Grizzly Steppe: Lighting up Like A Christmas Tree – Fauie Technology

fauie.com (https://fauie.com/2016/12/30/grizzly-steppe-lighting-up-like-a-christmas-tree/) · by Chris Fauerbach

Grizzly Steppe: JAR-16-20296

Yesterday, US CERT along with the US Department of Homeland Security (DHS) released a Joint Analysis Report (JAR) on GRIZZLY STEPPE. If you've been reading the news over the past few months, you've seen the accusations of Russia's interference on the 2016 US Election. In generalities, the US alleges that Russian nationals hacked into the Democratic National Conventions systems, and through a series of campaigns, were able to leak internal documents that were a bit damning. Many believe there was a direct influence into the results of the election, therefore messing with our need for a pure and 'internal' election. This post is not to discuss the politics of it, but more to discuss the GRIZZLY STEPPE release that came out yesterday.

GRIZZLY STEPPE (https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity)

As you know from my other posts about Threat Intelligence (Overview (https://fauie.com/2016/08/23/stix-taxii-visualizing-and-understanding/), Mini Rant (https://fauie.com/2016/12/21/mini-rant-stix-confuses-my-computer/), etc)

a briefing like this comes across in a few formats. First is the writeup:

Security Briefing (https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity)

Then the STIX:

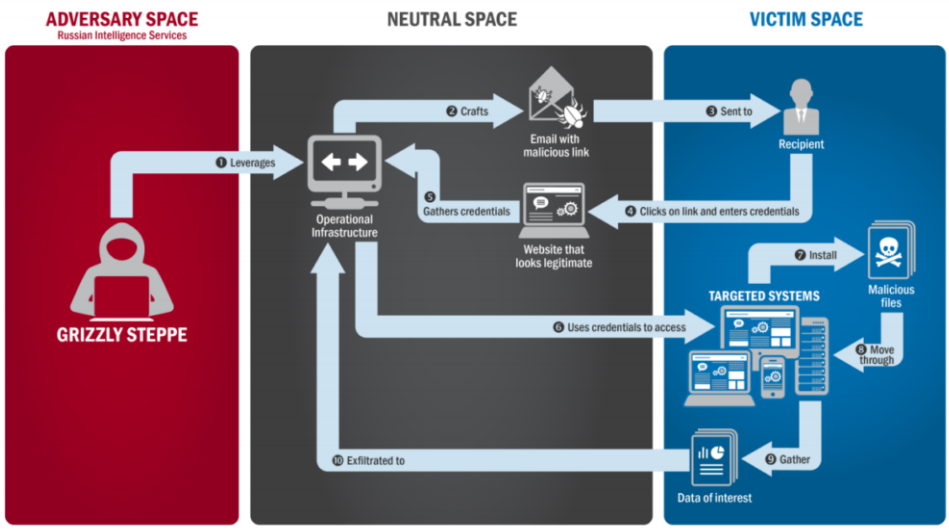
STIX Documents (https://www.us-cert.gov/sites/default/files/publications/JAR-16-20296A.xml)

Then a PDF:

PDF Documents (https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf)

Overview of the attack

These are a mix of analysis and marketing, in my opinion. That's not a bad thing. There is a ton of useful information in that PDF that describes that context around these attacks. You can read in there that there were two groups (APT 28 and APT 29) that were active over the same time period. The attacks came through 'neutral space' (AKA The Internet), so there was a tech/air gap between the attackers and the victims. This provides a way of hiding the true source of the attack.

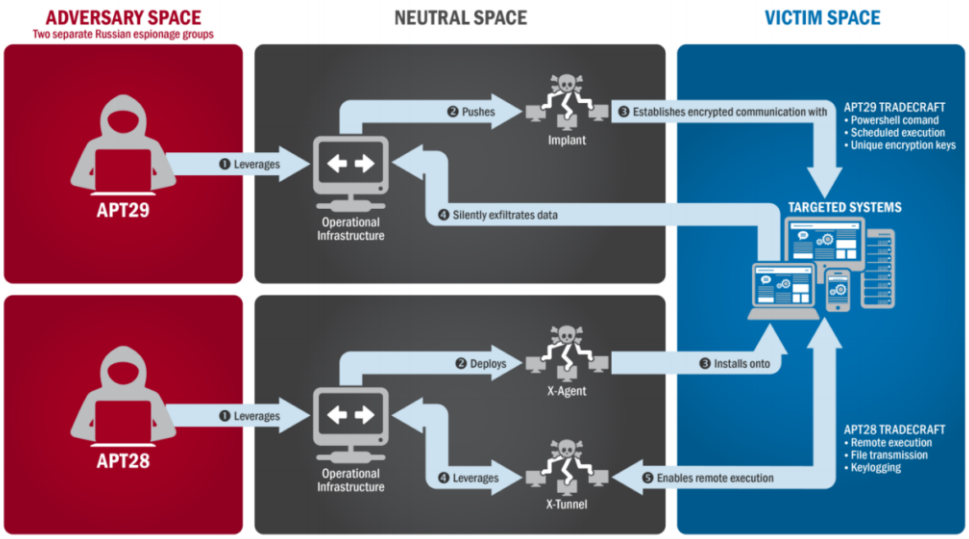


From US CERT – Grizzly Steppe Attack Flow

The initial penetration came from targeted spear-phishing. These are custom crafted emails, that are meant to seem legitimate. Spear-phishing is different from phishing, and can be generally distinguished between the approach. A typical phishing campaign will blast the same email to hundreds or thousands of email addresses, hoping someone clicks a link and enters their bank account information. Spear-phishing is hyper targeted. They will research the recipient, and craft messages to them.

