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:

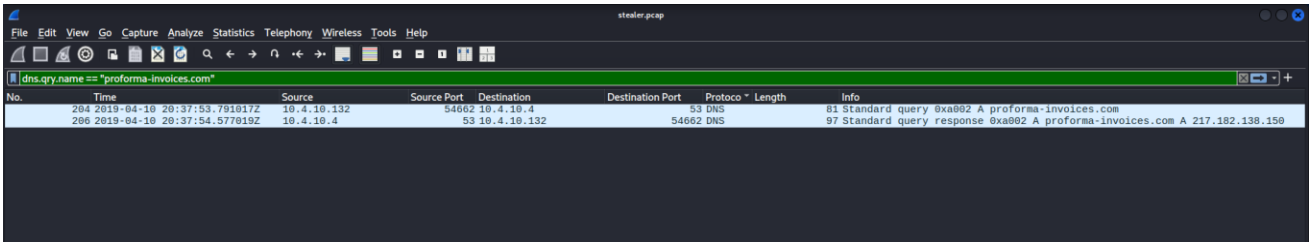
1. **DNS Resolution: Suspicious Domain → Malicious IP**

    Wireshark filter: dns.qry.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.



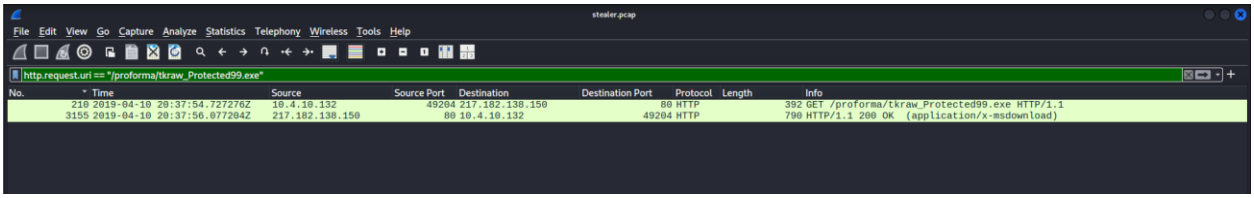
2. Payload Delivery: HTTP Download of Executable

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.



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).

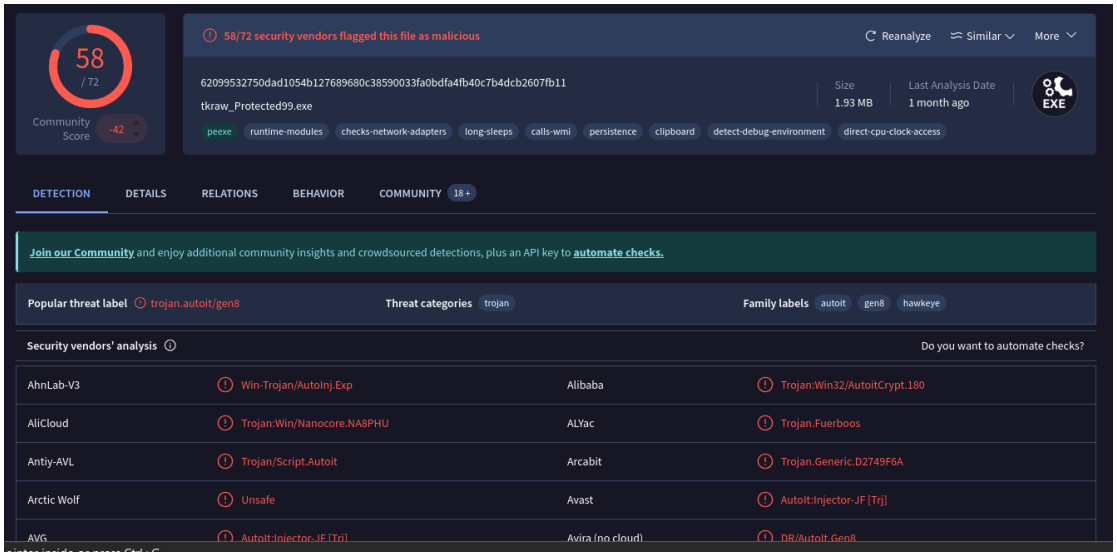
Hashes

- **MD5:** 71826ba081e303866ce2a2534491a2f7
- **SHA1:** b482d64a43f6bfbf758166ecba680b7f0c59a4f7
- **SHA256:** 62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4dcb2607fb11

