Botnet Homology Method Based on Symbolic Approximation Algorithm of Communication Characteristic Curve

Submitted by grigby1 on Fri, 04/05/2019 - 10:23am

Title	Botnet Homology Method Based on Symbolic Approximation Algorithm of Communication Characteristic Curve
Publication Type	Conference Paper
Year of Publication	2018
Authors	Nan, Z., Zhai, L., Zhai, L., Liu, H.
Conference Name	2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)
Keywords	Approximation algorithms, Botnet, botnet client, botnet control server, botnet homology method, botnets, clustering, Clustering algorithms, command and control systems, command control channels, command interaction, communication characteristic curve, compositionality, computational complexity, computer network security, dynamic network communication characteristic curves, dynamic time warping distance clustering, earliest botnet group, effective detection method, extracted curve, Heuristic algorithms, homogenous botnet, homologous botnets, homology, Internet, invasive software, IP networks, IRC botnet, IRC protocol, Metrics, most significant botnet group, multiple zombies hosts, network servers, network traffic, packet capture traffic monitoring, pattern clustering, Protocols, pubcrawl, resilience, Resiliency, Servers, symbolic approximation algorithm, telecommunication traffic, time series, Time series analysis, time warp simulation
Abstract	The IRC botnet is the earliest and most significant botnet group that has a significant impact. Its characteristic is to control multiple zombies hosts through the IRC protocol and constructing command control channels. Relevant research analyzes the large amount of network traffic generated by command interaction between the botnet client and the C&C server. Packet capture traffic monitoring on the network is currently a more effective detection method, but this information does not reflect the essential characteristics of the IRC botnet. The increase in the amount of erroneous judgments has often occurred. To identify whether the botnet control server is a homogenous botnet, dynamic network communication characteristic curves are extracted. For unequal time series, dynamic time warping distance clustering is used to identify the homologous botnets by category, and in order to improve detection. Speed, experiments will use SAX to reduce the dimension of the extracted curve, reducing the time cost without reducing the accuracy.

DOI 10.1109/AVSS.2018.8639356
Citation Key nan_botnet_2018

internet resilience pubcrawl Metrics invasive software computational complexity computer network security Servers Approximation algorithms pattern clustering IP networks telecommunication traffic botnet Protocols Clustering algorithms Compositionality network traffic Heuristic algorithms command and control systems Resiliency time series Time series analysis botnet client botnet control server botnet homology method clustering command control channels command interaction communication characteristic curve dynamic network communication characteristic curves dynamic time warping distance clustering earliest botnet group effective detection method extracted curve homogenous botnet homologous botnets homology IRC botnet IRC protocol most significant botnet group multiple zombies hosts network servers packet capture traffic monitoring symbolic approximation algorithm time warp simulation botnets