Surveying IT threats for server of small business in real-environment with honeypot

David Janos Feher

Óbuda University, Budapest, Hungary

david.janos.feher@gmail.com

David Baranyai

University of Debrecen, Debrecen, Hungary

david.baranyai@protonmail.com

Abstract: The cybercrimes are more and more popular nowadays and not just against the corporations, and the small businesses are vulnerable against the attack too. Most of the small businesses use IT tools, as they have websites, servers, and other information communication-related devices, limited by the smaller budget, they cannot buy the newest, most secure devices since they cannot spend a high amount of money as a typical corporation can. The small companies have less vulnerable data and less prestige to lose, but they are still the target of the attackers. Our article is surveying the external IT security attacks against a small business in the countryside with a honeypot solution.

Keywords: webserver, SSH, Telnet, honeypot, threat, small business

1 Introduction

Day by day, IT is becoming increasingly important to our society as it is getting digitized in every aspect of our lives. More and more electronic information is accessible, just like online activities. Companies that handle them have more data to protect. Everything is managed electronically in the most advanced countries of the world, through payment transactions and health data management, and therefore more data is created, rendering it a greater attack space. Previously, looking at the history of a device, it was possible to determine a present bug, but in the case of explosively growing giant networks, we have no chance of checking them and finding connections between them with the right automated methods and tools. They need to be protected and regulated for the unmanageable amount of data to be handled and analyzed, which can be the so-called Security Incident and Event Management (SIEM) system. SIEM tools work as a collection and

finetuning device between the vast array of protection devices, routers, operating systems, and other sources of information. For example, firewalls, IPSs, antispyware, DHCP servers, and proxy servers send information about each communication and login that SIEM manages and correlates, and decides on its rule base whether it is an attack or not. If it is, after the monitoring of the monitoring team, and the appropriate indications, based on the information gathered, the Triage team can start exploring and eliminating the problem by the so-called response team. Most of the small businesses use IT tools, as they have websites, servers, and other information communication-related devices, limited by the smaller budget, they cannot buy the newest, most secure devices since they cannot spend a huge amount of money as a typical corporation can. The small companies have less vulnerable data and less prestige to lose, but they are still the target of the attackers. Our article is researching the risks of the external attackers with the help of the IT tools. [1-5]

2 Background

Users have a key role in maintaining information security as they are the ones who actually have daily access to data and IT systems. They produce, transmit, and store all of the data on a variety of electronic devices, and if necessary, delete it. As a result, everyone is qualified as a user, manager, operator, expert or outsider who has access to the organization's data. The same thing can be said in the home environment. Every family member, friend, relative, or acquaintance who has access to home computer systems is considered a user. Most importantly, users are aware of threats, rules, and the processes they need to take in order to prevent information security incidents, or if they cannot prevent them, recognize them in time and know what channel they are can be reported to the wages. End-users represent a tremendous value for the incident management team or organization in the incident management process. However, they have an enormous responsibility. A suspicious attachment to the email mailbox, a suspicious phone call, an abandoned USB flash drive in the office on the corridor, or a suspicious wandering unknown in the office. It is vital for the organization to have the ability of users to detect the threats in a timely manner and assess the real risk and report it to the incident management organization. [1-3]

For information systems, the most important thing is to secure data security. There are three data security requirements:

- Confidentiality: something that only rightful people can recognize is limited to those who are eligible for recognition.
- Integrity: something that matches its original condition and is complete.

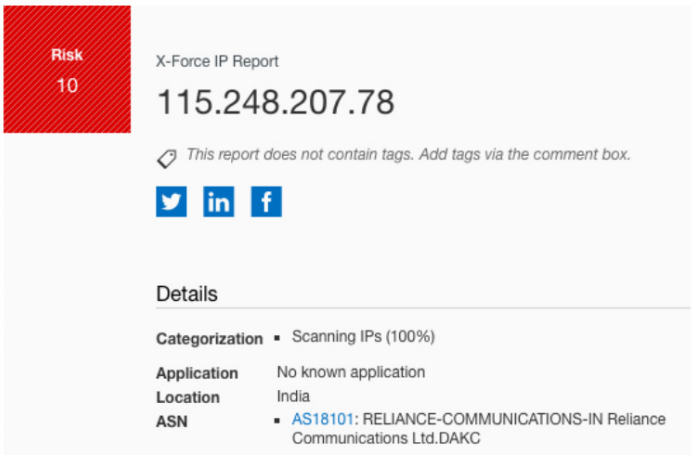
- Availability: the necessary infrastructure and data are available to you and whenever you need it

