SOC ANALYST REPORT

ON

Malware Analysis

Analyzed and Reported

By:

Oladayo Akinyode

Supervisor: Mr. Olaitan

September 2024

Executive Summary

The file was downloaded as part of an investigation being carried out on the event that took place on 2022-01-07 from 16:07:32 – 16:15:17. The interaction took place between the following IP address. The sender IP is 192.168.1.216 while the destination IP is 2.56.57.108 and 23.38.189.20. The owner of the IP address is using ASSUS Tek Computer and having conversations with CISCO and Dell.

Overview

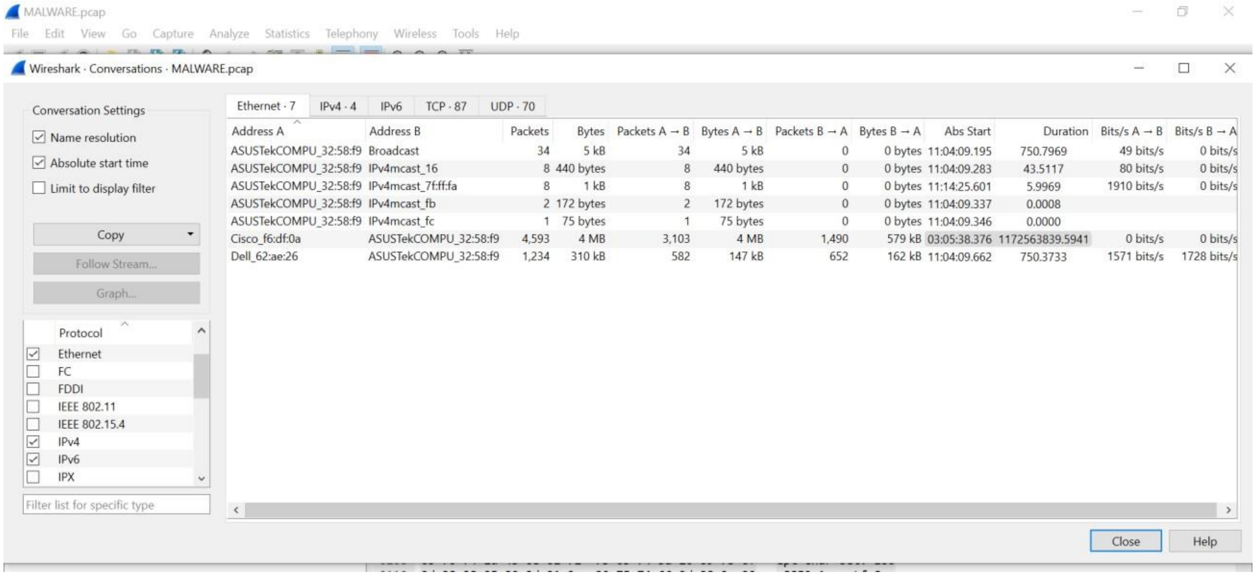
The malware contains protocols like HTTP, Kerberos, NetBIOS which indicated that packet of 32 was executed and this implies that there is a bug conversation between the system owner and another user which is suspected to be an attacker.

Method/ Approach

The malware analysis started opening the documents in Wireshark environments

Analysis

The expert information from Wireshark suggests and establishes that there could be a potential attack on the ASSUS Tek Computer through the HTTP web interphase. The picture below shows the conversations the client had with the HTTP web interphase.



