Investigation Log

Handled By Kush Patel

On February 13th at 10:12 AM I discovered that there was a phishing message from the internal user of jrobinson@securetech.com, which was reported by another user who was smorgan@securetech.com when she received an email

On February 13th at 10:17 AM I discovered that an employee in the company with the IP address of 10.10.1.7 made a login into a external website and gave information

On February 13th at 10:22 AM I discovered that the potential phishing had a website that started with http, which should show that it's insecure

On February 13th at 10:22 AM I discovered that the user “jrobinson@securetech.com” on Febuary 7 2:06 - 2:10 consistently send out emails to other clients and users in the securetech company with the securetech email server which shows that he is targeting people within the company by sending those emails

On February 13th at 10:25 AM I discovered that some the user “jrobinson@securetech.com” on Febuary 7 was receiving emails from outside the secretech domain to like “mary92@bradley-howe.info” ,”bbaker@hotmail.com” , “tommykirby@roberts.info”, “jtaylor@yahoo.com”, and many more outsider users, he was receiving it both before and after he sent those spam messages with the phishing link to 81 of those users, which could eitheir mean that he was either collaborating with outside users to coordinate or plan a phishing attack or just the usual emails he recieve like the other users do

On February 13th at 10:30 AM I discovered that in the HTTP logs, there were so many unknown and unsecure and unsafe dns domains like .biz which is also not secure,

On February 13th at 10:35 AM, I discovered that Many of the SMTP connections are coming from the ip address of 23.74.164.69, in which the srv-61.kim.johnson.biz is located. Every email from jrobinson@securetech.com is coming through this IP, which shows that an outside person has compromised his email

On February 13th at 10:38 AM, I also noticed that jrobinson@securetech.com did normal activity no malicious activity like the other securetech users did, based on the logs after he repeatedly sent messages to the other users in the same ip, it showed that he received emails from outsiders like the other securetech users did based on the logs at various times and from different users like the other securetech users did, which could hint that their account has been compromised

On February 13th at 10:41 AM, In the mail logs i discovered that jrobinson@securetech.com was the only user with securetech.com in the logs that sent a message and he only sent it to the other seucretech users no other email address which showed that he was targeting other securetech users in a phishing attack, and the mail logs showed that no other email with securetech or in the securetech domain sent out an email only jrobinson@securetech.com

On February 13th at 10:45 AM I discovered that there was there was POST when someone accessed the website which was “srv-61.kim.johnson.biz", which showed that person with the IP address of 10.10.3.185 who is sritter@securetech.com gave his personal or any information to the website which incidates he became a victim of phishing and he’ll end up loosing some important information, the POST indicated that he sent information to that website and gave them information

On February 13th at 10:49 AM In the mail logs I also noticed that no other user in the securetech domain sent any email to another user even to the users outside the securetech domain, and that jrobinson@securetech.com sent it to 81 other securetech users and he spammed other securetech users, because they didn’t ask for his email, it happened on Febuary 7 from 02:06-02:10

On February 13th at 10:53 AM I discovered that there was there was POST when someone accessed the website which was “srv-61.kim.johnson.biz", which showed that person with the IP address of 10.10.1.234 who is jfoster@securetech.com gave his personal or any information to the website which incidates he became a victim of phishing and he’ll end up loosing some important information, the POST indicated that he sent information to that website and gave them information, he became the second victim of the phishing email

On February 13th at 10:55 AM I discovered that there was there was POST when someone accessed the website which was “srv-61.kim.johnson.biz", which showed that person with the IP address of 10.10.2.64 who is bbarron@securetech.com gave his personal or any information to the website which incidates he became a victim of phishing and he’ll end up loosing some important information, the POST indicated that he sent information to that website and gave them information, he became the third victim of the phishing email

On February 13th at 10:57 AM I discovered that there was there was POST when someone accessed the website which was “srv-61.kim.johnson.biz", which showed that person with the IP address of 10.10.1.33 who is pmccoy@securetech.com gave his personal or any information to the website which incidates he became a victim of phishing and he’ll end up loosing some important information, the POST indicated that he sent information to that website and gave them information, he became the fourth victim of the phishing email

On February 13th at 10:59 AM I discovered that there was there was POST when someone accessed the website which was “srv-61.kim.johnson.biz", which showed that person with the IP address of 10.10.1.198 who is jball@securetech.com gave his personal or any information to the website which incidates he became a victim of phishing and he'll end up loosing some important information, the POST indicated that he sent information to that website and gave them information, he became the fifth victim of the phishing email

