

The Case of Encrochat

A Real-World Law-Enforcement Hack

Martin Albrecht

Sunoo Park

Michael Specter

Douglas Stebila

King's College London

New York University & NYU School of Law

Georgia Tech

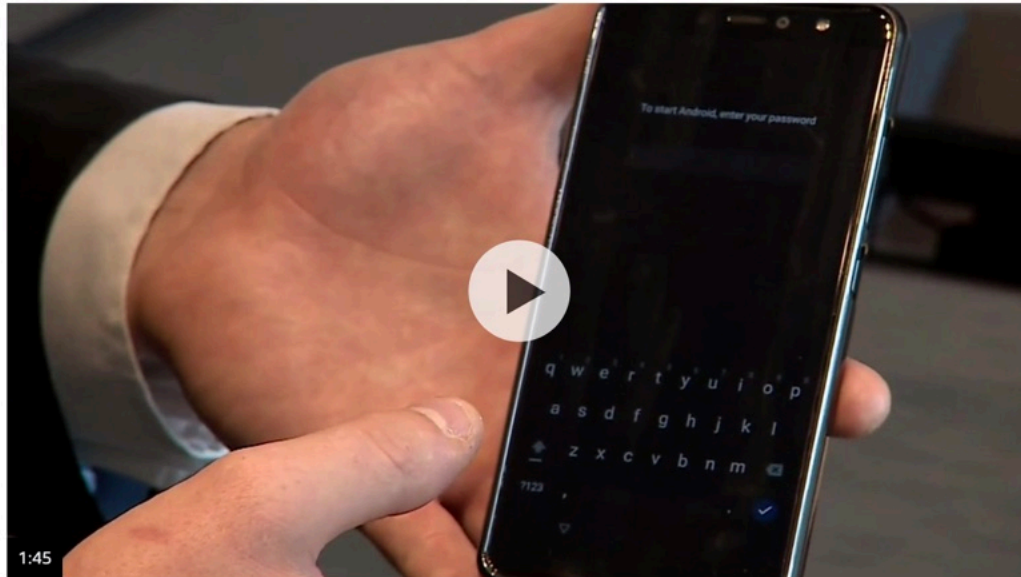
University of Waterloo

Hundreds arrested as crime chat network cracked

2 July 2020

By **Danny Shaw**, Home affairs correspondent

Share



The BBC's Tom Symonds is shown how a customised Android phone with EncroChat installed works

A top-secret communications system used by criminals to trade drugs and guns has been "successfully penetrated", says the National Crime Agency.

Chat users realised 'too late'

Analysis by BBC technology reporter David Molloy

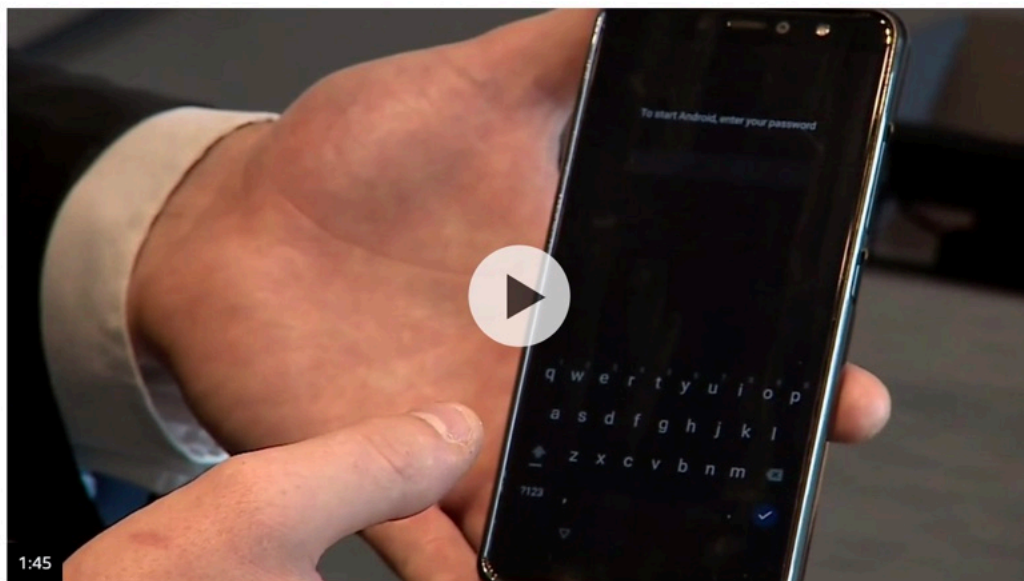
EncroChat sold encrypted phones with a guarantee of anonymity, with a range of special features to remove identifying information. The phones themselves cost roughly £900 (€1,000) each, with a subscription costing £1,350 (€1,500) for six months.

Hundreds arrested as crime chat network cracked

2 July 2020

By **Danny Shaw**, Home affairs correspondent

Share



The BBC's Tom Symonds is shown how a customised Android phone with EncroChat installed works

A top-secret communications system used by criminals to trade drugs and guns has been "successfully penetrated", says the National Crime Agency.

Major crime figures were among over 800 Europe-wide arrests after messages on EncroChat were intercepted and decoded.

Chat users realised 'too late'

Analysis by BBC technology reporter David Molloy

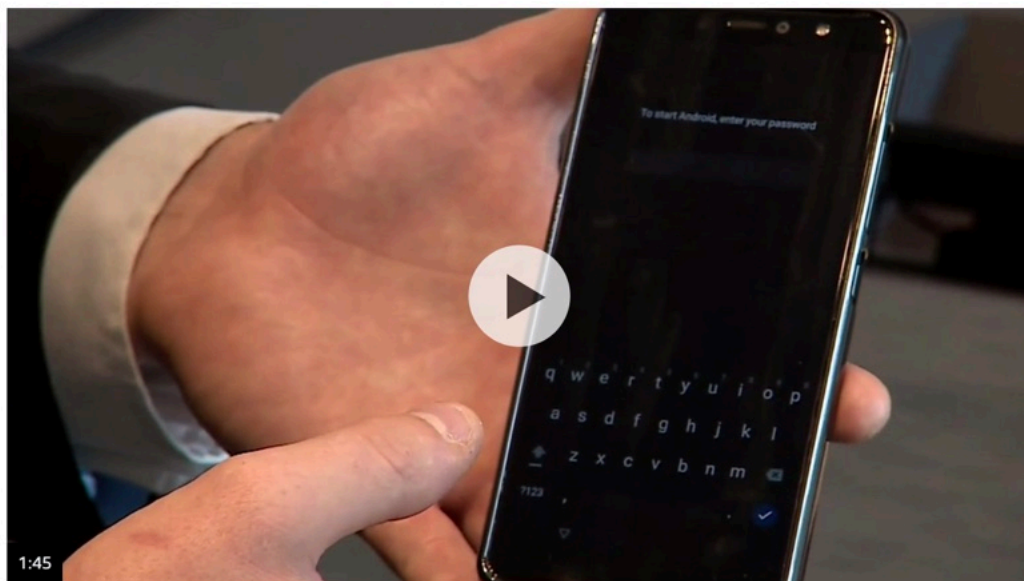
EncroChat sold encrypted phones with a guarantee of anonymity, with a range of special features to remove identifying information. The phones themselves cost roughly £900 (€1,000) each, with a subscription costing £1,350 (€1,500) for six months.

Hundreds arrested as crime chat network cracked

2 July 2020

By **Danny Shaw**, Home affairs correspondent

Share



The BBC's Tom Symonds is shown how a customised Android phone with EncroChat installed works

A top-secret communications system used by criminals to trade drugs and guns has been "successfully penetrated", says the National Crime Agency.

Major crime figures were among over 800 Europe-wide arrests after messages on EncroChat were intercepted and decoded.

Wil van Gemert, deputy executive director of Europol, told a press conference in the Hague that the hacking of the network had allowed the "disruption of criminal activities including violent attacks, corruption, attempted murders and large-scale drug transports".

Chat users realised 'too late'

Analysis by BBC technology reporter David Molloy

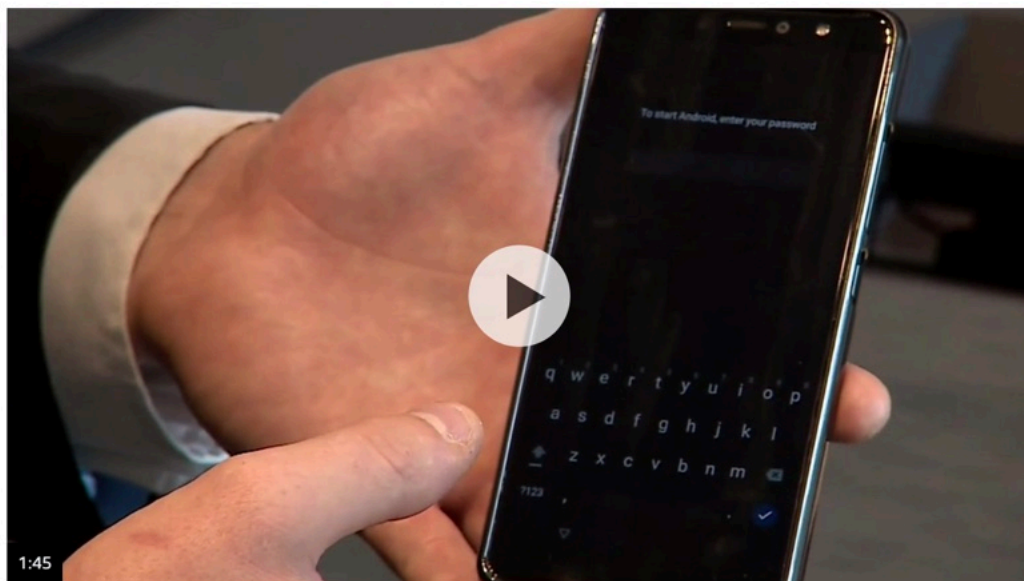
EncroChat sold encrypted phones with a guarantee of anonymity, with a range of special features to remove identifying information. The phones themselves cost roughly £900 (€1,000) each, with a subscription costing £1,350 (€1,500) for six months.

Hundreds arrested as crime chat network cracked

2 July 2020

By Danny Shaw, Home affairs correspondent

Share



1:45

The BBC's Tom Symonds is shown how a customised Android phone with EncroChat installed works

A top-secret communications system used by criminals to trade drugs and guns has been "successfully penetrated", says the National Crime Agency.

Major crime figures were among over 800 Europe-wide arrests after messages on EncroChat were intercepted and decoded.

Wil van Gemert, deputy executive director of Europol, told a press conference in the Hague that the hacking of the network had allowed the "disruption of criminal activities including violent attacks, corruption, attempted murders and large-scale drug transports".

More than two tonnes of drugs, several dozen guns and £54m in suspect cash have been seized, says the NCA.



Chat users realised 'too late'

Analysis by BBC technology reporter David Molloy

EncroChat sold encrypted phones with a guarantee of anonymity, with a range of special features to remove identifying information. The phones themselves cost roughly £900 (€1,000) each, with a subscription costing £1,350 (€1,500) for six months.

Hunderteste Festnahmen

Polizei hackt Krypto-Smartphones von Kriminellen

Europäischen Ermittlern ist ein großer Schlag gegen die organisierte Kriminalität gelungen. Ausgangspunkt war die Infiltration eines verschlüsselten Chat-Netzwerks.

02.07.2020, 18.43 Uhr



← Ads by Google

Send feedback

Why this ad? ↗

Hunderte Festnahmen

Polizei hackt Kriminellen

Europäischen Ermittlern
Ausgangspunkt war die I

02.07.2020, 18.43 Uhr



De Telegraaf

NIEUWS

SPORT

ENTERTAINMENT

FINANCIËEL

VROUW

LIFESTYLE

WAT U ZEGT



Abonneer voor
€0,99/week

Inloggen

De krant Video Podcast Puzzels 9 °C 3 km Klantenservice

Lees voor

Ruim 6500 arrestaties sinds oprollen van EncroChat

27 jun. 2023 in BUITENLAND



LILLE - Het kraken van de beveiligde communicatiedienst EncroChat, waar veel criminelen versleutelde berichten op verstuurden, heeft tot nu geleid tot 6558 arrestaties wereldwijd. Daarvan behoorden 197 tot de zwaarste categorie, maakten de Nederlandse en Franse autoriteiten dinsdag bekend tijdens een persconferentie in het Franse Lille.



© ANP

LAATSTE NIEUWS

- 21:43 **Verlamde patiënt kan dankzij deze oplossing potje schaken**
- 21:16 **PREMIUM Alarm om Russische dreiging richting NAVO: hoeveel zorgen moete...**
- 21:12 **PREMIUM Brits 'ping-pongen' over wegsturen van asielzoekers naar...**
- 20:19 **Zo komt zus Kim Jong-un aan gruwelijke bijnaam 'Duivelsvrouw'**
- 19:46 **PREMIUM Familie van aangereden Abdullah (17) in shock: 'Dader ging m...**
- 19:07 **Twintig Chinese gevechtsvliegtuigen opgemerkt in buurt van Taiwan**



Ads door Google

Feedback sturen

Waarom deze advertentie?

MEEST GELEZEN

10:59 | Buitenland

1 LIVE | 'Rusland maakt zich op voor grootschalige oorlog met NAVO, sneller dan westerse analisten denken'



Hunderte Festnahmen

Polizei hackt Kriminellen

Europäischen Ermittlern
Ausgangspunkt war die I

02.07.2020, 18.43 Uhr



De Telegraaf

NIEUWS

SPORT

ENTERTAINMENT

FINANCIËL

VROUW

LIFESTYLE

WAT U ZEGT



Abonneer voor
€0,99/week

Inloggen



Lees voor



Ruim 6500 arrestaties oprollen van EncroChat

27 jun. 2023 in BUITENLAND

LILLE - Het kraken van de beveiligde communicatie van criminelen versleutelde berichten op verstuurd berichten wereldwijd. Daarvan behoorden 197 tot Nederlandse en Franse autoriteiten dinsdag bekendmaken Franse Lille.



© ANP

De krant Video Podcast Puzzels 9 °C 3 km Klantenservice

LAATSTE NIEUWS

21:43 Verlamde patiënt kan dankzij deze oplossing potje schaken



Le Monde

Se connecter

S'abonner



ACTUALITÉS

ÉCONOMIE

VIDÉOS

DÉBATS

CULTURE

LE GOÛT DU MONDE

SERVICES



LE SALON DE L'EXECUTIVE EDUCATION

SAMEDI 23 MARS
Palais Brongniart, Paris

INSCRIPTION GRATUITE >

SOCIÉTÉ · CRIMINALITÉ ORGANISÉE

Criminalité organisée : le démantèlement de la messagerie EncroChat a permis d'arrêter plus de 6 500 personnes

Selon un premier bilan tiré par les agences européennes de coopération policière, Europol, et judiciaire, Eurojust, plus de sept mille années de peines de prison ont déjà été prononcées contre des utilisateurs, principalement actifs dans le trafic de drogue.

Par Jean-Pierre Stroobants (Bruxelles, bureau européen)

Publié le 27 juin 2023 à 16h28, modifié le 27 juin 2023 à 16h55 · Lecture 2 min.

Ajouter à vos sélections



Article réservé aux abonnés

Les enquêtes sont complexes, les procédures judiciaires longues, les personnes impliquées et leurs avocats prêts à en exploiter toutes les failles : face à la multiplication des questions sur le bilan exact du

PUBLICITÉ

CNEWA
Journey

Organisé par

Le Monde

L'OBS

Courrier international



Europe

Encrypted phone service 'Encrochat' shutdown leads to 6,500 arrests, Europol says

Reuters

June 27, 2023 7:58 AM EDT · Updated 9 months ago



Aa



[1/5] EncroChat and Europol logos are seen in this illustration taken, June 27, 2023. REUTERS/Dado Ruvic/Illustration
[Purchase Licensing Rights](#)

AMSTERDAM, June 27 (Reuters) - European policing agency Europol said on Tuesday that the takedown of Encrochat, an underground company that offered criminals supposedly secure encrypted communications, led to more than 6,500 arrests and 900 million euros (\$980 million) in seized assets.

The system had an estimated 60,000 users when it shut down abruptly in June 2020, and Europol revealed the following month that law enforcement officials had been intercepting users' communications for months.

← Ads by Google

Send feedback

Why this ad? ▸

Report this ad

Feedback

What was **Encrochat**?

Plan

- What was **Encrochat**?
- The **breach**
- The **legal process**
- **How we pieced it together** (so far)
- Some **takeaways** (so far)
- **Open questions**

What was Encrochat?

- A **communications service provider**
 - offering **modified Android smartphones**
 - with features including **e2ee messaging**



What was Encrochat?

EncroChatSure.com . . . Better Sure than sorry!

EncroChat® - Feature List

Advanced Off-the-Record Protocol

OTR is an electronic parallel of normal conversation happening in an empty room between two people.

Guaranteed Anonymity

Assurance of no association between customer accounts and SIM card or mobile device.

Customized Android Platform

Simple user settings centred on privacy and security. Completely encrypted as soon as you turn the power on.

Industry Leading Hardware

Customized to make security impregnable. Removal of Microphone, USB port, GPS and Camera.

Updates and Live Support

Directly receives enhancements and updates frequently, and the availability of live support if you encounter any problems while using our product.

Self-Destructible Messages

Making use of our advanced burn, a forced wiping of the messages can be performed through a timer countdown from the device of another user.

Panic Wipe

A user can wipe the data instantly just by typing the PIN on screen lock.

Password Wipe

All the data is wiped automatically after a certain number of unsuccessful password attempts.

Simplified Verification

Our Notary Verification process makes it far easier for the users to do the encryption.

Global Service


Supports CDMA, Quad-band GSM and UMTS in 120 countries and includes unlimited international SIM.

Tamper Proofing

Attack surfaces like recovery mode and ADB connectivity have been removed.

Secure Boot

The device performs a self check at the time of booting to make sure that the system files have not been tempered with.

A black smartphone with the EncroChat logo on the screen. The screen also shows a home indicator bar at the bottom with several app icons: a blue 'E' icon, a blue speech bubble icon, an orange envelope icon, a blue document icon, a green exclamation mark icon, and a red question mark icon.

EncroChatSure.com . . . Better Sure than sorry!

2

8

What was Encrochat?


- **Phone features**

- **Physically disconnected:** GPS, microphone, camera, USB port
- **Disabled:** Android debug bridge, recovery mode
- **Dual boot:** **Encrochat OS** & **Android OS**

EncroChatSure.com . . . Better Sure than sorry!

EncroChat® - Feature List

- Secure Boot**
The device performs a self check at the time of booting to make sure that the system files have not been tampered with.
- Advanced Off-the-Record Protocol**
OTR is an electronic parallel of normal conversation happening in an empty room between two people.
- Guaranteed Anonymity**
Assurance of no association between customer accounts and SIM card or mobile device.
- Customized Android Platform**
Simple user settings centred on privacy and security. Completely encrypted as soon as you turn the power on.
- Industry Leading Hardware**
Customized to make security impregnable. Removal of Microphone, USB port, GPS and Camera.
- Updates and Live Support**
Directly receives enhancements and updates frequently, and the availability of live support if you encounter any problems while using our product.
- Self-Destructible Messages**
Making use of our advanced burn, a forced wiping of the messages can be performed through a timer countdown from the device of another user.
- Panic Wipe**
A user can wipe the data instantly just by typing the PIN on screen lock.
- Password Wipe**
All the data is wiped automatically after a certain number of unsuccessful password attempts.
- Simplified Verification**
Our Notary Verification process makes it far easier for the users to do the encryption.
- Global Service**
Supports CDMA, Quad-band GSM and UMTS in 120 countries and includes unlimited international SIM.
- Tamper Proofing**
Attack surfaces like recovery mode and ADB connectivity have been removed.