Conversation Settings

☑ Name resolution

☑ Absolute start time

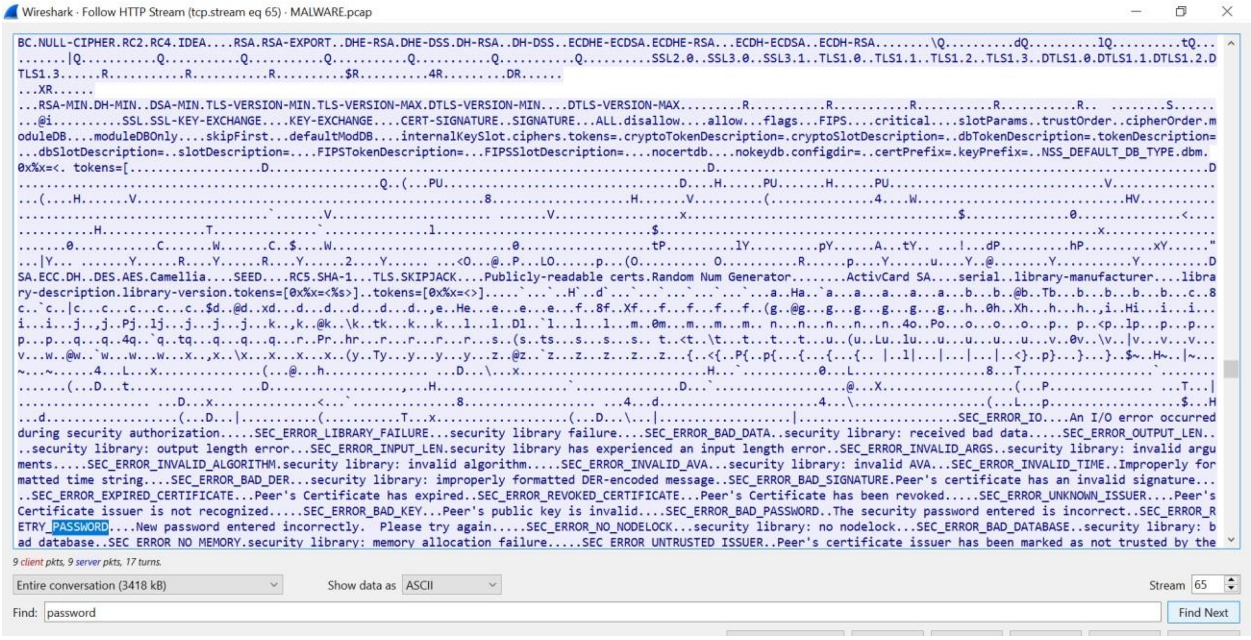
□ Limit to display filter

	Protocol
☑	Ethernet
□	FC
□	FDDI
□	IEEE 802.11
□	IEEE 802.15.4
☑	IPv4
☑	IPv6
□	IPX

Ethernet · 7 | IPv4 · 4 | IPv6 | TCP · 87 | UDP · 70

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Abs Start	Duration	Bits/s A → B	Bits/s B → A
ASUSTekCOMPU_32:58:f9	Broadcast	34	5 kB	34	5 kB	0	0 bytes	11:04:09.195	750.7969	49 bits/s	0 bits/s
ASUSTekCOMPU_32:58:f9	IPv4mcast_16	8	440 bytes	8	440 bytes	0	0 bytes	11:04:09.283	43.5117	80 bits/s	0 bits/s
ASUSTekCOMPU_32:58:f9	IPv4mcast_7f:ff:fa	8	1 kB	8	1 kB	0	0 bytes	11:14:25.601	5.9969	1910 bits/s	0 bits/s
ASUSTekCOMPU_32:58:f9	IPv4mcast_fb	2	172 bytes	2	172 bytes	0	0 bytes	11:04:09.337	0.0008		
ASUSTekCOMPU_32:58:f9	IPv4mcast_fc	1	75 bytes	1	75 bytes	0	0 bytes	11:04:09.346	0.0000		
Cisco_f6:df:0a	ASUSTekCOMPU_32:58:f9	4,593	4 MB	3,103	4 MB	1,490	579 kB	03:05:38.376	1172563839.5941	0 bits/s	0 bits/s
Dell_62:ae:26	ASUSTekCOMPU_32:58:f9	1,234	310 kB	582	147 kB	652	162 kB	11:04:09.662	750.3733	1571 bits/s	1728 bits/s

I analyze the HTTP follow stream I observed there was a lot of attempt by the attacker to guess the password and it was established that the password was stolen using Microsoft outlook.