On February 13th at 11:03 AM I discovered that there was there was POST when someone accessed the website which was “srv-61.kim.johnson.biz", which showed that person with the IP address of 10.10.3.175 who is mbutler@securetech.com gave his personal or any information to the website which incidates he became a victim of phishing and he'll end up loosing some important information, the POST indicated that he sent information to that website and gave them information, he became the sixth victim of the phishing email

On February 13th at 11:06 AM, I noticed that every user who received an email that wasn't from jrobinson@securetech.com was from outside the securetech domain, which showed that it wasn't malicious emails from the outside domain, even jrobinson@securetech.com received a email from an outside domain which showed that the internal user whose account was compromised was actuall still able to log into his account and do his usual actvities recieved his usual emails and checked it, the actual user was logged in before his account was compromised and did his usual activities and after his account was compromised and did his usual activities

On February 13th at 11:10 AM,, I noticed that the user jrobinson@securetech.com sent most of the spams at IP address 23.74.164.69, which showed that the malicious website is at that IP address and after he sent the spams he received some messages at various ip addresses like 158.221.111.254,68.53.24.26,99.118.240.33,etc which showed whoever was logged in as jrobinson@securetech.com was doing his normal activity, which showed that he didn't loose access to his account, the attacker who compromised his account before sending those spam messages decided not to change his password or credentials because he wanted to cover himself up, it showed that his account was compromised by an attacker, the attack used jrobinson@securetech.com account to send out a huge long spam and mass email which showed it is a tactic for lateral phishing which is compromising a account without changing any credentials and sending unusual spam emails to people close to you in the network like employees in the company

On February 13th at 11:16 AM, I also discovered in the mail logs that many of the users including jrobinson@securetech.com were also receiving their usual emails from outside domains before and after the phishing attack and spamming from the compromised account of jrobinson@securetech.com , a person who somehow found the credentials, which indeed showed that there was a compromise in the account during the middle of the mail logs

On February 13th at 11:21 AM, I looked that the inventory to see which IP address does jrobinson@securetech.com belong to 10.10.1.7, I looked through the http logs and found that

that he also opened the website and entered his credentials but he opened it way before he sent that huge emai to the internal usesl and the other users with the IP address of opened that website or gave their information if they opened it which indicates that his account that was compromised by the attack was responsible for for that huge long spam phishing message he sent before the all the other users opened it, another indication that it was a phishing attack was that the user accessed the website way before everyone else did to check to see if he was able to log in as the administrator of the website and was able to gain access to other people log in information, and since he logged in way before everyone else did he was planning this attack accordingly to maked sure he doesnt have any problems in the long run, the other users who accessed the website later all accessed at or around or close to the same time frame,jrobinson@secure-tech.com or 10.10.1.7(Jason Robinson) accessed the website 10 pages in the http log before everyone else did which incidates the website was own by the attacker and then he sent it to the other users and the users with source ip address 10.10.2.123(Kaitlyn Garcia),10.10.1.98(Valerie Leach),10.10.2.236(Jamie White),10.10.3.185,10.10.1.124,10.10.1.117,10.10.2.168, who all opened the link and email around the same time frame when they received the email together

On February 13th at 11:27 AM, while reading through the mail logs I noticed that all the emails who sent a message to another person who were not apart of the secure tech domain had like at least a 1000 emails sent from that domain, like an email with “@gmail.com” had like 8,525 sent from that domain, emails ending in “.info” had like 2000 emails sent from them to a secure tech user, whereas “securetech” emails only had 81 emails which was all from jrobinson@securetech.com which indicates that the email was involved in malicious activity because no other securetech email sent an email to another securetech email which shows that is malicious and unsual activity and it was a sign of someone trying to get information from the other securetech users

On February 13th at 11:31 AM when looking through the logs I discovered the way the attacker was able to gain access to “jrobinson@securetech.com” account was when jrobinson@securetech.com logged into that malicious website of “srv-61.kim.johnson.biz”, he gave his personal information and after he left the website the attacker used his personal information to find his login and password information which he did eventually found the login information through the personal information, and because of this he logged into the jrobinson@securetech.com way later after he got the credentials and started to send emails to the other employees in the company so he could get information from them as well, all because of a email that jrobinson@securetech.com opened it caused the attacker to get his credentials and send that link to the other employees once compromised and logging in as the user. It happened to me one time on Instagram during middle school when someone sent me a link, I clicked on the link and the user got access to my account and sent spam emails to my follows and friends on instagram, and because of this I had to delete my instagram account and start a new one, and when “jrobinson@securetech.com” clicked there could’ve been malware at the link or site which caused the attacker to gain access to the account and then send it to any external users, like when jrobinson@securetech.com was still able to access hi account and do his usual activities of opening emails after the compromise and spam message sending like how i was able to log in and gain access to my instagram.

On February 13th at 11:38 AM after I found out the user while logged in as the legitimate user who clicked the malicious link of “srv-61.kim.johnson.biz” had given some personal information because the HTTP log shows that there was a POST method at the login api endpoint which indicated that the user gave his password and username and because of this, the attacker could have pieced together the given information from the POST method to find the credentials of the securetech users, and was able to log in as the user.

On February 13th at 11:45 AM, I discovered that the email the user “jrobinson@securetech.com” received had the link, which caused his account to be compromised after he gave his personal information based on the POST request, was part of the emails that the user usually receives like the other users in the company, and that email unknowingly lead to a malicious website that an attacker owned which he used the given information to compromise into his securetech account , which indicates the company lacks scanning of websites and emails to determine if they are safe and secure websites or malicious websites, they need to scan the link to see if they have a security certificate or not

On February 13th at 2:50 PM, I looked through all the activity after the phishing email was sent out to all the members of the securetech community,the first user that opened the link in the the spam phishing email and gave them information which was “jfoster@securetech.com” at ip address 10.10.1.234, the user accessed another website laptop-68.miller-stanley.org which indicates he accessed a safe and secure website based on the domain name, then later in the http logs i found out that the user accessed another untrusted or suspicious website ,.biz websites usually are privately owned businesses that just either want to make money from you our trying to scam or get a ransom out of the visitor which from “email-73.petersen-clark.biz” at ip addresse 208.158.16.181, but didnt give any information to that website because there was no POST, he then accessed another website which was from “db-89.mccall.com/posts/categories”, which was from a “.com”, a trusted domain, he didn’t send out any information but there was a TRACE method in which the user saw an exact message that was received and he sent out a loop test to that website to see if they received it ,

On February 13th at 3:10 PM, I looked through all the activity after the phishing email was sent out to all the members of the securetech community, the second user that opened the link in the spam phishing email and gave them information, which was “bbarron@securetech.com” at ip address 10.10.2.64, the user then accessed another website "web-81.juarez-raymond.woodward.com/main/blog/app" at ip address 102.218.197.221, which was a part of a trusted domain “.com”, there was a DELETE http message, which incidates he had accessed to his data and deleted an blog from the website he was at, the user then accessed the website “srv-02.mcdonald.chaney-forbes.info/tags/categories”, there was a PUT method which incidates that information on this website was changed and modified by the user or replaced the resources at the site with something malicious or unkown which indicates that his account was compromised and gained access to another website and used the compromised account to gain access to the website and replace its current resources with something new and malicious, the user then accessed the website "desktop-42.garcia.com/category/explore"at ip address 216.232.33.244, there was a TRACE method in which the user saw an exact message that was received, which showed there is a possible sign of an exploit which can open up the network and user to malicious website which can send it to third party websites, the user then received more emails from other .biz websites like msutton@kramer.biz, gonzalezjames@wheeler-clark.biz , ashleyhogan@allen.biz, nicole38@rhodes.biz, but didn't enter, change, or send any information to them and other websites the account received an email from but didn't send or change any information at the website

On February 13th at 3:40 PM, I looked through all the activity after the phishing email was sent out to all the members of the securetech community, the third user that opened the link in the spam phishing email and gave them information, which was "pmccoy@securetech.com" at ip address 10.10.1.33, the user then accsedd the website "lt-22.graham-bates.gill.org/category/categories", there was an DELETE http method which shows that there was a sign of malicious activity that his account was compromised andthe attacker went to that website and DELETE all the subcategories in the category to ruin the reputation of the actual user who has access to the website and was also trying to destroy the data of that website as part of the attack just to ruin the reputation of the account. The account then accessed another website "web-12.garcia.small.info/blog/category/categories", there was a PUT method which indicated the compromised account with the attacker changed some of the information in the category and replaced it with some new information, which showed that the attacker was spreading misinformation

On February 13th at 4:20 PM, I looked through all the activity after the phishing email was sent out to all the members of the securetech community, the fourth user that opened the link in the spam phishing email and gave them information, which was "jball@securetech.com" at ip address 10.10.1.198, the user then accsedd the website "laptop-93.mcgee-miller.com/tag/tag/category", based on the request it was a PUT method, which showed that the account changed and modified informationon that website, it could've been the compromised account tricking the website that it is the actual authorized user but in reality it isnt, the user then accessed the website db-63.cook.com/tags/blog at 38.49.113.71 , in which there was a HEAD method which indicates that the user wasn't able to get all of the contents of the website just only the header, the user then accessed the website "laptop-73.morton.com", there was an endpoint of /wp-content and there was a PATCH method which incidates that the user added something malicious to that website, like a wordpress plug in , he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again, the user then accessed the website srv-36.vazquez.wilson.org, there was a Head requests which indicates he was only able to get the headers of the website not the other information which shows he wasn't able to get more information

