



GRINDROD SHIP MANAGEMENT
a division of GRINDROD SHIPPING (PTE) LTD

MEMORANDUM

To: General Manager

My Ref:

From: Brett McElligott

Date: 30 Nov 2020

Good day Quentin

EMERGENCY RESPONSE CENTRE EXERCISE REPORT: 30 Nov 2020 @ 10h00 hrs

1. Purpose.

- To test company and vessel readiness should an emergency occur
- To test the ability of emergency response team to effectively work together to mitigate the effects of the incident
- To practice coordination between the different teams such as company emergency team and outside parties on a real time basis.
- To test the 24-hour emergency number and all communication equipment
- To test Grindrod Shipping response to the (simulated) media.
- To assess the effectiveness of implementation of contingency plan
- To understand and evaluate logistics requirement.
- To familiarize and to rehearse key personnel of their role during an emergency
- To identify the weakness / lapses (which can be improved later) in our system

2. Attendees

Brett McElligott	SHEQ Manager/Marine Support (Facilitator)
Rennie Govender	Incident Manager
Rajesh Sharma	Incident Coordinator
Mike Allen	Ship Manager/Technical Support
Rajaraman Krishnamoorthy	SHEQ Support
Kerry Everett	SHEQ Support
BREED	
Secure Sphere Cyber Security Consultants	

3. Exercise rule “Cyber Security Virus attack onboard BREEDE”

- SAFETY FIRST. All personnel on board shall be responsible for the safe Navigation and Operation during exercise. If an unsafe condition or operation is discovered, ensure to notify the team members. The Master to determine whether the situation can be corrected and if exercise should continue.
- Begin and end all telephone and radio conversations with the statement “**THIS IS A DRILL**”. Ensure this statement is included on all email exercise documents.
- RECORDS - All documents and checklists exchanged by email used during the Exercise should be maintained. All details to be logged in the as an evidence of the Ship Shore Exercise.
- Some external communication – Flag state, P&I Club and Media (MTI) during this exercise shall be done only with the “role play” person. Port Authorities shall be communicated through agent or as required by agent.
- In the event of a REAL EMERGENCY THIS EXERCISE WILL BE TERMINATED
- All actions taken during the exercise, time, event, and description of activity (such as telephone call or personal contact) shall be recorded.
- ERC shall not be set up in the office in view of governmental restrictions and protection measures against Covid19, but emergency response/video conference shall be set up consisting of the response team members using MS Teams. The video conference shall be treated equivalent to the emergency response centre.
- Debriefing shall be held in office after the exercise. During this debriefing, participants shall discuss the response and identify areas that were well handled, opportunities for improvement, and suggested action items.
- The Master shall follow-up this exercise with a debriefing and evaluation, involving all the exercise participants.

4. Scenario Summary – Exercise “Crossbones”

See Appendix A for full transcript:

....” Yesterday The Vessel BREEDE received a package containing a USB drive. The package was from ChartWorld Navigation and contained USB. The package itself had previously been opened and re sealed with an official customs tape indicating that the South African customs had accessed the package found it to be legitimate and re-sealed the package.

The second mate then upload it the USB contents onto the navigation computer on the bridge once he had completed his duties he went to bed leaving navigation PC running. This morning he returned to the navigation computer to see a skull and crossbones on the screen. He switched the computer off and back on again and the skull and crossbones are still on the screen. I have tried to access computer and cannot do that....”

5. Sequence of Events

	Time, South Africa timings	Event	Remark / Action
1	10h10	Rennie Govender/First Responder received a call from the Master, MT BREEDE: The Navigation PC screen is showing a Skull and Crossbones picture and both ECDIS's are not functioning.	RG
2	10h15	Rennie informs Brett of the incident onboard and Brett is required to assemble the virtual Emergency Response team	BMM
3	10h20	Virtual Emergency team assembled. Rennie briefs the team on the situation onboard the vessel	ALL
4	10h25	Rajesh contacts the vessel to confirm he is the Incident Coordinator and confirms the status of the vessel	RS
5	10h28	IT is also invited to the Virtual ECR. Secure Sphere Cyber Security consultants contacted. RS provided details of suspected PC's onboard BREEDE.	RS
6	10h30	Rennie confirms that Quentin Foyle has been informed. QF to contact CEO.	RG
7	10h33	Initial report sent out.	KE/RG
8	10h35	RK asked to activate the electronic Polestar Charts in order to provide the BREEDE details of diversion to Mossel Bay	RK
9		IT Dept and Secure Sphere Cyber Security consultants begin to run diagnostics on BREEDE's server and two suspected PC's	IT
10	10h36	RG confirmed Charterers, JM and Rahil had been notified of intention to divert the vessel to a safe port i.e. Mossel Bay.	
11	10h38	MBA Requested to get further information regarding Suspected Cyber-attack on ECDIS and also to appoint an agent in Mossel Bay.	MBA

12	10h40	Vessel contacted and provided with coordinates for vessel to follow towards Mossel Bay anchorage. Vessel now confirmed that the masters Laptop was rebooting with suspect wording. Picture of the Laptop and the Navigational PC provided to ECR and Secure Sphere Cyber Security consultants.	
13	10h45	Secure Sphere Cyber Security consultants confirmed that both pc's are to be isolated until further notice.	SSC/IT
14	10h53	MBA Confirmed agent been put on notice and Radio Holland on standby to join the vessel. RG requested that the agent provide paper charts from Mossel Bay to Cape Town to the vessel.	MBA
15	10h56	Sitrep 1 released.	KE
16	11h02	RK Confirmed that Flag State, P&I and Class had been informed regarding a potential Cyber Security attack.	RK
17	11h09	Sitrep 2 released	KE
18	11h10	Secure Sphere Cyber Security consultants confirm that the virus is called Petya ransomware and provide IT Dept. guidance on how to eradicate the virus off the vessel.	SS
19	11h15	Secure Sphere Cyber Security consultants provided software and Grindrod IT Dept commenced the removal of the virus from the affected machines.	SS/IT
20	11h20	Sitrep 3 released	KE
21	11h20	Drill completed.	

6. Conclusion

All present expressed satisfaction with the drill. Minor issue was faced regarding Virtual ECR video conference etiquette with the response team members. All outstanding remarks are contained in Appendix H.



Brett McElligott
SHEQ Manager

Refer attached appendices

Appendix A – Drill description as sent to the BREEDE

Appendix B – Initial report

Appendix C – SITREP

Appendix D – Notification to flag state, P&I Club and Media company (Role play)

Appendix E – Agent Communications

Appendix F - Master's communication with OFFICE

Appendix G – Secure Sphere Cyber Security Consultant Report

Appendix H – Lessons learned and Room for Improvement list.

EXERCISE “Crossbones” - NOTIFICATION

Exercise “Crossbones” is an exercise involving the chemical/oil tanker BREEDE which is currently positioned in South Africa. The exercise is scheduled to take place on Monday 30th November 2020.

1. PARTICIPANTS

MT BREEDE

Grindrod Ship Management Durban – Ship Management/ERC Team.

Secure Sphere Consulting – Cyber Security consultants

Rajaraman and James – Will be observer

Brett McElligott is the facilitator.

Hilton Stroebel and Quentin Foyle are not available to participate in the Drill.

Note: The extent of involvement of Grindrod Ship Management satellite offices and external parties will be determined by the Grindrod Ship Management team as the need arises.

2. GROUND RULES

- a. **Safety is the first priority during the exercise.**
- b. In the event of a real emergency or the exercise becoming compromised the following message will be relayed to all parties **“STOP, STOP, STOP EXERCISE”**.
- c. Begin and end all calls, conversations, and e-mail with **“This is an exercise”**.
- d. Simulated weather conditions will be used during the exercise.

3. OBJECTIVES OF THE EXERCISE

- a. To test the ERC Team and vessels response to an un-announced exercise.
- b. To test ship/shore satellite communications.
- c. To provide the opportunity for the vessel and ERC team to practice handling an un-announced unfolding emergency and to test their response.
- d. To test media response.

4. SCENARIO (Known to Master BREEDE)

- a. The BREEDE is at anchorage or en-route in South Africa

EXERCISE 'Crossbones' – BREEDE SCENARIO STAGE 1

Yesterday The Vessel BREEDE received a package containing a USB drive. The package was from ChartWorld navigation and contained USB. The package itself had previously been opened and re sealed with an official customs tape indicating that the South African customs hat accessed the package found it to be legitimate and re-sealed the package .

The second mate then upload it the USB contents onto the navigation computer on the bridge once he had completed his duties he went to bed leaving navigation PC running. This morning he returned to the navigation computer to see a skull and crossbones on the screen. He switched the computer off and back on again and the skull and crossbones are still on the screen. I have tried to access computer and cannot do that.

