ROCKE

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

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

-NERDS OF AX1AL

I. INTRODUCTION

Rocke is a threat group which is attributed to China also known as Iron Group which is focused on financial gain.

II. TARGETS

Targets of this threat actor/group are various servers where they could mine cryptocurrencies.

III. METHODS USED

This group primarily uses cryptojacking . Also they have been using tools like Godlua , Xbash and several 0-day vulnerabilities.

In their latest major update, they have added a function that exploits systems running the software development automation server Jenkins to increase their chance of infecting more systems, thereby generating more profits.

Rocke threat group has alsp utilized CVE-2019-3396

IV. CAMPAIGNS

The campaigns of this threat group includes Linux coin mining malware used by the Rocke groupin January 2019.

This threat group was also attributed leveraging both Western and Chinese Git repositories to deliver malwares in April 2018.

ATTRIBUTION

The family was suspected to be developed by the Iron cybercrime group and it's also associated with the Xbash malware we reported on in Septembe rof 2018. The threat actor Rocke was originally revealed by Talos in August of 2018.

Rocke, a China-based cryptomining threat actor, has changed its Command and Control (C2) infrastructure away from Pastebin to a self-hosted solution during the summer of 2019.

[cited from Anomali Threat Research & Talos]

AX1AL

V. IOCS

Hashes
To be added .

C2
systemten[.]org
lsd.systemten[.]org
update.systemten[.]org
1x32.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
2x32.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
3x32.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
1x64.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
2x64.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
3x64.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
shell.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
update.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com
cron.iap5u1rbety6vifaxsi9vovnc9jjay2l[.]com

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Rocke%2C%20Iron%20Group

https://www.anomali.com/blog/illicit-cryptomining-threat-actor-rocke-changes-tactics-now-more-difficult-to-detect#When:14:00:00Z