Cyber Event Webinar Q&A 7-30-2019 - 8-2-2019

Question	Answer
Allowed to any DNS destination over port 53*	Allow DNS servers to communicate over port 53 (TCP and UDP) outbound to known external DNS servers ONLY.
And is there any shared threat intel? For example is there reason to believe this a targeted attack vs. random and just spreading through like orgs	Yes, we will post this information in the Cyber Information section of the LouisianaBelieves website.
Are agencies who utilize Statewide Email that is managed by DOA at risk?	No spam filter is impervious. Malicious email can get through.
Are backups on a Microsoft Data Protection Management Server safe from this attack?	Any cloud storage configured in your environment to function like a typical network share is vulnerable to encryption by ransomware.
Are BYOD devices an infection risk that are not part of the domain itself?	Yes, if they are connected to your network. It is recommend that any BYOD devices are segmented from other domain-joined devices in your network.
Are hosted solutions affected?	Infections target Windows workstations and servers. If you have a hosted solution that is not being exposed to you as a Windows server then the hosted solution should be good to go for current target impact standpoint.
Are mac devices and Chromebooks still immune to this? Can smaller leas use mi-fi cellular hotspots with non-windows devices (mentioned above) to maintain contact with critical cloud based systems (PowerSchool, and oneapp mainly)	Have not seen any infections in the Mac devices or chrome books. Solely impacting windows devices. Using mifi with those devices does not seem to be infected. There is a concern of using mifi then reconnecting to the network.
are the connections DNS based and can Cisco Umbrella help stop it?	No. One of the impacted districts uses Cisco Umbrella.
Are the suspect ports inbound or outbound?	Both. We are watching the traffic coming in and out.
Are there any common phishing template/trends used in this attack? We deal with phishing on a daily basis so would want to know what would be a reportable finding.	No, but we do believe there is a preference for phishing emails with attachments.
Are there resources to help vet our content filter configurations?	InfoSec advises schools to complete the six phases; if this is accomplished, we can help with additional content filtering configurations.
Are there specific behaviors that have been exhibited?	One consistent behavior we have seen with this malware is that it attacks at the most inopportune time – e.g. late night, early morning, over the weekend.
Are we saying mac clients can be allowed connect to the internet by other means?	No
Are we supposed to wait for a period of time between executing the various phases of the critical task list? If so, then what is the recommended wait time between phases?	No specific period of time to wait.
Are you able to release what the known encryption file extensions are?	.RYK
As a Google District, can our users access their files in Google Drive while we are down (in Offline Mode)?	Yes in Offline mode
Can a user bring this through out wireless guest network is it a good idea to down the guest wireless network service?	Follow the critical tasks lists.
Can restricting internet access to the servers be done through the filter, or does it have to be done through the hardware?	You do not want to allow any direct server or direct client connection to the internet. Web filters should be configured as a proxy. Ideally all your client communication goes out under user authentication. Not saying this is mandatory. You would have three separate policies on your web content filter proxy. One for students, one for teachers and administrators and one for servers(done by proxies, whitelist resources you need by name).
Can you explain why rebooting servers/workstations has an impact? If the payload has been delivered, will it not execute again upon reboot?	Very important to reboot servers and work stations.......We have seen consistency in certain portions of the phase this malware delays itself is by calling an external PowerShell script, loading it in memory and setting it with a sleep time of a large number of seconds. The way it is executed leaves you with no actual evidence or residue of an executable. It is literally loaded in memory, sleeping waiting to execute. Rebooting your machine will flush that memory.
Can you share a screenshot of what an infected machine does? What does a successful ransomware message look like to the end user?	No.
Did this strain jump sub nets?	Yes.
Do we believe this is a targeted attack?	We do not know for certain, but based on the intel we have gotten so far it appears to be targeting local and state government entities.
Do we have a good list of Google IPs to allow for mail?	Google IP ranges were added to the Critical Task list as an Addendum. Gmail Public IPs https://support.google.com/a/answer/60764?hl=en
Do we have any external IPs or ports yet for DRC and COS?	DRC ports and urls are in the DRC manual-page 26. We can also email you the instructions. Send email to EdTech@la.gov.
