Initial mail:

Feb 06 21:08:15 mailserver postfix/smtpd[5036]: 23442EA146: client=unknown[23.74.164.69]

Feb 06 21:08:15 mailserver postfix/qmgr[5036]: 23442EA146: from=<carrie64@ford.com>, size=5760, nrcpt=1 (queue active)

Feb 06 21:08:15 mailserver postfix/local[5036]: 23442EA146: to=<jrobinson@securetech.com>, relay=local, delay=0.10, delays=0.10/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

**Attacker IP: 23.74.164.69 (**carrie64@ford.com)

Phishing email script send to 79 users

Feb 07 02:06:16 mailserver postfix/qmgr[21627]: DFEB35441B: from=<jrobinson@securetech.com>, size=6672, nrcpt=1 (queue active)

Feb 07 02:06:18 mailserver postfix/qmgr[15685]: A687131E8E: from=<jrobinson@securetech.com>, size=5404, nrcpt=1 (queue active)

Feb 07 02:06:20 mailserver postfix/qmgr[17442]: D942F49FFA: from=<jrobinson@securetech.com>, size=2492, nrcpt=1 (queue active)

Feb 07 02:06:21 mailserver postfix/qmgr[11023]: EA8B8E1B10: from=<jrobinson@securetech.com>, size=8456, nrcpt=1 (queue active)

Feb 07 02:06:25 mailserver postfix/qmgr[25614]: BA4FD9B9DE: from=<jrobinson@securetech.com>, size=9803, nrcpt=1 (queue active)

Feb 07 02:06:28 mailserver postfix/qmgr[2716]: 5A43CD855A: from=<jrobinson@securetech.com>, size=5706, nrcpt=1 (queue active)

Feb 07 02:06:30 mailserver postfix/qmgr[16227]: CA96A59E45: from=<jrobinson@securetech.com>, size=4240, nrcpt=1 (queue active)

Feb 07 02:06:32 mailserver postfix/qmgr[12692]: A33DA748C3: from=<jrobinson@securetech.com>, size=8430, nrcpt=1 (queue active)

Feb 07 02:06:33 mailserver postfix/qmgr[11182]: 450B5FC336: from=<jrobinson@securetech.com>, size=8122, nrcpt=1 (queue active)

Feb 07 02:06:34 mailserver postfix/qmgr[11518]: 94D0983173: from=<jrobinson@securetech.com>, size=8614, nrcpt=1 (queue active)

Feb 07 02:06:35 mailserver postfix/qmgr[14589]: AE0FEF8967: from=<jrobinson@securetech.com>, size=3138, nrcpt=1 (queue active)

Feb 07 02:06:38 mailserver postfix/qmgr[7458]: 141813315A: from=<jrobinson@securetech.com>, size=7331, nrcpt=1 (queue active)

Feb 07 02:06:42 mailserver postfix/qmgr[8989]: 6E6524348A: from=<jrobinson@securetech.com>, size=5189, nrcpt=1 (queue active)

Feb 07 02:06:46 mailserver postfix/qmgr[14050]: 7CA27F5114: from=<jrobinson@securetech.com>, size=9028, nrcpt=1 (queue active)

Feb 07 02:06:50 mailserver postfix/qmgr[9443]: 23B02259A5: from=<jrobinson@securetech.com>, size=4405, nrcpt=1 (queue active)

Feb 07 02:06:55 mailserver postfix/qmgr[17158]: B4D54CCC8A: from=<jrobinson@securetech.com>, size=7630, nrcpt=1 (queue active)

Feb 07 02:06:59 mailserver postfix/qmgr[19321]: 6369214491: from=<jrobinson@securetech.com>, size=3756, nrcpt=1 (queue active)

Feb 07 02:07:02 mailserver postfix/qmgr[24499]: FAF29736AE: from=<jrobinson@securetech.com>, size=4627, nrcpt=1 (queue active)

Feb 07 02:07:03 mailserver postfix/qmgr[26581]: 85AD72D5B5: from=<jrobinson@securetech.com>, size=8186, nrcpt=1 (queue active)

Feb 07 02:07:05 mailserver postfix/qmgr[21722]: 4071CD7AC5: from=<jrobinson@securetech.com>, size=6845, nrcpt=1 (queue active)

Feb 07 02:07:06 mailserver postfix/qmgr[25856]: 54C1F6C74D: from=<jrobinson@securetech.com>, size=2524, nrcpt=1 (queue active)

Feb 07 02:07:09 mailserver postfix/qmgr[8663]: F59E06E940: from=<jrobinson@securetech.com>, size=3553, nrcpt=1 (queue active)

Feb 07 02:07:12 mailserver postfix/qmgr[2249]: DAF7EBC967: from=<jrobinson@securetech.com>, size=3226, nrcpt=1 (queue active)

Feb 07 02:07:16 mailserver postfix/qmgr[19500]: EBECBEC8EB: from=<jrobinson@securetech.com>, size=2841, nrcpt=1 (queue active)

Feb 07 02:07:18 mailserver postfix/qmgr[24724]: EE3E10309E: from=<jrobinson@securetech.com>, size=5016, nrcpt=1 (queue active)

Feb 07 02:07:20 mailserver postfix/qmgr[12089]: 28C9C0D408: from=<jrobinson@securetech.com>, size=4705, nrcpt=1 (queue active)

Feb 07 02:07:21 mailserver postfix/qmgr[13455]: FF4A179235: from=<jrobinson@securetech.com>, size=5559, nrcpt=1 (queue active)

Feb 07 02:07:22 mailserver postfix/qmgr[1733]: 0712554DC9: from=<jrobinson@securetech.com>, size=3547, nrcpt=1 (queue active)

Feb 07 02:07:27 mailserver postfix/qmgr[8011]: 13DA46B698: from=<jrobinson@securetech.com>, size=4842, nrcpt=1 (queue active)

Feb 07 02:07:32 mailserver postfix/qmgr[13941]: 8AD1E258ED: from=<jrobinson@securetech.com>, size=7050, nrcpt=1 (queue active)

Feb 07 02:07:37 mailserver postfix/qmgr[6522]: 20FE0DCA66: from=<jrobinson@securetech.com>, size=8743, nrcpt=1 (queue active)

Feb 07 02:07:38 mailserver postfix/qmgr[27130]: 6BFAD0B13C: from=<jrobinson@securetech.com>, size=9901, nrcpt=1 (queue active)

Feb 07 02:07:40 mailserver postfix/qmgr[20294]: 8A6BFAB4BE: from=<jrobinson@securetech.com>, size=4662, nrcpt=1 (queue active)

Feb 07 02:07:42 mailserver postfix/qmgr[4476]: 2F2FEB6682: from=<jrobinson@securetech.com>, size=2411, nrcpt=1 (queue active)

Feb 07 02:07:43 mailserver postfix/qmgr[9636]: C5830FA296: from=<jrobinson@securetech.com>, size=7742, nrcpt=1 (queue active)

Feb 07 02:07:45 mailserver postfix/qmgr[8941]: DFA4627685: from=<jrobinson@securetech.com>, size=3061, nrcpt=1 (queue active)

Feb 07 02:07:48 mailserver postfix/qmgr[15965]: 8A340A8A35: from=<jrobinson@securetech.com>, size=9560, nrcpt=1 (queue active)

Feb 07 02:07:52 mailserver postfix/qmgr[25346]: 3798B86689: from=<jrobinson@securetech.com>, size=8285, nrcpt=1 (queue active)

Feb 07 02:07:55 mailserver postfix/qmgr[16611]: 711700BCA4: from=<jrobinson@securetech.com>, size=4570, nrcpt=1 (queue active)

Feb 07 02:07:56 mailserver postfix/qmgr[4542]: E733448081: from=<jrobinson@securetech.com>, size=2303, nrcpt=1 (queue active)

Feb 07 02:07:57 mailserver postfix/qmgr[12621]: 7C06072EB8: from=<jrobinson@securetech.com>, size=6799, nrcpt=1 (queue active)

Feb 07 02:08:01 mailserver postfix/qmgr[13337]: E0D6B2B963: from=<jrobinson@securetech.com>, size=8196, nrcpt=1 (queue active)

Feb 07 02:08:03 mailserver postfix/qmgr[26975]: 80B309078E: from=<jrobinson@securetech.com>, size=6415, nrcpt=1 (queue active)

Feb 07 02:08:08 mailserver postfix/qmgr[14512]: 89D4280DA8: from=<jrobinson@securetech.com>, size=3317, nrcpt=1 (queue active)

Feb 07 02:08:10 mailserver postfix/qmgr[18307]: 1127283AD5: from=<jrobinson@securetech.com>, size=6669, nrcpt=1 (queue active)

Feb 07 02:08:12 mailserver postfix/qmgr[7039]: C445EAF254: from=<jrobinson@securetech.com>, size=2301, nrcpt=1 (queue active)

Feb 07 02:08:16 mailserver postfix/qmgr[5787]: 8BF86F6846: from=<jrobinson@securetech.com>, size=5722, nrcpt=1 (queue active)

Feb 07 02:08:19 mailserver postfix/qmgr[28955]: 45EB551CF3: from=<jrobinson@securetech.com>, size=7404, nrcpt=1 (queue active)

Feb 07 02:08:21 mailserver postfix/qmgr[25684]: CD2A45639A: from=<jrobinson@securetech.com>, size=8678, nrcpt=1 (queue active)

Feb 07 02:08:22 mailserver postfix/qmgr[26481]: 5B58648761: from=<jrobinson@securetech.com>, size=2461, nrcpt=1 (queue active)

Feb 07 02:08:27 mailserver postfix/qmgr[17962]: 33B8D37645: from=<jrobinson@securetech.com>, size=9309, nrcpt=1 (queue active)

Feb 07 02:08:30 mailserver postfix/qmgr[9097]: 1099BE936F: from=<jrobinson@securetech.com>, size=9474, nrcpt=1 (queue active)

Feb 07 02:08:32 mailserver postfix/qmgr[18640]: 5624844B1D: from=<jrobinson@securetech.com>, size=8306, nrcpt=1 (queue active)

Feb 07 02:08:34 mailserver postfix/qmgr[27472]: CA9CBE79B7: from=<jrobinson@securetech.com>, size=6623, nrcpt=1 (queue active)

Feb 07 02:08:35 mailserver postfix/qmgr[20740]: 99C658717F: from=<jrobinson@securetech.com>, size=3566, nrcpt=1 (queue active)

Feb 07 02:08:39 mailserver postfix/qmgr[6060]: 5615E3D507: from=<jrobinson@securetech.com>, size=3924, nrcpt=1 (queue active)

Feb 07 02:08:41 mailserver postfix/qmgr[14231]: 0D50AF6F6A: from=<jrobinson@securetech.com>, size=3069, nrcpt=1 (queue active)

Feb 07 02:08:44 mailserver postfix/qmgr[16802]: D2225D61B6: from=<jrobinson@securetech.com>, size=9940, nrcpt=1 (queue active)

Feb 07 02:08:46 mailserver postfix/qmgr[9415]: 8243945A9A: from=<jrobinson@securetech.com>, size=8335, nrcpt=1 (queue active)

Feb 07 02:08:48 mailserver postfix/qmgr[28011]: B182A60497: from=<jrobinson@securetech.com>, size=2348, nrcpt=1 (queue active)

Feb 07 02:08:52 mailserver postfix/qmgr[2060]: 85E1329C5C: from=<jrobinson@securetech.com>, size=8158, nrcpt=1 (queue active)

Feb 07 02:08:56 mailserver postfix/qmgr[14310]: 7A599A2786: from=<jrobinson@securetech.com>, size=3890, nrcpt=1 (queue active)

Feb 07 02:08:59 mailserver postfix/qmgr[8729]: 5F587A7632: from=<jrobinson@securetech.com>, size=7480, nrcpt=1 (queue active)

Feb 07 02:09:02 mailserver postfix/qmgr[20549]: 5DA834FDA1: from=<jrobinson@securetech.com>, size=2948, nrcpt=1 (queue active)

Feb 07 02:09:05 mailserver postfix/qmgr[6622]: 586F30B049: from=<jrobinson@securetech.com>, size=3869, nrcpt=1 (queue active)

Feb 07 02:09:10 mailserver postfix/qmgr[17724]: 7DBE9EA448: from=<jrobinson@securetech.com>, size=2169, nrcpt=1 (queue active)

Feb 07 02:09:14 mailserver postfix/qmgr[17290]: F8E0BB92B9: from=<jrobinson@securetech.com>, size=8493, nrcpt=1 (queue active)

Feb 07 02:09:16 mailserver postfix/qmgr[12663]: C7023D220C: from=<jrobinson@securetech.com>, size=7670, nrcpt=1 (queue active)

Feb 07 02:09:21 mailserver postfix/qmgr[10324]: 83D31FB900: from=<jrobinson@securetech.com>, size=6450, nrcpt=1 (queue active)

Feb 07 02:09:25 mailserver postfix/qmgr[16527]: 02A15B3F56: from=<jrobinson@securetech.com>, size=7964, nrcpt=1 (queue active)

Feb 07 02:09:29 mailserver postfix/qmgr[11525]: 93C2343223: from=<jrobinson@securetech.com>, size=6904, nrcpt=1 (queue active)

Feb 07 02:09:34 mailserver postfix/qmgr[5769]: F29EB22E09: from=<jrobinson@securetech.com>, size=6435, nrcpt=1 (queue active)

Feb 07 02:09:39 mailserver postfix/qmgr[26389]: 767AB29E9A: from=<jrobinson@securetech.com>, size=5542, nrcpt=1 (queue active)

Feb 07 02:09:43 mailserver postfix/qmgr[16893]: 49D3483C91: from=<jrobinson@securetech.com>, size=7047, nrcpt=1 (queue active)

Feb 07 02:09:48 mailserver postfix/qmgr[11020]: EF1E919841: from=<jrobinson@securetech.com>, size=6986, nrcpt=1 (queue active)

Feb 07 02:09:49 mailserver postfix/qmgr[24439]: 5D6E13F092: from=<jrobinson@securetech.com>, size=6871, nrcpt=1 (queue active)

Feb 07 02:09:52 mailserver postfix/qmgr[4075]: 1DC7EF4C11: from=<jrobinson@securetech.com>, size=6052, nrcpt=1 (queue active)

Feb 07 02:09:55 mailserver postfix/qmgr[9408]: 90DB80284A: from=<jrobinson@securetech.com>, size=5390, nrcpt=1 (queue active)

Feb 07 02:09:58 mailserver postfix/qmgr[17892]: CEB497FB89: from=<jrobinson@securetech.com>, size=4089, nrcpt=1 (queue active)

Feb 07 02:10:01 mailserver postfix/qmgr[4131]: 5C0CBCEF3E: from=<jrobinson@securetech.com>, size=8870, nrcpt=1 (queue active)

Feb 07 02:10:03 mailserver postfix/qmgr[8110]: A9069ED1C9: from=<jrobinson@securetech.com>, size=6043, nrcpt=1 (queue active)

On **February 7, 2025**, the SecureTech SOC received a report from an employee, Stephanie Morgan, who identified a suspicious email containing a phishing link originating from an internal address: jrobinson@securetech.com.

Upon investigation of the mail logs, it was discovered that between **02:06:16 and 02:10:03**, **over 79 phishing emails** were sent from Jason Robinson’s account to various internal recipients. Each message included a link to an external domain (srv-61.kim.johnson.biz) designed to impersonate a login page.

The mail logs confirmed the messages were sent from within the organization's mail server (relay=local), but notably, the connection was initiated by an **external IP address (23.74.164.69)**, strongly indicating that **Jason’s credentials were compromised** and accessed externally.

Recipients of the phishing campaign included internal users such as jwhite@securetech.com, with additional affected users being identified through ongoing log correlation.

**Sessions log of 79 user with their email who recived the email**

For DFEB35441B:

Feb 07 02:06:16 mailserver postfix/smtpd[21627]: DFEB35441B: client=unknown[23.74.164.69]

Feb 07 02:06:16 mailserver postfix/qmgr[21627]: DFEB35441B: from=<jrobinson@securetech.com>, size=6672, nrcpt=1 (queue active)

Feb 07 02:06:16 mailserver postfix/local[21627]: DFEB35441B: to=<jwhite@securetech.com>, relay=local, delay=0.49, delays=0.49/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

For A687131E8E:

Feb 07 02:06:18 mailserver postfix/smtpd[15685]: A687131E8E: client=unknown[23.74.164.69]

Feb 07 02:06:18 mailserver postfix/qmgr[15685]: A687131E8E: from=<jrobinson@securetech.com>, size=5404, nrcpt=1 (queue active)

Feb 07 02:06:18 mailserver postfix/local[15685]: A687131E8E: to=<dking@securetech.com>, relay=local, delay=0.48, delays=0.48/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

D942F49FFA

Feb 07 02:06:20 mailserver postfix/smtpd[17442]: D942F49FFA: client=unknown[23.74.164.69]

Feb 07 02:06:20 mailserver postfix/qmgr[17442]: D942F49FFA: from=<jrobinson@securetech.com>, size=2492, nrcpt=1 (queue active)

Feb 07 02:06:20 mailserver postfix/local[17442]: D942F49FFA: to=<aroman@securetech.com>, relay=local, delay=0.92, delays=0.92/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

EA8B8E1B10

Feb 07 02:06:21 mailserver postfix/smtpd[11023]: EA8B8E1B10: client=unknown[23.74.164.69]

Feb 07 02:06:21 mailserver postfix/qmgr[11023]: EA8B8E1B10: from=<jrobinson@securetech.com>, size=8456, nrcpt=1 (queue active)

Feb 07 02:06:21 mailserver postfix/local[11023]: EA8B8E1B10: to=<ncardenas@securetech.com>, relay=local, delay=0.11, delays=0.11/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

BA4FD9B9DE

Feb 07 02:06:25 mailserver postfix/smtpd[25614]: BA4FD9B9DE: client=unknown[23.74.164.69]

Feb 07 02:06:25 mailserver postfix/qmgr[25614]: BA4FD9B9DE: from=<jrobinson@securetech.com>, size=9803, nrcpt=1 (queue active)

Feb 07 02:06:25 mailserver postfix/local[25614]: BA4FD9B9DE: to=<bmccall@securetech.com>, relay=local, delay=0.83, delays=0.83/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

5A43CD855A

Feb 07 02:06:28 mailserver postfix/smtpd[2716]: 5A43CD855A: client=unknown[23.74.164.69]

Feb 07 02:06:28 mailserver postfix/qmgr[2716]: 5A43CD855A: from=<jrobinson@securetech.com>, size=5706, nrcpt=1 (queue active)

Feb 07 02:06:28 mailserver postfix/local[2716]: 5A43CD855A: to=<mbutler@securetech.com>, relay=local, delay=0.18, delays=0.18/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

CA96A59E45

Feb 07 02:06:30 mailserver postfix/smtpd[16227]: CA96A59E45: client=unknown[23.74.164.69]

Feb 07 02:06:30 mailserver postfix/qmgr[16227]: CA96A59E45: from=<jrobinson@securetech.com>, size=4240, nrcpt=1 (queue active)

Feb 07 02:06:30 mailserver postfix/local[16227]: CA96A59E45: to=<rmoses@securetech.com>, relay=local, delay=0.95, delays=0.95/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

A33DA748C3

Feb 07 02:06:32 mailserver postfix/smtpd[12692]: A33DA748C3: client=unknown[23.74.164.69]

Feb 07 02:06:32 mailserver postfix/qmgr[12692]: A33DA748C3: from=<jrobinson@securetech.com>, size=8430, nrcpt=1 (queue active)

Feb 07 02:06:32 mailserver postfix/local[12692]: A33DA748C3: to=<thiggins@securetech.com>, relay=local, delay=0.19, delays=0.19/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

450B5FC336

Feb 07 02:06:33 mailserver postfix/smtpd[11182]: 450B5FC336: client=unknown[23.74.164.69]

Feb 07 02:06:33 mailserver postfix/qmgr[11182]: 450B5FC336: from=<jrobinson@securetech.com>, size=8122, nrcpt=1 (queue active)

Feb 07 02:06:33 mailserver postfix/local[11182]: 450B5FC336: to=<abaxter@securetech.com>, relay=local, delay=0.89, delays=0.89/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

94D0983173

Feb 07 02:06:34 mailserver postfix/smtpd[11518]: 94D0983173: client=unknown[23.74.164.69]

Feb 07 02:06:34 mailserver postfix/qmgr[11518]: 94D0983173: from=<jrobinson@securetech.com>, size=8614, nrcpt=1 (queue active)

Feb 07 02:06:34 mailserver postfix/local[11518]: 94D0983173: to=<djordan@securetech.com>, relay=local, delay=0.40, delays=0.40/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

AE0FEF8967

Feb 07 02:06:35 mailserver postfix/smtpd[14589]: AE0FEF8967: client=unknown[23.74.164.69]

Feb 07 02:06:35 mailserver postfix/qmgr[14589]: AE0FEF8967: from=<jrobinson@securetech.com>, size=3138, nrcpt=1 (queue active)

Feb 07 02:06:35 mailserver postfix/local[14589]: AE0FEF8967: to=<mmichael@securetech.com>, relay=local, delay=0.21, delays=0.21/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

141813315A

Feb 07 02:06:38 mailserver postfix/smtpd[7458]: 141813315A: client=unknown[23.74.164.69]

Feb 07 02:06:38 mailserver postfix/qmgr[7458]: 141813315A: from=<jrobinson@securetech.com>, size=7331, nrcpt=1 (queue active)

Feb 07 02:06:38 mailserver postfix/local[7458]: 141813315A: to=<aharrell@securetech.com>, relay=local, delay=0.13, delays=0.13/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

6E6524348A

Feb 07 02:06:42 mailserver postfix/smtpd[8989]: 6E6524348A: client=unknown[23.74.164.69]

Feb 07 02:06:42 mailserver postfix/qmgr[8989]: 6E6524348A: from=<jrobinson@securetech.com>, size=5189, nrcpt=1 (queue active)

