ADVICE TO MINISTER

CONFIDENTIAL ISSUES NOTE **Ministry: Technology, Innovation and Citizens' Services** **Date: December 22, 2014** **Minister Responsible: Hon. Amrik Virk** Created by Government Communications and Public Engagement	**Malware e-mail attack**

ADVICE AND RECOMMENDED RESPONSE:

- **On December 18, Government was attacked by a malicious file distributed as an e-mail attachment.**
- **As soon as we became aware of the issue, our IT staff took the immediate step to temporarily shut down government email communications to mitigate the exposure to the network and protect against the loss of government information.**
- **Staff rectified the problem and e-mail functionality was restored by the end of the day.**
- **As a result of the attack, the virus had sent out infected e-mails to some external users.**
- **Out of an abundance of caution we have sent an email notification to those external users potentially impacted.**
- **Protection of our data and networks is a top priority and we continue to monitor the situation.**
- **As a result of our measures, we were able to intercept a second attempt by the attackers to disseminate a second infected file.**
- **There is no evidence of any risk or loss to government data.**

If asked about the proliferation to non-government email addresses:

- **According to our investigations, 3,422 external email addresses may have received an infected email.**
- **Out of an abundance of caution on Saturday, December 20 we have sent an email notification to those potentially impacted.**
- **Those individuals who have reason to believe their computer may be infected we recommended to cease online activities that may expose sensitive information.**
- **Best practices are that all computers connected to the internet benefit from updated anti-virus programs and that regular anti-virus scans be conducted.**
- **If individuals have questions regarding this communication please email: citizencontact@gov.bc.ca.**

KEY FACTS ABOUT THE ISSUE:

An email containing an infected attachment was downloaded, and the file contained within it was opened by staff.

As a result, the infected email was automatically sent to everyone in their contact list, causing a rapid proliferation through the government e-mail servers.

To prevent the further spread of the email and downloading the infected email, we took the immediate step to disable the government email system. Government e-mail was unavailable between 10:30 AM and 3:00 PM on Thursday, December 18 2014.

Government continues to monitor and update its security to prevent further attacks.

Infected e-mails may have gone to external recipients.

Government IT security staff have resolved the issue and reiterated the need to avoid opening any suspicious attachments to all staff.

BACKGROUND:

On Thursday December 18, government e-mail servers became infected sending out multiple emails with a malware attachment.

Opening the attachment causes rapid infection as it would send out copies of itself to all e-mail contacts.

1834 out of over 30,000 government computers were infected. This was the direct result of 1834 people opening the attachment.

The attachment contained the 'Dyer' virus which attempts to capture personal financial information from users.

After shutting down the government e-mail servers, IT staff was able to remove the infection and updated the anti-virus definitions to intercept any further attempts.

Up to 3,422 external email addresses may have received infected emails from a government address.

In response government sent out an e-mail to each potential recipient to advise them of the potential issue.

On Monday December 22, 2014 a second attack with a similar virus was intercepted by the government's anti-virus system.

Molyneux, Jennifer MTIC:EX

From: SSBC Client Services MTIC:EX
Sent: Monday, December 22, 2014 10:18 AM
Subject: UPDATE: Security Communique - Malicious eMail

Expires: Sunday, November 27, 2016 12:00 AM

OCIO | Office of the Chief Information Office

To: Information Security Advisory Committee (ISAC), Ministry Service Managers, BPS Service Managers, Ministry Information S Information Officers

UPDATE: Monday, December 22, 2014 – The OCIO has detected a new variant of the malicious email incident that occurred W current variant is a "doc" file, not a "zip" file. The email appears with the following subject line and attachment:

Subject Line: Card Receipt
Attachment Name: CAR014 151239.doc

Please do not open this file should you or your staff receive an email with this subject line or attachment name. The OCIO has to remediate this new variant.

We remind all employees to adhere to the OCIO's Appropriate Use Policy for accessing and managing government informatior

UPDATE: Friday, December 19, 2014 – Email is flowing and disabled IDIRs have now been enabled. Passwords for these infecte of remediation activities, the OCIO is receiving reports of issues sending and receiving email to/from external parties.

ACTIONS: The OCIO is going to take steps to remediate the email issue immediately. This may result in additional risk to Broad clients. These clients should take steps to secure their infrastructure.

