<hunter_strategy>

Email Header Analysis: Return-Path to the Future

Jake Williams, VP R&D
Jake.Williams@hunterstrategy.net

Agenda

SPF and DKIM

Email Header Analysis

Email Header Analysis

In the next several slides, we'll discuss various email headers from a scam message

```
Delivered-To: notarealusername@victimorg.com
Received: by 2002:a26:4e43:0:0:0:0:0 with SMTP id c64csp410928yab;
        Tue, 9 Feb 2021 08:57:16 -0800 (PST)
X-Google-Smtp-Source: ABdhPJz9k0H
+z9NnXzpmNoLmyPlI8hJtZ8Udi52s8242h/aGGUZY734rZP4i2gex4eW8d5o7i2Op
X-Received: by 2002:a05:6402:7ce:: with SMTP id u14mr19495111edy.370.1612889835854;
        Tue, 09 Feb 2021 08:57:15 -0800 (PST)
ARC-Seal: i=1; a=rsa-sha256; t=1612889835; cv=none;
        d=google.com; s=arc-20160816;
        b=txqdrwKnEzj0/q/tz778am4C5ZDWwq7hpx+5EbOF/u9b8zJm7+yGSAPOiGJcq3FAqd
         0W14BwWinNZHcUif32f8hfxcfzvjaL+ZCVHbSkQErWoEm7fMfqJHNuMim++ZdQ0S5WZt
         ZqexxAoRX0cFUb+kjOQh0O/Z5k4XZ7CjlR2XcpqDspLX/RVQZE3GQtSj/1Dsf0OWYteG
         oCqZPPqXUG/kpSH1MisH5juW/M/g1twdVA5NU+KWdpbbJt/LyL6hZbQtuFSocOovNdk4
         Vi9dFOO81mi71+XzwEV/XJIZwr2k/S9gs4u7UMAwFcWBV/GeqaSOZ3mpxNMTFDxJFe8S
         fzXw==
```

Continuing our analysis

```
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@odhtoqjf.ga header.s=default header.b=fw4lFny1;
       spf=temperror (google.com: error in processing during lookup of
return.ydo3qzn5gdoy0ynxqdn00ymzgdmzitmwqzm@odhtoqjf.ga: DNS error)
smtp.mailfrom=return.YDO3QzN5gDOy0yNxQDN00yMzgDMzITMwQzM@odhtoqjf.ga
Return-Path: <return.YDO3QzN5gDOy0yNxQDN00yMzgDMzITMwQzM@odhtoqjf.ga>
Received: from 2602fed273000548103ecee700000001.odhtoqjf.ga
(2602fed273000548103ecee700000001.odhtoqjf.ga. [2602:fed2:7300:548:103e:cee7:0:1])
        by mx.google.com with ESMTPS id 63si4656801ede.541.2021.02.09.08.57.14
        for <notarealusername@victimorg.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 09 Feb 2021 08:57:15 -0800 (PST)
Received-SPF: temperror (google.com: error in processing during lookup of
return.ydo3qzn5gdoy0ynxqdn00ymzgdmzitmwqzm@odhtoqjf.ga: DNS error) client-
ip=2602:fed2:7300:548:103e:cee7:0:1;
```

Can we trust the date field wasn't forged?

```
Authentication-Results: mx.google.com;
       dkim=pass header.i=@odhtoqjf.ga header.s=default header.b=fw4lFny1;
       spf=temperror (google.com: error in processing during lookup of
return.ydo3qzn5gdoy0ynxqdn00ymzgdmzitmwqzm@odhtoqjf.ga: DNS error)
smtp.mailfrom=return.YDO3QzN5gDOy0yNxQDN00yMzgDMzITMwQzM@odhtoqjf.ga
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=odhtoqjf.ga;
 q=dns/txt; s=default; bh=D5BJfsJKqFOUjjcRBBtCkZluzfiL+wmJ4rvTXOZq/II=;
 h=from:subject:to:mime-version:content-type:content-transfer-encoding;
 b=fw4lFny1GEzZgCXkphsjIvAFHjgccvAEu269zNh+T4Adotguo2oDkjxyHMaRX1BRXmJwGkEzlSUg
 MJ0N7bbDB2Im0Mp01J+jzgTIh4wqAD3wpc9DpN/A/r+vTW/4ua7SjQMSnQ+lK64hew+uaDSim3cF
 vvunyVGuBuB51P5zZaU=
Date: Tue, 09 Feb 2021 16:27:34 GMT
```

Can we trust the subject field wasn't forged?