Feb 07 02:06:42 mailserver postfix/local[8989]: 6E6524348A: to=<bbarron@securetech.com>, relay=local, delay=0.68, delays=0.68/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

7CA27F5114

Feb 07 02:06:46 mailserver postfix/smtpd[14050]: 7CA27F5114: client=unknown[23.74.164.69]

Feb 07 02:06:46 mailserver postfix/qmgr[14050]: 7CA27F5114: from=<jrobinson@securetech.com>, size=9028, nrcpt=1 (queue active)

Feb 07 02:06:46 mailserver postfix/local[14050]: 7CA27F5114: to=<rgardner@securetech.com>, relay=local, delay=0.29, delays=0.29/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

23B02259A5

Feb 07 02:06:50 mailserver postfix/smtpd[9443]: 23B02259A5: client=unknown[23.74.164.69]

Feb 07 02:06:50 mailserver postfix/qmgr[9443]: 23B02259A5: from=<jrobinson@securetech.com>, size=4405, nrcpt=1 (queue active)

Feb 07 02:06:50 mailserver postfix/local[9443]: 23B02259A5: to=<jbarber@securetech.com>, relay=local, delay=0.12, delays=0.12/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

B4D54CCC8A

Feb 07 02:06:55 mailserver postfix/smtpd[17158]: B4D54CCC8A: client=unknown[23.74.164.69]

Feb 07 02:06:55 mailserver postfix/qmgr[17158]: B4D54CCC8A: from=<jrobinson@securetech.com>, size=7630, nrcpt=1 (queue active)

Feb 07 02:06:55 mailserver postfix/local[17158]: B4D54CCC8A: to=<lsmith@securetech.com>, relay=local, delay=0.36, delays=0.36/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

6369214491

Feb 07 02:06:59 mailserver postfix/smtpd[19321]: 6369214491: client=unknown[23.74.164.69]

Feb 07 02:06:59 mailserver postfix/qmgr[19321]: 6369214491: from=<jrobinson@securetech.com>, size=3756, nrcpt=1 (queue active)

Feb 07 02:06:59 mailserver postfix/local[19321]: 6369214491: to=<dcollins@securetech.com>, relay=local, delay=0.07, delays=0.07/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

FAF29736AE

Feb 07 02:07:02 mailserver postfix/smtpd[24499]: FAF29736AE: client=unknown[23.74.164.69]

Feb 07 02:07:02 mailserver postfix/qmgr[24499]: FAF29736AE: from=<jrobinson@securetech.com>, size=4627, nrcpt=1 (queue active)

Feb 07 02:07:02 mailserver postfix/local[24499]: FAF29736AE: to=<mespinoza@securetech.com>, relay=local, delay=0.85, delays=0.85/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

85AD72D5B5

Feb 07 02:07:03 mailserver postfix/smtpd[26581]: 85AD72D5B5: client=unknown[23.74.164.69]

Feb 07 02:07:03 mailserver postfix/qmgr[26581]: 85AD72D5B5: from=<jrobinson@securetech.com>, size=8186, nrcpt=1 (queue active)

Feb 07 02:07:03 mailserver postfix/local[26581]: 85AD72D5B5: to=<akeith@securetech.com>, relay=local, delay=0.11, delays=0.11/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

4071CD7AC5

Feb 07 02:07:05 mailserver postfix/smtpd[21722]: 4071CD7AC5: client=unknown[23.74.164.69]

Feb 07 02:07:05 mailserver postfix/qmgr[21722]: 4071CD7AC5: from=<jrobinson@securetech.com>, size=6845, nrcpt=1 (queue active)

Feb 07 02:07:05 mailserver postfix/local[21722]: 4071CD7AC5: to=<ftravis@securetech.com>, relay=local, delay=0.85, delays=0.85/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

54C1F6C74D

Feb 07 02:07:06 mailserver postfix/smtpd[25856]: 54C1F6C74D: client=unknown[23.74.164.69]

Feb 07 02:07:06 mailserver postfix/qmgr[25856]: 54C1F6C74D: from=<jrobinson@securetech.com>, size=2524, nrcpt=1 (queue active)

Feb 07 02:07:06 mailserver postfix/local[25856]: 54C1F6C74D: to=<dmendoza@securetech.com>, relay=local, delay=0.26, delays=0.26/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

F59E06E940

Feb 07 02:07:09 mailserver postfix/smtpd[8663]: F59E06E940: client=unknown[23.74.164.69]

Feb 07 02:07:09 mailserver postfix/qmgr[8663]: F59E06E940: from=<jrobinson@securetech.com>, size=3553, nrcpt=1 (queue active)

Feb 07 02:07:09 mailserver postfix/local[8663]: F59E06E940: to=<dreed@securetech.com>, relay=local, delay=0.89, delays=0.89/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

DAF7EBC967

Feb 07 02:07:12 mailserver postfix/smtpd[2249]: DAF7EBC967: client=unknown[23.74.164.69]

Feb 07 02:07:12 mailserver postfix/qmgr[2249]: DAF7EBC967: from=<jrobinson@securetech.com>, size=3226, nrcpt=1 (queue active)

Feb 07 02:07:12 mailserver postfix/local[2249]: DAF7EBC967: to=<mjenkins@securetech.com>, relay=local, delay=0.82, delays=0.82/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

EBECBEC8EB

Feb 07 02:07:16 mailserver postfix/smtpd[19500]: EBECBEC8EB: client=unknown[23.74.164.69]

Feb 07 02:07:16 mailserver postfix/qmgr[19500]: EBECBEC8EB: from=<jrobinson@securetech.com>, size=2841, nrcpt=1 (queue active)

Feb 07 02:07:16 mailserver postfix/local[19500]: EBECBEC8EB: to=<jlee@securetech.com>, relay=local, delay=0.96, delays=0.96/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

EE3E10309E

Feb 07 02:07:18 mailserver postfix/smtpd[24724]: EE3E10309E: client=unknown[23.74.164.69]

Feb 07 02:07:18 mailserver postfix/qmgr[24724]: EE3E10309E: from=<jrobinson@securetech.com>, size=5016, nrcpt=1 (queue active)

Feb 07 02:07:18 mailserver postfix/local[24724]: EE3E10309E: to=<vleach@securetech.com>, relay=local, delay=0.87, delays=0.87/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

28C9C0D408

Feb 07 02:07:20 mailserver postfix/smtpd[12089]: 28C9C0D408: client=unknown[23.74.164.69]

Feb 07 02:07:20 mailserver postfix/qmgr[12089]: 28C9C0D408: from=<jrobinson@securetech.com>, size=4705, nrcpt=1 (queue active)

Feb 07 02:07:20 mailserver postfix/local[12089]: 28C9C0D408: to=<tmedina@securetech.com>, relay=local, delay=0.24, delays=0.24/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

FF4A179235

Feb 07 02:07:21 mailserver postfix/smtpd[13455]: FF4A179235: client=unknown[23.74.164.69]

Feb 07 02:07:21 mailserver postfix/qmgr[13455]: FF4A179235: from=<jrobinson@securetech.com>, size=5559, nrcpt=1 (queue active)

Feb 07 02:07:21 mailserver postfix/local[13455]: FF4A179235: to=<jmason@securetech.com>, relay=local, delay=0.02, delays=0.02/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

0712554DC9

Feb 07 02:07:22 mailserver postfix/smtpd[1733]: 0712554DC9: client=unknown[23.74.164.69]

Feb 07 02:07:22 mailserver postfix/qmgr[1733]: 0712554DC9: from=<jrobinson@securetech.com>, size=3547, nrcpt=1 (queue active)

Feb 07 02:07:22 mailserver postfix/local[1733]: 0712554DC9: to=<thoward@securetech.com>, relay=local, delay=0.94, delays=0.94/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

13DA46B698

Feb 07 02:07:27 mailserver postfix/smtpd[8011]: 13DA46B698: client=unknown[23.74.164.69]

Feb 07 02:07:27 mailserver postfix/qmgr[8011]: 13DA46B698: from=<jrobinson@securetech.com>, size=4842, nrcpt=1 (queue active)

Feb 07 02:07:27 mailserver postfix/local[8011]: 13DA46B698: to=<lgreen@securetech.com>, relay=local, delay=0.99, delays=0.99/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

8AD1E258ED

Feb 07 02:07:32 mailserver postfix/smtpd[13941]: 8AD1E258ED: client=unknown[23.74.164.69]

Feb 07 02:07:32 mailserver postfix/qmgr[13941]: 8AD1E258ED: from=<jrobinson@securetech.com>, size=7050, nrcpt=1 (queue active)

Feb 07 02:07:32 mailserver postfix/local[13941]: 8AD1E258ED: to=<jball@securetech.com>, relay=local, delay=0.85, delays=0.85/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

20FE0DCA66

Feb 07 02:07:37 mailserver postfix/smtpd[6522]: 20FE0DCA66: client=unknown[23.74.164.69]

Feb 07 02:07:37 mailserver postfix/qmgr[6522]: 20FE0DCA66: from=<jrobinson@securetech.com>, size=8743, nrcpt=1 (queue active)

Feb 07 02:07:37 mailserver postfix/local[6522]: 20FE0DCA66: to=<sritter@securetech.com>, relay=local, delay=0.04, delays=0.04/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

6BFAD0B13C

Feb 07 02:07:38 mailserver postfix/smtpd[27130]: 6BFAD0B13C: client=unknown[23.74.164.69]

Feb 07 02:07:38 mailserver postfix/qmgr[27130]: 6BFAD0B13C: from=<jrobinson@securetech.com>, size=9901, nrcpt=1 (queue active)

Feb 07 02:07:38 mailserver postfix/local[27130]: 6BFAD0B13C: to=<kgarcia@securetech.com>, relay=local, delay=0.04, delays=0.04/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

8A6BFAB4BE

Feb 07 02:07:40 mailserver postfix/smtpd[20294]: 8A6BFAB4BE: client=unknown[23.74.164.69]

Feb 07 02:07:40 mailserver postfix/qmgr[20294]: 8A6BFAB4BE: from=<jrobinson@securetech.com>, size=4662, nrcpt=1 (queue active)

Feb 07 02:07:40 mailserver postfix/local[20294]: 8A6BFAB4BE: to=<rhoffman@securetech.com>, relay=local, delay=0.32, delays=0.32/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

2F2FEB6682

Feb 07 02:07:42 mailserver postfix/smtpd[4476]: 2F2FEB6682: client=unknown[23.74.164.69]

Feb 07 02:07:42 mailserver postfix/qmgr[4476]: 2F2FEB6682: from=<jrobinson@securetech.com>, size=2411, nrcpt=1 (queue active)

Feb 07 02:07:42 mailserver postfix/local[4476]: 2F2FEB6682: to=<cstanley@securetech.com>, relay=local, delay=0.84, delays=0.84/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

C5830FA296

Feb 07 02:07:43 mailserver postfix/smtpd[9636]: C5830FA296: client=unknown[23.74.164.69]

Feb 07 02:07:43 mailserver postfix/qmgr[9636]: C5830FA296: from=<jrobinson@securetech.com>, size=7742, nrcpt=1 (queue active)