I have taken a photograph off the screen and send it to you by WhatsApp. Please be advised this navigation computer is extremely important because it has all the electronic chart updates which was exactly what the second mate was doing yesterday. He also updated the Master ECDIS1 using the same USB yesterday. He is about to update the Slave ECDIS 2



EXERCISE 'Crossbones' – BREEDE SCENARIO STAGE 2**Scenario Stage 2 – IMMEDIATE AFTERMATH** (Only known to the Master)

I've just gone down to my cabin and have noted on my laptop that's my C drive has been compromised and there is a full reboot occurring at the moment. Currently it is 16% complete. I have taken a photograph off my screen on the laptop and will send it to you by WhatsApp.

Please advise what action we need to be taking it because it appears that our computer system and network may have been compromised. Please note that now both the navigation computer and my laptop have been compromised so we have no means updating electronic charts.

```
Repairing file system on C:
```

```
The type of the file system is NTFS.
```

```
One of your disks contains errors and needs to be repaired. This process  
may take several hours to complete. It is strongly recommended to let it  
complete.
```

```
WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD  
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED  
IN!
```

```
CHKDSK is repairing sector 32576 of 191968 (16%)
```

The OOW has just reported that the Master ECDIS and the Slave ECDIS have now failed.

• Bunker quantity on board:	Nil
• Any Oil Spill:	Nil
• Approx Quantity spilt over board:	Nil
• Next Port and distance	Mossel Bay 31 miles
<u>Weather conditions:</u>	
• Wind:	Force 4
• Direction :	SW
• Speed (Beaufort):	
• Sea:	Moderate - visibility good
• Direction	
• Height (m)	

Reminder: Master/Office to follow the relevant contingency plan

Inform:

QF, HS, DPA :

Appendix C

All Emails are to be sent to the following address:
globalerc@grindrodshipping.com



FOLLOW UP SITUATION REPORT

Ship Name	MT BREEDE
SITREP NO:	01
Date and Time (UTC) of situation report:	30/11/2020 10h56
<u>Summary / Update of the incident</u>	Vessel ECDIS not working Vessel instructed to stop Vessel will be updated of next co-ordinates to sail to Captain connected laptop to bridge - laptop now updating. IT to check Passage plan has been updated manually Vessel instruction to disconnect bridge PC from LAN connection and not to connect Captains Laptop
Information received from:	Captain Moodley
Number/Details of Casualties:	0
Damages:	ECDIS Fail
Any external assistance required:	Cyber Security Consultants - Hayden Anderson Radio Holland
Authorities Involved:	
Emergency Services Involved:	

Response Services Involved:	
Company Emergency Response Activities:	Emergency Response Team activated via Teams Jeremy Miles / Unicorn Tankers / Shaminder Rahil notified
Press Media Coverage:	
Press Response:	
Report Sheet Issued By:	
Name:	Kerry Everett
Title:	SHEQ Representative
Contact Details:	031 3027911



FOLLOW UP SITUATION REPORT

Ship Name	MT BREEDE
SITREP NO:	02
Date and Time (UTC) of situation report:	30/11/2020 11:09
<u>Summary / Update of the incident</u>	Captain received cyber security message - has been forwarded to Cyber Security Consultants for analysis Vessel now at anchor in Mossel Bay Agents appointed IT Department reviewing

	FURUNO technicians have been appointed and will be on their way to Mossel Bay later today Ship to remain at anchorage until IT and makers technician have rectified the problems
Information received from:	Captain Moodley
Number/Details of Casualties:	0
Damages:	ECDIS Fail
Any external assistance required:	Cyber Security Consultants - Hayden Anderson Radio Holland Sturrock to be appointed as Agents
Authorities Involved:	Flag State informed P & I informed Class Informed
Emergency Services Involved:	
Response Services Involved:	
Company Emergency Response Activities:	Emergency Response Team activated via Teams Jeremy Miles / Unicorn Tankers / Shaminder Rahil notified
Press Media Coverage:	
Press Response:	
Report Sheet Issued By:	
Name:	Kerry Everett
Title:	SHEQ Representative
Contact Details:	031 3027911



FOLLOW UP SITUATION REPORT

Ship Name	MT BREEDE
SITREP NO:	03
Date and Time (UTC) of situation report:	30/11/2020 11:09
<u>Summary / Update of the incident</u>	Both USB and Bridge laptop has been isolated Captains laptop at 60% of scan ECDIS Updates will be e-mailed to Masters laptop Updated paper charts to be sent onboard for voyage from Mossel Bay to Cape Town. New USB with updates to be sent to Cape Town for the vessel to update Virus identified
Information received from:	Captain Moodley
Number/Details of Casualties:	0
Damages:	ECDIS Fail
Any external assistance required:	Cyber Security Consultants - Hayden Anderson Radio Holland Sturrock to be appointed as Agents
Authorities Involved:	Flag State informed P & I informed Class Informed

Emergency Services Involved:	
Response Services Involved:	
Company Emergency Response Activities:	Emergency Response Team activated via Teams Jeremy Miles / Unicorn Tankers / Shaminder Rahil notified
Press Media Coverage:	
Press Response:	
Report Sheet Issued By:	
Name:	Kerry Everett
Title:	SHEQ Representative
Contact Details:	031 3027911

Appendix D

From: [Rajaraman Krishnamoorthy - GSM SG](#)
To: [Rajesh Sharma - UNT SG](#); [Rennie Govender - DURUNT](#); [Brett McElligott - DURUNT](#)
Cc: [Mike Allen - DURUNT](#); [Kerry Everett - DURUNT](#)
Subject: RE: Cyber Security Drill - IVS BREEDE - DRILL DRILL DRILL - SITREP
Date: Monday, 30 November 2020 11:11:48

TO:

Flag State

P&I CLUB

CLASS

H&M

Dear Sirs

Vessel updated position: **1050lt: 34° 29.1'S / 022° 28.0'E - Mossel Bay Pilot station bearing 323° x 23.1' miles.**

Current course 323°T / Speed 10.5knts

Capt K. Rajaraman

Capt K. Rajaraman

DPA/CSO/SHEQ Manager

Grindrod Ship Management, A Division Of Grindrod Shipping Pte. Ltd.

200 Cantonment Road, #03-01

Southpoint, Singapore 089763

☎: +65 6323 0048 | 📠: +65 9777 1521

✉ technical@grindrodshipman.com

From: Rajaraman Krishnamoorthy - GSM SG

Sent: Monday, 30 November 2020 5:04 pm

To: Rajesh Sharma - UNT SG <RajeshS@unicornshipping.co.za>; Rennie Govender - DURUNT <Rennieg@grindrodshipping.com>; Brett McElligott - DURUNT <BrettM@grindrodshipping.com>

Cc: Mike Allen - DURUNT <mikea@grindrodshipping.com>

Subject: RE: Cyber Security Drill - IVS BREEDE - DRILL DRILL DRILL

TO:

Flag State

P&I CLUB

CLASS

H&M

Dear Sirs

Please note that Master of IVS BREEDE has informed that both the eccdis have failed.

Please find below INITIAL REPORT from the Master.

We have activated the emergency response plan as per our SMS.

We will update the situation report in due course

Capt K. Rajaraman

Capt K. Rajaraman

DPA/CSO/SHEQ Manager

Grindrod Ship Management, A Division Of Grindrod Shipping Pte. Ltd.

200 Cantonment Road, #03-01

Southpoint, Singapore 089763

☎: +65 6323 0048 | 📠: +65 9777 1521

✉ technical@grindrodshipman.com

From: BREEDE - MASTER (O365) <breede.master@grindrodfleet.com>

Sent: Monday, 30 November 2020 4:48 pm

To: Rajesh Sharma - UNT SG <RajeshS@unicornshipping.co.za>; Rennie Govender - DURUNT <Rennieg@grindrodshipping.com>; Brett McElligott - DURUNT <BrettM@grindrodshipping.com>

Cc: Mike Allen - DURUNT <mikea@grindrodshipping.com>; Rajaraman Krishnamoorthy - GSM SG <RajaramanK@grindrodshipman.com>

Subject: RE: Cyber Security Drill - Exercise Crossbones

Good Day Rajesh,

FOR DRILL PURPOSES ONLY!!!

Master was advised by 3NO shortly before 1000lt this morning that ECDIS 1 (Master) had crashed.

Shortly after I appeared on the bridge, we had ECDIS 2 (Slave) crash.

Following actions have been taken as per vessel contingency:

- Bridge manning level increased to BML 4 – Master Moodley / 2NO Campos / 3NO Griffiths / AB Mbanjwa
- Contingency anchorage on passage selected. Due to bridge team familiarity and proximity to Mossel Bay approach, we have decided to divert towards Mossel Bay anchorage for assistance.
- **Position: 34° 35.5' S / 022° 33.8'E Mossel Bay Pilot station bearing 323° x 31.1' miles.**
- MRCC Cape Town has been advised via Cape Town radio of vessels ECDIS failure and subsequent diversion to Mossel Bay.
- Engine room has been informed of ECDIS failure and main engine is on standby.
- Mossel Bay port control will be advised of situation once we are within VHF range
- As per local requirements permission to anchor in Mossel Bay must be obtained from

local SAMSA office, and I will contact agents to obtain permission.