Please note, FAQ's related to this incident will be posted on the Client Services SharePoint site. This document will be updated

Wednesday, December 17, 2014

We have reason to believe that starting on December 17, 2014, you may have received an email with the subject line "Invoice

The email notice is malicious as it contains an infected ZIP attachment. In some cases, the attachment may be a link file leadin recommended that you delete the email notice immediately without opening.

To help prevent further infections, we are requesting that you please redistribute this email message to your ministry staff.

ACTIONS REQUIRED:

If you have opened the email but did not open the attachment:

Delete the email

If you have opened the email and have clicked on the attachment (whether or not it "opened"):

Remove the network cable
On laptops, disable the Wireless access tab
Contact the Shared Services Service Desk at 250-387-7000 option 1 immediately for further direction

If you do not 'remember' clicking on the attachment:

Remove the network cable
On laptops, disable the Wireless access tab
Contact the Shared Services Service Desk at 250-387-7000 option 1 immediately for further direction

OCIO efforts are underway to obtain a virus detection solution that can be implemented to prevent further infections.

If you have any questions or require a reimage, clients are advised to contact their Ministry helpdesk or the Customer Service
cschelp@gov.bc.ca or call 7-7000 (toll-free 1 866 660-0811), option 1.

Thank you.
Client Services

2014	12	14	09:00

SIRT (SECURITY INCIDENT RESPONSE TEAM)
December 18, 2014 meeting, 09:00
RE: Malicious email

Summary from notes taken by Jocelyn Schaefer, Change Management
(250) 387-8058

SIRT Director: David Witzer (250 356-0526)
TRACKING TICKET: IM348286 exchange outlook unavailable (P2)
Security Incident # SIRT2014 – 01

Attendees: David Witzer (IT-OC Director) (P); Jocelyn Schaefer (Change Management); Documentation Janice Smyth

Service Management: Martin Webb; Dan Ehle

OCIO: Bette-Jo Hughes; Ian Bailey

OCIO Security:
Perkins, Gary; Prosser, Ken; Michael Foltinek; Muldoon, Trace; Burke Gillespie; Roy Watson

Hosting:
Ian Donaldson; Astinder Singhera

Device Services:
Michael Gergel; Mike Swift; Sandra Guadagni

Network and Messaging Services:
Manfred Wagner; Steve F Smith; Chris Hauff

IDIM: Elizabeth Gillcash; Tonja Quinn

Client Services
Pattie Smith; Sharon Koot; Quinn Daly

IBM:
Natalie Branch; Philip Duffy; Glen Bartlett; Brad Morgan

HPAS:
Richard Edwards

SUMMARY:

2014	12	14	09:00

SIRT (SECURITY INCIDENT RESPONSE TEAM)
December 18, 2014 meeting, 09:00
RE: Malicious email

Discussed shutting down exchange or to take offline to remove the copies and prevent further propogation.

09:23 Decision: stop mail flow and block 2 ZIP files at the gateways

Communications: FEM put up at 77000 option 1, Message posted on @WORKBC, LYNC distlist set up with MCIOs

09:27 Gary to brief Bette Jo for communication to DM
Gary to send note to MCIOs

09:32 Reviewed controls
Remove all copies
determine if more than 2 ZIP files need to be blocked.
Develop plan to scan and remove- this would be a large impact to government and business.
Decision: Block all ZIP files at the gateway.

Requested a strategy from IBM for cleaning desktops and preventing propagation.

Michael Swift to test smart phones to see if impacted.

Investigate sending a broadcast message using Lync

Engage vendors
Team looking for options to disable 2 ZIP files.

Microsoft premier has been engaged, A1 ticket opened. Microsoft is working with several customers on this issue. Ed Capko has been engaged.

Reports that the Gateway block is not complete and messages are being sent via winmail.dat

Decision: Burke Gillespie will block winmail.dat inbound and outbound at the gateway. Manfred will have executable files blocked in Exchange. (or ZIPS inbound and outbound)

HPAS reported No Firewall actions or impact at this time.

Command and control IP addresses 202.156.35.133
192.254.231.157

2014	12	14	09:00

SIRT (SECURITY INCIDENT RESPONSE TEAM)
December 18, 2014 meeting, 09:00
RE: Malicious email

216.177.134.4

10:10 Messaging group reported they did not shutdown information store on exchange 2007. Not necessary.

IBM preparing a GPO to block 2 ZIP files.

10:15 Burke Gillespie reported winmain.dat files are blocked at the gateway.

Gary Perkins reported this is a DYRE virus with the attempt to obtain personal or financial information.

10:20 validating that mail is not flowing in Exchange 2013. (Reports some mail still flowing)

10:35 IBM continues to prepare GPO to block executables. Discussed the options to block at Outlook or to disable 2 ZIP files.
Decision: to review the outlook level once the list of impacted workstations has been compiled.

Quinn Daly reported that approximately 100 social workers idir ids have been disabled and they cannot work on any other applications.
Decision: at this time they should revert to BCP.

413 workstations have been infected and need to get prioritized for reimaging.

Decision: Quinn Daly to communicate that identified prioritized ids will be enabled and individual should work from a different workstation. Also a prioritized list of workstations to be reimaged is required.

Reported that Forefront was blocking on Sharepoint

10:33 Shared File server Shrub server not available. (not related)

10:35 Messaging group is working with Microsoft to remove malicious email from exchange. Severity A. Ed Capko engaged. Messaging is pulling updates from Microsoft every 15 minutes.

09:59 GEMS blocked attachments DAT and ZIP files at the gateway.

10:40 Glen Bartlett reports there are 30 different file types to block discussed focusing on ZIP .

2014	12	14	09:00

SIRT (SECURITY INCIDENT RESPONSE TEAM)
December 18, 2014 meeting, 09:00
RE: Malicious email

Decision: focus on 2 ZIP files then review others once the 2 ZIP files have been blocked. Gary Perkins will manage.

Discussed applying GPO to exchange server as well as GPO. Messaging to investigate.

IBM reported GPO was ready at 10:10 in test. ETA 11:00 for release of GPO in production.
IBM to investigate a script to expedite the deployment. (run GPO force).

Direction to 77000 option1 is to enable priority idir ids but leave infected workstations offline.

Meeting reconvene 11:05.

10:55 invited IDIM group to attend to develop plan for re-enabling idir ids.

Microsoft updated list of files ZIP and Dat files. Payment REF02812_pdf.zip and document 81772.zip.

Rooms 155G and 155H booked for breakouts

10:57 update by devices services smartphones not impacted.

10:44 SF server Shrub rebooted and online. (not related)

11:00 Security to share priority list with ids to be enabled and workstations to be reimaged. With IDIM and IBM.

Quinn Daly to set up conference call with MCIOs

SSISD reported that external clients are impacted, because emails with virus were sent out from the Government email system.

11:05 Blackberry may be impacted. Michael Swift to follow up

Reports of email still flowing. (Haleen Roberts and Wendy Robinson) using DTS. Manfred following up.

Glen Bartlett and Brad Morgan of IBM has joined the team.

11:15 another 12 command and control IP addresses have been identified.

2014	12	14	09:00

SIRT (SECURITY INCIDENT RESPONSE TEAM)
December 18, 2014 meeting, 09:00
RE: Malicious email

Michael Foltinek to forward list to Richard Edwards.

Client Services communicated that technicians are blocking email at the legislature.

12 antivirus vendors detecting the virus, not Symantec yet.

Communications continue to be updated @workbc, FEM at 77000 and lync with MCIO another conference call at 11:45.

Communication with PSA internal communication group to ministry contacts.

Philip reported that the GPO testing is complete and have confidence in the GPO.
Decision: to deploy at 11:30 for Windows 7. Test and go with windows8 and vista machines, and run the script to expedite the GPO propagation.

Cannot test in in TIDIR because of changes made to the environment.

IBM reported 800 tickets received at 77000. Agreed to continue disabling idirs until further notice.

Messaging investigating discovery process to search and destroy – requires privilege access. Approval granted from Chris Hauff.

Gary Perkins noted that we need to widen the scope to include a recommendation on blocking future events if signature is unknown.
GPO secure mail infrastructure waiting for a recommendation from Microsoft.

Roy Watson reported patient 0 opened the original email in Yahoo.com

HPAS reported no performance issues in environment including firewalls.

Network reported autodial to every number in the GAL is available to be sent out. Decision to hold off until reviewed with Ian Bailey and Bette-Jo, then MCIOs. FEM message updated.

