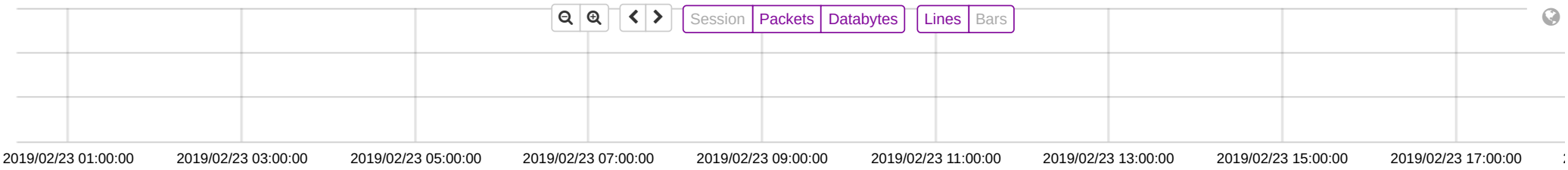
ip == 89.177.109.254 && port == 41748 && ip == 212.158.157.3 && port == 22 && protocols == tcp | Search

Last 24 hours | Start 2019/02/23 00:24:29 | End 2019/02/24 00:24:29 | Bounding Last Packet | Interval Auto

50 per page « ‹ 1 › » Showing 1 - 1 of 1 entries

Session | Packets | Databytes | Lines | Bars



Start Time	Stop Time	Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Moloch Node	Info
tcp	2019/02/23 23:48:27	2019/02/23 23:51:14	89.177.109.254 CZ	41748	212.158.157.3 CZ	22	63	7,450 11,624	SELKS	

Download Pcap | Source Raw | Destination Raw | Permalink | Actions

Id 190223-xjMn39iBnc9AuL9WLHgHPxTh

Time 2019/02/23 23:48:27 - 2019/02/23 23:51:14

Node SELKS

Protocols ssh tcp

IP Protocol tcp

Src **Packets** 32 **Bytes** 5,857 **Databytes** 3,737

Dst **Packets** 31 **Bytes** 5,767 **Databytes** 3,713

Ethernet **Src Mac** 00:25:90:0e:e8:a5 **OUI** Super Micro Computer, Inc. **Dst Mac** 00:15:17:26:33:c8 **OUI** Intel Corporate

Src IP/Port 89.177.109.254 : 41748 (CZ) [AS6830 Liberty Global B.V.] { RIPE }

Dst IP/Port 212.158.157.3 : 22 (CZ) [AS25248 RADIOKOMUNIKACE a.s.] { RIPE }

Payload8 **Src** 5353482d322e302d (SSH-2.0-) **Dst** 5353482d322e302d (SSH-2.0-)

Tags

Files /data/nsm/log.5.1550961671.pcap

TCP Flags **SYN** 1 **SYN-ACK** 1 **ACK** 21 **PSH** 39 **RST** 0 **FIN** 2 **URG** 0

SSH

Versions ssh-2.0-openssh_7.6p1 ubuntu-4ubuntu0.2 ssh-2.0-openssh_7.2p2 ubuntu-4ubuntu2.7

Suricata

Signature SSH to_client, established, not zabbix

Category Generic Protocol Command Decode

Flow Id 365402089285163

Action allowed

Gid 1

Severity 3

Signature id 500,111

Packets 200 | natural | ascii | utf8 | hex | Line Numbers | Uncompress | Show Image & Files | Show Timestamps | UnXOR Brute GZip Header | UnXOR | Unbase64

Source

2019/02/23 23:48:27.2727 **41 bytes**

SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.2

2019/02/23 23:48:27.2727 **1360 bytes**

□L□□N
□!□□□□p□□9sA□l□0curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha256,diffie-hellman-group14-sha1,ext-info-c□"ssh-ed25519-cert-v01@openssh.com,ssh-ed25519,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-rsa-cert-v01@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,rsa-sha2-512,rsa-sha2-256,ssh-rsalchacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.comlchacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com□umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1□umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1□none,zlib@openssh.com,zlib□none,zlib@openssh.com,zlib

Destination

2019/02/23 23:48:27.2727

SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.7

2019/02/23 23:48:27.2727

□<
□□□□k□"□□@□□jR□□curve25519-sha256@libssh.org-ed25519lchacha20-poly1305@openssh.com,aes256-gcm@ope

Start Time | Stop Time | Src IP / Country | Src Port | Dst IP / Country | Dst Port | Packets | Databytes / Bytes | Moloch Node | Info

ip == 89.177.109.254 && port == 41748 && ip == 212.158.157.3 && port == 22 && protocols == tcp

Search

Last 24 hours | Start 2019/02/23 00:24:29 | End 2019/02/24 00:24:29 | Bounding Last Packet | Interval Auto

