Letterman, Chris E (DOA)

From:	Letterman, Chris E (DOA)
Sent:	Tuesday, November 8, 2016 1:46 PM
To:	Steele, Jim A (DOA)
Cc:	Druyvestein, Jay A (DOA)
Subject:	per text message

Per my text message. Below is the message draft. Pasted further below that is a message between Leonard (GOVs office) and FBI Special Agent Jason Chaney that Jay was CC'd on (I was not).

DP

Commissioner,
This morning at 5:37am we were notified via an alert that an unknown individual (@CyberZeist twitter handle) had posted a screen shot from what appeared to be a compromised Alaska Division of Elections reporting system.

Here is what we know:

1. The individual successfully executed an exploit to PHP (a computer scripting language used heavily in web presentation)
2. The individual was able to use privilege escalation to access the server's underlying file system.
3. The individual posted to their Twitter account a screen shot from the GEMS Election Results System as proof they were capable of accessing administrative areas of the server.
4. Along with the screen shot, the following message was posted "#USElections2016 Alaska Election Division online #ballot administrator access #pwned.. waiting for people to start voting"

At this time I have SSO staff working with Gov's office staff to get the server's vulnerable PHP installation patched. Additionally, we are building more aggressive hunting rules for our McAfee security solutions. Finally, this server will eventually be taken down once results begin to come in and are reported. The SOP for elections results posting are to turn up new VMs with the static results. Our analysis of this event is that there was no compromise of classified information as election results are public data. With the PHP vulnerability patched and the SOP for elections reporting, I am confident we have this matter resolved.

It is worth mentioning @CyberZeist did make a general threat to launch distributed denial of service attack(s) today. The threat is not specific to the State of Alaska, but if such an attack is launched against elections.alaska.gov we may be impacted which would result in delays and timeouts when people attempt to access the election results online at elections.alaska.gov.

If you have any further questions please let me know.

-

PASTED MESSAGE FOLLOWS:

From: Robertson, Leonard N (GOV)

Sent: Tuesday, November 08, 2016 11:56 AM
To: jason.cheney[redacted]
Cc: Druyvestein, Jay A (DOA) <[redacted]ov >; Davis, Myron L (DOA) <[redacted]>; Clark, Kami S (GOV) [redacted]; Malander, Phillip J (GOV) <[redacted]ov >
Subject: Alaska Election System Claim by cyberzeist

Dear Mr. Cheney,

Phillp Malander from our Elections division suggested I follow-up with you on the summary from our different parties.

The Elections webserver is a server that hosts flat content, and does not use the database backend. The most dynamic content on this server is a php page that pulls from an xml file. For servers hosted by the Governor's Office, we avoid hosting any DMZ content that is sensitive. As a policy we avoid and discourage any web services in this DMZ area that collects and stores confidential information.

Claimed Compromise:
So far the cyberzeist twitter post has proven they can read a public web page. This party has not proven they can alter any results, even though the boast in the tweet may subtly imply that ability. In actuality, results are tabulated in an isolated network without any internet access. They claim to have discovered a vulnerability, but this has not been proven true. So unless this party can hack and compromise our "Sneaker Net", There is no path from Elections.alaska.gov to reach the tabulation system. Tabulation results are hand carried one way from the tabulation system to the elections webserver.

Results of Review:
Our security office reviewed the server and found a recent patch missing that was of minimal risk and did not pose a significant threat. In addition, they reviewed the server hardening we had enabled, and feel it is still a strong box. Preliminary log review does not show a compromise of system integrity. The worst vulnerability found was the ability to read information that may not be intended but not critical or confidential. This patch has been applied along with some updates, that are not required for security, but are prudent.

Elections staff reviewed procedures and logic of information flow to reiterate there is no path to compromise tabulation. In addition, fall back procedure in case of an actual breach of the elections webserver are in place. Basically, we would point traffic to our alternate hosting sites for elections results.

Moving forward:
All parties involved will continue to monitor and be available. Phillip mentioned you may wish to review logs. I can work with you to make sure that is available. We appreciate your help and remain available to answer any questions and take any suggestions.

Today feel free to contact me on my cell at [redacted] BOI in case I am away from my desk phone.

Leonard Robertson
Network Systems Specialist
Division of Administrative Services
Office of Governor Bill Walker

240 Main Street, Suite 300
Court Plaza Building
Juneau, Alaska 99801
[redacted]

Cc: Jay Druyvestein (State Security Office Representative), Myron Davis(State Security Analyst), Kami Clark (Governor's Office I.T. Director), Phillip Malander (Elections Systems Expert)

Steele, Jim A (DOA)

From:	Steele, Jim A (DOA)
Sent:	Tuesday, November 8, 2016 1:51 PM
To:	Letterman, Chris E (DOA)
Cc:	Druyvestein, Jay A (DOA)
Subject:	Re: per text message

I would do two things here -

1. Spell out SOP and VM's in their first appearance; use acronyms thereafter.
2. Send it.

Jim Steele
State Information Technology Officer
Enterprise Technology Services Director
Alaska Department of Administration
Anchorage [redacted] Mobile BOI

On Nov 8, 2016, at 1:46 PM, Letterman, Chris E (DOA) <chris.letterman@alaska.gov> wrote:

> Per my text message. Below is the message draft. Pasted further below that is a message between Leonard (GOVs office) and FBI Special Agent Jason Chaney that Jay was CC'd on (I was not). DP
>
> Commissioner,
> This morning at 5:37am we were notified via an alert that an unknown individual (@CyberZeist twitter handle) had posted a screen shot from what appeared to be a compromised Alaska Division of Elections reporting system.
>
> Here is what we know:
> 1. The individual successfully executed an exploit to PHP (a computer scripting language used heavily in web presentation)
> 2. The individual was able to use privilege escalation to access the server's underlying file system.
> 3. The individual posted to their Twitter account a screen shot from the GEMS Election Results System as proof they were capable of accessing administrative areas of the server.
> 4. Along with the screen shot, the following message was posted "#USElections2016 Alaska Election Division online #ballot administrator access #pwned.. waiting for people to start voting"
>
> At this time I have SSO staff working with Gov's office staff to get the server's vulnerable

PHP installation patched. Additionally, we are building more aggressive hunting rules for our McAfee security solutions. Finally, this server will eventually be taken down once results begin to come in and are reported. The SOP for elections results posting are to turn up new VMs with the static results. Our analysis of this event is that there was no compromise of classified information as election results are public data. With the PHP vulnerability patched and the SOP for elections reporting, I am confident we have this matter resolved.

It is worth mentioning @CyberZeist did make a general threat to launch distributed denial of service attack(s) today. The threat is not specific to the State of Alaska, but if such an attack is launched against elections.alaska.gov we may be impacted which would result in delays and timeouts when people attempt to access the election results online at elections.alaska.gov.

If you have any further questions please let me know.

PASTED MESSAGE FOLLOWS:

From: Robertson, Leonard N (GOV)
Sent: Tuesday, November 08, 2016 11:56 AM
To: jason.cheney[redacted]
Cc: Druyvestein, Jay A (DOA) <[redacted]gov >; Davis, Myron L (DOA) <[redacted]>; Clark, Kami S (GOV) <[redacted]Malander, Phillip J (GOV) <[redacted]gov >
Subject: Alaska Election System Claim by cyberzeist

Dear Mr. Cheney,

Phillp Malander from our Elections division suggested I follow-up with you on the summary from our different parties.

The Elections webserver is a server that hosts flat content, and does not use the database backend. The most dynamic content on this server is a php page that pulls from an xml file. For servers hosted by the Governor's Office, we avoid hosting any DMZ content that is sensitive. As a policy we avoid and discourage any web services in this DMZ area that collects and stores confidential information.

Claimed Compromise:
So far the cyberzeist twitter post has proven they can read a public web page. This party has not proven they can alter any results, even though the boast in the tweet may subtly imply that ability. In actuality, results are tabulated in an isolated network without any internet access. They claim to have discovered a vulnerability, but this has not been proven true. So unless this party can hack and compromise our "Sneaker Net", There is no path from Elections.alaska.gov to reach the tabulation system. Tabulation results are hand carried one way from the tabulation system to the elections webserver.

Results of Review:
Our security office reviewed the server and found a recent patch missing that was of minimal risk and did not pose a significant threat. In addition, they reviewed the server hardening we had enabled, and feel it is still a strong box. Preliminary log review does not show a

compromise of system integrity. The worst vulnerability found was the ability to read information that may not be intended but not critical or confidential. This patch has been applied along with some updates, that are not required for security, but are prudent.

Elections staff reviewed procedures and logic of information flow to reiterate there is no path to compromise tabulation. In addition, fall back procedure in case of an actual breach of the elections webserver are in place. Basically, we would point traffic to our alternate hosting sites for elections results.

Moving forward:
All parties involved will continue to monitor and be available. Phillip mentioned you may wish to review logs. I can work with you to make sure that is available. We appreciate your help and remain available to answer any questions and take any suggestions.

Today feel free to contact me on my cell at BOI in case I am away from my desk phone.

Leonard Robertson
Network Systems Specialist
Division of Administrative Services
Office of Governor Bill Walker

240 Main Street, Suite 300
Court Plaza Building
Juneau, Alaska 99801
[redacted]

Cc: Jay Druyvestein (State Security Office Representative), Myron Davis(State Security Analyst), Kami Clark (Governor's Office I.T. Director), Phillip Malander (Elections Systems Expert)

Letterman, Chris E (DOA)

From:	Letterman, Chris E (DOA)
Sent:	Tuesday, November 8, 2016 1:51 PM
To:	Steele, Jim A (DOA)
Cc:	Druyvestein, Jay A (DOA)
Subject:	RE: per text message

Roger. I was NOT going to share the pasted email – that was for you. Unless you believe I should include it?

-Chris
[redacted]
BOI mobile.

From: Steele, Jim A (DOA)
Sent: Tuesday, November 8, 2016 1:51 PM
To: Letterman, Chris E (DOA) <c[redacted]v>
Cc: Druyvestein, Jay A (DOA) <ja[redacted]v>
Subject: Re: per text message

I would do two things here -

1. Spell out SOP and VM's in their first appearance; use acronyms thereafter.
2. Send it.

Jim Steele
State Information Technology Officer
Enterprise Technology Services Director
Alaska Department of Administration
Anchorag[redacted]M[redacted]

On Nov 8, 2016, at 1:46 PM, Letterman, Chris E (DOA) <c[redacted]v> wrote:

> Per my text message. Below is the message draft. Pasted further below that is a message between Leonard (GOVs office) and FBI Special Agent Jason Chaney that Jay was CC'd on (I was not).
> [redacted]
> DP
> [redacted]
>
> Commissioner,
> This morning at 5:37am we were notified via an alert that an unknown individual (@CyberZeist twitter handle) had posted a screen shot from what appeared to be a compromised Alaska Division of Elections reporting system.
>
> Here is what we know:

1. The individual successfully executed an exploit to PHP (a computer scripting language used heavily in web presentation)
2. The individual was able to use privilege escalation to access the server's underlying file system.
3. The individual posted to their Twitter account a screen shot from the GEMS Election Results System as proof they were capable of accessing administrative areas of the server.
4. Along with the screen shot, the following message was posted "#USElections2016 Alaska Election Division online #ballot administrator access #pwned.. waiting for people to start voting"

At this time I have SSO staff working with Gov's office staff to get the server's vulnerable PHP installation patched. Additionally, we are building more aggressive hunting rules for our McAfee security solutions. Finally, this server will eventually be taken down once results begin to come in and are reported. The SOP for elections results posting are to turn up new VMs with the static results. Our analysis of this event is that there was no compromise of classified information as election results are public data. With the PHP vulnerability patched and the SOP for elections reporting, I am confident we have this matter resolved.