Decision block all outbounds to newly identified IP addresses after validated (Michael Foltinek)

Reconvene at 13:00

2014	12	14	09:00

SIRT (SECURITY INCIDENT RESPONSE TEAM)
December 18, 2014 meeting, 09:00
RE: Malicious email

12:30 GPO setup on VISTA and Windows 8. (expect to take 3 hours to fully propagate).
All antivirus providers have identified virus signature.

IBM presented two options for reimage – remotely or onsite. Communication required to reimage workstations any data will be deleted and unable to recover. Client may wish to hold off until files are backed up. IBM to communicate to Security Services of any workstations that have opted to hold off for the backup.

Priorities established. Enable – disabled IDIR then restore mail transport.

Messaging reported that LYNC broadcast is doable.

13:00 IBM reported GPO has been deployed, waiting on status of GPO force.

Messaging reported success on transport layer filter – initiated discusson on when mail transport can be turned back on.

May take 3 days to remove existing files from exchange.

Client Services reported BCEHS requires email for payroll run. BC nurses payroll requires email for their payroll run.

Reconvene at 14:00 to determine when to enable mail transport.

14:30 conference with MCIO scheduled

Requested a list of all users who have been disabled. 1050

IBM reported that Symantec has issued a new definition and is now available. Discussed implementation options during business hours or wait until 20:00. Decision: not to enforce scan during the business day and perform at 20:00. A forced admin scan will be used unless the workstation is on the Ministry exception list. Quinn Daly/ Gary Perkins to validate whether the exceptions should be exempt.
The Symantic scan will include MAC devices.

Search and Destroy – subject lines not file names – Microsoft to report back in 15 minutes with recommendations.

Communications to connect with GCPE Blair Philips to have consistent message through to the Ministries.

2014	12	14	09:00

SIRT (SECURITY INCIDENT RESPONSE TEAM)
December 18, 2014 meeting, 09:00
RE: Malicious email

IBM to prepare reimaging strategy for infected workstations.

JAG is enabling their disconnected workstations. (Future reconsiderations could be an issue with clients taking actions without consulting OCIO.)

14:05 IBM reported 1300 service requests, 1100 incidents opened.
GPO update done compliance report in progress.

Symantec has released a scan and to protect and potentially remediate affected workstations. The scan will be run tonight at 20:00 to protect, but do not expect this will fully remediate infected machines. This will only apply to managed workstations.

Decision : Reimage strategy needs to be reviewed and recommendations made.

Noted it will take time to reimage 1000 workstations. Strategy needs to be developed.

IBM is testing the scan and remediation from Symantec.

Messaging reports a dedicated engineer from Microsoft has been assigned to the incident.

14:30 conference scheduled with MCIO's. Blair Phelps (GCPE) to provide messaging to media and to third parties.

A list of IDIR ids to be enabled has been received.

Decision: 77000 to stop disabling ids.

Discussed the risk of restoration of mail transport.
Decision to restore mail transport with blocking 2 ZIP files. Others to be reviewed. Messaging to monitor.

At gateway, blocking all ZIP and winmail.dat files inbound and outbound

14:30 913 workstations enabled. BC nurses require a disabled id to be enabled to support payroll. Pattie to confirm.

Decision: Begin Search and destroy remediation.

SIRT (SECURITY INCIDENT RESPONSE TEAM)
December 18, 2014 meeting, 09:00
RE: Malicious email

Manfred to send list of exchange servers for proactive monitoring of servers performance. Messaging group is working with SAs Ed Sills and Russ Forester.

14:40 Decision: Mail transport to be started with prudent monitoring.

HPAS reported real time scanning is generally done during the Sunday window because of the impact.
Decision: run scan during Sunday change window.

HPAS reported no infections detected in the Data centres.

Meeting reconvene at 15:30.

15:30 Messaging reported enabled mail transport. Confirmed successful detection and blocking and deletion of the malicious file. All being logged in the message logs. It should take a couple of hours to clear the backlog of emails.

Noted storage would have been an issue if the decision had been made to leave Mail transport disabled overnight. HPAS is monitoring for performance.

15:33 Hot Ticket tracker sent out.

Question was asked if we have control to detect if 100 or more attachments with same name is sent out. This is still in the refinement stage.

Messaging is generating the commands to do search and destroy ETA 16:00.

A new Malware engine has been sent by Microsoft.

IBM reported 1400 SRS and 1200 incident tickets opened. 67% of online workstations have received GPO update including DTS and OUTLOOK.

IBM reported Scan for tonight tested successfully to clear second variant.

