Reported as Confirmed Log4Shell Payloads
Credible sources have observed trusted reporting, or directly observed, the following malware payloads, and their linked distribution IP address. All of the distribution IP addresses have been callbacks from Log4Shell exploitation. Malware names, where applicable, are also listed.

3.145.115.94 - **f2e3f685256e5f31b05fc9f9ca470f527d7fdae28fa3190c8eba179473e20789** (**Khonsari**)
3.145.115.94 - **95bac3dbd20a3af70864dbeb07b41537e84ba02bcf1a8c1dc7e20187ef590658**
45.146.164.160 - **a6ef8216979b8b7f8f033bbcba91b4cba9a8cead9c4553e0855cd51956f61efd** (Empire **Stager**)
45.146.164.160 - **ed77c28f2115e221d32e032db915ddd4247b665aa28e9f391f96b1730a41a861** (Empire **Stager**)
mctw-entry.herokuapp.com/Deploy01.class
- **7123f2f82fccfcb3a1dfd17f6d93f711062848f139106585bbb2f62c59fcea62**
31.220.58.29 - **2b5f04d15e459132a5935260746788db39b469ea46859c4a5bb8625f8a80bd41**
31.220.58.29 - **eb76b7fb22dd442ba7d5064dce4cec79e6db745ace7019b6dfe5642782bf8660**
45.146.164.160 - **7405784a9c08161ca6f344659f7d8ccf54d407fe3fa22cbf0e6a9698ed6c0e79**
167.172.44.255 - **6b293d92fe1415e7c1430f53b6b7afc3e94385e7452fe5704f65444b3bfd1aef**
92.242.40.21 - **7e9663f87255ae2ff78eb882efe8736431368f341849fec000543f027bdb4512** (**Kinsing**)
92.242.40.21 - **3ba2c4ae64be8d03747dffd5e4dc98730a54fdbb4aad50516428dc2507fdbfcf** (**Kinsing**)
80.71.158.44 - **4d44e9ffdaa91e0d63795b9a263a19ad1edd330d800005708cd44710ac09e653** (**Kinsing**)
80.71.158.12 - **063ccf736c2c19ca5db70b8d8a7cf00377899c16023c63fee836bdefadd336c1** (**CoinMiner**)
80.71.158.12 - **86131d16b06cefe85b96e3ceaa6f3291b03c60c5b8d5196eb68d2a72e29f311f** (**CoinMiner**)
http://agent.apacheorg.top:1234/xmss
159.89.182.117 - **ac8f86909b45f36d7ab862081bce71676b1e90b5c22f195d359a023eb7bf2589**
159.89.182.117 - **0f5cb7f8c43d3ebf71d7e22a2ac2fb94d0457ffea870daa2c402508caa39aca8**
62.210.130.250 - **3f6120ca0ff7cf6389ce392d4018a5e40b131a083b071187bf54c900e2edad26**
93.189.42.8 - **46bd3a99981688996224579db32c46af17f8d29a6c90401fb2f13e918469aff6**
93.189.42.8 - **6f512377d499668f81a26662d0a0a747747e7e7641d217ef96d3aab16f0a235f**
45.155.205.233 - **e22bfa4dfa8e7bb5edac4394344baa2b66c0cf42c514b9c468431497eec2ce0f**
62.182.158.156 - **be52669997419cd52e42262e5b9049cafe3fe591c8ff2d1b2380e5835b666c63**
155.94.154.170 - **90ee1a8e8f0ea5085b83b8efe174674a93260b599729bf53e1b140e2acc7d26f** (**Elknot**)
155.94.154.170 - **90ee1a8e8f0ea5085b83b8efe174674a93260b599729bf53e1b140e2acc7d26f** (**Elknot**)
205.185.113.59 - **10fad59b071db09aafcb7f40e775f28180aed182786557e9ee7f2f2e332b4513**
170.178.196.41 - **138e372113f10e9caeefddd9fbd52eccb30382d4dc965a74f5be669ee0634c79** (Meterpreter)
141.98.83.139 - **760839a67fbd2b2b00bd4384af69e0f22a90a8da1a5695b6ef4d67dc459684c9**
154.82.110.5 - **36796319567f5a05571006b874903e87**
185.250.148.157 - **933568969efe6b3f8c0621200f0eea5a**
47.243.78.246 - **5ac6ded41f9a61cd9d026e91af47b695**