It is worth mentioning @CyberZeist did make a general threat to launch distributed denial of service attack(s) today. The threat is not specific to the State of Alaska, but if such an attack is launched against elections.alaska.gov we may be impacted which would result in delays and timeouts when people attempt to access the election results online at elections.alaska.gov.

If you have any further questions please let me know.

PASTED MESSAGE FOLLOWS:

From: Robertson, Leonard N (GOV)
Sent: Tuesday, November 08, 2016 11:56 AM
To: [redacted]
Cc: Druyvestein, Jay A (DOA) <[redacted]>; Davis, Myron L (DOA) <[redacted]>; Clark, Kami S (GOV) <[redacted]>; Malander, Phillip J (GOV) <[redacted]>
Subject: Alaska Election System Claim by cyberzeist

Dear Mr. Cheney,

Phillp Malander from our Elections division suggested I follow-up with you on the summary from our different parties.

The Elections webserver is a server that hosts flat content, and does not use the database backend. The most dynamic content on this server is a php page that pulls from an xml file. For servers hosted by the Governor's Office, we avoid hosting any DMZ content that is sensitive. As a policy we avoid and discourage any web services in this DMZ area that collects and stores confidential information.

Claimed Compromise:
So far the cyberzeist twitter post has proven they can read a public web page. This party has not proven they can alter any results, even though the boast in the tweet may subtly imply that ability. In actuality, results are tabulated in an isolated network without any internet access. They claim to have discovered a vulnerability, but this has not been proven true. So unless this party can hack and compromise our "Sneaker Net", There is no path from Elections.alaska.gov to reach the tabulation system. Tabulation results are hand carried one way from the tabulation system to the elections webserver.

Results of Review:
Our security office reviewed the server and found a recent patch missing that was of minimal risk and did not pose a significant threat. In addition, they reviewed the server hardening we had enabled, and feel it is still a strong box. Preliminary log review does not show a compromise of system integrity. The worst vulnerability found was the ability to read information that may not be intended but not critical or confidential. This patch has been applied along with some updates, that are not required for security, but are prudent.

Elections staff reviewed procedures and logic of information flow to reiterate there is no path to compromise tabulation. In addition, fall back procedure in case of an actual breach of the elections webserver are in place. Basically, we would point traffic to our alternate hosting sites for elections results.

Moving forward:
All parties involved will continue to monitor and be available. Phillip mentioned you may wish to review logs. I can work with you to make sure that is available. We appreciate your help and remain available to answer any questions and take any suggestions.

Today feel free to contact me on my cell at BOI in case I am away from my desk phone.

Leonard Robertson
Network Systems Specialist
Division of Administrative Services
Office of Governor Bill Walker

240 Main Street, Suite 300
Court Plaza Building
Juneau, Alaska 99801
[redacted]

Cc: Jay Druyvestein (State Security Office Representative), Myron Davis(State Security Analyst), Kami Clark (Governor's Office I.T. Director), Phillip Malander (Elections Systems Expert)

Letterman, Chris E (DOA)

From:	Letterman, Chris E (DOA)
Sent:	Tuesday, November 8, 2016 1:57 PM
To:	Fisher, Sheldon A (DOA)
Cc:	Steele, Jim A (DOA)
Subject:	Elections Results Issue

Commissioner,
This morning at 5:37am we were notified via an alert that an unknown individual (@CyberZeist twitter handle) had posted a screen shot from what appeared to be a compromised Alaska Division of Elections reporting system.

Here is what we know:

1. The individual successfully executed an exploit to PHP (a computer scripting language used heavily in web presentation)
2. The individual was able to use privilege escalation to access the server's underlying file system.
3. The individual posted to their Twitter account a screen shot from the GEMS Election Results System as proof they were capable of accessing administrative areas of the server.
4. Along with the screen shot, the following message was posted "#USElections2016 Alaska Election Division online #ballot administrator access #pwned.. waiting for people to start voting"

At this time I have SSO staff working with Gov's office staff to get the server's vulnerable PHP installation patched. Additionally, we are building more aggressive hunting rules for our McAfee security solutions. Finally, this server will eventually be taken down once results begin to come in and are reported. The standard operating procedure for posting elections results are to turn up new virtual machines with the static results. Our analysis of this event is that there was no compromise of classified information as election results are public data. With the PHP vulnerability patched and the SOP for elections reporting, I am confident we have this matter resolved.

It is worth mentioning @CyberZeist did make a general threat to launch distributed denial of service attack(s) today. The threat is not specific to the State of Alaska, but if such an attack is launched against elections.alaska.gov we may be impacted which would result in delays and timeouts when people attempt to access the election results online at elections.alaska.gov.

If you have any further questions please let me know.

-*Chris*

Chris Letterman
Chief Information Security Officer
State of Alaska : Enterprise Technology Services
PO Box 110206
333 Willoughby Avenue
5th Fl. State Office Building
Juneau, AK 99811-0206

Letterman, Chris E (DOA)

From:	Letterman, Chris E (DOA)
Sent:	Tuesday, November 8, 2016 1:57 PM
To:	Fisher, Sheldon A (DOA)
Cc:	Steele, Jim A (DOA)
Subject:	Elections Results Issue

Commissioner,
This morning at 5:37am we were notified via an alert that an unknown individual (@CyberZeist twitter handle) had posted a screen shot from what appeared to be a compromised Alaska Division of Elections reporting system.

Here is what we know:

1. The individual successfully executed an exploit to PHP (a computer scripting language used heavily in web presentation)
2. The individual was able to use privilege escalation to access the server's underlying file system.
3. The individual posted to their Twitter account a screen shot from the GEMS Election Results System as proof they were capable of accessing administrative areas of the server.
4. Along with the screen shot, the following message was posted "#USElections2016 Alaska Election Division online #ballot administrator access #pwned.. waiting for people to start voting"

At this time I have SSO staff working with Gov's office staff to get the server's vulnerable PHP installation patched. Additionally, we are building more aggressive hunting rules for our McAfee security solutions. Finally, this server will eventually be taken down once results begin to come in and are reported. The standard operating procedure for posting elections results are to turn up new virtual machines with the static results. Our analysis of this event is that there was no compromise of classified information as election results are public data. With the PHP vulnerability patched and the SOP for elections reporting, I am confident we have this matter resolved.

It is worth mentioning @CyberZeist did make a general threat to launch distributed denial of service attack(s) today. The threat is not specific to the State of Alaska, but if such an attack is launched against elections.alaska.gov we may be impacted which would result in delays and timeouts when people attempt to access the election results online at elections.alaska.gov.

If you have any further questions please let me know.

-*Chris*

Chris Letterman
Chief Information Security Officer
State of Alaska : Enterprise Technology Services
PO Box 110206
333 Willoughby Avenue
5th Fl. State Office Building
Juneau, AK 99811-0206

Letterman, Chris E (DOA)

From:	Letterman, Chris E (DOA)
Sent:	Tuesday, November 8, 2016 1:57 PM
To:	Steele, Jim A (DOA)
Cc:	Druyvestein, Jay A (DOA)
Subject:	RE: per text message

Done

-Chris
[redacted]
BOI mobile.

From: Steele, Jim A (DOA)
Sent: Tuesday, November 8, 2016 1:51 PM
To: Letterman, Chris E (DOA) <chris.letterman@alaska.gov>
Cc: Druyvestein, Jay A (DOA) <jay.druyvestein@alaska.gov>
Subject: Re: per text message

I would do two things here -

1. Spell out SOP and VM's in their first appearance; use acronyms thereafter.
2. Send it.

Jim Steele
State Information Technology Officer
Enterprise Technology Services Director
Alaska Department of Administration
Anchora[redacted]

On Nov 8, 2016, at 1:46 PM, Letterman, Chris E (DOA) [redacted]gov> wrote:

> Per my text message. Below is the message draft. Pasted further below that is a message between Leonard (GOVs office) and FBI Special Agent Jason Chaney that Jay was CC'd on (I was not).
> DP
>
> Commissioner,
> This morning at 5:37am we were notified via an alert that an unknown individual (@CyberZeist twitter handle) had posted a screen shot from what appeared to be a compromised Alaska Division of Elections reporting system.
>
> Here is what we know:

1. The individual successfully executed an exploit to PHP (a computer scripting language used heavily in web presentation)
2. The individual was able to use privilege escalation to access the server's underlying file system.
3. The individual posted to their Twitter account a screen shot from the GEMS Election Results System as proof they were capable of accessing administrative areas of the server.
4. Along with the screen shot, the following message was posted "#USElections2016 Alaska Election Division online #ballot administrator access #pwned.. waiting for people to start voting"

At this time I have SSO staff working with Gov's office staff to get the server's vulnerable PHP installation patched. Additionally, we are building more aggressive hunting rules for our McAfee security solutions. Finally, this server will eventually be taken down once results begin to come in and are reported. The SOP for elections results posting are to turn up new VMs with the static results. Our analysis of this event is that there was no compromise of classified information as election results are public data. With the PHP vulnerability patched and the SOP for elections reporting, I am confident we have this matter resolved.

It is worth mentioning @CyberZeist did make a general threat to launch distributed denial of service attack(s) today. The threat is not specific to the State of Alaska, but if such an attack is launched against elections.alaska.gov we may be impacted which would result in delays and timeouts when people attempt to access the election results online at elections.alaska.gov.

If you have any further questions please let me know.

PASTED MESSAGE FOLLOWS:

From: Robertson, Leonard N (GOV)
Sent: Tuesday, November 08, 2016 11:56 AM
To: [redacted]
Cc: Druyvestein, Jay A (DOA) <ja[redacted]v >; Davis, Myron L (DOA) <r[redacted]; Clark, Kami S (GOV[redacted]>; Malander, Phillip J (GOV) <j[redacted]gov >
Subject: Alaska Election System Claim by cyberzeist

Dear Mr. Cheney,

Phillp Malander from our Elections division suggested I follow-up with you on the summary from our different parties.

The Elections webserver is a server that hosts flat content, and does not use the database backend. The most dynamic content on this server is a php page that pulls from an xml file. For servers hosted by the Governor's Office, we avoid hosting any DMZ content that is sensitive. As a policy we avoid and discourage any web services in this DMZ area that collects and stores confidential information.

Claimed Compromise:
So far the cyberzeist twitter post has proven they can read a public web page. This party has not proven they can alter any results, even though the boast in the tweet may subtly imply that ability. In actuality, results are tabulated in an isolated network without any internet access. They claim to have discovered a vulnerability, but this has not been proven true. So unless this party can hack and compromise our "Sneaker Net", There is no path from Elections.alaska.gov to reach the tabulation system. Tabulation results are hand carried one way from the tabulation system to the elections webserver.

Results of Review:
Our security office reviewed the server and found a recent patch missing that was of minimal risk and did not pose a significant threat. In addition, they reviewed the server hardening we had enabled, and feel it is still a strong box. Preliminary log review does not show a compromise of system integrity. The worst vulnerability found was the ability to read information that may not be intended but not critical or confidential. This patch has been applied along with some updates, that are not required for security, but are prudent.

Elections staff reviewed procedures and logic of information flow to reiterate there is no path to compromise tabulation. In addition, fall back procedure in case of an actual breach of the elections webserver are in place. Basically, we would point traffic to our alternate hosting sites for elections results.

Moving forward:
All parties involved will continue to monitor and be available. Phillip mentioned you may wish to review logs. I can work with you to make sure that is available. We appreciate your help and remain available to answer any questions and take any suggestions.

Today feel free to contact me on my cell at BOI in case I am away from my desk phone.

Leonard Robertson
Network Systems Specialist
Division of Administrative Services
Office of Governor Bill Walker

240 Main Street, Suite 300
Court Plaza Building
Juneau, Alaska 99801
[redacted]

Cc: Jay Druyvestein (State Security Office Representative), Myron Davis(State Security Analyst), Kami Clark (Governor's Office I.T. Director), Phillip Malander (Elections Systems Expert)

Steele, Jim A (DOA)

From:	Steele, Jim A (DOA)
Sent:	Thursday, November 10, 2016 3:15 PM
To:	Fisher, Sheldon A (DOR); Ridle, Leslie D (DOA)
Subject:	Fwd: notification of convo with fbi regarding elections server compromise

As requested, here is the summary of the call Myron Davis, an ETS Security Analyst, had with the FBI earlier this afternoon. If you need further details, the call was recorded and we can provide you or anyone else with a copy.