Feb 07 02:07:43 mailserver postfix/local[9636]: C5830FA296: to=<aho@securetech.com>, relay=local, delay=0.20, delays=0.20/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

DFA4627685

Feb 07 02:07:45 mailserver postfix/smtpd[8941]: DFA4627685: client=unknown[23.74.164.69]

Feb 07 02:07:45 mailserver postfix/qmgr[8941]: DFA4627685: from=<jrobinson@securetech.com>, size=3061, nrcpt=1 (queue active)

Feb 07 02:07:45 mailserver postfix/local[8941]: DFA4627685: to=<cberger@securetech.com>, relay=local, delay=0.16, delays=0.16/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

8A340A8A35

Feb 07 02:07:48 mailserver postfix/smtpd[15965]: 8A340A8A35: client=unknown[23.74.164.69]

Feb 07 02:07:48 mailserver postfix/qmgr[15965]: 8A340A8A35: from=<jrobinson@securetech.com>, size=9560, nrcpt=1 (queue active)

Feb 07 02:07:48 mailserver postfix/local[15965]: 8A340A8A35: to=<sgray@securetech.com>, relay=local, delay=0.89, delays=0.89/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

3798B86689

Feb 07 02:07:52 mailserver postfix/smtpd[25346]: 3798B86689: client=unknown[23.74.164.69]

Feb 07 02:07:52 mailserver postfix/qmgr[25346]: 3798B86689: from=<jrobinson@securetech.com>, size=8285, nrcpt=1 (queue active)

Feb 07 02:07:52 mailserver postfix/local[25346]: 3798B86689: to=<troberts@securetech.com>, relay=local, delay=0.89, delays=0.89/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

711700BCA4

Feb 07 02:07:55 mailserver postfix/smtpd[16611]: 711700BCA4: client=unknown[23.74.164.69]

Feb 07 02:07:55 mailserver postfix/qmgr[16611]: 711700BCA4: from=<jrobinson@securetech.com>, size=4570, nrcpt=1 (queue active)

Feb 07 02:07:55 mailserver postfix/local[16611]: 711700BCA4: to=<anguyen@securetech.com>, relay=local, delay=0.57, delays=0.57/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

E733448081

Feb 07 02:07:56 mailserver postfix/smtpd[4542]: E733448081: client=unknown[23.74.164.69]

Feb 07 02:07:56 mailserver postfix/qmgr[4542]: E733448081: from=<jrobinson@securetech.com>, size=2303, nrcpt=1 (queue active)

Feb 07 02:07:56 mailserver postfix/local[4542]: E733448081: to=<mnelson@securetech.com>, relay=local, delay=0.74, delays=0.74/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

7C06072EB8

Feb 07 02:07:57 mailserver postfix/smtpd[12621]: 7C06072EB8: client=unknown[23.74.164.69]

Feb 07 02:07:57 mailserver postfix/qmgr[12621]: 7C06072EB8: from=<jrobinson@securetech.com>, size=6799, nrcpt=1 (queue active)

Feb 07 02:07:57 mailserver postfix/local[12621]: 7C06072EB8: to=<cedwards@securetech.com>, relay=local, delay=0.97, delays=0.97/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

E0D6B2B963

Feb 07 02:08:01 mailserver postfix/smtpd[13337]: E0D6B2B963: client=unknown[23.74.164.69]

Feb 07 02:08:01 mailserver postfix/qmgr[13337]: E0D6B2B963: from=<jrobinson@securetech.com>, size=8196, nrcpt=1 (queue active)

Feb 07 02:08:01 mailserver postfix/local[13337]: E0D6B2B963: to=<jfoster@securetech.com>, relay=local, delay=0.02, delays=0.02/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

80B309078E

Feb 07 02:08:03 mailserver postfix/smtpd[26975]: 80B309078E: client=unknown[23.74.164.69]

Feb 07 02:08:03 mailserver postfix/qmgr[26975]: 80B309078E: from=<jrobinson@securetech.com>, size=6415, nrcpt=1 (queue active)

Feb 07 02:08:03 mailserver postfix/local[26975]: 80B309078E: to=<kallen@securetech.com>, relay=local, delay=0.36, delays=0.36/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

89D4280DA8

Feb 07 02:08:08 mailserver postfix/smtpd[14512]: 89D4280DA8: client=unknown[23.74.164.69]

Feb 07 02:08:08 mailserver postfix/qmgr[14512]: 89D4280DA8: from=<jrobinson@securetech.com>, size=3317, nrcpt=1 (queue active)

Feb 07 02:08:08 mailserver postfix/local[14512]: 89D4280DA8: to=<smoreno@securetech.com>, relay=local, delay=0.00, delays=0.00/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

1127283AD5

Feb 07 02:08:10 mailserver postfix/smtpd[18307]: 1127283AD5: client=unknown[23.74.164.69]

Feb 07 02:08:10 mailserver postfix/qmgr[18307]: 1127283AD5: from=<jrobinson@securetech.com>, size=6669, nrcpt=1 (queue active)

Feb 07 02:08:10 mailserver postfix/local[18307]: 1127283AD5: to=<ahogan@securetech.com>, relay=local, delay=0.68, delays=0.68/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

C445EAF254

Feb 07 02:08:12 mailserver postfix/smtpd[7039]: C445EAF254: client=unknown[23.74.164.69]

Feb 07 02:08:12 mailserver postfix/qmgr[7039]: C445EAF254: from=<jrobinson@securetech.com>, size=2301, nrcpt=1 (queue active)

Feb 07 02:08:12 mailserver postfix/local[7039]: C445EAF254: to=<ksanders@securetech.com>, relay=local, delay=0.48, delays=0.48/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

8BF86F6846

Feb 07 02:08:16 mailserver postfix/smtpd[5787]: 8BF86F6846: client=unknown[23.74.164.69]

Feb 07 02:08:16 mailserver postfix/qmgr[5787]: 8BF86F6846: from=<jrobinson@securetech.com>, size=5722, nrcpt=1 (queue active)

Feb 07 02:08:16 mailserver postfix/local[5787]: 8BF86F6846: to=<kthompson@securetech.com>, relay=local, delay=0.41, delays=0.41/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

45EB551CF3

Feb 07 02:08:19 mailserver postfix/smtpd[28955]: 45EB551CF3: client=unknown[23.74.164.69]

Feb 07 02:08:19 mailserver postfix/qmgr[28955]: 45EB551CF3: from=<jrobinson@securetech.com>, size=7404, nrcpt=1 (queue active)

Feb 07 02:08:19 mailserver postfix/local[28955]: 45EB551CF3: to=<dpotter@securetech.com>, relay=local, delay=0.72, delays=0.72/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

CD2A45639A

Feb 07 02:08:21 mailserver postfix/smtpd[25684]: CD2A45639A: client=unknown[23.74.164.69]

Feb 07 02:08:21 mailserver postfix/qmgr[25684]: CD2A45639A: from=<jrobinson@securetech.com>, size=8678, nrcpt=1 (queue active)

Feb 07 02:08:21 mailserver postfix/local[25684]: CD2A45639A: to=<lcortez@securetech.com>, relay=local, delay=0.91, delays=0.91/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

5B58648761

Feb 07 02:08:22 mailserver postfix/smtpd[26481]: 5B58648761: client=unknown[23.74.164.69]

Feb 07 02:08:22 mailserver postfix/qmgr[26481]: 5B58648761: from=<jrobinson@securetech.com>, size=2461, nrcpt=1 (queue active)

Feb 07 02:08:22 mailserver postfix/local[26481]: 5B58648761: to=<fwilliamson@securetech.com>, relay=local, delay=0.29, delays=0.29/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

33B8D37645

Feb 07 02:08:27 mailserver postfix/smtpd[17962]: 33B8D37645: client=unknown[23.74.164.69]

Feb 07 02:08:27 mailserver postfix/qmgr[17962]: 33B8D37645: from=<jrobinson@securetech.com>, size=9309, nrcpt=1 (queue active)

Feb 07 02:08:27 mailserver postfix/local[17962]: 33B8D37645: to=<sboyd@securetech.com>, relay=local, delay=0.42, delays=0.42/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

1099BE936F

Feb 07 02:08:30 mailserver postfix/smtpd[9097]: 1099BE936F: client=unknown[23.74.164.69]

Feb 07 02:08:30 mailserver postfix/qmgr[9097]: 1099BE936F: from=<jrobinson@securetech.com>, size=9474, nrcpt=1 (queue active)

Feb 07 02:08:30 mailserver postfix/local[9097]: 1099BE936F: to=<bhowell@securetech.com>, relay=local, delay=0.04, delays=0.04/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

5624844B1D

Feb 07 02:08:32 mailserver postfix/smtpd[18640]: 5624844B1D: client=unknown[23.74.164.69]

Feb 07 02:08:32 mailserver postfix/qmgr[18640]: 5624844B1D: from=<jrobinson@securetech.com>, size=8306, nrcpt=1 (queue active)

Feb 07 02:08:32 mailserver postfix/local[18640]: 5624844B1D: to=<smorgan@securetech.com>, relay=local, delay=0.85, delays=0.85/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

CA9CBE79B7

Feb 07 02:08:34 mailserver postfix/smtpd[27472]: CA9CBE79B7: client=unknown[23.74.164.69]

Feb 07 02:08:34 mailserver postfix/qmgr[27472]: CA9CBE79B7: from=<jrobinson@securetech.com>, size=6623, nrcpt=1 (queue active)

Feb 07 02:08:34 mailserver postfix/local[27472]: CA9CBE79B7: to=<bgonzalez@securetech.com>, relay=local, delay=0.13, delays=0.13/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

99C658717F

Feb 07 02:08:35 mailserver postfix/smtpd[20740]: 99C658717F: client=unknown[23.74.164.69]

Feb 07 02:08:35 mailserver postfix/qmgr[20740]: 99C658717F: from=<jrobinson@securetech.com>, size=3566, nrcpt=1 (queue active)

Feb 07 02:08:35 mailserver postfix/local[20740]: 99C658717F: to=<aaguirre@securetech.com>, relay=local, delay=0.44, delays=0.44/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

5615E3D507

Feb 07 02:08:39 mailserver postfix/smtpd[6060]: 5615E3D507: client=unknown[23.74.164.69]

Feb 07 02:08:39 mailserver postfix/qmgr[6060]: 5615E3D507: from=<jrobinson@securetech.com>, size=3924, nrcpt=1 (queue active)

Feb 07 02:08:39 mailserver postfix/local[6060]: 5615E3D507: to=<jsmith@securetech.com>, relay=local, delay=0.00, delays=0.00/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

0D50AF6F6A

Feb 07 02:08:41 mailserver postfix/smtpd[14231]: 0D50AF6F6A: client=unknown[23.74.164.69]

Feb 07 02:08:41 mailserver postfix/qmgr[14231]: 0D50AF6F6A: from=<jrobinson@securetech.com>, size=3069, nrcpt=1 (queue active)

Feb 07 02:08:41 mailserver postfix/local[14231]: 0D50AF6F6A: to=<bho@securetech.com>, relay=local, delay=0.14, delays=0.14/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