On February 13th at 4:40 PM, I looked through all the activity after the phishing email was sent out to all the members of the securetech community, the fifth user that opened the link in the spam phishing email and gave them information, which was "mbutler@securetech.com" at ip address 10.10.3.175, the user then accsedd the website "srv-78.owens-randolph.maldonado.com", there was a TRACE method which indicates that the which showed there is a possible sign of an exploit which can open up the network and user to malicious website which can send it to third party websites, which shows that this is dangerous

On February 14th at 8:00 AM, I noticed that not all members of the secure tech company received that spam/phishing email from jrobinson@securetech.com, other users like latkins@securetech.com , didn't receive an email from them, which indicates some of the users in the company are safe,

On February 14th at 9:32 AM, mjones@securetech.com at IP address 10.10.3.119, deleted a category from the WordPress part of the website db-31.cross.chang.com, which is an API endpoint of WordPress, however, she did not receive an email from jrobinson@securetech.com, which indicates this was activity that won't affect the other users

On February 14th at 10:14 AM, i discovered that twelch@securetech.com at IP address 10.10.1.136 deleted something at email-71.gibbs-jackson.espinoza.info, but didn't receive that phishing email from jrobinson@securetech.com ,

On February 14th at 11:01 AM, i discovered that mbennet@securetech.com at ip address 10.10.0.170, modified something based on the patch method, which was a website which was a a post at lt-54.ibarra-hernandez.com, he did open the malicious link sent by jrobinson@securetech.com, but didn't give any information because there was no POST method, but we should change his credentials, quarantine the affectws users just in case if he could be a potential threat.

On February 14th at 11:36 AM, i discovered that jlee@securetech.com at ip address 10.10.3.231 modified a post at lt-54.ibarra-hernandez.com" but no other user accessed that website but jlee@securetech.com accessed the malicious website of srv-61.kim.johnson.biz but didnt give any information because there was no POST method

On February 14th at 12:24 PM, I discovered that anything harm something would occur at PUT DELETE,TRACE or PATCH, because data gets changed, replaced, or modified at those methods which would narrow my search, whereas people would be lead into traps and problems at POST methods, because POST methods incidate that the user gives data in which the attacker could use that data and compromise the server. TRACE indicates that there is a information being sent in a loop back and forth in which attackers can get information that is sensitive

On February 14th at 12:26 PM, I discovered that user jmeyers@securetech.com with the IP address of 10.10.2.111, modified a website by adding a wordpress plug in to a website based on the method PATCH and the API endpoint wp-content at website db-76.mays-mann.melendez-anderson.com which indicates there was some malicious software in the plug in and his account may have been compromised but it is not guaranteed but just in case we should talk to him and change his credentials but that website only occurred once in the logs

On February 14th at 12:29 PM, I discovered that user jthomas@securetech.com with ip address 10.10.1.47 deleted a wordpress plugin which showed that he was trying to delete something malcious

On February 14th at 12:35 PM i discovered that user mmorales@securetech.com at ip address 10.10.3.157 deleted an explore from srv-40.trujillo.garcia.com, he received a scam email from jrobinson@securetech.com but didn't open the link since there was no GET method for the link jrobinson@securetech.com sent which shows his account is fine and wasn't compromised

On February 14th at 12:37 PM i discovered that user tprice@securetech.com at ip address 10.10.2.0, replaced a wordpress search content with something new based on the PUT method , he didnt open the link that was in the phishing email from jrobinson@securetech.com nor received the email from him

On February 14th at 12:38 PM i discovered that jrobinson@securetech.com who sent out the spam emails with the phishing link of srv-61.kim.johnson.biz acccessed, he couldve done a another malicious thing by deleting all the categories from srv-82.adkins-hinton.romero.biz based on the HTTP delete method

On February 14th at 12:45 PM I discovered csanders@securetech.com with IP address 10.10.0.14 modified and replaced a web content at a website based on the PUT method and the API endpoint "wp-content/main" at srv-97.romero-liu.com", which could suggest its a malicious attempt to modify web content.

On February 14th at 2:52 PM, I discovered that jbrown@securetech.com, with IP address 10.10.3.176, modified Web content in categories section at a website based on the PATCH method and the API endpoint "categories/wp-content/explore" at srv-97.romero-liu.com, which could suggest a malicious attempt to modify web content.

