Recurring outlier network connection analysis for RAT detection

Ezekiel Kruglick, Ph.D.

***Abstract*—This paper was originally submitted to Xinova as a response to a Request for Invention (RFI) on cyber-attack forecasting, detection, and stabilization methods. In this paper, a RAT detection analysis for recurring outlier network connections is proposed.**

In more detail, this describes a solution that can detect repeated "unusual" connections, when any single machine making unusual numbers of outliers is either compromised or has a user performing something deemed unusual.

I. Introduction

AFTER initial compromise, attackers often download and install a Remote Access Trojan (RAT) to establish a persistent, long-term, remote access to an environment. Sometimes the RAT is the initial infection, for example delivered via email[i]. These Trojans often provide long-term vulnerability and may be established months or even years in advance of a main attack. Such RATs communicate with command and control infrastructure that is very complex.

To avoid detection RATs may have lists of hundreds of domains they communicate with, sending and receiving messages to any one address perhaps less than once a year to avoid detection. For some RATs this is done one each contact whereupon the RAT is given the next few addresses to try (multiple addresses are kept in case one is detected and black-holed). For other RATs they may have a complex hashing-style algorithm to generate addresses dynamically. To serve many of these RATs some malware groups register immense numbers of nonsensical domain names.

II. Summary of the invention

The solution is a signature-free detection means for enterprise-level detection of RAT and other Advanced Persistent Threat (APT) attacks. The solution works by collecting aggregate network traffic data and looking for single machines (small source node count) that communicate with a large number of rare/unique external addresses (large rare destination node count).

This is different from previous systems which, at their most similar, use ad hoc rules of thumb to try to recognize suspicious network destinations. The benefit here is that enterprise scale (which may be from a single large customer or across customers for a security provider to benefit from scale) network data can be used to automatically figure out which computers are engaged in RAT command-and-control style communication patterns.

The closest existing work is probably Zhao et. Al. [ii] which sampled large amounts of network traffic and attempted both signature and anomaly-based detection. Signature-based detection is complementary but not relevant to the concept presented here because it presumes captive and analyzed samples of the malware are available. The anomaly based detector presented by Zhao is designed for single-machine level analysis and thus limited to ad hoc features to look for suspicious communications, for example they look for "Phishing names", IPs that are "silent" (don't respond to normal requests), and communications that are slow ("Very Low frequency query"), for example exchanging packets once per day.

By contrast, here we present the concept of taking the traffic from a large organization, using it to determine IP addresses that are very rare or unique among the communications of that organization, and then identifying single machines within the organization that communicate with a statistically large number of these rare or unique destinations. This approach has the benefit of automatically building and adapting the connection statistics to match both a particular population of users and their use over time.

This is complementary and may be used together with previous solutions, but gains advantage from scale and is capable of detecting novel attackers even with zero-day exploits.

III. Detailed Explanation

This system may work from live network traffic or from log data. For the sake of discussion, we will assume below working from log data, for example on a batch basis run when servers are less busy. Real-time data analysis techniques can be applied for each piece presented.

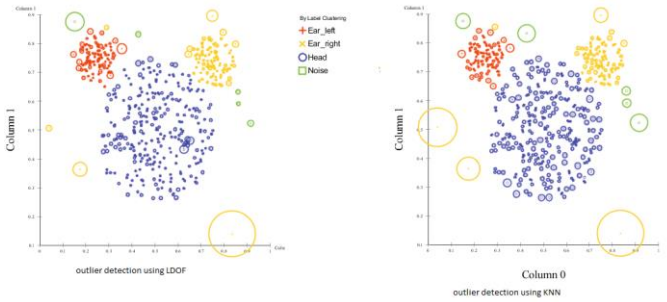
An example implementation might be described as below:

1. Enterprise network logs record IP access communications from computers on the network
2. Statistical distributions are generated from the network logs
3. Infrequency (or rareness) scores are generated for the rarest destination addresses
4. A metric is accumulated for each specific machine based on the infrequency scores

5. Machines with the highest accumulated metric, which thus have statistically unusually high numbers of contacts with unusual destinations, are identified for further actions

The additional actions taken may be proactive - such as increased security limitations - or may simply involve highlighting the devices and traffic to humans for evaluation.

Fig. 1. Nearest Neighbor Grouping



Outlier detection can be done using any desired characteristics. As in Figure 1 shows using K-nearest-neighbor grouping on parametrically reduced representation. In practice, network data will have many dimensions to analyze.

IV. Conclusion

In order to test and demonstrate an enterprise level offering, it would be good to obtain a large reservoir of network logs to perform an example analysis. This would be helpful in drafting the exact implementation of features such as role-attached or device-attached filtering rules or special whitelists. To demonstrate proof of concept, analysis on network activity to generate infrequency scores in the presence of whitelisting may be beneficial. Similarly, generating specific suspicion metrics on a per-machine level based on the infrequency scoring would be recommended.

Acknowledgment

This research was originally submitted to Xinova, LLC by the author in response to a Request for Invention. It is among several submissions that Xinova has chosen to make available to the wider community. The author wishes to thank Xinova, LLC for their funding support of this research.

More information about Xinova, LLC is available at www.xinova.com.

References

[i] https://blog.trendmicro.com/trendlabs-security-intelligence/spam-remote-access-trojan-adwind-jrat/ community

[ii] G. Zhao, K. Xu, L. Xu, and B. Wu, “Detecting APT Malware Infections Based on Malicious DNS and Traffic Analysis,” IEEE Access, vol. 3, pp. 1132–1142, 2015.