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=odhtoqjf.ga;
 q=dns/txt; s=default; bh=D5BJfsJKqFOUjjcRBBtCkZluzfiL+wmJ4rvTXOZq/II=;
 h=from:subject:to:mime-version:content-type:content-transfer-encoding;
 b=fw4lFny1GEzZgCXkphsjIvAFHjgccvAEu269zNh+T4Adotguo2oDkjxyHMaRX1BRXmJwGkEzlSUg
 MJ0N7bbDB2Im0Mp01J+jzgTIh4wqAD3wpc9DpN/A/r+vTW/4ua7SjQMSnQ+lK64hew+uaDSim3cF
 vvunyVGuBuB51P5zZaU=
Date: Tue, 09 Feb 2021 16:27:34 GMT
Return-Path: return.YDO3QzN5gDOy0yNxQDN00yMzgDMzITMwQzM@3o9qm0ohqa16u1.r103e-cee7.odhtoqjf.ga
Errors-To: return.YDO3QzN5gDOy0yNxQDN00yMzgDMzITMwQzM@3o9qm0ohqa16u1.r103e-cee7.odhtoqjf.ga
Message-Id: <d68aae1650e17d0c5aa6c48691ff14@odhtoqjf.ga>
From: "Accounts Receivable" <ehm44417@l44417.odhtoqjf.ga>
To: notarealusername@victimorg.com
Subject: Please Update Banking Information
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: quoted-printable
MIME-Version: 1.0
```

Sender Policy Framework: SPF

SPF provides a way for receiving email servers to determine if an email came from a legitimate source IP address

- Before SPF, the receiving email server had simply trust that the headers (including the claimed sender) on an email were legitimate

SPF can be complicated to configure, especially when third-parties (such as a CRM) may send email on your behalf

SPF entries are stored in DNS, but SPF implements a limit such that a maximum of 10 DNS records may be required to retrieve the full list of authorized senders

Sender Policy Framework: SPF (2)

Consider this sample SPF header:

- The Received header shows the IP address of the sending server
- The Received-SPF header shows that **at the time the email was received**, 192.28.144.201 was a valid sender in SPF
- ESMTPS in the Received header also says the message was transmitted using encryption (recall that SMTP defaults to plaintext)

```
Return-Path: <113-DTN-266.0.1211.0.0.3163.9.6218200@info.digitalocean.com>
Received: from info.digitalocean.com (info.digitalocean.com. [192.28.144.201])
        by mx.google.com with ESMTPS id o27si4208675qtl.354.2021.02.09.12.40.06
        for <cehtrump@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 09 Feb 2021 12:40:06 -0800 (PST)
Received-SPF: pass (google.com: domain of 113-dtn-
266.0.1211.0.0.3163.9.6218200@info.digitalocean.com designates 192.28.144.201 as
permitted sender) client-ip=192.28.144.201;
```

DomainKeys Identified Mail (DKIM)

DKIM digitally signs outgoing email, including some headers and possibly the message body, as it leaves the origination server

The receiving server reads the DKIM signature, obtains the public key via DNS, and calculates a signature

- If the signatures do not match, the receiving server knows that the email has been modified in transit

In BEC, DKIM is an excellent tool for establishing nonrepudiation

- If the DKIM signature is intact, fields included in the signature were not modified by an attacker

DomainKeys Identified Mail (2)

DKIM has a few issues that you should be aware of:

- The public key is retrieved by DNS and if DNSSEC is not configured for the sender's domain or enforced by the receiving server, DNS spoofing could trick the receiver into validating a DKIM signature using an attacker-controlled key
- DKIM signatures do not encompass all header, destination headers are often cited as a concern
- DKIM signatures may not include a hash of the entire message body, possibly including the attachments
- Unicode conversions of headers may invalidate signatures
- Weak keys can be factored and abused

DomainKeys Identified Mail (3)

Consider the following DKIM signature example:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=customer.box.com;
    s=scph0717; t=1612282502; i=@customer.box.com;
    bh=kz396TsXaSIWe2W5NmC8V7QAk4XSfzWBB3bZY/fOr1o=;
    h=To:Message-ID:Date:Content-Type:Subject:From;
    b=gza5ugueSmyvnGvZCJIMYa0HS8iGRmD9p8xOkMUsbM9ep1EEUhbov339ef+XZ0cg7
     91msefUNey9CDPzBAag6RKtGgy7ZQ0wGV5+5WXKs0rl+2fK0IXk/h0TUbBiMuJFMsv
     YEB4Cbu0HpirntTJxkGr5Wy8QthoAc6/H5GY0L4E=
```

To view the public key, use dig:

- `dig TXT scph0717._domainkey.customer.box.com`

```
;; ANSWER SECTION:
scph0717._domainkey.customer.box.com. 0 IN TXT  "v=DKIM1; h=sha256; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
9hYBcD3OXbA3FpQKGjbqJXGHoguyQmZYcydd9zf9uQJN4hLtmwzKKq8eEzxwk4kdJ0VxrfjmkhecWFs3dH003JXF0sHCVIselTyG9RoWnh
```