EncroChatSure.com . . . Better Sure than sorry!

What was Encrochat?

- **Phone features**

- **Physically disconnected:** GPS, microphone, camera, USB port
- **Disabled:** Android debug bridge, recovery mode
- **Dual boot:** **Encrochat OS** & **Android OS**


- **Applications**

- **Encrochat:** e2ee messaging
- **Encrotalk:** ZRTP-based VOIP
- **Encronotes:** encrypted note-taking

EncroChatSure.com . . . Better Sure than sorry!

EncroChat® - Feature List

- Secure Boot**
The device performs a self check at the time of booting to make sure that the system files have not been tampered with.
- Advanced Off-the-Record Protocol**
OTR is an electronic parallel of normal conversation happening in an empty room between two people.
- Guaranteed Anonymity**
Assurance of no association between customer accounts and SIM card or mobile device.
- Customized Android Platform**
Simple user settings centred on privacy and security. Completely encrypted as soon as you turn the power on.
- Industry Leading Hardware**
Customized to make security impregnable. Removal of Microphone, USB port, GPS and Camera.
- Updates and Live Support**
Directly receives enhancements and updates frequently, and the availability of live support if you encounter any problems while using our product.
- Self-Destructible Messages**
Making use of our advanced burn, a forced wiping of the messages can be performed through a timer countdown from the device of another user.
- Panic Wipe**
A user can wipe the data instantly just by typing the PIN on screen lock.
- Password Wipe**
All the data is wiped automatically after a certain number of unsuccessful password attempts.
- Simplified Verification**
Our Notary Verification process makes it far easier for the users to do the encryption.
- Global Service**
Supports CDMA, Quad-band GSM and UMTS in 120 countries and includes unlimited international SIM.
- Tamper Proofing**
Attack surfaces like recovery mode and ADB connectivity have been removed.



EncroChatSure.com . . . Better Sure than sorry!

What was Encrochat?

- **Phone features**

- **Physically disconnected:** GPS, microphone, camera, USB port
- **Disabled:** Android debug bridge, recovery mode
- **Dual boot:** **Encrochat OS** & **Android OS**

- **Applications**

- **Encrochat:** e2ee messaging
- **Encrotalk:** ZRTP-based VOIP
- **Encronotes:** encrypted note-taking

(Confusingly, "Encrochat" refers to both the **devices** & the **messaging app**.) 8

EncroChatSure.com . . . Better Sure than sorry!

EncroChat® - Feature List

- Secure Boot**
The device performs a self check at the time of booting to make sure that the system files have not been tampered with.
- Advanced Off-the-Record Protocol**
OTR is an electronic parallel of normal conversation happening in an empty room between two people.
- Guaranteed Anonymity**
Assurance of no association between customer accounts and SIM card or mobile device.
- Customized Android Platform**
Simple user settings centred on privacy and security. Completely encrypted as soon as you turn the power on.
- Industry Leading Hardware**
Customized to make security impregnable. Removal of Microphone, USB port, GPS and Camera.
- Updates and Live Support**
Directly receives enhancements and updates frequently, and the availability of live support if you encounter any problems while using our product.
- Self-Destructible Messages**
Making use of our advanced burn, a forced wiping of the messages can be performed through a timer countdown from the device of another user.
- Panic Wipe**
A user can wipe the data instantly just by typing the PIN on screen lock.
- Password Wipe**
All the data is wiped automatically after a certain number of unsuccessful password attempts.
- Simplified Verification**
Our Notary Verification process makes it far easier for the users to do the encryption.
- Global Service**
Supports CDMA, Quad-band GSM and UMTS in 120 countries and includes unlimited international SIM.
- Tamper Proofing**
Attack surfaces like recovery mode and ADB connectivity have been removed.



EncroChatSure.com . . . Better Sure than sorry!

Encrochat — the messaging app



Encrochat — the messaging app

- End-to-end encrypted chat



Encrochat — the messaging app

- End-to-end encrypted chat
- Traffic routed through servers on VMs of cloud service provider OVH in Roubaix, France



Encrochat — the messaging app

- End-to-end encrypted chat
- Traffic routed through servers on VMs of cloud service provider OVH in Roubaix, France
- Disappearing messages



Encrochat — the messaging app

- End-to-end encrypted chat
- Traffic routed through servers on VMs of cloud service provider OVH in Roubaix, France
- Disappearing messages
- Pseudonymous user handles



Encrochat — the messaging app

- End-to-end encrypted chat
- Traffic routed through servers on VMs of cloud service provider OVH in Roubaix, France
- Disappearing messages
- Pseudonymous user handles
- Encryption protocol:
 - Some 2019 marketing materials said OTR
 - Investigative reporting and court documents describe it as based on Signal

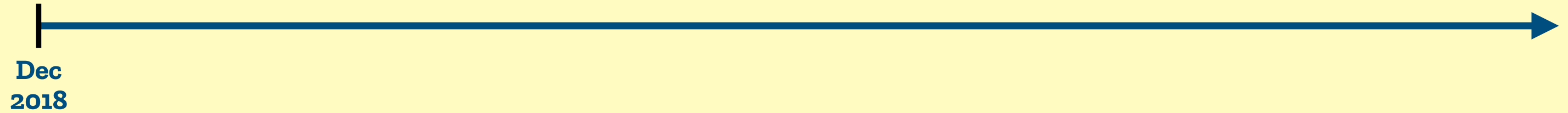


Encrochat — the messaging app

- End-to-end encrypted chat
- Traffic routed through servers on VMs of cloud service provider OVH in Roubaix, France
- Disappearing messages
- Pseudonymous user handles
- Encryption protocol:
 - Some 2019 marketing materials said OTR
 - Investigative reporting and court documents describe it as based on Signal
- Only for communicating with other Encrochat users



Timeline of the breach



Timeline of the breach

French court authorises
French law enf. to take
copies of Encrochat VMs
from server in Roubaix.

Dec
2018

A horizontal blue arrow pointing to the right, representing the timeline.

Timeline of the breach

French court authorises French law enf. to take copies of Encrochat VMs from server in Roubaix.

Dec
2018

Procedure reference	Relevant department	Nature of the facts
S711/2017	SR ORLEANS (SR = Research section)	In January 2018, the Orléans SR arrested the perpetrators of drug trafficking and seized 436 kilos of cannabis resin ; this operation led to the seizure of a BQ brand phone, an Aquaris X model encrypted by Encrochat.
663/2018	SR CLERMONT FERRAND	The SR of CLERMONT FERRAND arrested, in June 2018, an individual transporting in his vehicle nearly 30 kilos of cannabis resin ; he had a BQ phone model Aquaris X, encrypted by Encrochat, as well as a handwritten note with an Encrochat identifier on it.
105/2018	SR CAEN	The Caen SR stopped a motorist carrying 30 kilos of cannabis resin during a road check. Placed in police custody for drug trafficking, the defendant, who had an Encrochat encrypted telephone , admitted that it was exclusively dedicated to trafficking.
121/2017	SR METZ	During the year 2017, SR METZ, seized of the facts of organized gang vehicle thefts, stolen goods, and organized gang fraud, proceeded to arrest the perpetrators and seized a BQ Aquaris phone encrypted by Encrochat .
1590/2017	SR METZ	In December 2017, SR Metz arrested several key players involved in a significant drug trafficking operation imported from the Netherlands, 12 kilos of cannabis herb, 6 kilos of heroin, 1 kilo of crack cocaine , and two BQ model Aquaris X telephones encrypted by Encrochat were seized.
14/2018	SR METZ	Acting as part of the dismantling of a network involved in numerous home jacking thefts of luxury cars, which also operated in Luxembourg and Belgium, the Metz SR seized 6 kilos of cannabis resin and a BQ model Aquaris phone encrypted by Encrochat . The user of this phone stated that he was using it to contact his suppliers of narcotic products.
13/2018	SR METZ	The METZ SR was seized during 2018 of a transport of 100 kilos of cannabis resin , the driver being found carrying a BQ telephone, model Aquaris, encrypted by Encrochat , for which he refused to give details.

Timeline of the breach

French court authorises French law enf. to take copies of Encrochat VMs from server in Roubaix.

LE takes VM copies.

Dec
2018

Jan &
Oct
2019

Procedure reference	Relevant department	Nature of the facts
S711/2017	SR ORLEANS (SR = Research section)	In January 2018, the Orléans SR arrested the perpetrators of drug trafficking and seized 436 kilos of cannabis resin ; this operation led to the seizure of a BQ brand phone, an Aquaris X model encrypted by Encrochat.
663/2018	SR CLERMONT FERRAND	The SR of CLERMONT FERRAND arrested, in June 2018, an individual transporting in his vehicle nearly 30 kilos of cannabis resin ; he had a BQ phone model Aquaris X, encrypted by Encrochat, as well as a handwritten note with an Encrochat identifier on it.
105/2018	SR CAEN	The Caen SR stopped a motorist carrying 30 kilos of cannabis resin during a road check. Placed in police custody for drug trafficking, the defendant, who had an Encrochat encrypted telephone , admitted that it was exclusively dedicated to trafficking.
121/2017	SR METZ	During the year 2017, SR METZ, seized of the facts of organized gang vehicle thefts, stolen goods, and organized gang fraud, proceeded to arrest the perpetrators and seized a BQ Aquaris phone encrypted by Encrochat .
1590/2017	SR METZ	In December 2017, SR Metz arrested several key players involved in a significant drug trafficking operation imported from the Netherlands, 12 kilos of cannabis herb, 6 kilos of heroin, 1 kilo of crack cocaine , and two BQ model Aquaris X telephones encrypted by Encrochat were seized.
14/2018	SR METZ	Acting as part of the dismantling of a network involved in numerous home jacking thefts of luxury cars, which also operated in Luxembourg and Belgium, the Metz SR seized 6 kilos of cannabis resin and a BQ model Aquaris phone encrypted by Encrochat . The user of this phone stated that he was using it to contact his suppliers of narcotic products.
13/2018	SR METZ	The METZ SR was seized during 2018 of a transport of 100 kilos of cannabis resin , the driver being found carrying a BQ telephone, model Aquaris, encrypted by Encrochat , for which he refused to give details.

The VM copies

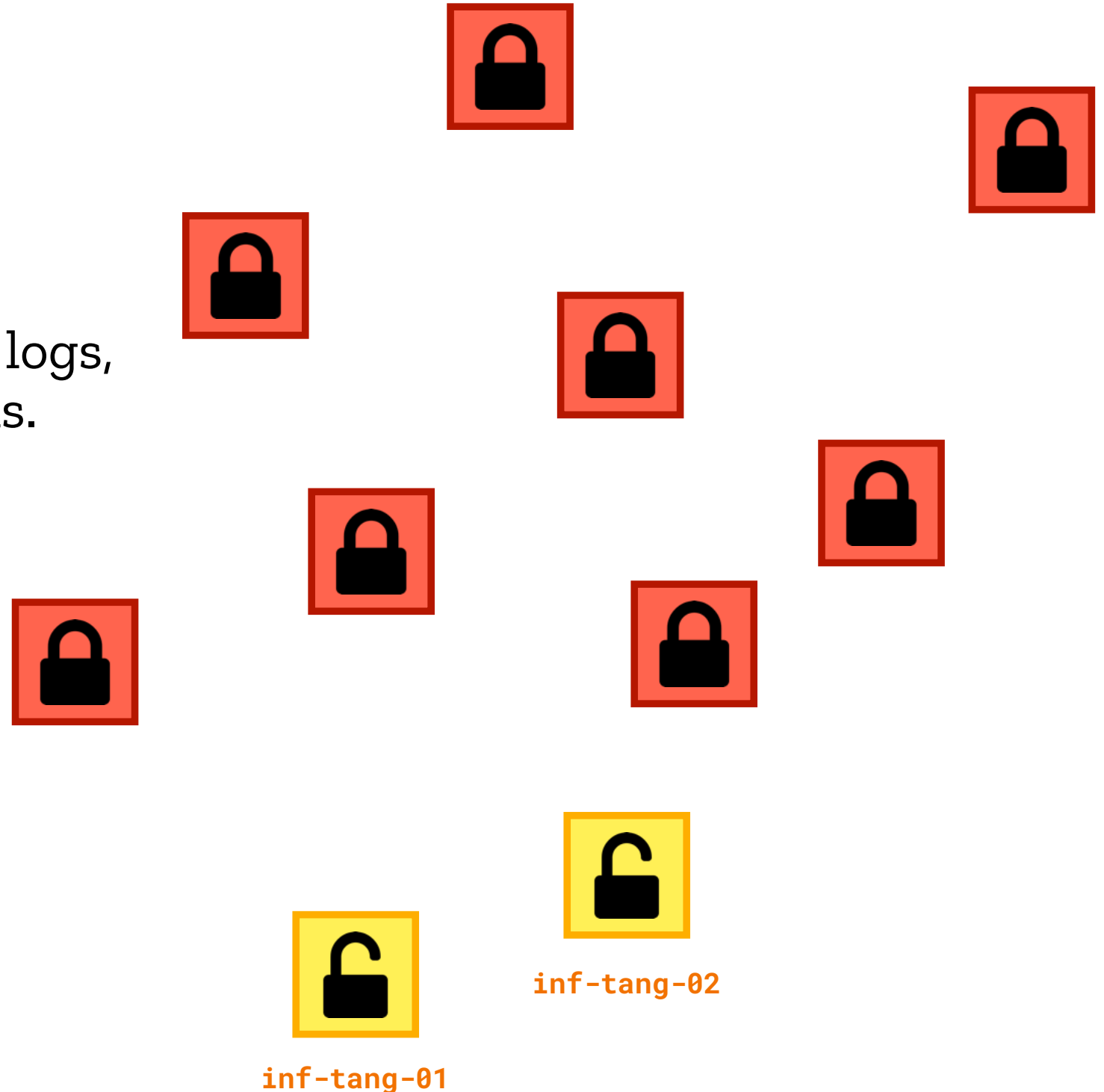
The VM copies

- Mostly full-disk encrypted VMs.
- Managing cryptographic keys, event logs, customer support, notes, & SIM cards.



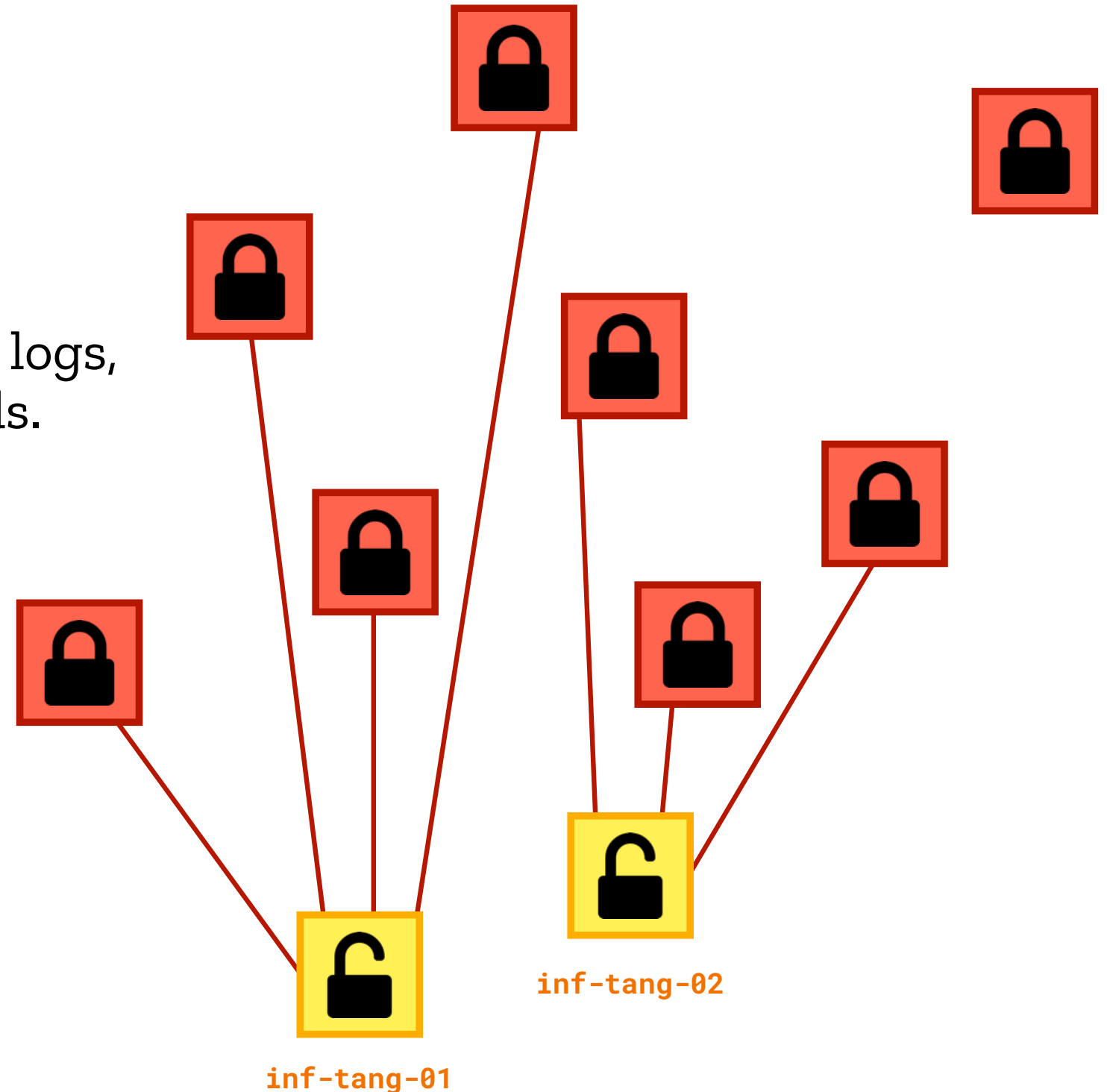
The VM copies

- Mostly full-disk encrypted VMs.
 - Managing cryptographic keys, event logs, customer support, notes, & SIM cards.
- But also some unencrypted ones, crucially including TANG servers.