Do we know allowable IPs for PowerSchool?	Can possibly be found at https://support.powerschool.com/dir/6687?from=search
Do we know if that vulnerability is specific to Windows 7, or is it also present in Windows 10?	All Windows versions are impacted
Do we know if the execution fires from a scheduled task?	We have noticed this so far in our forensics.

Do we know the reach back target of the software?	No
Do we know where this is coming from? Any specific domains?	No, but review IoCs for outgoing traffic from you network for specific ports that are connected to the malware.
DO we need to be worried about classroom computer management software i.e. LanSchool, Impero?	Anything with a Windows OS you should be concerned about.
Does it bypass user account control?	Yes
Does it use zero day exploits?	Unknown at this time.
Does securly block uncategorized sites? Not seeing an option for that	Please contact your vendor for support.
Does that rule out cloud based web filters?	Dustin least familiar with these. Send screenshot of config and we can give you some instructions.
does this back up system. work with virtual servers	Yes
Does this seem to be automated or active engagement from a threat actor	Both.
Does this virus affect Google Education Suite?	If it is configured like a network share (SMB), it will be encrypted by Ransomware.
does unitrends back up VMware servers as well?	Yes. Good for up to several terabytes. Not meant for really large installations. Doesn't take the place of phase 5. This is a solution to future proof. This is something that would take several months to implement. We can look into rolling it out as a service. Not currently offered to local government. if you want to implement on your own, we can help with that. OTS gets economy of scale when it comes to pricing.
Does VMware infrastructure need to be rebooted before phase 1 and 2 are completed, if an infected system is rebooted is there an indicator of the PowerShell script running that could be use to guess if the system if infected?	No
Don't want to be picky...very grateful, but is the IP list on the updated task list available in excel?	Working on an IP list. Put it in a document to share internally with IT directors based on contact list we have.
Even if we have not been impacted, do we still need to go through these steps?	Yes, if you are school district, charter, or non-public school it is recommended you complete these steps.
Has any AV been picking up on this strand of malware?	No.
Has any information been delivered about what patches needs to installed on servers/workstation to help stop emotet and trickbot from spreading if a machine gets infected?	No, but you should patch all hardware and software with latest firmware and security updates. Also, make sure your AV client is installed on all endpoints and server with the updated definitions.
has any of the virus been decrypted yet for forensics?	No. But sample files are being sent to the FBI for analysis.
Has anyone been able to obtain ports and ips from Heartland or Frontline/Aesop?	Heartland told us that all of their on prim apps communicate over TCP/2923. If you have cloud, it's all 80 and 443
Has data been exfilled or believed to have exfilled or is it lockup in place and ransom for access	No confirm reports of data exfiltration so far.
Has Malwarebytes for teams been patched to detect this if emotet or trickbot are lurking on a system?	Malwarebytes and other vendors are continuously updating their malware/ransomware signatures. However, AV is not a silver bullet to stop this attack. With this malware outbreak every single instance in a new permutation from a signature standpoint making AV detection difficult.
Have all superintendents been notified of these steps?	All superintendents will receive a message from John White today(7-30-19)
Have any Linux based backup solutions been encrypted that we know of?	Linux is not impacted, but if it hosts Samba shares to Windows devices it is backing up it is possible that the files exposed via the service can be encrypted.
Heartland / Mosaic also please	Email was sent to district contacts
How do private schools get notified of updates of information?	Information is being posted under the Cyber Security Info section on the LDOE Homepage - louisianabelieves. com. Also, any email communications related to the Cyber Incident will be sent to public, charter, and non-public schools.
How do we handle SFTP outbound and inbound	Follow the critical task list. If SFTP services is a critical function you will need create ACLs to allow outbound and inbound access to SFTP sites. This should only be allowed by explicit source IPs, destination IPs, and destination ports.