This same individual received a call from the Juneau Empire this afternoon. The call was not answered nor was a voicemail left. We don't know the name of the reporter nor, for that matter, whether this call was even related to this cyber incident. That is an assumption on our part.

Finally, I will be issuing a memo of procedure to my staff outlining our standard operating procedures for handling any future calls from either law enforcement or the press.

Thanks,
Jim

Jim Steele
State Information Technology Officer
Enterprise Technology Services Director
Alaska Department of Administration
Anchorag[redacted] BOI

Begin forwarded message:

> **From:** "Davis, Myron L (DOA)" <[redacted]ov>
> **Date:** November 10, 2016 at 2:30:11 PM AKST
> **To:** "Steele, Jim A (DOA)" <[redacted]
> **Cc:** "Druyvestein, Jay A (DOA)" <j[redacted]gov>, "Letterman, Chris E (DOA)" <c[redacted]ov>
> **Subject: notification of convo with fbi regarding elections server compromise**
>
> As requested a summarization of the conversation regarding the elections server compromise;
>
> Talked to Special Agent Jason Cheney; he had to go to a Federal Judge and give a report of the elections compromise. I recorded the phone call; the information I imparted over the phone was basically as follows:
>
> Information on network firewall holes. Elections server is silo'd into a blackhole part of the dmz. Only incoming connections on port 80 from the internet and some port 22 from parts of the inside network. Outgoing connections from that silo are allowed to [redacted] on port 80 (update server

I manage), and the syslog server, and I mentioned time server access, but in retrospec I'm not sure if time is allowed either, no dns is allowed. All host entries are hard coded on the box in the /etc/hosts file.

I detailed what the external IPs were, and the reasons why I choose the Indian power company IP address as related to the attacker (cyberzeist). I transferred all of the logs of the identified external IP address to him as well as the "related" connections. I identified the related connections due to a information disclosure on the twitter page with the keyword "pick_target".

With that keyword all IPs that decided to investigate the twitter post were tagged and I pulled all of the logs of everyone that investigated and transferred that to Special Agent Jason Cheney.

I detailed that I didn't know how the actual method elections was updated, Leonard might be a good person to talk too at elections, but that is was essentially a sneaker network and the elections data did not travel over the regular state network.

I discussed the exploit which was covered in this release: https://www.ubuntu.com/usn/usn-3095-1/https://www.ubuntu.com/usn/usn-3095-1/

The vulnerability was when PHP incorrectly handles certain invalid objects and caused a informational disclosure. Theoretically one could have executed content. I didn't see anything like that; and executing content by forcing downloads from remote sites would be extremely difficult as this host did not have internet access.

The only behavior I noticed was the post to twitter which included a page that was already public. Albeit the way the data was retrieved was unconventional.

The attacker did not modify anything on the box.

The reason the box was not updated was due to a script I ran on the update server at the end of September. I was attempting to better optimize disk space usage through a de-duper script that used hard links.

This broke the rsync process for this part of the mirror as the rsync process did not expect the changes I made to the repository.

The fix was released October 4th and was not applied as it should have. (all security updates normally are automatically applied to this box)

The mirror was fixed November 8th a few hours after the twitter feed was announced. Additionally they were using a /admin portion which I chmod 000'd in order to prevent anyone from getting to that location again.

Letterman, Chris E (DOA)

From:	Letterman, Chris E (DOA)
Sent:	Monday, November 14, 2016 5:05 PM
To:	Steele, Jim A (DOA)
Subject:	FYI
Attachments:	pickedup.pdf

Well it hasn't hit ADN yet, but we should let "them" know the tweet was picked up by cyberwarn.info ...can we talk about the FBI comment around Myron tomorrow?

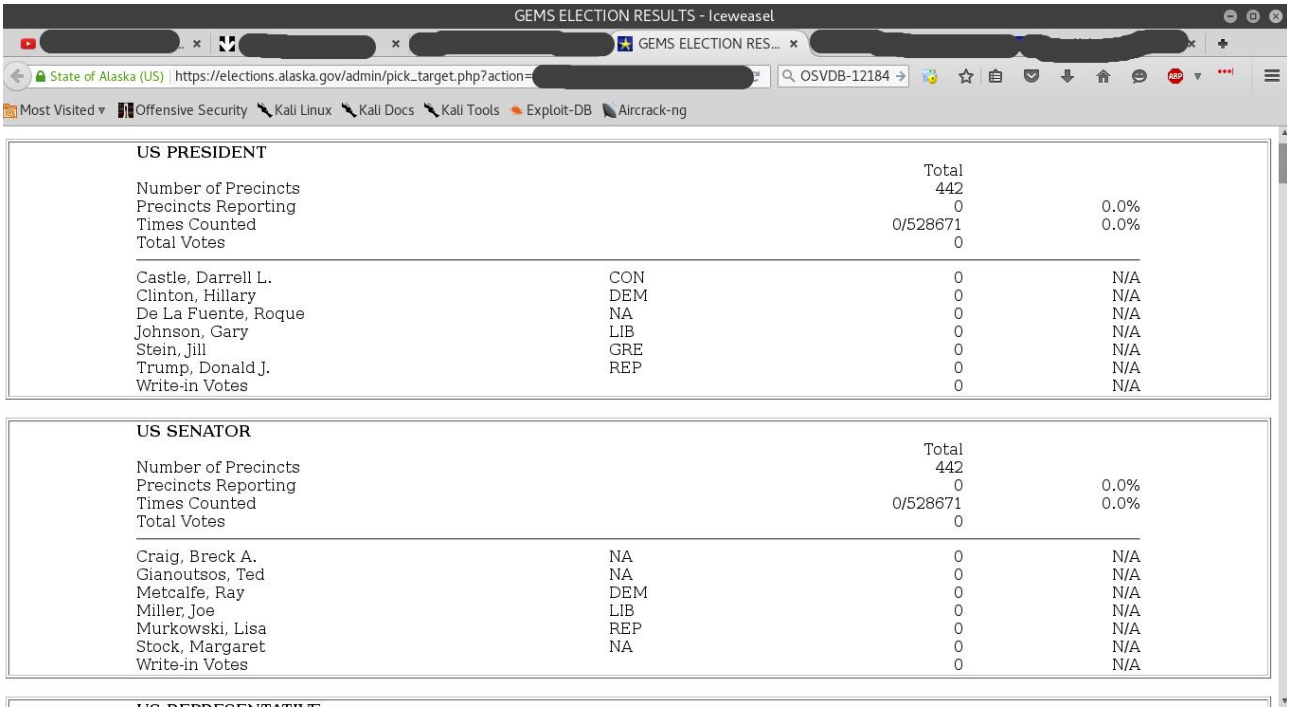
MENU

Alaskan Elections Results Site Hacked By CyberZeist

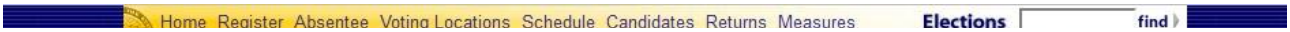
09 NOVEMBER 2016

Today is a big day in america with the elections taking place, its been fairly expected that at some staging a hacking incident will happen but it was more then question of who and what.

Not to long ago now a hacker who uses the handle CyberZeist tweeted an screen cap along with an message claiming that the an Alaskan Elections Results website (http://www.elections.alaska.gov/) has been breached.



After speaking to CyberZeist, they provided me with further proof that they had access to administration section of the Alaskan Elections Results and disclosed the servers ip and admin/password combination.



They also disclosed that the server is running out-dated Ubuntu OS and Apache HTTPD and still subject to many older vulnerabilities still. It does appear that one part of the security that this system does actually have is GEO-location blocking which is stopping all access to the administration features unless from an Alaskan IP address.

The system that is running on this is GEMS which stands for Global Election Management System.

GEMS Integrates

- Election data entry
- Interfaces to voter registration
- Ballot layout
- Accumulation and reporting of results
- Audio recording for visually impaired voting

Now while this website in no way controls the current election it does appear that a persons with administration access could remove and create candidates, thou as stated this would have no effect on the election at all.

Lee Johnstone

Information Security Data Analyst

Sydney, Australia *http://www.ctrlbox.com*

Share this post

READ THIS NEXT

Panda Security Advised By ARN

YOU MIGHT ENJOY

Bradley Foundation

To Foot PC Repair Bill For Customer

Breached, 56245 Files Leaked

Letterman, Chris E (DOA)

From:	Letterman, Chris E (DOA)
Sent:	Tuesday, December 6, 2016 8:30 AM
To:	Fisher, Sheldon A (DOA)
Cc:	Steele, Jim A (DOA)
Subject:	RE: Elections Results Issue
Attachments:	CyberZeist CTIG-048.pdf; FW_ New LookingGlass CTIG Report_ CyberZeist-CTIG-048 (TLP_Green).pdf

Commissioner,
I have attached for your information and situational awareness an email received this morning from the Multi-State Information Sharing and Analysis Center (MS-ISAC). It is a forward of a message from Roisin S. Suver who is the Senior Liaison to Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) regarding new information about the cyber actor who targeted the state's election result website. The information is classified traffic light protocol green (TLP) which means it may be shared within our organization, however I defer to your judgement to share as you see fit with the Governor's Office/Division of Elections personnel/other parties.

-*Chris*
(907) 465-5775 desk.
BOI mobile.

From: Letterman, Chris E (DOA)
Sent: Tuesday, November 8, 2016 1:57 PM
To: Fisher, Sheldon A (DOA) <sheldon.fisher@alaska.gov>
Cc: Steele, Jim A (DOA) <jim.steele@alaska.gov>
Subject: Elections Results Issue

Commissioner,
This morning at 5:37am we were notified via an alert that an unknown individual (@CyberZeist twitter handle) had posted a screen shot from what appeared to be a compromised Alaska Division of Elections reporting system.