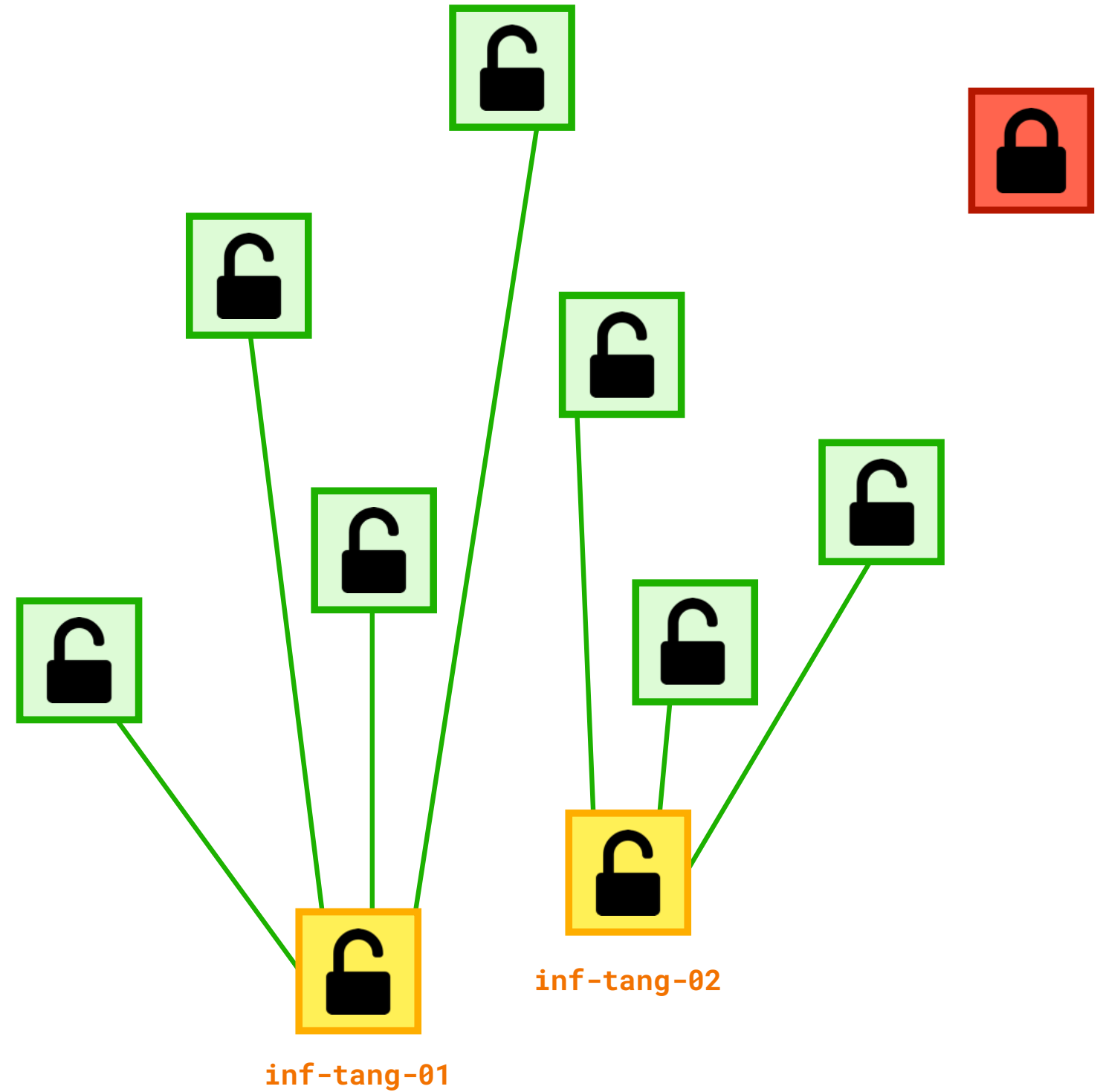


The VM copies

- Mostly full-disk encrypted VMs.
 - Managing cryptographic keys, event logs, customer support, notes, & SIM cards.
- But also some unencrypted ones, crucially including TANG servers.

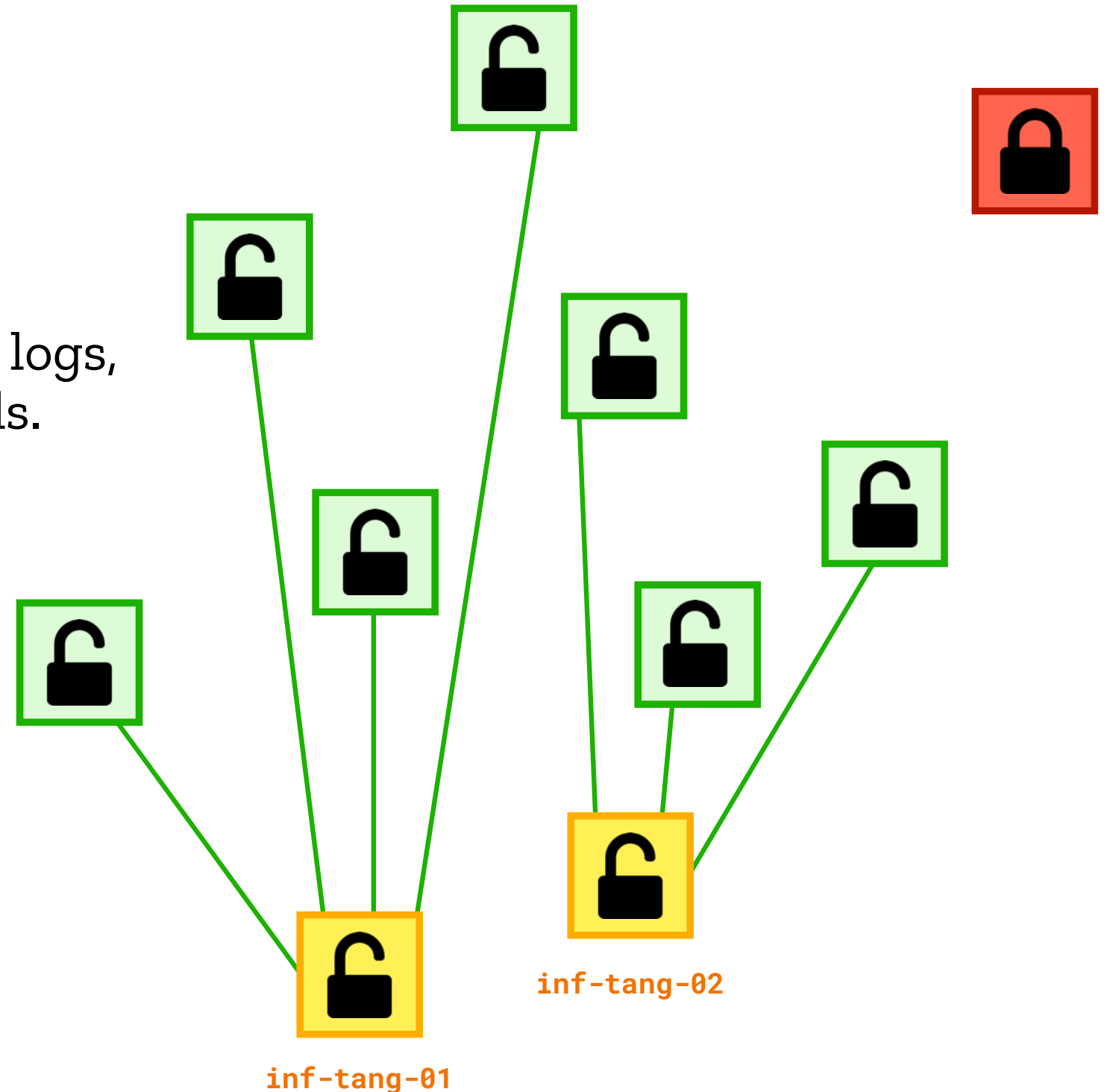


The VM copies



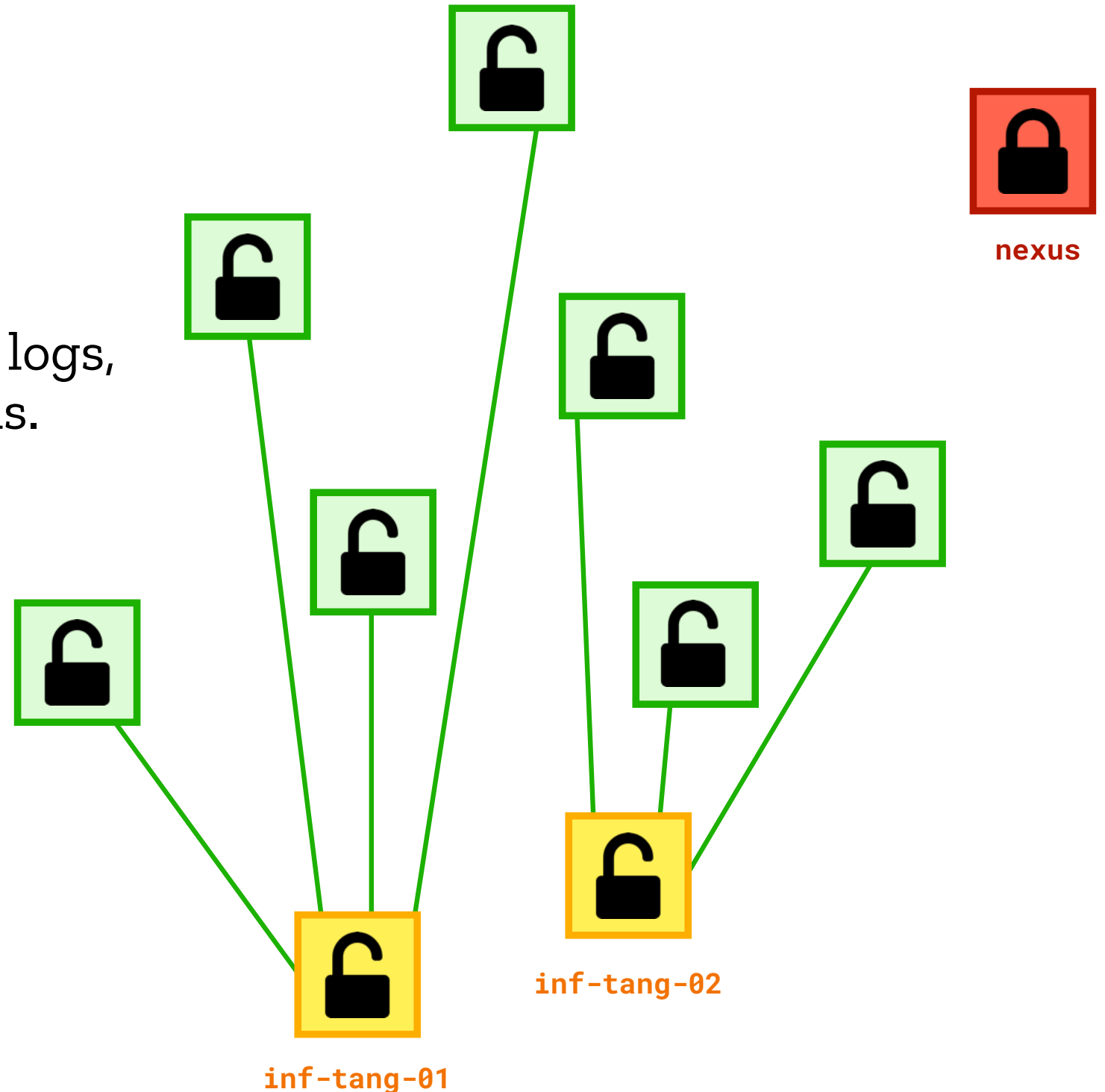
The VM copies

- Mostly full-disk encrypted VMs.
 - Managing cryptographic keys, event logs, customer support, notes, & SIM cards.
- Also some unencrypted ones, crucially including TANG servers.



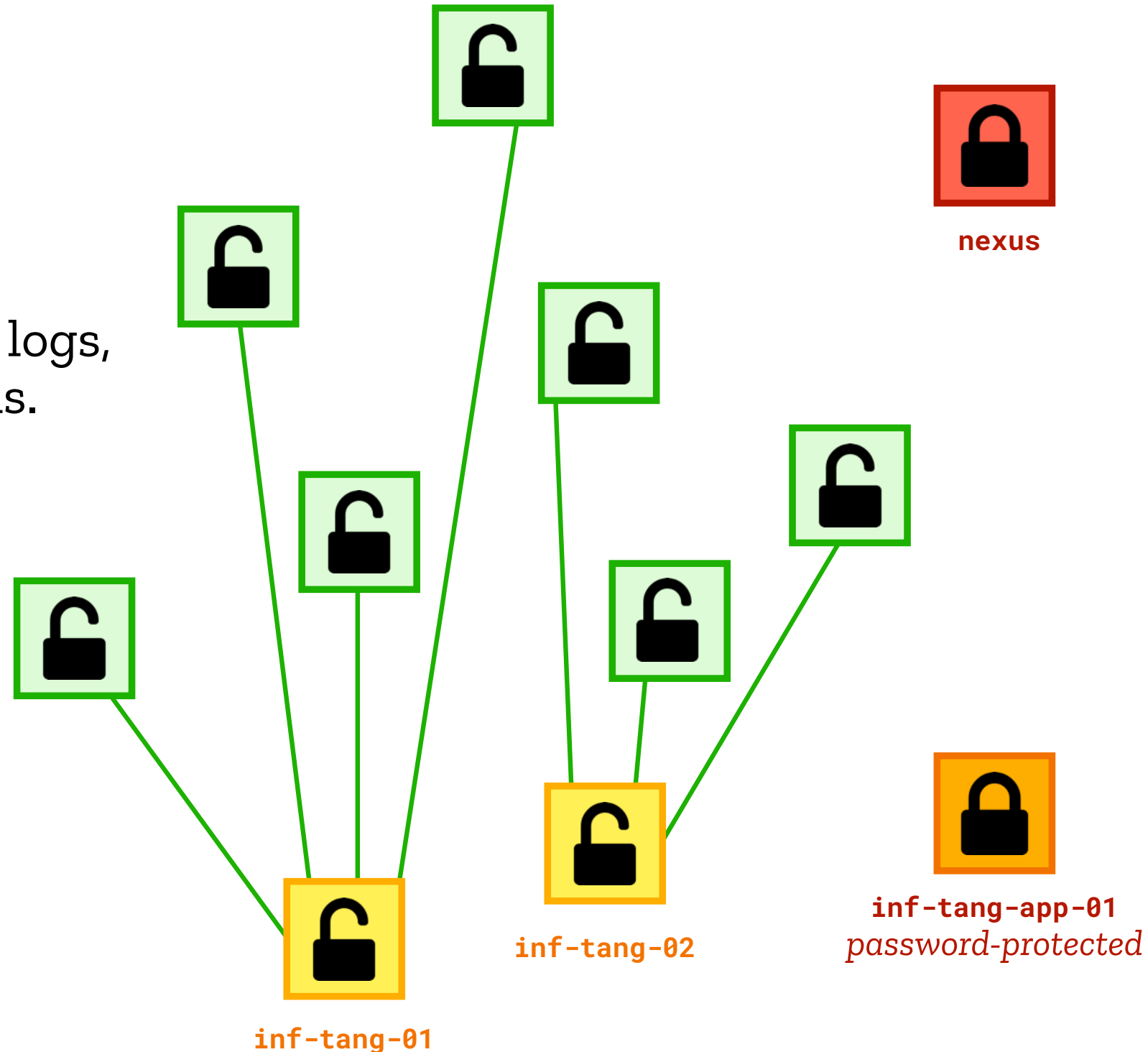
The VM copies

- Mostly full-disk encrypted VMs.
 - Managing cryptographic keys, event logs, customer support, notes, & SIM cards.
- Also some unencrypted ones, crucially including TANG servers.



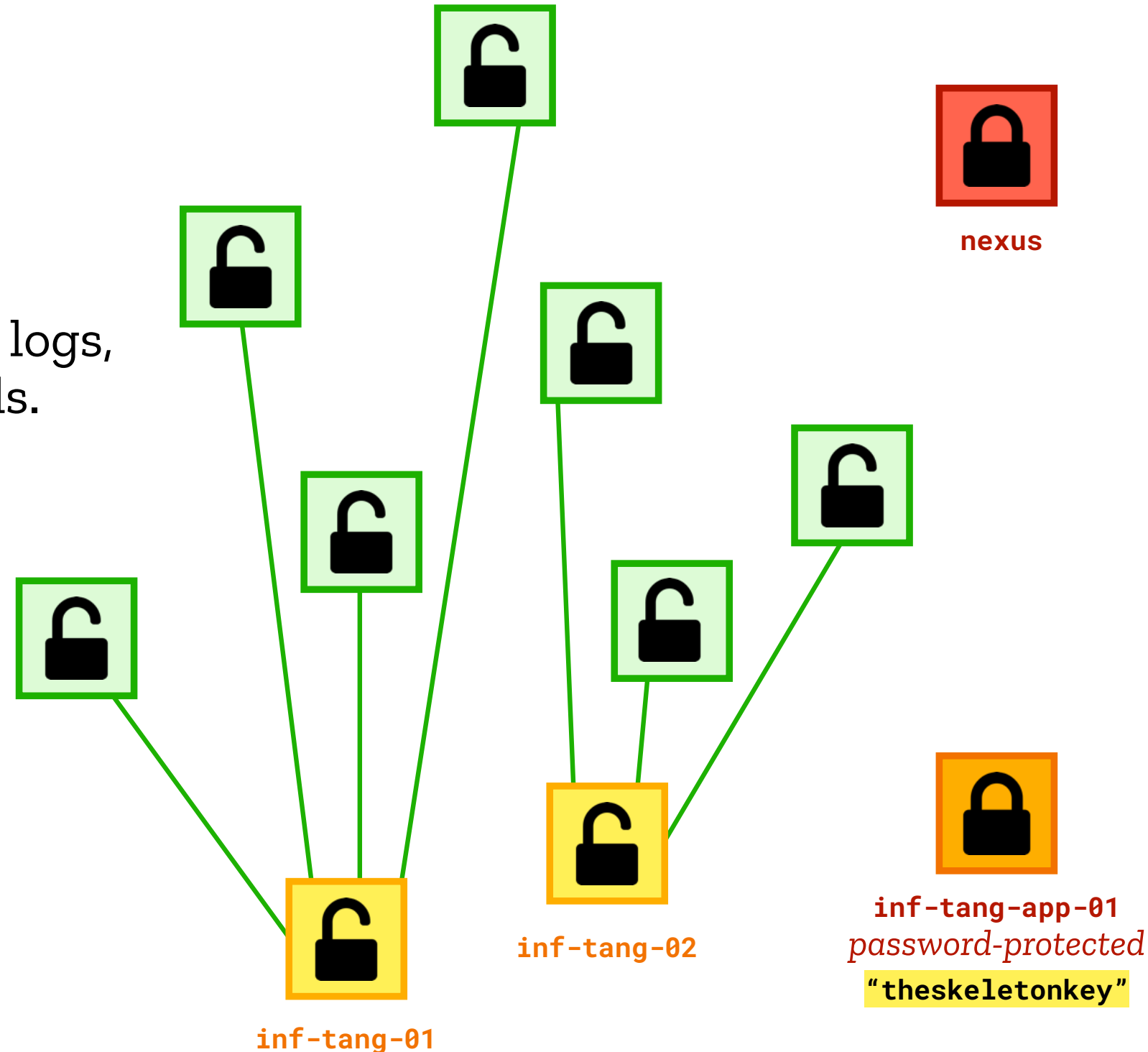
The VM copies

- Mostly full-disk encrypted VMs.
 - Managing cryptographic keys, event logs, customer support, notes, & SIM cards.
- Also some unencrypted ones, crucially including TANG servers.



