementation of 2FA by making it mandatory for all RIPE NCC Access accounts as soon as possible.

Consequences.

The worst part of the incident is that "Snow's" motives are still unknown. Given the way the attacker behaved when changing the global routing table, the researchers believe they were simply experimenting with access to see what could be done.

Additionally, it's possible that the attacker was slow to raise awareness of the weak password and only escalated when he saw the company's soft response.

'Sea Turtle' hackers target Netherlands

During 2023, an Advanced Persistent Threat (APT) actor tracked as Sea Turtle (aliases: Cosmic Wolf, Marbled Dust, Silicon, and Teal Kurma, UNC1326) conducted successful espionage campaigns targeting government, telecommunications, media, and non-governmental organizations, as well as ISPs and IT service providers in the Netherlands.

Sea Turtle was first identified by Cisco Talos in April 2019 and is believed to be sponsored by the Turkish government. Their primary attack method involves DNS hijacking, redirecting targets attempting to request a specific domain to a server controlled by the threat. This server is capable of collecting victims' credentials.

According to the Talos, Sea Turtle poses a more serious threat than DNS espionage due to the actor's methodology of targeting various registrars and DNS registries. Microsoft also reported that the adversary is collecting intelligence to serve Turkey's interests, focusing on countries such as Armenia, Cyprus, Greece, Iraq and Syria.

The Netherlands security firm Hunt & Hackett analyzed the campaigns and found that the infrastructure of the targets was vulnerable to supply chain and island-hopping attacks. Sea Turtle used these flaws to collect politically motivated information, including personal data on minority groups and potential dissidents.

According to analysts, this APT is considered "moderate". Hackers mainly focus on exploiting available vulnerabilities to gain initial access to organizations.

Compromise cPanel and SnappyTCP Malware.

Sea Turtle, previously known for DNS hijacking, has deployed new TTPs in new campaigns. During one of the campaigns in 2023, Sea Turtle reportedly used a compromised account on cPanel, the web hosting control panel, from a VPN IP address.

The cPanel account was used to login via SSH from an IP address belonging to the hosting provider. This allowed the Sea Turtle to enter the target's IT infrastructure.

The APT then used the Unix Bash shell to execute malicious commands. The hacking group used a reverse TCP shell for Linux/Unix operating systems called SnappyTCP (available on GitHub).

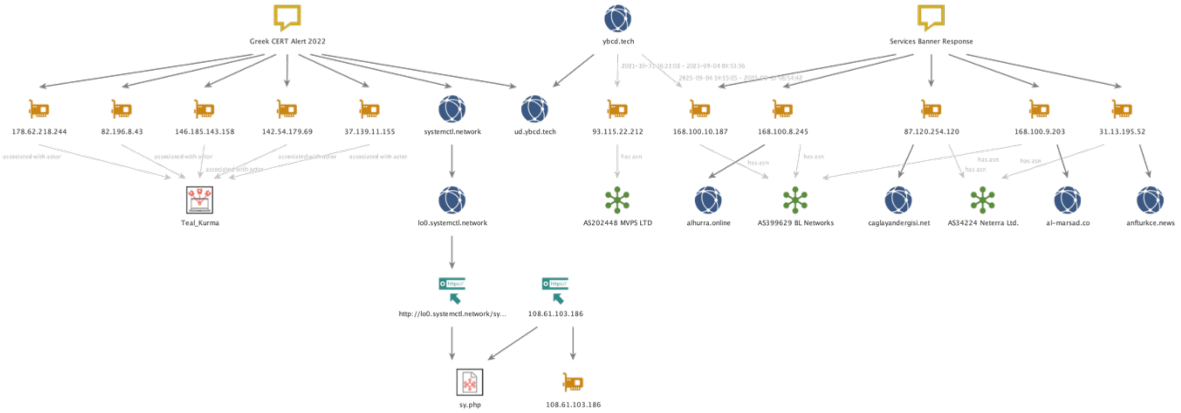
Additionally.
SnappyTCP can be used to steal data, install additional malware, or perform other attacks.

Next, the Adminer tool was installed in the public web directory of one of the compromised cPanel accounts.

Additionally.
Adminer is a public database management tool that can be used to remotely log into a system's MySQL service.

Finally, the attacker sent commands to the system using SnappyTCP to create a copy of the email archive in the public web directory of the website accessible from the Internet.

The email archive was created using 'tar', a utility designed to collect files into a single archive file for distribution or backup.



Source by PwC. Sea Turla infrastructure. Some of the pivots made to identify additional and more recent infrastructure

Recommendation.

To mitigate the risks associated with such attacks, organizations are encouraged to implement strong password policies, use two-factor authentication (2FA), limit the number of login attempts to reduce the likelihood of brute force attacks, monitor SSH traffic, and keep all systems and software up-to-date.

For more details about Sea Turle you can find in Strike Ready and PwC Threat Intelligence reports.