Here is what we know:

1. The individual successfully executed an exploit to PHP (a computer scripting language used heavily in web presentation)
2. The individual was able to use privilege escalation to access the server's underlying file system.
3. The individual posted to their Twitter account a screen shot from the GEMS Election Results System as proof they were capable of accessing administrative areas of the server.
4. Along with the screen shot, the following message was posted "#USElections2016 Alaska Election Division online #ballot administrator access #pwned.. waiting for people to start voting"

At this time I have SSO staff working with Gov's office staff to get the server's vulnerable PHP installation patched. Additionally, we are building more aggressive hunting rules for our McAfee security solutions. Finally, this server will eventually be taken down once results begin to come in and are reported. The standard operating procedure for posting elections results are to turn up new virtual

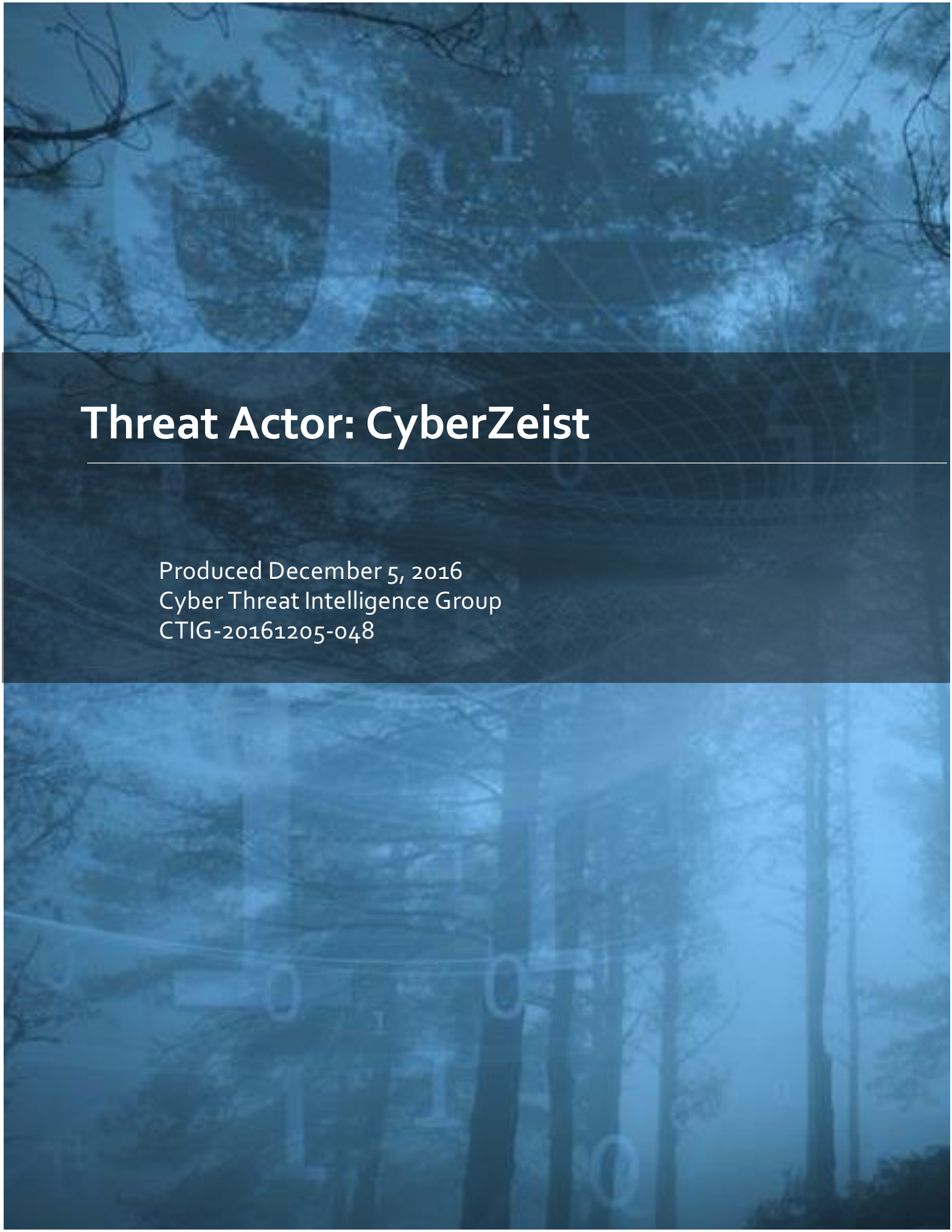
machines with the static results. Our analysis of this event is that there was no compromise of classified information as election results are public data. With the PHP vulnerability patched and the SOP for elections reporting, I am confident we have this matter resolved.

It is worth mentioning @CyberZeist did make a general threat to launch distributed denial of service attack(s) today. The threat is not specific to the State of Alaska, but if such an attack is launched against elections.alaska.gov we may be impacted which would result in delays and timeouts when people attempt to access the election results online at elections.alaska.gov.

If you have any further questions please let me know.

-*Chris*

Chris Letterman
Chief Information Security Officer
State of Alaska : Enterprise Technology Services
PO Box 110206
333 Willoughby Avenue
5th Fl. State Office Building
Juneau, AK 99811-0206



Threat Actor: CyberZeist

Produced December 5, 2016
Cyber Threat Intelligence Group
CTIG-20161205-048

Overall Report Distribution is TLP: GREEN
Overall Source/Information Reliability: B2

Executive Summary

Threat actor **CyberZeist** is currently targeting global banks exploiting the LFI vulnerability. In two instances, the actor has threatened to sell access to the banks in exchange for Bitcoins if the vulnerabilities are not patched promptly. The actor has a history of conducting hostile cyber activity having been part of the UGNazi hacker group that conducted attacks against high profile organizations, as well as participating in some Anonymous operations. The shift to targeting banks is disconcerting, and it is the belief of the Cyber Threat Intelligence Group (CTIG) that CyberZeist will likely follow through on his threats, based on previous history with breaches and leaking data.

Key Points

- **CyberZeist** is a hacker with a history of conducting hostile acts against high profile organizations. The actor has been involved in breaches and data leaks.

- The actor's shift toward banks is an indication that the actor is seeking to monetize his hacking efforts under the guise of security concern for banks' slow vulnerability patching processes. Based on previous history, CTIG believes that the actor has the intent and capability to leak data and/or sell access.

**This report is based on open source findings. Therefore, the report is open source intelligence and does not constitute definitive evidence. Information found in the open source cannot necessarily be verified and is presented as intelligence and as additional information to enhance or expand current investigations.*

Background

UGNazi Hacking Group

Threat actor **"CyberZeist"** was formerly a member of the UGNazi collective, a group of hackers that gained notoriety for disrupting and breaching several high-profile websites, including the ones of NASDAQ, the Central Intelligence Agency (CIA), Department of Justice, WHMCS (a web hosting automation platform), 4Chan, and CloudFlare.[i] Several of the Collectives members were arrested during 2012[ii], notably their leader, prompting a hiatus from their hacking activities. While with UGNazi, **CyberZeist** spearphished U.S. federal employees, obtaining their usernames and password credentials. The actor subsequently leaked more than 250 record sets comprising e-mail addresses and clear text passwords.[iii] Sometime in 2012, **CyberZeis**t broke from the group for "personal reasons" to pursue his own hacking endeavors, concentrating on attacking the U.S. Government.

Going Solo

Under the alias "**comrade**" in a June 17, 2012 Pastebin posting, **CyberZeist** claimed to have maintained access to Cobank (a national cooperative bank serving vital industries across rural America) for over a year after disclosing it on June 17, 2012. **CyberZeist** exposed the logins of Cobank employees, as well as the software used by the bank. In addition, **CyberZeist** provide logs compromised from Citibank.[iv] Also in 2012, using the Twitter alias "**@l34ky**," **CyberZeist** targeted the CIA, the Federal Bureau of Investigation (FBI), Comcast, Nepal Bank, Intel, and Baidu.

- In another Pastebin posting, **CyberZeist** under the alias **comrade** claimed responsibility for hacking into major airlines including American Airlines, United Airlines, Vietnam Airlines, and Sabre Airlines (note: the actor may have meant Sabre Airline Solutions, systems on which many comprehensive technology solutions that help the airline industry). The actor claimed internal access to flight booking, ticketing info, hotel booking, card swaps, employee information, and flight and passenger information.[v]

In June 2013, fearing that the FBI was tracking his activities, **CyberZeist** apologized to companies he had hacked and publicly exposed. He wanted everyone to know that he could have been stealing credit cards and private travel information but didn't in an attempt to downplay the seriousness and scope of the attacks.[vi]

Anonymous Operations

CyberZeist has been involved in a number of Anonymous operations over the years. In particular, the actor claimed credit for 2012's #Opstopg4s (he did this under the alias **l34ky**. The target was one of the largest security company in the United Kingdom),[vii] #OpSaveTheArctic (he did this under the alias

CyberZeist and referenced **L34ky's** Twitter handle. Targets included global gas companies exploring the Arctic),[viii, ix] and #OpLithChild (a campaign to stop pedophilia in Lithuania as well as worldwide).

The Interlude

From August 2, 2014 to October 6, 2016 there was a long period of unexplained silence from **CyberZeist.** However, on October 9, **CyberZeist** broke the inactivity by releasing login credentials of Pakistan government officials from the Twitter alias "**@cyberzeist**."[x]

Politics

CyberZeist was also deeply invested in the U.S. presidential election, and participated in the hacking the cell phone of John Podesta, the then chairman of Hilary Clinton's campaign.[xi] On October 11, he leaked e-mail addresses and passwords compromised from Hilaryclinton[dot]com (see Figure 1). On October 14, in a Pastebin posting, **CyberZeist** detailed how the Democratic National Committee was hacked.[xii] In early November 2016, the actor dumped the database of Moreland.ny.gov.

Figure 1: Screenshot of Hilaryclinton.com Dump

Also in November, **CyberZeist's** activities ventured into the world of botnets. The actor stated that the intent was to launch distributed denial-of-service (DDoS) attacks during the November 8 election (see Figure 2). On Election Day, **CyberZeist** showed that he had administrative access over the Alaska Election Division website.[xiii] On November 9, **CyberZeist** was ultimately blocked from elections[dot]Alaska[dot]gov, and on November 11, the actor proceeded to leak the passwords of Washington State government employees.

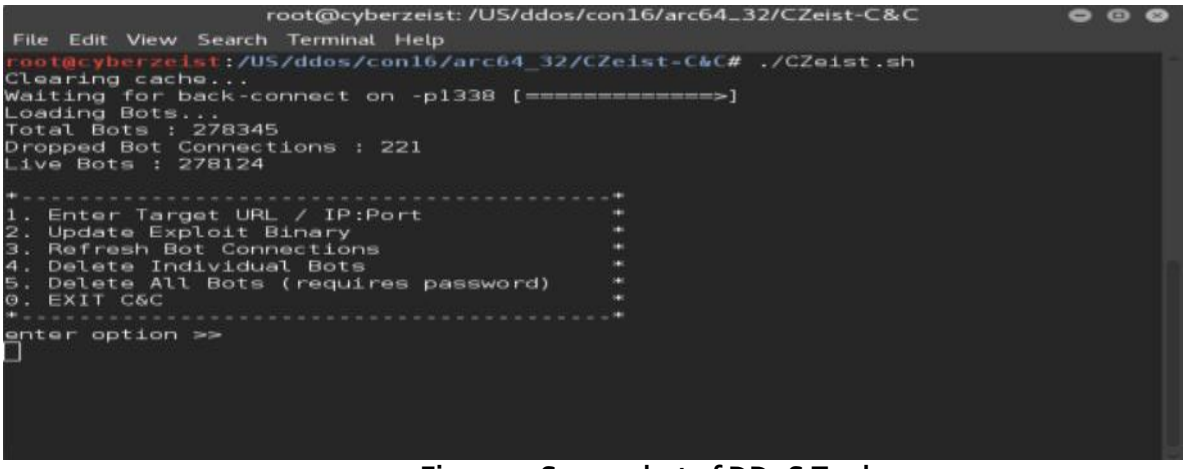


Figure 2: Screenshot of DDoS Tool

Target Shift: Banks

In mid-November 2016, **CyberZeist** realized the enormous profits to be made by hacking banks' websites. On November 15, the actor released an LFI Vulnerability (Remote File Inclusion (RFI) and Local File Inclusion (LFI) are vulnerabilities which are often found in poorly written web applications. These vulnerabilities occur when a web application allows the user to submit input into files or upload files to the server.

LFIs allow an attacker to read and sometimes execute files on the victim machine. This can be very dangerous because if the web server is misconfigured and running with high privileges, the attacker may gain access to sensitive information. If the attacker is able to place code on the web server through other means, then they may be able to execute arbitrary commands.) he found on Barclay's[dot]co[dot]uk (see Figure 3).

Figure 3: Screenshot of Barclay's bank

Afterwards, **CyberZeist** hacked the Royal Bank of Scotland. LFI vulnerabilities were used to target other banks as well including JP Morgan Chase (see Figure 4), Abu Dhabi Islamic Bank (November 21), Bank of India and Axis Bank (November 22), and HSBC Bank (November 28).

Figure 4: Screenshot of JP Morgan Chase

On December 1, the National Australia Bank was hacked using an LFI attack with CyberZeist threatening to sell access to it for Bitcoins if the vulnerability was not patched within 7 days (see Figure 5). As of this writing, the Royal Bank of Scotland is still vulnerable with CyberZeist making the same threat if it is not patched promptly.