On February 14th at 3:22 PM, I discovered that kleach@securetech.com, with IP address 10.10.2.177, modified Web content in categories section at a website based on the PATCH methid and the API endpoint "wp-content/tag/category" at srv-90.brown.com, which could suggest a malicious attempt to modify web content. It potentially indicates unauthorised modifications or tampering with the tag/category.

On February 14th at 3:42 PM, I discovered that jsanders@securetech.com with ip address 10.10.3.74, modified the tags in the explore end point, based on the PATCH method at email-63.moyer-choi.net which could suggest a malicious attempt to modify web content.

On February 14th at 4:22 PM, I discovered that jdiaz@securetech.com, with IP address 10.10.1.147, modified Web content at a website based on the PUT method and the API endpoint "tags/main/wp-content" at desktop-43.glover.com, which could suggest a malicious attempt to replace web content.

On February 14th at 4:46 PM, I discovered that cchavez@securetech.com, with IP address 10.10.2.35 and jmendoza@securetech.com with ip address 10.10.0.232 modified Web content in the posts section at a website based on the PUT method and the API endpoint "wp-content/posts" at email-11.smith-cross.org, which could suggest a malicious attempt to replace web content.

On February 14th at 5:02 PM, I discovered that cstrickland@securetech.com, with IP address 10.10.0.118, modified Web content in the explore section at a website based on the PUT method and the API endpoint "wp-content/explore" at laptop-80.reeves.com", which could suggest a malicious attempt to replace web content.
On February 14th at 5:37 PM, I discovered that bbenjamin@securetech.com, with IP address 10.10.0.159, modified Web content in the blog section of an endpoint based on the PUT method and the API endpoint "blog/categories/wp-content"" at "desktop-99.dunn.org", which could suggest a malicious attempt to replace web content.

On February 14th at 5:53 PM, I discovered that mmorales@securetech.com, with IP address 10.10.3.75, modified Web content in the explore section of an endpoint based on the PUT method and the API endpoint "category/explore/wp-content"" at "laptop-86.brown.org", which could suggest a malicious attempt to replace web content. He, however, opened the malicious link srv-61.kim.johnson.biz jrobinson@securetech.com sent to the other users, which indicates his account could have been infected when he clicked on the link, but there was no POST method of his opening the link srv-61.kim.johnson.biz, which incidates he didn't give any personal information which shows his account wont be compromised by other outside users

On February 14th at 6:12 PM, I discovered that jhenry@securetech.com, with IP address 10.10.2.191, modified Web content based on the PUT method and the API endpoint "wp-content"" at "laptop-93.reese-rasmussen.biz", which could suggest a malicious attempt to replace web content. Wp-content is often targetted in exploits

On February 15th at 7:56 AM, I discovered that cparker@securetech.com with IP address 10.10.3.149, modified content based on the PATCH method at srv-30.duncan.com which suggests there is something malicious there

On February 15th at 8:00 AM, I discovered that many of the users in the securetech company are using outdated versions of software and devices that no longer get updated, based on the http log containing old versions of chrome

On February 15th at 8:02 AM,, I discovered user brobertson@securetech.com with IP address 10.10.2.134, changed and modified the main part of the website at web-85.house.munoz.info based on api end points tags/main, which incidates there is something malicious

On February 15th at 8:05 AM, I discovered user jbrown@securetech.com at with IP address 10.10.0.226 modified but didnt replace content at lt-40.kelly.com by adding tags to it based on the PATCH Method

On February 15th at 8:12 AM, I discovered user nmiranda@securetech.com at with IP address 10.10.1.70, added a WordPress plug in to the website lt-23.stevens-wilson.biz" based on api endpoint “wp-content/search”, based on the patch method he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 8:25 AM,I discovered joneil@securetech.com with ip address 10.10.0.236, added posts to website laptop-47.hardy-mora.young-hernandez.info, based on the Patch method which could be malicious

On February 15th at 8:42 AM, I discovered khart@securetech.com with ip address 10.10.2.91, added a tag to website db-64.perez.com, based on the Patch method, which could be malicious

On February 15th at 9:25 AM, I discovered achristian@securetech.com with ip address 10.10.1.19, added some things to a website desktop-03.torres.gill-diaz.com

On February 15th at 9:42 AM, I discovered user jmarshall@securetech.com at with IP address 10.10.0.112, added a WordPress plug in to the website lt-47.dominguez.sheppard-franco.org based on api endpoint “wp-content”, based on the patch method he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 9:52 AM, i discovered that jbarber@securetech.com with IP address 10.10.0.89, added a list based to a website desktop-39.rios.gray.com based on the patch http method, and I also found that he opened the phishing link that was sent by jrobinson@securetech.com based on the GET method, however these is no POST method which shows that he didn’t give any information to that website which shows his account is safe