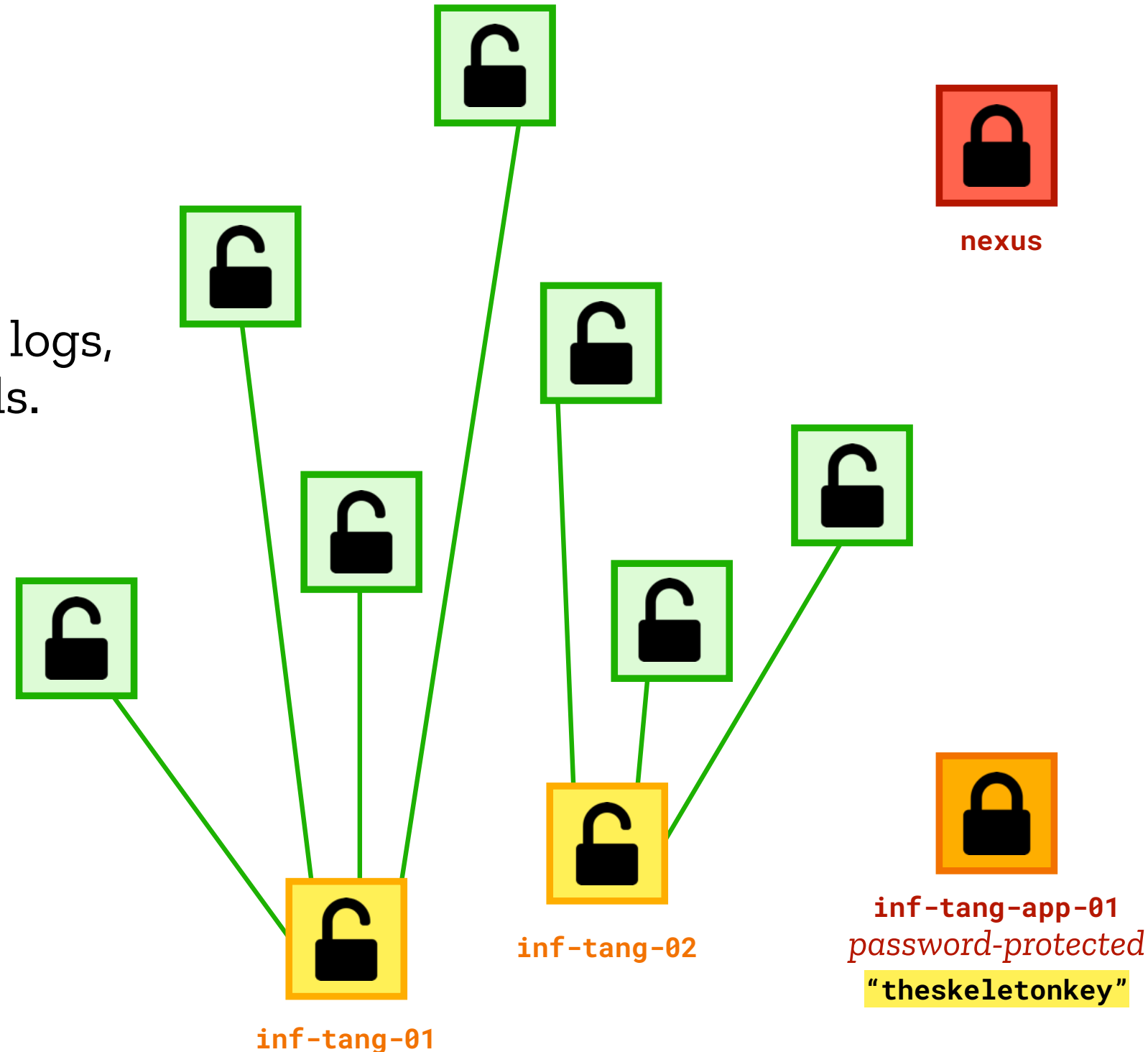
The VM copies

- Mostly full-disk encrypted VMs.
 - Managing cryptographic keys, event logs, customer support, notes, & SIM cards.
- Also some unencrypted ones, crucially including TANG servers.
- With Europol technical assistance, password "theskeletonkey" recovered.



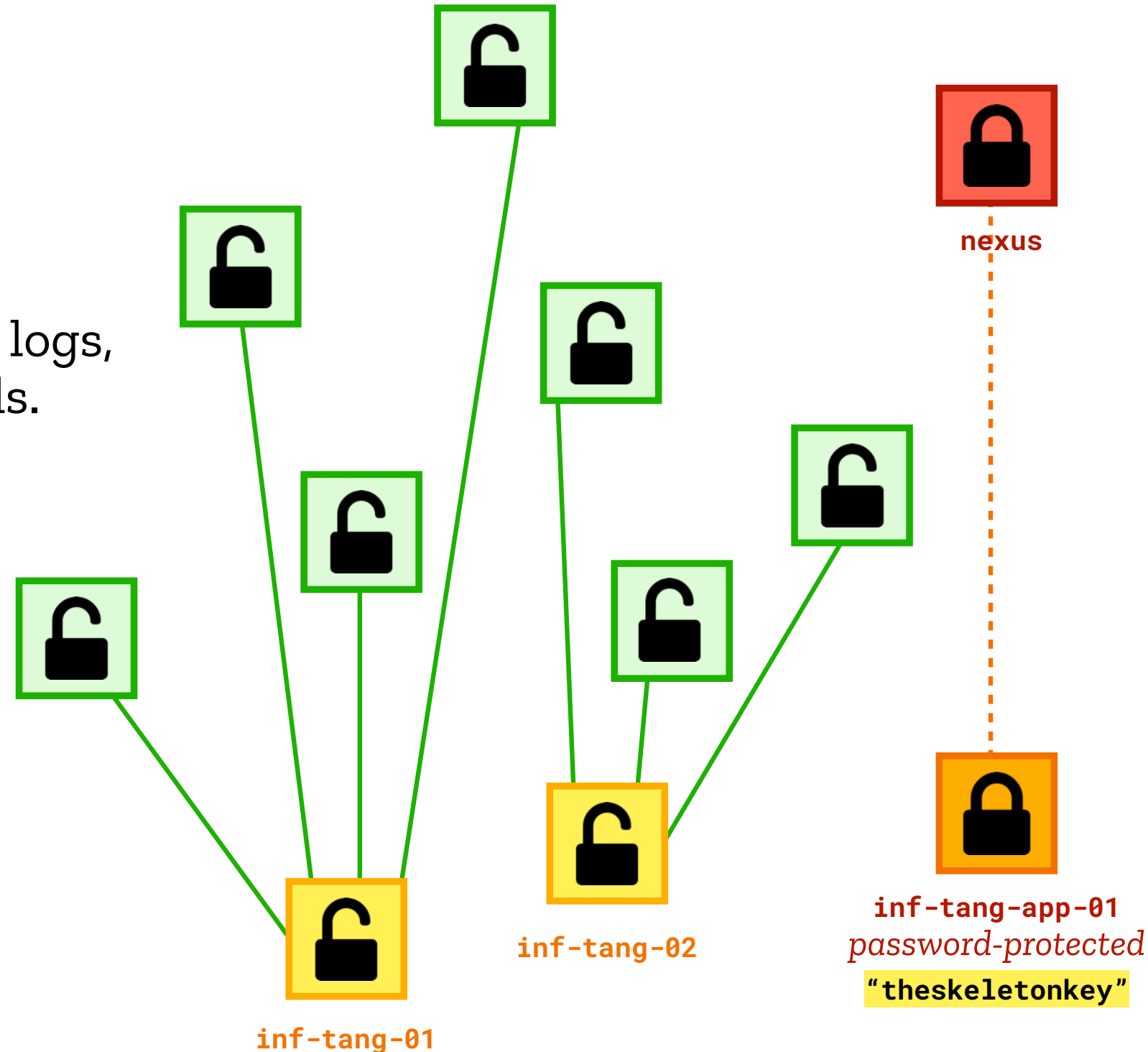
The VM copies

- Mostly full-disk encrypted VMs.
 - Managing cryptographic keys, event logs, customer support, notes, & SIM cards.
- Also some unencrypted ones, crucially including TANG servers.
- With Europol technical assistance, password "theskeletonkey" recovered.
- (We found that this took **0.01s** using Hashcat / rockyou dictionary.)



The VM copies

- Mostly full-disk encrypted VMs.
 - Managing cryptographic keys, event logs, customer support, notes, & SIM cards.
- Also some unencrypted ones, crucially including TANG servers.
- With Europol technical assistance, password "theskeletonkey" recovered.
- (We found that this took **0.01s** using Hashcat / rockyou dictionary.)



The VM copies

What was in the decrypted VMs?



prd-oas-01



prd-portal-live-app



prd-portal-live-db

The VM copies

What was in the decrypted VMs?

- **Client management system**

- "authentication logins, real IP addresses, and [resellers'] locations by country"
- data related to "payments, users, resellers' pseudonyms linked to delivery addresses, the IMEI [numbers], ..."



prd-oas-01



prd-portal-live-app



prd-portal-live-db

The VM copies

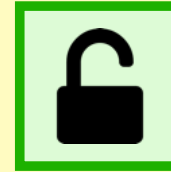
What was in the decrypted VMs?

- **Client management system**

- "authentication logins, real IP addresses, and [resellers'] locations by country"
- data related to "payments, users, resellers' pseudonyms linked to delivery addresses, the IMEI [numbers], ..."

- **Encrypted EncroNotes backups**

- SQLCipher/cacheword: keys encrypted with passwords ≥ 15 chars
- **7,582 encrypted keys** identified for password cracking
- **981 passwords cracked** (~12.5%)
- **8,725 files decrypted**, many related to drug trade