Wireshark · Follow HTTP Stream (tcp.stream eq 65) · MALWARE.pcap

```
BC.NULL-CIPHER.RC2.RC4.IDEA....RSA.RSA-EXPORT..DHE-RSA.DHE-DSS.DH-RSA..DH-DSS..ECDHE-ECDSA.ECDHE-RSA...ECDH-ECDSA..ECDH-RSA........\Q.........dQ.........lQ.........tQ...
.......|Q..........Q..........Q..........Q..........Q..........Q..........Q.........SSL2.0..SSL3.0..SSL3.1..TLS1.0..TLS1.1..TLS1.2..TLS1.3..DTLS1.0.DTLS1.1.DTLS1.2.D
TLS1.3......R..........R..........R.........$R.........4R........DR......
...XR......
...RSA-MIN.DH-MIN..DSA-MIN.TLS-VERSION-MIN.TLS-VERSION-MAX.DTLS-VERSION-MIN....DTLS-VERSION-MAX........R..........R..........R..........R..........R..  ........S......
...@i.........SSL.SSL-KEY-EXCHANGE....KEY-EXCHANGE....CERT-SIGNATURE..SIGNATURE...ALL.disallow....allow...flags...FIPS....critical....slotParams..trustOrder..cipherOrder.m
oduleDB....moduleDBOnly....skipFirst...defaultModDB....internalKeySlot.ciphers.tokens=.cryptoTokenDescription=.cryptoSlotDescription=..dbTokenDescription=.tokenDescription=
...dbSlotDescription=..slotDescription=....FIPSTokenDescription=...FIPSSlotDescription=....nocertdb....nokeydb.configdir=..certPrefix=.keyPrefix=..NSS_DEFAULT_DB_TYPE.dbm.
0x%x=<. tokens=[..................D.....................................................................D...................................................................D
.................................................Q..(...PU.............................D...H.....PU.......H......PU...............................V.............
...(....H......V..................................................8.....................H......V.........(...............4...W............................HV..........
.................................`......V.....................  ......V.................x......................................$..............0...........<....
..........H..............T..............`..............1..............................$.....................................................x.............
.......0..........C.......W.......C..$....W..........................0.................tP.........lY.........pY......A...tY..  ...!...dP..........hP.........xY......"
...|Y...  .......Y......R....Y......R....Y......2....Y......  ...<O...@..P...LO.....p...(O.........  O..........R......p....Y......u....Y..@........Y..........Y.........D
SA.ECC.DH..DES.AES.Camellia....SEED....RC5.SHA-1...TLS.SKIPJACK....Publicly-readable certs.Random Num Generator........ActivCard SA....serial..library-manufacturer....libra
ry-description.library-version.tokens=[0x%x=<%s>]..tokens=[0x%x=<>].....`...`..H`..d`...`...`...`...`...a..Ha..`a...a...a...a...a...b...b..@b..Tb...b...b...b...b...c..8
c..`c..|c...c...c...c...c..$d..@d..xd...d...d...d...d...d..,e..He...e...e...e...f..8f..Xf...f...f...f...f..(g..@g...g...g...g...g...g...h..0h..Xh...h...h..,i..Hi...i...i...
i...i...j..,j..Pj..lj...j...j...j...k..,k..@k..\k..tk...k...k...l...l..Dl..`l...l...l...m..0m...m...m...m..  n...n...n...n...n..4o..Po...o...o...o...p..  p..<p..lp...p...p...
p...p...q...q..4q..`q..tq...q...q...q...r..Pr..hr...r...r...r...r...s..(s..ts...s...s...s..  t..<t..\t...t...t...t...u..(u..Lu..lu...u...u...u...u...v..0v..\v..|v...v...v...
v...w..@w..`w...w...w...x..,x..\x...x...x...x..(y..Ty...y...y...y...z..@z..`z...z...z...z...z...{..<{..P{..p{...{...{...{..  |..l|...|...|...|..<}..p}...}...}..$~..H~..|~...
~...~......4...L...x..............(...@...h.............  ...D...\...x........................H...`..........0...L..................8...T..................`........
.......(...D...t..............  ...D...................,...H...................`..............D...`...................@...X.................(...P..............  ...T...|
..................  ...D...x..............<...`.............8.....................  ...4...d.......................4...\.................(...L...p..................$...H
...d..................(...D...|..........(...........T...x.....................(...D...\...|...................|........................SEC_ERROR_IO....An I/O error occurred
during security authorization.....SEC_ERROR_LIBRARY_FAILURE...security library failure....SEC_ERROR_BAD_DATA..security library: received bad data.....SEC_ERROR_OUTPUT_LEN..
..security library: output length error...SEC_ERROR_INPUT_LEN.security library has experienced an input length error..SEC_ERROR_INVALID_ARGS..security library: invalid argu
ments.....SEC_ERROR_INVALID_ALGORITHM.security library: invalid algorithm.....SEC_ERROR_INVALID_AVA...security library: invalid AVA...SEC_ERROR_INVALID_TIME..Improperly for
matted time string....SEC_ERROR_BAD_DER...security library: improperly formatted DER-encoded message..SEC_ERROR_BAD_SIGNATURE.Peer's certificate has an invalid signature...
..SEC_ERROR_EXPIRED_CERTIFICATE...Peer's Certificate has expired..SEC_ERROR_REVOKED_CERTIFICATE...Peer's Certificate has been revoked.....SEC_ERROR_UNKNOWN_ISSUER....Peer's
Certificate issuer is not recognized.....SEC_ERROR_BAD_KEY...Peer's public key is invalid....SEC_ERROR_BAD_PASSWORD..The security password entered is incorrect..SEC_ERROR_R
ETRY_PASSWORD....New password entered incorrectly.  Please try again.....SEC_ERROR_NO_NODELOCK...security library: no nodelock...SEC_ERROR_BAD_DATABASE..security library: b
ad database..SEC ERROR NO MEMORY.security library: memory allocation failure.....SEC ERROR UNTRUSTED ISSUER..Peer's certificate issuer has been marked as not trusted by the
```