Once a message ends up in someone's inbox, the user still has to typically perform an action (click a link). When the user clicks the link, they are directed to a malicious website that will drop malware on their machine. After the

malware is installed, it can do the nasty things we're all scared of. In this case, the two types of malware behaved a little differently.

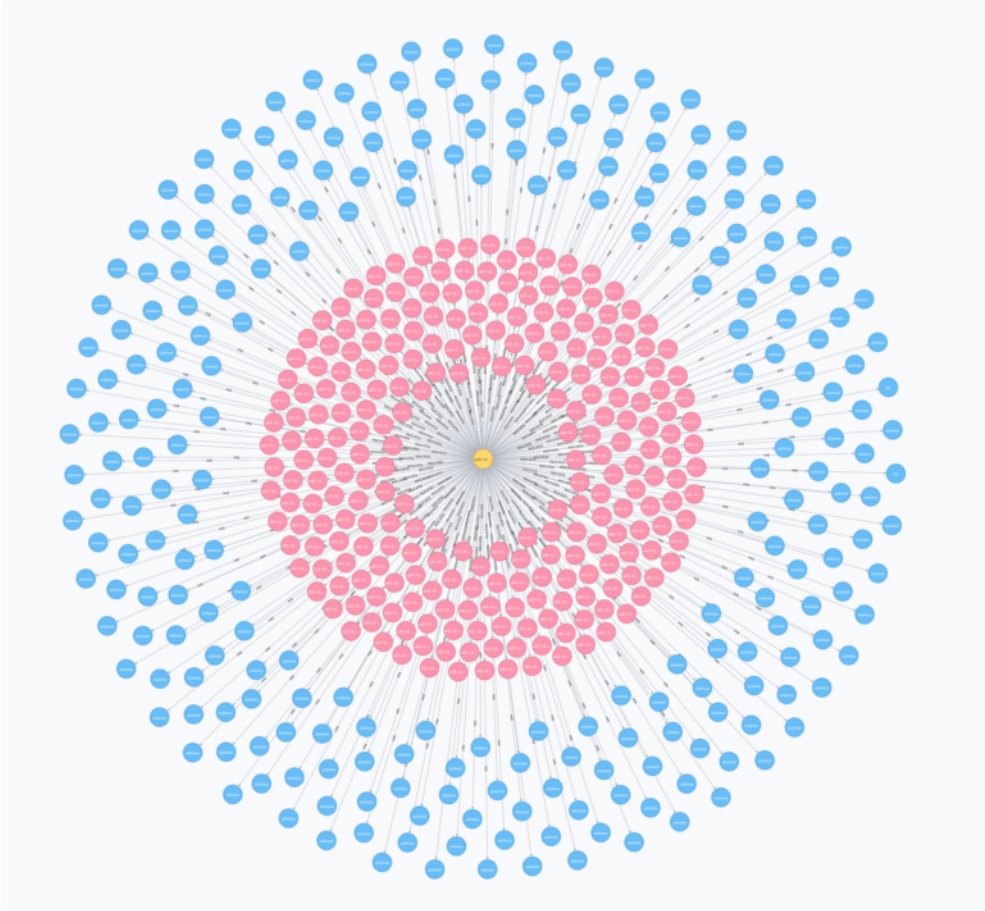


From US CERT – APT 28 and APT 29 Comparison

APT 29's malware was focused on finding internal data, and sending it out over an encrypted channel using their own encryption keys, making it impossible for anyone to read what was coming out. APT 28's malware acted more as a zombie piece of code. It waited for command and control messages from an external system before executing. According to the writeup, it logged real time data (keyloggers) and executed code , instead of finding existing files to exfiltrate.
Let's talk about the observables

Before the briefing (above) got to my inbox, the Perch Security system had already pulled the latest data from DHS AIS. DHS AIS is the Automated Indicator Sharing platform that the Department of Homeland Security runs. Essentially, it's their TAXII feed that serves STIX data. ((For a refresher, look here:))

The data comes out in a bunch of documents, that together, form this story.



Grizzly Step STIX content in graphical format

The yellow in the center is the STIX Package. This package let's us know the general context. In this case, there isn't much beyond a title: "JAR-16-20296" and the description: "This indicator is alleged to be connected to suspicious malicious activity.". The TLP (Traffic Light Protocol) of all this is WHITE , which means I can freely share all this information.

There are 912 Indicators (Pink) and each Indicator has an Observable (Blue). The indicator descriptions are also quite generic.

877 of them have the description"Malicious IPv4 Indicator"

24 of them have the description "Malicious File Indicator"

10 of them have the description "Malicious FQDN Indicator"

1 of them has the description "Malicious URL Indicator"

You can see a full breakdown of the Observables below.. mostly IP addresses, a few domain names and a few file hashes.

Slicing and Dicing

Title Description Count Malicious IPv4 Indicator This IP address is located in China. 45 Malicious File Indicator It is recommended that network administrators review systems for the existence of this hash and determine possible malicious activity. 17 Malicious IPv4 Indicator This IP address is located in France. 11 Malicious IPv4 Indicator This IP address is located in Japan. 6 Malicious IPv4 Indicator This IP address is located in Canada. 6 Malicious IPv4 Indicator This IP address is located in Thailand. 6 Malicious IPv4 Indicator This IP address is located in Mexico. 3 Malicious IPv4 Indicator This IP address is located in the United Kingdom. 3 Malicious IPv4 Indicator This IP address is located in Puerto Rico. 3 Malicious IPv4 Indicator This IP address is located in Italy. 3 Malicious IPv4 Indicator This IP address is located in Luxembourg. 2 Malicious IPv4 Indicator This IP address is located in Iran. 2 Malicious IPv4 Indicator (empty) 2 Malicious IPv4 Indicator This IP address is located in India. 2 Malicious IPv4 Indicator This IP address is located in Brazil. 2 Malicious File Indicator This DLL is a fully functioning Remote Access Tool and variant of OnionDuke malware family. The following text is … 1 Malicious FQDN Indicator It is recommended that network administrators review traffic to/from the IP address to determine possible malicious activity. 1 Malicious FQDN Indicator The Remote Access Tool malware "AE7E3E531494B201FBF6021066DDD188" attempts to use this C2. 1 Malicious IPv4 Indicator This IP address is located in Mongolia. 1 Malicious IPv4 Indicator This IP address is located in Kenya. 1 Malicious IPv4 Indicator This IP address is located in Cambodia. 1 Malicious IPv4 Indicator This IP address is located in United Kingdom. 1 Malicious IPv4 Indicator This IP address is located in Ukraine. 1 Malicious IPv4 Indicator This IP address is located in Austria. 1 Malicious URL Indicator It is recommended that network administrators review traffic to/from the URL address to determine possible malicious activity. 1

Looking at the data

One issue that is regularly seen is the quality of the Observables, and I've blogged about this before ((Mini Rant, again (https://fauie.com/2016/12/21/mini-rant-stix-confuses-my-computer/))). Just because an IP address was found during research, doesn't mean it's an Indicator of Compromise (IOC). This is a challenge, because sometimes, a 'safe' IP address can act bad. How do we list that in STIX? For instance, when a known shared web host, or even a CDN like Amazon or Akamai, temporarily hosts a bad file

that one of their customers (hacker?) uploaded. Do you put that IP address in your list of Observables? Do you put the full URL of the specific file? The file hash?

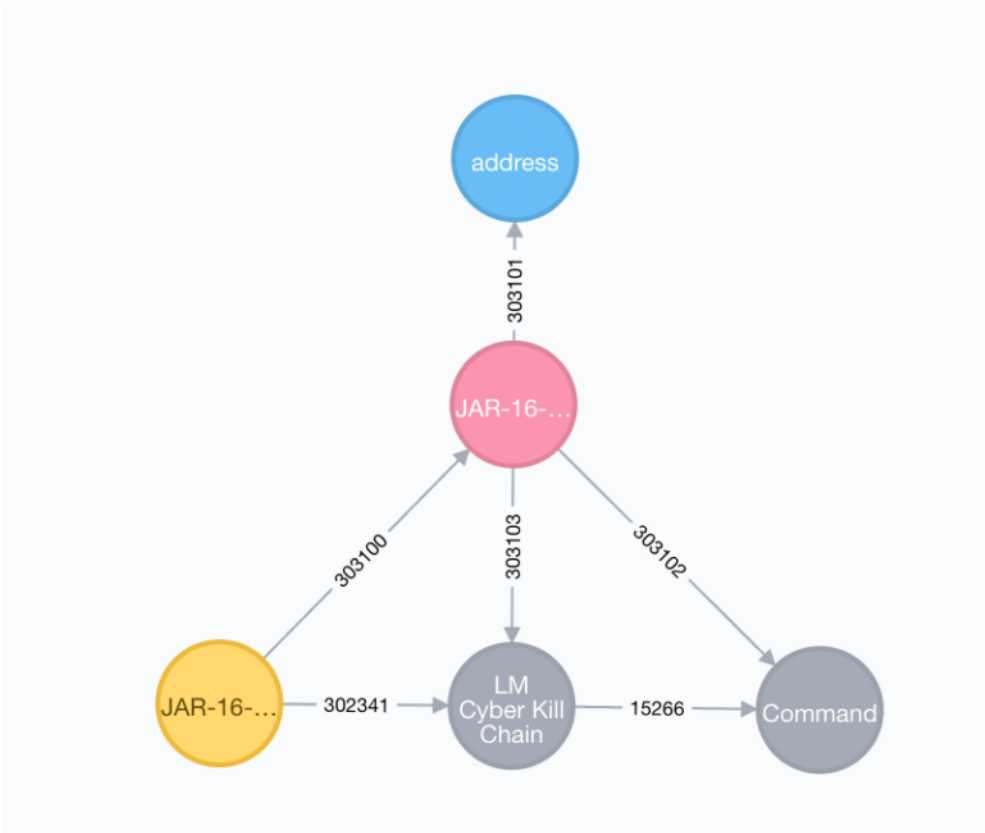
1. In this technologists opinion, we need a few things.
2. In the STIX standard, indicators give us context. We need to know when something is always bad (file hash)
   If a URL, web domain, etc are maliciousn (www[.]g00gle[.]com, let me know that.. then I need a way to know what IP address that domain resolved to at the time of attack… but consider that 'meta-data'. Don't consider the IP address as necessarily malicious.

