Flow-based detection of RDP brute-force attacks

Martin Vizváry
vizvary@ics.muni.cz

Jan Vykopal
vykopal@ics.muni.cz

Institute of Computer Science
Masaryk University, Brno

Motivation

- Increase in attacks on the authentication of the Remote Desktop Protocol – RDP (e. g., the worm Morto [1])
- Host level detection is not suitable for large networks such as the campus network of Masaryk University
- The lack of network-based detection tools

Is it possible?

Design of the flow-based signature of RDP authentication I.

- Flow-based analysis of:
  - RDP clients for various operating systems,
  - tools for brute-force attacks.

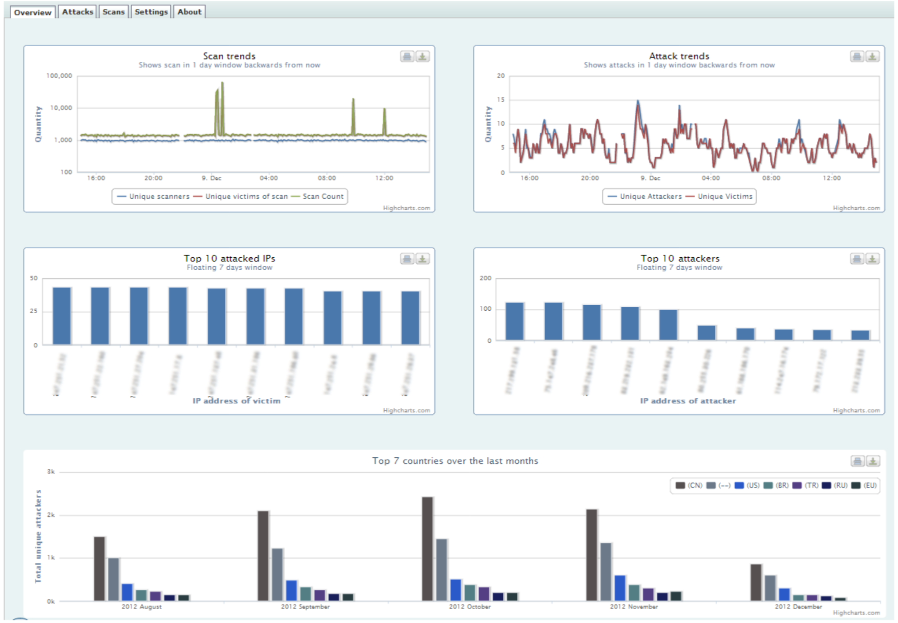
- Flow-based signature of authentication:
  - *in packets* – <20, 100>,
  - *in bytes* – <2200, 8001>,
  - *out packets* – <30, 190>,
  - *out bytes* – <3000, 180000>,
  - *TCP flags* – ACK, PUSH, RESET, SYN,
  - *dst net* – <the address of the local network>.

Design of the flow-based signature of RDP authentication II.

- Additional conditions to lower false positives:
  - attacker used a TCP SYN scan technique,
  - time factor of attack,
  - at least three authentication attempts per victim,
  - at least three victims at the same time.

RdpMonitor – NfSen plugin

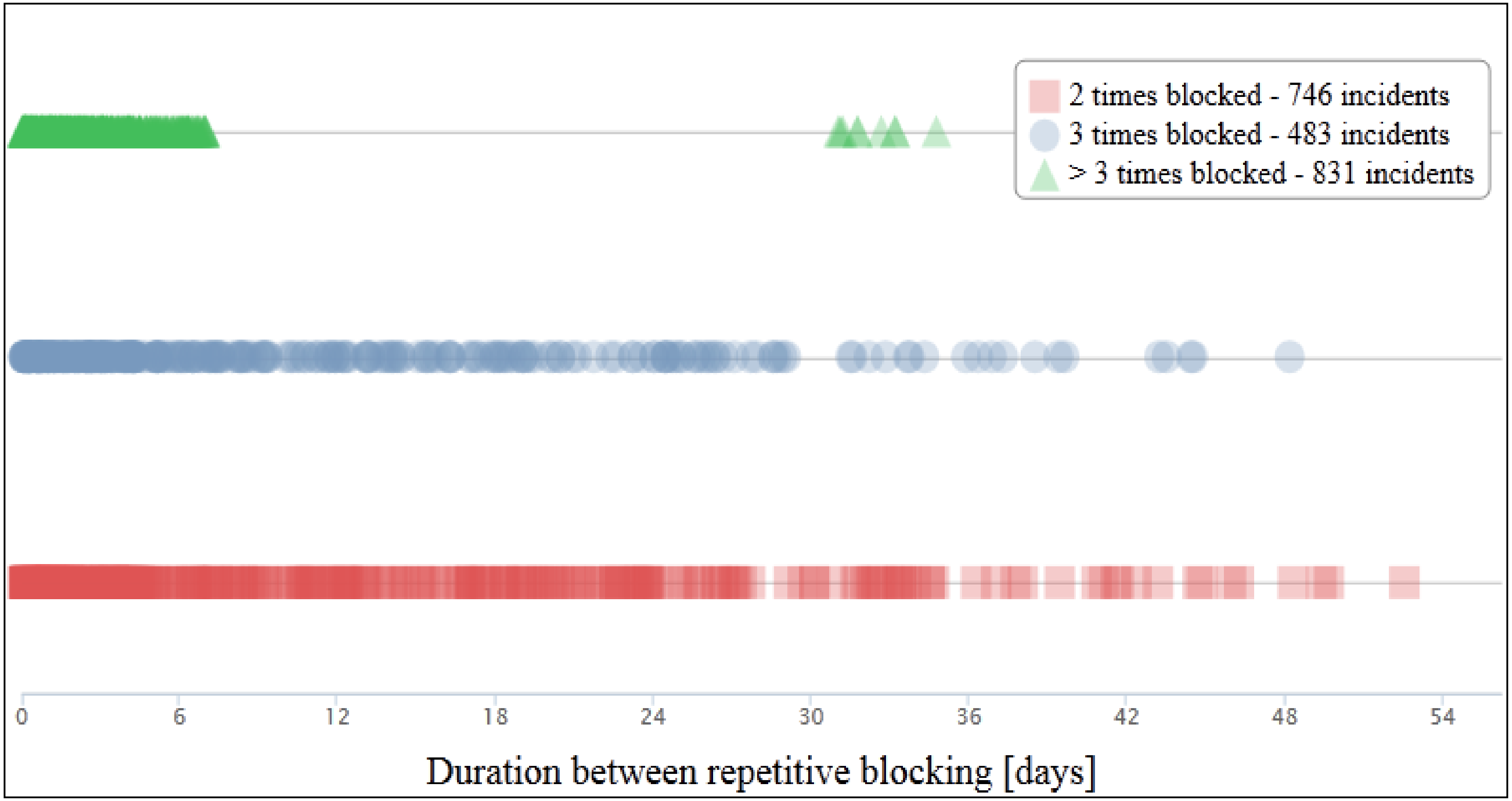
- Publicly available brute-force detection plugin for widely used **NfSen collector** [2]
- The plugin uses the derived NetFlow signature to automate the attack **detection and reporting**



Evaluation of the flow-based detection signature I.

- Data acquired in the large campus network of Masaryk University from October 1 to November 30, 2012
- The plugin has detected 3,430 attacks originating from 2,057 unique IP addresses
- Approximately 40 % of all RDP related traffic is malicious
- Attackers were blocked for two days

Evaluation of the flow-based detection signature II.



Conclusions

- We have analyzed network flows acquired during RDP authentication of various clients and proposed the general **signature for detection** of RDP brute-force attacks.
- The detection method was successfully implemented as a publicly available **plugin for the NfSen collector**.
- Thousands of attacks with almost **zero false positive rate** have been mitigated and reported.

Future work

- Analyze the impact of various values of **thresholds** of additional conditions to false positive/negative rate

- Analyze the impact of changes in **duration of blocking** to attackers’ behavior

Q&A

Flow-based detection of RDP brute-force attacks

Martin Vizváry
vizvary@ics.muni.cz

Jan Vykopal
vykopal@ics.muni.cz

Institute of Computer Science
Masaryk University
Brno, Czech Republic

References

- [1] F-secure: Worm:W32/Morto.A analysis : http://www.f-secure.com/v-desc/worm_w32_morto_a.shtml
- [2] CSIRT-MU tools webpage: http://www.muni.cz/ics/services/csirt/tools