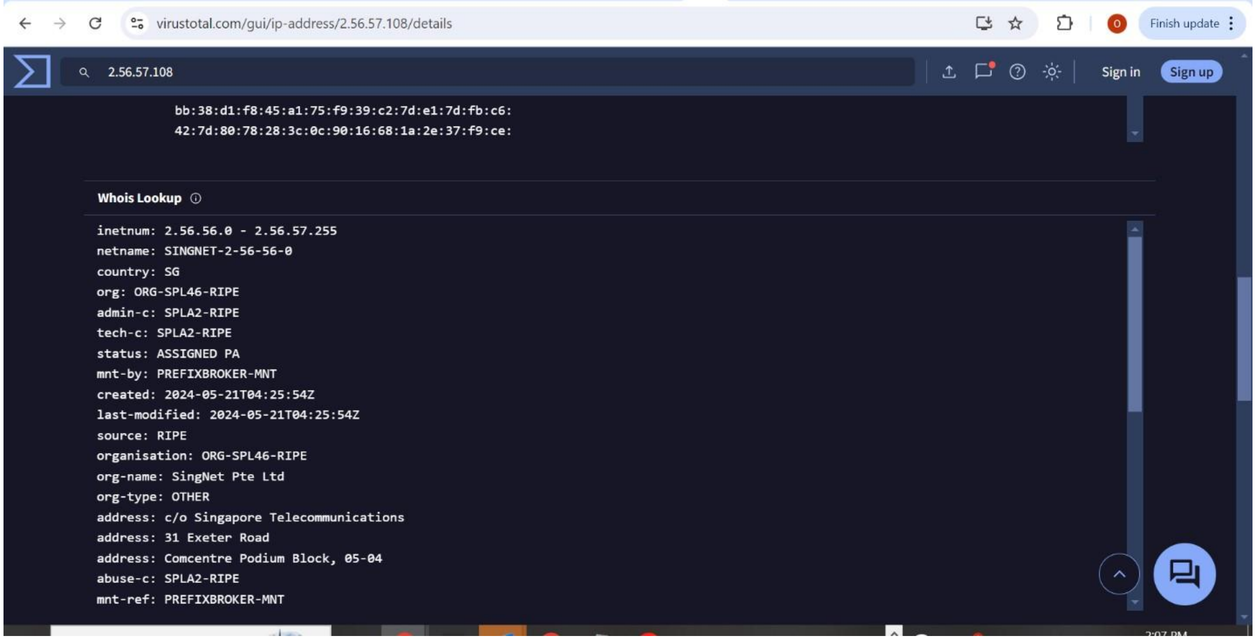
9 client pkts, 9 server pkts, 17 turns.