How does this strain migrate across the network? If a person has local admin, but does not have domain admin are they are a risk for allowing it move sideways to the domain controller?	Attackers move laterally across your network collecting credentials, looking for highest privilege account. Never run as an administrator and browse the internet or check email.
How long should we leave the internet turned off?	Follow the critical tasks lists. Internet services we become available in phases.
How many PCs and servers have been found to be infected so far in the (4) districts?	It is a large number. Do not have a total but Windows devices are targeted.
How thorough must the reboot step be? What if we miss a few workgroup computers?	Do not miss any devices.
how will all this affect VoIP systems?	VoIP service will be impacted and will need to be restored in Phase 2
How will we access Jcampus and SER during School hours?	As you get through the phases you will able to get back to your systems. You may have to use paper processes near term. School by school decision. Good to start the process
If end user machines are not rebooted before phase 3 will it cause an issue?	Yes every windows machine must be rebooted before you go to phase 3

If Google is being used and you are only using the web access for it, does that meet the requirements for google only servers?	If you are only using Google then allow port 443 to Gmail IPs
if it calls back out to the internet and we block according to the state police release 19-8480 would that protect us? -tech	No
If our content filter does not proxy, but all 80 and 443 traffic is going through the content filter, can we ignore your statement about proxy only to the internet	This is the only extension we have seen so far.
If server has been set up to dynamically update some specific data to outside vendors like for our cafeteria management software. How do we not have them allowed internet access?	Only allow the server to communicate to with the IPs associated with the vendors and only over the ports required.
If the rogue executable is unknown, then how will backing up systems be effective, i.e., restoring from backup could potentially reintroduce the infected file?	Avoid restoring VMs from backups if it has been impacted by malware. Do a data level restore and do not restore any executable files. Download/Install executables from the original trusted source (CD/DVD media, vendor website or FTP)
If we are using DNS Root Hints for our DNS, should our Firewall rule be Inside DNS Servers Allowed to Any DNS source over port 53?	Only allow internal DNS servers to communicate with root DNS servers over port 53. Client and other servers should be pointing to your internal DNS servers for DNS resolution.
if we detect hits on port 445 trying to hit us and are getting denied, should we assume the devices that are being hit are infected?	Inside your network if you have identified one of the indicators of compromise contact OTS immediately.
If we have done all of the steps except reboot servers, would we need to go back and reblock the other items (to Phase 2) and redo all phases after the reboot.	The order of the task list is very important. It must be followed in the order listed. Do not skip any steps.
If you are using onsite patch management and it is on the same VLAN as the rest of the servers. Working with the recommendation that all internet communication is blocked from all servers, what is the recommendation you would give to make sure that patching can continue? This may not be asked in the correct phase but please answer if possible.	It is not recommended in this phase.
If your BYOD & Guest networks have firewall rules stopping all traffic from crossing over to the student & staff networks is it ok to leave those networks more open to the internet?	No
In phase 6, you have a line item that says to block "websites using IP addresses instead of DNS names". What does this mean and what's the best way to do this? firewall? content filter?	This should be configured at the web content filter. This will prevent browsing to websites using https:\\x.x.x.x IP address instead of the domain name.
in the Indicators of Compromise, the presence of adavapi32.dll is an indicator. This dll though is a core part of windows. Does this dll appear in specific places that are more suspicious than others?	adavapi32- Dustin doesn't consider this as high on the list. It's important to look at domain controllers, core server infrastructure and network traffic. Looking for the ports we listed.
In yesterday's call, it was mentioned that filtering should scan all internet files. Is this the antivirus, not filtering?	Traditionally you have one of two options. You have a filtering mechanism part of a larger suite. The other option is someone not owned by a large software company but they interact with mcafee, etc. If you are not sure what to do contact us through the edtech email, screenshot what you are seeing and we can provide guidance.