prd-oas-01



prd-portal-live-app



prd-portal-live-db



prd-notepad-backup-app-01

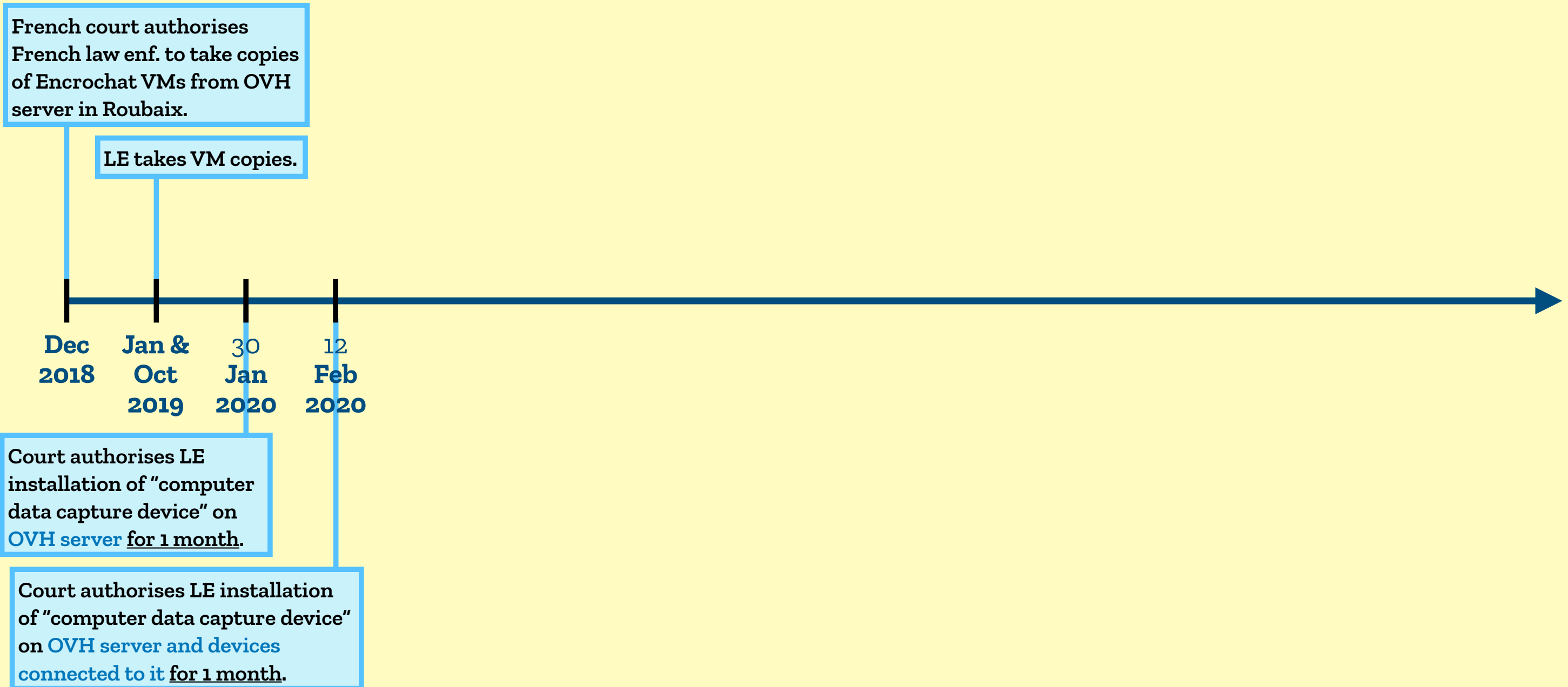
Timeline of the breach



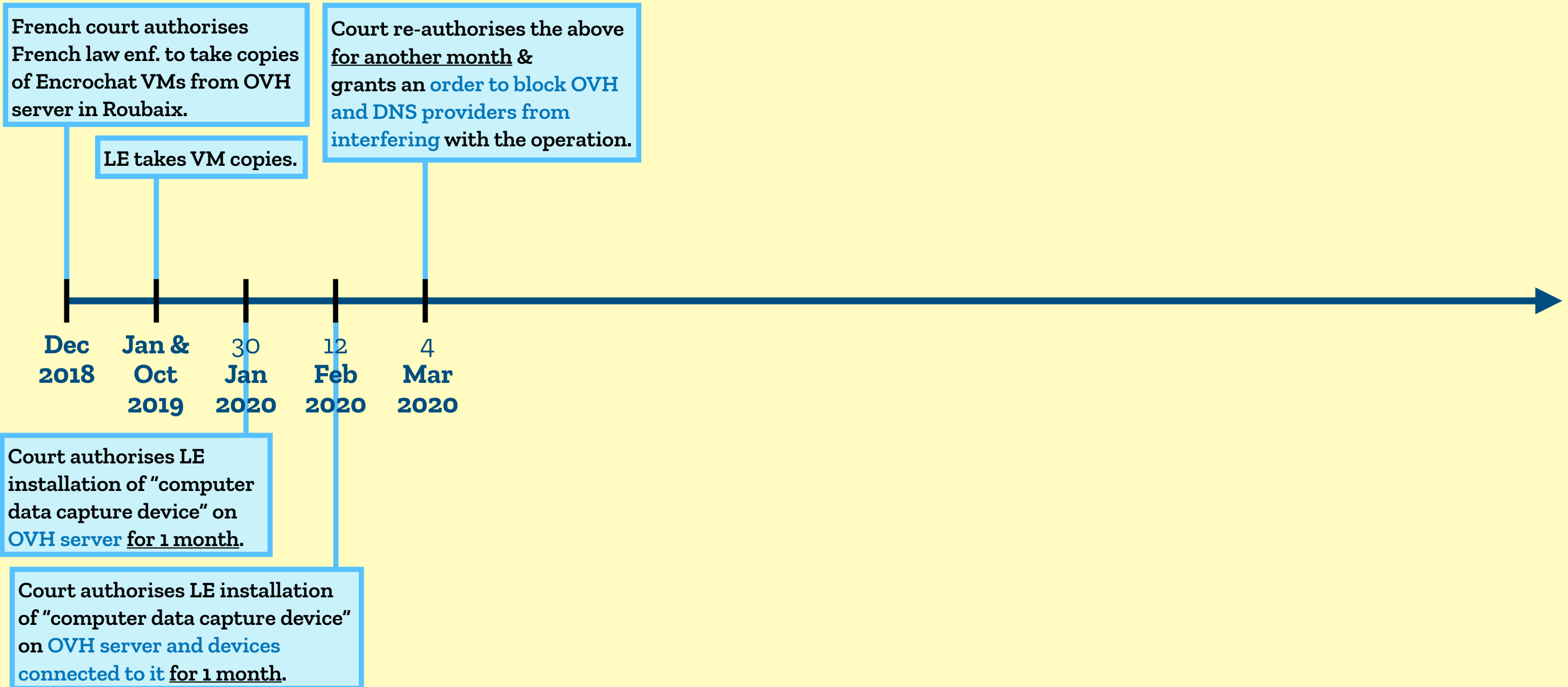
Timeline of the breach



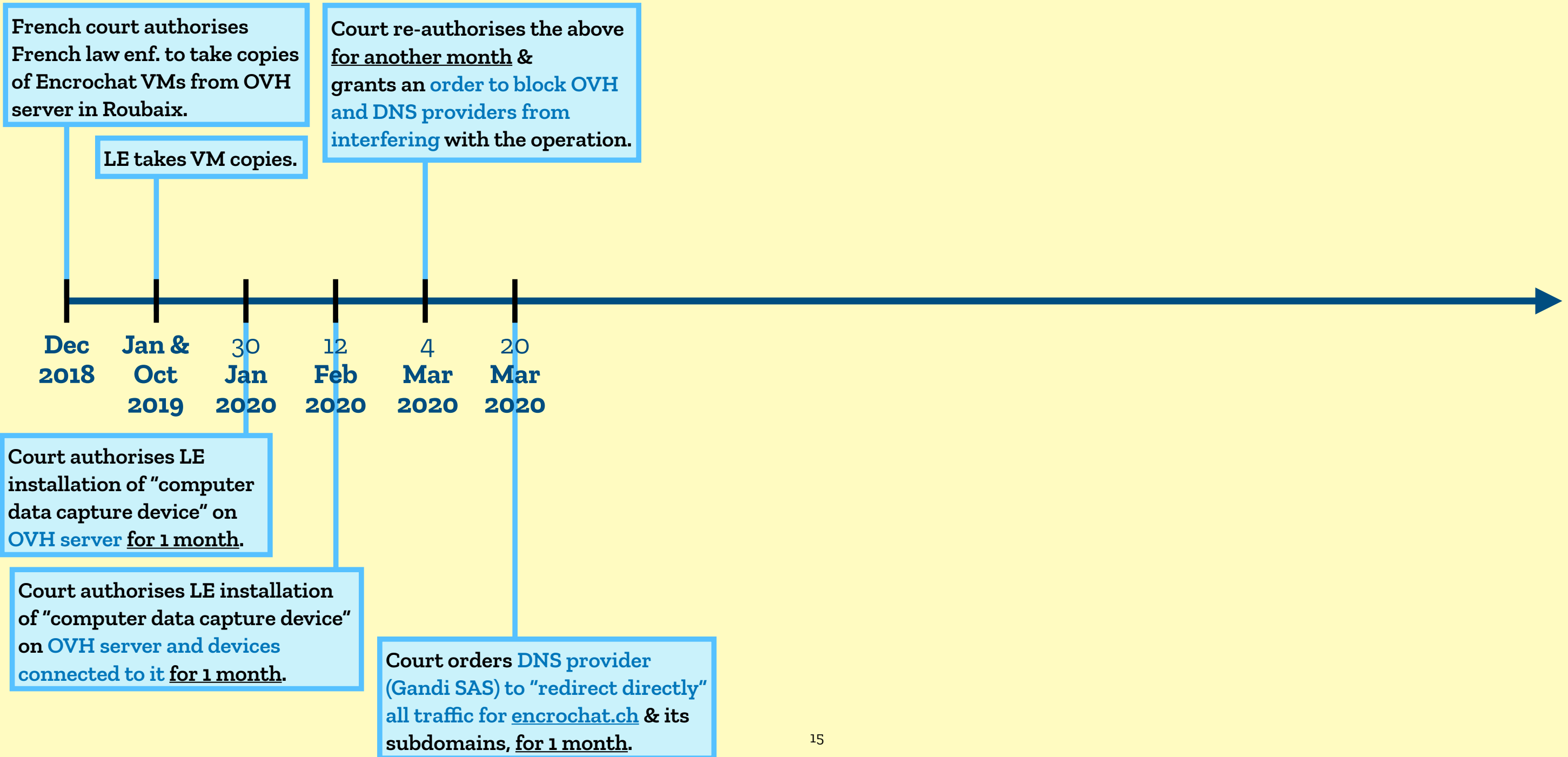
Timeline of the breach



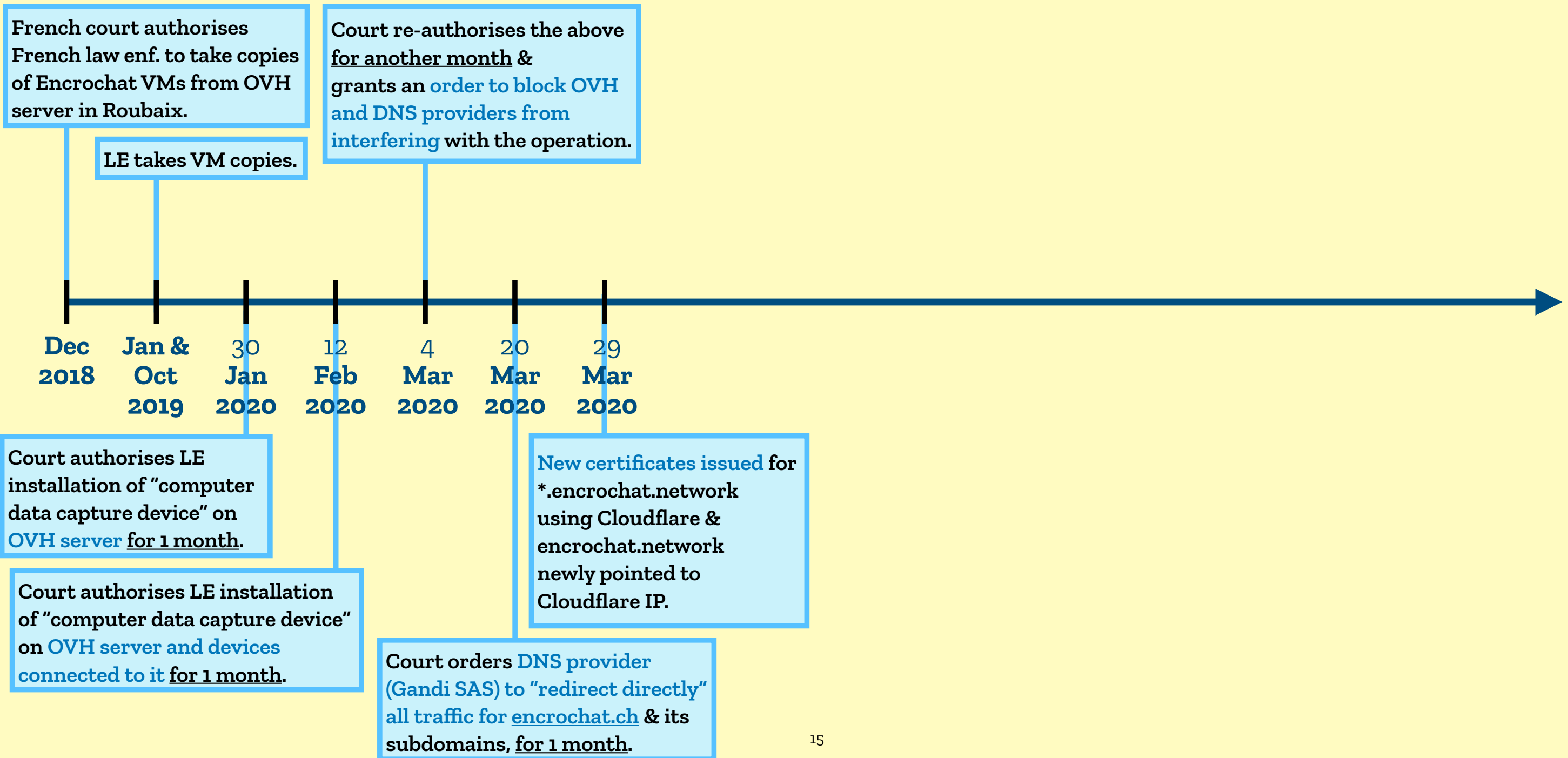
Timeline of the breach



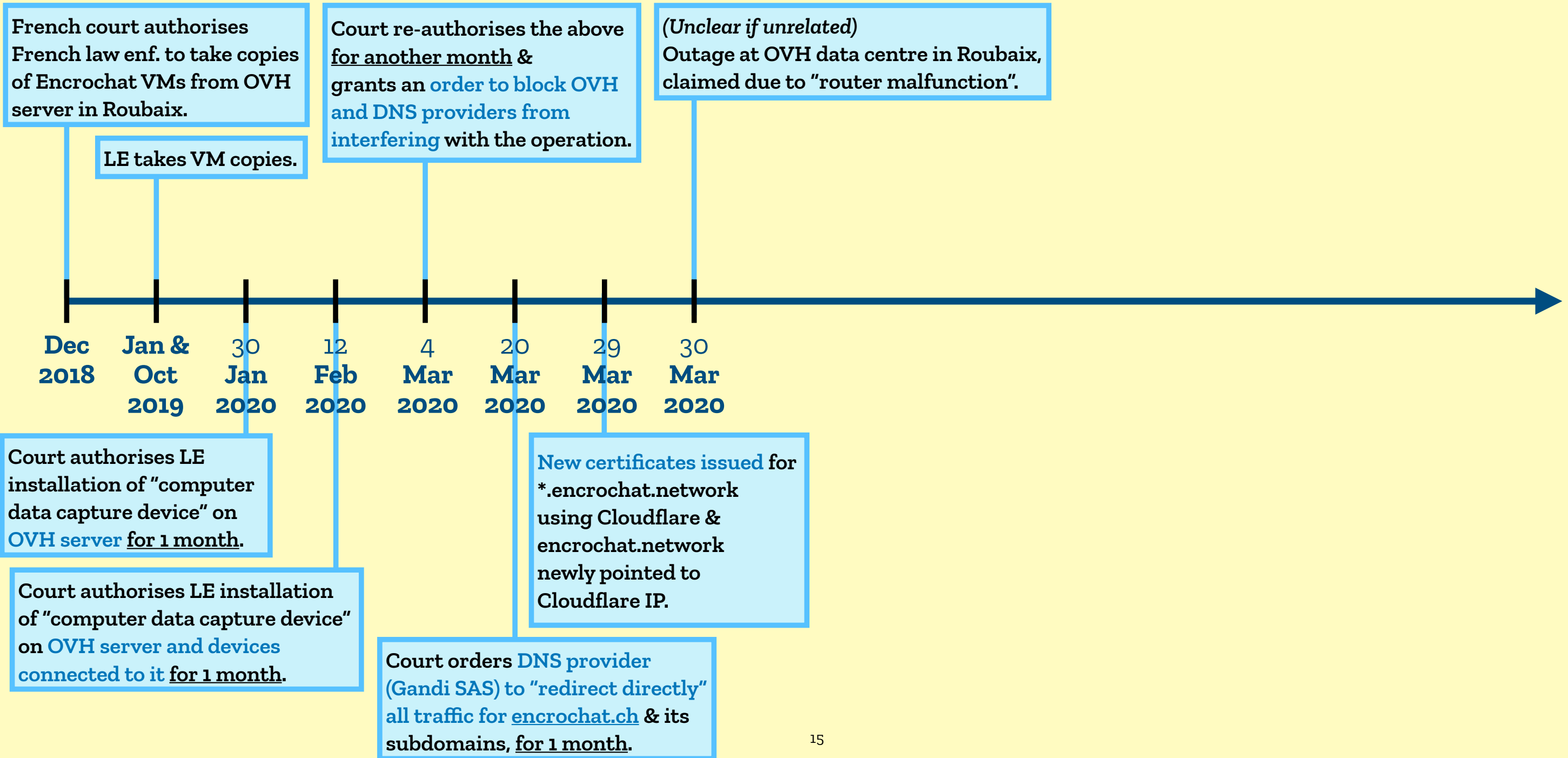
Timeline of the breach



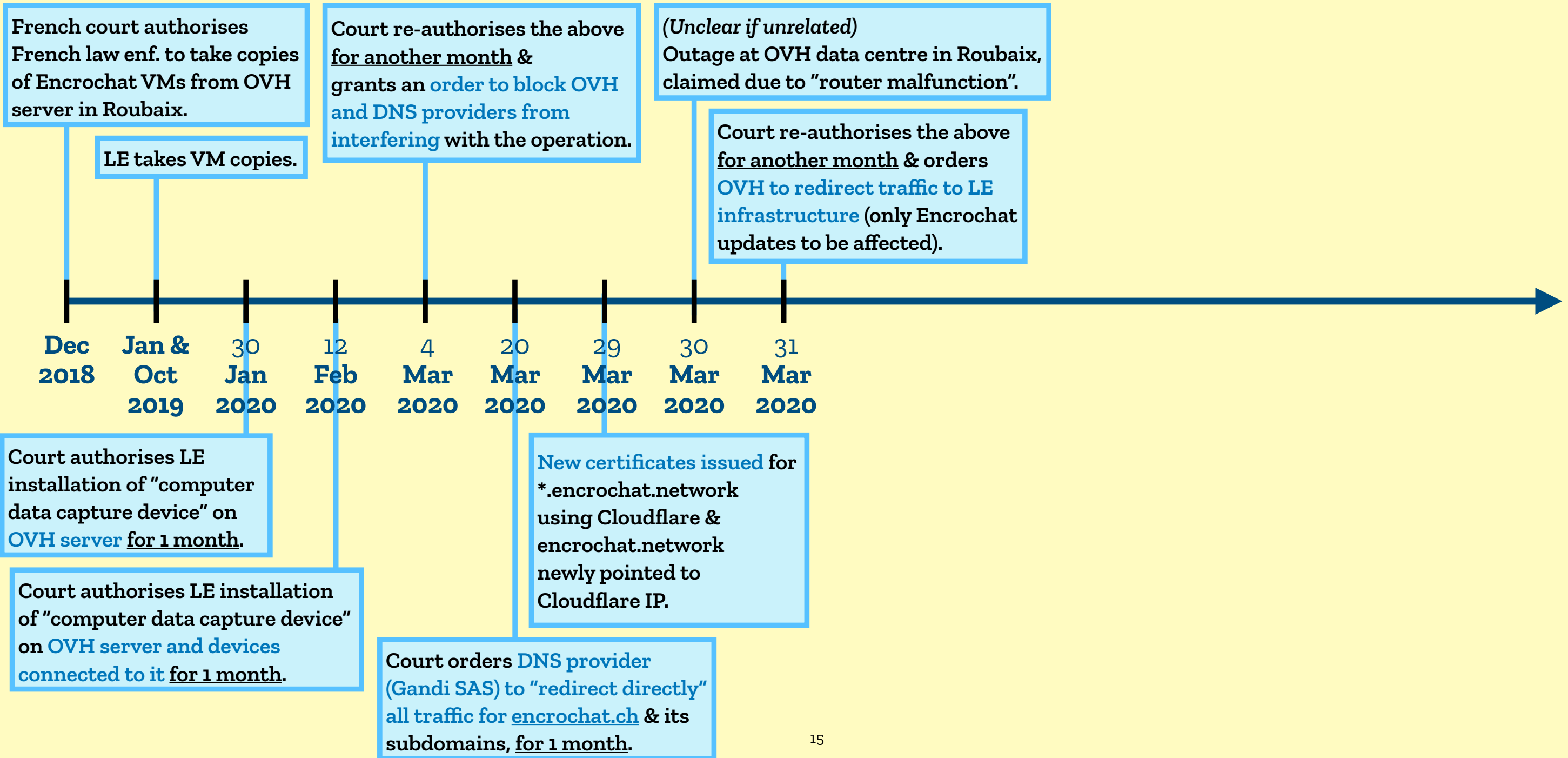
Timeline of the breach



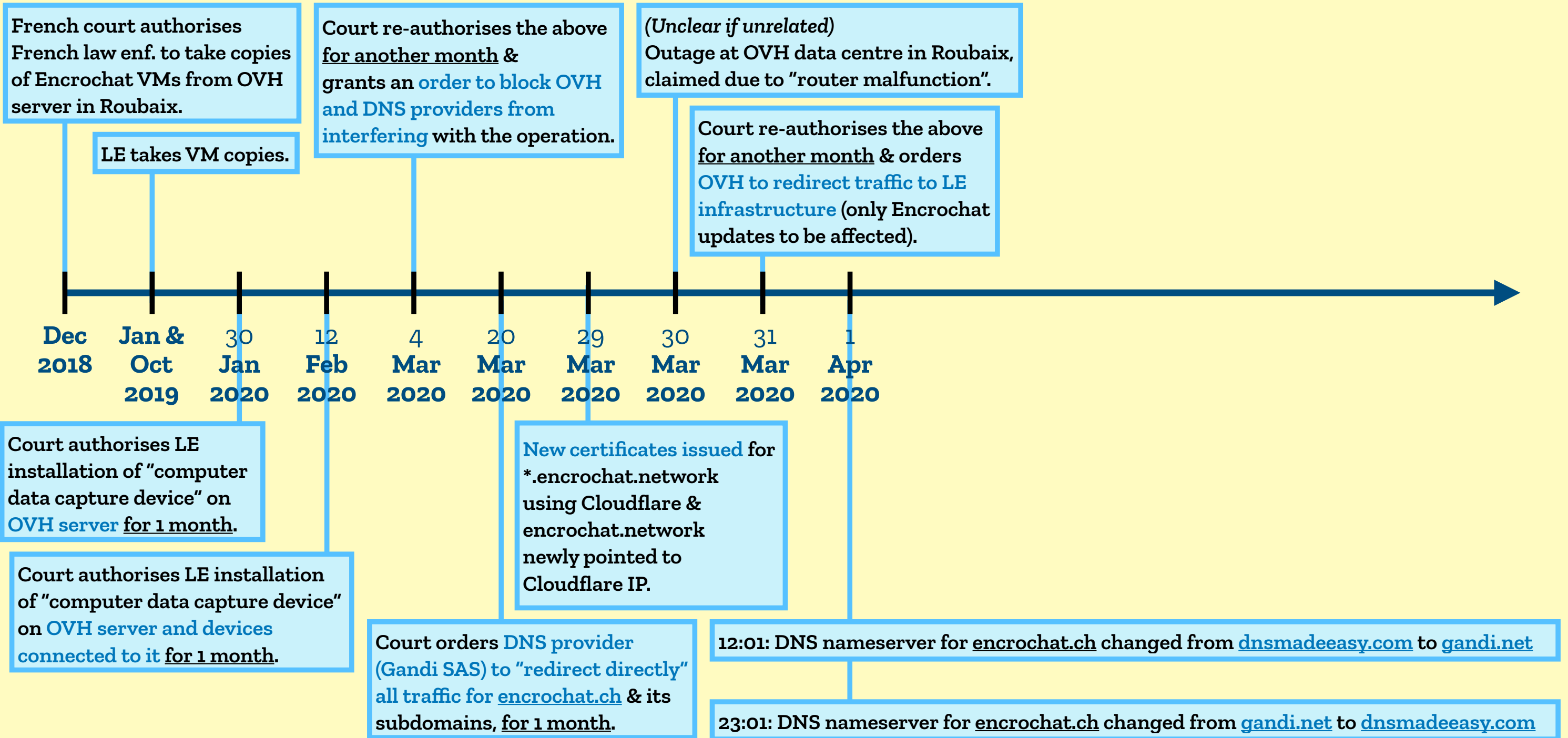
Timeline of the breach



Timeline of the breach



Timeline of the breach



WHOIS records

Table 1. WHOIS records for `encrochat.ch` in the period covering 1 January 2019 to 31 December 2020 [SWI24].

encrochat.ch				
2020-07-07 15:47	ns	ns0.dnsmadeeasy.com ns1.dnsmadeeasy.com ns2.dnsmadeeasy.com ns3.dnsmadeeasy.com ns4.dnsmadeeasy.com	—	
2020-04-04 19:42	reg	Gandi	Hostpoint	
2020-04-01 23:11	ns	ns5.dnsmadeeasy.com ns6.dnsmadeeasy.com ns7.dnsmadeeasy.com	ns0.dnsmadeeasy.com ns1.dnsmadeeasy.com ns2.dnsmadeeasy.com ns3.dnsmadeeasy.com ns4.dnsmadeeasy.com	
2020-04-01 23:01	ns	ns-134-c.gandi.net ns-155-a.gandi.net ns-99-b.gandi.net	ns5.dnsmadeeasy.com ns6.dnsmadeeasy.com ns7.dnsmadeeasy.com	
2020-04-01 12:01	ns	ns0.dnsmadeeasy.com ns1.dnsmadeeasy.com ns2.dnsmadeeasy.com ns3.dnsmadeeasy.com ns4.dnsmadeeasy.com	ns-134-c.gandi.net ns-155-a.gandi.net ns-99-b.gandi.net	
2019-11-09 14:26	Restore Domain by Registrar (Gandi)			
2019-11-09 14:26	Delete Domain by Registrar (Gandi)			

In the table above “reg” means a registrar change, “ns” means a nameserver change.

WHOIS records

Table 1. WHOIS records for `encrochat.ch` in the period covering 1 January 2019 to 31 December 2020 [SWI24].

encrochat.ch				
2020-07-07 15:47	ns	ns0.dnsmadeeasy.com ns1.dnsmadeeasy.com ns2.dnsmadeeasy.com ns3.dnsmadeeasy.com ns4.dnsmadeeasy.com	–	
2020-04-04 19:42	reg	Gandi	Hostpoint	
2020-04-01 23:11	ns	ns5.dnsmadeeasy.com ns6.dnsmadeeasy.com ns7.dnsmadeeasy.com	ns0.dnsmadeeasy.com ns1.dnsmadeeasy.com ns2.dnsmadeeasy.com ns3.dnsmadeeasy.com ns4.dnsmadeeasy.com	
2020-04-01 23:01	ns	ns-134-c.gandi.net ns-155-a.gandi.net ns-99-b.gandi.net	ns5.dnsmadeeasy.com ns6.dnsmadeeasy.com ns7.dnsmadeeasy.com	
2020-04-01 12:01	ns	ns0.dnsmadeeasy.com ns1.dnsmadeeasy.com ns2.dnsmadeeasy.com ns3.dnsmadeeasy.com ns4.dnsmadeeasy.com	ns-134-c.gandi.net ns-155-a.gandi.net ns-99-b.gandi.net	
2019-11-09 14:26	Restore Domain by Registrar (Gandi)			
2019-11-09 14:26	Delete Domain by Registrar (Gandi)			

In the table above “reg” means a registrar change, “ns” means a nameserver change.