50 per page « ‹ 1 › » Showing 1 - 1 of 1 entries

,□□ ��□f�����P�;�J�P����8z
|Ks�5YA□

2019/02/23 23:48:27.2727

2019/02/23 23:48:27.2727 **60 bytes**

□����E□2��□□□E,�c□□#¹□:□y□□□;□□X□□□Di8

2019/02/23 23:48:28.2828 **68 bytes**

#□□□_□6□□0□ぶX□□cd□X□□□□□V□□
□`j□K□□>%□_□□D□□f□@□□)1@U□K□□Z□m}F□NΠ

2019/02/23 23:48:28.2828 **1164 bytes**

□>□9□□□V□□@□□cf□□□□칎 %□i□s]□□i
V□□□2*□!□□~□□□/$□IU□!□□|□"L□□_.□]o□□□Uσ□J□□iK□~□□Z
□□z□□□□□My`m□□ċ□□%□{h L□□□□:q□d8□□H□□□□□□□□v!$□&□3□□?W□□|
□□□□□□□□□-□Hz□□□□Φ□□□□v□:□²
□□R)□□□□□\□□□□□□□j□□□y□□f,E<'J[□□C[□`@□4□□□c□□>□□□□,q□□,Ꮋ□Z□}
□Cy□□Z\yD)□□□H~□□□bs□□□I□*□1□□平^U□1KKJ%&i}□□f□'□4□
□□□□□z□F□□□□□brx□$U□N#8□□□(&□□X□□□□□ X□□□□ɪ□ □h
□□nF□□□□□□□□Mq□□w□□QZЈ□_n]&□□u□cR□□wph□□ZƊ]/qTĞ□□□□□:□□
H□%□□□□%: z□□
;w□tk□□□□Wi□S□□s□<□□<
{□I□A]□□□sO□□□S□□x□□'□□F□.Q□□□□□□^□□□□□,1!B#□□<□ı□□z̨*□a□□!S□
c8□5F□¨$□3□□□v□□□□□t□d□3□□□□TTB~□□.□□M□□a}
□yJ□]□ug□□□m□□□x□=@□>ZN□□□□ʜ□Z□3□T□□Gn>□+□□□F□`t7/
̨P0O□□9□□□□Tf□□5)□□6□□□□□□□□n□□□C+□□□□□□a□Ó
□m□z□□J□□□(□_>#□d□aЈ□j□□□٩□□G□o□M□□□□e
□□[y□9□S□`□□Ш□ox□□*
□|□pL□h□Ť□]□□[□%′□x□□□{□□#□□□□e□O□!□p.hl□□□□(□□□8□□□□□C□
□□[B=Tls□□!
□□)xO□□m5□X□V□sG□□,+N□2□□□□□□□nt□L□□F□i□□56□b□□□□□□h□□!:□
0□S};□□□□{□□_□}#□oLı□j□□□TU,□□lx'Q□□,K%□X□J□ PBq□D□oJO□□8[N□□□□}
□□_□]0□□□□`□□""Q~Z□□~B□□=i□□δ□I□`□D□P□□%□z□□□□□{□□□_□□□□
□□□r□r□□□□□$□Ⱶ□□8□.□$□W□□A□□□□=?~□□□q92□□[□[□□□□□tO□□/0□?
{□□□□□:□i□□□□T□□□m□'□1rS□□]□□□@□□@□□L□□□□□□V
=□□□□CќN□*□□mP□□{□□□N□-□□□□□□□(□[*□□□□□□f□

2019/02/23 23:48:33.3333 **148 bytes**

i□□□O□□□=□zY□MĞ□_#w9}TDB□□2-
□T8□Č□□o□□□□Gl□□u□>R□□□□□I□□+:□Ш□|
Ьl□□2□□~P"□j<□□̧yk□P□Q□t7□□□ □□□□□□L□P□0"$□9□□Njqj□{S□□□Ɒ=
□□:□□□□V□□

2019/02/23 23:48:33.3333 **112 bytes**

□□4□□A□n:□r□□
4□□□c□□□□□□□□P1.□□L□□mTs□□otd□]□ă□□□4D□□=□□□T□I□
□□>□U□□□X□^□□□□?)□□PMB□cr□□□;M□□□k□□E□□□□□Ms

2019/02/23 23:48:34.3434 **460 bytes**

K□2□□f□□+n□□□9=□?ũ□□□□HN□□□□□□□□□□GEU□*□□□M□v□K□□K
+¨□G0;□0□~□□G□□□<□□S□f□¨□□8□□□□d□□□P□□□!o□□Z□Tû□□□□□□□□`"□3□P
□□P□I!I□>□□□X$□□R□ŏ҂KB□
鈞□9>□□M□(9□<vj□9□□□c.&□̣□e,T□□i□ж□□T□□□□□□8□~.□□□I
□U\□72□□J□ob□=□□□1□□□□
□□o$□a□PHђ?[□□□□□̣□□□7I□□□□□v □□L□□Y□N□□u□씎□t□#1[P;□□R=□3Ꝋ□
`E□□□$□□□k□ y^□A□□□□;<□□\□□)7□Cp@8□□□
=□E□=□□□□□;Yp□y□□□k□B□□□ҁ□□□□TI5□□P□~□□V□L□ET□□&dn□n~□□"]蠔
□^□□[□□ж□m□¼W□□F4I□'□ɣ"□/
□□G<u□!YU□□(□{Q(dz2"□O□□□□□□□\Y□B]5□□□J□□<7□

2019/02/23 23:48:27.2727

□□3□ssh-ed25519 □□□□w□/"*□□□□□□ t□□~□□G
]/□□z□`e□□}□E□\□s7S□ssh-
ed25519@□□□□□□~□(□"□□□□v□i□|I□□u□V□jI(□F
□J□□XTC□□□hx□}
%□n□□
□□□□□□(□T□dXg□□□□d□/7□□□WT□[□□Q5ɹ□T_
□□□□+□I<□□@□Ţ□□□□□□□□^□□N□-y>□□Ta\□

2019/02/23 23:48:28.2828

□$□-□pd□□□>□uq□□"□)9G L□□3ZioՂ (O3□□H□□□l

2019/02/23 23:48:28.2828

□ □□S□!□□□□aHy□□f□□□&□6□□□□7½*□□Hu□□□

2019/02/23 23:48:28.2828

]□^(□l}□□□` □kD□,□'□□□j□□"□9t□□□□□
□□□□9□B□-□>□□a□□

2019/02/23 23:48:33.3333

;□□;□□□□=□□□)□□P#a□@□□□□T~□

2019/02/23 23:48:33.3333

}□□□g□RW□□□□JH□8/t:K□ /OS□7□F!□□/□□M□
□W□a□□L□□□&□□B□\□□□□[□v□□□8□;□□ç□□□
□\□J□□□□p□□$'□6<□6$□FM□F□□□□□3□b#□NT
□□□□□z□M□□□}□□□□\u□□□□□þu□□1c□{□\□□
□□f□□/nuc□o□□c□H□?□□□□>□+□□[□W□□□□<□
ω@□N□□□ъ□□`@□□z□□□□□r□□Z(□□E□□□□r□□
□□□□Z□□{4□t□□]=□]□□4/□□ □□□ɟl□□~)U7□□:I
□□;□□□wą<□□Q□(□□!□□□□□N;□□□~□□s□4□□□|
□\□□w□□□i□X□U`□ □]:p□□□□□□□JnP2□□□□c"□n
□□□Ju□vw□?dx□□yl-□□6N#¨□a2₱Uy|$□G$o□[□d□
□□t□□□□□□□□□%□□a□□W□□□NuS□□□X□□/K□
□□s□□>□v□□v^□□f□□)□^ □□□□Z`□□□}13a□;□□
□(□c□□□□□]□WUj□□®□A,1□H□□□□t"□PK□□$□□
(6□N□□□ą,□□7□□□Ц4□□□T□□□□□'/JY□□□□□O□
m□□\□e□□M□y□□□vYJ□□□□□o□Zu□□q□□hX□Y
Cqs□^XV□"□□<□□}Wk□□□+□WA□□h&□□E□~□%□
□□d□□B□□3□□!□□d□□□[□`5□□rɲ6□o□"_T□>□S□
□0D□5□□□uw>□□□du□□□□□□ 0□□□~l□

Start Time | Stop Time | Src IP / Country | Src Port | Dst IP / Country | Dst Port | Packets | Databytes / Bytes | Moloch Node | Info

ip == 89.177.109.254 && port == 41748 && ip == 212.158.157.3 && port == 22 && protocols == tcp

Search

Last 24 hours | Start 2019/02/23 00:24:29 | End 2019/02/24 00:24:29 | Bounding Last Packet | Interval Auto

50 per page « ‹ 1 › » Showing 1 - 1 of 1 entries

2019/02/23 23:51:12.1212 36 bytes

c��I�#���¨~LD[������{�&O?I���z��

2019/02/23 23:51:13.1313 36 bytes

Bo�z�h�s�üw�P*3�Ч6>*9�7=���%n��

2019/02/23 23:51:13.1313 36 bytes

_ s*ow��Y��L6��0)p~��S^3��|6T��

2019/02/23 23:51:13.1313 36 bytes

W`��PW |#��}����

H��?_ρ��8 ��P

2019/02/23 23:51:14.1414 36 bytes

J��q=R²G «[p��pJ��:B`y)I Dz

2019/02/23 23:51:14.1414 96 bytes

P y8!t8/im��s������k_��)3SNN��0��e????

G@t���Ss=g e}��,Nk���h~~{e/=

2019/02/23 23:51:12.1212

o��s Qj!pS 5###E 5m

2019/02/23 23:51:13.1313

n 拌) q 景V? a c

2019/02/23 23:51:13.1313

K+S)UT /g N(*1 e 4$ {

2019/02/23 23:51:13.1313

2&;L~Cj B)*蚔 Y [[! 1k

2019/02/23 23:51:14.1414

y EVCM IAP Q h3 Om \C <

W/& y p^ /m{ H Q

>.a KJ k w.w(cK[$ q> d _ E 0sR /// 4

F:&) OU "m& ~

Packets 200 | natural | ascii | utf8 | hex | Line Numbers | Uncompress | Show Image & Files | Show Timestamps | UnXOR Brute GZip Header | UnXOR | Unbase64