Indicator o(f)r Compromise

Tools tested against threats in a Manufacturing Environment

Introduction

Malware, Trojans, Backdoors, RAT's and much other vulnerability nowadays are threatening companies. Besides these threats most organizations use measures like penetration testing to evaluate the security of their information systems, virus scanners, Intrusion detection and prevention systems, Firewalls, switches and other network elements with build-in threat modules, CERT teams and forensics expertise to cope with all these possible attacks. The question is: "Is this enough?" or "which measure fits best?" Cyber4Z did some tests with three solutions in a Manufacturing environment in China: Paolo Alto's Wildfire, NTOP and Redsocks. All three solution where used next to each other where the SPAN port information from the routers on the edge of the network was re-routed to all solutions directly with the same data. The results were very interesting. Without additional configuration the Redsocks appliance was able to show 60% more threats than the other two solutions. In addition only 10% of these detections were false positives, with a 40-60% false positive rate for the other solutions. The output generated by Paolo Alto and NTOP however gave more information with which a forensic or CERT team could analyze more related information. NTOP and Paolo Alto were cheaper solutions in relation to Redsocks. Still the answer for this specific company was: Which one should we use? And why? Do we have an indictor of compromise (IOC) or are we compromised? The goal of this document is too let the reader decide which solution or set of solutions fits best for their company. The analyzed data of all three solutions is used to write this whitepaper.

Palo Alto and Wildfire

WildFire is an integrated Palo Alto malware detection service in their next-generation firewalls and provides detection and prevention of modern malware. WildFire should be able to identify and detect unknown or zero-day malware by directly executing files in a virtual environment and observing malicious behavior. WildFire makes use of the client's on-premises firewalls for in-line prevention in conjunction with a cloud-based service to provide the protection. The Wildfire functionality has proved a very flexible solution during the Proof of Concept, with many configuration settings.

An example of the Palo Alto output is shown in Figure 1.

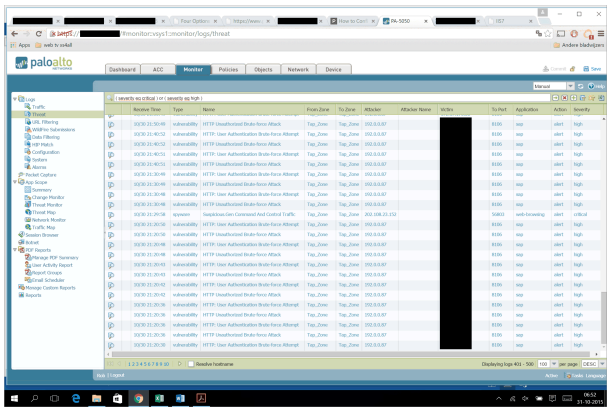

Figure 1: Palo Alto Wilfire dashboard

NTOPNG

ntopng is a next generation version of the original ntop, which is used as a network traffic probe that shows the network usage, similar to what the popular top Unix command does. ntopng is based on libpcap and in this environment it was installed on a Raspberry PI. We used a web browser to navigate through ntop (that acted as a web server) traffic information and got a dump of the network status from the edge of the client's network. In this specific case, ntopng was used as a simple monitoring agent with an embedded web interface.

An example of the NTOP output is shown in Figure 2.

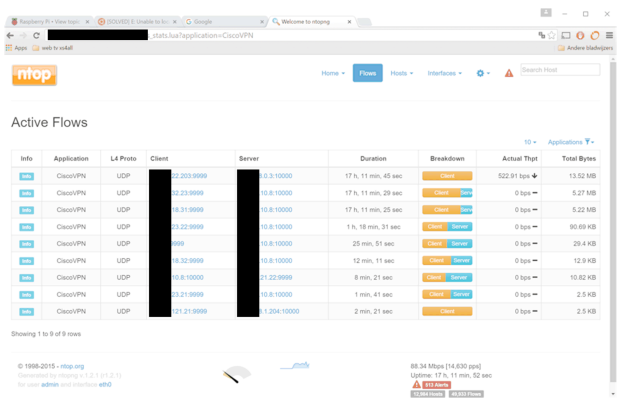

Figure 2: NTOP Dashboard

Redsocks

The RedSocks Malware Threat Defender is a hardware

device, but for this specific Proof of Concept (POC) a VM version is used with a VM probe. The probe is similar to the NTOP probe in functionality. It is used to convert the output from the SPAN ports from the routers into the IPFIX protocol, which is used for security monitoring. The information from the probe is than routed to the Redsocks Malware Threat Defender, which analyzes this information into the RS Dashboard. RedSocks Malware Threat Defender should offer real-time protection against all forms of data espionage. It is able to see current threats, but with Redsocks it is also possible to detect outdated data.

In this specific PoC, The Redsocks appliance immediately gave the client information about internal threats. The IT department was able to mitigate these threats and set up a procedure to neutralize a possible future attack. Redsocks gave also an overview of all top 10 systems that are possibly infected. Also mobile users with an infected device were recognized. All of this with a success rate over 90% without any tuning.

An example of the Redsocks output is shown in Figure 3.