- Weather is moderate, and visibility very good. Currently not much traffic in the area.

Will revert with updates.

Best Regards,

Captain Sagren Moodley

MT BREEDE : Master

Email : breede.master@grindrodfleet.com

Mobile : +27 (0)82 891 5492

Sat phone : +65 315 89054 (Master)

Sat phone : +65 315 89086 (Bridge)

FBB : +870 773 929962

SatC email :456417311.satC@GLOBEMAIL.COM

CAUTION: Our Email system is Internet based but not monitored continuously.

If you require an **URGENT** response please phone the ship (numbers listed above) and/or kindly send us an INM-C TELEX msg.

=====

Email Legal Notice - <http://www.grinshipping.com/Content/EmailLegalNotice>

Appendix E

From: [Jethro Moses](#)
To: [Mike Allen - DURUNT](#)
Cc: [Unicorn Shipping - Safety](#)
Subject: RE: Drill Drill Drill
Date: Monday, 30 November 2020 11:13:23
Attachments: [0.png](#)
[1.png](#)
[2.png](#)

To: Mike Allen

Fm: Jethro Moses |Sturrock Grindrod Maritime | Mossel Bay | As agents only|

Re: MESSAGE ACKNOWLEDGEMENT

Good day Mike

Your message well received and noted.

We will arrange for the transport and embarkation of the service engineer.

Regards

Jethro Moses
Operations Superintendent
Sturrock Grindrod Maritime (Pty) Ltd - As Agents Only
Tel: +27 44 690 5151 | Cell: +27 82 322 3483
Email: JethroM@sturrockgrindrod.com | sgm.mzy.agency@sturrockgrindrod.com



As Agents Only

55 Marsh Street, Mossel Bay, 6506
PO Box 17, Mossel Bay, 6500, South Africa
P +27 44 690 5151, **F** +27 44 691 3311, **M** +27 82 322 3483
E JethroM@sturrockgrindrod.com

www.sturrockgrindrod.com



Sturrock Grindrod Maritime is Trace and ISO 9001:2015 certified, a member of the South African Association of Ship Operators and Agents (SAASOA) and the South African Oil and Gas Association (SAOGA).

SGM | A Grindrod Group Company

SHIPS AGENCY | TECHNICAL | LOGISTICS | OFFSHORE

Email Legal Notice - http://www.grindrod.com/email_legal.aspx

From: Mike Allen - DURUNT <mikea@grindrodshipping.com>
Sent: 30 November 2020 11:09 AM
To: Jethro Moses <JethroM@sturrockgrindrod.com>
Cc: Unicorn Shipping - Safety <safety@unicornshipping.co.za>

Subject: Drill Drill Drill

Hi Jethro

Drill Drill Drill : We have the Breede anchored in Mossel bay with both ECDIS failed due to Cyber Attach. There is a Radio Holland Branch in Mossel Bay we need you to arrange to send a service Engineer out to the vessel on a launch to assist with getting them both operational operational.

Regards
Mike Allen

CAUTION: Our Email system is Internet based, but not monitored continuously. If you need an URGENT reply by return, please phone us.

Ship Manager | Grindrod Ship Management, A Division of Grindrod Shipping Pte. Ltd.
| 📞: +27 31 302 7215 | 📠 +27 82 737 7535
| ✉️ mikea@grindrodshipping.com



Please consider the environment before printing this email and/or any related attachments

Email Legal Notice - <http://www.grinshipping.com/Content/EmailLegalNotice>

Appendix F

From: [BREDE - MASTER \(O365\)](#)
To: [Rajesh Sharma - UNT SG](#); [Rennie Govender - DURUNT](#); [Brett McElligott - DURUNT](#); [Dereck Webb - GSH DBN](#)
Cc: [Mike Allen - DURUNT](#); [Rajaraman Krishnamoorthy - GSM SG](#); [Unicorn Shipping - Technical](#)
Subject: RE: Cyber Security Drill - Exercise Crossbones
Date: Monday, 30 November 2020 11:21:34
Attachments: [image001.png](#)

Hi Rajesh,

FOR DRILL PURPOSES ONLY!!!

Confirming receipt of below position plot, and noted we can stand down from the drill.

Best Regards,

Captain Sagren Moodley
MT BREDE : Master

Email : brede.master@grindrodfleet.com
Mobile : +27 (0)82 891 5492
Sat phone : +65 315 89054 (Master)
Sat phone : +65 315 89086 (Bridge)
FBB : +870 773 929962
SatC email : 456417311.satC@GLOBEEMAIL.COM

CAUTION: Our Email system is Internet based but not monitored continuously.
If you require an **URGENT** response please phone the ship (numbers listed above) and/or kindly send us an INM-C TELEX msg.

From: Rajesh Sharma - UNT SG [<mailto:RajeshS@unicornshipping.co.za>]

Sent: 30 November 2020 11:18

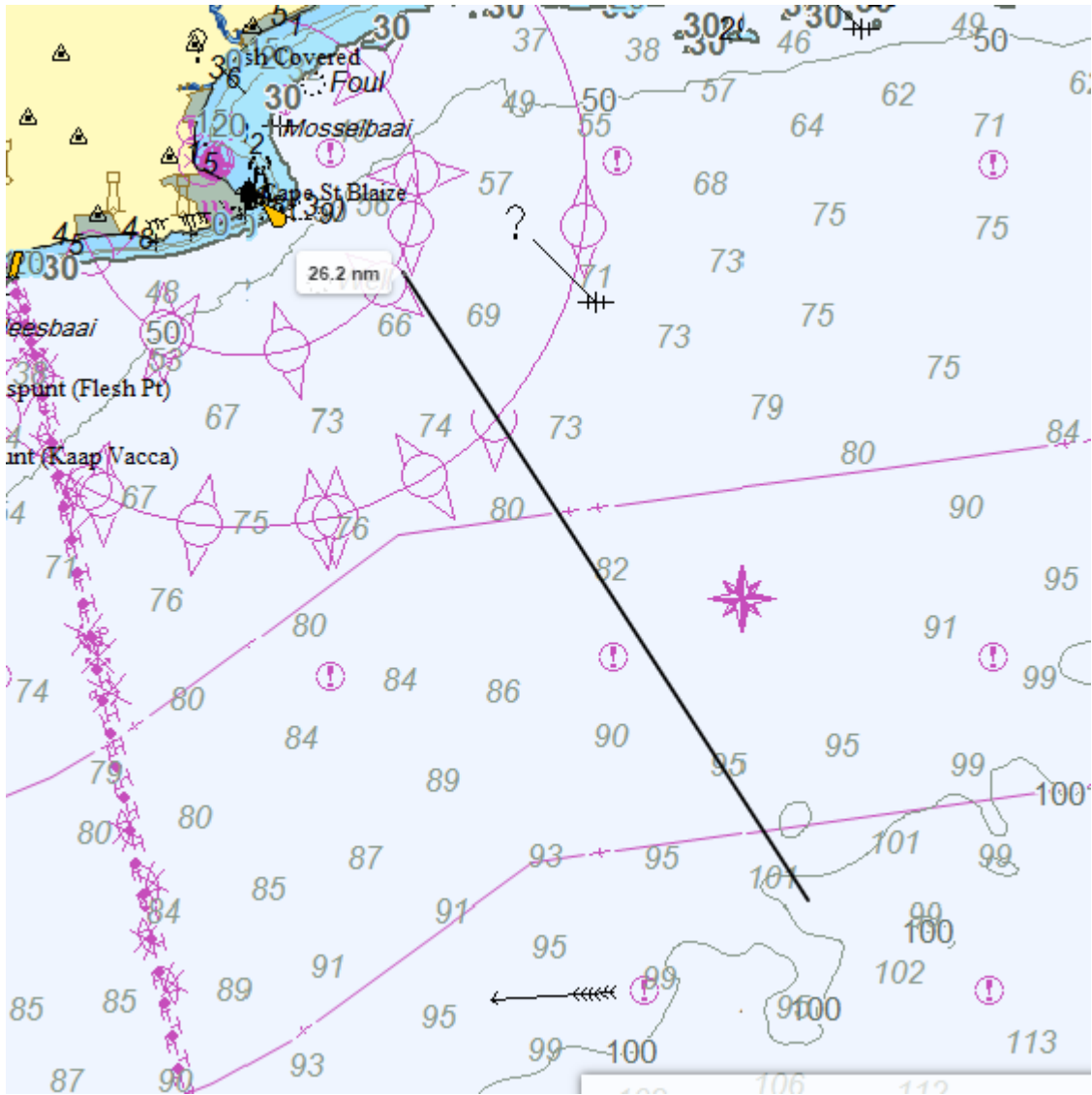
To: BREDE - MASTER (O365) <brede.master@grindrodfleet.com>; Rennie Govender - DURUNT <Rennieg@grindrodshipping.com>; Brett McElligott - DURUNT <BrettM@grindrodshipping.com>

Cc: Mike Allen - DURUNT <mikea@grindrodshipping.com>; Rajaraman Krishnamoorthy - GSM SG <RajaramanK@grindrodshipman.com>; Unicorn Shipping - Technical <technical@unicornshipping.co.za>

Subject: RE: Cyber Security Drill - Exercise Crossbones

Hi Sagren

This is a drill, position plotting on the chart for your information.
Please stand down from the drill.