As far as I know, some tools like to add the IP address at the time an analyst enters the domain name. That's fine, but it should not be treated as the 'Observable' of concern. This is a tough concept for some analysts who aren't as well versed in how networks/shared hosts, etc work, but with education, we should be able to fix some of this.

Example From the GRIZZLY STEPPE documentation

You can find reference to:
65[.]55.252.43
Observable ID: NCCIC:Observable-bfb9577a-f49e-49f8-8e71-02bf68e4cc1b
Which I've related to Indicator NCCIC:Indicator-3b9b8d85-ad2c-4759-83d7-b2b2d29e35be

The indicator is also related to a phase of the Lockheed Martin Kill Chain phase of "Command".



Command IP Address defined from Lockheed Martin Kill Chain

After our research, (nslookup and whois), we determined this to be a Microsoft node used for telemetry.

NSLOOKUP

```
$ nslookup 65.55.252.43
Server: 192.168.1.1
Address: 192.168.1.1#53

Non-authoritative answer:
43.252.55.65.in-addr.arpa name = msnbot-65-55-252-43.search.msn.com.
```

WHOIS

Snippet (Full Whois below):

> NetRange: 65.52.0.0 – 65.55.255.255
> CIDR: 65.52.0.0/14
> NetName: MICROSOFT-1BLK
> NetHandle: NET-65-52-0-0-1
> Parent: NET65 (NET-65-0-0-0-0)
> NetType: Direct Assignment
> OriginAS:
> Organization: Microsoft Corporation (MSFT)

Yep, that's pretty straight forward that it's part of the Microsoft block of IPs. With a little networking-foo, it can be determined that this MAY have been observed during the incident.. and if it were a CDN (which this isn't, from what we can tell), it MAY have been used to serve static content that acted as the C&C channel… but we know that this isn't forever bad, or permanently bad.

Impact to Analysts

If you aren't aware, give me a second to tell you about the startup I'm working on right now. I'm building a platform that allows communities to share and detect threat intelligence data. There are intelligence sharing communities out there (ISAC: Information Sharing and Analysis Center, ISAO: Information Sharing and Analysis Organization). ISACs are centered around critical infrastructure, ISAOs are centered around companies/industries of like-ness. Find more here:

National Council of ISACs (http://www.nationalisacs.org/)

DHS ISAO FAQ (https://www.dhs.gov/isao-faq)

We pull in data regularly on behalf of our customers in order to allow them to effectively leverage the intelligence. Essentially, we pull the data, and use it in our network monitoring platform to detect bad things for them. In addition to ISAC/ISAO data, we provide a 'community' around the DHS AIS data.

Ok, that's the context, now the reason I'm telling you this.

When a system like ours gets this 'muddy' intel data, our system lights up like a Christmas Tree. Within an hour of the DHS AIS system having the GRIZZLY STEPPE data available, we started notifying our customers that they're seeing those Observables (IOCs) on their network. AWESOME!! Except that the data is

pretty much determined to be a False Positive (FP). Sure, the intel was found during the analysis to write up the paper for US-CERT/DHS, but now every consumer of that intel has to determine that this Observable is a FP. Normally, every consumer would do this research. Thankfully, with a shared community around DHS AIS within our system, we do the research once, and suppress it for the time being. This goes to the power of a community as I write up in "Other People's Analysts (https://fauie.com/2016/12/29/other-peoples-analysts/)".

Ok, if you don't belong to an ISAC/ISAO, or any sharing communities, we'd be happy to help you find the right one. Check us out at https://perchsecurity.com or email 'info[@]perchsecurity[.]com'

> defanging email addresses in a blog post feels so 1999, but, I think I still have to do it....

Thanks for reading!

chris.

