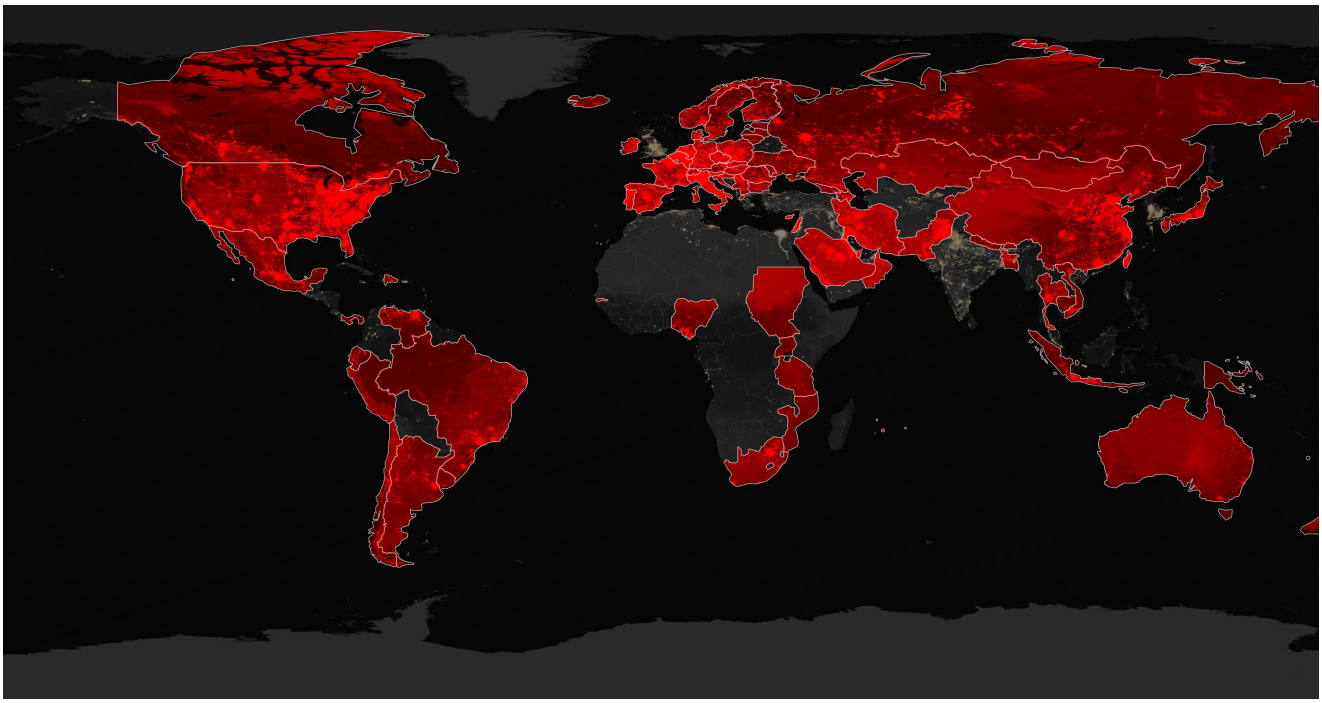
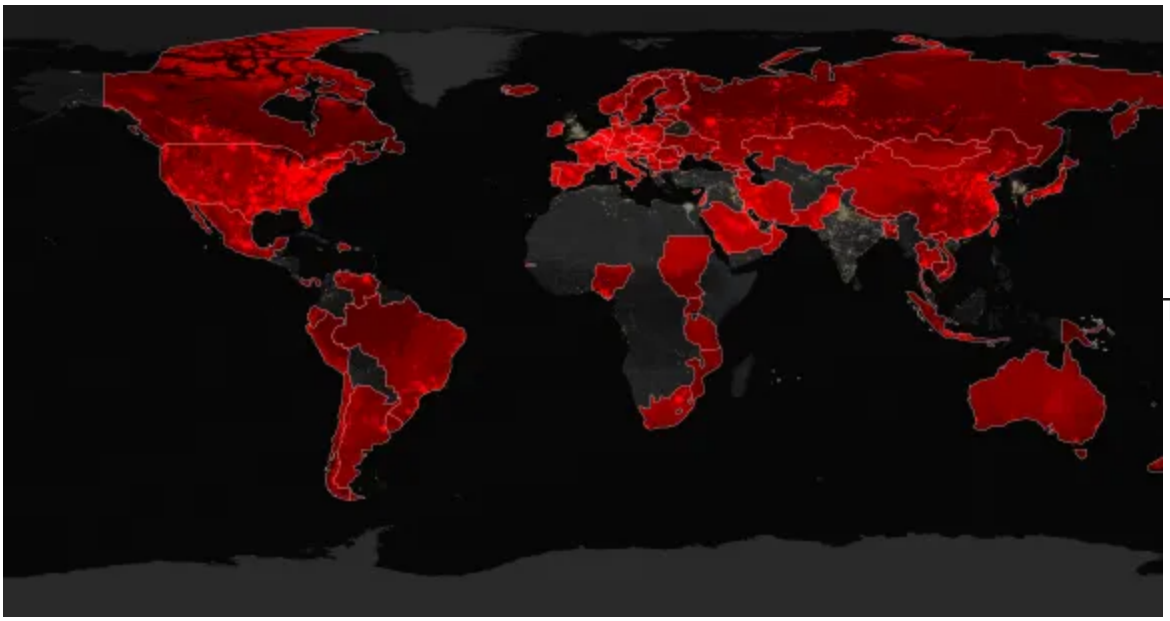
Kobalos Malware Mapping

team-cymru.com/blog/2021/02/05/kobalos-malware-mapping/

David Monnier View all posts by David Monnier February 5, 2021





Team Cymru works with CSIRTs worldwide.

On February 2nd the great team at ESET released their findings on malware being used to compromise UNIX-like systems, including various distributions of Linux and also FreeBSD, named Kobalos.

Malware that targets these platforms is always of great interest to me. Having started my career in high performance computing (HPC) and then having moved into hardened Linux system architecting, I can say that it is not often we get the chance to study wide-spread malware that targets these operating systems.

Kobalos is designed to replace the ssh client and server on a host. Once installed, it replaces the normal ssh to allow collection of passwords to be used to access remote hosts. As the listening service, it creates a backdoor when a client connects with the specific TCP source port of 55201. This specific detail allows us to leverage Team Cymru's Pure Signal™ threat reconnaissance solution to understand the potential size and scope of the Kobalos network.

Using a signature of TCP connections with a destination port of 22 and a source port of 55201, and removing noise like syn-scanners and other noisy hosts, we were able to look at the past seven days of Internet activity. With search parameters we see 3475 hosts across 1460 separate ASNs.

Given the ephemeral and service port combination as the only litmus, it's possible that this port combination seen across the Internet is a coincidence. However, as it is our only IOC that can be applied externally, this will have to do. That said, here is the list of potentially impacted networks.

https://www.cymru.com/ThreatReports/Kobalos_ASN050221.txt

The full IP list, and this kind of data, is shared daily via our CSIRT Assistance Program and our membership in various trust groups. If you see your network listed and you're not aware of how to get started receiving alerts, please don't hesitate to contact us.

My thanks again to the fine team at ESET. Without their sharing of these indicators, we couldn't have looked into the scope of this activity. If you're a researcher and have an IOC you'd like to see matched against our Pure Signal intelligence, drop me a line!