T-Mobile US

First T-Mobile security breach.

Over the past year, T-Mobile US has faced several cyberattacks. In early 2023, the company suffered the second most impactful cybersecurity incident in its lifetime, resulting in the data theft of approximately 37 million users.

According to the content of the statement of T-Mobile US to the US Securities and Exchange Commission, access to a limited set of customer account data was disclosed. However, the company claims that sensitive user data was not compromised by attackers.

Via API.

According to official information, the incident became known on January 5, 2023. During the investigation, it was determined that the attackers had access from around November 25, 2022, and the data was obtained through an enterprise application programming interface (API) without authorization.

T-Mobile noted that the malicious activity was completely stopped within 24 hours of detection. However, the company later announced that this incident could cause significant losses. However, which ones exactly, official sources do not report.

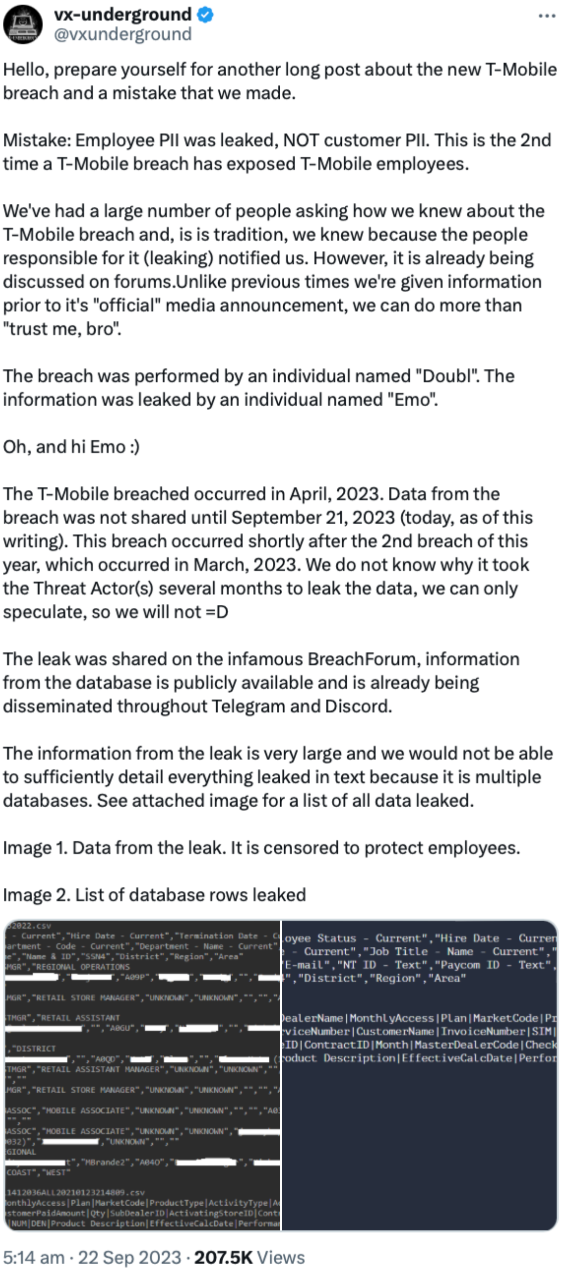
Second T-Mobile security breach.

In April 2023, T-Mobile disclosed a second data breach in which attackers had access to the information of 836 customers beginning in late February 2023. Official T-Mobile sources reported that the volume of compromised information is very large and exposes affected individuals to further theft of confidential data and targeted phishing attacks.

Between late February and March 2023, an attacker was found to have accessed restricted information from multiple T-Mobile accounts.

Later, on September 22, “vx-underground” published a tweet about 90 GB of personal data of T-Mobile employees being stolen as a result of the data leak.

This was linked to the April hack of Connectivity Source, a T-Mobile retailer. T-Mobile itself has denied wrongdoing and does not appear to have been directly implicated in the incident.



vx-underground
@vxunderground

Hello, prepare yourself for another long post about the new T-Mobile breach and a mistake that we made.

Mistake: Employee PII was leaked, NOT customer PII. This is the 2nd time a T-Mobile breach has exposed T-Mobile employees.

We've had a large number of people asking how we knew about the T-Mobile breach and, is is tradition, we knew because the people responsible for it (leaking) notified us. However, it is already being discussed on forums.Unlike previous times we're given information prior to it's "official" media announcement, we can do more than "trust me, bro".

The breach was performed by an individual named "Doubl". The information was leaked by an individual named "Emo".

Oh, and hi Emo :)

The T-Mobile breached occurred in April, 2023. Data from the breach was not shared until September 21, 2023 (today, as of this writing). This breach occurred shortly after the 2nd breach of this year, which occurred in March, 2023. We do not know why it took the Threat Actor(s) several months to leak the data, we can only speculate, so we will not =D

The leak was shared on the infamous BreachForum, information from the database is publicly available and is already being disseminated throughout Telegram and Discord.

The information from the leak is very large and we would not be able to sufficiently detail everything leaked in text because it is multiple databases. See attached image for a list of all data leaked.

Image 1. Data from the leak. It is censored to protect employees.

Image 2. List of database rows leaked

```
2022.csv
 - Current","Hire Date - Current","Termination Date - C
artment - Code - Current","Department - Name - Current"
e","Name & ID","SSN4","District","Region","Area"
MGR","REGIONAL OPERATIONS
[redacted],"[redacted]","A09P","[redacted]","[redacted]","","[redacted]

MGR","RETAIL STORE MANAGER","UNKNOWN","UNKNOWN","","","

TMGR","RETAIL ASSISTANT
[redacted]","","A0GU","[redacted]","[redacted]","","[redacted]

,"DISTRICT
[redacted]","","A0QD","[redacted]","[redacted]","","[redacted] (
TMGR","RETAIL ASSISTANT MANAGER","UNKNOWN","UNKNOWN",""
",""

MGR","RETAIL STORE MANAGER","UNKNOWN","UNKNOWN","","",

ASSOC","MOBILE ASSOCIATE","UNKNOWN","UNKNOWN","","","A0
"",""
ASSOC","MOBILE ASSOCIATE","UNKNOWN","UNKNOWN","[redacted]
032)","[redacted]","UNKNOWN","",""
GIONAL
[redacted]t","MBrande2","A040","[redacted]","[redacted]
COAST","WEST"

1412036ALL20210123214809.csv
onthlyAccess|Plan|MarketCode|ProductType|ActivityType|A
stomerPaidAmount|Qty|SubDealerID|ActivatingStoreID|Cont
|NUM|DEN|Product Description|EffectiveCalcDate|Performa
```

```
oyee Status - Current","Hire Date - Curren
 - Current","Job Title - Name - Current","
"E-mail","NT ID - Text","Paycom ID - Text",
","District","Region","Area"


DealerName|MonthlyAccess|Plan|MarketCode|Pr
viceNumber|CustomerName|InvoiceNumber|SIM|
ID|ContractID|Month|MasterDealerCode|Check
roduct Description|EffectiveCalcDate|Perfor
```

5:14 am · 22 Sep 2023 · **207.5K** Views

Source by "vx-underground"

Recovery.
T-Mobile has reset account PINs for affected customers and is now offering them two years of free credit monitoring and identity theft detection through TransUnion myTrueIdentity.

Other cybersecurity issues.

It's worth noting that T-Mobile is not the first to face significant data security issues.

- **In August 2018**, T-Mobile released details of a cyberattack that compromised the information of approximately 3% of all T-Mobile customers.

- **In November 2019**, an attacker gained access to the account information of a certain number of prepaid customers (the exact number of affected customers was not disclosed).
- **In March 2020**, a data breach caused by a hacking attack on the email provider exposed the personal and financial information of some of its customers (the exact number of affected customers was not disclosed).
- **In December 2020**, attackers stole Customer proprietary network information (CPNI), including phone numbers and call records.
- **In February 2021**, attackers gained unauthorized access to an internal T-Mobile application.
- **In August 2021**, the company suffered its biggest impact, after an investigation revealed the data theft of more than 76.6 million current and former customers. American hacker John Brinns claimed responsibility for the attack. He claimed that T-Mobile maintained unsecured routers and weak addresses that allowed him to steal information from more than 100 servers. He did not explain what exactly he did with the information, but most of the compromised data is sold on the Darknet for use in identity theft or other cyberattacks. Brynn said only that the purpose of the T-Mobile attack was "revenge against the United States for the kidnapping and torture of John Erin Binns".

  The 2021 data breach was T-Mobile's largest loss of customer information. That made many tech experts wary of the company's ability to learn from its mistakes and left T-Mobile in a weak position in future litigation.

  Faced with a class-action lawsuit after breaching its customer privacy and data protection policies, T-Mobile has agreed to pay $350 million to class-action plaintiffs and invest $150 million in its cybersecurity systems.

- **In April 2022**, the hacker group Lapsus$ stole the source code for a number of the company's projects.

Conclusion

With all the recent data breaches, it's hard to believe that all of your personal information isn't just floating around, waiting to be used. It would be great if all companies affected by cyberattacks learned from their mistakes and took even more precautions to protect their systems and networks.

The following practices are partial recommendations for strengthening defenses against cyber threats:

1. Tracking cyber incidents using SIEM, IPS and EDR systems.
2. Apply a strong password policy.
3. Introduction of mandatory two-factor authentication (2FA) for all users.
4. Limit the number of authorizations attempts in the systems.
5. Monitor SSH traffic.
6. Update systems and software in a timely manner.
7. Fill the database of indicators of compromise.
8. Educate your employees and customers on the rules of cyber hygiene, since, in practice, malicious actors, using social engineering, successfully manipulate users to obtain primary access.