File size consistency

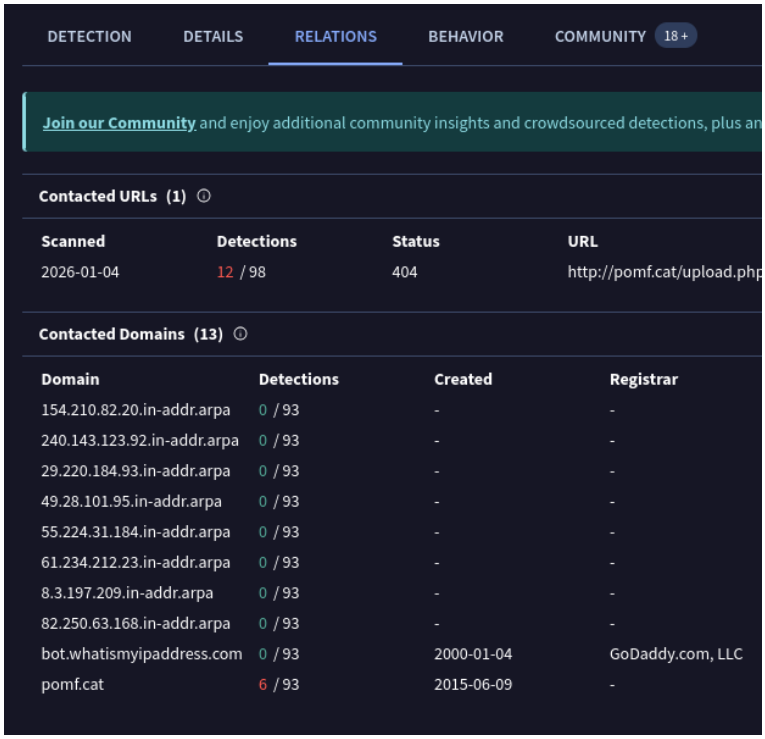
- VirusTotal size: **1.93 MB (2,025,472 bytes)**
- Wireshark HTTP object export size: **~2,025 KB**

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



Basic properties

MD5	71826ba081e303866ce2a2534491a2f7
SHA-1	b482d64a43f6bfbf758166ecba680b7f0c59a4f7
SHA-256	62099532750dad1054b127689680c38590033fa0bdfa4fb40c7b4dcb2607fb11
Vhash	026056655d15156210b02002300a46z161d013zf2za0030e039z
Authentihash	1d50140145e3511ec4d3ea0cdffee93f66ffac580f86547749091441cd03bdf6
Imphash	afcdf79be1557326c854b6e20cb900a7
Rich PE header hash	a5d888b5a108c327d65f490cc1a712f2
SSDEEP	24576:EAHnh+eWsN3skA4RV1Hom2KXMmHa/F9OdaxwwHelbiZLpFC1XJLc/r7/vRP0r2dU:Th+ZkldoPK8Ya/6U
TLSH	T12695C0C6A3A980E2FE0677F79E1577C74B785A314532401D23AD3D59AE730F2412EAA3
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
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+

