PROMETHIUM

PROMETHIUM

TURKEY

VEITNAM , INDIA ,
CANADA, CAMBODIA

TRUVASYS

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON PROMETHIUM ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Promethium is a threat group based out of Turkey also known as StrongPity which focuses on information theft and espionage .

II. TARGETS

Targets of this threat group is attributed to area of Turkey and Syria also various other countries.

III. METHODS USED

This group primarily uses Truvasys malware .
This group has also used watering hole attacks to deliver malicious versions of legitimate installers.
This group has used a script that configures the knockd service and firewall to only accept C2 connections from systems that use a specified sequence of knock ports.

IV. CAMPAIGNS

The campaigns of this threat group has conducted a campaign in May 2016 and has heavily targeted Turkish victims.

This group has also been involved in several attack campaigns where it has destroyed as one of server common computer utilities, including WinUtils, TrueCrypt, WinRAR, or SanDisk .

This group has also involved with , ongoing data exfiltration campaign targeting victims in Turkey that started in February 2020.

ATTRIBUTION

PROMETHIUM is an activity group focused on espionage that has been active since at least 2012. The group has conducted operations globally with a heavy emphasis on Turkish targets.PROMETHIUM is an activity group focused on espionage that has been active since at least 2012. The group has conducted operations globally with a heavy emphasis on Turkish targets.

[cited from Volexity]

AX1AL

V. IOCS

Hashes

5cb8f86e03a544531d972e132c81d6785b66dd1b15b6c35a0a04fd83a8bed695
ea4b507c3236b56ef4ea44f5ac9a531a175d643d184e356ae8833d36c1957372
fad11a279c6fe195f8110702f962c5296015344da17919b361f73f7f504063ca
f8c953a9b737c5fe69ab9cfb5b20d576f15396a40de10ea6c3216042a97132f4
bdbc514e274d70e260620d9b7dcfc3ee4cf4eb321474dfbd1eb81d2f17cebc23
3ce08ada9cf964789ce70fd2637ded197ac5b154e0b71e9cdb4d99de7ab52267
b75fbe3b21d83e2000928349d1610f292e1a4c072fd0454309fe1c6c7d85ff46
bac8489de573f614d988097e9eae53ffc2eb4e7dcb0e68c349f549a26d2130a8
835a545fe93bfa75931079ef36169bfc56906f74b9b9862848ff79534b33f416
55e83292bd9a1f843639bfb98648a40b931a9829d62e6b23904034c417ffa430
e2cd8fd988a9a08f4bd73d7343ae54e68ee2a0a4728277792115edc86900e899
3feb6ecbc3b5f4ef64cf974fc117e58ac750188c483c488dd5b5970263bfdb0e
dd40b8ddb5a5795536a65cc0ab6dcc84862d4e14965cde6b4e9ad2b89a0e3905
02d68d2a9b62d1fd79c80e7c01182d18966a8fccc07d997b0f4c3ef71e87910f
f1a3c2bd241e09f4e98ca15c0d3d804297086c84883d81bb8b74960c6e986555
5b5b0a0ff8e5bdf11657e0134a638a818e31af9517e5feffea247eaa2660ee23
e4135bfeda1de00c3834f7782b77fdb2811f5d07fc60f643553426d9e45b664c
80ad6598f6e0b7c2b7258cbb69aa782dbcac308ca3d9d451b9bb5290b943a58f
e80034618538abc1c86a7021ab869c4ce63429d35adbaf8c07ce25f297a61bd2
5190c4fbddb2bfd08ce4a11714ec54dcaf57978f6193720c5b2c7127ef2c5f1f
783b3c61a4069f0325f3560ab9664ff5fb381f37b08a3d4eb4866ba6bc194135

C2

upd-ncx4-server[.]com
upd3-srv-system-app[.]com
syse-update-app4[.]com
upd32-secure-serv4[.]com
system2-cdn5-mx8[.]com
secure-upd21-app2[.]com
ms21-app3-upload[.]com
apt5-secure3-state[.]com
upd8-sys2-apt[.]com
update5-sec3-system[.]com
state-awe3-apt[.]com
app-system2-update[.]com
awe232-service-app[.]com
ms6-upload-serv3[.]com
updt-servc-app2[.]com
cdn2-system3-secrv.[]com
file3-netwk-system[.]com
service-net2-file[.]com
system2-access-sec43[.]com
ms-sys-security[.]com
mailtransfersagents[.]com

VI. REFRENCES

https://blogs.blackberry.com/en/2018/10/whack-a-mole-the-impact-of-threat-intelligence-on-adversaries
https://attack.mitre.org/groups/G0056/
https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Promethium%2C%20StrongPity
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html