Regards
Rajesh

From: Rajesh Sharma - UNT SG <RajeshS@unicornshipping.co.za>

Sent: Monday, 30 November 2020 5:05 pm

To: BREEDE - MASTER (O365) <breede.master@grindrodfleet.com>; Rennie Govender - DURUNT <Rennieg@grindrodshipping.com>; Brett McElligott - DURUNT <BrettM@grindrodshipping.com>

Cc: Mike Allen - DURUNT <mikea@grindrodshipping.com>; Rajaraman Krishnamoorthy - GSM SG <RajaramanK@grindrodshipman.com>; Unicorn Shipping - Technical <technical@unicornshipping.co.za>

Subject: RE: Cyber Security Drill - Exercise Crossbones

Hi Sagren

We find present course safe and keep us updated your position every 10 minutes.

Regards
Rajesh

From: BREEDE - MASTER (O365) <breede.master@grindrodfleet.com>

Sent: Monday, 30 November 2020 4:48 pm

To: Rajesh Sharma - UNT SG <RajeshS@unicornshipping.co.za>; Rennie Govender - DURUNT <Rennieg@grindrodshipping.com>; Brett McElligott - DURUNT <BrettM@grindrodshipping.com>

Cc: Mike Allen - DURUNT <mikea@grindrodshipping.com>; Rajaraman Krishnamoorthy - GSM SG <RajaramanK@grindrodshipman.com>

Subject: RE: Cyber Security Drill - Exercise Crossbones

Good Day Rajesh,

FOR DRILL PURPOSES ONLY!!!

Master was advised by 3NO shortly before 1000lt this morning that ECDIS 1 (Master) had crashed.

Shortly after I appeared on the bridge, we had ECDIS 2 (Slave) crash.

Following actions have been taken as per vessel contingency:

- Bridge manning level increased to BML 4 – Master Moodley / 2NO Campos / 3NO Griffiths / AB Mbanjwa
- Contingency anchorage on passage selected. Due to bridge team familiarity and proximity to Mossel Bay approach, we have decided to divert towards Mossel Bay anchorage for assistance.
- **Position: 34° 35.5' S / 022° 33.8'E Mossel Bay Pilot station bearing 323° x 31.1' miles.**
- MRCC Cape Town has been advised via Cape Town radio of vessels ECDIS failure and subsequent diversion to Mossel Bay.
- Engine room has been informed of ECDIS failure and main engine is on standby.
- Mossel Bay port control will be advised of situation once we are within VHF range
- As per local requirements permission to anchor in Mossel Bay must be obtained from local SAMSA office, and I will contact agents to obtain permission.
- Weather is moderate, and visibility very good. Currently not much traffic in the area.

Will revert with updates.

Best Regards,

Captain Sagren Moodley

MT BREEDE : Master

Email : breede.master@grindrodfleet.com

Mobile : +27 (0)82 891 5492

Sat phone : +65 315 89054 (Master)

Sat phone : +65 315 89086 (Bridge)

FBB : +870 773 929962

SatC email :456417311.satC@GLOBEMAIL.COM

CAUTION: Our Email system is Internet based but not monitored continuously.

If you require an **URGENT** response please phone the ship (numbers listed above) and/or kindly send us an INM-C TELEX msg.

=====

From: Brett McElligott - DURUNT [<mailto:BrettM@grindrodshipping.com>]

Sent: 30 November 2020 07:44

To: BREEDE - MASTER (O365) <breede.master@grindrodfleet.com>

Subject: Cyber Security Drill - Exercise Crossbones

Hi Capt. Sagren

I see you are on your way to CT.

I hope you still have time for the drill.

Please could we start the drill at 10h00....

Kind Regards,

Brett

Brett McElligott

SHEQ Manager

Unicorn Shipping, A Division Of Grindrod Shipping South Africa (Pty) Ltd

8th Floor, Grindrod House, 108 Margaret Mncadi Avenue (Victoria Embankment)

Durban 4001, South Africa

P O Box 3483, Durban, 4000, South Africa

☎: +27 (0)31 302 7964 | 📠: +27 (0)82 314 9983

✉ brettm@grindrodshipping.com

CAUTION: Our Email system is not monitored continuously. If you need an URGENT reply please phone the mobile number (number listed above).

Email Legal Notice - <http://www.grinshipping.com/Content/EmailLegalNotice>

Email Legal Notice - <http://www.grinshipping.com/Content/EmailLegalNotice>

Email Legal Notice - <http://www.grinshipping.com/Content/EmailLegalNotice>

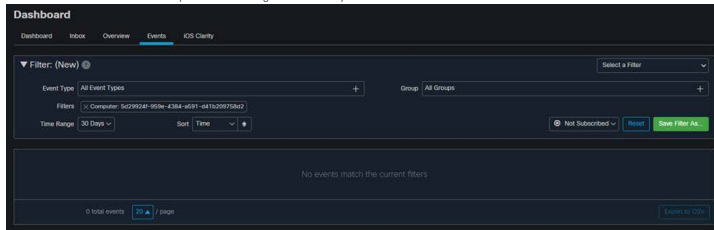
Appendix G

From: [Hayden Anderson \(SSC\)](#)
To: [Brett McElroy \(PDR/IT\)](#), [Rajesh Sharma \(INT/SG\)](#), [Ken Bradford \(SG\)](#)
Cc: [Renuk Shinde \(CSA/DB\)](#), [Zain Dhooma \(CSA/DB\)](#), [SAC - Mike Hayes](#), [Brenn Gowder \(PDR/INT\)](#), [Mike Allen \(ENR/IT\)](#), [Elham Shabbar \(CSA/SG\)](#), [Quentin Egan \(PVS/DB\)](#), [BSE/DC - MASTERS \(DB/IL\)](#)
Subject: Breede Drill Response
Date: Monday, 30 November 2020 14:16:42
Attachments: [image004.png](#)
[BreedeDrillResponse30Nov16.png](#)
[LARGE001 01.01rem - Public Security Incident.pdf](#)

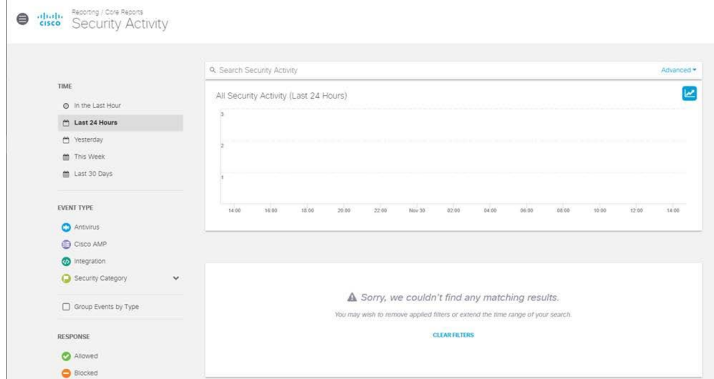
Hi,

On the 30th of November at 10:30 a Cybersecurity drill was conducted on the Grindrod ship Breede. At approximately 10:30 a call was raised with the Secure Sphere Consulting SOC to raise a ticket for an infected PC, a ticket was logged, GRD-907 and escalated to start the investigation.