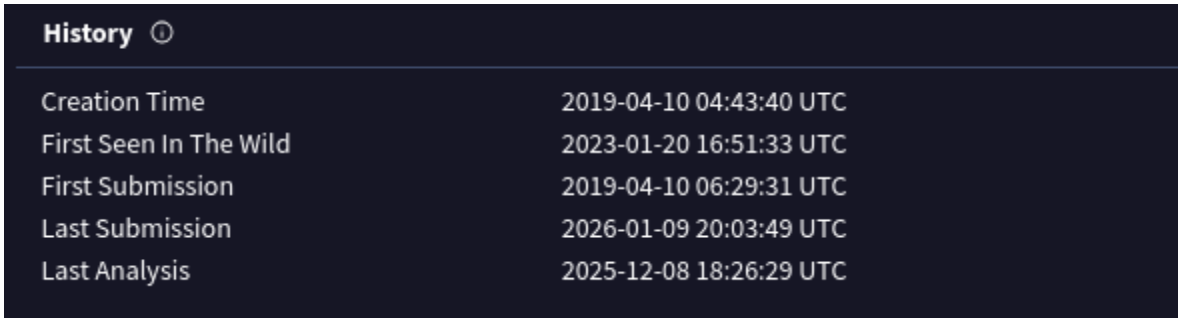
Join our Community and enjoy additional community insights and crowdsourced detections, plus an

Contacted URLs (1)

Scanned	Detections	Status	URL
2026-01-04	12 / 98	404	http://pomf.cat/upload.php

Contacted Domains (13)

