Forensic Report on Network Intrusion

[Your Name]
Bank of Hong Kong

[Date of the Report]

1 Overview / Case Summary

On the 29th of October 2022, at approximately 3:00 p.m., the Intrusion Detection System (IDS) of the Bank of Hong Kong flagged abnormal network activities aimed at the Bank's web server. This prompted an immediate and thorough examination, leading to the suspicion of a deliberate cyber-attack. As the appointed network security engineer, my task was to investigate these anomalies, analyze network traffic, and reconstruct the whole attack.

2 Objective/Tools Used/Evidence Map & Table

The primary objective of this forensic investigation is to analyze the pcap file to identify suspicious activities and reconstruct the events that occurred during the attack. Tools used for this analysis include Wireshark for packet inspection. The Evidence Map & Table, provided as follows, organizes the evidence collected during the investigation.

Table 1: Evidence Table (Private IP Addresses)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
192.168.56.1 or 147.8.178.172	ATHENA	Server Type: 0x00011007 (Workstation, Server, SQL, NT Workstation, Potential Browser)	Keep getting ICMP request from 192.168.93.131 / Keep getting 0x19(FIN, PSH, ACK) TCP packets in port 49159 from 147.8.179.15:80	Windows XP (5.1)	
192.168.93.1	–	Using Dropbox's LAN sync feature	Search for media renderer and media server	Dropbox LAN Sync Discovery Protocol	
192.168.93.2	–	Router/DNS/NBNS	–	–	
192.168.93.131	WIN-0GR9LTN6K0J.localdomain	(Workstation/Redirector)	Keep sending ICMP request to 192.168.56.1	MSFT 5.0 (maybe .NET 5.0 compatible)	
192.168.93.254	localdomain (domain name)	DHCP Server	–	–	
192.168.93.255	–	Broadcast	–	–	
192.168.240.11	SHRN100CB310	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.12	SHRN100LG103	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.13	SHRN100HW305	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.14	SHRN100HW307	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.15	SHRN100HW308	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	

Continued on next page

Table 1: Evidence Table (Private IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
192.168.240.16	SHRN100HW310	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.17	SHRN100HW311	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.19	SHRN100HW335A	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.20	SHRN100HW335	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.21	SHRN100CPLG104	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.22	SHRN100HW327	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.23	SHRN100CB315	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.24	SHRN100LG101	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	
192.168.240.25	SHRN100LG102	iGuard Security System Slave	Send heartbeat or status update every 30 seconds to Master (through broadcast)	–	

Continued on next page

Table 1: Evidence Table (Private IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
192.168.240.253 or 147.8.176.11	INTRALINK (Master Browser Server Name)	iGuard Security System Master / Local Master Browser within subnet 192.168.240.0/24 (Machine Group: CSISAD) Server Type: 0x00849a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Master Browser, DFS	Messages using BROWSER protocol	Windows Millenium Edition (Windows NT 4.9) / iGuard Security System	
192.168.240.255	–	Broadcast address of 192.168.240.0 /24	–	–	