Appendix

Full WHOIS

```
$ whois 65.55.252.43

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/public/whoisinaccuracy/index.xhtml
#

#
# Query terms are ambiguous. The query is assumed to be:
# "n 65.55.252.43"
#
# Use "?" to get help.
#

#
# The following results may also be obtained via:
# https://whois.arin.net/rest/nets;q=65.55.252.43?
showDetails=true&showARIN=false&showNonArinTopLevelNet=false&ex
t=netref2
#

NetRange: 65.52.0.0 – 65.55.255.255
CIDR: 65.52.0.0/14
NetName: MICROSOFT-1BLK
NetHandle: NET-65-52-0-0-1
Parent: NET65 (NET-65-0-0-0-0)
NetType: Direct Assignment
OriginAS:
Organization: Microsoft Corporation (MSFT)
RegDate: 2001-02-14
Updated: 2013-08-20
Ref: https://whois.arin.net/rest/net/NET-65-52-0-0-1

OrgName: Microsoft Corporation
OrgId: MSFT
Address: One Microsoft Way
City: Redmond
StateProv: WA
```

PostalCode: 98052
Country: US
RegDate: 1998-07-10
Updated: 2016-06-30
Comment: To report suspected security issues specific to traffic emanating from Microsoft online services, including the distribution of malicious content or other illicit or illegal material through a Microsoft online service, please submit reports to:
Comment: * https://cert.microsoft.com.
Comment:
Comment: For SPAM and other abuse issues, such as Microsoft Accounts, please contact:
Comment: * abuse@microsoft.com.
Comment:
Comment: To report security vulnerabilities in Microsoft products and services, please contact:
Comment: * secure@microsoft.com.
Comment:
Comment: For legal and law enforcement-related requests, please contact:
Comment: * msndcc@microsoft.com
Comment:
Comment: For routing, peering or DNS issues, please
Comment: contact:
Comment: * IOC@microsoft.com
Ref: https://whois.arin.net/rest/org/MSFT

OrgAbuseHandle: MAC74-ARIN
OrgAbuseName: Microsoft Abuse Contact
OrgAbusePhone: +1-425-882-8080
OrgAbuseEmail: abuse@microsoft.com
OrgAbuseRef: https://whois.arin.net/rest/poc/MAC74-ARIN

OrgTechHandle: MRPD-ARIN
OrgTechName: Microsoft Routing, Peering, and DNS
OrgTechPhone: +1-425-882-8080
OrgTechEmail: IOC@microsoft.com
OrgTechRef: https://whois.arin.net/rest/poc/MRPD-ARIN

#
ARIN WHOIS data and services are subject to the Terms of Use
available at: https://www.arin.net/whois_tou.html

```
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/public/whoisinaccuracy/index.xhtml
#
```

Bad URI Found:

http://efax.pfdregistry.org/eFax/37486.ZIP

Bad Domain Names Found

editprod.waterfilter.in.ua efax.pfdregistry.net insta.reduct.ru littjohnwilhap.ru mymodule.waterfilter.in.ua one2shoppee.com private.directinvesting.com ritsoperrol.ru wilcarobbe.com www.cderlearn.com

Bad File Hashes Found

617BA99BE8A7D0771628344D209E9D8A
7FCE89D5E3D59D8E849D55D604B70A6F
81F1AF277010CB78755F08DFCC379CA6
8F154D23AC2071D7F179959AABA37AD5
AE7E3E531494B201FBF6021066DDD188

Bad IP Addresses Found

1.112.1.1 1.212.1.1 101.64.234.86 101.98.11.146 103.16.152.10 103.21.198.13 103.226.132.7 103.23.136.10 103.244.164.3 103.253.41.55 103.254.108.7 103.254.16.168 103.38.193.6 103.38.43.207 103.41.177.77 103.41.52.37 103.41.52.39 103.8.24.66 104.128.161.233 104.152.208.166 104.207.130.126 104.233.108.157 104.236.58.27 104.237.152.195 104.36.83.204 104.93.114.201 106.187.37.101 106.187.99.148 107.181.174.84 107.182.131.117 108.166.168.158 108.28.164.248 108.61.123.73 108.61.123.81 108.61.152.252 108.61.166.139 108.61.187.24 108.61.228.153 109.103.167.206 109.163.234.2 109.163.234.5 109.163.234.8 109.173.113.248 109.173.45.225 109.188.124.120 109.188.124.135 109.188.124.168 109.188.124.23 109.188.124.25 109.188.124.36 109.188.124.43 109.188.124.46 109.188.124.47 109.188.124.65 109.188.124.80 109.188.125.12 109.188.125.13 109.188.125.19 109.188.125.20 109.188.125.3 109.188.125.30 109.188.125.32 109.188.125.33 109.188.125.4 109.188.125.40 109.188.125.5 109.188.125.52 109.188.125.60 109.188.125.9 109.188.126.11 109.188.126.12 109.188.126.13 109.188.126.14 109.188.126.15 109.188.126.18 109.188.126.181 109.188.126.21 109.188.126.30 109.188.126.39 109.188.126.43 109.188.126.44