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	-

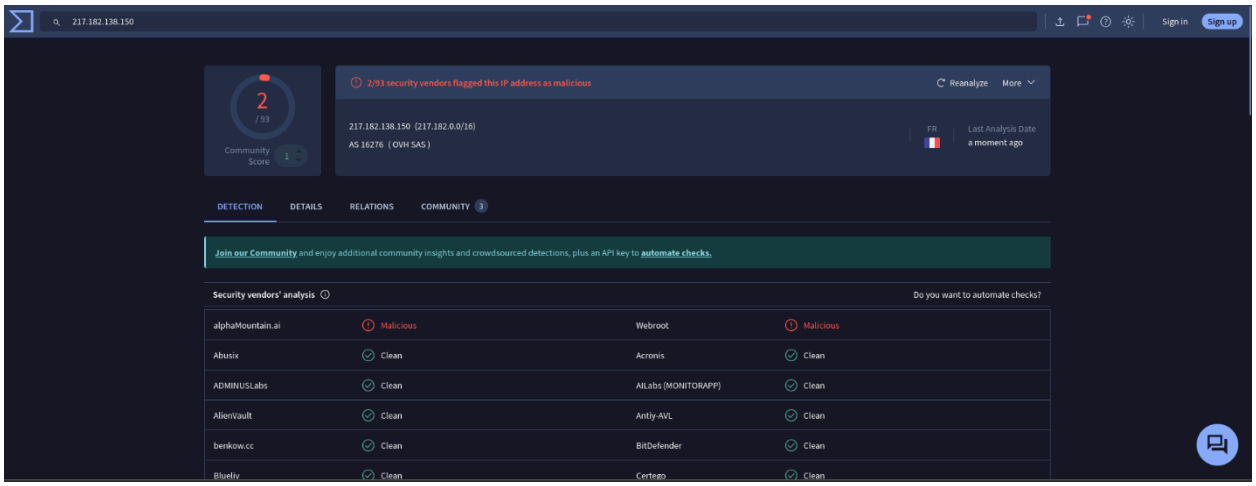


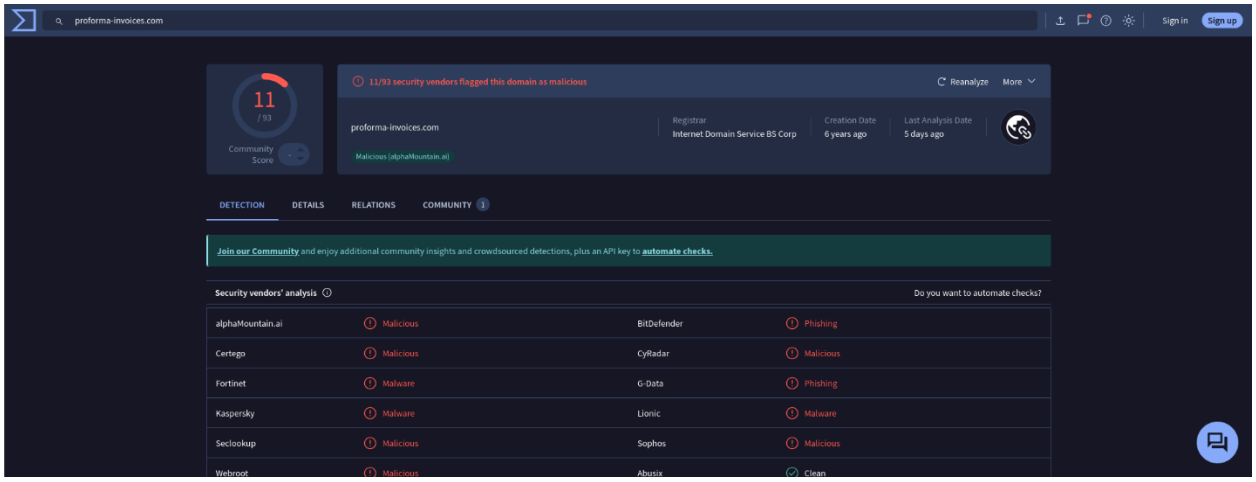
History

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**





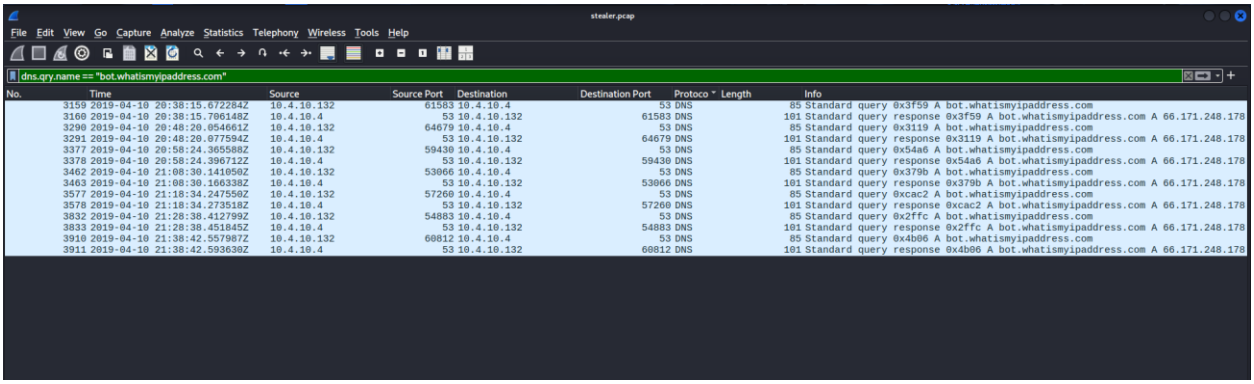
4. **Post-Download Behavior: External IP Check Domain**

   The PCAP shows repeated DNS queries for:

   - bot.whatismyipaddress.com

   Wireshark filter:

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



   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

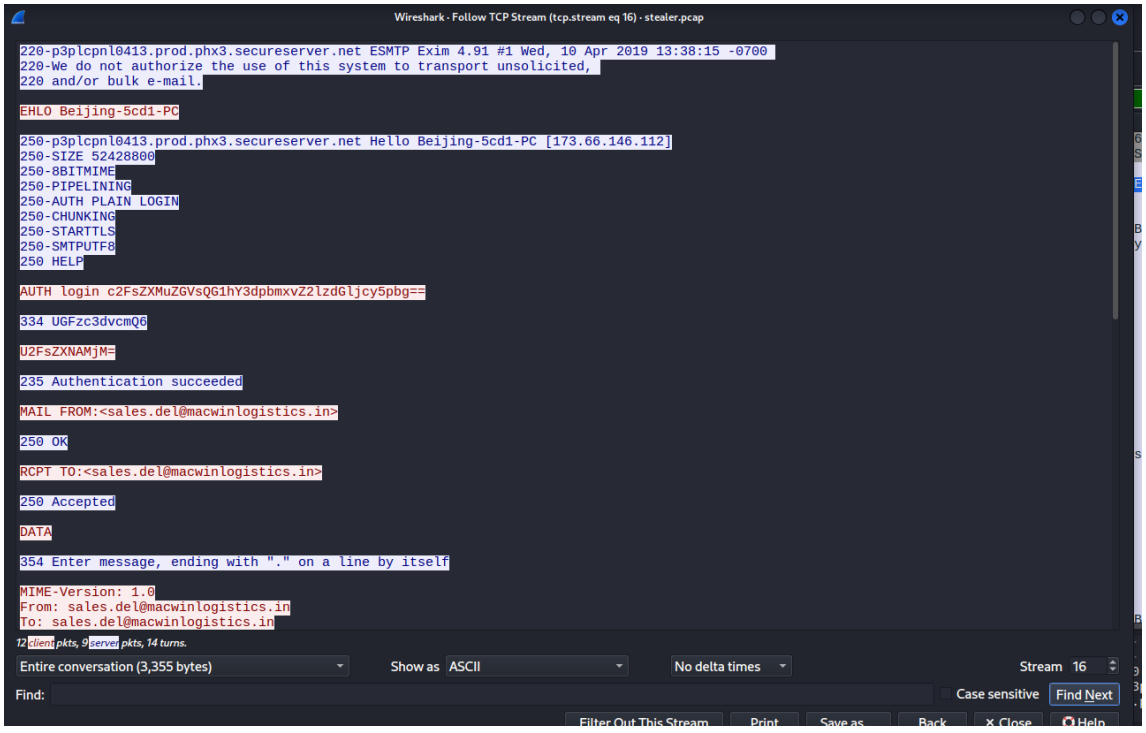
The message content (Base64 body) decodes to a HawkEye log header similar to:

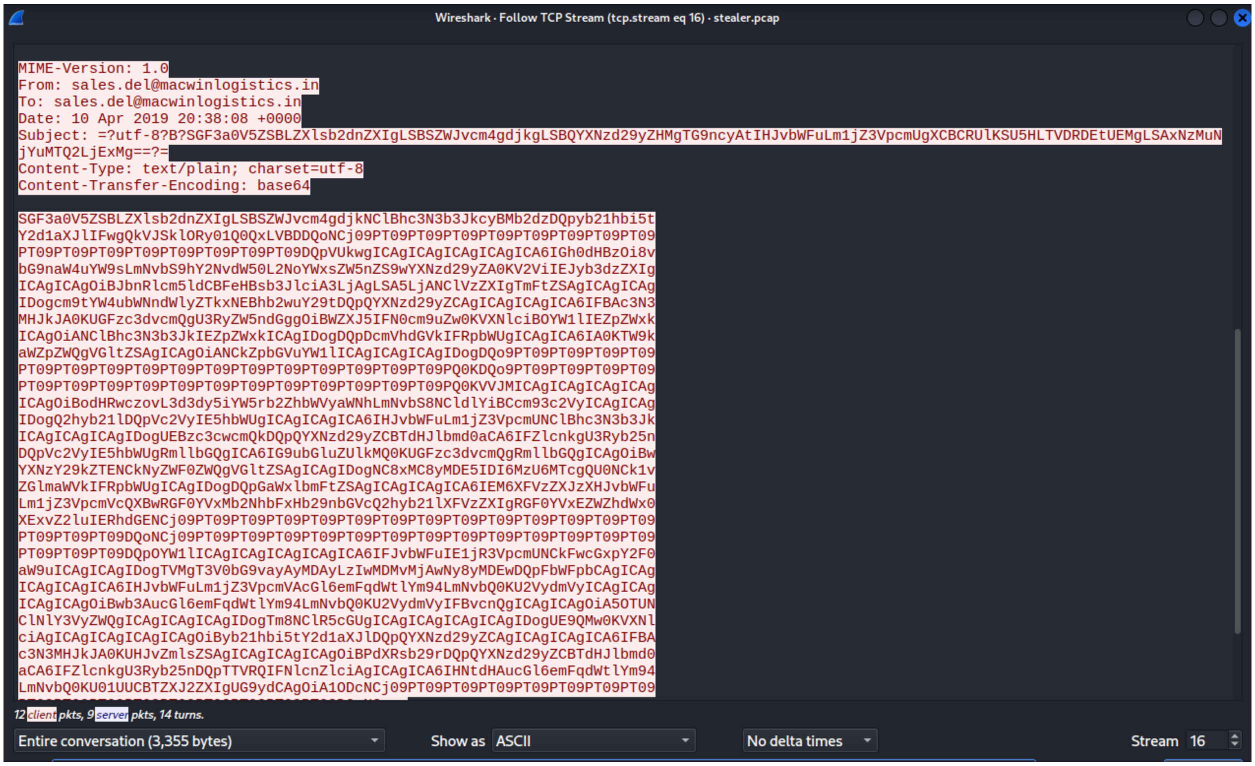
- HawkEye Keylogger - Reborn v9 - Passwords Logs – roman.mcguire \ BEIJING-5CD1-PC - 173.66.146.112