Note: – means no specific information available

Table 2: Evidence Table (Public IP Addresses)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
87.230.55.33	ds87-230-55-33.dedicated.psmanaged.com	Cloud Service Provider (https://www.plusserver.com/en/)	–	–	
108.160.163.44	dropbox.com	Cloud Storage	–	–	
147.8.2.5	ntp.hku.hk	A Network Time Protocol server hosted by The University of Hong Kong (HKU)	Referred by packet No. 627882	–	
147.8.175.1	–	Probable router	Multiple ARP packets from different source requesting the MAC address of this IP Address	–	
147.8.175.5	–	Router equipped with Mobile IP functionality	ICMP Mobile IP Advertisement	–	
147.8.175.8	–	Communicate with PowerChute Network Shutdown	The NMC communicates with PCNS (PowerChute Network Shutdown) over UDP port 3052, A UDP packet is sent every 25 second to ensure communication between the NMC and PCNS Agent. Also, an Individual Client Notification packet (MACONFIG packet) is sent by the NMC every 100 seconds	APC UPS Network Management Card	
147.8.175.9	–	Communicate with PowerChute Network Shutdown	The NMC communicates with PCNS (PowerChute Network Shutdown) over UDP port 3052, A UDP packet is sent every 25 second to ensure communication between the NMC and PCNS Agent. Also, an Individual Client Notification packet (MACONFIG packet) is sent by the NMC every 100 seconds	APC UPS Network Management Card	
147.8.175.21	–	A NTP server	NTP packet No. 627882	–	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.175.25	–	Black and white laser multifunction printer	SSDP packets sent by this IP	RICOH Aficio MP 7500	
147.8.175.28	–	–	NBNS name query MINI1	–	
147.8.175.32	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	–	
147.8.175.38	CONFIDENCE	Web server running on a Windows XP operating system, with UPnP and HTTP Server API components (from UPnP) / Server Type: 0x00031003, Workstation, Server, NT Workstation, Potential Browser, Backup Browser / Using Dropbox's LAN sync feature	Port 2869 for UPnP / Host announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	Windows XP (Microsoft-Windows-NT/5.1, from UPnP) / Windows 7 or Windows Server 2008 R2 (from BROWSER protocol)	
147.8.175.41	c301b.local	Allows for printing over a network using the IPP / Supports Printer Description Language (PDL) for direct printing commands to the printer / Traditional LPD (Line Printer Daemon) service for network printing	Messages using mDNS from this IP	HP LaserJet 400 color M451dn printer	
147.8.175.43	–	–	Requesting the IP address of a device with a given NetBIOS name DUMMY	–	
147.8.175.49	–	–	NBNS name query MINI1	–	
147.8.175.52	–	–	Searching for an Internet gateway device that supports UPnP / Searching for yychung-pc	–	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.175.59	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	–	
147.8.175.66	WSCHAN-WIN7-32	Server Type: 0x00001003, Workstation, Server, NT Workstation	Host announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / Hardware and software for access control, video surveillance, time recording, and production data collection (from MAC address)	
147.8.175.69	sage.local	Offering an SSH file transfer service on port 22	Messages using mDNS	–	
147.8.175.70	PASSION	Server Type: 0x00009102, Server, Member, NT Workstation, NT Server	Host announcement using BROWSER	Windows 2000	
147.8.175.72	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	–	
147.8.175.74	HWCHAN-PC	Server Type: 0x00051003, Workstation, Server, NT Workstation, Potential Browser, Master Browser	Local Master announcement using BROWSER	Windows 7 or Windows Server 2008 R2	
147.8.175.78	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	–	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.175.80	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	–	
147.8.175.81	MyLinkStation.local	Server Type: 0x00019a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Potential Browser / Supporting Apple Filing Protocol over TCP (_afpovertcp) / Supporting TwonkyMedia UPnP SDK	Host announcement using BROWSER / SSDP NOTIFY messages	Network-Attached Storage (NAS) device from Buffalo Technology (Operating System: Linux)	
147.8.175.91	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	–	
147.8.175.105	–	Asking for the domain name pointers (PTR) of the services	Messages using mDNS	–	
147.8.175.109	–	Searching for BRUNOPC	NBNS name query message	–	
147.8.175.111	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	–	
147.8.175.122	–	Using Dropbox's LAN sync feature / Searching for printers and other devices using mDNS	Messages using Dropbox LAN Sync Discovery Protocol and mDNS	Apple device	
147.8.175.128	–	Using Dropbox's LAN sync feature / Sending printer commands to Canon printers	Messages using Dropbox LAN Sync Discovery Protocol and Canon BJNP	Apple device	
147.8.175.165	–	–	NBNS name query MINI1	Dell device	
147.8.175.168	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.175.181	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Device from Universal Global Scientific Industrial Co., Ltd.	
147.8.175.193	–	Using Dropbox's LAN sync feature / Trying to contact a remote license server through a UDP broadcast to port 1947 / Querying about HP02F966 (Workstation/Redirector)	Messages using Dropbox LAN Sync Discovery Protocol / UDP packets / NBNS packets	Dell device	
147.8.175.197	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.175.198	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.175.208	–	Using Dropbox's LAN sync feature / Searching for many names through NBNS	Messages using Dropbox LAN Sync Discovery Protocol and NBNS	Apple device	
147.8.175.209	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.175.215	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.175.216	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Device from FUJITSU LIMITED	
147.8.175.221	–	Using Dropbox's LAN sync feature / Sending printer commands to Canon printers	Messages using Dropbox LAN Sync Discovery Protocol and BJNP	Apple device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.175.222	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Device from Universal Global Scientific Industrial Co., Ltd.	
147.8.175.225	–	Using Dropbox's LAN sync feature / Sending SSDP discovery request for a device that is the root of a device tree / Sending messages to probable HP printers	Messages using Dropbox LAN Sync Discovery Protocol and SSDP / UDP broadcast to port 3702	MSI device	
147.8.175.230	–	–	NBNS name query MINI1	Dell device	
147.8.175.238	–	Querying about HP LaserJet / color LaserJet printers	Messages using mDNS protocol	Apple device	
147.8.175.246	–	Searching for media server / media renderer	Messages using SSDP	Device from PCS Systemtechnik	
147.8.175.252	–	Using Dropbox's LAN sync feature / Searching for Internet Gateway Device	Messages using Dropbox LAN Sync Discovery Protocol and SSDP	HP device	
147.8.175.255	–	Broadcast	–	–	
147.8.176.1	–	Router from Cisco Systems, Inc	Referred by DHCP packets	Cisco router	
147.8.176.11 or 192.168.240.253	INTRALINK	Server Type: 0x00819a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Potential Browser, DFS	Messages using BROWSER protocol	Windows Millenium Edition (Windows NT 4.9) / iGuard Security System	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.176.12	–	–	Referred by ARP broadcast (reply to 147.8.176.15) from source MAC address 00:14:4f:02:06:42, this IP and 147.8.178.15 belong to the same device	Oracle device	
147.8.176.15	–	DNS server	DNS queries and responses	A DNS server from Newisys,Inc.	
147.8.176.22	c316a2.local	Supporting the LPD protocol (port 515) for printing / raw printing via the PDL data stream (port 9100) / IPP (port 631)	Messages using mDNS	HP LaserJet P3010 Series printer	
147.8.176.23	c316b.local	Supporting the LPD protocol (port 515) for printing / raw printing via the PDL data stream (port 9100) / Sending additional details	Messages using mDNS	HP Color LaserJet 4650 printer	
147.8.176.26	c405c.local	Supporting raw printing via the PDL data stream (port 9100)	Messages using mDNS	HP Color LaserJet CP3505 printer	
147.8.176.27	c405b.local	Supporting raw printing via the PDL data stream (port 9100)	Messages using mDNS	HP LaserJet P3005 printer	
147.8.176.28	c405a.local	Printer	Messages using mDNS	HP LaserJet 8150 Series	
147.8.176.40	–	Announcement about domain CB315 and Master Browser Server Name (DVR315)	Message using BROWSER protocol	Device from QUANTUM DESIGNS (H.K.) LTD.	
147.8.176.44	SMART315	Server Type: 0x00001003, Workstation, Server, NT Workstation	Message using BROWSER protocol	Windows XP / iGuard API Server	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.176.46	–	–	Referred by ARP broadcast (requested by 147.8.176.12)	–	
147.8.176.55	–	Router	UPnP Device Description transmitted in TCP stream 3	Wireless Router TL-WR740	
147.8.176.56	PROMISE	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Messages using BROWSER protocol	Dell device	
147.8.176.75	Photo-NAS.local	NAS device	Message using mDNS	NAS from Synology Incorporated	
147.8.176.77	–	Searching for multiple names (e.g., HKUCS, CB411-COMPVISIO)	Messages using SSDP	Device from PCS Systemtechnik	
147.8.176.80	CSEX	Server Type: 0x0084102b, Workstation, Server, Domain Controller, Time Source, NT Workstation, Master Browser, DFS	Local Master Announcement using BROWSER	Windows Server 2003 R2 or Windows Server 2003 / Dell device	
147.8.176.112	TESTINGICDFI-PC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / Dell device	
147.8.176.114	–	Searching for KWCCHAN-PC (Domain Controller)	Message using NBNS	–	
147.8.176.118	–	Running SSH on port 22	SSH connection from 147.8.178.254	–	
147.8.176.145	–	–	Requesting for 147.8.176.146 using ARP request	–	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.176.146	–	–	Wanted by 147.8.176.145 through ARP request	–	
147.8.176.196	–	–	Referred by ARP broadcast (requested by 147.8.178.15	–	
147.8.176.197	KMBT69E8F2	Server Type: 0x00000303, Workstation, Server, Member, Print	Host Announcement using BROWSER	Printer from KONICA MINOLTA HOLDINGS, INC.	
147.8.176.199	–	Searching for a Internet Gateway Device	Messages using SSDP	MSI device	
147.8.176.221	lg102-pschan	Using Dropbox's LAN sync feature / Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Messages using Dropbox LAN Sync Discovery Protocol / Host Announcement using BROWSER	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.19	CSISNAS2	Server Type: 0x00869007, Workstation, Server, SQL, NT Workstation, NT Server, Backup Browser, Master Browser, DFS	Local Master Announcement using BROWSER	Windows Server 2003 R2 or Windows Server 2003 / Device from BUFFALO.INC	
147.8.177.21	TESTWINS2012	Server Type: 0x00009007, Workstation, Server, SQL, NT Workstation, NT Server	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / Device from PCS Systemtechnik	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.177.22	–	Querying about CSISNAS2(Server Service)	Message using NBNS	Device from PCS Systemtechnik	
147.8.177.24	TFWONGATCECID	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Searching for Internet Gateway Device	Host Announcement using BROWSER / SSDP search messages	Windows 7 / Dell device	
147.8.177.25	–	–	Referred by ARP broadcast (requested by 147.8.178.15	–	
147.8.177.28	NPI39E91F.local	Printer	Messages using mDNS	HP LaserJet 2300 series	
147.8.177.29	YXFANGPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.37	CPMENGPC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.42	–	Searching for media server / media renderer	Messages using SSDP	HP device	
147.8.177.51	–	Notifying the network that this is a media server / content directory / connection manager	SSDP Notify messages	Windows 8.1 / Dell device	
147.8.177.54	ARLIN	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.177.55	YDZHENG2PC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.56	CB411-COMPVISION	Server Type: 0x00849a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Master Browser, DFS	Local Master Announcement using BROWSER protocol	IBM device	
147.8.177.59	–	Searching for Internet Gateway Device / Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol and SSDP	HP device	
147.8.177.63	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Acer device	
147.8.177.70	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	HP device	
147.8.177.73	–	–	Referred by ARP broadcast (requested by 147.8.178.15	–	
147.8.177.85	XLZHUPC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.177.87	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.177.94	JYANG2PC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.177.96	LYMOPC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.177.97	YLCAIPC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.100	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.177.105	IMINKINPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.115	MYANGPC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.177.116	CHDHUNGPC	Server Type: 0x00031003, Workstation, Server, NT Workstation, Potential Browser, Backup Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.177.127	CZZHANGPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.177.148	YTYEPC	Server Type: 0x00011203, Workstation, Server, Print, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.149	HWANG	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	Device from Universal Global Scientific Industrial Co., Ltd. / Windows XP	
147.8.177.156	JMSHIPC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser / Searching for name PGPC2984 (Workstation/Redirector) and Internet Gateway Device	Host Announcement using BROWSER / NBNS and SSDP messages	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.177.158	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.177.161	SFJIANGPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.165	–	Looking for services related to Apple's mobile device management or related functionalities	Messages using mDNS query	–	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.177.170	XJZHUPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.177.172	QHSUNPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.177.174	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	HP device	
147.8.177.178	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	HP device	
147.8.177.180	XXFANPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.182	–	–	–	Dell device	
147.8.177.186	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	HP device	
147.8.177.188	HLI2PC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.196	JPDUANPC	Server Type: 0x00001003, Workstation, Server, NT Workstation	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.177.202	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Device from Universal Global Scientific Industrial Co., Ltd.	
147.8.177.205	YWANGPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.213	–	Media renderer	SSDP messages	Device from Universal Global Scientific Industrial Co., Ltd.	
147.8.177.214	–	–	Referred by ARP broadcast (requested by 147.8.178.15)	–	
147.8.177.216	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Device from Universal Global Scientific Industrial Co., Ltd.	
147.8.177.221	YBTANGPC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser / Looking for multiple names (e.g., zkyrqzwmss)	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.177.223	YKLAM2PC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / Device from Universal Global Scientific Industrial Co., Ltd.	
147.8.177.227	WTTUPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.228	CMLEUNG2PC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / MSI device	
147.8.177.229	SLHOPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Searching for media server / media renderer	Host Announcement using BROWSER / SSDP search messages	Windows 7 or Windows Server 2008 R2 / Device from Universal Global Scientific Industrial Co., Ltd.	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.177.230	XHJIAPC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.232	–	Looking for services related to Apple's mobile device management or related functionalities / Using Dropbox's LAN sync feature	Messages using mDNS query and Dropbox LAN Sync Discovery Protocol	HP device	
147.8.177.233	JZQINPC	Server Type: 0x00001003, Workstation, Server, NT Workstation / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	Dell device / Windows 7 or Windows Server 2008 R2	
147.8.177.241	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	HP device	
147.8.177.242	HWUPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.177.243	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	HP device	
147.8.177.245	YWZHANG2PC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.177.252	SHCHANPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.177.253	RBLIPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature / Using Platinum UPnP SDK (Platinum/1.0.4.11) / SHPlayer UPnP Media Server	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol / UPnP Device Description transmitted in TCP stream 35	HP device / Windows 7 or Windows Server 2008 R2	
147.8.178.15	–	–	–	Oracle device	
147.8.178.23	lg102a.local	Printer	Messages using mDNS	HP LaserJet 2420	
147.8.178.24	WINBACKUP	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows XP / Device from Universal Global Scientific Industrial Co., Ltd.	
147.8.178.27	–	Querying about CB411-COMPVISIO and HKUCS	NBNS messages	Device from PCS Systemtechnik	
147.8.178.32	hw501a.local	Printer	Messages using mDNS	HP LaserJet P3005	
147.8.178.33	NPI87FCC4.local	–	mDNS query from 147.8.177.182	–	
147.8.178.34	lg101a.local	Printer	Messages using mDNS	HP LaserJet 2300L	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.178.35	NPI23A4A4.local	Printer	Messages using mDNS	HP LaserJet P3005	
147.8.178.39	hw324a.local	Printer	Messages using mDNS	HP LaserJet 4100 Series	
147.8.178.107	–	Suspicious SYN flood attack to 147.8.178.220 / Service misconfiguration	High volume of SYN requests	Dell device	
147.8.178.112	–	–	Referred by ARP broadcast (requested by 147.8.178.15)	–	
147.8.178.125	–	–	Referred by ARP broadcast (requested by 147.8.178.15)	–	
147.8.178.127	–	Trying to contact a remote license server through a UDP broadcast to port 1947	UDP broadcast to port 1947	MSI device	
147.8.178.133	–	–	–	VMware	
147.8.178.142 or 147.8.178.206	CISC-CRAWLER02	Server service	NBNS packets	Dell device	
147.8.178.152	WALLACE-PC	Server Type: 0x00011203, Workstation, Server, Print, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature / Communicating with Memcached caching system	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol / UDP broadcast to port 1211	Dell device / Windows 7 or Windows Server 2008 R2	
147.8.178.153	–	Using Dropbox's LAN sync feature / Searching for Internet Gateway Device	Messages using Dropbox LAN Sync Discovery Protocol / SSDP search message	Dell device	
147.8.178.165	–	Trying to contact a remote license server through a UDP broadcast to port 1947 / Searching for name wpad	UDP broadcast to port 1947 / LLMNR packets	Device from Wistron InfoComm(Kunshan)Co.,Ltd.	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.178.172	ATHENA	Server Type: 0x00011007 (Workstation, Server, SQL, NT Workstation, Potential Browser)	Keep getting ICMP request from 192.168.93.131 / Keep getting 0x19(FIN, PSH, ACK) TCP packets in port 49159 from 147.8.179.15:80	Windows XP (5.1)	
147.8.178.177	–	–	–	HP device	
147.8.178.179	–	–	Referred by ARP broadcast (requested by 147.8.178.15)	–	
147.8.178.206 or 147.8.178.142	CISC-CRAWLER02	Server service	NBNS packets	Dell device	
147.8.178.209	–	Announcing the establishment of services to the multicast group	SSDP packets	NAS	
147.8.178.216	–	Trying to contact a remote license server through a UDP broadcast to port 1947	UDP broadcast to port 1947	Dell device	
147.8.178.218	–	Extremely high volume of same-size UDP packets every 0.0005s from 12.401672s to 181.054703 (duration 168.653031s) (UDP flood)	UDP packets to 147.8.178.220:8888	Dell device	
147.8.178.219	–	Trying to contact a remote license server through a UDP broadcast to port 1947	UDP broadcast to port 1947	Device from Universal Global Scientific Industrial Co., Ltd.	
147.8.178.220	–	Experiencing TCP SYN flood from 147.8.178.107 and UDP flood from 147.8.178.218	TCP SYN packets and UDP packets	Dell device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.178.222	USER-HP	Server Type: 0x00011203, Workstation, Server, Print, NT Workstation, Potential Browser / Using Gnutella	Host Announcement using BROWSER / UDP packets to port 6346	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.178.223	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.178.225	CBCHANPC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser / Trying to contact a remote license server through a UDP broadcast to port 1947	Host Announcement using BROWSER / UDP broadcast to port 1947	Windows XP / Device from Universal Global Scientific Industrial Co., Ltd.	
147.8.178.227	CISC-CRAWLER01	Server Type: 0x00001003, Workstation, Server, NT Workstation	Host Announcement using BROWSER	Windows XP / Dell device	
147.8.178.228	–	Searching for media server / media renderer	Messages using SSDP	Dell device	
147.8.178.229	–	Searching for media server / media renderer	Messages using SSDP	Dell device	
147.8.178.235	–	Announcing the establishment of services to the multicast group	SSDP packets	NAS	
147.8.178.236	bio-nas2.local	NAS device	Message using mDNS	NAS from Synology Incorporated	
147.8.178.239	–	Router	ICMP router advertisement packets	Dell device	
147.8.178.241	–	–	–	Dell device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.178.248	DiskStation.local	Supporting Apple Filing Protocol over TCP ($_{a}fpovertcp$)	mDNS packets	NAS from Synology Incorporated	
147.8.178.253	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	MSI device	
147.8.178.254	–	Running application using SSH	SSH connection to 147.8.176.118	HP device	
147.8.179.42	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	MSI device	
147.8.179.46	–	–	Referred by ARP broadcast (requested by 147.8.178.15)	–	
147.8.179.48	–	–	Referred by ARP broadcast (requested by 147.8.178.15)	–	
147.8.179.53	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	MSI device	
147.8.179.56	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.179.74	–	–	–	Dell device	
147.8.179.81	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Device from Universal Global Scientific Industrial Co., Ltd.	
147.8.179.82	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.179.84	–	Using Dropbox's LAN sync feature / Sending SSDP discovery request for a device that is the root of a device tree / Sending messages to probable HP printers	Messages using Dropbox LAN Sync Discovery Protocol and SSDP / UDP broadcast to port 3702	Dell device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.179.105	–	–	SSDP notify messages	Linux / Network camera (or gateway) from fitivision technology Inc.	
147.8.179.106	–	–	SSDP notify messages	Linux / Network camera (or gateway) from fitivision technology Inc.	
147.8.179.131	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.179.140	–	Using Dropbox's LAN sync feature / Sending SSDP discovery request for a device that is the root of a device tree / Sending messages to probable HP printers	Messages using Dropbox LAN Sync Discovery Protocol and SSDP / UDP broadcast to port 3702	Dell device	
147.8.179.141	–	Media server	SSDP messages	MSI device	
147.8.179.144	–	Announcement about domain WORKGROUP and Master Browser Server Name (PEREA) / Sending messages to probable HP printers	Message using BROWSER protocol / UDP broadcast to port 3702	MSI device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.179.150	ZYLUPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.179.151	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	MSI device	
147.8.179.153	CZHANG2PC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.179.156	XMCUIPC	Server Type: 0x00011203, Workstation, Server, Print, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.179.157	CYYEUNGPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Sending messages to probable HP printers	Host Announcement using BROWSER / UDP broadcast to port 3702	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.179.158	FLIANGPC	Server Type: 0x00011203, Workstation, Server, Print, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.179.159	–	Supporting UPnP through QQ Music	SSDP messages	HP device	
147.8.179.162	–	–	Referred by ARP broadcast (requested by 147.8.178.15)	–	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.179.163	LZHANG3PC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.179.165	JXWANGPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.179.167	PGPC159F	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.179.198	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.179.205	–	Using Dropbox's LAN sync feature / Running multiple services (e.g., media server, connection manager)	Messages using Dropbox LAN Sync Discovery Protocol and SSDP	Device from LCFC(HeFei) Electronics Technology co., ltd / Windows 8.1	
147.8.179.210	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Device from RADSTONE TECHNOLOGY	
147.8.179.217	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.179.224	WZHANG2PC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.179.225	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	Dell device	
147.8.179.227	–	Using Dropbox's LAN sync feature / Looking for ONWITH.NET and xn–7ou354dv5jrrc	Messages using Dropbox LAN Sync Discovery Protocol, NBNS and LLMNR	HP device	
147.8.179.228	HPANPC	Server Type: 0x00001003, Workstation, Server, NT Workstation / Searching for Internet Gateway Device	Host Announcement using BROWSER / SSDP messages	Windows XP / Dell device	
147.8.179.231	–	Multiple UDP packet from port 8889 to 224.0.0.88:8000 every 10s, the TTL is larger than 1 (maybe misconfiguration)	UDP packets	Dell device	
147.8.179.235	YTYUEPC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.179.236	–	Using Dropbox's LAN sync feature	Messages using Dropbox LAN Sync Discovery Protocol	HP device	
147.8.179.240	YPLIPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Searching for Internet Gateway Device	Host Announcement using BROWSER / SSDP messages	Windows 7 or Windows Server 2008 R2 / HP device	

Continued on next page

Table 2: Evidence Table (Public IP Addresses) (Continued)

IP Address	Host Name	Function	Digital Evidence	Type	Priority
147.8.179.242	GMJINGPC	Server Type: 0x00011003, Workstation, Server, NT Workstation, Potential Browser / Using Dropbox's LAN sync feature	Host Announcement using BROWSER / Messages using Dropbox LAN Sync Discovery Protocol	HP device / Windows 7 or Windows Server 2008 R2	
147.8.179.244	–	Sending messages to probable HP printers	UDP broadcast packets to port 3702	HP device	
147.8.179.245	GBLI-PC	Server Type: 0x00011007, Workstation, Server, SQL, NT Workstation, Potential Browser	Host Announcement using BROWSER	Windows 7 or Windows Server 2008 R2 / HP device	
147.8.179.254	NPIA4138B.local	Printer	mDNS messages	HP LaserJet P3005	
147.8.179.255	–	Broadcast address of 147.8.176.0 /22	–	–	
147.8.255.255	–	Broadcast address of 147.8.0.0 /16	–	–	
224.0.0.1	–	Used by BJNP (Canon printer command)	–	–	
224.0.0.88	–	Reserved for multicast addresses	–	–	
224.0.0.251	–	Used by mDNS	–	–	
224.0.0.252	–	Used by Link-Local Multicast Name Resolution (LLMNR)	–	–	
224.0.1.60	–	Used by Service Location Protocol (SRVLOC)	–	–	
239.235.0.8	–	Multicast	–	–	
239.255.255.250	–	Used by Simple Service Discovery Protocol (SSDP)	–	–	
255.255.255.255	–	Broadcast	–	–	

Note: – means no specific information available

3 Investigation on Attack

3.1 Hosts List

The analysis of the pcap file revealed several hosts with a substantial amount of network traffic, constituting more than 1% of the captured packets. The details of these hosts, including IP and MAC addresses, are tabulated as follows.

IP Address	MAC Address	Count	Rate (ms)	Percent	Burst Rate	Burst Start
All Addresses	–	744827	3.4890	100%	7.4300	6.635
192.168.93.131	00:0c:29:db:d0:dc	410761	1.9242	55.15%	7.4300	6.635
192.168.56.1	00:50:56:e0:26:7f (MAC address of router 192.168.93.2) / 00:23:ae:74:d0:5e	408635	1.9142	54.86%	7.4200	6.635
147.8.178.220	90:b1:1c:84:73:43	330518	1.5483	44.38%	2.7900	147.695
147.8.178.218	90:b1:1c:80:23:c4	330193	1.5467	44.33%	2.3400	154.870

3.2 Attack Classification

In the obtained pcap file, three kinds of Denial of Service (DoS) attacks are prevalent, namely: SYN flood, UDP flood, and ICMP flood.

3.2.1 SYN Flood

The SYN flood attack is a form of DoS attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

The I/O graph of the SYN flood attack is shown in Figure??.

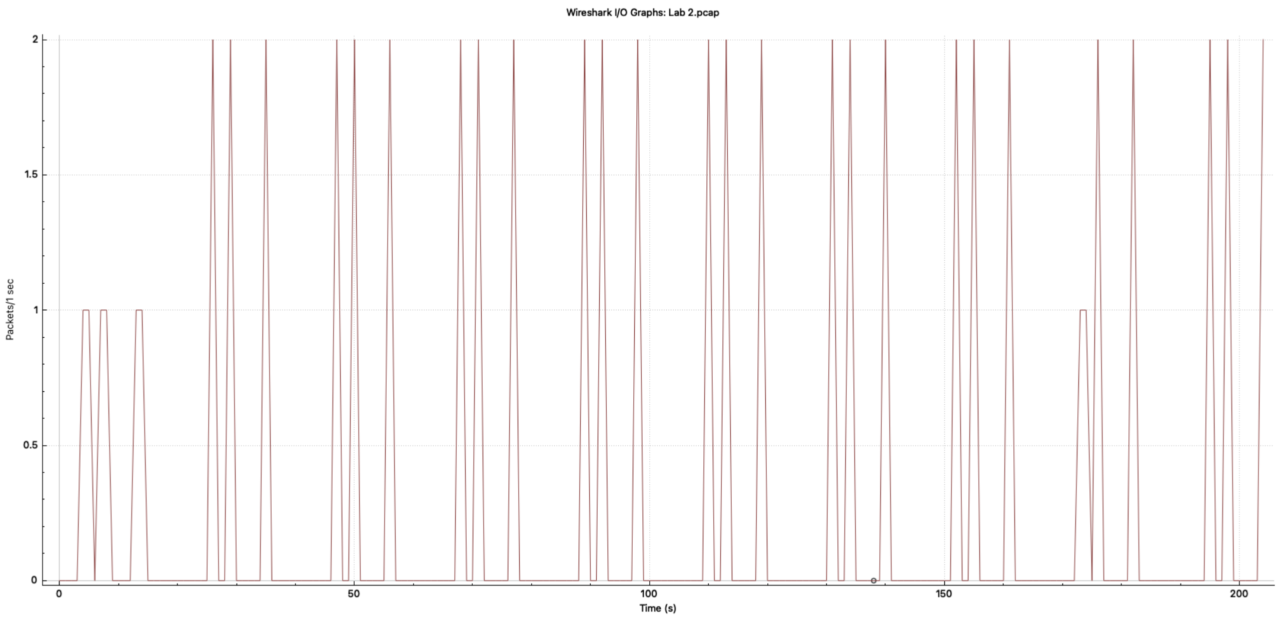

Figure 1: I/O Graph of SYN Flood Attack

Based on the packet captures, the SYN flood attack was observed from the IP address 147.8.178.107 to 147.8.178.220. In total of 60 packets (4 kB) were sent from 147.8.178.107, starting from 4.969162s, during a duration of 199.2520s. The TCP SYN packets were directed towards ports 9990 and 9991. Initially, a packet originated from port 58274 to port 9990, followed approximately 0.1 seconds later by another packet from port 58275 to port 9991. Subsequently, a 3-second pause was observed before the attacker dispatched two identical packets in the same sequence. This pattern was repeated after a 6-second interval. Eventually, the attacker executed the aforementioned sequence again following a 12-second delay. This activity was consistently performed ten times, spanning from October 29, 2022, at 15:16:39.505950000 HKT to October 29, 2022, at 15:19:58.757932000 HKT.

However, this attack was not intense enough to cause a significant impact on the target system. As based on the information obtained from the packet captures, the target system 147.8.178.220 still responded to other network traffic during the attack. The pattern of the attack resembles a normal network traffic pattern. There's a chance that the target system was running a service that was listening on the targeted ports previously. Out of some reason, these ports were no longer in use, and the attacker's system was still trying to connect to these ports.

In a nutshell, the suspicious SYN flood attack was not successful in causing a significant impact on the target system. It might very well be a false positive.

3.2.2 UDP Flood

The UDP flood attack is a form of DoS attack in which an attacker sends a large number of User Datagram Protocol (UDP) packets to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

The I/O graph of the UDP flood attack is shown in Figure??.