Entire conversation (3418 kB) Show data as ASCII Stream 65

Find: password

I conducted more analysis on the IP address **2.56.57.108** using OSINT tools.

Virus Total: The tool flagged the IP address as malicious, the organization name is Signet Pte Ltd and also shows that the owner of the IP is located in Singapore.

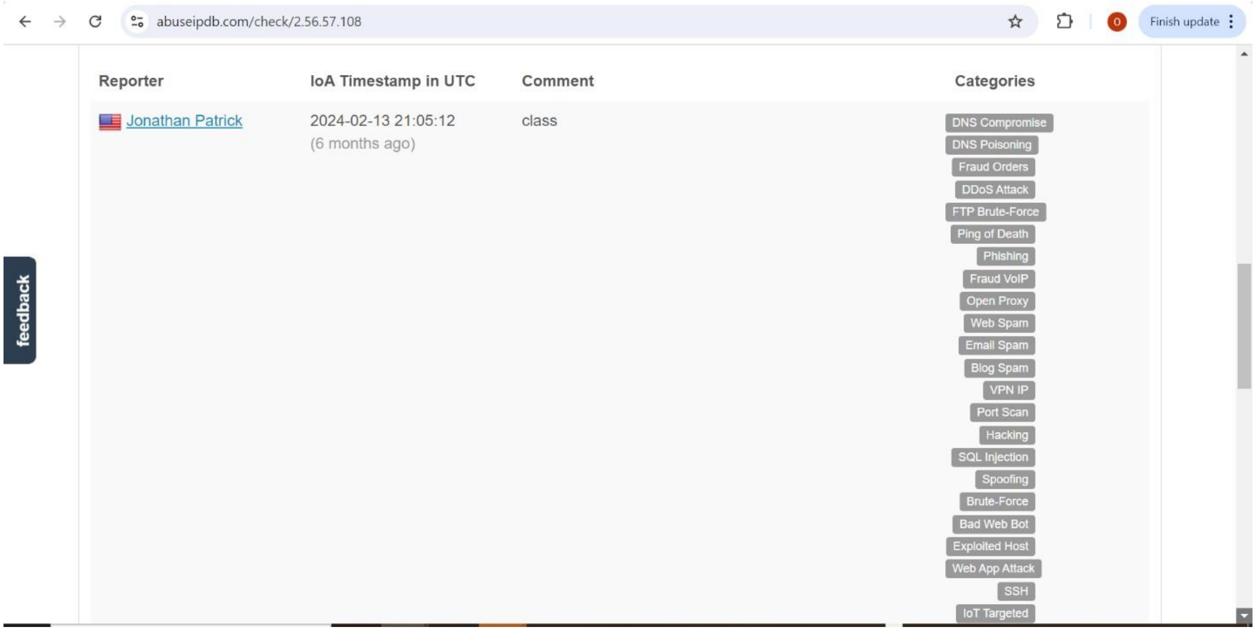


```
bb:38:d1:f8:45:a1:75:f9:39:c2:7d:e1:7d:fb:c6:
42:7d:80:78:28:3c:0c:90:16:68:1a:2e:37:f9:ce:
```

