APT-35

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON APT-35: ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

It is an Iranian-sponsored threat group operating primarily in the Middle East that dates back as early as 2014. The group behind the campaign has primarily targeted organizations in the energy, government, and technology sectors that are either based or have business interests in Saudi Arabia.

II. TARGETS

Defense , Financial , Technology , Telecommunications , Government , Energy , Technology based Saudi Arabia, US

III. METHODS USED

- The group uses tools like CWoogler , DistTrack , DownPaper , FireMalv , Ghambar m Havij , Mimikatz , Leash , PsList.
- This group has also been witnessed in supply chain compromise.
- Magic Hound malware has used BVS scripts for execution.
- Magic Hound used custom -developed malware which collects passwords from the firefox browser storage.

.

AXIAL

IV. ATTRIBUTIONS

A group of cyber actors utilizing infrastructure located in Iran have been conducting computer network exploitation activity against public and private U.S. organizations, including Cleared Defense Contractors (CDCs), academic institutions, and energy sector companies.

[Cited from malpedia]

VII. IOCS

Magichound.fetch : http://www7.chrome-up[.]date/0m5EE

MagicHound.DropIt SHA256

c21074f340665935e6afe2a972c8d1ab517954e2dd05cc73e5ff0e8df587b99d
ea139a73f8ec75ea60dfa87027c7c3ef4ed61b45e1acb5d1650cc54e658984ba
da2abdc951e4b2272fea5c8989debd22e26350bab4b4219104bccec5b8a7ff5a
0d3ae682868cb3ff069ec52e1ffc5ef765453fd78e47b6366d96aebb09afd8ab
f0ecc4388f0d84501499711681a64a74c5d95e0bb6a2174cbe3744bd5a456396
860f4cd44371a180a99bc16526f54f8b051c420a3df334d05d569d0cdadac3d2
b42b1186211633c2d47f3d815f0371ba234fee2ed0f26e487badc58e1ab81061
4beee6e7aa244335e161fdc05296ea100090c2114b4ff2e782e3ee3e1f936fdf
5e0e09c9860b293c4c9a2382a7392963adc54d6a23440abb9a2d89c50f8fd305
3161f9087d89a2d036ea32741d5a006c6bb279d36ff8d1acde63f2e354f8c502

MagicHound.Fetch PE SHA256

b6c159cad5a867895fd41c103455cebd361fc32d047b573321280b1451bf151c
6a7537f2cedbf453114cfba086e4746e698713777fb4fa4fc8964247dde741ed
16d87fbd8667677da1af5433b6d797438f8dc0ab565fb40ecb29f83f148888cd
92bc7d04445cf67aa7ddf15792cd62778d2d774d06616d1986f4c389b3d463f5
86d3409c908f667dd298b6a7e1e17652bb29af73e7daed4a5e945fbdf742e9f4
c3a8f5176351e87d28f45e58c79bb6646bb5d94ade7a24c6556514c860004143
a390365ddfcce146a8fa8435022f19b9a1be29f2b11a049cb660ec53f36beb06
d2ffc757a12817e4b58b3d58d71da951b177dedd3f65ca41fad04a03fc63fac6
79c9894b50cde62b182bd1560060c5c2bf5a1cef2b8afdffc4766e8c55ff6932
2f7f3582504fbce349a6991fbb3b5f9577c5c014b6ce889b80d51977fa6fb31a
8c2e4aa8d73ad2e48d70dfa18abea62769c7bef59c8c1607720f4f6162413f75
abe8e86b787998a07411ee24f3f3d8a79e37c6da539650ceed566b081f968c26
9e4d2e983f8a807f741f8873e6fa5d222dc6f3b358ccfc3a6c700398b342f656
e57f77cc3d117923ec01aa0e044edc11b1042e57993ca7f74d971630893ca263
ca6e823dedd6ca5fada2b1fa63d0acb288027f5a3cdd2c60dcace3c424c5ced0
eaaecabb439c81e522d9f5681fdb047ee62381e763f0d9646e68cd507479ba5a
1c3e527e496c4b0594a403d6d582bc6db3029d27369720d0d5122f862b10d8f1
29a659fb0ef0262e4de0dc3c6a140677b6ddee13c1819b791bd280be0547e309

MagicHound.Fetch PE C2
service.chrome-up[.]date

www3.chrome-up[.]date
www7.chrome-up[.]date
timezone[.]live
service1.chrome-up[.]date
104.238.184[.]252

V. REFERENCES

1. www.unit42.paloaltonetworks.com
2. www.attack.mitre.org
3. www.securelist.com
4. www.darkreading.com
5. Talos