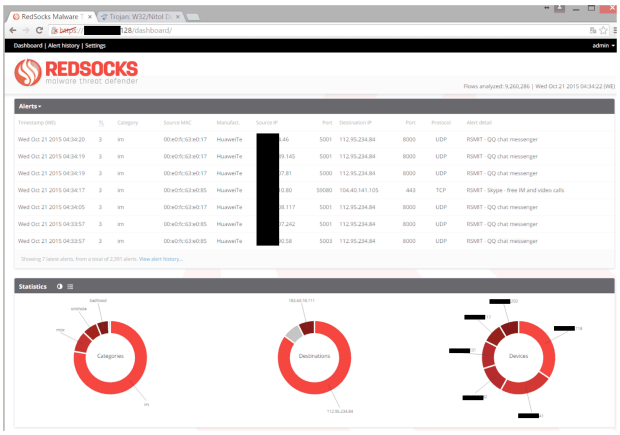

Figure 3: RedSocks Dashboard

The Proof of concept

Cyber4Z was able to test all three solutions in a live manufacturing environment under similar conditions with the same dataflow. Figure 4 shows how the data was captured, mirrored to a switch and how the results have been analyzed.

The Advantage of the Palo Alto Firewall is that it has 12 ports available. During this test we had 8 free ports of which two were used in promiscuous mode. The Palo alto is able to use several functionalities as Firewall and as threat feed with the WildFire functionality at the same time.

The capturing period was three weeks. During this time we were able to catch over 15.000.000 data packets as flow data. All three devices were fed with the same traffic flow. In some cases the results have been analyzed directly if a critical issue was shown on two of the three applications. If it was applicable to an end-point, the Internet Access Controller has been used to lock down the traffic from that IP-address.

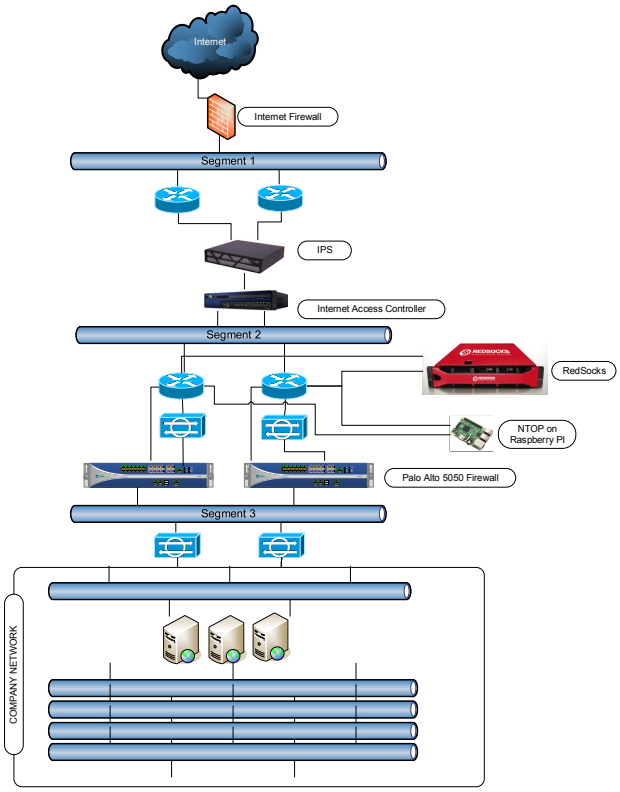

Figure 4: Test environment

Findings and analyzed results

After the data has been captured we analyzed all results during three weeks. From the results we can conclude the following

Redsocks

The Redsocks appliance was able to find the most results with the least number of false positives. A total of about 10% of the false positives could be explained rather quickly from which 6-7% false positives still needed some deeper analysis. With blocking the Internet access controller after a finding and informing the IT helpdesk, a process was created to find the infected system within 24 hours after the dataflow was stopped within an hour. The Redsocks appliance also could be used as a privacy monitor. The appliance was not able to execute rulesets to address vulnerabilities automatically.

Wildfire

The Wildfire functionality gave more than 60% false positives, but with tuning by a Palo Alto Engineer it was able to lower the rate to 40%. The Palo Alto however was able to execute rules and block IP's automatically and the price of the Wildfire functionality was significantly lower than Redsocks. For a more accurate number of actual threats, an extra FTE is needed.

NTOP

The NTOP application is freeware and is based on

libpcap. NTOP functions as a network monitor and shows all in- and outbound traffic. It reacts on behavior, but has no intelligent algorithm build in. Still a lot of analysis power and knowledge is needed to make the translation to a 'possible' threat. Alerts are given based on an indication of a threat, but no threat levels are given and no other malware relation is shown. Behavior is listed, but profound knowledge is needed to actually find threats from the inside out.

NTOP gives a lot of information on application level and is perfectly equipped to do performance analysis. It is very hard to actually understand an inbound threat from the output.

The table below shows an overview of the products tested and the functionalities. Based on this matrix the reader can decide which tool or combination of tools works best in their organization.