Figure 5: Screenshot of CyberZeist Twitter

Social Media and Contact Information

Twitter Accounts

@officialcomrade

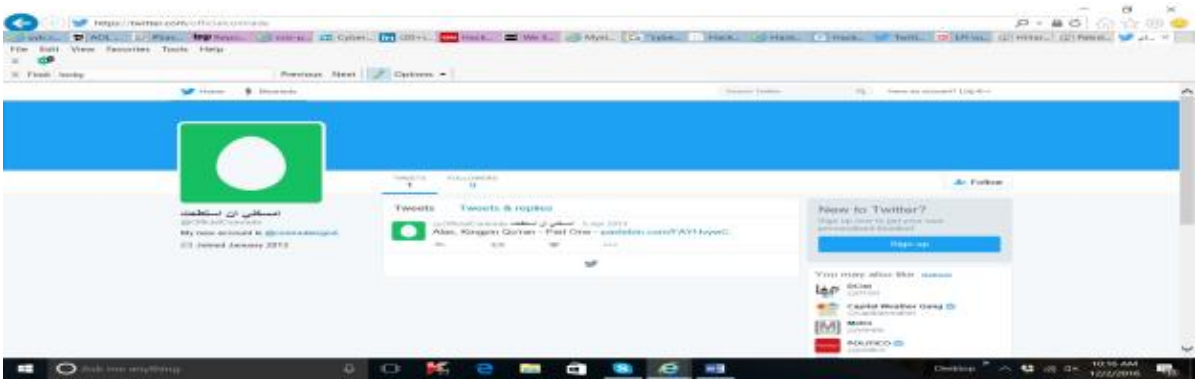


Figure 6: @officialcomrade Notifying of New Twitter Handle

@comradeisgod

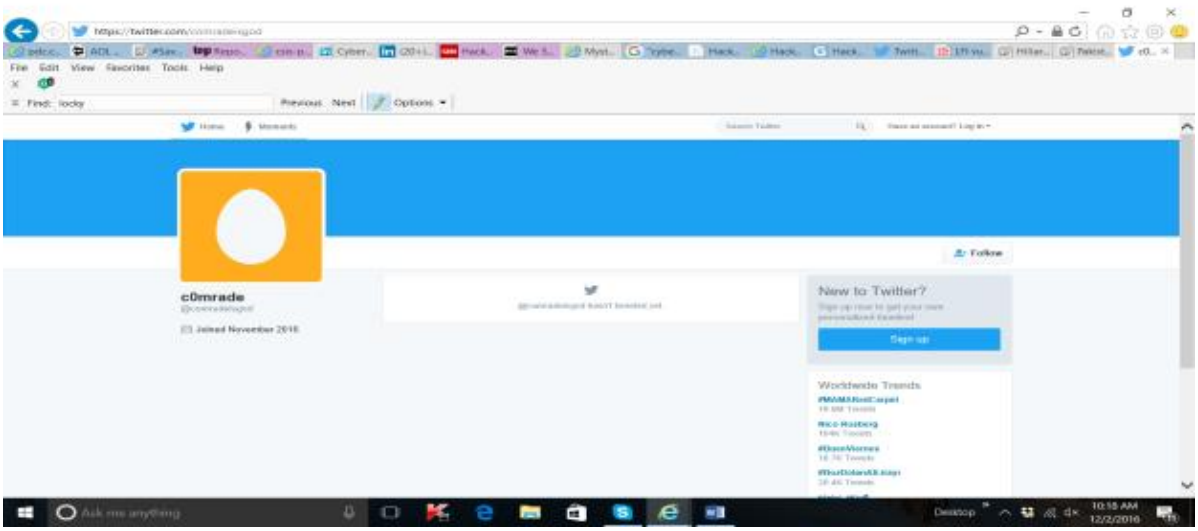


Figure 7: @comradeisgod New Twitter Page

@le4ky

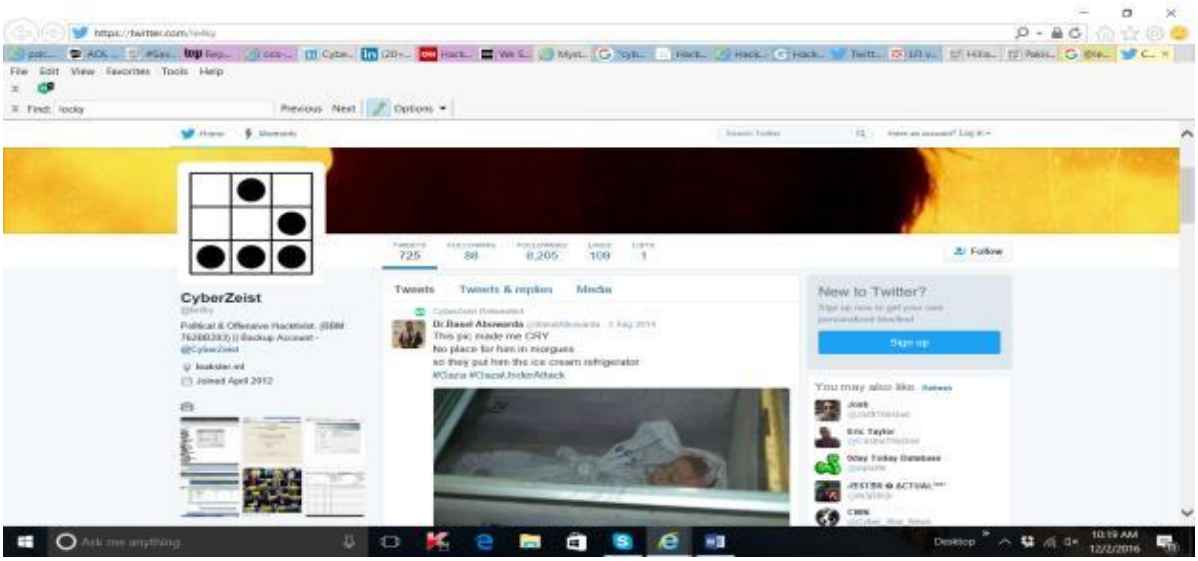


Figure 8: @le4ky Twitter Page

@CyberZeist

Account currently suspended.

@CyberZeist2

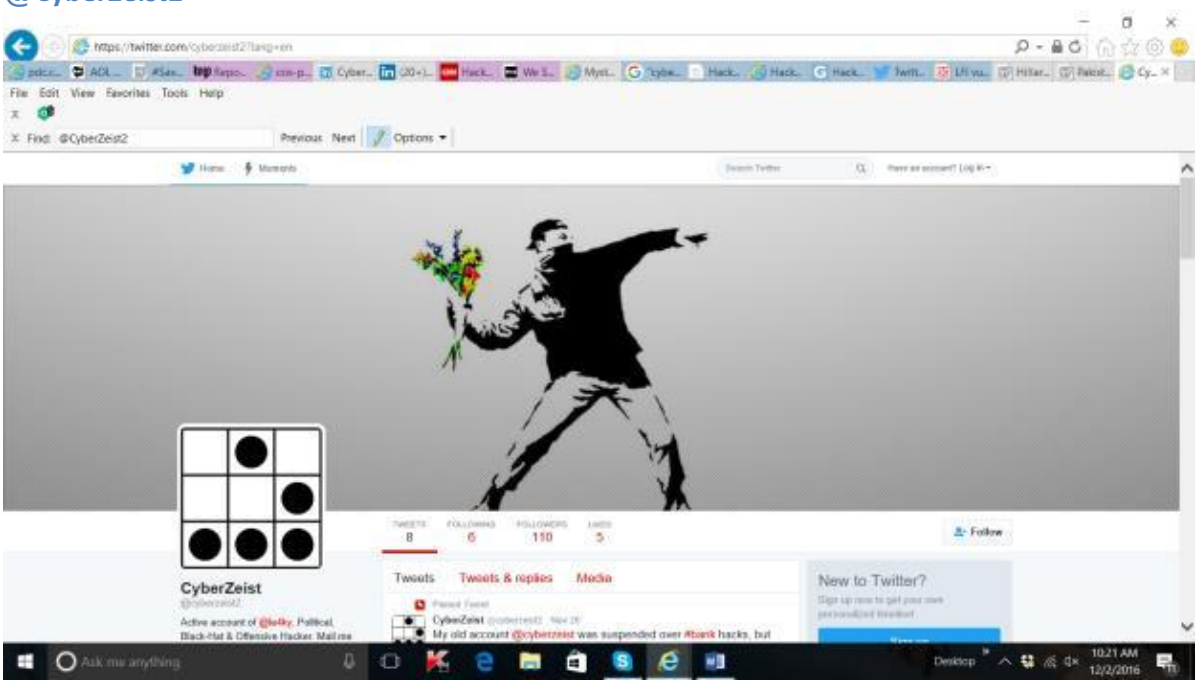


Figure 9: @CyberZeist2 Twitter Page

E-mail Addresses

CyberZeist[@]live.com
Cyberzeist[@]protonmail.com
Anonymous.cyberzeist[@]gmail.com

Known Domains Associated with CyberZeist

Leakster[dot]net

Purchased by @JoshTheGod (@VariousLulz), the leader of UGNazi.

Leakster[dot]ml

No Whois history associated with the domain. The domain is likely used by webhostooo, and the likely password is 3316opc8. The domain may be administrated using e-mail address anonymous.cyberzeist[@]gmail.com

Passwords Used by the Actor

3316opc8[xiv] - [MD5] 3e275d7d78c16368089b82278fc43d0b

Conclusions

CTIG believes that **CyberZeist** is a credible threat to banks based on recent activity and statements threatening to sell accesses to vulnerable banks who do not promptly patch their systems. **CyberZeist** has a history of malicious hacking activity with known hacking groups and hacktivist enclaves like Anonymous. **CyberZeist's** recent activities – breaching Podesta's cell phone and interest in developing DDoS capability indicate that the actor is interested in activities that garner media attention, and thus further solidifying his bona fides as an individual of note. We expect **CyberZeist** to continue to target banks as the actor refines his techniques and modus operandi over the next several months.

Traffic-Light Protocol for Information Dissemination

Color	When Should It Be Used?	How May It Be Shared
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use the TLP: AMBER when information requires support to be effectively acted upon but carries the risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Source and Information Reliability

Source

	Rating	Description
A	Reliable	No doubt about the source's authenticity, trustworthiness, or competency. History of complete reliability.
B	Usually Reliable	Minor doubts. History of mostly valid information.
C	Fairly Reliable	Doubts. Provided valid information in the past.
D	Not Usually Reliable	Significant doubts. Provided valid information in the past.
E	Unreliable	Lacks authenticity, trustworthiness, and competency. History

		of invalid information.
F	Can't Be Judged	Insufficient information to evaluate reliability. May or may not be reliable.

Information

	Rating	**Description**
1	Confirmed	Logical, consistent with other relevant information, confirmed by independent sources.
2	Probably True	Logical, consistent with other relevant information, not confirmed by independent sources.
3	Possibly True	Reasonably logical, agrees with some relevant information, not confirmed.
4	Doubtfully True	Not logical but possible, no other information on the subject, not confirmed.
5	Improbable	Not logical, contradicted by other relevant information.
6	Can't Be Judged	The validity of the information can not be determined.

[i] http://news.softpedia.com/news/UGNazi-Hacker-Cosmo-the-God-Sentenced-to-Six-Years-Without-Internet-305967.shtml
[ii] http://news.softpedia.com/news/24-Cybercriminals-From-13-Countries-Arrested-Ugnazi-Hacker-Among-Them-277753.shtml
[iii] http://news.softpedia.com/news/CyberZeist-Claims-to-Have-Gained-Access-to-Hundreds-of-Federal-Accounts-276384.shtml
[iv] http://pastebin.com/q5UNiK4B
[v] http://pastebin.com/E4cPi7md
[vi] http://pastebin.com/E4cPi7md
[vii] https://www.cyberwarnews.info/2012/06/22/uks-biggest-private-security-company-g4s-hacked-data-leaked-by-le4ky/
[viii] http://pastebin.com/1ca3BR19
[ix] http://pastebin.com/b79cJV5f
[x] http://pastebin.com/KpVPRehV
[xi] http://www.gizmodo.in/news/Hackers-Claim-They-Wiped-John-Podestas-iPhone/articleshow/54839826.cms
[xii] http://pastebin.com/fYCWmNGU
[xiii] https://www.cyberwarnews.info/2016/11/09/alaskan-elections-website-hacked-by-cyberzeist-2/
[xiv] http://pastebin.com/yvS9NWWP

From: Thomas Duffy
To: Letterman, Chris E (DOA); Davis, Myron L (DOA)
Cc: Brian Calkin
Subject: FW: New LookingGlass CTIG Report: CyberZeist-CTIG-048 (TLP:Green)
Date: Tuesday, December 6, 2016 7:03:43 AM
Attachments: CyberZeist CTIG-048.pdf

FYI

Thomas Duffy
Senior Vice President of Operations
Chair, Multi-State ISAC
31 Tech Valley Drive
East Greenbush, NY 12061
[redacted]

From: Roisin Suver <[redacted]
Date: Tuesday, December 6, 2016 at 10:44 AM
To: "IIC.Analysis.dl" <[redacted]ty.org>, Ms-Isac Soc[redacted]
Cc: Thomas Duffy <[redacted]y.org>, Brian Calkin <[redacted]org>
Subject: FW: New LookingGlass CTIG Report: CyberZeist-CTIG-048 (TLP:Green)

TLP GREEN

FYSA:
Attached is a report from LookingGlass on the actor CyberZeist. This was the actor that claimed the compromise of Alaska's Online Voter system via Twitter during the Presidential Election. The actor has now moved to the banking and finance sector.

Thanks,
Roisin

Roisin S. Suver
Senior Liaison to DHS NCCIC
Multi-State ISAC
Center for Internet Security
[redacted]

From: Craig Wilson [mailto[redacted]r.com]
Sent: Tuesday, December 06, 2016 10:28 AM
To: Suver, Roisin (CTR); Fosmire, Kurt; NCCIC - USCERT; US-CERT operation center; Moran, Kevin (CTR)
Subject: New LookingGlass CTIG Report: CyberZeist-CTIG-048 (TLP:Green)

Attached please find a newly developed LookingGlass Threat Actor report on CyberZeist. The actor was deeply invested in the US Presidential campaign, hacking the cell phone of John

Podesta (Campaign Manager). On October 11, he leaked e-mail addresses and passwords compromised from Hilaryclinton[dot]com. On October 14, in a Pastebin posting, **CyberZeist** detailed how the Democratic National Committee was hacked. In early November 2016, the actor dumped the database of Moreland.ny.gov.

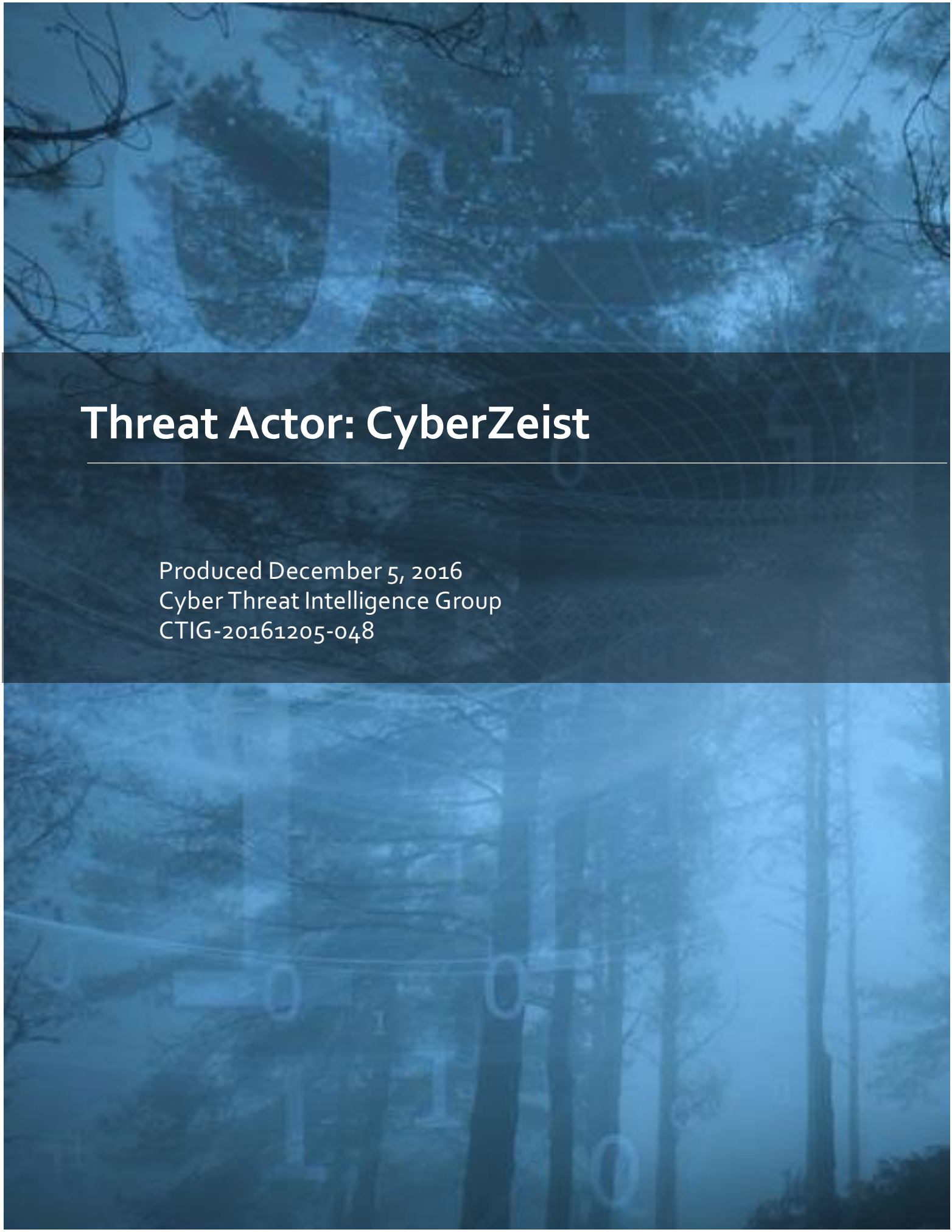
Threat actor **CyberZeist** is currently targeting global banks exploiting the LFI vulnerability. In two instances, the actor has threatened to sell access to the banks in exchange for Bitcoins if the vulnerabilities are not patched promptly. The actor has a history of conducting hostile cyber activity having been part of the UGNazi hacker group that conducted attacks against high profile organizations, as well as participating in some Anonymous operations. The shift to targeting banks is disconcerting, and it is the belief of the Cyber Threat Intelligence Group (CTIG) that CyberZeist will likely follow through on his threats, based on previous history with breaches and leaking data.

The actor was deeply invested in the US Presidential campaign, hacking the cell phone of John Podesta (Campaign Manager). On October 11, he leaked e-mail addresses and passwords compromised from Hilaryclinton[dot]com. On October 14, in a Pastebin posting, **CyberZeist** detailed how the Democratic National Committee was hacked. In early November 2016, the actor dumped the database of Moreland.ny.gov.

Craig R. Wilson
LookingGlass Cyber Solutions
Federal Account Manager
[redacted]

...

. . .



Threat Actor: CyberZeist

Produced December 5, 2016
Cyber Threat Intelligence Group
CTIG-20161205-048

Overall Report Distribution is TLP: GREEN
Overall Source/Information Reliability: B2

Executive Summary

Threat actor **CyberZeist** is currently targeting global banks exploiting the LFI vulnerability. In two instances, the actor has threatened to sell access to the banks in exchange for Bitcoins if the vulnerabilities are not patched promptly. The actor has a history of conducting hostile cyber activity having been part of the UGNazi hacker group that conducted attacks against high profile organizations, as well as participating in some Anonymous operations. The shift to targeting banks is disconcerting, and it is the belief of the Cyber Threat Intelligence Group (CTIG) that CyberZeist will likely follow through on his threats, based on previous history with breaches and leaking data.

Key Points

- **CyberZeist** is a hacker with a history of conducting hostile acts against high profile organizations. The actor has been involved in breaches and data leaks.

- The actor's shift toward banks is an indication that the actor is seeking to monetize his hacking efforts under the guise of security concern for banks' slow vulnerability patching processes. Based on previous history, CTIG believes that the actor has the intent and capability to leak data and/or sell access.

**This report is based on open source findings. Therefore, the report is open source intelligence and does not constitute definitive evidence. Information found in the open source cannot necessarily be verified and is presented as intelligence and as additional information to enhance or expand current investigations.*

Background

UGNazi Hacking Group

Threat actor **"CyberZeist"** was formerly a member of the UGNazi collective, a group of hackers that gained notoriety for disrupting and breaching several high-profile websites, including the ones of NASDAQ, the Central Intelligence Agency (CIA), Department of Justice, WHMCS (a web hosting automation platform), 4Chan, and CloudFlare.[i] Several of the Collectives members were arrested during 2012[ii], notably their leader, prompting a hiatus from their hacking activities. While with UGNazi, **CyberZeist** spearphished U.S. federal employees, obtaining their usernames and password credentials. The actor subsequently leaked more than 250 record sets comprising e-mail addresses and clear text passwords.[iii] Sometime in 2012, **CyberZeis**t broke from the group for "personal reasons" to pursue his own hacking endeavors, concentrating on attacking the U.S. Government.

Going Solo

Under the alias "**comrade**" in a June 17, 2012 Pastebin posting, **CyberZeist** claimed to have maintained access to Cobank (a national cooperative bank serving vital industries across rural America) for over a year after disclosing it on June 17, 2012. **CyberZeist** exposed the logins of Cobank employees, as well as the software used by the bank. In addition, **CyberZeist** provide logs compromised from Citibank.[iv] Also in 2012, using the Twitter alias "**@l34ky**," **CyberZeist** targeted the CIA, the Federal Bureau of Investigation (FBI), Comcast, Nepal Bank, Intel, and Baidu.

- In another Pastebin posting, **CyberZeist** under the alias **comrade** claimed responsibility for hacking into major airlines including American Airlines, United Airlines, Vietnam Airlines, and Sabre Airlines (note: the actor may have meant Sabre Airline Solutions, systems on which many comprehensive technology solutions that help the airline industry). The actor claimed internal access to flight booking, ticketing info, hotel booking, card swaps, employee information, and flight and passenger information.[v]

In June 2013, fearing that the FBI was tracking his activities, **CyberZeist** apologized to companies he had hacked and publicly exposed. He wanted everyone to know that he could have been stealing credit cards and private travel information but didn't in an attempt to downplay the seriousness and scope of the attacks.[vi]

Anonymous Operations

CyberZeist has been involved in a number of Anonymous operations over the years. In particular, the actor claimed credit for 2012's #Opstopg4s (he did this under the alias **l34ky**. The target was one of the largest security company in the United Kingdom),[vii] #OpSaveTheArctic (he did this under the alias

CyberZeist and referenced **L34ky's** Twitter handle. Targets included global gas companies exploring the Arctic),[viii, ix] and #OpLithChild (a campaign to stop pedophilia in Lithuania as well as worldwide).