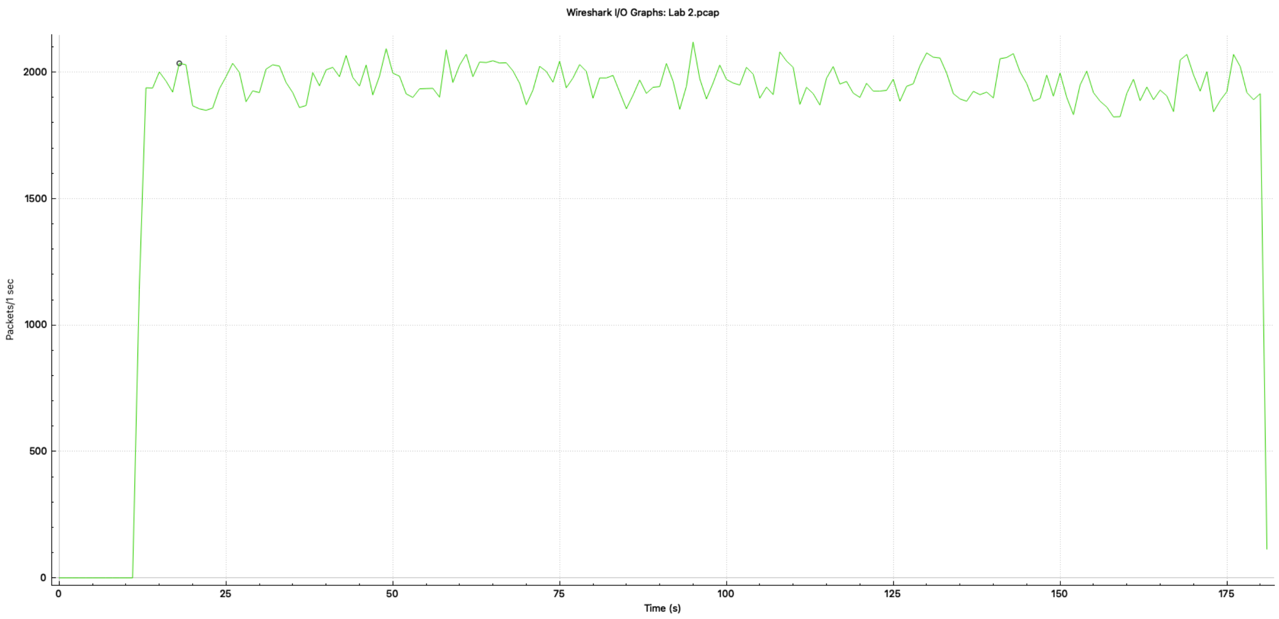

Figure 2: I/O Graph of UDP Flood Attack

Analysis of the pcap file revealed that the attacker 147.8.178.218 dispatched 330,192 UDP packets of uniform size to port 8888 on the victim's system 147.8.178.220. Each packet contributed to a cumulative data volume of 20MB. The assault commenced at 12.401672 seconds, enduring for 168.6530 seconds, with UDP packets being sent at intervals ranging from 0.0005 to 0.001 seconds.

This is a typical UDP flood attack, which is so intense that it comprises 44.1% of the total network traffic.

However, the target system 147.8.178.220 still was able to respond to other network traffic during and after the attack.

3.2.3 ICMP Flood

The ICMP flood attack is a form of DoS attack in which an attacker aims to overwhelm a target's system by flooding it with ICMP echo-requests.

The I/O graph of request packets of the ICMP flood attack is shown in Figure??.

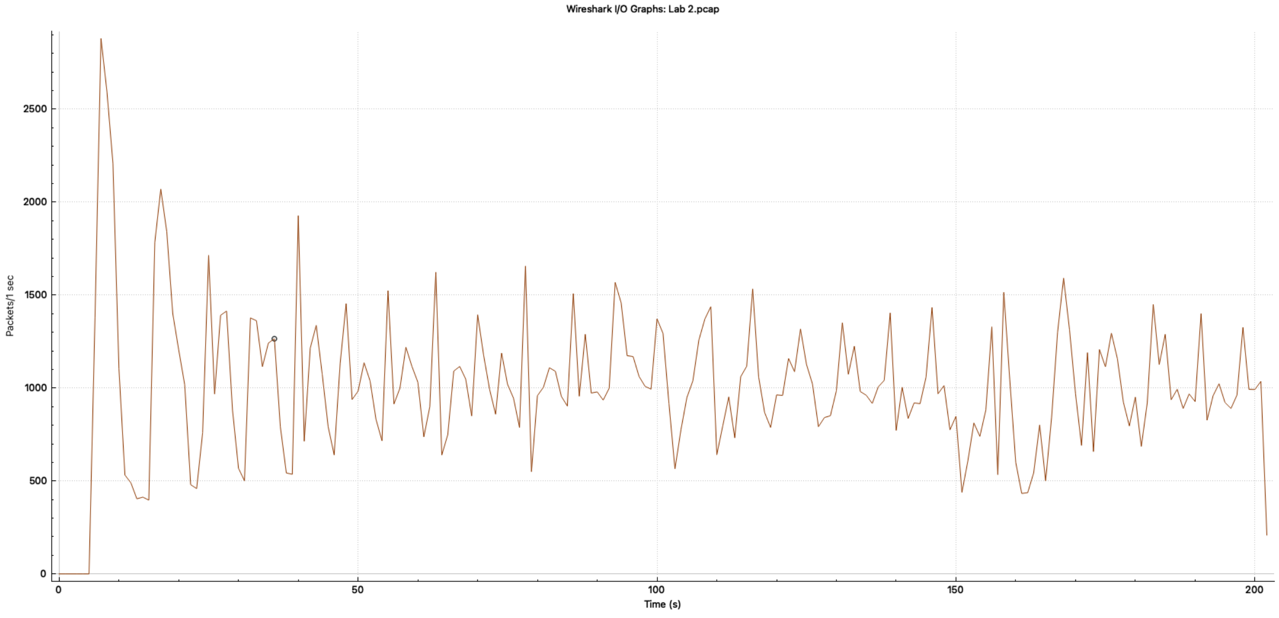

Figure 3: I/O Graph of ICMP Flood Attack (Request Packets)

The I/O graph of reply packets of the ICMP flood attack is shown in Figure??.