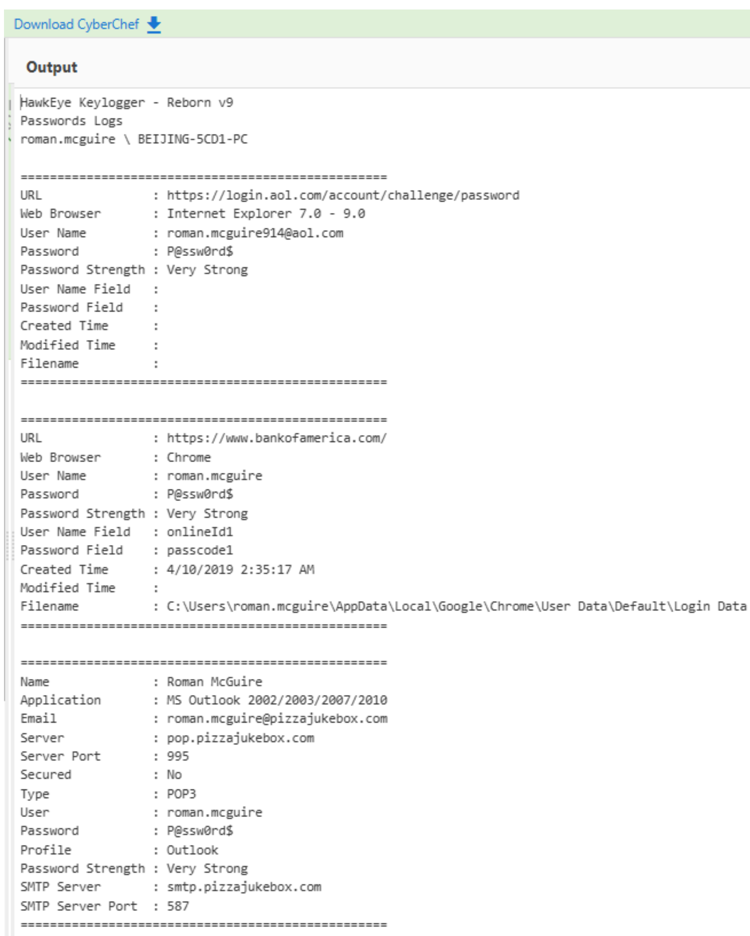
The body included multiple credential items (web logins + email client details).

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
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?SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gdjkgLSBQYXNzd29yZHMgTG9ncyAtIHJvbWFuLm1jZ3VpcmUgXCBCRUlKSU5HLTVDRDEtUEMgLSAxNzMuN
jYuMTQ2LjExMg==?=
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64
SGF3a0V5ZSBLZXlsb2dnZXIgLSBSZWJvcm4gdjkNClBhc3N3b3JkcyBMb2dzDQpyb21hbi5t
Y2d1aXJlIFwgQkVJSklORy01Q0QxLVBDDQoNCj09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09DQpVUkwgICAgICAgICAgICAgICA6IGh0dHBzOi8v
bG9naW4uYW9sLmNvbS9hY2NvdW50L2NoYWxsZW5nZS9wYXNzd29yZA0KV2ViIEJyb3dzZXIg
ICAgICAgOiBJbnRlcm5ldCBFeHBsb3JlciA3LjAgLSA5LjANClVzZXIgTmFtZSAgICAgICAg
IDogcm9tYW4ubWNndWlyZTkxNEBhb2wuY29tDQpQYXNzd29yZCAgICAgICAgICA6IFBAc3N3
MHJkJA0KUGFzc3dvcmQgU3RyZW5ndGggOiBWZXJ5IFN0cm9uZw0KVXNlciBOYW1lIEZpZWxk
ICAgOiANClBhc3N3b3JkIEZpZWxkICAgIDogDQpDcmVhdGVkIFRpbWUgICAgICA6IA0KTW9k
aWZpZWQgVGltZSAgICAgOiANCkZpbGVuYW1lICAgICAgICAgIDogDQo9PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PQ0KDQo9PT09PT09PT09PT09PT09PT09
PT09PT09PT09PT09PT09PT09PT09PT09PQ0KVVJMICAgICAgICAgICAgICAg
ICAgOiBodHRwczovL3d3dy5iYW5rb2ZhbWVyaWNhLmNvbS8NCldlYiBCcm93c2VyICAgICAg
IDogQ2hyb21lDQpVc2VyIE5hbWUgICAgICAgICA6IHJvbWFuLm1jZ3VpcmUNClBhc3N3b3Jk
ICAgICAgICAgIDogUEBzc3cwcmQkDQpQYXNzd29yZCBTdHJlbmd0aCA6IFZlcnkgU3Ryb25n
DQpVc2VyIE5hbWUgRmllbGQgICA6IG9ubGluZUlkMQ0KUGFzc3dvcmQgRmllbGQgICAgOiBw
YXNzY29kZTENCkNyZWF0ZWQgVGltZSAgICAgIDogNC8xMC8yMDE5IDI6MzU6MTcgQU0NCk1v
ZGlmaWVkIFRpbWUgICAgIDogDQpGaWxlbmFtZSAgICAgICAgICA6IEM6XFVzZXJzXHJvbWFu
Lm1jZ3VpcmVcQXBwRGF0YVxMb2NhbFxHb29nbGVcQ2hyb21lXFVzZXIgRGF0YVxEZWZhdWx0
XExvZ2luIERhdGENCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09DQoNCj09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09PT09
PT09PT09DQpOYW1lICAgICAgICAgICAgICA6IFJvbWFuIE1jR3VpcmUNCkFwcGxpY2F0
aW9uICAgICAgIDogTVMgT3V0bG9vayAyMDAyLzIwMDMvMjAwNy8yMDEwDQpFbWFpbCAgICAg
ICAgICAgICA6IHJvbWFuLm1jZ3VpcmVAcGl6emFqdWtlYm94LmNvbQ0KU2VydmVyICAgICAg
ICAgICAgOiBwb3AucGl6emFqdWtlYm94LmNvbQ0KU2VydmVyIFBvcnQgICAgICAgOiA5OTUN
ClNlY3VyZWQgICAgICAgICAgIDogTm8NClR5cGUgICAgICAgICAgICAgIDogUE9QMw0KVXNl
ciAgICAgICAgICAgICAgOiByb21hbi5tY2d1aXJlDQpQYXNzd29yZCAgICAgICAgICA6IFBA
c3N3MHJkJA0KUHJvZmlsZSAgICAgICAgICAgOiBPdXRsb29rDQpQYXNzd29yZCBTdHJlbmd0
aCA6IFZlcnkgU3Ryb25nDQpTTVRQIFNlcnZlciAgICAgICA6IHNtdHAucGl6emFqdWtlYm94
LmNvbQ0KU01UUCBTZXJ2ZXIgUG9ydCAgOiA1ODcNCj09PT09PT09PT09PT09PT09PT09PT09
12 client pkts, 9 server pkts, 14 turns.
Entire conversation (3,355 bytes)
Show as ASCII
No delta times
Stream 16


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 : onlineId1
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.