The Interlude

From August 2, 2014 to October 6, 2016 there was a long period of unexplained silence from **CyberZeist.** However, on October 9, **CyberZeist** broke the inactivity by releasing login credentials of Pakistan government officials from the Twitter alias "**@cyberzeist**."[x]

Politics

CyberZeist was also deeply invested in the U.S. presidential election, and participated in the hacking the cell phone of John Podesta, the then chairman of Hilary Clinton's campaign.[xi] On October 11, he leaked e-mail addresses and passwords compromised from Hilaryclinton[dot]com (see Figure 1). On October 14, in a Pastebin posting, **CyberZeist** detailed how the Democratic National Committee was hacked.[xii] In early November 2016, the actor dumped the database of Moreland.ny.gov.

Figure 1: Screenshot of Hilaryclinton.com Dump

Also in November, **CyberZeist's** activities ventured into the world of botnets. The actor stated that the intent was to launch distributed denial-of-service (DDoS) attacks during the November 8 election (see Figure 2). On Election Day, **CyberZeist** showed that he had administrative access over the Alaska Election Division website.[xiii] On November 9, **CyberZeist** was ultimately blocked from elections[dot]Alaska[dot]gov, and on November 11, the actor proceeded to leak the passwords of Washington State government employees.

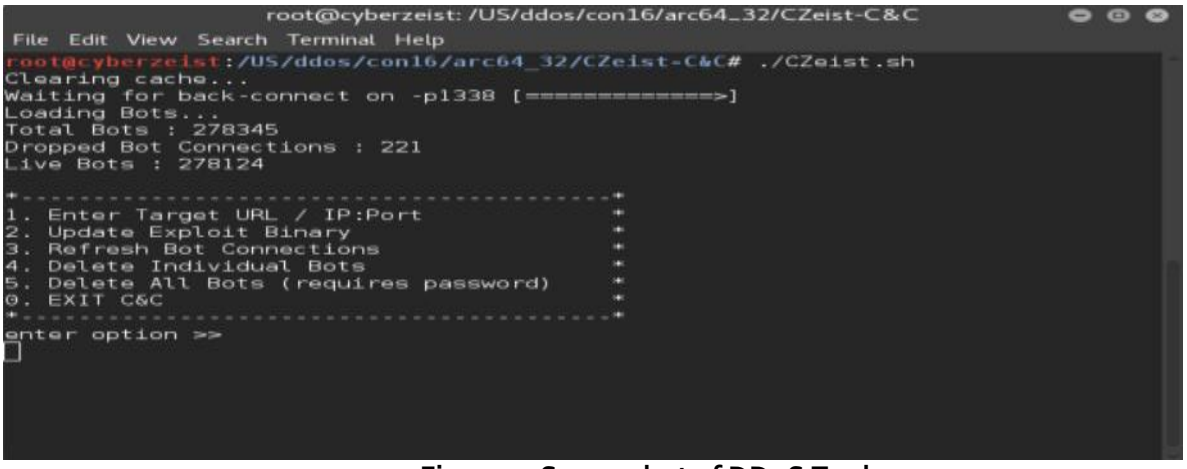


Figure 2: Screenshot of DDoS Tool

Target Shift: Banks

In mid-November 2016, **CyberZeist** realized the enormous profits to be made by hacking banks' websites. On November 15, the actor released an LFI Vulnerability (Remote File Inclusion (RFI) and Local File Inclusion (LFI) are vulnerabilities which are often found in poorly written web applications. These vulnerabilities occur when a web application allows the user to submit input into files or upload files to the server.

LFIs allow an attacker to read and sometimes execute files on the victim machine. This can be very dangerous because if the web server is misconfigured and running with high privileges, the attacker may gain access to sensitive information. If the attacker is able to place code on the web server through other means, then they may be able to execute arbitrary commands.) he found on Barclay's[dot]co[dot]uk (see Figure 3).

Figure 3: Screenshot of Barclay's bank

Afterwards, **CyberZeist** hacked the Royal Bank of Scotland. LFI vulnerabilities were used to target other banks as well including JP Morgan Chase (see Figure 4), Abu Dhabi Islamic Bank (November 21), Bank of India and Axis Bank (November 22), and HSBC Bank (November 28).

Figure 4: Screenshot of JP Morgan Chase

On December 1, the National Australia Bank was hacked using an LFI attack with CyberZeist threatening to sell access to it for Bitcoins if the vulnerability was not patched within 7 days (see Figure 5). As of this writing, the Royal Bank of Scotland is still vulnerable with CyberZeist making the same threat if it is not patched promptly.

Figure 5: Screenshot of CyberZeist Twitter

Social Media and Contact Information

Twitter Accounts

@officialcomrade

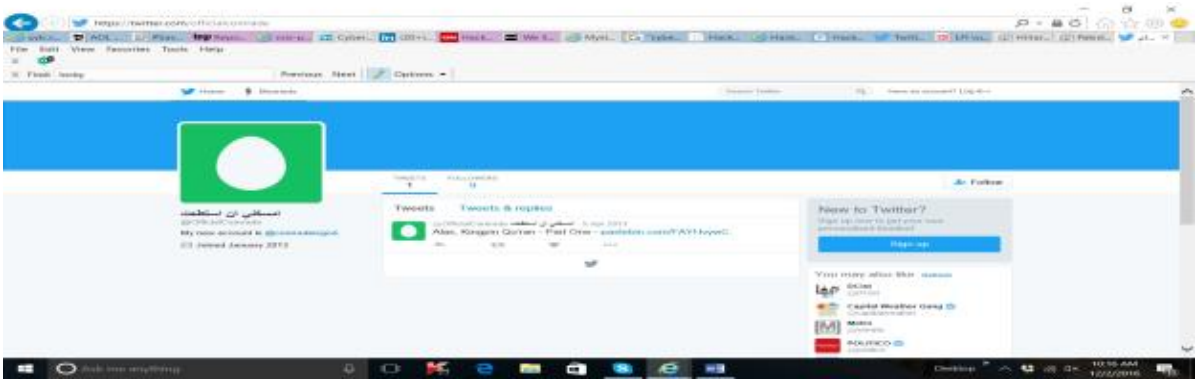


Figure 6: @officialcomrade Notifying of New Twitter Handle

@comradeisgod

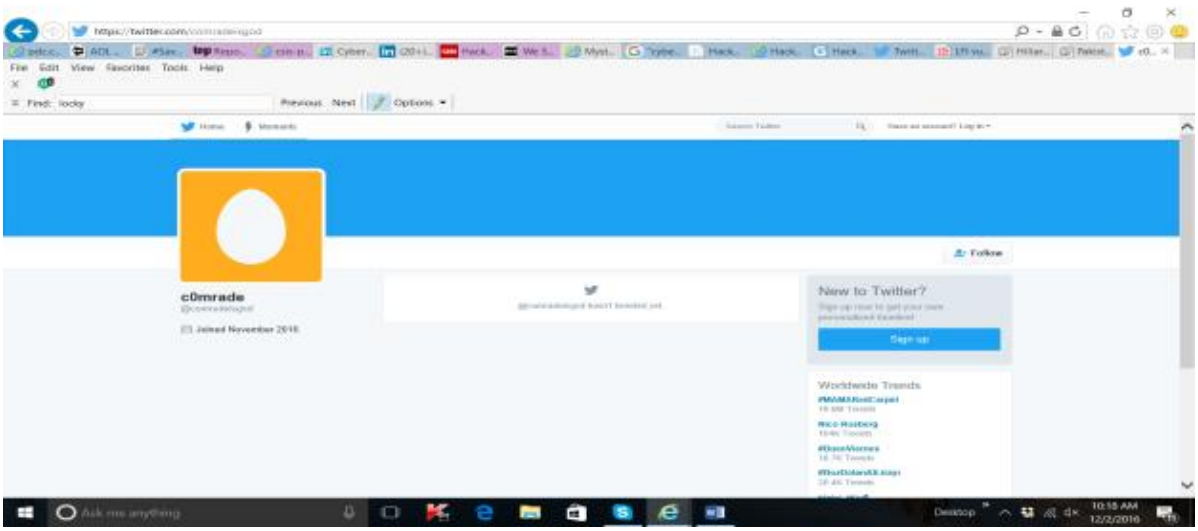


Figure 7: @comradeisgod New Twitter Page

@le4ky

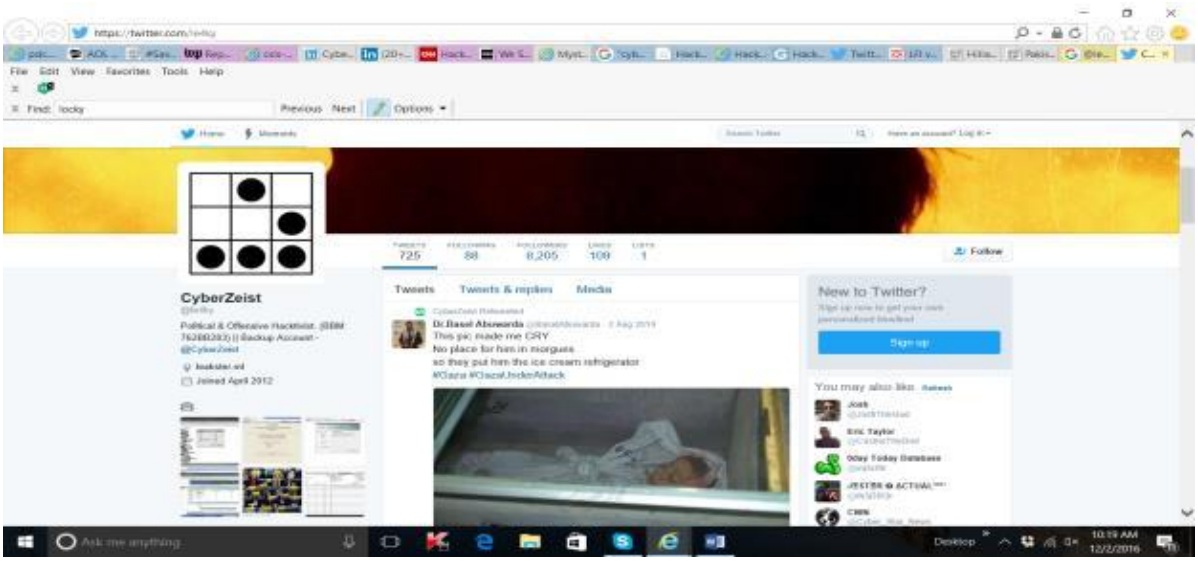


Figure 8: @le4ky Twitter Page

@CyberZeist

Account currently suspended.

@CyberZeist2

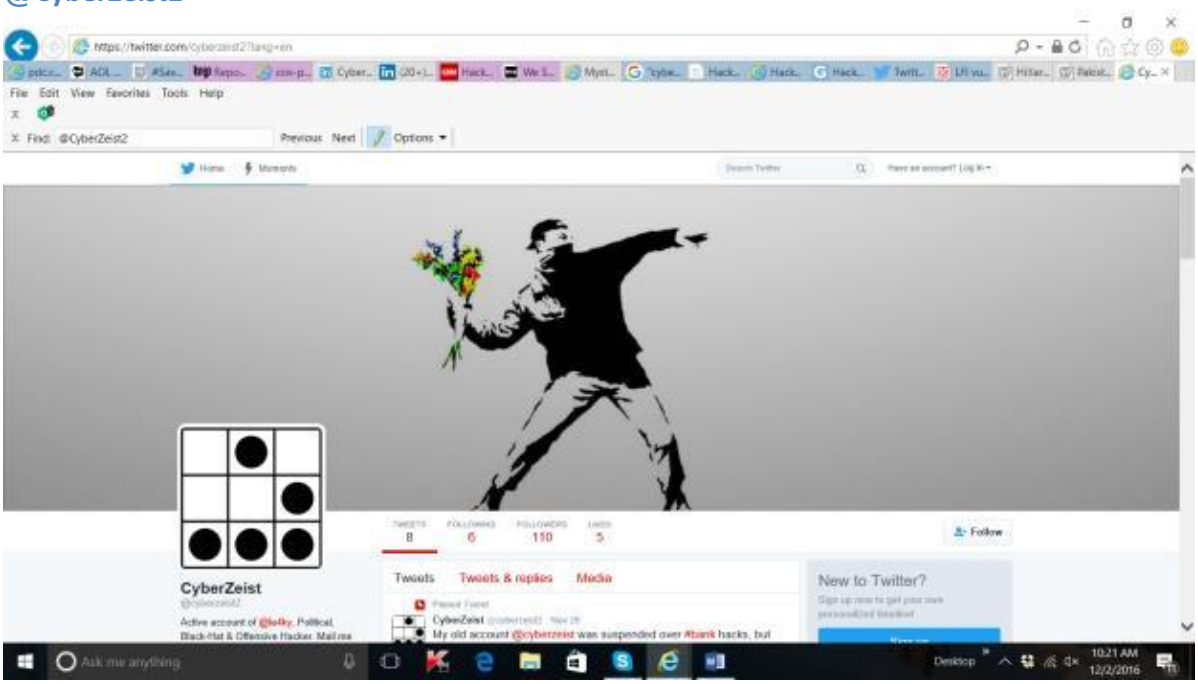


Figure 9: @CyberZeist2 Twitter Page

E-mail Addresses

CyberZeist[@]live.com
Cyberzeist[@]protonmail.com
Anonymous.cyberzeist[@]gmail.com

Known Domains Associated with CyberZeist

Leakster[dot]net

Purchased by @JoshTheGod (@VariousLulz), the leader of UGNazi.