Table 2. “Name Server History” for `encrochat.ch` [Dom24]

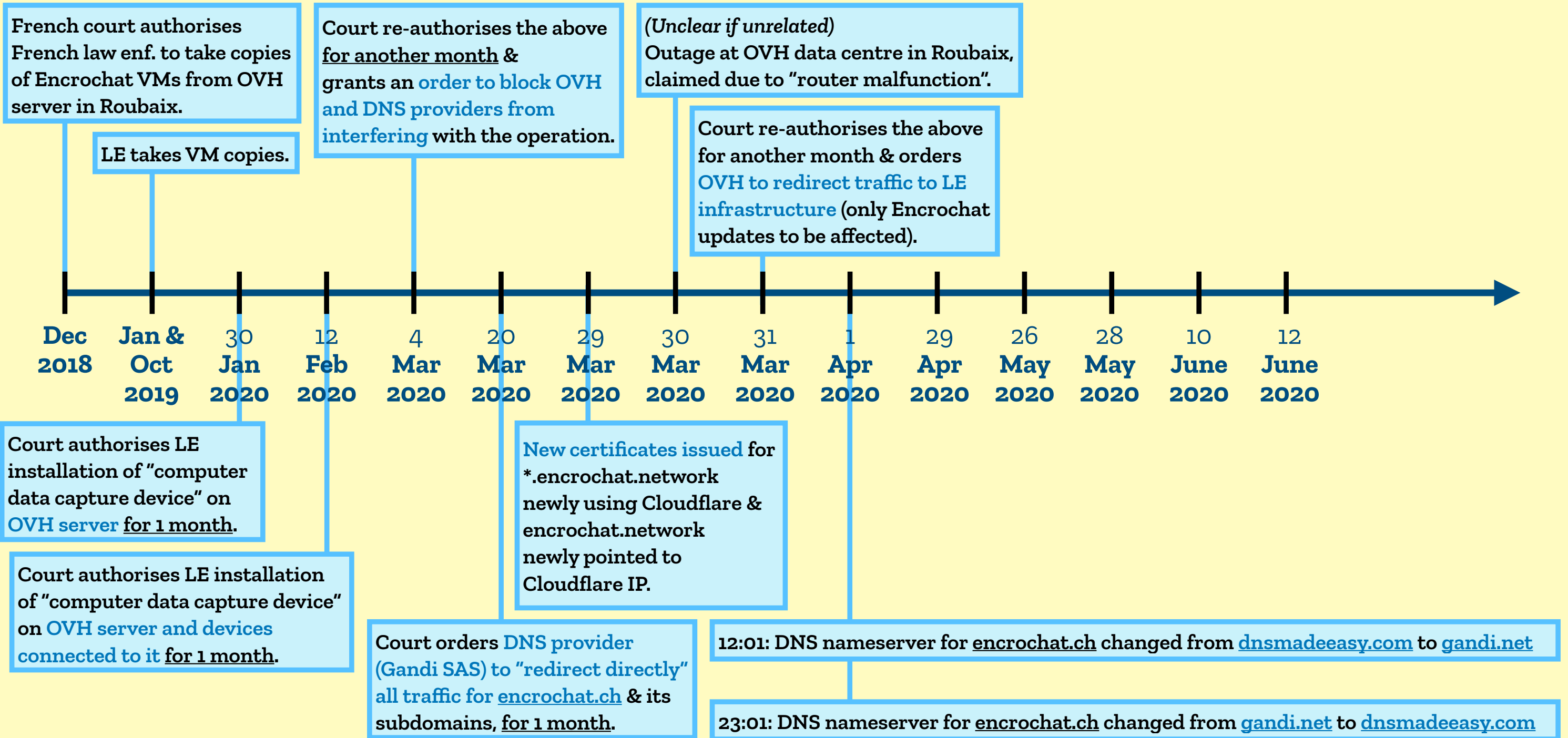
event date	action	previous server	new server
2023-09-10	delete	gandi.net	<i>none</i>
2022-09-02	new	<i>none</i>	gandi.net
2020-07-09	delete	dnsmadeeasy.com	<i>none</i>
2020-04-03	transfer	gandi.net	dnsmadeeasy.com
2020-04-02	transfer	dnsmadeeasy.com	gandi.net
2015-04-24	transfer	easydns.com	dnsmadeeasy.com
2013-11-08	transfer	gandi.net	easydns.com
2013-10-14	new	<i>none</i>	gandi.net

Table 3. WHOIS records for `encrochat.ch` [Dom24]

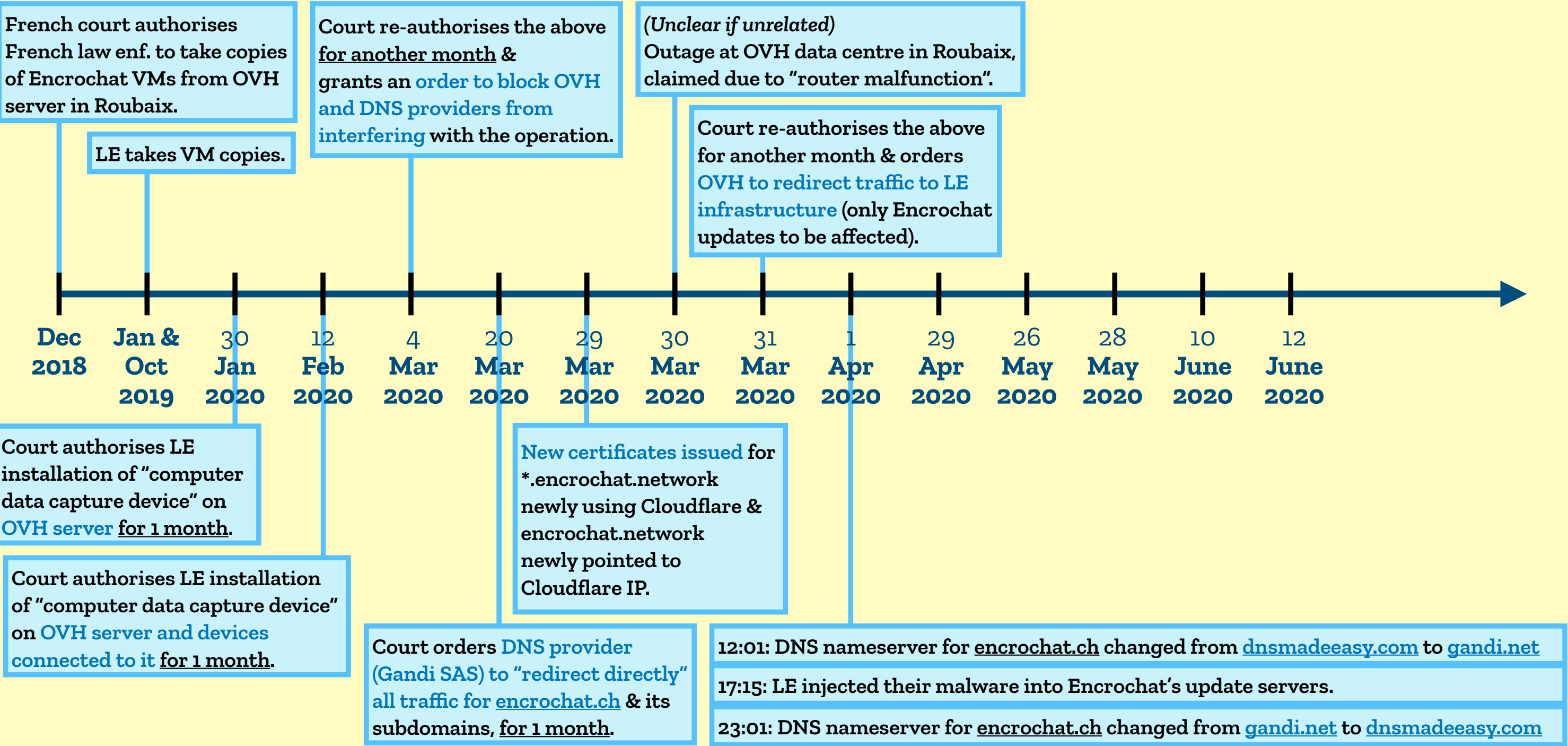
date	registrar	namerserver	domain	extra
2022-08-31	<i>none given</i>	gandi.net		
2020-04-03	<i>none given</i>	dnsmadeeasy.com		
2020-04-01	<i>none given</i>	gandi.net		
2020-03-22	<i>none given</i>	dnsmadeeasy.com		+
2020-01-10	<i>none given</i>	dnsmadeeasy.com		
2019-03-29	<i>none given</i>	dnsmadeeasy.com		
2019-02-14	Gandi SAS	dnsmadeeasy.com		
2018-12-19	Gandi SAS	dnsmadeeasy.com		
2017-12-13	Gandi SAS	dnsmadeeasy.com		
2016-10-18	Gandi SAS	dnsmadeeasy.com		
2015-07-04	Gandi SAS	dnsmadeeasy.com		
2015-04-06	Gandi SAS	easydns.com		
2013-12-19	Gandi SAS	easydns.com		
2013-10-15	Gandi SAS	gandi.net		

Entries marked with “+” are taken from Whois records separately downloaded from `domaintools.com` but not included in [Dom24].

Timeline of the breach



Timeline of the breach



The malware

- **Stage 1: Historical data collection**

- Transmitted all data stored on device to French authorities
 - Identifiers (e.g., IMEI & username), stored chat messages and notes, phonebook, Wifi (SSID), passwords, call logs, ...

- **Stage 2: Live data collection**

- Chat messages forwarded to French police servers in real time
 - Plaintext copy of message sent directly from device (E2EE left unchanged)

Was Encrochat's update signing key compromised?

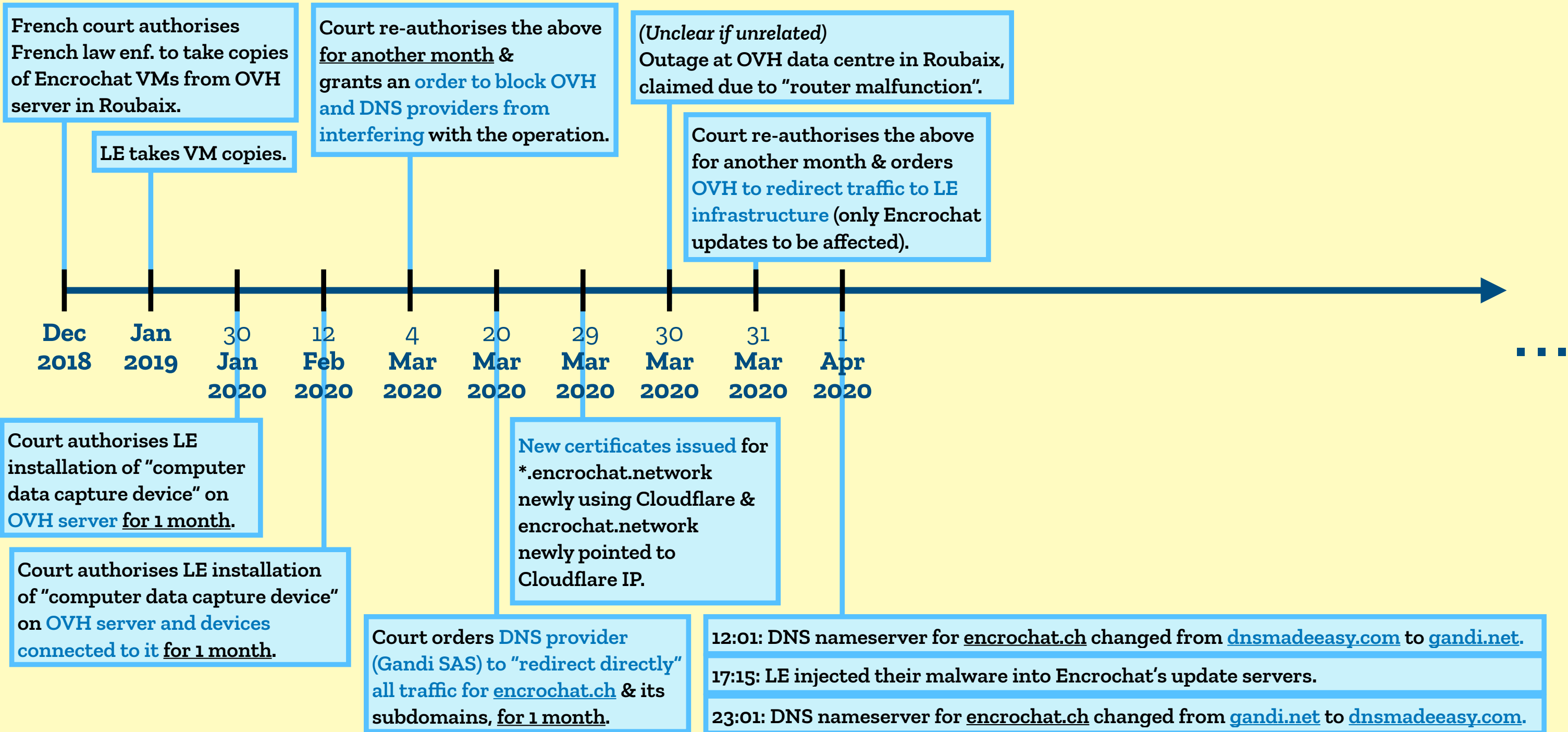
Was Encrochat's update signing key compromised?

- **All applications on Android must be cryptographically signed.**
 - Signature verification on installation, by Android's Package Manager.
 - No certificate chain.
 - Package Manager will reject "updates" not signed using same private key as currently installed version of app.

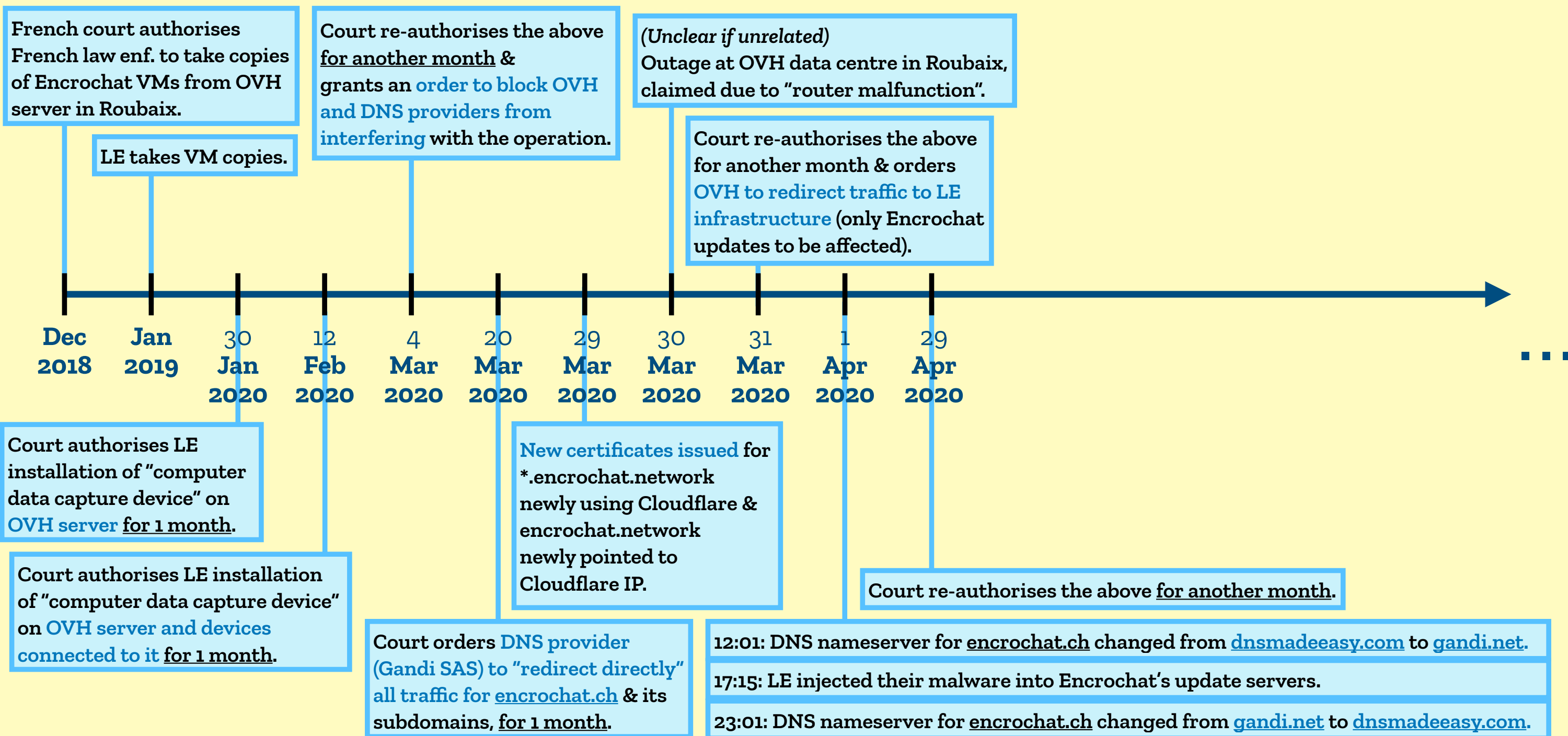
Was Encrochat's update signing key compromised?

- **All applications on Android must be cryptographically signed.**
 - Signature verification on installation, by Android's Package Manager.
 - No certificate chain.
 - Package Manager will reject "updates" not signed using same private key as currently installed version of app.
- **Platform-signed applications**
 - Apps signed by OEMs using on-device keys, with more permissions.

Timeline of the breach



Timeline of the breach



Timeline of the breach

Users report problems w/ remote wipe functionality.

French court authorises French law enf. to take copies of Encrochat VMs from OVH server in Roubaix.

LE takes VM copies.

Court re-authorises the above for another month & grants an order to block OVH and DNS providers from interfering with the operation.

(Unclear if unrelated)
Outage at OVH data centre in Roubaix, claimed due to "router malfunction".

Court re-authorises the above for another month & orders OVH to redirect traffic to LE infrastructure (only Encrochat updates to be affected).

Dec 2018 Jan 2019 30 Jan 2020 12 Feb 2020 4 Mar 2020 20 Mar 2020 29 Mar 2020 30 Mar 2020 31 Mar 2020 1 Apr 2020 29 Apr 2020 May 2020 ...

Court authorises LE installation of "computer data capture device" on OVH server for 1 month.

Court authorises LE installation of "computer data capture device" on OVH server and devices connected to it for 1 month.

New certificates issued for *.encrochat.network newly using Cloudflare & encrochat.network newly pointed to Cloudflare IP.

Court orders DNS provider (Gandi SAS) to "redirect directly" all traffic for encrochat.ch & its subdomains, for 1 month.

Court re-authorises the above for another month.

12:01: DNS nameserver for encrochat.ch changed from dnsmadeeasy.com to gandi.net.

17:15: LE injected their malware into Encrochat's update servers.

23:01: DNS nameserver for encrochat.ch changed from gandi.net to dnsmadeeasy.com.

Timeline of the breach

Users report problems w/ remote wipe functionality.

Encrochat investigates & finds malware on devices.

French court authorises French law enf. to take copies of Encrochat VMs from OVH server in Roubaix.

LE takes VM copies.

Court re-authorises the above for another month & grants an order to block OVH and DNS providers from interfering with the operation.

(Unclear if unrelated)
Outage at OVH data centre in Roubaix, claimed due to "router malfunction".

Court re-authorises the above for another month & orders OVH to redirect traffic to LE infrastructure (only Encrochat updates to be affected).

Dec 2018 Jan 2019 30 Jan 2020 12 Feb 2020 4 Mar 2020 20 Mar 2020 29 Mar 2020 30 Mar 2020 31 Mar 2020 1 Apr 2020 29 Apr 2020 May 2020 ...

Court authorises LE installation of "computer data capture device" on OVH server for 1 month.

Court authorises LE installation of "computer data capture device" on OVH server and devices connected to it for 1 month.

New certificates issued for *.encrochat.network newly using Cloudflare & encrochat.network newly pointed to Cloudflare IP.

Court orders DNS provider (Gandi SAS) to "redirect directly" all traffic for encrochat.ch & its subdomains, for 1 month.

Court re-authorises the above for another month.

12:01: DNS nameserver for encrochat.ch changed from dnsmadeeasy.com to gandi.net.

17:15: LE injected their malware into Encrochat's update servers.

23:01: DNS nameserver for encrochat.ch changed from gandi.net to dnsmadeeasy.com.

Timeline of the breach

Users report problems w/ remote wipe functionality.

Encrochat investigates & finds malware on devices.

Encrochat pushes update to fix the issue.

French court authorises French law enf. to take copies of Encrochat VMs from OVH server in Roubaix.

LE takes VM copies.

Court re-authorises the above for another month & grants an order to block OVH and DNS providers from interfering with the operation.

(Unclear if unrelated)
Outage at OVH data centre in Roubaix, claimed due to "router malfunction".

Court re-authorises the above for another month & orders OVH to redirect traffic to LE infrastructure (only Encrochat updates to be affected).