D2225D61B6

Feb 07 02:08:44 mailserver postfix/smtpd[16802]: D2225D61B6: client=unknown[23.74.164.69]

Feb 07 02:08:44 mailserver postfix/qmgr[16802]: D2225D61B6: from=<jrobinson@securetech.com>, size=9940, nrcpt=1 (queue active)

Feb 07 02:08:44 mailserver postfix/local[16802]: D2225D61B6: to=<jbarry@securetech.com>, relay=local, delay=0.73, delays=0.73/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

8243945A9A

Feb 07 02:08:46 mailserver postfix/smtpd[9415]: 8243945A9A: client=unknown[23.74.164.69]

Feb 07 02:08:46 mailserver postfix/qmgr[9415]: 8243945A9A: from=<jrobinson@securetech.com>, size=8335, nrcpt=1 (queue active)

Feb 07 02:08:46 mailserver postfix/local[9415]: 8243945A9A: to=<jjacobs@securetech.com>, relay=local, delay=0.25, delays=0.25/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

B182A60497

Feb 07 02:08:48 mailserver postfix/smtpd[28011]: B182A60497: client=unknown[23.74.164.69]

Feb 07 02:08:48 mailserver postfix/qmgr[28011]: B182A60497: from=<jrobinson@securetech.com>, size=2348, nrcpt=1 (queue active)

Feb 07 02:08:48 mailserver postfix/local[28011]: B182A60497: to=<cvaldez@securetech.com>, relay=local, delay=0.99, delays=0.99/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

85E1329C5C

Feb 07 02:08:52 mailserver postfix/smtpd[2060]: 85E1329C5C: client=unknown[23.74.164.69]

Feb 07 02:08:52 mailserver postfix/qmgr[2060]: 85E1329C5C: from=<jrobinson@securetech.com>, size=8158, nrcpt=1 (queue active)

Feb 07 02:08:52 mailserver postfix/local[2060]: 85E1329C5C: to=<mhannah@securetech.com>, relay=local, delay=1.00, delays=1.00/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

7A599A2786

Feb 07 02:08:56 mailserver postfix/smtpd[14310]: 7A599A2786: client=unknown[23.74.164.69]

Feb 07 02:08:56 mailserver postfix/qmgr[14310]: 7A599A2786: from=<jrobinson@securetech.com>, size=3890, nrcpt=1 (queue active)

Feb 07 02:08:56 mailserver postfix/local[14310]: 7A599A2786: to=<lrussell@securetech.com>, relay=local, delay=0.92, delays=0.92/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

5F587A7632

Feb 07 02:08:59 mailserver postfix/smtpd[8729]: 5F587A7632: client=unknown[23.74.164.69]

Feb 07 02:08:59 mailserver postfix/qmgr[8729]: 5F587A7632: from=<jrobinson@securetech.com>, size=7480, nrcpt=1 (queue active)

Feb 07 02:08:59 mailserver postfix/local[8729]: 5F587A7632: to=<etran@securetech.com>, relay=local, delay=0.02, delays=0.02/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

5DA834FDA1

Feb 07 02:09:02 mailserver postfix/smtpd[20549]: 5DA834FDA1: client=unknown[23.74.164.69]

Feb 07 02:09:02 mailserver postfix/qmgr[20549]: 5DA834FDA1: from=<jrobinson@securetech.com>, size=2948, nrcpt=1 (queue active)

Feb 07 02:09:02 mailserver postfix/local[20549]: 5DA834FDA1: to=<lgriffin@securetech.com>, relay=local, delay=0.27, delays=0.27/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

586F30B049

Feb 07 02:09:05 mailserver postfix/smtpd[6622]: 586F30B049: client=unknown[23.74.164.69]

Feb 07 02:09:05 mailserver postfix/qmgr[6622]: 586F30B049: from=<jrobinson@securetech.com>, size=3869, nrcpt=1 (queue active)

Feb 07 02:09:05 mailserver postfix/local[6622]: 586F30B049: to=<rsingleton@securetech.com>, relay=local, delay=0.84, delays=0.84/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

7DBE9EA448

Feb 07 02:09:10 mailserver postfix/smtpd[17724]: 7DBE9EA448: client=unknown[23.74.164.69]

Feb 07 02:09:10 mailserver postfix/qmgr[17724]: 7DBE9EA448: from=<jrobinson@securetech.com>, size=2169, nrcpt=1 (queue active)

Feb 07 02:09:10 mailserver postfix/local[17724]: 7DBE9EA448: to=<adudley@securetech.com>, relay=local, delay=0.96, delays=0.96/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

F8E0BB92B9

Feb 07 02:09:14 mailserver postfix/smtpd[17290]: F8E0BB92B9: client=unknown[23.74.164.69]

Feb 07 02:09:14 mailserver postfix/qmgr[17290]: F8E0BB92B9: from=<jrobinson@securetech.com>, size=8493, nrcpt=1 (queue active)

Feb 07 02:09:14 mailserver postfix/local[17290]: F8E0BB92B9: to=<tlawson@securetech.com>, relay=local, delay=0.19, delays=0.19/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

C7023D220C

Feb 07 02:09:16 mailserver postfix/smtpd[12663]: C7023D220C: client=unknown[23.74.164.69]

Feb 07 02:09:16 mailserver postfix/qmgr[12663]: C7023D220C: from=<jrobinson@securetech.com>, size=7670, nrcpt=1 (queue active)

Feb 07 02:09:16 mailserver postfix/local[12663]: C7023D220C: to=<sdoyle@securetech.com>, relay=local, delay=0.87, delays=0.87/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

83D31FB900

Feb 07 02:09:21 mailserver postfix/smtpd[10324]: 83D31FB900: client=unknown[23.74.164.69]

Feb 07 02:09:21 mailserver postfix/qmgr[10324]: 83D31FB900: from=<jrobinson@securetech.com>, size=6450, nrcpt=1 (queue active)

Feb 07 02:09:21 mailserver postfix/local[10324]: 83D31FB900: to=<jbaker@securetech.com>, relay=local, delay=0.94, delays=0.94/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

02A15B3F56

Feb 07 02:09:25 mailserver postfix/smtpd[16527]: 02A15B3F56: client=unknown[23.74.164.69]

Feb 07 02:09:25 mailserver postfix/qmgr[16527]: 02A15B3F56: from=<jrobinson@securetech.com>, size=7964, nrcpt=1 (queue active)

Feb 07 02:09:25 mailserver postfix/local[16527]: 02A15B3F56: to=<aroberts@securetech.com>, relay=local, delay=0.85, delays=0.85/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

93C2343223

Feb 07 02:09:29 mailserver postfix/smtpd[11525]: 93C2343223: client=unknown[23.74.164.69]

Feb 07 02:09:29 mailserver postfix/qmgr[11525]: 93C2343223: from=<jrobinson@securetech.com>, size=6904, nrcpt=1 (queue active)

Feb 07 02:09:29 mailserver postfix/local[11525]: 93C2343223: to=<kjohnson@securetech.com>, relay=local, delay=0.47, delays=0.47/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

F29EB22E09

Feb 07 02:09:34 mailserver postfix/smtpd[5769]: F29EB22E09: client=unknown[23.74.164.69]

Feb 07 02:09:34 mailserver postfix/qmgr[5769]: F29EB22E09: from=<jrobinson@securetech.com>, size=6435, nrcpt=1 (queue active)

Feb 07 02:09:34 mailserver postfix/local[5769]: F29EB22E09: to=<mmorales@securetech.com>, relay=local, delay=0.74, delays=0.74/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

767AB29E9A

Feb 07 02:09:39 mailserver postfix/smtpd[26389]: 767AB29E9A: client=unknown[23.74.164.69]

Feb 07 02:09:39 mailserver postfix/qmgr[26389]: 767AB29E9A: from=<jrobinson@securetech.com>, size=5542, nrcpt=1 (queue active)

Feb 07 02:09:39 mailserver postfix/local[26389]: 767AB29E9A: to=<kjones@securetech.com>, relay=local, delay=0.87, delays=0.87/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

49D3483C91

Feb 07 02:09:43 mailserver postfix/smtpd[16893]: 49D3483C91: client=unknown[23.74.164.69]

Feb 07 02:09:43 mailserver postfix/qmgr[16893]: 49D3483C91: from=<jrobinson@securetech.com>, size=7047, nrcpt=1 (queue active)

Feb 07 02:09:43 mailserver postfix/local[16893]: 49D3483C91: to=<awilson@securetech.com>, relay=local, delay=0.37, delays=0.37/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

EF1E919841

Feb 07 02:09:48 mailserver postfix/smtpd[11020]: EF1E919841: client=unknown[23.74.164.69]

Feb 07 02:09:48 mailserver postfix/qmgr[11020]: EF1E919841: from=<jrobinson@securetech.com>, size=6986, nrcpt=1 (queue active)

Feb 07 02:09:48 mailserver postfix/local[11020]: EF1E919841: to=<jmendoza@securetech.com>, relay=local, delay=0.94, delays=0.94/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

5D6E13F092

Feb 07 02:09:49 mailserver postfix/smtpd[24439]: 5D6E13F092: client=unknown[23.74.164.69]

Feb 07 02:09:49 mailserver postfix/qmgr[24439]: 5D6E13F092: from=<jrobinson@securetech.com>, size=6871, nrcpt=1 (queue active)

Feb 07 02:09:49 mailserver postfix/local[24439]: 5D6E13F092: to=<pmccoy@securetech.com>, relay=local, delay=0.60, delays=0.60/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

1DC7EF4C11

Feb 07 02:09:52 mailserver postfix/smtpd[4075]: 1DC7EF4C11: client=unknown[23.74.164.69]

Feb 07 02:09:52 mailserver postfix/qmgr[4075]: 1DC7EF4C11: from=<jrobinson@securetech.com>, size=6052, nrcpt=1 (queue active)

Feb 07 02:09:52 mailserver postfix/local[4075]: 1DC7EF4C11: to=<scalhoun@securetech.com>, relay=local, delay=0.27, delays=0.27/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

90DB80284A

Feb 07 02:09:55 mailserver postfix/smtpd[9408]: 90DB80284A: client=unknown[23.74.164.69]

Feb 07 02:09:55 mailserver postfix/qmgr[9408]: 90DB80284A: from=<jrobinson@securetech.com>, size=5390, nrcpt=1 (queue active)

Feb 07 02:09:55 mailserver postfix/local[9408]: 90DB80284A: to=<jhampton@securetech.com>, relay=local, delay=0.93, delays=0.93/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

CEB497FB89

Feb 07 02:09:58 mailserver postfix/smtpd[17892]: CEB497FB89: client=unknown[23.74.164.69]

Feb 07 02:09:58 mailserver postfix/qmgr[17892]: CEB497FB89: from=<jrobinson@securetech.com>, size=4089, nrcpt=1 (queue active)

Feb 07 02:09:58 mailserver postfix/local[17892]: CEB497FB89: to=<nmiranda@securetech.com>, relay=local, delay=0.20, delays=0.20/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

5C0CBCEF3E

Feb 07 02:10:01 mailserver postfix/smtpd[4131]: 5C0CBCEF3E: client=unknown[23.74.164.69]

Feb 07 02:10:01 mailserver postfix/qmgr[4131]: 5C0CBCEF3E: from=<jrobinson@securetech.com>, size=8870, nrcpt=1 (queue active)

Feb 07 02:10:01 mailserver postfix/local[4131]: 5C0CBCEF3E: to=<tpeters@securetech.com>, relay=local, delay=0.72, delays=0.72/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

A9069ED1C9

Feb 07 02:10:03 mailserver postfix/smtpd[8110]: A9069ED1C9: client=unknown[23.74.164.69]

Feb 07 02:10:03 mailserver postfix/qmgr[8110]: A9069ED1C9: from=<jrobinson@securetech.com>, size=6043, nrcpt=1 (queue active)

Feb 07 02:10:03 mailserver postfix/local[8110]: A9069ED1C9: to=<spope@securetech.com>, relay=local, delay=0.81, delays=0.81/0/0/0, dsn=2.0.0, status=send (delivered to mailbox)

**Attacker IP: 23.74.164.69 (**[carrie64@ford.com](mailto:carrie64@ford.com))

**Out of this 79 only 6 of them submitted their credentials, So total of 7**

List of employees who got interacted with phishing emails:

|  |  |  |
| --- | --- | --- |
| **Jamie White** | c0:83:ec:10:a1:7c | 10.10.2.236 |
| **Darrell King** | f5:37:d4:52:b7:a6 | 10.10.0.251 |
| **Aaron Roman** | e2:10:60:fe:54:d1 | 10.10.1.195 |
| **Nicholas Cardenas Jr.** | e3:dd:04:05:16:35 | 10.10.0.61 |
| **Brenda Mccall** | 22:eb:d7:d5:8a:3f | 10.10.3.59 |
| **Melissa Butler** | 5a:b5:b1:96:eb:75 | 10.10.3.175 |
| **Renee Moses** | 6c:e4:92:1b:c2:a6 | 10.10.2.142 |
| **Tiffany Higgins** | 08:6a:ff:78:13:a0 | 10.10.1.63 |
| **Andrea Baxter** | 83:36:d8:47:31:2b | 10.10.0.94 |
| **Daniel Jordan** | c1:22:45:93:cc:59 | 10.10.2.251 |
| **Mr. Michael Martin MD** | 33:e8:88:d8:5d:d1 | 10.10.2.204 |
| **Amy Harrell** | db:29:a4:39:28:69 | 10.10.1.117 |
| **Brian Barron** | 30:6e:c4:97:62:cc | 10.10.2.64 |
| **Richard Gardner** | 61:83:84:84:37:c2 | 10.10.2.17 |
| **Jennifer Barber** | 5c:c0:fd:4d:dd:73 | 10.10.0.89 |
| **Larry Smith** | 56:07:7d:f6:e3:9d | 10.10.2.86 |
| **Daniel Collins** | 5f:dc:7f:ba:8a:65 | 10.10.2.168 |
| **Melinda Espinoza** | 0a:eb:43:36:e1:10 | 10.10.1.217 |
| **Angela Keith** | 02:b9:00:56:2c:cc | 10.10.0.198 |
| **Fernando Travis** | 4d:71:d5:4b:90:95 | 10.10.1.68 |
| **Daniel Mendoza** | e4:a4:63:29:32:0b | 10.10.2.78 |
| **Dale Reed** | 5b:b9:29:19:b5:4a | 10.10.3.120 |
| **Mike Jenkins** | 8b:3a:77:ca:d1:c5 | 10.10.2.46 |
| **John Lee** | 07:2a:a3:d2:26:57 | 10.10.3.231 |
| **Valerie Leach** | 03:a3:3c:03:90:f9 | 10.10.1.98 |
| **Tonya Medina** | 7f:42:ed:ee:a7:79 | 10.10.2.246 |
| **Jonathan Mason** | 9d:2f:f4:74:f9:1c | 10.10.0.98 |
| **Travis Howard** | 37:3c:8c:39:9a:e7 | 10.10.1.139 |
| **Lynn Green** | 4c:5f:72:ac:f0:93 | 10.10.1.24 |
| **Jesse Ball** | 09:9b:bc:9a:9a:1e | 10.10.1.198 |
| **Steven Ritter** | 21:c2:c0:53:3f:ef | 10.10.3.185 |
| **Kaitlyn Garcia** | 97:c1:8f:e3:8f:43 | 10.10.2.123 |
| **Robert Hoffman** | 85:71:ee:8f:4b:14 | 10.10.0.191 |
| **Christina Stanley** | ec:b7:80:db:16:ec | 10.10.1.50 |
| **Angela Ho** | ce:7d:0a:5b:7d:de | 10.10.0.32 |
| **Cassandra Berger** | 30:3d:ac:e0:34:ae | 10.10.2.193 |
| **Stephen Gray** | 1f:b9:c7:a3:2d:a6 | 10.10.3.216 |
| **Tricia Roberts** | e2:6a:88:aa:1b:ea | 10.10.3.44 |
| **Andrew Nguyen** | 1e:57:2f:c7:5c:86 | 10.10.0.50 |
| **Megan Nelson** | c8:ca:1a:27:6d:4c | 10.10.1.10 |
| **Megan Nelson** | 04:4b:7f:4c:32:39 | 10.10.1.233 |
| **Charles Edwards** | 32:cf:b7:23:14:76 | 10.10.2.137 |
| **Joseph Foster** | b7:dc:43:d5:49:ae | 10.10.1.234 |
| **Kimberly Allen** | 3f:06:1c:b2:0e:e5 | 10.10.3.139 |
| **Scott Moreno** | 7a:da:ee:81:03:77 | 10.10.1.206 |
| **Alejandro Hogan** | e9:4f:ce:7d:a1:7b | 10.10.0.146 |
| **Kayla Sanders** | 4b:40:9e:4f:b7:dd | 10.10.2.167 |
| **Krista Thompson** | 7f:ae:27:3c:77:ff | 10.10.3.90 |
| **Daniel Potter** | 34:b8:96:80:2f:4f | 10.10.1.249 |
| **Linda Cortez** | 89:20:43:b9:83:66 | 10.10.2.39 |
| **Franklin Williamson** | 39:64:c4:84:2c:0d | 10.10.1.83 |
| **Stacey Boyd** | 3a:29:2c:21:8b:d2 | 10.10.2.238 |
| **Brian Howell** | 40:5e:76:66:24:c3 | 10.10.0.21 |
| **Stephanie Morgan** | 63:25:49:3d:a3:0c | 10.10.3.225 |
| **Betty Gonzalez** | 0f:7a:e5:c7:f8:fb | 10.10.3.81 |
| **Aaron Aguirre** | c5:4e:e0:11:78:84 | 10.10.3.173 |
| **Jennifer Smith** | ab:78:36:04:98:d5 | 10.10.2.120 |
| **Bobby Ho** | b0:dd:c4:08:72:e2 | 10.10.2.54 |
| **Joseph Barry** | db:53:26:f0:8b:a3 | 10.10.0.123 |
| **Julie Jacobs** | f1:32:ed:73:70:2e | 10.10.0.92 |
| **Charles Valdez** | 19:68:63:4e:cb:11 | 10.10.1.113 |
| **Ms. Hannah Young** | 2f:eb:58:b1:b1:a0 | 10.10.2.125 |
| **Lisa Russell** | 22:9a:c1:0a:14:50 | 10.10.1.140 |
| **Erik Tran** | 13:ae:90:a0:11:32 | 10.10.1.172 |
| **Linda Griffin** | 7c:1c:13:50:0f:26 | 10.10.0.114 |
| **Ryan Singleton** | 69:1d:d0:97:a5:e3 | 10.10.1.104 |
| **Anna Dudley** | 5b:c2:ba:85:99:12 | 10.10.0.106 |
| **Thomas Lawson** | a9:79:a4:b3:c4:45 | 10.10.2.247 |
| **Stephanie Doyle** | d8:d0:0d:1e:3d:83 | 10.10.0.216 |
| **Johnathan Baker** | 7e:03:15:e2:7b:76 | 10.10.2.27 |
| **Amanda Roberts** | d2:f4:4e:14:b6:19 | 10.10.2.76 |
| **Keith Johnson** | 3c:81:03:cd:4f:29 | 10.10.3.221 |
| **Mary Morales** | 01:9a:b0:13:31:9f | 10.10.3.75 |
| **Kevin Jones** | 8b:9d:d2:05:72:e9 | 10.10.0.39 |
| **Anna Wilson** | e5:f0:7e:7f:39:7f | 10.10.1.72 |
| **Jerry Mendoza** | 42:db:a0:5e:ae:38 | 10.10.1.124 |
| **Patricia Mccoy** | af:07:b4:cc:ab:5a | 10.10.1.33 |
| **Spencer Calhoun** | e0:8d:6a:8c:cb:96 | 10.10.0.178 |
| **Jesse Hampton** | 2e:a6:0b:f3:99:f9 | 10.10.3.118 |
| **Nathan Miranda** | 06:70:37:2a:14:d5 | 10.10.1.70 |
| **Tony Peters** | 25:7a:9e:03:70:27 | 10.10.0.22 |
| **Stephen Pope** | a0:80:ea:8f:1b:9f | 10.10.3.21 |
| **Jason Robinson** | f9:cb:e3:f4:18:5c | 10.10.1.7 |

http.log

That has shown Malicious file was accessed by some of the employees.