Leakster[dot]ml

No Whois history associated with the domain. The domain is likely used by webhostooo, and the likely password is 3316opc8. The domain may be administrated using e-mail address anonymous.cyberzeist[@]gmail.com

Passwords Used by the Actor

3316opc8[xiv] - [MD5] 3e275d7d78c16368089b82278fc43d0b

Conclusions

CTIG believes that **CyberZeist** is a credible threat to banks based on recent activity and statements threatening to sell accesses to vulnerable banks who do not promptly patch their systems. **CyberZeist** has a history of malicious hacking activity with known hacking groups and hacktivist enclaves like Anonymous. **CyberZeist's** recent activities – breaching Podesta's cell phone and interest in developing DDoS capability indicate that the actor is interested in activities that garner media attention, and thus further solidifying his bona fides as an individual of note. We expect **CyberZeist** to continue to target banks as the actor refines his techniques and modus operandi over the next several months.

Traffic-Light Protocol for Information Dissemination

Color	When Should It Be Used?	How May It Be Shared
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use the TLP: AMBER when information requires support to be effectively acted upon but carries the risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Source and Information Reliability

Source

	Rating	Description
A	Reliable	No doubt about the source's authenticity, trustworthiness, or competency. History of complete reliability.
B	Usually Reliable	Minor doubts. History of mostly valid information.
C	Fairly Reliable	Doubts. Provided valid information in the past.
D	Not Usually Reliable	Significant doubts. Provided valid information in the past.
E	Unreliable	Lacks authenticity, trustworthiness, and competency. History

		of invalid information.
F	Can't Be Judged	Insufficient information to evaluate reliability. May or may not be reliable.

Information

	Rating	**Description**
1	Confirmed	Logical, consistent with other relevant information, confirmed by independent sources.
2	Probably True	Logical, consistent with other relevant information, not confirmed by independent sources.
3	Possibly True	Reasonably logical, agrees with some relevant information, not confirmed.
4	Doubtfully True	Not logical but possible, no other information on the subject, not confirmed.
5	Improbable	Not logical, contradicted by other relevant information.
6	Can't Be Judged	The validity of the information can not be determined.

[i] http://news.softpedia.com/news/UGNazi-Hacker-Cosmo-the-God-Sentenced-to-Six-Years-Without-Internet-305967.shtml
[ii] http://news.softpedia.com/news/24-Cybercriminals-From-13-Countries-Arrested-Ugnazi-Hacker-Among-Them-277753.shtml
[iii] http://news.softpedia.com/news/CyberZeist-Claims-to-Have-Gained-Access-to-Hundreds-of-Federal-Accounts-276384.shtml
[iv] http://pastebin.com/q5UNiK4B
[v] http://pastebin.com/E4cPi7md
[vi] http://pastebin.com/E4cPi7md
[vii] https://www.cyberwarnews.info/2012/06/22/uks-biggest-private-security-company-g4s-hacked-data-leaked-by-le4ky/
[viii] http://pastebin.com/1ca3BR19
[ix] http://pastebin.com/b79cJV5f
[x] http://pastebin.com/KpVPRehV
[xi] http://www.gizmodo.in/news/Hackers-Claim-They-Wiped-John-Podestas-iPhone/articleshow/54839826.cms
[xii] http://pastebin.com/fYCWmNGU
[xiii] https://www.cyberwarnews.info/2016/11/09/alaskan-elections-website-hacked-by-cyberzeist-2/
[xiv] http://pastebin.com/yvS9NWWP

Steele, Jim A (DOA)

From:	Steele, Jim A (DOA)
Sent:	Tuesday, December 6, 2016 10:52 AM
To:	Letterman, Chris E (DOA); Fisher, Sheldon A (DOA)
Subject:	RE: Elections Results Issue

Thanks Chris.

Sheldon – both attachments provide an overview of CyberZeist and his/her known aliases, email addresses, domains used and other such activities. It's essentially a rap sheet.

Nothing essential here; more of an FYI.

JS

Jim Steele
State Information Technology Officer
Enterprise Technology Services Director
State of Alaska | Department of Administration
Anchorag[redacted]
Mobile[redacted] BOI

From: Letterman, Chris E (DOA)
Sent: Tuesday, December 6, 2016 8:30 AM
To: Fisher, Sheldon A (DOA) <s[redacted]v>
Cc: Steele, Jim A (DOA) [redacted]
Subject: RE: Elections Results Issue

Commissioner,
I have attached for your information and situational awareness an email received this morning from the Multi-State Information Sharing and Analysis Center (MS-ISAC). It is a forward of a message from Roisin S. Suver who is the Senior Liaison to Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) regarding new information about the cyber actor who targeted the state's election result website. The information is classified traffic light protocol green (TLP) which means it may be shared within our organization, however I defer to your judgement to share as you see fit with the Governor's Office/Division of Elections personnel/other parties.

-Chris
[redacted]
BOI mobile.

From: Letterman, Chris E (DOA)
Sent: Tuesday, November 8, 2016 1:57 PM
To: Fisher, Sheldon A (DOA) <s[redacted]v >
Cc: Steele, Jim A (DOA) <jim.steele@alaska.gov >
Subject: Elections Results Issue

Commissioner,
This morning at 5:37am we were notified via an alert that an unknown individual (@CyberZeist twitter handle) had posted a screen shot from what appeared to be a compromised Alaska Division of Elections reporting system.

Here is what we know:

1. The individual successfully executed an exploit to PHP (a computer scripting language used heavily in web presentation)
2. The individual was able to use privilege escalation to access the server's underlying file system.
3. The individual posted to their Twitter account a screen shot from the GEMS Election Results System as proof they were capable of accessing administrative areas of the server.
4. Along with the screen shot, the following message was posted "#USElections2016 Alaska Election Division online #ballot administrator access #pwned.. waiting for people to start voting"

At this time I have SSO staff working with Gov's office staff to get the server's vulnerable PHP installation patched. Additionally, we are building more aggressive hunting rules for our McAfee security solutions. Finally, this server will eventually be taken down once results begin to come in and are reported. The standard operating procedure for posting elections results are to turn up new virtual machines with the static results. Our analysis of this event is that there was no compromise of classified information as election results are public data. With the PHP vulnerability patched and the SOP for elections reporting, I am confident we have this matter resolved.

It is worth mentioning @CyberZeist did make a general threat to launch distributed denial of service attack(s) today. The threat is not specific to the State of Alaska, but if such an attack is launched against elections.alaska.gov we may be impacted which would result in delays and timeouts when people attempt to access the election results online at elections.alaska.gov.

If you have any further questions please let me know.

-*Chris*

Chris Letterman
Chief Information Security Officer
State of Alaska : Enterprise Technology Services
PO Box 110206
333 Willoughby Avenue
5th Fl. State Office Building
Juneau, AK 99811-0206

Steele, Jim A (DOA)

From: Steele, Jim A (DOA)
Sent: Tuesday, December 6, 2016 10:53 AM
To: Letterman, Chris E (DOA)
Subject: FW: Elections Results Issue

Will explain later why I did that.

Jim Steele
State Information Technology Officer
Enterprise Technology Services Director
State of Alaska | Department of Administration
Anchorage [redacted]
Mobile [redacted] BOI

From: Steele, Jim A (DOA)
Sent: Tuesday, December 6, 2016 10:52 AM
To: Letterman, Chris E (DOA) <[redacted]ov>; Fisher, Sheldon A (DOA) <[redacted]v>
Subject: RE: Elections Results Issue

Thanks Chris.

Sheldon – both attachments provide an overview of CyberZeist and his/her known aliases, email addresses, domains used and other such activities. It's essentially a rap sheet.

Nothing essential here; more of an FYI.

JS

Jim Steele
State Information Technology Officer
Enterprise Technology Services Director
State of Alaska | Department of Administration
Anchorage [redacted]
Mobile [redacted] BOI

From: Letterman, Chris E (DOA)
Sent: Tuesday, December 6, 2016 8:30 AM
To: Fisher, Sheldon A (DOA) <[redacted]>
Cc: Steele, Jim A (DOA) <[redacted]>
Subject: RE: Elections Results Issue

Commissioner,
I have attached for your information and situational awareness an email received this morning from the Multi-State Information Sharing and Analysis Center (MS-ISAC). It is a forward of a message from Roisin S.

Suver who is the Senior Liaison to Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) regarding new information about the cyber actor who targeted the state's election result website. The information is classified traffic light protocol green (TLP) which means it may be shared within our organization, however I defer to your judgement to share as you see fit with the Governor's Office/Division of Elections personnel/other parties.

-Chris

[redacted]
BOI mobile.

From: Letterman, Chris E (DOA)
Sent: Tuesday, November 8, 2016 1:57 PM
To: Fisher, Sheldon A (DOA) <[redacted]>
Cc: Steele, Jim A (DOA) <jim.steele@alaska.gov>
Subject: Elections Results Issue

Commissioner,
This morning at 5:37am we were notified via an alert that an unknown individual (@CyberZeist twitter handle) had posted a screen shot from what appeared to be a compromised Alaska Division of Elections reporting system.

Here is what we know:

1. The individual successfully executed an exploit to PHP (a computer scripting language used heavily in web presentation)
2. The individual was able to use privilege escalation to access the server's underlying file system.
3. The individual posted to their Twitter account a screen shot from the GEMS Election Results System as proof they were capable of accessing administrative areas of the server.
4. Along with the screen shot, the following message was posted "#USElections2016 Alaska Election Division online #ballot administrator access #pwned.. waiting for people to start voting"

At this time I have SSO staff working [redacted] to get the server's vulnerable PHP installation patched. Additionally, we are building more aggressive hunting rules for our McAfee security solutions. Finally, this server will eventually be taken down once results begin to come in and are reported. The standard operating procedure for posting elections results are to turn up new virtual machines with the static results. Our analysis of this event is that there was no compromise of classified information as election results are public data. With the PHP vulnerability patched and the SOP for elections reporting, I am confident we have this matter resolved.

It is worth mentioning @CyberZeist did make a general threat to launch distributed denial of service attack(s) today. The threat is not specific to the State of Alaska, but if such an attack is launched against elections.alaska.gov we may be impacted which would result in delays and timeouts when people attempt to access the election results online at elections.alaska.gov.

If you have any further questions please let me know.

-Chris

Chris Letterman
Chief Information Security Officer
State of Alaska : Enterprise Technology Services

PO Box 110206
333 Willoughby Avenue
5th Fl. State Office Building
Juneau, AK 99811-0206