109.188.126.57 109.188.127.23 109.188.127.27 109.188.127.28 109.188.127.34
109.188.127.52 109.188.127.60 109.201.133.100 109.201.152.246 109.201.152.26
109.201.154.170 109.201.154.186 109.201.154.205 109.236.89.125 109.68.20.194
109.72.73.18 109.74.151.149 115.178.58.19 115.238.95.4 115.249.128.114
116.211.105.140 116.76.255.86 117.121.136.83 117.34.88.250 120.29.217.46
121.243.46.164 122.147.230.8 122.154.162.222 122.155.194.125 122.192.65.73
122.228.113.135 122.228.193.115 122.228.89.137 123.103.23.169 123.125.196.254
123.81.251.190 125.129.112.29 125.181.204.230 125.90.93.55 128.146.176.6
128.153.145.125 128.199.108.0 128.52.128.105 128.73.141.124 128.75.159.209
131.72.138.33 131.72.138.99 132.248.64.121 134.121.241.31 134.170.108.26
134.74.98.42 139.59.9.200 140.130.213.5 141.138.141.208 141.255.162.162
141.255.162.166 141.255.162.175 142.10.38.212 146.0.74.7 146.0.77.50
146.185.135.43 146.185.139.55 146.185.161.126 146.185.177.103 147.102.10.1
148.202.105.33 148.202.239.38 148.251.255.92 149.154.158.51 149.202.17.236
149.202.42.188 149.202.44.177 149.202.47.181 149.202.62.12 149.56.223.241
149.56.229.17 149.56.99.36 149.56.99.37 149.56.99.38 151.1.182.128
151.100.179.50 151.236.195.105 151.236.20.113 151.236.23.54 151.236.25.57
151.80.220.34 153.214.197.133 153.92.126.148 153.92.127.138 154.70.153.175
158.130.0.242 158.255.211.156 158.58.170.186 158.58.170.222 158.69.172.225
158.69.194.36 158.69.208.131 158.69.244.40 159.203.30.48 162.209.125.127
162.209.125.237 162.209.125.247 162.244.25.249 162.244.26.76 162.247.72.199
162.247.72.200 162.247.72.201 162.247.72.202 162.247.72.216 162.247.72.217
162.247.72.27 162.247.73.204 162.247.73.206 162.250.234.177 162.253.42.208
163.172.129.70 163.172.135.172 163.172.136.101 163.172.138.68 163.172.140.30
163.172.143.114 163.172.152.231 163.172.154.105 163.172.158.208 163.172.209.46
163.172.211.135 163.172.214.76 163.172.29.81 163.172.29.9 163.172.38.173
163.172.43.52 163.177.65.209 163.47.21.101 164.132.102.184 164.132.51.91
167.114.238.104 167.114.35.70 167.114.92.50 171.25.193.132 171.25.193.20
171.25.193.235 171.25.193.25 171.25.193.77 171.25.193.78 172.98.67.32
173.208.213.114 173.246.103.8 173.254.216.66 173.255.231.225 175.105.185.86
175.126.148.37 176.10.104.243 176.10.107.180 176.10.99.200 176.10.99.208
176.111.109.155 176.114.0.120 176.114.0.157 176.31.180.157 176.31.7.241
176.58.100.98 176.9.25.114 177.85.98.227 178.140.158.79 178.151.182.123
178.162.193.233 178.162.199.142 178.162.205.2 178.162.211.216 178.162.216.42
178.17.163.82 178.17.170.124 178.17.170.164 178.17.170.179 178.17.170.201
178.17.170.238 178.17.174.10 178.17.174.99 178.175.128.50 178.175.131.194
178.175.144.43 178.20.55.16 178.20.55.18 178.217.187.39 178.239.167.15
178.32.251.109 178.32.53.124 178.32.53.131 178.32.53.94 178.62.18.173 178.62.71.57
179.43.143.162 182.16.23.41 184.105.220.24 185.100.84.254 185.100.84.82
185.100.85.101 185.100.85.132 185.100.85.176 185.100.85.190 185.100.85.191
185.100.85.192 185.100.85.236 185.100.86.122 185.100.86.128 185.100.86.155