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.7", "src\_port": 51251, "event\_type": "http", "timestamp": "2025-02-06T21:15:15", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.2; Trident/4.0)"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.7", "src\_port": 58557, "event\_type": "http", "timestamp": "2025-02-06T21:15:29", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.2; Trident/4.0)"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.0.21", "src\_port": 57483, "event\_type": "http", "timestamp": "2025-02-07T02:11:37", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.65.(X11; Linux x86\_64; aa-DJ) Presto/2.9.189 Version/12.00"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.104", "src\_port": 50564, "event\_type": "http", "timestamp": "2025-02-07T02:13:05", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/8.93.(X11; Linux x86\_64; fa-IR) Presto/2.9.170 Version/10.00"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.123", "src\_port": 54291, "event\_type": "http", "timestamp": "2025-02-07T02:22:16", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.10.(Windows NT 5.01; bho-IN) Presto/2.9.177 Version/10.00"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.98", "src\_port": 54990, "event\_type": "http", "timestamp": "2025-02-07T02:32:53", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.236", "src\_port": 51294, "event\_type": "http", "timestamp": "2025-02-07T02:33:45", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (iPod; U; CPU iPhone OS 3\_1 like Mac OS X; hy-AM) AppleWebKit/531.27.3 (KHTML, like Gecko) Version/3.0.5 Mobile/8B113 Safari/6531.27.3"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.185", "src\_port": 51205, "event\_type": "http", "timestamp": "2025-02-07T02:42:32", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10 12\_0 rv:5.0; sat-IN) AppleWebKit/531.6.6 (KHTML, like Gecko) Version/4.1 Safari/531.6.6"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.185", "src\_port": 62383, "event\_type": "http", "timestamp": "2025-02-07T02:42:41", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10 12\_0 rv:5.0; sat-IN) AppleWebKit/531.6.6 (KHTML, like Gecko) Version/4.1 Safari/531.6.6"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.124", "src\_port": 53313, "event\_type": "http", "timestamp": "2025-02-07T03:04:46", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Windows; U; Windows 95) AppleWebKit/534.5.5 (KHTML, like Gecko) Version/4.0.5 Safari/534.5.5"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.117", "src\_port": 58914, "event\_type": "http", "timestamp": "2025-02-07T03:15:50", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Linux; Android 1.6) AppleWebKit/536.0 (KHTML, like Gecko) Chrome/26.0.836.0 Safari/536.0"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.102", "src\_port": 52900, "event\_type": "http", "timestamp": "2025-02-07T03:19:43", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Windows; U; Windows NT 6.2) AppleWebKit/535.12.2 (KHTML, like Gecko) Version/5.0.3 Safari/535.12.2"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.168", "src\_port": 50608, "event\_type": "http", "timestamp": "2025-02-07T03:33:46", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (iPad; CPU iPad OS 14\_2 like Mac OS X) AppleWebKit/535.0 (KHTML, like Gecko) FxiOS/16.0o7523.0 Mobile/73K508 Safari/535.0"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.206", "src\_port": 55195, "event\_type": "http", "timestamp": "2025-02-07T03:48:18", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Windows; U; Windows NT 6.1) AppleWebKit/533.28.6 (KHTML, like Gecko) Version/5.0.5 Safari/533.28.6"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.238", "src\_port": 59999, "event\_type": "http", "timestamp": "2025-02-07T03:48:22", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (X11; Linux i686) AppleWebKit/535.1 (KHTML, like Gecko) Chrome/35.0.829.0 Safari/535.1"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.0.191", "src\_port": 55391, "event\_type": "http", "timestamp": "2025-02-07T04:29:26", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.46.(Windows NT 4.0; csb-PL) Presto/2.9.178 Version/12.00"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.81", "src\_port": 61653, "event\_type": "http", "timestamp": "2025-02-07T04:37:45", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10 10\_8; rv:1.9.2.20) Gecko/2025-02-13 08:34:03 Firefox/3.6.15"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.78", "src\_port": 53561, "event\_type": "http", "timestamp": "2025-02-07T04:46:56", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 10.0; Trident/4.0)"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.64", "src\_port": 51298, "event\_type": "http", "timestamp": "2025-02-07T04:51:37", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.88.(X11; Linux i686; cs-CZ) Presto/2.9.188 Version/10.00"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.64", "src\_port": 62731, "event\_type": "http", "timestamp": "2025-02-07T04:51:48", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.88.(X11; Linux i686; cs-CZ) Presto/2.9.188 Version/10.00"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.86", "src\_port": 53957, "event\_type": "http", "timestamp": "2025-02-07T05:07:53", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (iPod; U; CPU iPhone OS 4\_2 like Mac OS X; pl-PL) AppleWebKit/534.48.5 (KHTML, like Gecko) Version/3.0.5 Mobile/8B114 Safari/6534.48.5"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.234", "src\_port": 60790, "event\_type": "http", "timestamp": "2025-02-07T05:37:18", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/532.2 (KHTML, like Gecko) Chrome/27.0.890.0 Safari/532.2"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.234", "src\_port": 63797, "event\_type": "http", "timestamp": "2025-02-07T05:37:42", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/532.2 (KHTML, like Gecko) Chrome/27.0.890.0 Safari/532.2"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.75", "src\_port": 49739, "event\_type": "http", "timestamp": "2025-02-07T05:58:07", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (iPod; U; CPU iPhone OS 3\_2 like Mac OS X; iu-CA) AppleWebKit/532.45.5 (KHTML, like Gecko) Version/4.0.5 Mobile/8B118 Safari/6532.45.5"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.0.89", "src\_port": 50259, "event\_type": "http", "timestamp": "2025-02-07T06:03:25", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (compatible; MSIE 5.0; Windows NT 5.2; Trident/4.1)"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.33", "src\_port": 56633, "event\_type": "http", "timestamp": "2025-02-07T06:04:31", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; PPC Mac OS X 10 5\_9) AppleWebKit/536.2 (KHTML, like Gecko) Chrome/22.0.834.0 Safari/536.2"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.33", "src\_port": 53313, "event\_type": "http", "timestamp": "2025-02-07T06:05:01", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; PPC Mac OS X 10 5\_9) AppleWebKit/536.2 (KHTML, like Gecko) Chrome/22.0.834.0 Safari/536.2"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.172", "src\_port": 60319, "event\_type": "http", "timestamp": "2025-02-07T06:15:58", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Android 2.3.3; Mobile; rv:23.0) Gecko/23.0 Firefox/23.0"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.198", "src\_port": 52308, "event\_type": "http", "timestamp": "2025-02-07T06:17:55", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/8.37.(Windows NT 6.1; tr-TR) Presto/2.9.169 Version/11.00"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.198", "src\_port": 55920, "event\_type": "http", "timestamp": "2025-02-07T06:18:18", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/8.37.(Windows NT 6.1; tr-TR) Presto/2.9.169 Version/11.00"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.231", "src\_port": 53304, "event\_type": "http", "timestamp": "2025-02-07T06:32:35", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10 8\_3) AppleWebKit/536.1 (KHTML, like Gecko) Chrome/26.0.873.0 Safari/536.1"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.50", "src\_port": 51014, "event\_type": "http", "timestamp": "2025-02-07T06:45:54", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.87.(X11; Linux x86\_64; niu-NU) Presto/2.9.166 Version/12.00"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.175", "src\_port": 55503, "event\_type": "http", "timestamp": "2025-02-07T06:59:24", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 9\_4) AppleWebKit/533.0 (KHTML, like Gecko) Chrome/20.0.818.0 Safari/533.0"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.175", "src\_port": 57493, "event\_type": "http", "timestamp": "2025-02-07T06:59:35", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 9\_4) AppleWebKit/533.0 (KHTML, like Gecko) Chrome/20.0.818.0 Safari/533.0"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.140", "src\_port": 64706, "event\_type": "http", "timestamp": "2025-02-07T07:13:49", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/8.84.(X11; Linux x86\_64; ne-NP) Presto/2.9.186 Version/11.00"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.17", "src\_port": 57562, "event\_type": "http", "timestamp": "2025-02-07T07:17:02", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (iPod; U; CPU iPhone OS 4\_3 like Mac OS X; cmn-TW) AppleWebKit/533.24.7 (KHTML, like Gecko) Version/4.0.5 Mobile/8B116 Safari/6533.24.7"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.120", "src\_port": 59612, "event\_type": "http", "timestamp": "2025-02-07T07:18:20", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Windows; U; Windows 95) AppleWebKit/535.39.3 (KHTML, like Gecko) Version/5.1 Safari/535.39.3"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.217", "src\_port": 60198, "event\_type": "http", "timestamp": "2025-02-07T07:19:04", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 10.0; Trident/3.1)"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.21", "src\_port": 54587, "event\_type": "http", "timestamp": "2025-02-07T07:27:17", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (iPhone; CPU iPhone OS 5\_1\_1 like Mac OS X) AppleWebKit/532.2 (KHTML, like Gecko) CriOS/56.0.850.0 Mobile/46P478 Safari/532.2"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.0.251", "src\_port": 50394, "event\_type": "http", "timestamp": "2025-02-07T07:33:42", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Linux; Android 4.2) AppleWebKit/532.2 (KHTML, like Gecko) Chrome/21.0.873.0 Safari/532.2"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.0.146", "src\_port": 49798, "event\_type": "http", "timestamp": "2025-02-07T07:47:25", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.12.(Windows 98; Win 9x 4.90; kok-IN) Presto/2.9.175 Version/11.00"}

**List of employees who click on the website and also list of employees who might have submitted their credentials**

Src\_ip:

GET:

1. 10.10.1.7
2. 10.10.0.21
3. 10.10.1.104
4. 10.10.2.123
5. 10.10.1.98
6. 10.10.2.236
7. 10.10.3.185
8. 10.10.1.124
9. 10.10.1.117
10. 10.10.1.102
11. 10.10.2.168
12. 10.10.1.206
13. 10.10.2.238
14. 10.10.0.191
15. 10.10.3.81
16. 10.10.2.78
17. 10.10.2.64
18. 10.10.2.86
19. 10.10.1.234
20. 10.10.3.75
21. 10.10.0.89
22. 10.10.1.33
23. 10.10.1.172
24. 10.10.1.198
25. 10.10.3.231
26. 10.10.1.50
27. 10.10.3.175
28. 10.10.1.140
29. 10.10.2.17
30. 10.10.3.120
31. 10.10.1.217
32. 10.10.3.21
33. 10.10.0.251
34. 10.10.0.146

POST:

1. 10.10.1.7
2. 10.10.3.185
3. 10.10.2.64
4. 10.10.1.234
5. 10.10.1.33
6. 10.10.1.198
7. 10.10.3.175

**Employers who were affected by attack:**

1. Melissa Butler: 10.10.3.175. email: mbutler@securetech.com
2. Brian Barron: 10.10.2.64 email: bbarron@securetech.com
3. Jesse Ball: 10.10.1.198 email: jball@securetech.com
4. Steven Ritter: 10.10.3.185 email: sritter@securetech.com
5. Joseph Foster: 10.10.1.234 email: jfoster@securetech.com
6. Patricia McCoy: 10.10.1.33 email: pmccoy@securetech.com
7. Jason Robinson: 10.10.1.7 email: jrobinson@securetech.com

**Suspicious activity:**

**Jason Robinson**

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.7", "src\_port": 51251, "event\_type": "http", "timestamp": "2025-02-06T21:15:15", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.2; Trident/4.0)"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.7", "src\_port": 58557, "event\_type": "http", "timestamp": "2025-02-06T21:15:29", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.2; Trident/4.0)"}

{"http.http\_method": "DELETE", "http.url": "list/list/categories", "http.protocol": "HTTP/1.1", "http.hostname": "srv-82.adkins-hinton.romero.biz", "src\_ip": "10.10.1.7", "src\_port": 62491, "event\_type": "http", "timestamp": "2025-02-07T18:31:43", "dest\_ip": "191.162.143.18", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.2; Trident/4.0)"}

{"http.http\_method": "POST", "http.url": "categories/search", "http.protocol": "HTTP/1.1", "http.hostname": "lt-18.washington.com", "src\_ip": "10.10.1.7", "src\_port": 53714, "event\_type": "http", "timestamp": "2025-02-08T13:00:43", "dest\_ip": "134.146.18.196", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 6.2; Trident/4.0)"}

**Brian Barron**

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.64", "src\_port": 51298, "event\_type": "http", "timestamp": "2025-02-07T04:51:37", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.88.(X11; Linux i686; cs-CZ) Presto/2.9.188 Version/10.00"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.2.64", "src\_port": 62731, "event\_type": "http", "timestamp": "2025-02-07T04:51:48", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.88.(X11; Linux i686; cs-CZ) Presto/2.9.188 Version/10.00"}