Whois Lookup

```
inetnum: 2.56.56.0 - 2.56.57.255
netname: SINGNET-2-56-56-0
country: SG
org: ORG-SPL46-RIPE
admin-c: SPLA2-RIPE
tech-c: SPLA2-RIPE
status: ASSIGNED PA
mnt-by: PREFIXBROKER-MNT
created: 2024-05-21T04:25:54Z
last-modified: 2024-05-21T04:25:54Z
source: RIPE
organisation: ORG-SPL46-RIPE
org-name: SingNet Pte Ltd
org-type: OTHER
address: c/o Singapore Telecommunications
address: 31 Exeter Road
address: Comcentre Podium Block, 05-04
abuse-c: SPLA2-RIPE
mnt-ref: PREFIXBROKER-MNT
```

Abuse IPDB: This tool established that the IP address have been reported for different cyber attacks like bruce force, exploited host, DNS, web spam, VPN IP, email spam, web spam etc.



Reporter	IoA Timestamp in UTC	Comment	Categories
Jonathan Patrick	2024-02-13 21:05:12 (6 months ago)	class	DNS Compromise DNS Poisoning Fraud Orders DDoS Attack FTP Brute-Force Ping of Death Phishing Fraud VoIP Open Proxy Web Spam Email Spam Blog Spam VPN IP Port Scan Hacking SQL Injection Spoofing Brute-Force Bad Web Bot Exploited Host Web App Attack SSH IoT Targeted

I also use filter in the Wireshark to extract more information about the conversation that took place.

DHCP – Dynamic Host Configuration Protocol

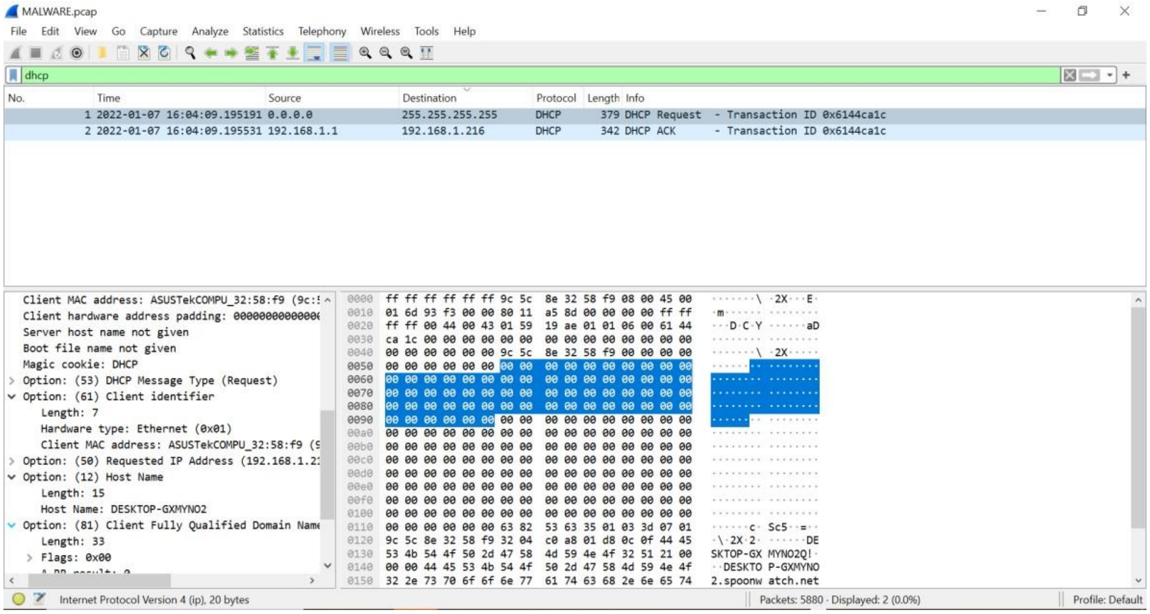
Using the filter to find the DHCP in the traffic shows the following results

