AEGIS Defender Now Blocking Snatch Ransomware IPs

The FBI and CISA issued warnings this week on the Snatch ransomware gang, which AEGIS has been blocking the IP addresses they use since 2020.

Cyber Defense Software

HUDSON, NH, USA, September 22, 2023 /EINPresswire.com/ -- The FBI and Cybersecurity and Infrastructure Security Agency (CISA) issued warnings this week on the Snatch ransomware gang, which has recently attacked South Africa's Defense Department and the city of Modesto California, USA. AEGIS has traced the IPs used by this criminal organization and has been blocking the IP addresses they use - since 2020.

> We are proud to serve our clients by blocking the IPs used by SNATCH gangs, as well as millions of others. Aegis Defender Pro is the only solution that blocks bad actors instead of dealing with them."
>
> *Charlie Trig*

Event logs from victims and CISA reports have shown traffic from both Russian Command and Control (C2) servers (Russian web hosting servers) and VPNs; all of which AEGIS has had in the Master Block List (MBL) for over 2 years. As new attacks are reported additional IPs are constantly researched and added to our MBL , 24/7/365.

According to the CISA, "Since mid-2021, Snatch threat actors have consistently evolved their tactics to take advantage of current trends in the cybercriminal space and leveraged successes of other ransomware variants' operations. Snatch threat actors have targeted a wide range of critical infrastructure sectors including the Defense Industrial Base (DIB), Food and Agriculture, and Information Technology sectors."

The hackers, formerly known as "Team Truniger," are using a Snatch variant used since 2019 that reboots computers in Safe Mode, disabling many AV software and endpoint protections. One of the only ways to defend against this threat is to block the IPs used to initiate contact in the first place and AEGIS Defender Pro is the only cybersecurity product that blocks IP's used by criminal actors.

Here is a list of IPs reported by various sources used by Snatch actors:

188.22.29 (:443) *
188.22.29 (:37462) *
188.22.26 *
188.22.25 *
211.209.151 (:3306) *
59.146.180 *
147.228.91 *
61.149.242 *
140.125.150 *
91.229.77.161 * - Ukraine DeltaHost server - initial contact from this IP
193.70.12.240 * - France based OVH Sas
178.162.209.135 * - Germany based LeaseWeb server

* AEGIS Defender Pro is actively blocking these CIDRs

mydatasuperhero.com
mydatassuperhero.com
snatch24uldhpwrm.onion
snatch6brk4nfczg.onion

commands executed during the attack:
vssadmin delete shadows /all /quiet
bcdedit.exe /set {current} safeboot minimal
shutdown.exe /r /f /t 00
net stop SuperBackupMan

registry keys:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\SuperBackupMan

Build IDs:
Go Build ID:
`9sbGxHyc5vSAXzwvg6iZ/c_gG_xy9d6xmNt9nMlii/HdKHUjGFLxliYJycPc5E/yTT_FNpw78SfII62lGUn
`
Go build ID: `2KZVw_piBNB6c74hlRt4/ueMyrcUcK4ismcjykWop/ZQYGFEYcaBSofxZbcs4g/GK-
7e3PY8vHyy_lSkbVi`
Go build ID:
`jPF3Jrx2uZ7VjN0GyDBL/x3B31XZylJgOhAVFZiym/o_aCHMB9kgaxIibXVOox/VQQhgCuLOuABGRrX
zFdl`
Go build ID: `ULgusZVAlPcWOJcj9LKW/fOp_xyXqQQO5nzk3CZIW/LV-
l8Ye8SLuN39dCmiDH/_34hEcu3a_yVC0sdeBdP`

Go build ID: `BIFnB6MdgF4djhq39TIM/0F-O_BMJNaIkMOFRC1kQ/j2Fm9d-Ilq-6KP4f1cuF/I07Xn6PJTdAcrP3IsVX4`
Go build ID: `cN2S005MM6pjpFXzNYd7/Lu1OzfnOLXKCy8mQdge9/GnIsH3q8hyF-pEAWP4K0/ISXM5yfoGT6hDQpcP08E`
Go build ID: `jPF3Jrx2uZ7VjN0GyDBL/x3B31XZylJgOhAVFZiym/o_aCHMB9kgaxIibXVOox/VQQhgCuLOuABGRrXzFdl`
Go build ID: `D4uZyyRaOm8WP2m599HU/gZkWHWmCm-S2lk0u6tJQ/F9Wz3xBbUlF3TISfF8Gu/uPBkEF2KfTla4ver6O79`
Go build ID: `nz4NhyAgWYITxG9Gw5rT/an0sbWQDT73tZEat72I5/KKmIcIIeFCNSYj4p5koW/BHky2GAanYgZQqXGSyei`

Ransom e-mails:
imBoristheBlade@protonmail.com
jimmtheworm@dicksinmyan.us
doctor666@mail.fr
doctor666@cock.li
newrecoveryrobot@pm.me

Ransom extensions:
.snatch
.jimm
.googl
.dglnl
.ohwqg
.wvtr0
.hceem

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-263a

https://thedfirreport.com/2020/06/21/snatch-ransomware/

https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/

https://github.com/sophoslabs/IoCs/blob/master/Ransomware-Snatch

Charlie Trig
Aegis Cyber Defense Systems
+1 6178195877

email us here