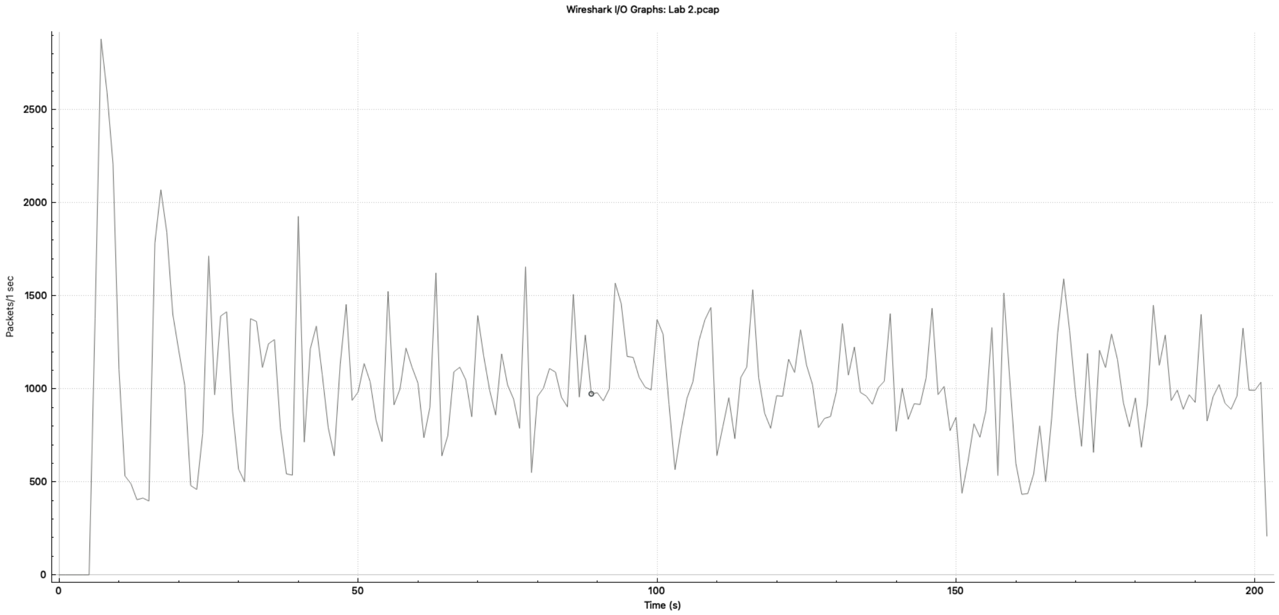

Figure 4: I/O Graph of ICMP Flood Attack (Reply Packets)

Combine the I/O graph of request and reply packets, the graph is shown in Figure??.

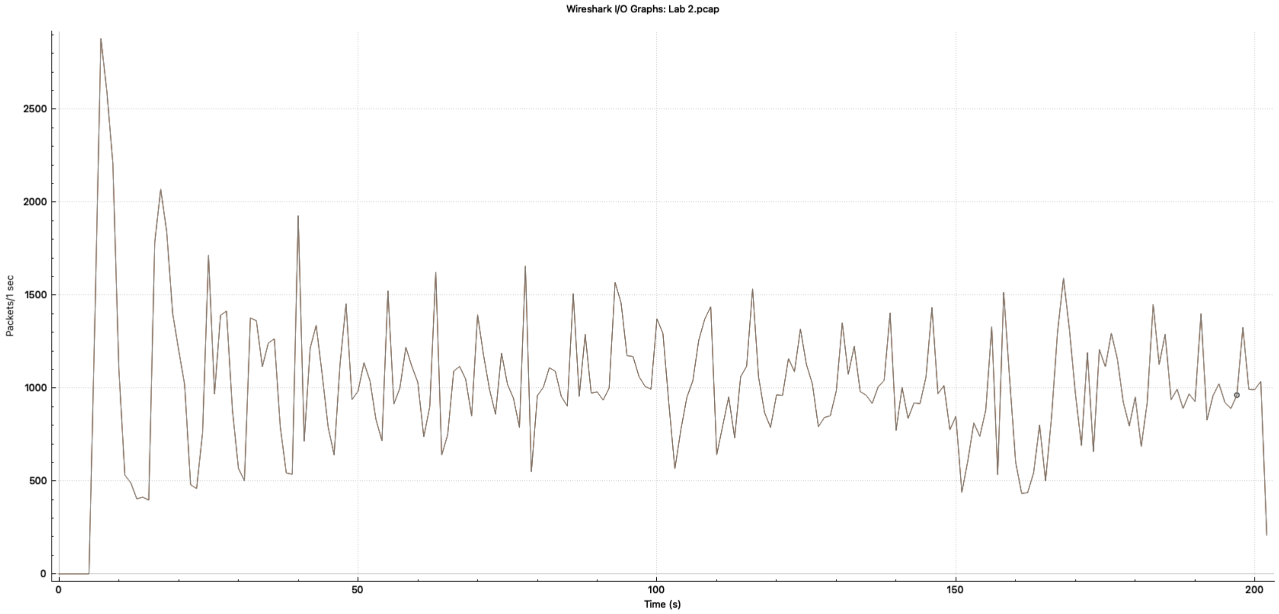

Figure 5: I/O Graph of ICMP Flood Attack (Combined)

The pcap file revealed that the attacker 192.168.93.131 sent 408,614 ICMP packets to the victim's system 192.168.56.1. The ICMP flood attack commenced at 6.589908 seconds, lasting for 195.7510 seconds, with a total of 17MB data transmitted over the network. The rate of ICMP request and reply packets fluctuated between 1,000 to 4,000 per second, peaking at nearly 6,000 packets per second. Interestingly, the frequency of reply packets per second did not significantly increase as the attack progressed. A comparison of the input/output graph for the number of request packets per second over time with that of the reply packets per second reveals a substantial overlap, indicating no notable impact on the victim. Further analysis of the evidence table reveals that the IP address 192.168.93.2 serves as the router for the subnet 192.168.93.0/24. This observation suggests that the router remained operational and unaffected by the attack.

3.2.4 TCP FIN PSH ACK Flood

The TCP FIN PSH ACK flood attack has similar characteristics to the TCP SYN flood attack.

The I/O graph of the TCP FIN PSH ACK flood attack is shown in Figure??.