185.100.86.167 185.100.86.69 185.100.86.86 185.100.87.120 185.100.87.139
185.100.87.44 185.100.87.63 185.100.87.73 185.100.87.82 185.104.11.154
185.104.120.2 185.104.120.4 185.104.120.7 185.104.9.39 185.11.180.67
185.12.46.178 185.128.40.220 185.129.62.62 185.129.62.63 185.13.76.45
185.135.156.94 185.16.200.176 185.17.184.228 185.3.135.58 185.34.33.2
185.36.100.145 185.38.14.171 185.38.14.215 185.55.217.127 185.61.138.104
185.65.134.75 185.65.134.76 185.65.134.81 185.69.168.112 185.7.34.251
185.76.35.10 185.76.35.11 185.77.128.27 185.80.222.78 185.80.50.33
185.82.202.102 185.82.202.174 185.82.202.45 185.86.148.111 185.86.148.227
185.86.149.223 185.86.149.97 186.215.192.2 188.126.81.155 188.138.1.217
188.138.9.41 188.162.64.72 188.162.64.83 188.42.254.26 188.93.234.203
190.97.163.207 191.96.66.15 192.121.252.153 192.121.46.121 192.151.155.130
192.160.102.164 192.160.102.166 192.195.80.10 192.198.82.58 192.207.61.178
192.40.57.129 193.111.136.162 193.138.219.231 193.15.16.4 193.169.4.29
193.169.86.78 193.169.87.71 193.171.202.150 193.182.144.34 193.200.241.195
193.238.157.16 193.24.208.113 193.24.240.200 193.90.12.86 193.90.12.87
193.90.12.88 193.90.12.89 193.90.12.90 194.187.249.135 194.187.249.87
194.88.143.66 195.154.15.227 195.154.255.174 195.154.8.111 195.154.81.29
195.154.90.122 195.228.45.176 197.251.205.172 198.105.125.74 198.134.125.78
198.167.223.38 198.50.159.231 198.50.177.202 198.50.200.131 198.50.200.135
198.50.200.137 198.50.200.139 198.58.107.53 198.96.155.3 199.127.226.150
199.59.148.23 199.68.196.125 199.71.233.138 199.71.233.139 199.71.233.140
199.71.233.141 199.71.233.142 199.87.154.251 199.87.154.255 2.189.142.80
201.77.124.118 202.158.120.51 202.28.103.150 202.28.194.6 203.157.155.8
203.169.48.15 203.190.241.33 203.218.5.241 204.11.50.131 204.155.30.75
204.155.30.76 204.155.30.77 204.155.30.78 204.155.30.79 204.155.30.80
204.155.30.81 204.155.30.82 204.194.29.4 204.85.191.30 207.176.226.8
207.244.70.35 207.244.97.183 209.133.66.214 209.222.77.220 209.249.180.198
209.66.119.150 210.14.70.140 210.245.123.180 211.194.50.61 211.226.72.236
212.109.194.126 212.113.32.242 212.117.180.130 212.117.180.21 212.47.194.250
212.47.195.52 212.47.227.72 212.47.238.193 212.47.246.21 212.47.247.226
212.47.248.81 212.68.41.83 212.7.192.148 212.7.217.50 212.7.219.155 212.83.190.65
212.83.40.238 212.83.40.239 213.179.207.166 213.202.214.148 213.215.9.162
213.39.51.93 216.110.195.12 216.17.99.183 216.218.134.12 216.230.148.77
216.239.90.19 216.58.216.142 216.58.216.174 216.75.21.31 217.115.10.131
217.115.10.132 217.12.201.109 217.12.204.104 217.13.197.5 217.13.56.9 217.23.10.184
217.23.10.188 217.23.10.189 217.23.12.10 217.23.14.168 217.79.188.43
219.249.95.108 221.138.128.116 23.239.10.144 23.254.211.232 27.111.202.78
27.24.190.240 27.50.94.251 31.132.0.11 31.132.0.12 31.148.219.166 31.148.219.168
31.148.219.176 31.148.219.50 31.16.91.237 31.168.172.147 31.185.104.19
31.186.96.19 31.186.96.20 31.192.228.185 31.210.109.147 31.210.111.154

31.210.117.131 31.210.118.89 31.210.123.213 31.210.123.214 31.210.125.100
31.210.125.105 31.210.125.99 31.220.43.99 31.31.72.43 35.0.127.52 37.0.127.44
37.123.130.176 37.123.130.186 37.139.52.47 37.146.14.44 37.187.239.8 37.187.247.3
37.187.7.74 37.220.35.202 37.220.35.36 37.233.99.157 37.235.53.237 37.247.54.157
37.48.109.107 37.48.93.246 37.59.123.142 37.59.14.201 37.59.42.55 37.59.63.190
38.110.220.169 41.206.188.206 41.212.1.1 41.215.241.147 41.77.136.250 42.1.1.1
42.112.33.43 42.51.11.66 43.1.1.1 45.32.239.246 45.33.48.204 45.55.178.34
45.56.90.85 45.62.255.94 45.79.85.112 46.101.138.211 46.101.197.155
46.102.152.132 46.105.100.149 46.108.39.193 46.108.39.198 46.148.17.100
46.148.17.210 46.148.17.98 46.148.17.99 46.148.26.78 46.165.196.229 46.165.197.1
46.165.223.217 46.165.228.119 46.165.230.5 46.166.137.224 46.166.137.240
46.166.137.245 46.166.138.129 46.166.138.141 46.166.138.142 46.166.138.147
46.166.186.243 46.166.188.208 46.166.188.228 46.166.190.182 46.166.190.192
46.166.190.223 46.17.100.14 46.182.106.190 46.242.66.240 46.28.110.136
46.28.111.122 46.28.68.158 46.29.248.238 46.39.102.250 46.4.193.146
46.73.164.160 5.1.82.130 5.1.82.140 5.133.179.243 5.133.8.152 5.133.8.162
5.134.1.250 5.135.158.101 5.135.186.35 5.135.199.28 5.135.65.145 5.135.65.146
5.149.249.172 5.149.254.114 5.152.205.159 5.153.233.58 5.153.234.90 5.157.38.34
5.189.188.111 5.196.1.129 5.196.58.96 5.199.171.58 5.199.172.147 5.2.64.10 5.212.1.1
5.249.145.164 5.255.80.27 5.28.62.85 5.34.150.2 5.34.183.55 5.40.21.27
5.45.183.194 5.56.133.125 5.56.133.19 5.56.133.23 5.77.47.142 5.9.32.230 5.9.98.43
50.2.64.140 50.7.176.2 50.7.62.27 51.254.215.7 51.255.202.66 51.255.33.0
51.255.38.226 52.29.252.84 54.146.128.140 58.20.114.95 58.250.19.237
58.49.61.252 58.68.148.37 58.68.148.42 58.80.109.59 58.83.208.24 59.115.115.115
60.12.119.222 60.18.131.233 60.18.147.185 60.190.22.202 60.191.138.222
60.191.139.42 60.191.139.86 60.2.237.27 60.211.204.110 61.135.149.124
61.144.244.217 62.1.1.1 62.102.148.67 62.113.238.165 62.149.25.15 62.193.51.144
62.210.105.116 62.210.129.246 62.212.73.141 62.244.176.139 62.4.22.48
63.141.226.34 63.214.136.153 64.113.32.29 64.124.32.84 64.137.178.3 64.137.206.52
64.137.215.208 64.27.12.41 64.27.17.140 64.79.108.197 65.15.88.243 65.158.81.132
65.181.112.128 65.19.167.130 65.19.167.131 65.19.167.132 65.23.129.79 65.36.205.1
65.55.252.43 66.158.142.2 66.180.193.219 66.196.116.112 67.52.39.166
68.64.143.103 69.10.162.154 69.12.73.174 69.162.139.9 69.25.242.15 69.30.251.26
69.30.251.27 69.30.251.28 69.30.251.29 69.30.251.30 69.63.147.49 69.70.199.50
69.89.191.8 69.89.37.90 69.89.37.91 69.89.37.92 71.19.157.127 72.21.91.121
72.30.196.161 72.5.72.225 72.52.75.27 74.11.216.239 74.208.191.194
74.208.191.202 74.217.184.206 78.106.220.129 78.108.154.254 78.138.104.178
78.138.106.231 78.138.106.234 78.138.106.235 78.138.106.247 78.138.97.15
78.138.98.92 78.138.98.95 79.134.234.247 79.134.255.200 79.143.111.228
79.172.193.32 79.98.107.90 8.39.147.120 80.221.159.67 80.240.139.111
80.244.81.191 80.255.12.232 80.67.172.162 81.17.18.50 81.170.184.90