Client Mac Address – ASUS Tek Compu-32

Host name – Desktop-GXMYNO2

Domain – Spoonwatch.net

Client Name – Desktop-GXMYNO2


MALWARE.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

```
No.    Time                        Source        Destination       Protocol  Length  Info
     1 2022-01-07 16:04:09.195191 0.0.0.0       255.255.255.255   DHCP         379  DHCP Request  - Transaction ID 0x6144ca1c
     2 2022-01-07 16:04:09.195531 192.168.1.1   192.168.1.216     DHCP         342  DHCP ACK      - Transaction ID 0x6144ca1c
```

```
  Client MAC address: ASUSTekCOMPU_32:58:f9 (9c:!
  Client hardware address padding: 0000000000000(
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
> Option: (53) DHCP Message Type (Request)
v Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: ASUSTekCOMPU_32:58:f9 (9
> Option: (50) Requested IP Address (192.168.1.2:
v Option: (12) Host Name
    Length: 15
    Host Name: DESKTOP-GXMYNO2
v Option: (81) Client Fully Qualified Domain Name
    Length: 33
  > Flags: 0x00
```

```
0000  ff ff ff ff ff ff 9c 5c  8e 32 58 f9 08 00 45 00   ·······\ ·2X···E·
0010  01 6d 93 f3 00 00 80 11  a5 8d 00 00 00 00 ff ff   ·m······ ········
0020  ff ff 00 44 00 43 01 59  19 ae 01 01 06 00 61 44   ···D·C·Y ······aD
0030  ca 1c 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 9c 5c  8e 32 58 f9 00 00 00 00   ·······\ ·2X·····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
0120  9c 5c 8e 32 58 f9 32 04  c0 a8 01 d8 0c 0f 44 45   ·\·2X·2· ······DE
0130  53 4b 54 4f 50 2d 47 58  4d 59 4e 4f 32 51 21 00   SKTOP-GX MYNO2Q!·
0140  00 00 44 45 53 4b 54 4f  50 2d 47 58 4d 59 4e 4f   ··DESKTO P-GXMYNO
0150  32 2e 73 70 6f 6f 6e 77  61 74 63 68 2e 6e 65 74   2.spoonw atch.net
```

Internet Protocol Version 4 (ip), 20 bytes | Packets: 5880 · Displayed: 2 (0.0%) | Profile: Default