The botnet may include computers in a home, school, or corporate networks. Computers are infected by a pest program and then receive commands from central control computers (Command & Control servers) and use them to perform different tasks. They can perform counting tasks, send unwanted emails, steal personal information from infected machines, or even initiate attacks on service denials (DDoS). A large botnet network can consist of tens of thousands of computers. Computers can be infected with malware by using a comprehensive endpoint protection software package, anti-virus software, firewall software, antimalware software and periodically updating software installed on your computer, which can usually be automated with proper settings.[2-3]

Honeypots have quickly become an accepted tool for security arsenals and have gained more and more space in the corporate sphere as high precision, early warning systems. Since honeypots do not have any practical benefits (i.e. no sharp service is run on them), all of their activity can be viewed as an attack and we can take the necessary steps to parry the expected attacks and we can recognize the fact of the attack. Honeypots usually have one or more network connections and some weak operating system and service emulation. Since the only purpose of a honeypot is to detect the attack early, the system has been secure enough to the attacker cannot actually cause damage. System-simulated “server”' or a complete computer network emulates minimal functions, such as listening to ports, providing minimal text banners, or making simpler login screens. Commonly known services include Auth, Finger, FTP, HTTP, IMAP, POP, SMTP, SSH (Secure Shell), Telnet, Server Message Block (SMB), UDP (User Datagram Protocol) and RPC services. The attacker detects the honeypot, which looks like a lightweight prey, and while he is analyzing the system, he may leave unwanted traces which could be used to reveal the attacker’s identity. [4-6]

3 Measurement

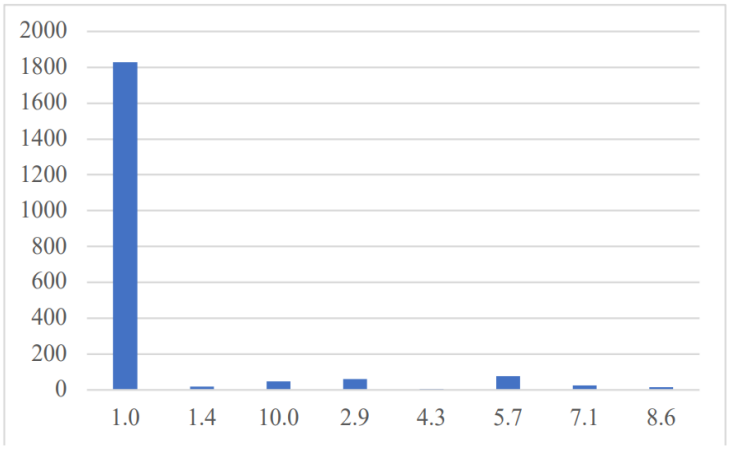
We used the Splunk Light application to handle the high amount of records from our source device. To Analyze the results we used the IBM X-Force Exchange is a cloud-based threat intelligence platform that allows you to consume, share and act on threat intelligence. It enables you to rapidly research the latest global security threats, aggregate actionable information, consult with experts and collaborate with peers. IBM X-Force Exchange, supported by human- and machine-generated intelligence, leverages the scale of IBM X-Force to help users stay ahead of emerging threats. [7-9]



1. figure IBM X-Force Exchange IP report

To analyze the high amount of data we used the X-Force Exchange (XFE) API which provides programmatic access to X-Force Exchange. Each call in the API supports a capability in the UI of the X-Force Exchange platform. The API follows guidelines for RESTful APIs, with the HTTP path defining the service to the call and the resource being requested. [8, 10]