Product matrix			
Functionality	**Palo Alto**	**Redsocks**	**NTOP**
Assignable real attacks or vulnerabilities (Low number of False positives)	+ + +	+ + + + +	+
Blocking functionality	+ +	-	-
Price	+ +	+ +	+ + +
Performance measurements	-	-	+ +
Analysis effort by a CERT team	+	+ + +	- -
Configuration effort needed	+	+ + +	+ +
More than 2 functionalities in one device	+ + +	+ +	+ +
Global support	+ + + +	+	+ +

Table 1: Product matrix

Assignable real attacks or vulnerabilities (Low number of False positives): The Redsocks showed the lowest number of False Positives. Almost 90% of all alerts were direct assignable to a real threat against 60% of the Palo Alto service. However, when Palo Alto was informed, a cyber security expert was assigned within 24 hours to tune the configuration. With this support the 60% False positives were decreased to just below 40%.

Blocking functionality: Because the Palo Alto's Wildfire malware detection service is part of the Firewall's functionality, the user has the ability to block a specific service automatically. This ability is not part of Redsocks or NTOP. However, in our example, production could be affected when certain services were blocked automatically. In that case the Redsocks appliance detected the problem from which the IT service department could choose wether or not to block specific services with an internet access controller. This gives the service department a lot of flexibility and control.

Price: The price of all three solutions are based on commercial prices. NTOP is Open source, but still a commercial fee must be paid if the product is commercially used. We also compared the support fee, training fee and the ability to respond on an event from an internal CERT (Computer Emergency Response Team) in relation to pricing. In that case the NTOP application is the cheapest of all. The configuration we used would be around 300 euro with one year of update support. The client however should be invest a lot in the analysis power of a CERT. NTOP gave a lot of information, but without proper knowledge it would not be very helpful in addressing malware in our setup. The Palo Alto was also not too expensive. The submission is approximately 8000 Euro a year, but also in this case we needed training, support and a Cyber security team with the ability to address possible attacks and be able to filter out the false positives. A specialized team would cost approximately 80-120k in euro's a year. The Redsocks appliance was 60k a year, but gave the client a lot of information. The existing team was also able to respond quickly on the outcome without any additional knowledge needs.

Performance measurements: We added this requirement, even though it does not say anything about malware. Because NTOP specially was designed to fill in this need, it could be a very helpful tool to address performance issues in a company, without directly point out to a possible malware attack or any other problem. NTOP gave a lot of information on data flows, but was less strong in the detection of malware.

Analysis effort by a CERT: In our specific case the Redsocks appliance gave the most concrete information without having enough knowledge on different versions of malware or attack mechanisms. In our situation the current service delivery team was equipped to solve the malware problems in just a couple of hours. The information from the Redsocks dashboard was sufficient to detect and respond in an appropriate matter within the timeframe of the policy.

Configuration effort needed: For all three solutions the effort needed to start the service was relatively low. All three solutions were up and running within 4 hours. The Palo Alto however needed some extra configuration time, but the local support team from Paolo Alto were able to configure optimally within 24 hours.

More functionalities: As described earlier in this document, the Palo Alt device was the only one that could be connected to the firewall's functionality. The other solutions were able to run pro-actively, but only with a SIEM (Security Incident and Event Monitoring) system. The Palo Alto device has also the ability to connect to a SIEM solution and correlate the Wildfire events with other Indictors of Compromise.

Global Support: For the support team in China, we have had the Palo Alto local team up and running within one day. That makes the Palo Alto service team the strongest of the three solutions. The other two solutions had the right intensions, but Redsocks did not have a footprint in China. In Japan however they had a local support team available. NTOP did not had local support

presence in China, but they responded very fast on questions. Additionally, their solution was very easy to use.

Conclusion

During the test we worked on the best way to detect possible malware and to make sure that it would be neutralized within the appropriate time. For the best possible solution still a combination with end-point security, network security and performance is the best. However to achieve the best possible results the combination between Redsocks and Palo Alto with the Wildfire Functionality would be the best possible solution in our business case.

We also believe that every company should perform a Risk Analysis first to analyze the true needs for handling malware. A manufacturing environment is different than a cloud provider or a hospital. Also local law and other related items could ask for a different approach.

Small and medium small companies, that have less knowledge about cyber defense capabilities could use the Redsocks appliance, because little knowledge is needed to recognize the threats.

With this test the reader can decide for himself which product he would like to use in a Proof of Concept for their own. We just hope we could help the reader taking a burden of their shoulders in analyzing different solutions. Furthermore the reader is given a good insight in the different solutions. If however more information is needed, than Cyber4Z can be consulted any time.

With kind regards,

Rob Mellegers, General Manager and Co-owner of Cyber4Z B.V.

For more information on this whitepaper, please contact us through 4z4u@cyber4z.com or call Rob Mellegers, General Manager Cyber4Z, rob.mellegers@cyber4z.com, +31-(0)643587481

CYBER4Z
Ernani 21
5629 NB Eindhoven

www.cyber4z.com

Cyber4Z Helps our clients to reach their strategic goals by mitigating IT Risks in order to profit the use of IT maximally.