Kerberos

The filter for Kerberos brought out the following

Cname realm – Spoonwatch.net

Host Address – DESKTOP-GXMYN02

Name Type: KRBS-NT-PRINCIPAL

HTTP.Request

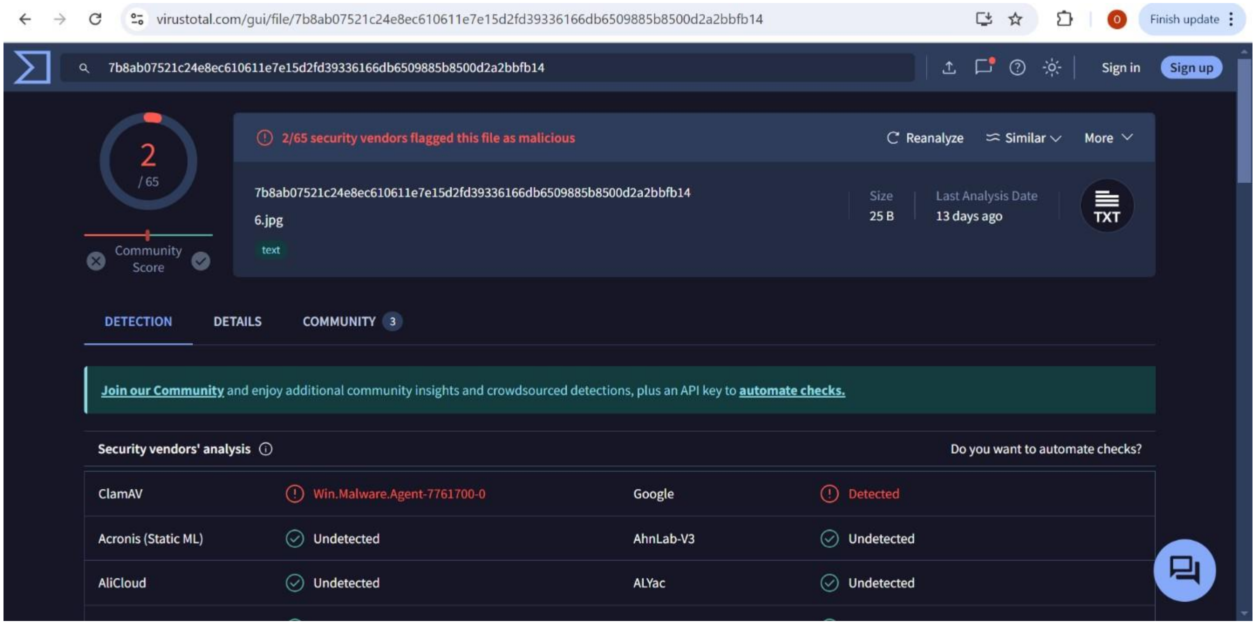
We were able to trace the password request and confirm the password was stolen.

Kerberos.CName string

CName String: Steve Smith

Hash File

I downloaded about six of the files shared in the conversation and hash them through Windows command prompt and one of the hash addresses indicated malicious activity when I analyzed it on virus total, It shows that the picture contains text. The hash file number is 7b8ab0751c24e8c610611e7e15d2fd39336166db6509885b8500d2a2bbfb14. This is the image below.


virustotal.com/gui/file/7b8ab07521c24e8ec610611e7e15d2fd39336166db6509885b8500d2a2bbfb14
Finish update
Sign in
Sign up
2
/ 65
Community Score
Reanalyze
Similar
More
TXT
DETECTION
DETAILS
COMMUNITY 3
Do you want to automate checks?

7b8ab07521c24e8ec610611e7e15d2fd39336166db6509885b8500d2a2bbfb14

2/65 security vendors flagged this file as malicious

7b8ab07521c24e8ec610611e7e15d2fd39336166db6509885b8500d2a2bbfb14
6.jpg
text

Size 25 B

Last Analysis Date 13 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

ClamAV	Win.Malware.Agent-7761700-0	Google	Detected
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	ALYac	Undetected

Impression of the sender

The impression of the sender is malicious and the sender's goal is to steal password of one of the staff named Steve Smith which was achieved by the attacker so that he/she could gain access to company's resources.

Conclusion

The conversation that took place between one of the staff named Steve Smith with MAC address ASUS Tek COMPU and Host name DESKTOP – GXMYNO2 was compromised by the attacker with IP address is 2.56.57.108 after interacting with malicious IP. The aim of the attacker is to steal the password of the user mentioned above so that he could infiltrate the company system.

Recommendations

This is my recommendation:

- The client (Steve Smith) system and IP should be quarantined immediately to prevent the attacker from penetrating other systems and users.
- Every member of the team involving the user should be told to do mandatory password resets.
- We need to do more digital forensics to be sure that there is no SQL injection because following the HTTP stream shows couple of queries were performed during the interaction.