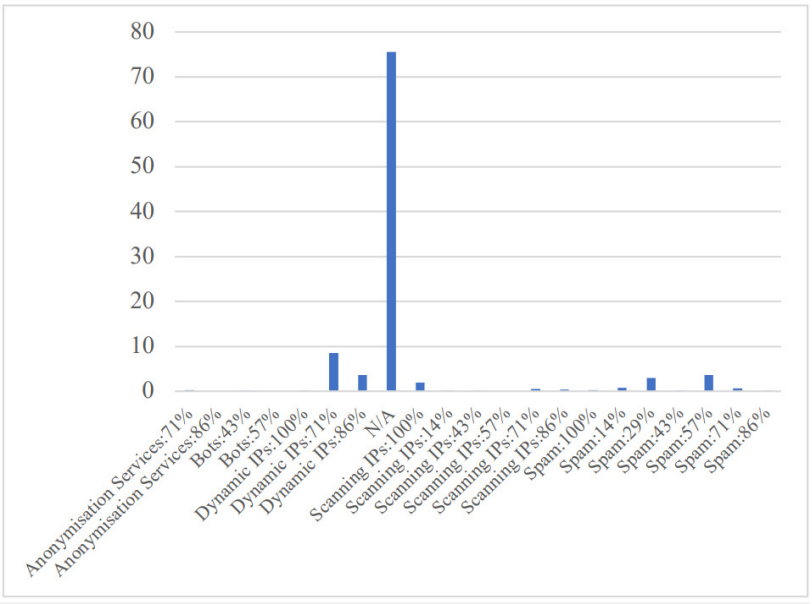
We had connections from 2082 different IPs, based on the results most of the attackers' IPs were unknown in the third-party threat intelligence databases. Only just a few amounts of them can create alerts based on these sources with the right SIEM system.



2. figure Risk scores of the IPs

The category of the IP gives us more information about the previously reported suspicious or malicious activity from the source IP. We implemented only the

most specific finding with the highest percentage. We found the much scanned IP related outcome, for example, the shodan.com is a popular scanner site, but other non-publics are in the findings, too. Some of the infected devices work as a Botnet Command and Communication server, or does Spamming or Scanning activity for the commander of the invention. Other IPs have relation or chance to connect, and Botnet related the IPs which confirms our hypothesis, that there exists a significant risk against the servers and publicly available devices.[11]



3. figure Categories of the IPs

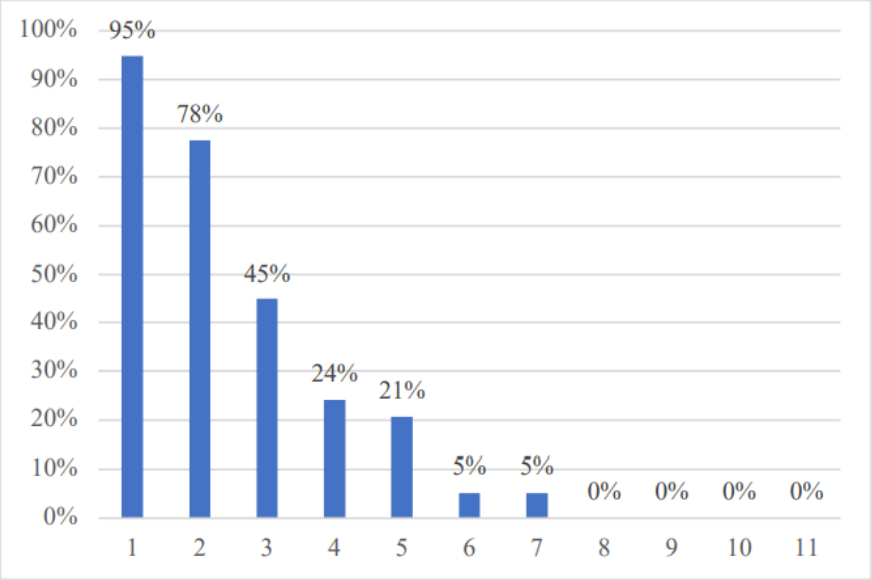
The following table shows the category of the IPs, related to the risk scores. Based on the findings we can do some more in-depth investigation on our environment by checking the status of our server. We can see our device connected to Botnet related IPs, but because of the risk score, some of them they could be false positive findings. The IPs with the risk score 10, can contain higher risk against our system, although only about scanning and spam related IPs. [11]