Dec 2018 Jan 2019 30 Jan 2020 12 Feb 2020 4 Mar 2020 20 Mar 2020 29 Mar 2020 30 Mar 2020 31 Mar 2020 1 Apr 2020 29 Apr 2020 May 2020 ...

Court authorises LE installation of "computer data capture device" on OVH server for 1 month.

Court authorises LE installation of "computer data capture device" on OVH server and devices connected to it for 1 month.

New certificates issued for *.encrochat.network newly using Cloudflare & encrochat.network newly pointed to Cloudflare IP.

Court orders DNS provider (Gandi SAS) to "redirect directly" all traffic for encrochat.ch & its subdomains, for 1 month.

Court re-authorises the above for another month.

12:01: DNS nameserver for encrochat.ch changed from dnsmadeeasy.com to gandi.net.

17:15: LE injected their malware into Encrochat's update servers.

23:01: DNS nameserver for encrochat.ch changed from gandi.net to dnsmadeeasy.com.

Timeline of the breach

Users report problems w/ remote wipe functionality.

Encrochat investigates & finds malware on devices.

Encrochat pushes update to fix the issue.

Almost immediately, malware strikes again.

French court authorises French law enf. to take copies of Encrochat VMs from OVH server in Roubaix.

LE takes VM copies.

Court re-authorises the above for another month & grants an order to block OVH and DNS providers from interfering with the operation.

(Unclear if unrelated)
Outage at OVH data centre in Roubaix, claimed due to "router malfunction".

Court re-authorises the above for another month & orders OVH to redirect traffic to LE infrastructure (only Encrochat updates to be affected).

Dec 2018 Jan 2019 30 Jan 2020 12 Feb 2020 4 Mar 2020 20 Mar 2020 29 Mar 2020 30 Mar 2020 31 Mar 2020 1 Apr 2020 29 Apr 2020 May 2020 ...

Court authorises LE installation of "computer data capture device" on OVH server for 1 month.

Court authorises LE installation of "computer data capture device" on OVH server and devices connected to it for 1 month.

New certificates issued for *.encrochat.network newly using Cloudflare & encrochat.network newly pointed to Cloudflare IP.

Court orders DNS provider (Gandi SAS) to "redirect directly" all traffic for encrochat.ch & its subdomains, for 1 month.

Court re-authorises the above for another month.

12:01: DNS nameserver for encrochat.ch changed from dnsmadeeasy.com to gandi.net.

17:15: LE injected their malware into Encrochat's update servers.

23:01: DNS nameserver for encrochat.ch changed from gandi.net to dnsmadeeasy.com.

Timeline of the breach

Users report problems w/ remote wipe functionality.

Encrochat investigates & finds malware on devices.

Encrochat pushes update to fix the issue.

Almost immediately, malware strikes again.

French court authorises French law enf. to take copies of Encrochat VMs from OVH server in Roubaix.

LE takes VM copies.

Court re-authorises the above for another month & grants an order to block OVH and DNS providers from interfering with the operation.

(Unclear if unrelated)
Outage at OVH data centre in Roubaix, claimed due to "router malfunction".

Court re-authorises the above for another month & orders OVH to redirect traffic to LE infrastructure (only Encrochat updates to be affected).

Malware installed on $\geq 20,000$ Encrochat devices; $\geq 100,000$ messages & 1,136 GB of data captured.

Dec 2018 Jan 2019 30 Jan 2020 12 Feb 2020 4 Mar 2020 20 Mar 2020 29 Mar 2020 30 Mar 2020 31 Mar 2020 1 Apr 2020 29 Apr 2020 May 2020 26 May 2020 ...

Court authorises LE installation of "computer data capture device" on OVH server for 1 month.

Court authorises LE installation of "computer data capture device" on OVH server and devices connected to it for 1 month.

New certificates issued for *.encrochat.network newly using Cloudflare & encrochat.network newly pointed to Cloudflare IP.

Court orders DNS provider (Gandi SAS) to "redirect directly" all traffic for encrochat.ch & its subdomains, for 1 month.

Court re-authorises the above for another month.

12:01: DNS nameserver for encrochat.ch changed from dnsmadeeasy.com to gandi.net.

17:15: LE injected their malware into Encrochat's update servers.

23:01: DNS nameserver for encrochat.ch changed from gandi.net to dnsmadeeasy.com.

Timeline of the breach

Users report problems w/ remote wipe functionality.

Encrochat investigates & finds malware on devices.

Encrochat pushes update to fix the issue.

Almost immediately, malware strikes again.

French court authorises French law enf. to take copies of Encrochat VMs from OVH server in Roubaix.

LE takes VM copies.

Court re-authorises the above for another month & grants an order to block OVH and DNS providers from interfering with the operation.

(Unclear if unrelated)
Outage at OVH data centre in Roubaix, claimed due to "router malfunction".

Court re-authorises the above for another month & orders OVH to redirect traffic to LE infrastructure (only Encrochat updates to be affected).

Malware installed on $\geq 20,000$ Encrochat devices; $\geq 100,000$ messages & 1,136 GB of data captured.

Dec
2018

Jan
2019

30
Jan
2020

12
Feb
2020

4
Mar
2020

20
Mar
2020

29
Mar
2020

30
Mar
2020

31
Mar
2020

1
Apr
2020

29
Apr
2020

May
2020

26
May
2020

28
May
2020

...

Court authorises LE installation of "computer data capture device" on OVH server for 1 month.

Court authorises LE installation of "computer data capture device" on OVH server and devices connected to it for 1 month.

New certificates issued for *.encrochat.network newly using Cloudflare & encrochat.network newly pointed to Cloudflare IP.

Court orders DNS provider (Gandi SAS) to "redirect directly" all traffic for encrochat.ch & its subdomains, for 1 month.

Court re-authorises the above for another 4 months.

Court re-authorises the above for another month.

12:01: DNS nameserver for encrochat.ch changed from dnsmadeeasy.com to gandi.net.

17:15: LE injected their malware into Encrochat's update servers.

23:01: DNS nameserver for encrochat.ch changed from gandi.net to dnsmadeeasy.com.

Timeline of the breach

Users report problems w/ remote wipe functionality.

Encrochat investigates & finds malware on devices.

Encrochat pushes update to fix the issue.

Almost immediately, malware strikes again.

French court authorises French law enf. to take copies of Encrochat VMs from OVH server in Roubaix.

LE takes VM copies.

Court re-authorises the above for another month & grants an order to block OVH and DNS providers from interfering with the operation.

(Unclear if unrelated)
Outage at OVH data centre in Roubaix, claimed due to "router malfunction".

Court re-authorises the above for another month & orders OVH to redirect traffic to LE infrastructure (only Encrochat updates to be affected).

Malware installed on $\geq 20,000$ Encrochat devices; $\geq 100,000$ messages & 1,136 GB of data captured.

Encrochat informed its SIM provider (KPN) of the attack, which blocked connections to the servers running the attack.

Dec 2018 Jan 2019 30 Jan 2020 12 Feb 2020 4 Mar 2020 20 Mar 2020 29 Mar 2020 30 Mar 2020 31 Mar 2020 1 Apr 2020 29 Apr 2020 May 2020 26 May 2020 28 May 2020 June 2020 ...

Court authorises LE installation of "computer data capture device" on OVH server for 1 month.

Court authorises LE installation of "computer data capture device" on OVH server and devices connected to it for 1 month.

New certificates issued for *.encrochat.network newly using Cloudflare & encrochat.network newly pointed to Cloudflare IP.

Court orders DNS provider (Gandi SAS) to "redirect directly" all traffic for encrochat.ch & its subdomains, for 1 month.

Court re-authorises the above for another 4 months.

Court re-authorises the above for another month.

12:01: DNS nameserver for encrochat.ch changed from dnsmadeeasy.com to gandi.net.

17:15: LE injected their malware into Encrochat's update servers.

23:01: DNS nameserver for encrochat.ch changed from gandi.net to dnsmadeeasy.com.

Timeline of the breach

Users report problems w/ remote wipe functionality.

Encrochat investigates & finds malware on devices.

Encrochat pushes update to fix the issue.

Almost immediately, malware strikes again.

French court authorises French law enf. to take copies of Encrochat VMs from OVH server in Roubaix.

LE takes VM copies.

Court re-authorises the above for another month & grants an order to block OVH and DNS providers from interfering with the operation.

(Unclear if unrelated)
Outage at OVH data centre in Roubaix, claimed due to "router malfunction".

Court re-authorises the above for another month & orders OVH to redirect traffic to LE infrastructure (only Encrochat updates to be affected).

Malware installed on ≥ 20,000 Encrochat devices; ≥ 100,000 messages & 1,136 GB of data captured.

Encrochat informed its SIM provider (KPN) of the attack, which blocked connections to the servers running the attack.

Dec 2018 Jan 2019 30 Jan 2020 12 Feb 2020 4 Mar 2020 20 Mar 2020 29 Mar 2020 30 Mar 2020 31 Mar 2020 1 Apr 2020 29 Apr 2020 May 2020 26 May 2020 28 May 2020 June 2020 10 June 2020 ...

Court authorises LE installation of "computer data capture device" on OVH server for 1 month.

Court authorises LE installation of "computer data capture device" on OVH server and devices connected to it for 1 month.

New certificates issued for *.encrochat.network newly using Cloudflare & encrochat.network newly pointed to Cloudflare IP.

Court orders DNS provider (Gandi SAS) to "redirect directly" all traffic for encrochat.ch & its subdomains, for 1 month.

Court re-authorises the above for another 4 months.

Court re-authorises the above for another month.

12:01: DNS nameserver for encrochat.ch changed from dnsmadeeasy.com to gandi.net.

17:15: LE injected their malware into Encrochat's update servers.

23:01: DNS nameserver for encrochat.ch changed from gandi.net to dnsmadeeasy.com.

Timeline of the breach

Users report problems w/ remote wipe functionality.

Encrochat investigates & finds malware on devices.

Encrochat pushes update to fix the issue.

Almost immediately, malware strikes again.

French court authorises French law enf. to take copies of Encrochat VMs from OVH server in Roubaix.

LE takes VM copies.

Court re-authorises the above for another month & grants an order to block OVH and DNS providers from interfering with the operation.

(Unclear if unrelated)
Outage at OVH data centre in Roubaix, claimed due to "router malfunction".

Court re-authorises the above for another month & orders OVH to redirect traffic to LE infrastructure (only Encrochat updates to be affected).

Malware installed on ≥ 20,000 Encrochat devices; ≥ 100,000 messages & 1,136 GB of data captured.

Encrochat informed its SIM provider (KPN) of the attack, which blocked connections to the servers running the attack.

Encrochat issues warning & shuts down.

Dec 2018 Jan 2019 30 Jan 2020 12 Feb 2020 4 Mar 2020 20 Mar 2020 29 Mar 2020 30 Mar 2020 31 Mar 2020 1 Apr 2020 29 Apr 2020 May 2020 26 May 2020 28 May 2020 June 2020 10 June 2020 12 June 2020 ...

Court authorises LE installation of "computer data capture device" on OVH server for 1 month.

Court authorises LE installation of "computer data capture device" on OVH server and devices connected to it for 1 month.

New certificates issued for *.encrochat.network newly using Cloudflare & encrochat.network newly pointed to Cloudflare IP.

Court orders DNS provider (Gandi SAS) to "redirect directly" all traffic for encrochat.ch & its subdomains, for 1 month.

Court re-authorises the above for another 4 months.

Court re-authorises the above for another month.

12:01: DNS nameserver for encrochat.ch changed from dnsmadeeasy.com to gandi.net.

17:15: LE injected their malware into Encrochat's update servers.

23:01: DNS nameserver for encrochat.ch changed from gandi.net to dnsmadeeasy.com.

Court authorises extension of attack to update.zerolegacy.ch.

Encrochat's announcement

12 June 2020

Important Security Notice

Date Issued: 2020-06-12 Date Viewed: 2020-06-13

Today we had our domains seized illegally by government entities. They repurposed our domain to launch an attack to compromise carbon units.

With control of our domain, they managed to launch a malware campaign against the carbon to weaken its security.

Due to the level of sophistication of the attack and the malware code, we can no longer guarantee the security of your device. We took immediate action on our network by disabling connectivity to combat the attack.

You are advised to power off and physically dispose of your device immediately. Period of compromise was about 30 minutes and the best we can ascertain was about 50% of the carbon devices in Europe (due to the Updater schedule).

Timeline of the breach

Users report problems w/ remote wipe functionality.

Encrochat investigates & finds malware on devices.

Encrochat pushes update to fix the issue.

Almost immediately, malware strikes again.

French court authorises French law enf. to take copies of Encrochat VMs from OVH server in Roubaix.

LE takes VM copies.

Court re-authorises the above for another month & grants an order to block OVH and DNS providers from interfering with the operation.

(Unclear if unrelated)
Outage at OVH data centre in Roubaix, claimed due to "router malfunction".

Court re-authorises the above for another month & orders OVH to redirect traffic to LE infrastructure (only Encrochat updates to be affected).

Malware installed on $\geq 20,000$ Encrochat devices; $\geq 100,000$ messages & 1,136 GB of data captured.

Encrochat informed its SIM provider (KPN) of the attack, which blocked connections to the servers running the attack.

Encrochat issues warning & shuts down.

Dec 2018 Jan 2019 30 Jan 2020 12 Feb 2020 4 Mar 2020 20 Mar 2020 29 Mar 2020 30 Mar 2020 31 Mar 2020 1 Apr 2020 29 Apr 2020 May 2020 26 May 2020 28 May 2020 June 2020 10 June 2020 12 June 2020 ...

Court authorises LE installation of "computer data capture device" on OVH server for 1 month.

Court authorises LE installation of "computer data capture device" on OVH server and devices connected to it for 1 month.

New certificates issued for *.encrochat.network newly using Cloudflare & encrochat.network newly pointed to Cloudflare IP.

Court orders DNS provider (Gandi SAS) to "redirect directly" all traffic for encrochat.ch & its subdomains, for 1 month.

Court re-authorises the above for another 4 months.

Court re-authorises the above for another month.

12:01: DNS nameserver for encrochat.ch changed from dnsmadeeasy.com to gandi.net.

17:15: LE injected their malware into Encrochat's update servers.

23:01: DNS nameserver for encrochat.ch changed from gandi.net to dnsmadeeasy.com.

Court authorises extension of attack to update.zerolegacy.ch.

July 2020

BBC

Watch Live

Register

Home

News

Sport

Business

Innovation

Culture

Travel

Earth

Video

Live

Hundreds arrested as crime chat network cracked

2 July 2020

By Danny Shaw, Home affairs correspondent

1:45

The BBC's Tom Symonds is shown how a customised Android phone with EncroChat installed wo

A top-secret communications system used by criminals to trade dr
been "successfully penetrated", says the National Crime Agency.

June 2023

Exclusive news, data and analytics for financial market professionals

LSEG

REUTERS

World

Business

Markets

Sustainability

Legal

Breakingviews

Technology

Investigations

More

My View

Q

Sign In

Register

Europe

Encrypted phone service 'Encrochat' shutdown leads to 6,500 arrests, Europol says

Reuters

June 27, 2023 7:58 AM EDT · Updated 9 months ago

Aa

EUROPOL

EncroChat

[1/5] EncroChat and Europol logos are seen in this illustration taken, June 27, 2023. REUTERS/Dado Ruvic/Illustration

[Purchase Licensing Rights](#)

AMSTERDAM, June 27 (Reuters) - European policing agency Europol said on Tuesday that the takedown of Encrochat, an underground company that offered criminals supposedly secure encrypted communications, led to more than 6,500 arrests and 900 million euros (\$980 million) in seized assets.

The system had an estimated 60,000 users when it shut down abruptly in June 2020, and Europol revealed the following month that law enforcement officials had been intercepting users' communications for months.

Ads by Google

Send feedback

Why this ad? ▸

Report this ad

Feedback

23

Legal process

DOUAI COURT OF APPEAL JUDICIAL COURT OF LILLE

ORDER AUTHORISING THE USE OF A DATA CAPTURE DEVICE (article 706-102-1 of the Code of Criminal Procedure)

We, Sandrine NORMAND, Liberty and Custody Judge at the Court of Lille.

Having regard to articles 706-73, 706-95-1 to 206-102-5 of the Code of Criminal Procedure ;

Having regard to the investigation currently being conducted by the General Directorate of the National Gendarmerie services and the Centre for the Fight against Digital Crime (C3N) under Minutes number 2018/140, of the charges of :

- criminal conspiracy to commit crimes or misdemeanours punishable by ten years' imprisonment (and in particular the offences of trafficking in narcotic products referred to in Article 222-37 of the Penal Code).
- provision of a means of cryptology that does not exclusively ensure authentication or integrity control functions without prior declaration,
- transfer of a means of cryptology not exclusively performing authentication or integrity control functions from a Member State of the European Community without prior declaration
- importing a means of cryptology that does not perform authentication or integrity control functions exclusively without prior declaration,

Legal process

DOUAI COURT OF APPEAL JUDICIAL COURT OF LILLE

ORDER AUTHORISING THE USE OF A DATA CAPTURE DEVICE (article 706-102-1 of the Code of Criminal Procedure)

We, Sandrine NORMAND, Liberty and Custody Judge at the Court of Lille.

Having regard to articles 706-73, 706-95-1 to 206-102-5 of the Code of Criminal Procedure ;

Having regard to the investigation currently being conducted by the General Directorate of the National Gendarmerie services and the Centre for the Fight against Digital Crime (C3N) under Minutes number 2018/140, of the charges of :

- criminal conspiracy to commit crimes or misdemeanours punishable by ten years' imprisonment (and in particular the offences of trafficking in narcotic products referred to in Article 222-37 of the Penal Code).
- provision of a means of cryptology that does not exclusively ensure authentication or integrity control functions without prior declaration,
- transfer of a means of cryptology not exclusively performing authentication or integrity control functions from a Member State of the European Community without prior declaration
- importing a means of cryptology that does not perform authentication or integrity control functions exclusively without prior declaration,

Legal process

DOUAI COURT OF APPEAL JUDICIAL COURT OF LILLE

ORDER AUTHORISING THE USE OF A DATA CAPTURE DEVICE (article 706-102-1 of the Code of Criminal Procedure)

We, Sandrine NORMAND, Liberty and Custody Judge at the Court of Lille.

Having regard to articles 706-73, 706-95-1 to 206-102-5 of the Code of Criminal Procedure ;

Having regard to the investigation currently being conducted by the General Directorate of the National Gendarmerie services and the Centre for the Fight against Digital Crime (C3N) under Minutes number 2018/140, of the charges of :

- criminal conspiracy to commit crimes or misdemeanours punishable by ten years' imprisonment (and in particular the offences of trafficking in narcotic products referred to in Article 222-37 of the Penal Code).

- provision of a means of cryptology that does not exclusively ensure authentication or integrity control functions without prior declaration,
- transfer of a means of cryptology not exclusively performing authentication or integrity control functions from a Member State of the European Community without prior declaration
- importing a means of cryptology that does not perform authentication or integrity control functions exclusively without prior declaration,

Legal process

Previous investigations have confirmed that Encrochat terminals were used for criminal purposes. As it is impossible to analyse the terminals, only the implementation of a computer data capture device would make it possible to bypass the encryption of the data exchanged by users, which all pass through the server located in ROUBAIX. The investigation showed that this was the only way to identify and arrest users engaged in illegal activities. The requested operations being consequently necessary and proportionate to the seriousness of the offences under investigation, the request will be granted.

Early French warrants

Legal process

Previous investigations have confirmed that Encrochat terminals were used for criminal purposes. As it is impossible to analyse the terminals, only the implementation of a computer data capture device would make it possible to bypass the encryption of the data exchanged by users, which all pass through the server located in ROUBAIX. The investigation showed that this was the only way to identify and arrest users engaged in illegal activities. The requested operations being consequently necessary and proportionate to the seriousness of the offences under investigation, the request will be granted.

Early French warrants

Legal process

Previous investigations have confirmed that Encrochat terminals were used for criminal purposes. As it is impossible to analyse the terminals, only the implementation of a computer data capture device would make it possible to bypass the encryption of the data exchanged by users, which all pass through the server located in ROUBAIX. The investigation showed that this was the only way to identify and arrest users engaged in illegal activities. The requested operations being consequently necessary and proportionate to the seriousness of the offences under investigation, the request will be granted.

Early French warrants

Legal process

the measure for the capture of computer data, which effectively began on 1st April 2020, for a period of one month, highlights the following elements:

to date, are very specifically concerned by this data capture measure:

- 32477 telephones, active in a total of 121 countries (list of the IMEI numbers concerned transmitted as an attachment to this request):

- 380 user telephones appear to be active, in whole or in part, on French soil;

Of the 380 telephones active on the national territory, 242 telephones (63.7%) are used for illicit or criminal purposes, the vast majority of which are in the hands of drug traffickers. It should be pointed out that the remaining 138 telephones are active telephones, on the one hand, or not yet in use, on the other hand, given the mass of data that the investigative service has to manage.

The exploited conversations, as well as the examination of the photo files exchanged, showed the importance of the traffic managed by these users, their profound impact on national public order and the profits they generated.

Previous investigations have confirmed that in order to analyse the terminals, only the implementation of a measure to bypass the encryption of the data exchanged was possible. The investigation showed that this was the only way to identify and arrest users engaged in illegal activities. The requested operations being consequently necessary and proportionate to the seriousness of the offences under investigation, the request will be granted.

Early French warrants

Legal process

Previous investigations have confirmed that Encrochat technicians, to analyse the terminals, only the implementation of a tool to bypass the encryption of the data exchanged. The investigation showed that this was the only way to identify and arrest users engaged in illegal activities. The requested operations being consequently necessary for the investigation, the request will be granted.

Early French warrants

the measure for the capture of computer data, which effectively began on 1st April 2020, for a period of one month, highlights the following elements:

to date, are very specifically concerned by this data capture measure:

- 32477 telephones, active in a total of 121 countries (list of the IMEI numbers concerned transmitted as an attachment to this request):

- 380 user telephones appear to be active, in whole or in part, on French soil;

Of the 380 telephones active on the national territory, 242 telephones (63.7%) are used for illicit or criminal purposes, the vast majority of which are in the hands of drug traffickers. It should be pointed out that the remaining 138 telephones are active telephones, on the one hand, or not yet in use, on the other hand, given the mass of data that the investigative service has to manage.

The exploited conversations, as well as the examination of the photo files exchanged, showed the importance of the traffic managed by these users, their profound impact on national public order and the profits they generated.

The elements already gathered since the beginning of this preliminary investigation, in relation to the dedicated nature of this encrypted telephone solution for criminal purposes, were also confirmed by the examination of the section relating to the resellers of these telephones, who appeared to maintain direct links with the technicians and administrators of the platform, and thus to interface with clients that seemed to be demanding.

This configuration was particularly apparent from what the investigators observed during the implementation of the capture tool, which caused a service interruption leading users who were identified as large telephone dealers to inform their customers of the causes and duration of this malfunction, ensuring what should be designated as an after-sales service. These resellers obtained answers from some of their contacts who could be identified as Encrochat technicians and administrators.

In a note on the Encrochat telephone of an Australian reseller, the investigators discovered a perfect manual for marketing encrypted terminals, explaining, in addition to the desired sequence of the various phases of the purchase by the seller until the final sale to the user, that payment should preferably be made by cryptomoney, and that it was obviously necessary to remain discreet in relation to the police, in particular by avoiding being detected by excessively large deliveries (see, in particular, PV 15-17). It could also be stressed that the primary activity of this unwilling dealer was cocaine trafficking.

Legal process

Previous investigations have confirmed that Encrochat, to analyse the terminals, only the implementation of a bypass the encryption of the data exchanged. The investigation showed that this was the only way to identify and arrest users engaged in illegal activities. The requested operations being consequently necessary for the investigation, the request will be granted.

Early French warrants

the measure for the capture of computer data, which effectively began on 1st April 2020, for a period of one month, highlights the following elements:

to date, are very specifically concerned by this data capture measure:

- 32477 telephones, active in a total of 121 countries (list of the IMEI numbers concerned transmitted as an attachment to this request):

- 380 user telephones appear to be active, in whole or in part, on French soil;

Of the 380 telephones active on the national territory, 242 telephones (63.7%) are used for illicit or criminal purposes, the vast majority of which are in the hands of drug traffickers. It should be pointed out that the remaining 138 telephones are active telephones, on the one hand, or not yet in use, on the other hand, given the mass of data that the investigative service has to manage.

The exploited conversations, as well as the examination of the photo files exchanged, showed the importance of the traffic managed by these users, their profound impact on national public order and the profits they generated.

The elements already gathered since the beginning of this preliminary investigation, in relation to the dedicated nature of this encrypted telephone solution for criminal purposes, were also confirmed by the examination of the section relating to the resellers of these telephones, who appeared to maintain direct links with the technicians and administrators of the platform, and thus to interface with clients that seemed to be demanding.

This configuration was particularly apparent from what the investigators observed during the implementation of the capture tool, which caused a service interruption leading users who were identified as large telephone dealers to inform their customers of the causes and duration of this malfunction, ensuring what should be designated as an after-sales service. These resellers obtained answers from some of their contacts who could be identified as Encrochat technicians and administrators.

In a note on the Encrochat telephone of an Australian reseller, the investigators discovered a perfect manual for marketing encrypted terminals, explaining, in addition to the desired sequence of the various phases of the purchase by the seller until the final sale to the user, that payment should preferably be made by cryptomoney, and that it was obviously necessary to remain discreet in relation to the police, in particular by avoiding being detected by excessively large deliveries (see, in particular, PV 15-17). It could also be stressed that the primary activity of this unwilling dealer was cocaine trafficking.

Legal process

the measure for the capture of computer data, which effectively began on 1st April 2020, for a period of one month, highlights the following elements:

to date, are very specifically concerned by this data capture measure

UK court case

"It is the contention of the prosecution that the Encrochat system is used exclusively by criminals engaged in serious organised crime. The reasons provided for this conclusion include, firstly, that the use of Encrochat devices and communications have featured in investigations undertaken by the [UK's National Crime Agency] from around 2016. **It is said that there is both an international and domestic consensus that Encrochat devices are used exclusively by criminals.** The systems provides a secure means for organized crime groups to communicate in relation to their criminal activity. The specific feature of the Encrochat communication system, including the inbuilt facility to erase messages after a given period of time (seven days is the default setting), and the fact that Encrochat devices can only communicate with other Encrochat devices, reinforces the conclusion that has been reached in relation to their use by the criminal community. The prosecution also points to the high cost of using the Encrochat system as supporting evidence: use of a device costs it is estimated between £2400 and £3000 per annum. Further, the devices are distributed by a limited network of outlets and, it is said, in a clandestine way. **The prosecution contends that there is no evidence of Encrochat devices being used for legitimate communication purposes, and in the evidence before the court reliance is placed upon the absence of complaint from any non-criminal or legitimate operator of the system following its disruption set out below."**

R v. Coggins (2021), Liverpool Crown Court (emphasis added)

Legal process

the measure for the capture of computer data, which effectively began on 1st April 2020, for a period of one month, highlights the following elements:

to date, are very specifically concerned by this data capture measure

UK court case

"It is the contention of the prosecution that the Encrochat system is used exclusively by criminals engaged in serious organised crime. The reasons provided for this conclusion include, firstly, that the use of Encrochat devices and communications have featured in investigations undertaken by the [UK's National Crime Agency] from around 2016. **It is said that there is both an international and domestic consensus that Encrochat devices are used exclusively by criminals.** The system provides a secure means for organized crime groups to communicate in relation to their criminal activity. The specific feature of the Encrochat communication system, including the inbuilt facility to erase messages after a given period of time (seven days is the default setting), and the fact that Encrochat devices can only communicate with other Encrochat devices, reinforces the conclusion that has been reached in relation to their use by the criminal community. The prosecution also points to the high cost of using the Encrochat system as supporting evidence: use of a device costs it is estimated between £2400 and £3000 per annum. Further, the devices are distributed by a limited network of outlets and, it is said, in a clandestine way. **The prosecution contends that there is no evidence of Encrochat devices being used for legitimate communication purposes, and in the evidence before the court reliance is placed upon the absence of complaint from any non-criminal or legitimate operator of the system following its disruption set out below."**

R v. Coggins (2021), Liverpool Crown Court (emphasis added)

Legal process

SOLUTIONS

REEDS

PERSONAL LAW

BUSINESS LAW

OUR PEOPLE

ABOUT US

INSIGHTS

CONTACT US

CAREERS

CAN THE DATA FROM THE HACK BE USED IN COURT?

The first question that needs to be answered is: *‘Can the data obtained through the hacking of the carbon units be admitted in court?’*

Unfortunately the answer is not yet clear.

Section 56(1) of the Investigatory Powers Act 2016 (IPA 2016) states that no interception evidence (which evidence that is the product of the hack would count as) can be relied on, **as long as the interception is carried out in the UK** and at least one of the parties to the communication is in the UK.

The question will be whether the hack took place in the UK. Information about the nature of the hack is scarce, and we are unlikely to get the full picture until the first cases go through the court system and the police are forced to disclose the methodology. On the information that we have right now, it appears that the hack itself took place on a French server by French authorities, and so on the face of it s.56(1) IPA 2016 would not apply. However, there is also suggestion that the malware was detected on the carbon units themselves, and it was this malware that provided access to the messages rather than access to the server itself. If this is correct, then there may be an argument that the relevant interception took place in the UK and as such s.56(1) IPA 2016 should apply.

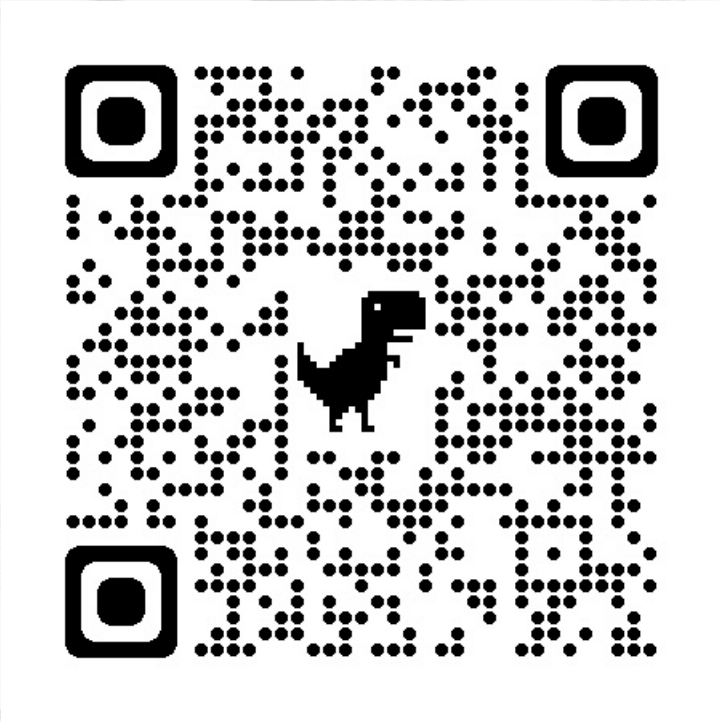
The next question that needs to be asked is whether the authorities properly applied for, and had been granted, the appropriate judicial authority to hack the EncroChat servers and the user's carbon devices. As it was the French authorities undertaking the hack, it is as yet unclear as to whether the appropriate authority was in place. While this avenue of defence will of course be assessed in due course as these cases run through the courts, it is reasonable at this point to assume that the proper authority would have been in place.

The final question is that of attribution: will the police and the prosecution be able link the individual with the phone given the high level of privacy measures in place on the phone. This question can only be answered on a case by case basis, and may well turn on whether the phone was found in the possession of the individual or the police have photographs or other evidence of the device being used by the individual. It will be the job of the defendants' representatives to make the prosecution prove this beyond reasonable doubt.

How we pieced it together (so far)

- 8 French warrants authorizing the surveillance
- Court cases from the UK and Germany
- Media reporting
- Historic DNS/WHOIS records

The warrants



<https://www.documentcloud.org/documents/24479116-lille-warrants>

DOUAI COURT OF APPEAL
JUDICIAL COURT OF

ORDER AUTHORISING THE USE OF A CAPTURE DEVICE
(article 706-102-1 of the Code of Criminal Procedure)

We, Sandrine NORMAND, Liberty and Custody Judge at the Court of Appeal of Douai,

Having regard to articles 706-73, 706-95-1 to 206-102-5 of the Code of Criminal Procedure,

Having regard to the investigation currently being conducted by the Gendarmerie services and the Centre for the Fight against Digital Crime, the charges of :

- criminal conspiracy to commit crimes or misdemeanours;
- particular offences of trafficking in narcotic products referred to in article 706-73 of the Code of Criminal Procedure;
- provision of a means of cryptology that does not exclusively perform functions without prior declaration,
- transfer of a means of cryptology not exclusively performed by a Member State of the European Community without prior declaration,
- importing a means of cryptology that does not perform an exclusively without prior declaration,

Having regard to the attachments and in particular, the report drawn up by the Gendarmerie services,

Having regard to the request of the Public Prosecutor of the Republic of Lille,

On the competence of the liberty and custody judge:

The use of a computer data capture device is a unique investigative tool. Title XXV, Chapter II of Book IV of the Code of Criminal Procedure, provides that the liberty and custody judge at the request of the Public Prosecutor of the Republic of Lille, may authorise the use of such a device in the case of offences falling within the scope of articles 706-73 and 706-74 of the Code of Criminal Procedure, in particular, the association of criminals with a view to the commission of offences, by 10 years' imprisonment, including drug trafficking. The matter is of particular importance for the liberty and custody judge.

On the merits of the case, the following points emerge from the report:

The Public Prosecutor's Office of the JIRS de LILLE was informed, upon request, by investigators from the Centre for the Fight against Digital Crime, the judicial division of the National Gendarmerie - Central Criminal Investigation Service in the problem of encrypted telephones, known as "Encrochat".

These elements were addressed to the JIRS of LILLE given the results of the investigation of the IRCGN, which had established based on the operation of the device that it would function in transmission and reception through contact with a server hosted by the company OVS SAS located in ROUBAIX, thus establishing the use of the device.

The telephones generally used were the OnePlus One; One Plus X, available on the <http://fr.encrochat.network/> website allowed the collection of data with this technology presented as "secure without risk"; guarantee of dual operating system, state-of-the-art hardware, automatic message encryption, hardware cryptographic engine). Several applications were available (instant messaging client), ENCROTALK (encrypts voice conversations and stores them locally on the device).

It appeared that the purchase of such a terminal could not be made directly on the internet. It was possible to find it on the eBay site proposed at the rate of 1610 € for a user license for a period of 6 months.

The investigators were researching to identify criminal proceedings in which such terminals had appeared:

Procedure reference	Relevant department	Nature of the facts
5711/2017	SR ORLEANS (SR = Research section)	In January 2018, the Orléans SR seized 436 kilos of cannabis, a BQ brand phone, an Aquaris X, and a BQ brand phone.
663/2018	SR CLERMONT FERRAND	The SR of CLERMONT FERRAND seized a transporting in his vehicle nearly 400 kilos of cannabis, a phone model Aquaris X, encrypted with an Encrochat identifier.
105/2018	SR CAEN	The Caen SR stopped a motorist during a road check. Placed in police custody, the motorist was found to have had an Encrochat encrypted terminal dedicated to trafficking.
121/2017	SR METZ	During the year 2017, SR METZ, seized 6 kilos of cannabis, stolen goods, and the perpetrators and seized a BQ.
1590/2017	SR METZ	In December 2017, SR Metz arrested a significant drug trafficking operation, seized 6 kilos of cannabis herb, 6 kilos of cannabis resin, two BQ model Aquaris X telephones.
14/2018	SR METZ	Acting as part of the dismantling of a criminal network specialising in jacking thefts of luxury cars, which Belgium, the Metz SR seized 6 kilos of cannabis resin, a phone encrypted by Encrochat, and a BQ brand phone.
13/2018	SR METZ	The METZ SR was seized during 2017, a phone encrypted by Encrochat, a BQ brand phone, and a BQ brand phone.

Several judicial police services may also have been confronted with this problem.

In view of the recurrent appearance of encrypted terminals with regard to criminal proceedings relating to organised crime, and the complexity of the investigation at the international level, the Public Prosecutor's Office of Lille, in the context of the investigation and seized, by means of a notice to proceed sent on 7 December 2017, to the national gendarmerie for commissioning the C3N, of the continuation of the investigation, in particular the crimes of trafficking in narcotic products referred to in article 706-73 of the Code of Criminal Procedure, in a means of cryptology not exclusively performing authentication or integrity control functions without prior declaration and import of a means of cryptology not exclusively performing authentication or integrity control functions without prior declaration.

on the server belonging to the company OVS SAS, located in ROUBAIX (59) rented by the company VIRTUE IMPORTS, located in VANCOUVER (CANADA), through the intermediary of its representative Miguel Eric, hosting the domain name "encrochat.ch" and the sub-domains linked to it, corresponding to the following IP addresses:

145.239.192.28
137.74.125.228
147.135.143.151
147.135.227.208/28
51.38.21.240/28
51.38.255.32/28
178.32.194.53
172.18.46.50
172.18.46.51
145.239.192.49
54.38.250.21
54.38.250.133
145.239.192.63
149.56.251.50
147.135.143.142

SAY THAT, following the combined provisions of Articles 706-95-17 and D 15-1-6, will be required by the judicial police officer, under the supervision of the public prosecutor, access the installation, use, and removal of the technical device(s), all qualified agents of service, unit or organization placed under the authority or supervision of the Ministry of the Interior or Defense and whose list is fixed by decree;

SAY THAT, following the article 706-95-14 provisions, the operations authorized may not, on pain of invalidity, have any purpose other than the investigation and establishment of the offences referred to in this Order, and that the fact that such operations reveal offences other than those referred to in this authorization shall not constitute grounds for invalidating the incidental proceedings;

SAY THAT these acts shall be carried out under our authority and control, that we may order their interruption at any time, that we shall be informed without delay of their completion by the Public Prosecutor and that we shall receive communication of the reports drawn up in the execution of our decision.

Done in Lille the 30th January 2020

Liberty and Custody Judge

[Signature and stamp]

J7

Some takeaways for **real world cryptography**

Not necessarily new, but well illustrated here...

- Herd immunity
- Weak passwords
- Single points of failure
- Attack detection
- Legal & technological barriers to surveillance
- Legal process may provide significant transparency

Some open questions

- What was going on with the nameserver switches on the 1st of April 2020?
- Was Encrochat's update signing key compromised?
- What was going on with zerolegacy.ch ?
- How much collateral damage was there?

The Case of Encrochat

A Real-World Law-Enforcement Hack

Martin Albrecht

Sunoo Park

Michael Specter

Douglas Stebila

King's College London

New York University & NYU School of Law

Georgia Tech

University of Waterloo

`martin.albrecht@kcl.ac.uk`

`sunoo.park@nyu.edu`

`mikespecter@gmail.com`

`dstebila@uwaterloo.ca`