On February 15th at 10:04 AM, I discovered that epham@securetech.com with IP address 10.10.1.14 replaced some content at the website desktop-88.ward.marquez.com and replaced it with wordpress plugin which incidates he did something malicious wp-content/app

On February 15th at 10:24 AM, I discovered that cbailey@securetech.com with IP 10.10.0.55 added something to the website srv-32.johnson.weaver.net

On February 15th at 10:42 AM i discovered that pclarke@securetech.com with IP address of 10.10.0.70, based on the PATCH method inserted a wordpress plugin based on AP endpoint app/wp-content at web-61.garza.com, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 10:52 AM i discovered that jcarter@securetech.com with IP address of 10.10.2.206, based on the PATCH method inserted a wordpress plugin based on AP endpoint tags/wp-content at web-16.fuentes.brown.biz, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 11:04 AM i discovered that rblack@securetech.com with IP address of 10.10.3.32, based on the PATCH method inserted a wordpress plugin based on AP endpoint main/search/wp-content at laptop-50.rhodes.frost.net, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 11:17 AM i discovered that bho@securetech.com with IP address of 10.10.2.54, based on the PUT method inserted a wordpress plugin based on AP endpoint explore/wp-content at desktop-15.green.com, which incidates that he was doing something malicious, he applied a complete updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 11:20 AM , I discovered in the HTTP logs that many users are using outdated versions of mozilla which an example is Mozilla/5.0 which could be spoofed and attackers could be trying to evade detection

On February 15th at 11:24 AM i discovered that tingram@securetech.com with IP address of 10.10.0.233, based on the PATCH method inserted a wordpress plugin based on AP endpoint wp-content at lt-78.steele.com, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 11:32 AM i discovered that drichardson@securetech.com with IP address of 10.10.1.39, based on the PATCH method inserted a wordpress plugin based on AP endpoint wp-content at srv-57.smith.howell.org, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 11:42 AM i discovered that drichardson@securetech.com with IP address of 10.10.3.23, based on the PATCH method inserted a wordpress plugin based on AP endpoint tag/category/wp-content at srv-56.casey.jordan.com, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 11:52 AM i discovered that cjohnson@securetech.com with IP address of 10.10.0.181, based on the PUT method inserted a wordpress plugin based on AP endpoint wp-content at db-30.curtis.com, which incidates that he was doing something malicious, he applied a complete updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 12:01 PM i discovered that dking@securetech.com with IP address of 10.10.0.251, based on the PUT method inserted a wordpress plugin based on AP endpoint category/wp-content/search at lt-44.ferguson.org, which incidates that he was doing something malicious, he applied a complete updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 12:12 PM i discovered that ssmith@securetech.com with IP address of 10.10.2.67, based on the PUT method inserted a wordpress plugin based on AP endpoint wp-content/wp-content at laptop-21.peterson.smith-rollins.com, which incidates that he was doing something malicious, he applied a complete updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 12:21 PM i discovered that drichardson@securetech.com with IP address of 10.10.2.137, based on the PATCH method inserted a wordpress plugin based on AP endpoint wp-content/posts/categories at lt-23.williams.com, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 12:34 PM i discovered that kbaldwin@securetech.com with IP address of 10.10.1.196, based on the PATCH method inserted a wordpress plugin based on AP endpoint category/wp-content at db-46.gonzalez.barnett.net, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 12:47 PM i discovered that brobertson@securetech.com with IP address of 10.10.2.134, based on the PATCH method inserted a wordpress plugin based on AP endpoint blog/wp-content at db-25.lopez.com, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 1:04 PM i discovered that mmartin@securetech.com with IP address of 10.10.1.130, based on the PATCH method inserted a wordpress plugin based on AP endpoint wp-content/app/posts at web-95.hernandez.net, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 1:12 PM i discovered that jhunt@securetech.com with IP address of 10.10.3.190, based on the PATCH method inserted a wordpress plugin based on AP endpoint wp-content at laptop-36.williams.com, which incidates that he was doing something malicious, he applied a partial updated the resource by adding a word press plugin to the website in which those potential plugins and changes to the website could contain malware which can infect their website with viruses and lead to problems, the comprmoised user was trying to add a plugin to a wordpress site which could exploit its software and vulnerabilities and attacking the website to get any personal or valuable information, the compromised account made an unauthorized modification attempt on a wordpress site which showed that his account needs to be changed, and locked out, deleted and remade again

On February 15th at 3:23 PM i discovered that bhowell@securetech.com with the IP address of 10.10.0.21 opened the malicious website at srv-61.kim.johnson.biz at the IP address 23.74.164.69, based on the HTTP GET method but he didn't give any information to that website because there was no http post method but we should change his credentials and remove anything from his account just in case. He received that phishing scam email from jrobinson@securetech.com but opened it before most of the other users did

On February 15th at 3:33 PM i discovered that rsingleton@securetech.com with the IP address of 10.10.1.104 opened the malicious website at srv-61.kim.johnson.biz at the IP address 23.74.164.69, based on the HTTP GET method but he didn't give any information to that website because there was no http post method but we should change his credentials and remove anything from his account just in case.He received that phishing scam email from jrobinson@securetech.com but opened before most of the other users did

On February 15th at 3:38 PM I discovered that pgriffin@securetech.com at ip address 10.10.2.129 received an email from carmen05@gmail.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn't open the link but we should block carmen05@gmail.com from the network to prevent her from sending that malicious link

On February 15th at 3:42 PM I discovered that swaters@securetech.com at ip address 10.10.1.243 received an email from jryan@morgan-hernandez.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn't open the link but we should block jryan@morgan-hernandez.com from the network to prevent her from sending that malicious link

On February 15th at 3:51 PM I discovered that jmeyers@securetech.com at ip address 10.10.2.111 received an email from danielle36@hotmail.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn't open the link but we should block danielle36@hotmail.com from the network to prevent her from sending that malicious link

On February 15th at 4:02 PM I discovered that gwilliams@securetech.com at ip address 10.10.3.124 received an email from sonia98@hotmail.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn't open the link but we should block sonia98@hotmail.com from the network to prevent her from sending that malicious link

On February 15th at 4:10 PM I discovered that aharrell@securetech.com at ip address 10.10.1.117 received an email from steven67@nunez-hester.net which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn't open the link but we should block steven67@nunez-hester.net from the network to prevent her from sending that malicious link

On February 15th at 4:25 PM I discovered that bgonzalez@securetech.com at ip address 10.10.3.81 received an email from thompsonjeremiah@stokes.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn't open the link but we should block thompsonjeremiah@stokes.com from the network to prevent her from sending that malicious link

On February 15th at 4:31 PM I discovered that dkathleen@securetech.com at ip address 10.10.1.74 received an email from baxterjody@hotmail.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn't open the link but we should block baxterjody@hotmail.com from the network to prevent her from sending that malicious link

On February 15th at 4:36 PM I discovered that mgeorge@securetech.com at ip address 10.10.1.35 received an email from kimberly39@yahoo.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn't open the link but we should block kimberly39@yahoo.com from the network to prevent her from sending that malicious link

On February 15th at 4:38 PM I discovered that lwells@securetech.com at ip address 10.10.1.79 received an email from gpeters@wang-fox.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn't open the link but we should block gpeters@wang-fox.com from the network to prevent her from sending that malicious link

On February 15th at 4:47 PM I discovered that wsmith@securetech.com at ip address 10.10.1.31 received an email from williamsmichael@gmail.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn't open the link but we should block williamsmichael@gmail.com from the network to prevent her from sending that malicious link

On February 15th at 5:17 PM I discovered that rhorne@securetech.com at ip address 10.10.1.239 received an email from gomezjennifer@gmail.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn’t open the link but we should block gomezjennifer@gmail.com from the network to prevent her from sending that malicious link

On February 15th at 5:24 PM I discovered that aturner@securetech.com at ip address 10.10.2.154 received an email from david55@hotmail.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn’t open the link but we should block david55@hotmail.com from the network to prevent her from sending that malicious link

On February 15th at 5:32 PM I discovered that swatson@securetech.com at ip address 10.10.1.185 received an email from hilljesse@jordan-ortiz.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn’t open the link but we should block hilljesse@jordan-ortiz.com from the network to prevent her from sending that malicious link

On February 15th at 5:43 PM I discovered that storres@securetech.com at ip address 10.10.2.132 received an email from julie70@hotmail.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn’t open the link but we should block julie70@hotmail.com from the network to prevent her from sending that malicious link

On February 15th at 6:02 PM I discovered that ksanders@securetech.com at ip address 10.10.0.14 received an email from anthonycooper@lang.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn’t open the link but we should block anthonycooper@lang.com from the network to prevent her from sending that malicious link

On February 15th at 6:12 PM I discovered that tcooper@securetech.com at ip address 10.10.2.115 received an email from davistravis@larson.com which included the malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, since there was no GET message it means that user didn’t open the link but we should block davistravis@larson.com from the network to prevent her from sending that malicious link