Is a tape backup on our financial server enough? We have four tapes and I think they do them nightly but not certain they do them every single day. Is that sufficient?	Recommend following the 3-2-1 backup strategy - https://www.cloudberrylab.com/resources/blog/following-3-2-1-backup-strategy/
Is it possible to get any indicators (Domains, Hashes, IPs)	Yes, IoC and other documents related to this malware will be posted to the DOE website.
Is it still the case that being totally offline is still a protection for a machine that may be potentially compromised?	Any computer that may be infected/compromised should be taken offline. Please unplug from the network or disable the network port but leave the computer powered on. Contact Carol Mosley and your local OEP Director so we can decide if a forensics team needs to come onsite.
Is not rated the same as not categorized in the firewall settings	Maybe. Please confirm with your web content filtering vendor.
Is offsite backup enough, or do you recommend offline backup as well?	You should have a least one offline copy of your backup if this is already happening with your offsite backup then you are in a good posture. Recommend following the 3-2-1 backup strategy - https://www.cloudberrylab.com/resources/blog/following-3-2-1-backup-strategy/
Is the list of outgoing ports listed somewhere that we need to look for?	See IoC document on DOE website
Is the OEP survey the same as the LDOE Cybersecurity Survey?	There are overlapping questions in both. Please complete both surveys.
Is there a "file name" we should look for? Is there a particular pattern to watch for?	There isn't a specific file name to look for. We will update the Indicators of Compromise (IoC) document as we have additional info to share.
is there a certain IP address, URL or file name we can block specifically?	Please follow the Critical Task List.
Is there a hash	No
Is there a minimum amount of time that needs to transpire between phases if the are followed in order?	No
Is there any documentation specific to the Threat Available get a better understanding of the threat?	https://www.louisianabelieves.com/measuringresults/digital-schools
Is there concern about remote access tools such as Log me in, team viewer, bomgar, and go to my pc being exploited and providing an avenue for access?	Yes. See IoC document on the DOE website.
Is this isolated to Louisiana or have nearby states been impacted?	No, it is a nationwide issue

Is this strain routable? Can it jump sub nets or gateways?	Yes.
It was said earlier that traffic was detected at infected sites outbound to pastebin. Do we know what information if any is being dumped there?	Pastebin is pulling. If someone is experiencing this contact OTS immediately. We will allocate a forensic resource to you.
Just so I am clear this is mandatory for all schools entities you listed earlier.	It is strongly recommended that this process is followed to protect your Districts/Schools.
Phase six question: What is the suggested best practices to have servers get their updates if they should have zero internet access?	After you complete phase six you should be able to facilitate your updates. Contact us and we will advise you on how to accomplish this. Please follow the task list and do not modify it.
please share the information with me. I don't know ports for all our sites or ip addresses we need to specify	https://www.louisianabelieves.com/measuringresults/digital-schools
Port 25/587 are for email (SMTP specifically) transmission only, will not enable webmail	If you have G-Suite solution then you can allow ports 80, 443 and 4444
Question on phase 3~5, It has been mentioned not to allow servers access to internet. Any advise on windows update, AV updates, etc.?	After you complete phase six you should be able to facilitate your updates. Contact us and we will advise you on how to accomplish this. Please follow the task list and do not modify it. Servers should not have access to the internet.
Recommendation for all off campus windows laptops?	If they are being used off campus and they are school managed/owned devices the same recommendation applies. Do not bring those devices back into your environment.
securely is a mitm DNS service that runs its own certs that have be pushed out to local machines	Not familiar with securely. Screenshot the web configuration page and send it. We will look at it and if we can't figure out how to configure for uncategorized web traffic we can contact the vendor.
Should we block flash drives or external media?	For this attack, we haven't seen any infections from USB drives. Workstations and servers should be configured to not auto-exec anything on a USB drive.
Should we disable access to Google Drive for now because we have Drive File Stream?	If Google Drive is presented as a network share or is being synced locally to the user's Windows desktop it can be encrypted with Ransomware
So if you can't vendor time until Saturday to help with core router config and assist in FW changes, should the internet be shut down until that time?	Yes. Shut down the Internet to prevent possible impact. This should be discussed with your administration and a final decision made.
so IOC detection is mostly firewall	Dustin stated if you only look at your firewall you are missing some things. Domain controllers are important. If your firewall is giving alerts or any indicators contact us?
So we have mostly off site servers I.e.: cloud servers do we need to worry about these as well?	Depends, If your cloud servers are setup to look and feel like a on-premise server and your users have access to these servers via normal Windows services like SMB shares then they can be impacted.
So will phase 4 be the phase where we can begin security updates and patches?	Yes, If all other phases have been completed.
The Louisiana Association of School Superintendents also has a Toolkit on their website that lists resources for school systems. Please send us any additional information you may have so we may support this effort.	All information is being posted to the Louisiana Believes website. You can link to the site - http://www.louisianabelieves.com/measuringresults/digital-schools
Theoretical question. Could an LEA with sufficiently small number of windows based machines in their inventory, if they could guarantee all such machines were either powered off, or physically disconnected from the network by cable removal or wireless adapter device disablement, could they maintain internet connection for their non-windows machines if they are a managed networking solution and need to wait on management support?	If you have completed phases 1-6 and want to get online with non-windows machine. That's fine. If you want to come up with an option other than following phases 1-6 that is your decision but you accept the risk. We don't want anyone experiencing what the districts that have been compromised have gone through. If you complete phase 1 and want to follow another path other than laid out in phases 1-6 then reach out to Carol.
To clarify, if a system is powered off, unplugged. It needs to be plugged in and turned on, and then rebooted?	If you know for a fact that device has not been plugged up then you do not need to power on then off again then reboot.
We are a google school - do we need to back up these files? I have asked all office staff and personnel to back-up info on their computers to external hard drives - is this sufficient?	Please contact your Google Rep for guidance/recommendation on backing up data store in Google.
We are a small school who uses a contractor for our security. What do we need to do specifically?	Provide the Critical Task list to the contractor that manages your firewall for them to implement. You will need to provide the contractor with the IP ranges of any domains you need to communicate with in each Phase of the task list.
We are being asked if staff can use Starbucks or other hotspot solutions in the time being. is that advised?	We do not advice that at this point in time.
We have 2 backup servers that are scheduled offline by scripts at different times (e.g. they are not online at same time) - one backups on weekdays, then we have the other one come online on the weekend. Then they upload all backups encrypted to google drive. Is this an acceptable solution? What is best practices for backups in windows environment?	If those backup servers are inside your data center, they are not "offline". They are not offline unless you log on to a portal or backup on a different network. Going to the cloud is an excellent idea, as long as they have multiple versions of the backup.
We have State Placement Testing through Thursday. If we allow the state IP ranges, will they be able to test?	That is not hosted through the state servers so we will have to get the IP addresses. Please email EdTech@la.gov if you need these IPs.
we have users trying to get to the LAGov Data Warehouse and the ECC system. The LA whitelist you gave us doesn't seem to completely cover these systems. Do you have additional IPs that can help us properly whitelist these features for LAGov?	Will reach out and get this information. Will add it as an update to incident prevention checklist on https://www.louisianabelieves.com/measuringresults/digital-schools
We have users who are not able to access LASERS, eGRANT?	Looking in to all the state IPs
We use primarily Google Suite for Education for our file services (not MS Server file shares). What is the proscribed backup/restore process for Suite files?	Please contact your Google Rep for guidance/recommendation on backing up data store in Google

We use Securly - do you recommend putting the filter in whitelist mode for now?	InfoSec advises schools to complete the six phases; if this is accomplished, we can help with additional content filtering configurations.
Were the districts hit by this ransomware Google districts?	This malware infection is not related to Google services. It impacts Windows clients and servers. We haven't found any infections on devices running Linux, MacOS, iOS, or Google Chromium (e.g. Google Chromebooks)
Were the suspicious ports UDP or TCP?	Will update on documents posted on https://www.louisianabelieves.com/measuringresults/digital-schools
What about allowing ports for security appliances, virus servers, IPS, Advanced Threat Protection, Cloud-based security and content filtering services etc.?	Not in phase 2
What about G Suite/Google Drive accounts?	If it is configured like a network share (SMB), it will be encrypted by Ransomware.