Windmain.dat block is causing impact between government and HPAS emails as well as others.
Decision: to leave in until we understand the implications to outside mail.

HPAS reported attachments being stripped and replaced with text file of information that was removed earlier this morning.
Messaging and Security Services to test if a more effective way to accomplish the benefit of blocking winmail.dat in a different way.

2014	12	14	09:00

SIRT (SECURITY INCIDENT RESPONSE TEAM)
December 18, 2014 meeting, 09:00
RE: Malicious email

Messaging reported that search and destroy activity has started

IBM reported that a Project will be required to reimage infected workstations.

Security Services to determine how many workstations have reached out to the control IPs.

IBM reported that 4 out of the 6 prioritized machines have been reimaged, including the patient 0, which was not intended to be reimaged. 1 workstation id requires validation.

Decision to keep infected machine offline until further notice.

Sharon Koot and Natalie Branch to review current FEM.to reaffirm not to reconnect infected workstations to the network.

IBM to prepare a strategy/plan to bring back infected machines.

Roy Watson Services requires an infected workstation (preferable at 4000 Seymour), to enable investigation.

Second variant patient 0 needs to be identified. Do not reimage.

Reconvene Friday Dec 19, at 09:00

2014	12	14	09:00

SIRT (SECURITY INCIDENT RESPONSE TEAM)
December 18, 2014 meeting, 09:00
RE: Malicious email

Action Item Number Closed in yellow	Priority (High, Medium)	Description	Assigned Group	Assignee or Lead		Completed? Y / N	Date Closed	General comments
1218-01	H	Sharon Koot to arrange front-end message on @Work to message to not open any .zip files and that access to email flow will be disabled and update as required.	Client Services	Sharon Koot				15:55 Front end message to be updated to confirm not to connect affected workstations into the network. 11:45 updated
1218-03	H	Natalie Branch will consult with Pattie Smith and update front-end messaging as required.	IBM	Natalie Branch				15:55 Front end message to be updated to confirm not to connect affected workstations into the network.
1218-04		Philip Duffy, IBM, to determine strategy for cleaning off workstations including .zip files	IBM	Philip Duffy				
1218-12		Philip Duffy to create, test and deploy a GPO for Outlook to block all executable content including .zip, .exe and .pdf.	IBM	Philip Duffy				
1218-14		Philip Duffy IBM to start deployment of GPO update script for Office 2010/Windows 7 and trigger script to update the GPO to workstations rather than wait for 90 minute cycle.	IBM	Philip Duffy				Deployed by 1300 hours and will take approximately 3 hours to fully deploy. Awaiting compliance report.
1218-15		Michael Swift to investigate impact to BlackBerries	Device Services	Michael Swift				Initial indications are an SCR cannot be run by BB phone. Further investigation required.
1218-19		Manfred Wagner to develop strategy to implement Search and Destroy on the Exchange application.	Network, Communications and Collaboration Services	Manfred Wagner				Microsoft has been consulted and can now discover by attachments as well as subject line.
1218-23		Michael Foltinek to block all outbound traffic to newly identified and validated IP addresses.	Information Security	Michael Foltinek				
1218-24		Philip Duffy IBM to ensure Symantec scan at 2000 hrs tonight is a forced administrative scan and that exceptions will not be overridden.	IBM	Philip Duffy				
1218-25		Gary Perkins, Information Security, to ask the MCIOs if exceptions from list provided by Natalie Branch should be overridden for the Symantec virus scan.	Information Security	Gary Perkins				
1218-29		Gary Perkins to manage if and when to block the other file types.	Information Security	Gary Perkins				
1218-30		Philip Duffy IBM to lead remediation for affected workstations.	IBM	Philip Duffy				13:50 Dec 18: Want to run full scan and then determine next steps as to reimaging. Reimaging for all those currently affected would involve project if at current number.
1218-31		Client Services to forward any priority lists of priority remediations for workstation to the Investigation branch SecurityInvestigations@gov.bc.ca and cc Michael Swift quoting 2014-2212 in the subject line.	Client Services	Sharon Koot				16:50 Ministry of Finance will send in their priority list to Client Services.
1218-32		Manfred Wagner, working with Burke Gillespie and Exchange group, to determine if winmail.dat still needs to be blocked and if there less impactful methods to accomplish the same results.	Network, Communications and Collaboration Services	Manfred Wagner				