Economics of Cybersecurity Block 2
Telnet scans
DRAFT

Calvin Hendriks - c.hendriks@student.utwente.nl
Christiaan van den Bogaard - c.h.m.vandenbogaard@student.utwente.nl
Sander Bakkum - s.bakkum@student.utwente.nl
Riccardo Colombo - r.colombo@student.utwente.nl

September 2019

1 Data set security issue

The analyzed data set consists in a collection of results of port scans performed by Shadowserver [1]. These port scans have been performed on both port 23 and port 2323, where devices commonly listen with a Telnet server. Telnet is a simple line-based plaintext protocol, often used to expose a commandline interface to devices over the internet. Telnet is an unencrypted protocol, as opposed to for example SSH which has similar functionalities. Often, Telnet servers ask for login credentials when a connection is successfully established.

Devices with an open Telnet port are exposed to remote command execution when authorization is disabled for the device, or its login credentials are easily guessed (for example when manufacturer passwords remain unchanged). When a device is compromised, it allows an attacker with malicious intent a set of actions:

- Steal any privacy-sensitive information on the device.
- Use the device as a pivot to gain further access to the network it resides in.
- Perform DDoS-attacks from the compromised device.

Port scans on Telnet ports are for example used by the Mirai-botnet to spread to IoT-devices connected to the internet.

In this paper we take a look at the security of telnet hosting machines and define a set of security metrics for them.

1.1 Data details

This research is based on a dataset from port scans performed between the 1st of january and august 30th 2018. Each column in the dataset is explained below:

- **Timestamp**: Date and time of the portscan.
- **IP**: Target IP-address.
- **Protocol**: IP-protocol used in the portscan (always 'TCP').
- **Port**: Target port.
- **Hostname**: Hostname associated with the IP-address (if any).
- **Tag**: 'telnet' if port is 23, 'telnet-alt' if port is 2323.
- **ASN**: Autonomous System Number of the target network.
- **Geo**: Country in which the target IP-address resides (always 'NL', Netherlands).
- **Region**: Province in which the target IP-address resides.
- **City**: City in which the target IP-address resides.
- **NAICS**: North American Industry Classification System number.
- **SIC**: Standard Industrial Classification number.
- **Banner**: Text response received upon successfully established connection.

2 Ideal metrics for security decision makers

The Mirai botnet represented one of the largest botnets ever existed, accounting for over 600K infected devices in its peak moment [2]. Launched in September 2016, the infection worked in a very simple yet extremely effective way. The initial phase consists in probing pseudo random IPv4 addresses with TCP SYN packets on port 23 and 2323 (common Telnet ports). Once a device replies to the probe, Mirai enters the second phase of the infection, effectively trying to bruteforce the login in order to establish a Telnet connection by using a credential combination selected by a pre-configured list. When the login is successful Mirai sends the IP address of the compromised device to the *report server*. At this point the second part of the infection would remotely login, get technical details on the victim and install hardware-compatible malware to take control over the device.

Although it would seem quite simple to prevent such an attack, the extremely high success that Mirai has achieved testifies the opposite. In particular, we can identify the main flaw that has acted as enabler for the spreading of the Mirai botnet and, more in general, for the successful exploitation of the Telnet

service, in the superficial configuration of the access control. The progress of the infection, in fact, completely relies on successfully bruteforcing the login, only made possible by a weak configuration of the service credentials. Therefore one of the main metrics would focus on the vulnerability of the controls that have been put in place rather than on the controls themselves.

3 Metrics that exist in practice

4 Designed metrics from the data set

4.1 Country heatmap

4.2 Analysis of success of connection attempts. Split in login required.

4.3 Analysis of vulnerable unpatched software.

CVE-2018-7445[1] reports a buffer overflow vulnerability discovered in the MikroTik RouterOS with a CVSS score of 10. The vulnerability was publicly disclosed on 2018-03-19 and every device running an operating system version lower than 6.41.3 are considered to be vulnerable. When analyzing the data on the telnet scans, it is possible to evaluate that 19,166 unique IPs are running MikroTik RouterOS over the whole time frame of the scans. When considering only the period before the disclosure of the vulnerability (where the timestamp is lower than 2018-03-19) it is possible to compute that 15 unique IPs are running a non-vulnerable version of the OS, accounting for the 0.08%. Moreover, when considering the period between June 1^{st} and July 31^{st}, four months after the disclosure of the vulnerability, only 46 unique IPs are running the non vulnerable OS, accounting for the 0.24%. This metric highlights how only a slight portion (0.16%) of the machines running the vulnerable OS actually updated to the patched version of the OS, leaving the vast majority completely vulnerable to a score 10 CVE.

5 Evaluation of designed metrics

[1] `https://www.cvedetails.com/cve/CVE-2018-7445/`

References

[1] "The Shadowserver Foundation: Telnet Scanning Project." [Online]. Available: https://telnetscan.shadowserver.org/

[2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, Aug. 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis