FINANCIAL INVESTMENT FIRM REDUCES RISK

Company:

Financial Investment Firm Specializing in High-Net-Worth Individuals

Industry: Finance

Key Issues:

With much to risk, this financial firm sought to:

- Strengthen security posture
- Maximize secuity solutions
- Improve time spent analyzing events

Solutions:

- ThreatARMOR
- Application and Threat Intelligence Processor (ATIP)

Results:

- Filters network traffic based on Ixia's continually-updated security intelligence to make NGFWs perform better
- Proactive monitoring stops malicious packets from outside or inside the network
- 60,000 connections blocked in a single week

The Customer

ThreatARMOR™

Financial firms face unique challenges from a defensive network security standpoint due to the simple fact that they are the guardians of people's financial assets. This is precisely why these firms make global news when regulations force them to report a breach. A firm that specializes in high-net-worth individuals, where the minimum investment in their products is a million dollars, requires even higher levels of due diligence. The clients of such a firm may include a global cadre of highly influential individuals such as captains of industry and people who make decisions at the highest levels of their respective governments. To safeguard sensitive information, in addition to the actual financial assets themselves, the network security team at such a firm must be constantly ready to adapt to a changing landscape by adopting the latest in defensive network security solutions.

Background

This institution had already invested in Ixia's Net Tool Optimizer (NTO) solution to gain a higher level of visibility into their networks. The Application and Threat Intelligence Processor (ATIP) feature was a major value-add to improve their network security. Now, the security team was very interested to see how the latest security offerings from Ixia could further enhance their security posture.

This customer was deploying several other security solutions, including a leading next-generation firewall (NGFW) and a leading cloud-based DNS service. Along with other network management tools, the customer deployed a leading security information and event management (SIEM) solution to aggregate and correlate the log messages of all of their networked equipment.

COMPANIES MUST EXPOSE RESOURCES TO THE ENTIRE INTERNET.

It's All About Reducing Risk

To offer financial services to a global marketplace, companies must expose resources, either inbound or outbound, to the entire Internet. This is a high-risk proposition and puts tremendous strain on existing security solutions as well as the individuals responsible for maintaining network fidelity. To reduce this risk, Ixia's ThreatARMOR strengthens network security in two highly valuable areas:

- **Increase your security posture —** Most companies have deployed a high-quality firewall, IPS, SIEM, and a security team. And yet, breaches still happen – and the average time to breach detection is 170 days. Why? Because there's so much security "noise" that it's hard to find the important evidence of a successful or ongoing breach. Eliminating hijacked IPs, untrusted countries, and malware and phishing sites cuts through that noise so you can focus on what's important. You may also be able to take advantage of the lower processing burden on your security tools to enable more advanced features.
- **Maximize your two most important security investments: Your existing security solutions and your team's time spent analyzing events —** By removing those known bad actors from attempting remote connections to your services, your existing network security solutions will see a sharp decline in events. With fewer events to analyze, your team will be able to more-efficiently execute their jobs as guardians of your networked resources.

These two points were met with three questions by the customer:

Question: Why can't we simply configure our existing NGFW to block these malicious IP addresses?

Answer: First, rules in an NGFW cost CPU and memory resources. Most NGFWs run out of capacity at about 10,000 rules. ThreatARMOR was specifically designed with custom hardware to handle millions of rules pertaining to IP addresses. ThreatARMOR devices automatically download updates from the ATI Research Center as frequently as every five minutes, giving you the most up-to-date list of known bad actors. Second, you want your NGFW to analyze application-layer events, which is the purpose of its design, not to understand the global Internet. Simply put, using ThreatARMOR to filter network traffic based on Ixia's continually-updated security intelligence will make your NGFW perform *better.*

Question: How do you select the IP addresses you deem malicious?

Answer: We deploy global honeypots to gather information while simultaneously scanning the Internet. All of the rules we create are fact-based that we have individually validated. We also whitelist IP addresses that are correlated with known mission-critical hosts. Those whitelists are comprised of ranges such as the Alexa 10000 and clouds such as Azure and Amazon.

Question: We have already invested in the cloud-based DNS security service that is meant to eliminate our exposure to botnets and other known malicious actors. This is a service we are paying for that uses their threat intelligence to prevent our users and servers from communicating with malicious actors. Why do I need two solutions to perform the same task?