IP Addresses
3.145.115.94
45.146.164.160
167.172.44.255
31.220.58.29
92.242.40.21
159.89.182.117
45.155.205.233
154.82.110.5
62.182.158.156

47.243.78.246
93.189.42.8
185.250.148.157
205.185.113.59
141.98.83.139
170.178.196.41
155.94.154.170
80.71.158.12
80.71.158.44
62.210.130.250

Domain **mctw-entry.herokuapp.com**

Hashes **ed77c28f2115e221d32e032db915ddd4247b665aa28e9f391f96b1730a41a861**
3ba2c4ae64be8d03747dffd5e4dc98730a54fdbb4aad50516428dc2507fdbfcf
eb76b7fb22dd442ba7d5064dce4cec79e6db745ace7019b6dfe5642782bf8660
a6ef8216979b8b7f8f033bbcba91b4cba9a8cead9c4553e0855cd51956f61efd
2b5f04d15e459132a5935260746788db39b469ea46859c4a5bb8625f8a80bd41
f2e3f685256e5f31b05fc9f9ca470f527d7fdae28fa3190c8eba179473e20789
7123f2f82fccfcb3a1dfd17f6d93f711062848f139106585bbb2f62c59fcea62
7e9663f87255ae2ff78eb882efe8736431368f341849fec000543f027bdb4512
7405784a9c08161ca6f344659f7d8ccf54d407fe3fa22cbf0e6a9698ed6c0e79
6b293d92fe1415e7c1430f53b6b7afc3e94385e7452fe5704f65444b3bfd1aef
ac8f86909b45f36d7ab862081bce71676b1e90b5c22f195d359a023eb7bf2589
4d44e9ffdaa91e0d63795b9a263a19ad1edd330d800005708cd44710ac09e653
e22bfa4dfa8e7bb5edac4394344baa2b66c0cf42c514b9c468431497eec2ce0f
36796319567f5a05571006b874903e87
5ac6ded41f9a61cd9d026e91af47b695
90ee1a8e8f0ea5085b83b8efe174674a93260b599729bf53e1b140e2acc7d26f
6f512377d499668f81a26662d0a0a747747e7e7641d217ef96d3aab16f0a235f
86131d16b06cefe85b96e3ceaa6f3291b03c60c5b8d5196eb68d2a72e29f311f

	138e372113f10e9caeefddd9fbd52eccb30382d4dc965a74f5be669ee0634c79 **063ccf736c2c19ca5db70b8d8a7cf00377899c16023c63fee836bdefadd336c1** **0f5cb7f8c43d3ebf71d7e22a2ac2fb94d0457ffea870daa2c402508caa39aca8** **3f6120ca0ff7cf6389ce392d4018a5e40b131a083b071187bf54c900e2edad26** **46bd3a99981688996224579db32c46af17f8d29a6c90401fb2f13e918469aff6** **be52669997419cd52e42262e5b9049cafe3fe591c8ff2d1b2380e5835b666c63** **760839a67fbd2b2b00bd4384af69e0f22a90a8da1a5695b6ef4d67dc459684c9** **933568969efe6b3f8c0621200f0eea5a** **10fad59b071db09aafcb7f40e775f28180aed182786557e9ee7f2f2e332b4513** **95bac3dbd20a3af70864dbeb07b41537e84ba02bcf1a8c1dc7e20187ef590658**
Person	**Stager**
Vulnerability	**CVE-2021-44228 (Log4Shell)**
URL	**http://agent.apacheorg.top/xmss**
Malwares	**Elknot** **CoinMiner** **Kinsing** **Khonsari Ransomware**
Validation URLs	https://businessinsights.bitdefender.com/technical-advisory-zero-day-critical-vulnerability-in-log4j2-exploited-in-the-wild https://urlscan.io/search/#files.mimeType%3A%22application%2Fx-java-applet%22%20 https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/ https://www.cadosecurity.com/analysis-of-novel-khonsari-ransomware-deployed-by-the-log4shell-vulnerability/ https://blog.netlab.360.com/ten-families-of-malicious-samples-are-spreading-using-the-log4j2-vulnerability-now/ https://www.trendmicro.com/en_us/research/21/l/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html