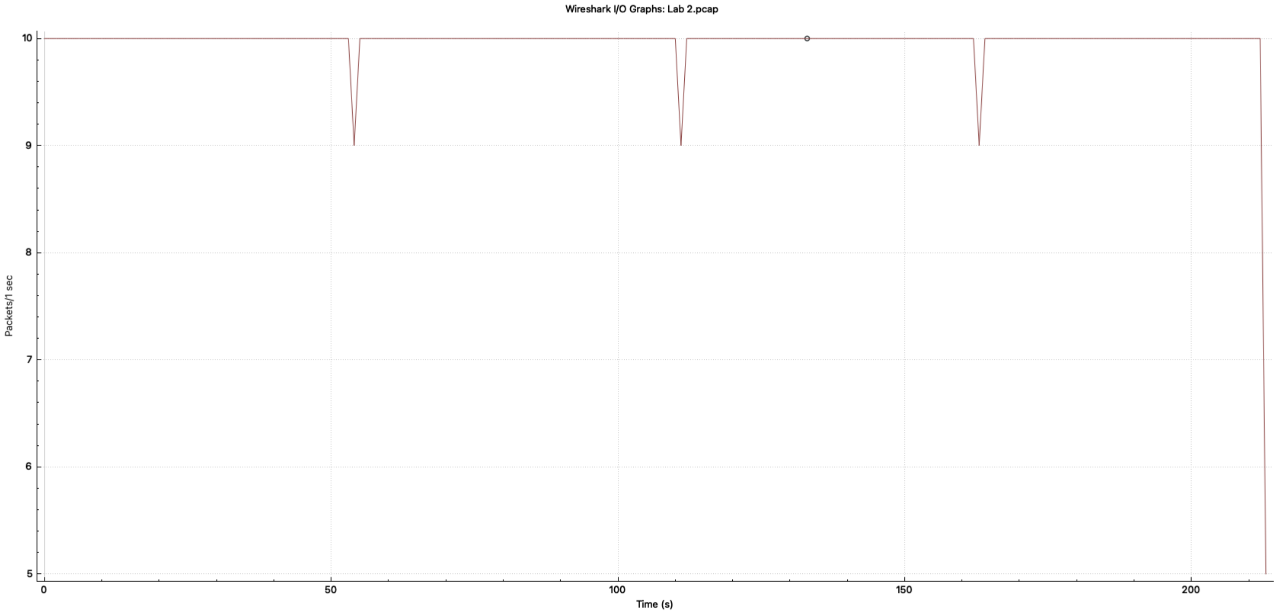

Figure 6: I/O Graph of TCP FIN PSH ACK Flood Attack

The IP address 147.8.179.15:80 was observed transmitting TCP [FIN, PSH, ACK] packets to 192.168.93.131:49159, starting from October 29, 2022, at 07:16:34.536788000 UTC until October 29, 2022, at 15:20:07.993527000 HKT, with a packet sent every 0.1 seconds, totaling 2,132 packets. No response was received from the receiver.

This pattern of persistent retransmissions could imply several underlying issues:

1. **Lack of Acknowledgment**: The continuous retransmission of [FIN, PSH, ACK] packets might suggest that the sender is not receiving the expected acknowledgment from the receiver. Normally, following a [FIN, ACK] transmission, a corresponding [FIN, ACK] reply from the receiver is anticipated, concluding with an [ACK] from the sender to gracefully terminate the connection. If the sender persistently retransmits the [FIN, PSH, ACK] packet, it may indicate the absence or mishandling of the final acknowledgment from the receiver.

2. **Network Issues**: Frequent retransmissions may also signal network-related problems such as congestion, high latency, or packet loss, potentially causing repeated packet losses, including acknowledgments, and forcing the sender to retransmit to ensure proper connection closure.

3. **Configuration Errors or Software Bugs**: The observed behavior could stem from network device misconfigurations or software bugs affecting TCP connection management, e.g., issues in NAT devices, firewalls, or the TCP stack leading to incorrect TCP teardown handling.

4. **Potential Malicious Activity**: Such patterns might indicate malicious attempts, like a denial-of-service (DoS) attack.

Despite these anomalies, the router and 192.168.93.131 appeared unaffected, as other activities on 192.168.93.131 proceeded normally.

3.3 Other Suspicious Activities

3.3.1 SSDP Flood

An SSDP (Simple Service Discovery Protocol) flood attack is a type of Distributed Denial of Service (DDoS) attack. It exploits the SSDP protocol, which is used for the discovery of UPnP (Universal Plug and Play) devices on a network. Attackers send a large number of SSDP discovery requests to a target's network using spoofed IP addresses. These requests are directed at UPnP devices, which then respond to the spoofed addresses, overwhelming the target with traffic and potentially causing disruption or denial of service.

The I/O graph of the suspicious SSDP flood attack is shown in Figure??.

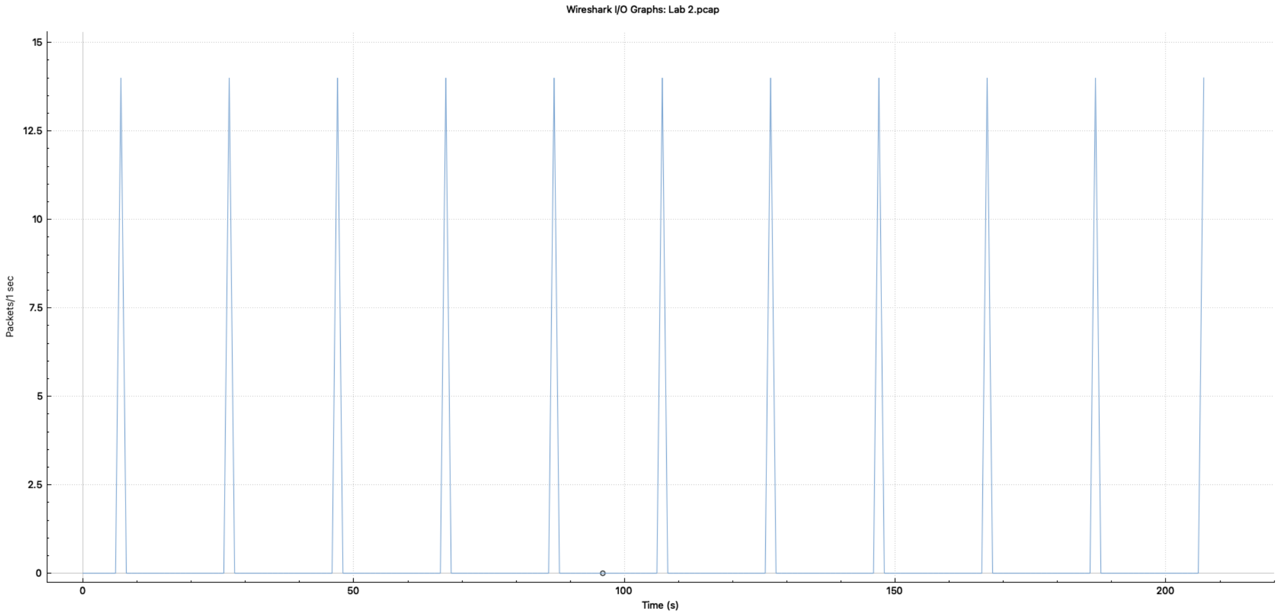

Figure 7: I/O Graph of SSDP Flood Attack

The suspicious activity, identified as an SSDP flood attack, commenced on October 29, 2022, at 15:16:41.762146000 HKT, with the source 147.8.179.159 dispatching SSDP NOTIFY packets at 20-second intervals, releasing 14 packets with each instance. This episode concluded on October 29, 2022, at 15:20:01.853385000 HKT.

Notably, the initiating device, 147.8.179.159, did not receive any responses from other UPnP devices, and the NOTIFY messages were attributed to the QQ Music application, suggesting legitimate usage. However, the QQ Music application's frequency of SSDP NOTIFY message transmission significantly exceeded that of other devices. This pattern could either indicate a normal behavior for the QQ Music application, characterized by a high frequency of SSDP NOTIFY message transmission, or represent a potential SSDP flood attack.

3.4 Victim Information

Based on the Attack Classification section??, the victim of UDP flood attack is 147.8.178.220, the victim of ICMP flood attack is 192.168.56.1,

3.5 Attacker Information

The attacker's IP addresses are 147.8.178.218, suspected to be the source of the UDP flood attack, and 192.168.93.131 , suspected to be the source of the ICMP flood attack.

4 Investigative Reconstruction

Upon scrutinizing the sequence of network events, a timeline of the attack was reconstructed, revealing the methods and progression of the malicious activities. This reconstruction is crucial for understanding the attack's impact and for developing future mitigation strategies.