Table: Packet Capture Highlights for Wireshark packet capture file

Time/s after packet capture	Packet Number	Description	Mitigation Measures
0	11	joannetey@icm.com composes email to adam@asc.com on 9/21/2021 at **5:19:36 PM**, Singapore Time using Thunderbird 78.14.0 on 64bit Windows 10 Hi Adam, how is it going, Best Regards, Joanne Joanne is using machine 192.168.0.12	
19	24	Joanne plugs a SanDisk Ultra 3.0 thumb drive into a Microsoft Windows Edge 10 machine, workgroup WORKGROUP	Install cloud enabled endpoint detection response software on all machines, block thumb drives by default
69	92	Joanne attempts to connect to 192.168.0.14 on port 4899 from port 4334	
83	108	Joanne attempts to connect to 192.168.0.14 on port 80	
86	112	Joanne attempts to connect to 192.168.0.14 on port 8080	
87	115	Joanne attempts to connect to 192.168.0.14 on port 21 (FTP)	
89	119	Joanne begins a SYN based port scan / SYN flood of 192.168.0.14	Use a next generation firewall and Intrusion Protection System to guard against suspicious traffic
90, 91	255, 344, 346, 383, selected packets between 433-446	Port 135 is open (RPC used by server applications and remote administration applications)	Close port 135 via firewall or configuring RPC
132	1061	Port 5900 (VNC) is open	Ensure VNC uses secure authentication, if this service is not required disable it or block it with a firewall
135, 147	1084, 1117	Joanne fails to authenticate with VNC on port 5900 on 192.168.0.14 from 192.168.0.12	

223	1217, 1242	Adam (adam@asc.com) sends Charles (charles@asc.com) an email, using Thunderbird 78.14 on 64bit Windows 10 on 21 Sep 2021 **17:23:37** +0800, with an attachment: Subject: Some help please Hi Charles, need some help with the product calculation. Thanks! Best Regards, Adam Attachment is an **infected (Trojan macro) excel spreadsheet** which uploads C:/secret/ files to 192.168.0.12 via FTP port 21 username IEUser, password Passw0rd on FTP folder /, this is done using a macro module1 InternetConnect.	Disable macros by default to protect against zero day exploits, also scan attachments for malware using cloud enabled endpoint detection software or tools like VirusTotal.
246	1311	Charles fetches his email from 209.165.200.236 and receives Adam's message.	
367	1561	Adam replies to Joanne using Thunderbird 78.14 on 64bit Windows 10 on 21 Sep 2021 **17:26:01** +0800 Subject: Re: Success? Hi Joanne, Done. American Express 1111 2222 3333 4444	Follow up investigation with American Express to identify Adam and possibly Joanne Share evidence with police and CSA

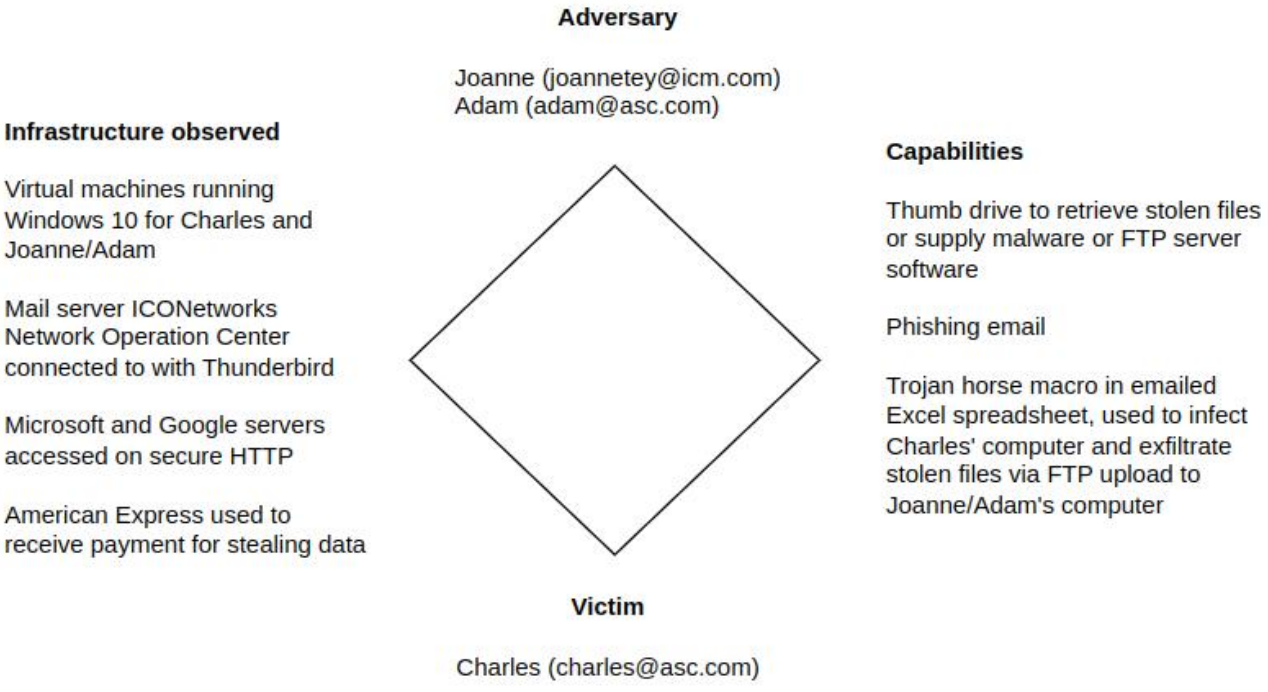

Image 3b. Non-technical diamond presentation for boardroom.

Adversary

Joanne (joannetey@icm.com)
Adam (adam@asc.com)

Victim
charles@asc.com

Infrastructure Details

192.168.0.12 (00:0c:29:04:d4:8a) - joannetey@icm.com (packet 11), adam@asc.com (packet 1217)
192.168.0.14 (00:0c:29:ba:bf:cd) - Probably charles@asc.com's computer
192.168.0.254 (00:0c:29:d1:a2:eb) - The acting router

209.165.200.236 ICONetworks Network Operations Center (IMAP, packet 2, connection from 192.168.0.12; IMAP, packet 1282 connection from 192.168.0.14): This is the mail server
13.107.22.200 Microsoft (443, packet 1054, connection from 192.168.0.12)
131.253.33.200 Microsoft (443, packet 1057, connection from 192.168.0.12, flagged by ESTsecurity as criminal IP VirusTotal score 2/90)

74.125.24.97 Google (port 443, packet 20, connection from 192.168.0.14)
142.250.4.94 Google (port 443, packet 1052, connection from 192.168.0.14)

Capabilities Details

Joanne:
Email (joannetey@icm.com)

Probably Joanne:
Thumb drive (Sandisk Ultra 3.0), probably contains FTP server software/malware and/or acts as media to receive stolen files.

Adam:
Email (adam@asc.com)
Infected Phone Pricing Excel 2007 Spreadsheet
- VirusTotal report says it contains a Trojan (Trojan Artemis VBA, virus total score 15/61), says it was created on Oct 8 2020. It uses the FTPPutFile function to upload all files in C:/secret/ to a FTP server on Adam's computer.