MUNI
C4E

Towards an Efficient Detection of Pivoting Activity

Martin Husák[1], Giovanni Apruzzese[2], Shanchieh Jay Yang[3], Gordon Werner[3]
husakm@ics.muni.cz, giovanni.apruzzese@uni.li, jay.yang@rit.edu, gxw9834@rit.edu

[1] Institute of Computer Science, Masaryk University
[2] Institute of Information Systems, University of Liechtenstein
[3] Department of Computer Engineering, Rochester Institute of Technology

May 21, 2021

Part I

Introduction

Motivation & Goals

Motivation

- Pivoting is a powerful technique, when used by adversaries

  If a network is accessible only through a VPN server, the adversary may exploit the VPN server to get access inside
- Pivoting detection capabilities are limited:

  Many phenomena may look like pivoting and cause false positive detections

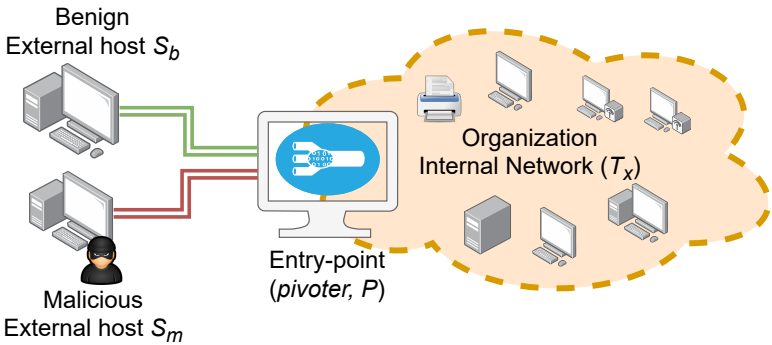
Research questions

1. Which phenomena are similar to pivoting?
2. Which NetFlow features are intrinsic to pivoting?
3. How to automatically reduce false positives?

Part II

Pivoting

Pivoting Scenario



From now on, *S* stands for Source, *P* for Pivot, and *T* for Target.

Existing Pivoting Detection Methods

- G. Apruzzese, F. Pierazzi, M. Colajanni, and M. Marchetti, “Detection and threat prioritization of pivoting attacks in large networks,” *IEEE Transactions on Emerging Topics in Computing*, vol. 8, no. 2, pp. 404–415, 2020.
- Temporal graph-analytics to detect pivoting by analyzing NetFlow data
  - *S* and *T* *must* go through *P*
  - *P* forwards the communications to *T* *after* receiving the communications from *S*
  - Pairs of NetFlows linking *S* with *P*, and *P* with *T*, are separated by at most ϵ time units
- Evaluated only in internal network with no background noise
- Would generate large number of false positives even with very small values of ϵ

Pivoting Detection Methodology

Splitting the detection in two phases:

- Pivoting candidate detection using the existing algorithm
- Pivoting selection over detection candidates

Pivoting candidate detection - consider network flows f_1 and f_2:

- destination IP of f_1 is source IP of f_2
- destination IP of f_2 is not source IP of f_1
- protocol and destination ports are the same in f_1 and f_2
- $\epsilon = 1s$: f_2 appears after f_1 but no later then 1 second after f_1

Pivoting selection

- Manual and automated, as shown later

Discovery of Phenomena Similar to Pivoting

Pivoting is expected if:

- the protocol that allow remote access, such as SSH, RDP, and Telnet
- S is anywhere in the Internet or T is in the internal network
- The set of S, P, and T is rather unique
- The duration of flows and numbers of transferred bytes/packets/flows are similar

False positive detection is expected if:

- The protocol is DNS, SMTP, or other benign protocol (in the context of pivoting)
- All actors are from the same network (e.g., internal) or are well-known and the activity may be explained otherwise
- There are many candidates with the same P and T but different S

Automatically Identifying Intrinsic Features

The following features will be observed:

- *S*, *P*, *T* Count – number of candidates that share the same *S*, *P*, or *T*
- *S*, *P*, *T* Location – location of the given IP address, i.e., 'Private' for ranges like 10.0.0.0/8, 'Internal' for the IP range of the organization, 'External' for IP addresses in the Internet
- Duration, In/Out Packets, In/Out Bytes, Flows ratios – the values of the first biflow (source to pivot) divided by the second biflow (from pivot to target)

Principal Component Analysis will be used to select the most meaningful features and their combinations

Part III

Experiment Results

Experiment Setup

Measurements

- Masaryk University campus network (public /16 IPv4 and /48 IPv6, private networks)
- NetFlow probe near server segment, including a VPN server and Wi-Fi access points
- Data from a full working day

Content

- Internet <-> Public IPs, Public IPs <-> Private IPs
- Only a few firewall rules, most of the traffic is enabled

Pivoting Candidate Detection

Candidates	Dst Port	Service	Comment
69,393	TCP 443	HTTPS	Mostly benign, further inspection required
6,102	TCP 53	DNS	Benign, legitimate servers
5,362	TCP 25	SMTP	Benign, legitimate servers
3,456	TCP 51413	BitTorrent	Benign, personal computers
2,251	UDP 6881	BitTorrent	Benign, personal computers
133	TCP 22	SSH	Suspicious candidates

- No candidates found on ports 3389 (RDP) and 23 (Telnet)
- Numerous other candidates were found in BitTorrent, VoIP, and online gaming traffic

Manual Investigation of Pivoting Candidates

SSH Candidates

- 7 distinct pivots, 3 benign and 4 suspicious
- Benign pivots initiated connections only to one other host, e.g.,
  - The machine accepted many connections throughout the day from many hosts
  - The single outgoing connection was a git checkout/commit or data back-up
  - No similarity between the flows -> random false positive
- Suspicious pivots – 13 candidates
  - Either Internet->Public->Internet or Public->Internet->Public

HTTP(S) candidates

- Mostly common and benign behavior of the protocol
- Left for future work, deeper analysis of HTTP headers or TLS is recommended

Investigation of Pivoting Candidates

False positives	HTTP(S)	70,312
	other services - DNS, SMTP, NTP	12,714
	p2p - BitTorrent, VoIP, online gaming	7,615
	SSH	120
True pivoting	SSH	**13**
Total		**90,774**

- Huge imbalance, very low number of suspicious candidates complicates the analysis
- Strong motivation for the reduction of false positives and future work

Principal Component Analysis

Setup

- Manually selected SSH candidates labeled as *Suspicious* or *Benign*
- Kaiser criterion – selecting only principal components with eigenvalue > 1
- Requirement on at least 90% of the variance explained for future analysis

Findings

- Strong association with 'Internal' S and T and 'External' P or vice versa
- Strong association with 'count' features, namely P and T count
- Rare associations with 'ratio' features

Part IV

Conclusion

Conclusion

Conclusion

- Accurate detection of pivoting activities is of paramount importance
- Existing approaches work only under specific circumstances
- The rate of false positives is overwhelming due to similar phenomena (e.g., p2p)
- Location of the actors is the most significant trait of pivoting candidates

Future Work

- Proposal of an efficient detector based on PCA-refined methods
- Further analysis of malicious and benign candidates

MUNI
C4E

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

C4E.CZ