What are the best practices for backups?	3-2-1: 3 copies of your backup, across 2 locations, with 1 off-site. The number of versions is up to your business case. "Air gap" where your backup server is offline, providing an air gap between your network and data.
What do we look for, and where do we find it? Did they follow a specific process to locate it?	https://www.louisianabelieves.com/measuringresults/digital-schools
What does an incident look like roughly? What are the symptoms of the phase 1 spread throughout the network?	What we are finding on the initial incident it's usually triggered by a trickbot. It crawls east and west across different machines looking for higher provincials until it can get to your domain controller. Also look for outbound web traffic to ports 445/447/449/8082/16993 (especially to international IP addresses). also traffic to or from Pastebin.com (104.20.209.21). https://www.louisianabelieves.com/measuringresults/digital-schools
What if Azure AD is being used? Completely blocking AD controllers would break sync.	Depending on your configuration positions of your accounts may be at a lower risk.
What if you have separate internet access that is dedicated to VOIP only?	If it is in the posture to where it is appropriately isolated in your environment.... Layer 2 total isolation.... and there is no opportunity for your voice system to connect to your computer and vice versa. This is critical. This is the typical setup. That internet connection should only support VOIP. Does that VOIP internet connection rest behind a firewall? It should. If it does You need to configure that firewall with an ACL that only allows the subnets of your phones out through that internet connection and back in through whatever natted address that range that facilitates your VOIP systems.
What if your payroll system is internal only?	This is not usually the case unless you are printing checks at your location. You must not need connectivity to the internet.
What is the anticipated end state for schools that need general internet access for instructional purposes? Will there be an end configuration that allows this?	This will be covered in a lower phase
What is the number to Unity Fiber Cyber Hotline?	Unity Fiber Cyber Hotline 877-329-2296
What types of antivirus, firewall, advanced threat protections were the infected districts using that were not able to identify the outgoing traffic to the command and control server?	We do not have a full list. We are asking all districts/schools to follow the Emergency Cyber Incident Prevention Critical Task List
What was the main Operating System that was affected?	Window Operating Systems workstation and server
what's your recommendation for using web-based email? should it be allowed (TCP80/443) in phase 2?	If you are only using Google then allow port 443 to Gmail IPs
When the secondary payload deploys. Is there an exe that can be watched for in an active fashion in an attempt to head it off?	No.
Where can we get the all Louisiana.gov addresses?	Most Louisiana.gov addresses should have been included in the IP ranges listed in the Critical Task List.
Where do we find the OEP Questionnaire mentioned in a previous webinar?	Contact your local OEP Director for a copy of the questionnaire
Will agencies that utilize State Payroll(Leo) have to allow a different set of IP addresses than those provided?	State Agencies should contact the DOA IT department. THIS TASK LIST IS FOR SCHOOLS ONLY NOT STATE AGENCIES.
Will the documents that have already released be updated to include required steps, such as rebooting every device on network?	Yes, we are continuously updating the documents.
Will the state ip ranges work with central office?	They will be added to the task list
will you post the additional IP addresses that you guys have found?	Any information we can share will be published to the DOE website.
Would a "whitelist" virus protection system like PC Matic work?	It would add value but effort should focus on completing the Critical Task List
Would external systems, such as TRSL, IRS, LA. Division of Administration, bank sites, etc. be part of phase 3?	If it is hosted by the state it should be allowed in phase 2. If it is not hosted by the state but it is critical then it needs to be added in Phase 3.
You said ALL workstations need to be rebooted. Student laptops are off campus at this time with students. We have to wait till students come back to reboot their laptops while connected to the network before proceeding to phase 3?	When the Student laptops come back on campus you will need to make sure to power cycle the devices completely. Do not pause or wait to proceed to phase 3.