On February 15th at 6:42 PM I discovered that 20 emails that were outside the securetech domain had send that malicious malicious phishing link or website of srv-61.kim.johnson.biz at the IP address 23.74.164.69, to other securetech users in the website, which incidates that jrobinson@secretech.com wasn’t the only infected email, other infected emails outside the domain sent that phishing email, since jrobinson@securetech.com accessed the website before everyone else did and his account was compromised by the attacker and must have found all the list of people in a company wrote their emails and printed their list of emails in a separate document and then the attacker used his personal email to send that email list to other attackers or other emails who opened that link and gave the link information like jrobinson@securetech.com did which caused their accounts to be compromised like jrobinson@securetech.com

On February 15th at 9:00 PM, I discovered that the service record of the malicious website as srv-61, which is a service record numbered at 61, the website and server the website is on is part of a service record, so we will look at the other websites with srv-61 in the url. Besides srv-61.kim.johnson.biz there are other websites srv-61.torres.walker.com, srv-61.sullivan-myers.andrade.com, srv-61.salinas-williams.terry.com, srv-61.fry.reyes.biz, srv-61.gill.reed-anderson.biz, all of these website share the same service record as the malicious phishing link which incidates they are could include phishing links and are owned by the attacker.All those websites are apart of the same server and domain service or DNS server

On February 16th at 9:00 AM, I discovered that cli@securetech with the IP address 10.10.1.175 accessed the other website of srv-61.torres.walker.com with the service record of 61, which is a part of the malicious website sent in the phishing email. He just connected to the website

On February 16th at 9:04 AM, I discovered that cfranklin@securetech.com with IP address of 10.10.0.166, accessed the other website of srv-61.sullivan-myers.andrade.com with the service record of 61 which is a part off the domain of malicious website sent in the phishing email. He added something to the website based on the patch method, which showed that his account could be in danger given he added something to a malicous website

On February 16th at 9:08 AM, I discovered that jflores@securetech.com with ip address of 10.10.1.146 accessed the other website of srv-61.salinas-williams.terry.com which is af the domain of malicious website sent in the phishing email. He performed a loop back test along its path, and was able to see all information which incidates he was testing something on the website to see if it works based on the trace method, he did it at a malicious domain server which indicates his account could be in danger

On February 16th at 9:12 AM, I discovered that eclark@securetech.com with the IP address of 10.10.1.134 accessed the other website of srv-61.fry.reyes.biz which is a part of the domain of malicious website sent in the phishing email. He performed a loop back test along its path, and was able to see all information which incidates he was testing something on the website to see if it works based on the trace method, he did it at a malicious domain server which indicates his account could be in danger

On February 16th at 9:16 AM, I discovered that dpotter@securetech.com with the IP address of 10.10.1.249 accessed the other website of srv-61.gill.reed-anderson.biz which is a part of the domain of malicious website sent in the phishing email. Hr then accessed the website based on the GET message

On February 16th at 10:22 AM, that many of the users who installed or added wordpress plugins and other information to a various amounts of different websites before and after jrobinson@securetech.com account was compromised which indicates its may not be malicious and is part of usual operations the company is trying to do by providing them security services to their websites

On February 16th at 10:25 AM, cfranklin@securetech.com opened up srv-61.sullivan-myers.andrade.com but he never received that phishing email from jrobinson@securetech.com, nor did he send any emails to other internal users but we should change his credentials just in case if his account gets compromised

On February 16th at 10:28 AM, jflores@securetech.com opened up srv-61.salinas-williams.terry.com but he never received that phishing email from jrobinson@securetech.com nor didnt send any emails to other internal users but we should change his credentials just in case if his account gets compromised

On February 16th at 10:31 AM, eclark@securetech.com opened up srv-61.fry.reyes.biz but he never received that phishing email from jrobinson@securetech.com nor didnt send any emails to other internal users but we should change his credentials just in case if his account gets compromised

On February 16th at 10:33 AM, dpotter@securetech.com opened up srv-61.gill.reed-anderson.biz but he did however receive that phishing email from jrobinson@securetech.com but he didnt open that email due to a lack of a GET message

On Febuary 16th at 10:40 AM, I discovered that jrobinson@securetech.com was compromised because he used the same password for another account and because of that the attacker was able to use that password and log in to his account and compromise it

On Febuary 16th at 10:55 AM, I discovered that the TRACE method was used when the user was performing a test or diagnostic on the website

On Febuary 16th at 11:23 AM, I discovered that the email that was sent to jrobinson@securetech.com came from carrie64@ford.com because the ip address from which the message came from was 23.74.164.69 which is the same ip address of the malicious website of srv-61.kim.johnson.biz , the attacker's email was carrie64@ford.com, he only sent out that email once based on the mail logs