{"http.http\_method": "DELETE", "http.url": "main/blog/app", "http.protocol": "HTTP/1.1", "http.hostname": "web-81.juarez-raymond.woodward.com", "src\_ip": "10.10.2.64", "src\_port": 62784, "event\_type": "http", "timestamp": "2025-02-10T19:21:43", "dest\_ip": "102.218.197.221", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.88.(X11; Linux i686; cs-CZ) Presto/2.9.188 Version/10.00"}

{"http.http\_method": "PUT", "http.url": "tags/categories", "http.protocol": "HTTP/1.1", "http.hostname": "srv-02.mcdonald.chaney-forbes.info", "src\_ip": "10.10.2.64", "src\_port": 65396, "event\_type": "http", "timestamp": "2025-02-11T19:17:43", "dest\_ip": "212.176.252.138", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.88.(X11; Linux i686; cs-CZ) Presto/2.9.188 Version/10.00"}

{"http.http\_method": "TRACE", "http.url": "category/explore", "http.protocol": "HTTP/1.1", "http.hostname": "desktop-42.garcia.com", "src\_ip": "10.10.2.64", "src\_port": 62116, "event\_type": "http", "timestamp": "2025-02-11T23:44:43", "dest\_ip": "216.232.33.244", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/9.88.(X11; Linux i686; cs-CZ) Presto/2.9.188 Version/10.00"}

**Melissa Butler**

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.175", "src\_port": 55503, "event\_type": "http", "timestamp": "2025-02-07T06:59:24", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 9\_4) AppleWebKit/533.0 (KHTML, like Gecko) Chrome/20.0.818.0 Safari/533.0"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.175", "src\_port": 57493, "event\_type": "http", "timestamp": "2025-02-07T06:59:35", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 9\_4) AppleWebKit/533.0 (KHTML, like Gecko) Chrome/20.0.818.0 Safari/533.0"}

{"http.http\_method": "TRACE", "http.url": "tags", "http.protocol": "HTTP/1.1", "http.hostname": "srv-78.owens-randolph.maldonado.com", "src\_ip": "10.10.3.175", "src\_port": 54376, "event\_type": "http", "timestamp": "2025-02-09T15:59:43", "dest\_ip": "111.36.181.39", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10 9\_4) AppleWebKit/533.0 (KHTML, like Gecko) Chrome/20.0.818.0 Safari/533.0"}

**Jesse Ball**

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.198", "src\_port": 52308, "event\_type": "http", "timestamp": "2025-02-07T06:17:55", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/8.37.(Windows NT 6.1; tr-TR) Presto/2.9.169 Version/11.00"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.198", "src\_port": 55920, "event\_type": "http", "timestamp": "2025-02-07T06:18:18", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/8.37.(Windows NT 6.1; tr-TR) Presto/2.9.169 Version/11.00"}

{"http.http\_method": "PUT", "http.url": "tag/tag/category", "http.protocol": "HTTP/1.1", "http.hostname": "laptop-93.mcgee-miller.com", "src\_ip": "10.10.1.198", "src\_port": 61750, "event\_type": "http", "timestamp": "2025-02-09T03:51:43", "dest\_ip": "175.243.29.128", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/8.37.(Windows NT 6.1; tr-TR) Presto/2.9.169 Version/11.00"}

{"http.http\_method": "HEAD", "http.url": "tags/blog", "http.protocol": "HTTP/1.1", "http.hostname": "db-63.cook.com", "src\_ip": "10.10.1.198", "src\_port": 54750, "event\_type": "http", "timestamp": "2025-02-09T23:54:43", "dest\_ip": "59.118.160.50", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/8.37.(Windows NT 6.1; tr-TR) Presto/2.9.169 Version/11.00"}

{"http.http\_method": "PATCH", "http.url": "wp-content", "http.protocol": "HTTP/1.1", "http.hostname": "laptop-73.morton.com", "src\_ip": "10.10.1.198", "src\_port": 52447, "event\_type": "http", "timestamp": "2025-02-10T10:27:43", "dest\_ip": "38.49.113.71", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/8.37.(Windows NT 6.1; tr-TR) Presto/2.9.169 Version/11.00"}

{"http.http\_method": "HEAD", "http.url": "tags", "http.protocol": "HTTP/1.1", "http.hostname": "srv-36.vazquez.wilson.org", "src\_ip": "10.10.1.198", "src\_port": 61418, "event\_type": "http", "timestamp": "2025-02-10T21:53:43", "dest\_ip": "65.96.163.175", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Opera/8.37.(Windows NT 6.1; tr-TR) Presto/2.9.169 Version/11.00"}

**Steven Ritter**

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.185", "src\_port": 51205, "event\_type": "http", "timestamp": "2025-02-07T02:42:32", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10 12\_0 rv:5.0; sat-IN) AppleWebKit/531.6.6 (KHTML, like Gecko) Version/4.1 Safari/531.6.6"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.3.185", "src\_port": 62383, "event\_type": "http", "timestamp": "2025-02-07T02:42:41", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10 12\_0 rv:5.0; sat-IN) AppleWebKit/531.6.6 (KHTML, like Gecko) Version/4.1 Safari/531.6.6"}

{"http.http\_method": "TRACE", "http.url": "categories/category/blog", "http.protocol": "HTTP/1.1", "http.hostname": "lt-57.reeves.com", "src\_ip": "10.10.3.185", "src\_port": 57212, "event\_type": "http", "timestamp": "2025-02-08T16:37:43", "dest\_ip": "98.74.113.222", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10 12\_0 rv:5.0; sat-IN) AppleWebKit/531.6.6 (KHTML, like Gecko) Version/4.1 Safari/531.6.6"}

{"http.http\_method": "GET", "http.url": "posts/main/categories", "http.protocol": "HTTP/1.1", "http.hostname": "email-06.espinoza.com", "src\_ip": "10.10.3.185", "src\_port": 51587, "event\_type": "http", "timestamp": "2025-02-10T03:48:43", "dest\_ip": "154.219.15.121", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10 12\_0 rv:5.0; sat-IN) AppleWebKit/531.6.6 (KHTML, like Gecko) Version/4.1 Safari/531.6.6"}

{"http.http\_method": "GET", "http.url": "list/category/category", "http.protocol": "HTTP/1.1", "http.hostname": "laptop-21.phillips.info", "src\_ip": "10.10.3.185", "src\_port": 60759, "event\_type": "http", "timestamp": "2025-02-10T03:54:43", "dest\_ip": "196.233.94.225", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10 12\_0 rv:5.0; sat-IN) AppleWebKit/531.6.6 (KHTML, like Gecko) Version/4.1 Safari/531.6.6"}

{"http.http\_method": "TRACE", "http.url": "app/category", "http.protocol": "HTTP/1.1", "http.hostname": "laptop-24.baker.org", "src\_ip": "10.10.3.185", "src\_port": 51378, "event\_type": "http", "timestamp": "2025-02-11T20:59:43", "dest\_ip": "152.160.201.28", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; U; PPC Mac OS X 10 12\_0 rv:5.0; sat-IN) AppleWebKit/531.6.6 (KHTML, like Gecko) Version/4.1 Safari/531.6.6"}

**Joseph Foster**

{"http.http\_method": "PUT", "http.url": "app", "http.protocol": "HTTP/1.1", "http.hostname": "db-94.lopez.clark-delacruz.net", "src\_ip": "10.10.1.234", "src\_port": 50134, "event\_type": "http", "timestamp": "2025-02-06T18:54:43", "dest\_ip": "182.105.97.166", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/532.2 (KHTML, like Gecko) Chrome/27.0.890.0 Safari/532.2"}

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.234", "src\_port": 60790, "event\_type": "http", "timestamp": "2025-02-07T05:37:18", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/532.2 (KHTML, like Gecko) Chrome/27.0.890.0 Safari/532.2"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.234", "src\_port": 63797, "event\_type": "http", "timestamp": "2025-02-07T05:37:42", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/532.2 (KHTML, like Gecko) Chrome/27.0.890.0 Safari/532.2"}

{"http.http\_method": "GET", "http.url": "category", "http.protocol": "HTTP/1.1", "http.hostname": "laptop-68.miller-stanley.org", "src\_ip": "10.10.1.234", "src\_port": 59371, "event\_type": "http", "timestamp": "2025-02-10T10:23:43", "dest\_ip": "144.148.49.39", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/532.2 (KHTML, like Gecko) Chrome/27.0.890.0 Safari/532.2"}

{"http.http\_method": "GET", "http.url": "wp-content/main/categories", "http.protocol": "HTTP/1.1", "http.hostname": "email-73.petersen-clark.biz", "src\_ip": "10.10.1.234", "src\_port": 64515, "event\_type": "http", "timestamp": "2025-02-10T16:39:43", "dest\_ip": "208.158.16.181", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/532.2 (KHTML, like Gecko) Chrome/27.0.890.0 Safari/532.2"}

{"http.http\_method": "TRACE", "http.url": "posts/categories", "http.protocol": "HTTP/1.1", "http.hostname": "db-89.mccall.com", "src\_ip": "10.10.1.234", "src\_port": 56657, "event\_type": "http", "timestamp": "2025-02-11T00:22:43", "dest\_ip": "212.112.44.19", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/532.2 (KHTML, like Gecko) Chrome/27.0.890.0 Safari/532.2"}

**Patricia McCoy**

{"http.http\_method": "GET", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.33", "src\_port": 56633, "event\_type": "http", "timestamp": "2025-02-07T06:04:31", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; PPC Mac OS X 10 5\_9) AppleWebKit/536.2 (KHTML, like Gecko) Chrome/22.0.834.0 Safari/536.2"}

{"http.http\_method": "POST", "http.url": "/login", "http.protocol": "HTTP/1.1", "http.hostname": "srv-61.kim.johnson.biz", "src\_ip": "10.10.1.33", "src\_port": 53313, "event\_type": "http", "timestamp": "2025-02-07T06:05:01", "dest\_ip": "23.74.164.69", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; PPC Mac OS X 10 5\_9) AppleWebKit/536.2 (KHTML, like Gecko) Chrome/22.0.834.0 Safari/536.2"}

{"http.http\_method": "DELETE", "http.url": "category/categories", "http.protocol": "HTTP/1.1", "http.hostname": "lt-22.graham-bates.gill.org", "src\_ip": "10.10.1.33", "src\_port": 55860, "event\_type": "http", "timestamp": "2025-02-10T20:42:43", "dest\_ip": "166.134.188.239", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; PPC Mac OS X 10 5\_9) AppleWebKit/536.2 (KHTML, like Gecko) Chrome/22.0.834.0 Safari/536.2"}

{"http.http\_method": "PUT", "http.url": "blog/category/categories", "http.protocol": "HTTP/1.1", "http.hostname": "web-12.garcia.small.info", "src\_ip": "10.10.1.33", "src\_port": 57276, "event\_type": "http", "timestamp": "2025-02-11T10:05:43", "dest\_ip": "206.182.146.64", "proto": "TCP", "dest\_port": 80, "http.http\_user\_agent": "Mozilla/5.0 (Macintosh; PPC Mac OS X 10 5\_9) AppleWebKit/536.2 (KHTML, like Gecko) Chrome/22.0.834.0 Safari/536.2"}