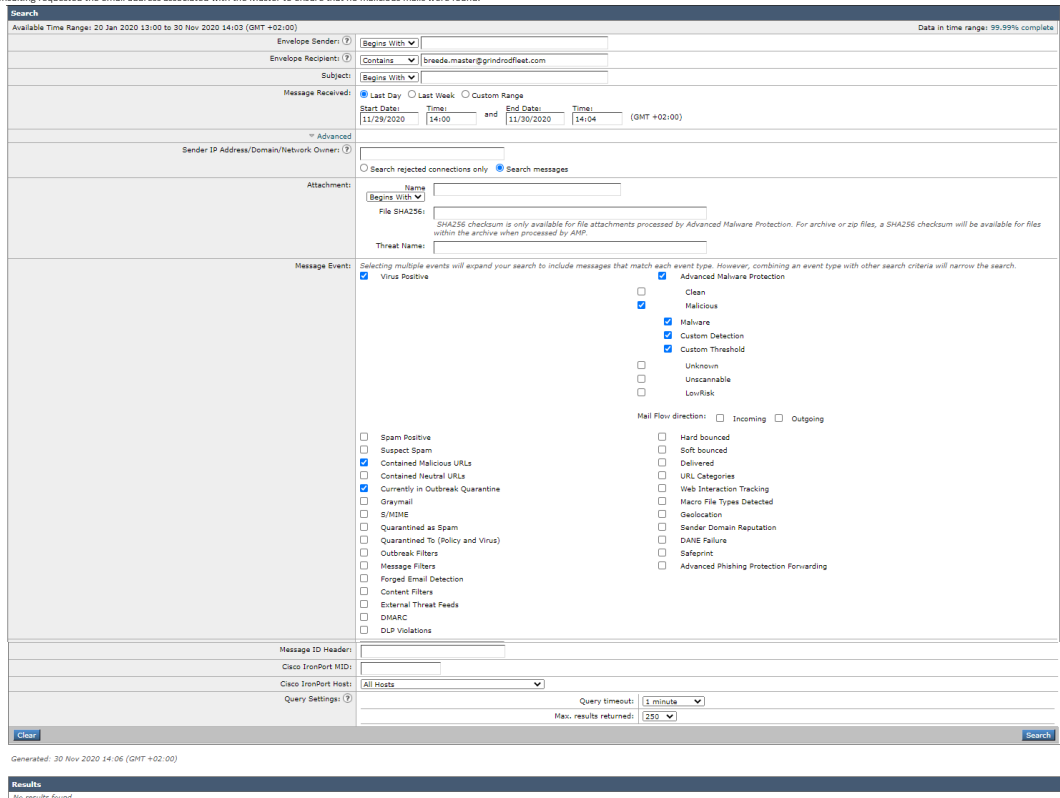
- The SOC analyst was unable to hear the Grindrod Agent and the call dropped before the SOC agent was able to get contact details.
- The call was escalated to Hayden Anderson.
- Hayden Anderson attempted to contact Zain Dhooma to establish communication but his phone went to voicemail.
- At 10:36 a teams session was sent out and Hayden Anderson joined the session.
- On the call asset information was gathered, the below information was gathered.
 - It was explained by Grindrod that an infected memory stick was plugged into the Breede-Bridge PC (IP 10.0.11.28). The system then went offline.
 - Secure Sphere Consulting requested that the Breede-Bridge be taken off the network.
 - Secure Sphere Consulting requested that the memory stick be quarantined by the captain.
 - Checks were performed on the Ship's IP range to ensure that no other systems were compromised.
 - Cisco AMP was checked to ensure that no other endpoints were showing malicious activity.



- Cisco Umbrella was checked to see if any hosts were making any unusual or malicious calls out. It has been noted that there are only two assets on Umbrella.



- Secure Sphere Consulting requested the email address associated with the Master to ensure that no malicious mails were found.



- Screenshots of the events happening on the PC were supplied by Grindrod to Secure Sphere Consulting.
 - Checks were performed on the supplied screenshots and it was determined that the PC was infected with Petya Ransomware (More specifically, Red Petya).

At this point, the drill was concluded and a review performed on the drill.

Secure Sphere Consulting was asked to provide remediation steps to Grindrod for the remediation of the infected PC. During the investigation, an article was found on the Malwarebytes website that outlined steps to attempt to recover the data, this article can be found [here](#). However, since the Ransomware was successfully executed on the Breede-Bridge PC and due to the sensitivity of the system Secure Sphere consulting would recommend that it be reimaged, this will ensure that the system is clean. Steps to be taken would be as follows.

- Secure Sphere Consulting would request Grindrod task an agent to reimage the Breede-Bridge PC.
- Once the base OS image has been installed Secure Sphere Consulting would get in touch with the remote agent to ensure that Cisco AMP and Umbrell be installed on the system.
- Once the device has been onboarded to AMP and Umbrella the OS should be updated to ensure that all patches are installed.
- Only once the system has been updated and onboarded to Cisco AMP and Umbrella should third party software be installed and configured.

- This attack started with a memory stick, as such Secure Sphere Consulting would recommend that all memory sticks on board the vessel be removed from the ship and new devices issues. If this is not possible a low priority device should be identified and taken off the network and drives be scanned to ensure that none of the other devices is infected. Logs of the scans should be taken and supplied to Secure Sphere Consulting to review before the memory sticks are used in the production environment.

Attached please find the ticket logged for the incident with all relevant logs, comments and screenshots.

Thanks

Hayden Anderson



Hayden Anderson
Principal Consultant
T: +27 31 100 0011
C: +27 93 342 5294
W: www.securesphere.co.za
E: hayden.anderson@securesphere.co.za

SECURE SPHERE
CONSULTING






“COVID-19 NOTICE” Please note that Secure Sphere Consulting will be operating as normal albeit that our staff are all working from their home locations during the lockdown. Our normal SOC processes apply for fault logging. Please email support@securesphere.co.za, or call us on 031 100 0011 to log any calls. This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the system manager.

Grindrod IT : PDF documents are flagged as possible threats. This could be a malicious attachment. Please exercise vigilance.

[GRD-907] P1 Alarm - Cyber Security Incident Created: 30/Nov/20 Updated: 30/Nov/20

Status:	Waiting for customer
Project:	Grindrod Shipping
Components:	None
Affects versions:	None
Fix versions:	None

Type:	SIEM	Priority:	Medium
Reporter:	graeme.young	Assignee:	hayden.anderson
Resolution:	Unresolved		
Labels:	None		
Remaining Estimate:	Not Specified		
Time Spent:	Not Specified		
Original Estimate:	Not Specified		

Attachments:	 Document1.docx  image-20201130-090714.png  image-20201130-090740.png  image-20201130-090858.png  image-20201130-090918.png
Timestamp:	30/Nov/20 10:31 AM
True/False grd:	True Positive (Allowed)
Threat Type grd:	Malware
Request participants:	None
Organizations:	None
Time to done:	
Time to first response:	
Time to triage normal change:	

Description

Received phone call from Singapore regarding a Cyber Security Incident on a ship.

The connection was very bad, was unable to gather any further details.

Alarm check on systems for 10.0.11.28

JIRA: 10.0.11.28

Grindrod Shipping ▾ Type: All ▾ Status: All ▾ Assignee: All ▾ + More [Search](#) [Switch to JQL](#)

1-1 of 1

T	Key	Summary	Assignee	Reporter	P	Status	Resolution	Cre
	GRD-907	P1 Alarm - Cyber Security Incident	hayden.anderson	graeme.young	↑	ESCALATED	Unresolved	30/

1-1 of 1

Alienvault: 10.0.11.28

DASHBOARDS ▾ **ACTIVITY** ▾ **ENVIRONMENT** ▾ **REPORTS** ▾ **DATA SOURCES** ▾ **INVESTIGATIONS** **SETTINGS** ▾

Alarms View: Default ▾ ↻

Last 24 Hours ▾ + Suppressed: False x + Alarm Status: Open OR In Review x + Search Phrases: 10.0.11.28 x [Reset](#)

Search & Filters Advanced [Alarms By Intent](#)

Configure filters

Enter search phrase

10.0.11.28 x

Suppressed Not Suppressed

Open In Review Closed

Labels No values found for this filter.

Intent No values found for this filter.

Strategy No values found for this filter.

Method No values found for this filter.

Sensors No values found for this filter.

Source Users No values found for this filter.

⌵ SORT BY: Time Created ▾

ALARM SUMMARY	PRIORITY	ALARM STATUS	SOURCES	DESTINATIONS	SOURCE USERS
No results found.					

Alarm check on systems for 10.0.11.20

JIRA: 10.0.11.20

Grindrod Shipping ▾ Type: All ▾ Status: All ▾ Assignee: All ▾ + More [Search](#) [Switch to JQL](#)

1-1 of 1

T	Key	Summary	Assignee	Reporter	P	Status	Resolution	Creat
	GRD-907	P1 Alarm - Cyber Security Incident	hayden.anderson	graeme.young	↑	ESCALATED	Unresolved	30/N

1-1 of 1

Alienvault: 10.0.11.20

DASHBOARDS ▾ **ACTIVITY** ▾ **ENVIRONMENT** ▾ **REPORTS** ▾ **DATA SOURCES** ▾ **INVESTIGATIONS** **SETTINGS** ▾

Alarms View: Default ▾ ↻

Last 24 Hours ▾ + Suppressed: False x + Alarm Status: Open OR In Review x + Search Phrases: 10.0.11.20 x [Reset](#)

Search & Filters Advanced [Alarms By Intent](#)

Configure filters

Enter search phrase

10.0.11.20 x

Suppressed Not Suppressed

Open In Review Closed

Labels No values found for this filter.

Intent No values found for this filter.

Strategy No values found for this filter.

Method No values found for this filter.

Sensors No values found for this filter.

Source Users No values found for this filter.

⌵ SORT BY: Time Created ▾

ALARM SUMMARY	PRIORITY	ALARM STATUS	SOURCES	DESTINATIONS	SOURCE USERS
No results found.					

Comments

Comment by [graeme.young](#) [30/Nov/20]

P1 Incident, Escalating to Hayden (L3)

Comment by [hayden.anderson](#) [30/Nov/20]

Connected to Microsoft Teams Session.

Comment by [hayden.anderson](#) [30/Nov/20]

Attempted to call Zain, No response from Zain.

Comment by [graeme.young](#) [30/Nov/20]

Investigated AlienVault Events, findings as follows:

No communication from this subnet for the past 90 days.

Comment by [Peter Priest \(SSC\)](#) [30/Nov/20]

Breede Laptop:

Definitions Last Updated

2020-11-30 07:58:09 UTC

Failed

The Connector was unable to reach the TETRA update server. Check your AMP Update Server settings on your policy. Contact Cisco support if the issue persists.

Cisco AMP Check:

Checked 10.0.11.28 at 10:45am - BREEDE-BRIDGE

Checked 10.0.11.20 at 10:am - BREEDE-LAPTOP

No notable event within Cisco AMP, manual investigation of processes executed on asset reveal nothing malicious either.

Comment by [hayden.anderson](#) [30/Nov/20]

Call from Grindrod Ship - Breeda off coast of Mossel Bay.

St Approximately 10:00 CAT a user plugged in a infected memory stick into the Breeda-Bridge PC (IP 10.0.11.28), the memory stick was infected and as such took down the Server, the Atlantis Nav system has gone offline.

SSC has requested that the suspected memory stick be isolated and that the Captin take charge of it and not plug it into any device.

Comment by [chelin.sampson](#) [30/Nov/20]

[Cisco Umbrella (DNS Layer Security) Findings:]

-Cisco Umbrella Multi-Org : SHIP - BREEDE

-x2 Active Roaming Clients:

--BDE-CREW-MINX

--BDE-OFF-MINX

-Cisco Umbrella has not triggered against any malicious DNS traffic between these two assets.

Comment by [graeme.young](#) [30/Nov/20]

As requested by Jon an investigation into the Ransomware variant detected has resulted in the following findings:

The Malware is an old variant of the Petya Ransomware (More specifically, Red Petya)

Read more about the specific variant in this blogpost: <https://blog.pcrisk.com/viruses/9919-petya-ransomware>

There is a master key available for this variant. Free decryptors as well as a remediation guide has been compiled by Malwarebytes at this link:

<https://blog.malwarebytes.com/malwarebytes-news/2017/07/bye-bye-petya-decryptor-old-versions-released/>

Comment by [graeme.young](#) [30/Nov/20]

Investigating ESA (Email security Compliance) findings as follows:

No Malicious emails in the quarantine folder.

Comment by [hayden.anderson](#) [30/Nov/20]

Screenshots from Breeda-Bridge PC supplied by Grindrod.

[Document1.docx](#)

Generated at Mon Nov 30 09:37:46 UTC 2020 by hayden.anderson using Jira 1001.0.0-SNAPSHOT#100152-sha1:66422cef533b318042230625840000d1378eac6a.

Search Labs



SUBSCRIBE



Bye, bye Petya! Decryptor for old versions released.

Posted: July 24, 2017 by [Malwarebytes Labs](#)

Last updated: July 26, 2017

Following the outbreak of the Petya-based malware in Ukraine, the author of the original version, Janus, decided to release his master key, probably closing the project. You can read the full story [here](#).

Based on the released key, we prepared a decryptor that is capable of unlocking all the legitimate versions of Petya ([read more about identifying Petyas](#)):

- Red Petya

- Green Petya (both versions) + Mischa



In case if you have a backup of Petya-encrypted disk, this is the time to take it out from the shelf and kiss your Petya goodbye 😊

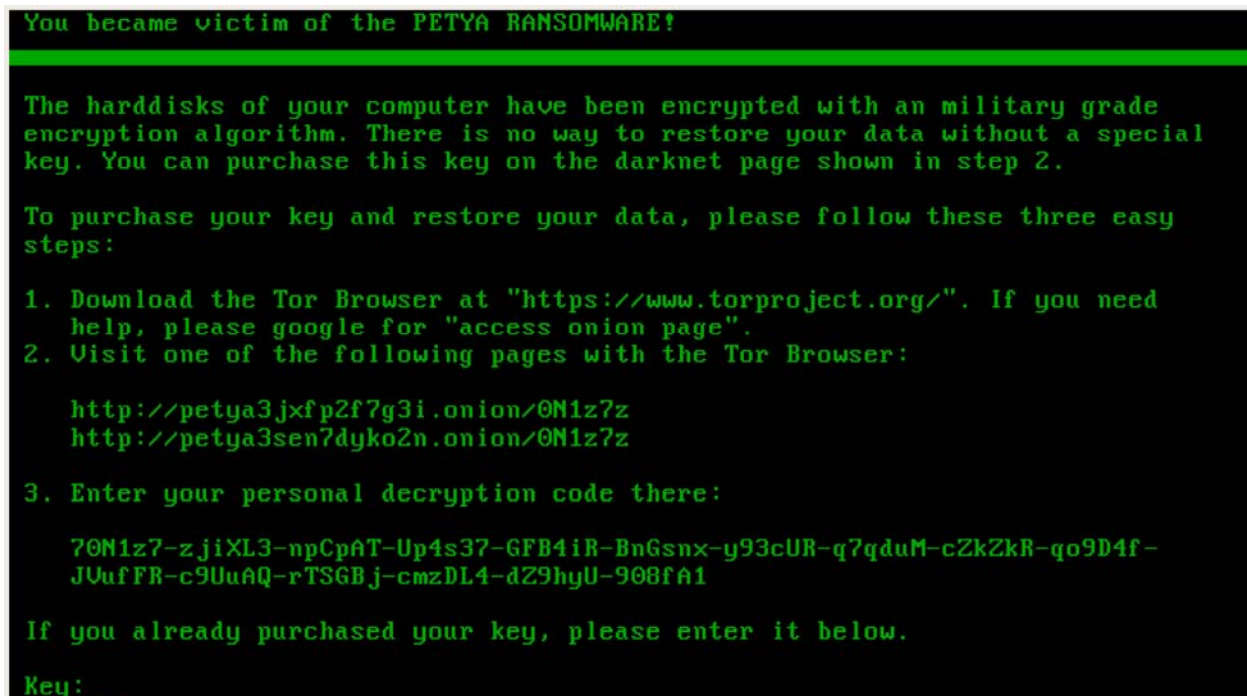
WARNING: During our tests we found that in some cases Petya may hang during decryption, or cause some other problems potentially damaging to your data. That's why, before any decryption attempts, we recommend you to make an additional backup.

// Special thanks to [@Th3PeKo](#) , [@vallejoc](#) and Michael Meyer for all the help in testing!






Variants of the attack

As we know, depending on version Petya may attack your data by two ways:

1 – at a low level, encrypting your Master File Table. For example:



2 – at a high level, encrypting your files one by one (like a typical ransomware). For example:

Malwarebytes LABS	Date modified	Type	Size
 square1 - Copy - Copy.bmp.7QzX	2016-05-12 18:47	7QZX File	141 KB
 square1 - Copy.bmp.7QzX	2016-05-12 18:47	7QZX File	141 KB
 square1.bmp.7QzX	2016-05-12 18:47	7QZX File	141 KB
 YOUR_FILES_ARE_ENCRYPTED.HTM	2016-05-12 18:47	Firefox HTML Doc...	2 KB
 YOUR_FILES_ARE_ENCRYPTED.TXT	2016-05-12 18:47	Text Document	1 KB

Fortunately, the released key allows for recovery in both cases. However the process of decryption will look a bit different.

Decryptors

We prepared two different builds of the recovery tool, to support the specific needs:

1. a [Live CD](#)
2. a [Windows executable](#)

In both cases, the tool decrypts the individual key from the victim ID.

After obtaining the key, you can use the original decryptors in order to recover your files. You can find the links here:

For **Mischa**: <https://drive.google.com/open?id=0Bzb5kQFOXkiSWUZ6dndxZkNTYLE>

For **Goldeneye**: <https://drive.google.com/open?id=0Bzb5kQFOXkiSdTzkUUYxZ0xEeDg>

DISCLAIMER: Those tools are provided as is and you are using them at your own risk. We are not responsible for any damage or lost data.

Defeating the bootlocker

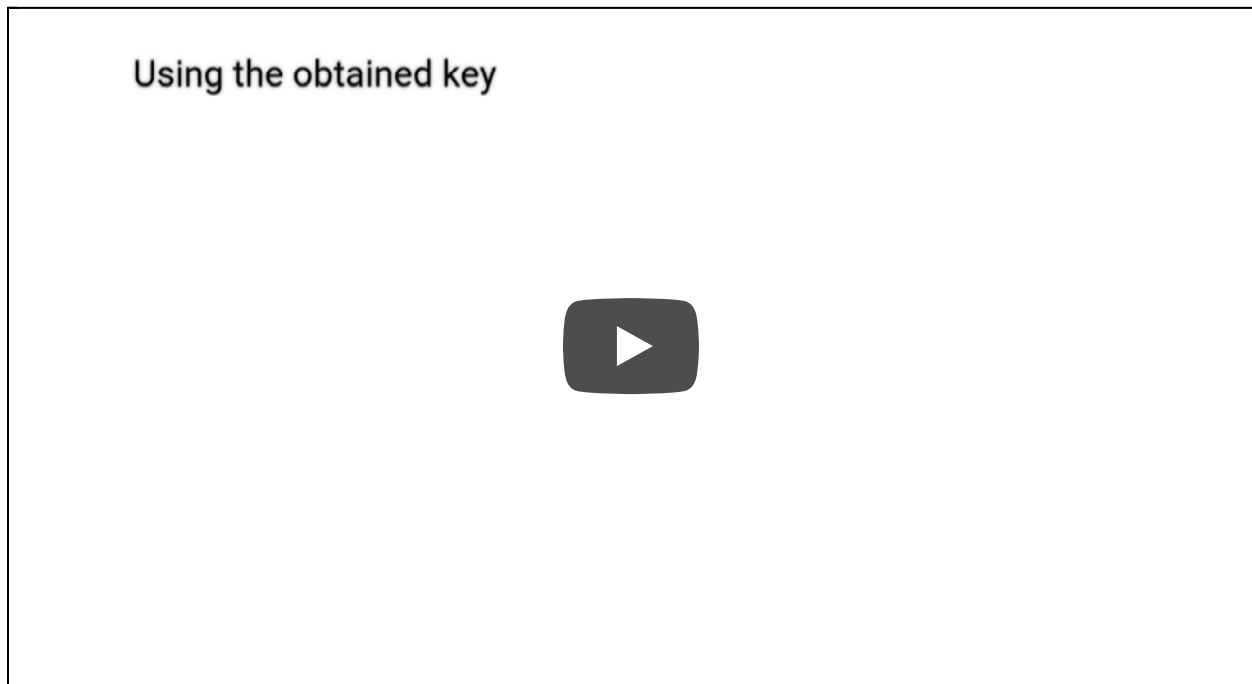
In both cases, you can obtain the key to your Petya by using a Windows Executable and supplying it your victim ID. Detailed instructions has been given [here](#) and on the video below:



However, victim IDs are very long, and retyping them may be painful and prone to mistakes. That's why, we prepared an alternative: a LiveCD that will automatically read it from the encrypted disk. In order to use it, you need to download the ISO and boot from it your infected machine. Then, follow the displayed instructions:



After obtaining the key, you can use it to decrypt your Master File Table:



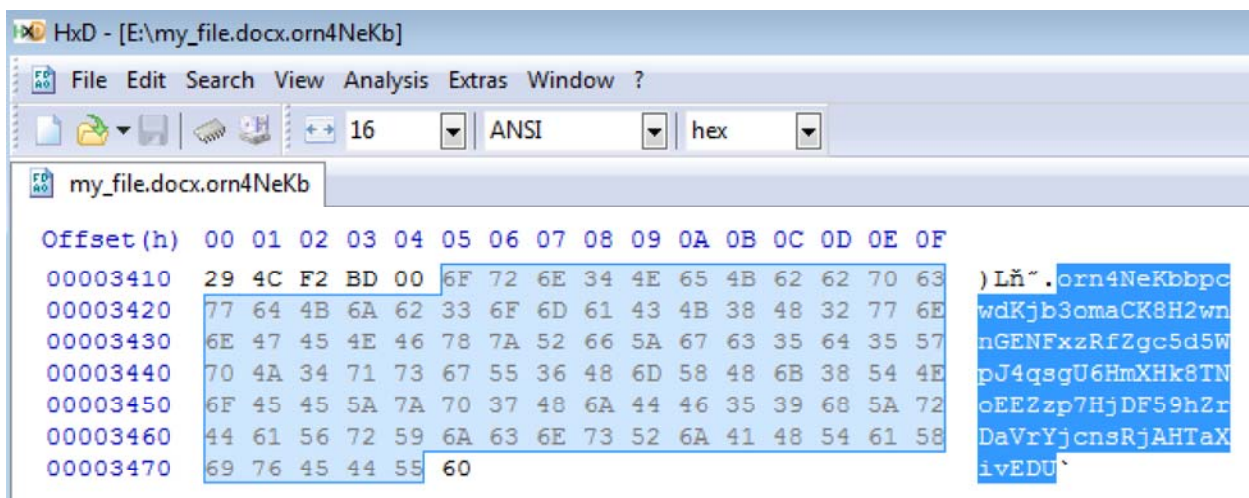
Decrypting files

In case if your files has been encrypted, i.e. by Goldeneye or Mischa, you can use the key decryptor [repaired by Malwarebytes Labs](#) executable.

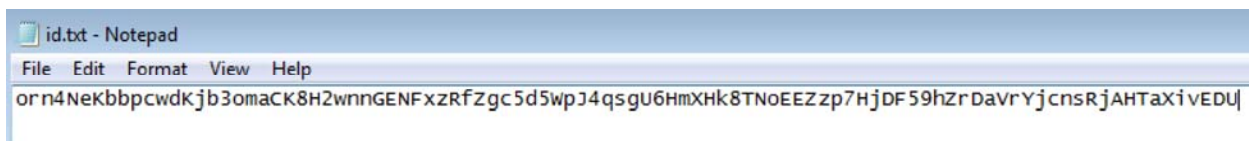
1. Find your victim ID (“personal decryption code”). It will be in your ransom note:



In case if you don't have the note, you can find the ID appended at the end of any of your encrypted files:



2. Save the ID in a file:



3. Use our tool to decrypt your key:



```

C:\Windows\system32\cmd.exe

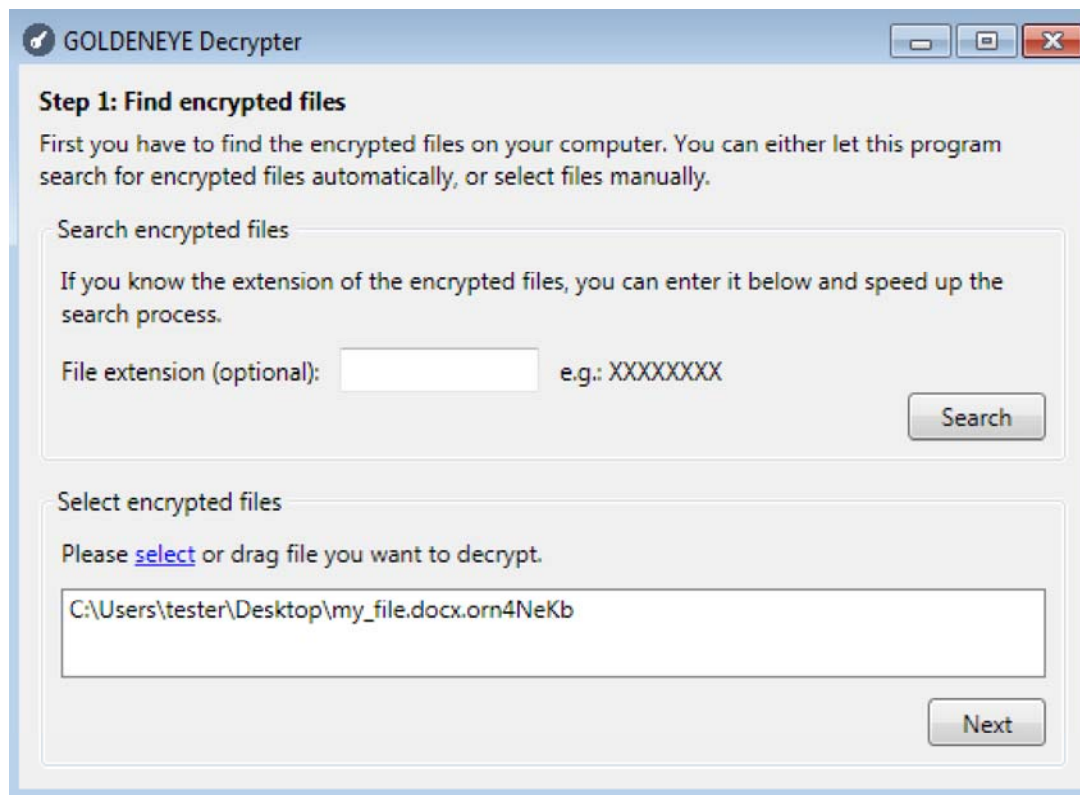
E:\petya_key>petya_key.exe id.txt
priv:      : 38dd46801ce61883433048d6d8c6ab8be18654a2695b4723
Victim file: id.txt
Choose one of the supported variants:
r - Red Petya
g - Green Petya or Mischa
d - Goldeneye
[*] My petya is: d
-----
[+] Your key   : c4ecfe97b775f08923ae2b076fbe9364
Press any key to continue . . . _
  