	1.0	1.4	10.0	2.9	4.3	5.7	7.1	8.6	Total
Anonymisation Services:71%	0	0	0	0	0	0	4	0	4
Anonymisation Services:86%	0	0	0	0	0	0	0	1	1
Bots:43%	0	0	0	0	**2**	0	0	0	2
Bots:57%	0	0	0	0	0	1	0	0	1
Dynamic IPs:100%	3	0	0	0	0	0	0	0	3
Dynamic IPs:71%	177	0	0	0	0	0	0	0	177
Dynamic IPs:86%	75	0	0	0	0	0	0	0	75
N/A	1574	0	0	0	0	0	0	0	1574
Scanning IPs:100%	0	0	**42**	0	0	0	0	0	42
Scanning IPs:14%	0	3	0	0	0	0	0	0	3
Scanning IPs:43%	0	0	0	0	2	0	0	0	2
Scanning IPs:57%	0	0	0	0	0	1	0	0	1
Scanning IPs:71%	0	0	0	0	0	0	9	1	10
Scanning IPs:86%	0	0	0	0	0	0	0	9	9
Spam:100%	0	0	**7**	0	0	0	0	0	7
Spam:14%	0	17	0	0	0	0	0	0	17
Spam:29%	0	0	0	62	0	0	0	0	62
Spam:43%	0	0	0	0	3	0	0	0	3
Spam:57%	0	0	0	0	0	74	0	0	74
Spam:71%	0	0	0	0	0	0	12	0	12
Spam:86%	0	0	0	0	0	0	0	3	3
Total	1829	20	49	62	7	76	25	14	2082

1. table Crosstabs of categories and risk scores

The X-Force results are based on the vendor, threat intelligence and end-user findings. In case of a miscategorization, we have the ability to report the problem to the site, and the team will check the report and update the database.

In this period, we had several attempts of harming our system, but all of them were unsuccessful. After a more in-depth look at the activities, the attackers tried to download the following 11 files, only 3 of them are well-known patterns by the antivirus or intrusion prevention/detection systems. Most of the malware agents tried to download more specific malware or hacking tools to the attached devices, as some of the files were Trojans and some other bash scripts.



4. figure IPS/IDS coverage

After a Cuckoo Malware Analyze with sandbox test, we know that 9 from the 11 malicious files can create real damage on the system, and we see most of them are not available in the specific pattern databank.

4 Conclusion

Based on the measurements we can confirm the importance of a well-configured firewall accompanied by other security tools. Most of the attacks came from unknown sources or sources with dynamic IP, therefore, it would be impossible banning them from the system in order to mitigate the risk of the external attacks. Every intrusion started with a scan. We recommend improving the security of the servers through the IPS/IDS device installation, password policy updating, privileges and accounts managing, backup rescue strategy creating or overviewing, redundancy providing for central servers/data storage. To prevent the attacks, it is very important to ensure the security-related design, and the regular patches and updates of devices, as well as, periodic full overview of the system to discover the occurred hazards. Some of the caught malware files are not available in majority of the antivirus databases, hence they are not able to provide total defense. By using applying the aforementioned steps, we will ensure that our system becomes more secure. That way, hopefully, we will make the hackers' efforts fruitless.

References

[1] János, Fehér Dávid, and Nguyen Huu Phuoc Dai. "Security Concerns Towards Security Operations Centers." 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI). IEEE, 2018.

[2] Peltier, Thomas R. Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Auerbach Publications, 2016.

[3] Safa, Nader Sohrabi, Rossouw Von Solms, and Steven Furnell. "Information security policy compliance model in organizations." Computers & Security 56 (2016): 70-82.

[4] Provos, Niels. "A Virtual Honeypot Framework." USENIX Security Symposium. Vol. 173. 2004.

[5] Krawetz, Neal. "Anti-honeypot technology." IEEE Security & Privacy 2.1 (2004): 76-79.

[6] Zammit, Daniel. "A machine learning based approach for intrusion prevention using honeypot interaction patterns as training data." University of Malta (2016): 1-55.

[7] Carasso, David. "Exploring splunk." Published by CITO Research, New York, USA, ISBN (2012): 978-0.

[8] Zadrozny, Peter, and Raghu Kodali. Big data analytics using Splunk: Deriving operational intelligence from social media, machine data, existing data warehouses, and other real-time streaming sources. Apress, 2013.

[9] More, Sumit, et al. "A knowledge-based approach to intrusion detection modeling." Security and Privacy Workshops (SPW), 2012 IEEE Symposium on. IEEE, 2012.

[10] Ayres, Daniel L., et al. "BEAGLE: an application programming interface and high-performance computing library for statistical phylogenetics." Systematic biology 61.1 (2011): 170-173.

[11] Esposito, Damiano, et al. "Exploiting the potential of web application vulnerability scanning." ICIMP 2018, Spain, July 22-26, 2018. IARIA, 2018.