81.171.56.203 81.210.129.164 81.30.158.81 81.7.15.115 81.7.16.13 81.95.126.15
82.163.79.61 82.211.19.129 82.211.19.143 82.221.129.96 82.221.139.25
83.136.253.147 83.138.176.21 83.220.236.147 84.117.113.152 84.200.56.34
84.232.5.230 84.251.91.165 85.143.219.211 85.143.95.50 85.159.237.210
85.195.97.226 85.195.97.227 85.195.97.230 85.204.74.91 85.207.155.39 85.24.197.4
85.248.227.163 85.248.227.164 85.248.227.165 85.25.100.104 85.25.103.119
85.90.244.52 86.105.18.111 86.127.210.14 87.120.254.200 87.170.206.84
87.185.31.200 87.236.194.23 87.236.211.182 88.150.157.14 88.198.14.171
88.198.25.92 88.80.7.5 89.163.135.98 89.163.142.94 89.163.237.45 89.169.218.249
89.187.142.208 89.187.144.122 89.187.145.103 89.188.9.91 89.190.34.200
89.248.162.179 89.31.57.5 89.32.40.4 89.33.246.114 89.34.237.101 89.34.237.11
89.34.237.12 89.35.178.104 89.36.208.231 89.45.67.6 89.46.101.79 90.154.72.187
91.1.1.1 91.108.183.170 91.121.230.209 91.134.232.63 91.146.121.3 91.213.8.235
91.213.8.236 91.213.8.84 91.217.91.79 91.219.236.136 91.219.236.218
91.219.236.222 91.219.236.232 91.219.238.231 91.219.239.245 91.219.30.81
91.228.151.52 91.229.77.64 91.230.60.42 91.230.61.68 91.241.33.73 92.114.92.107
92.114.92.125 92.222.103.234 92.222.28.243 92.222.6.12 92.222.71.173 92.222.88.7
92.222.92.152 92.240.253.181 93.115.241.194 93.115.38.141 93.115.94.23
93.115.94.26 93.115.95.201 93.115.95.202 93.115.95.205 93.115.95.39
93.171.203.244 93.174.90.30 93.174.93.133 93.184.215.200 93.184.66.227
93.219.113.201 94.102.49.175 94.102.49.64 94.102.53.177 94.102.63.139
94.103.175.86 94.126.8.21 94.142.242.84 94.185.85.42 94.185.85.43 94.185.85.44
94.185.85.46 94.198.100.8 94.23.147.30 94.242.195.186 94.242.206.196
94.242.222.23 94.242.239.162 94.242.239.163 94.242.239.165 94.242.239.177
94.242.239.181 94.242.239.183 94.242.239.189 94.242.251.32 94.242.57.104
94.242.57.2 94.254.2.71 94.26.140.150 94.31.53.203 95.0.26.199 95.105.72.78
95.130.11.147 95.153.31.53 95.163.107.14 95.163.107.15 95.183.50.23 95.211.205.151
95.211.214.81 95.213.157.140 95.213.157.141 95.215.44.115 97.74.237.196
98.138.199.240 98.138.79.73

Short URL: http://bit.ly/2hCug5J (http://bit.ly/2hCug5J)

fauie.com (https://fauie.com/2016/12/30/grizzly-steppe-lighting-up-like-a-christmas-tree/) · by Chris Fauerbach