```

3. Copy the obtained key. Download the original decryptor, appropriate for your version:

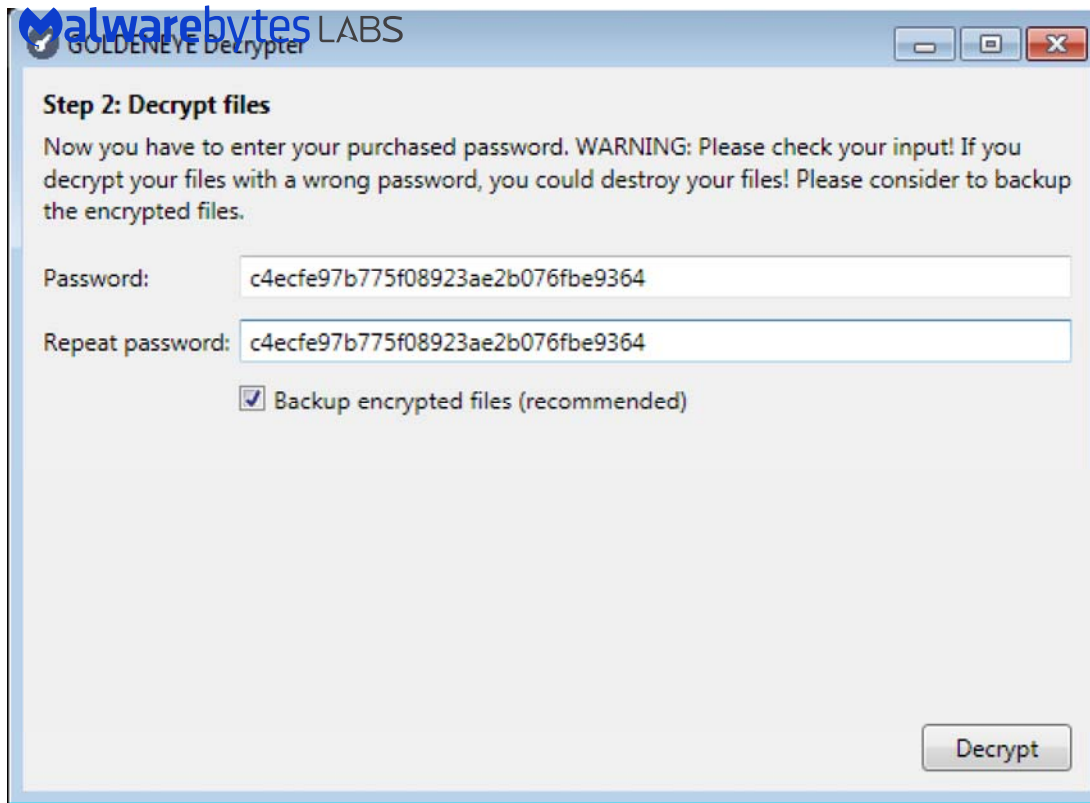
For **Mischa**: <https://drive.google.com/open?id=0Bzb5kQFOXkiSWUZ6dndxZkN1YLE>

For **Goldeneye**: <https://drive.google.com/open?id=0Bzb5kQFOXkiSdTZkUUYxZ0xEeDg>

Choose one of your encrypted files:



Supply the key obtained from the key decoder:



Decrypt the file and check if the output is valid. If everything is fine, you can use the same key to decrypt rest of your files. Supply the extension to the decryptor, and it will find them automatically:



Conclusion

The presented tools allow you to unlock all the legitimate versions of Petya that are released up to now by Janus Cybercrime Solutions. It cannot help the victims of pirated Petyas, like [PetrWrap](#) or [EternalPetya](#) (aka NotPetya). It matches the announcement made by Janus on twitter:



JANUS
@JanusSecretary

Following

Replying to [@hasherezade](#) [@MalwareTechBlog](#)

only [#mischa](#) [#petya](#) and [#goldeneye](#)

Is it the end of Petya's story? Probably yes, however, the future will learn.

This was a guest post written by Hasherezade, an independent researcher and programmer with a strong interest in malware. She is writing in details about malware and sharing threat information with the community. Check her out on Twitter @[hasherezade](#) and her personal blog: <https://hshrzd.wordpress.com>.

SHARE THIS ARTICLE



COMMENTS

Malwarebytes Labs Comment Policy

All comments are welcome, anything with profanity or a URL will be moderated to cut down on spam and offensive content.



Comments for this thread are now closed



8 Comments

Malwarebytes Labs

Disqus' Privacy Policy

Login ▾

Recommend 1

Tweet

Share

Sort by Best ▾



Battista • 3 years ago • edited

Hi guys, i don't find the ID someone can help me?

The infected file was on my site and i don't find the ID.

^ | v • Share ›



Anurag • 3 years ago

Hi,

My system got infected by a ransom malware and all images and important files got corrupted, and converted to be as .cesar files. I used spyhunter and removed the malware and viruses. But files got corrupted

Need your support to aet them decrvpted and to recover the files. As I have the files

RELATED ARTICLES

Spotlight on Troldeh ransomware, aka 'Shade'

March 6, 2019 - Troldeh is ransomware that relies heavily on user interaction. Nevertheless, a recent spike in detections shows it's been successful against businesses in the first few months of 2019.

[CONTINUE READING](#)

 1 Comment

Encryption 101: Decryptor's thought process

March 27, 2018 - In this part of the encryption 101 series, we will begin wrapping it up by going into detail on a ransomware with weak encryption and walking through step-by-step the thought process of creating a decryptor for it.

[CONTINUE READING](#)

 0 Comments

A stolen version of DMA Locker is making the rounds

May 29, 2017 - Pirated versions of DMA-locker are doing the rounds, but there is some good news. All the encrypted data can be decrypted with the same key and we can give it to you.

[CONTINUE READING](#)

 1 Comment

WannaDecrypt your files? The WannaCry solution, for some

May 19, 2017 - A decryptor (Wanakiwi) that has been developed for WannaCry/WannaCrypt/wCrypt. There is a catch though, it only works for some operating systems.

[CONTINUE READING](#)

 2 Comments

From a fake wallet to a Java RAT

January 18, 2017 - We take a look at Adwind, one of the most popular Java Remote Administration Tool. This RAT was distributed via a phishing email and amongst other things, can steal credentials or capture screenshots on the infected machine.

[CONTINUE READING](#)

 1 Comment

Malwarebytes LABS

ABOUT THE AUTHOR



Malwarebytes Labs



[Contributors](#)



[Threat Center](#)



[Glossary](#)



[Scams](#)



[Write for Labs](#)

HEADQUARTERS



Malwarebytes

3979 Freedom Circle, 12th Floor

Santa Clara, CA 95054

FOLLOW US



[Legal](#) [Privacy](#) [Accessibility](#) [Terms of Service](#) © 2020 Malwarebytes

Language [English](#)

Appendix H

	<u>Description of Lessons Learnt / Room for Improvement</u>	<u>Action By / When</u>
1	Certain OneNote software programs on individuals PC's were not operating correctly. Regular tests to be sent to the Ship Managers to ensure their OneNote software programs are correctly configured.	BMM – Once Per Month
2	Virtual ERC etiquette was an issue. People were not muting their microphones when communicating out of the virtual ERC to external Parties. All participants are to mute their microphones unless asked to talk by the Incident Coordinator.	All to Note
3	Virtual ERC etiquette: All participants are to put up their Teams hands to talk. The Incident Coordinator will then invite them to talk. Do not talk over others.	All to Note
4	Virtual ERC etiquette: Remember if you have shared your screen – only share it for as long as the discussion is continuing. Immediately un-share the screen.	All to Note
5	Situation Reports were too slow in getting out. Incident Manger is to ensure that these are done at least every 20 minutes	All to Note
6	With Virtual ERC's it was noted that support had problems trying to write the event log as well as the Sitreps. Another support staff member is to be brought in with the sole purpose of writing the event log.	Nikki to be notified
7	ECR team is to be mindful if external people are participating. They are there for a reason, please ensure their knowledge is brought to the table by giving them a chance to speak.	All to Note
8	Incident Coordinator is to delegate tasks and not take too much on himself. His primary objective is to liaise with the Vessel.	IC
9	The Contingency Plan is to be amended to include the following: <ul style="list-style-type: none"> • Crew to immediately take the pc's offline if they suspect a virus. This can be done by removing LAN or switching the pc's off. • IT Dept to check with other vessels in the fleet whether they are experiencing the same issues as has been reported. • Consider shutting down the entire Grinship Global network so as not to spread the virus. IT can then fault find and open up again under controlled conditions. • IMMARSAT/NSSL to be contacted to run their own diagnostics/virus security checks to ascertain how the virus has spread. 	IT to Note