

TEMP.VELES



TEMP.VELES



RUSSIA



SAUDI ARABIA
US



CRYPTCAT,
MIMIKATZ,
NETEXEC,
PSEXEC,
SECHACK,
TRITON, WII



A SURVEY ON TEMP.VELES ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

- NERDS OF AXIAL

I. INTRODUCTION

temp.Veles is a threat group based
ot of Russia and is also known by
names like Xenotime and ATK 91
focused on sabotahe and destruction
.

This group has been targeting ICS and energy based sectors onto Feb 2019 and multiple campaigns involving the
use of TRISIS and TRITON malware .

IV. CAMPAIGNS

II. TARGETS

Attack of this threat group ranges Critical
infrastructure, Energy, Manufacturing, Oil and
gas onto countries like Saudi Arabia , USA and
others .

ATTRIBUTION

III. METHODS USED

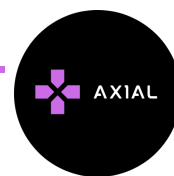
This threat group has been using TRISIS Malware

This threat group has been using TRITON Malware

This threat group has also been using multiple tools like Wii , SecHack & PsExec .

Temp,Veles has been attributed to Russia as per the ThaiCERT whereas Fireeye has
claimed this is a nation sponsored threat actor , the targeting of critical infrastructure
as well as the attacker's persistence, lack of any clear monetary goal and the technical
resources necessary to create the attack framework suggest a well-resourced
nation state actor.

[cited from ThaiCERT & Fireeye]



V. IOCS

Hashes (MD5)

6c39c3f4a08d3d78f2eb973a94bd7718
437f135ba179959a580412e564d3107f
0544d425c7555dc4e9d76b571f31f500
e98f4f3505f05bf90e17554fbc97bba9
6b3a73c8c87506acda430671360ce15
8b675db417cc8b23f4c43f3de5c83438

VI. REFERENCES

<https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=TEMP%2EVeles>

<https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html>