Answer: Your cloud-based DNS service is examining your client's domain lookups and refusing to service requests if their threat intelligence deems the domain, or corresponding IP address, to be malicious. This service has value, however, it is not inline and does nothing to stop malicious actors from attempting to send unsolicited network traffic to your network, even if they have knowledge that the IP address is known to be malicious. Also, your DNS service is reactive; it is waiting for a compromised machine in your trusted network to contact a known malicious IP address. If the network traffic from your compromised machine is contacting the cloud-based service, then that machine is free to send traffic anywhere. ThreatARMOR is proactive and will not let packets from either a malicious actor outside of your network, or a compromised machine in your network, traverse your network.

The Initial Deployment

These facts resonated with the customer and they were agreeable to deploying ThreatARMOR in their production network with a few caveats. They were apprehensive about placing a new solution inline in their production network. We assured the security team that our world-class inline bypass technology was built into the ThreatARMOR solution, however, as security people tend to be, they chose to remain cautious.

Due to the versatility of their NTO appliance, we were able to place ThreatARMOR in their production network out of band on a tapped link. ThreatARMOR can run out of band in reporting mode, inline in reporting mode, or inline in blocking mode.

We connected the first management port of the ThreatARMOR into their airgapped management network and our other management port, designed to get "Rap Sheet"[1] updates, into a DMZ that has access to the Internet. The first management interface acquired an IP address via DHCP, which was displayed on the front panel. We connected to that address via the security engineer's laptop, created a user account, and began browsing the ThreatARMOR dashboard[2] within minutes of racking the system.

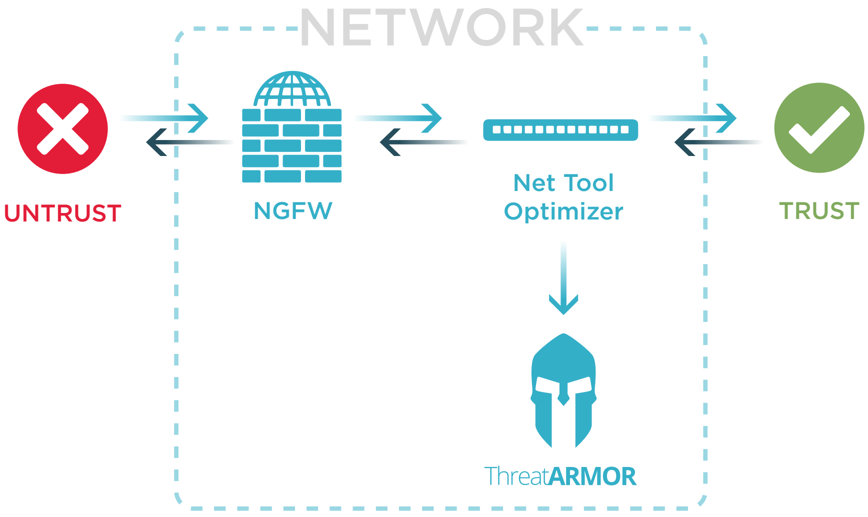

Figure 1: NTO appliance connected to ThreatARMOR

Initial Results

On average, the tapped port from the NTO fed between 500Mbps and 750Mbps into the ThreatARMOR to be examined in "Reporting Mode." It was a moot distinction to have the system in reporting mode, as it is impossible to block network traffic if you are out of band on a single tapped port. Within one hour we began seeing "Rap Sheets" describing network traffic events originated or destined to known bad IP addresses.

The information gleaned by the rap sheet was very straight forward, classifying the remote IP address in varying categories such as hijacked, phishing, malware, etc.

One event in particular was of high interest. An internal server IP address was flagged by ThreatARMOR as the target of an ongoing attack. This server was not meant to be directly accessible to the Internet. When the information gleaned from the Rap Sheet was correlated with information in the SIEM it was determined that a brute force SSH Login attempt had been going on for some time. The source of the attack was from a known hijacked IP address in Asia.

The attack had evaded the NGFW because SSH Login attempts are very normal and not inherently malicious network traffic. This is an obvious exception to that rule, as this was an unauthorized user's attempt to breach the customer's network. It is important to note that the vast majority of hacking attempts on the Internet are automated. This was not a user, or a team of users, sitting at their keyboards for months. This was a script that had been written to try millions to hundreds of trillions of passwords until the targeted system had been compromised.

Secondary Deployment

After confidence was gained in the ThreatARMOR solution, the decision was made by the financial institution's security team to place our solution inline in "blocking mode" in front of their NGFW. After the

[1] "Rap Sheets" are the basis on which we decide whether an IP Address is a malicious actor

[2] The ThreatARMOR Dashboard is the main panel where a user may view the current state of the network with respect to how much of the traffic it has analyzed has been deemed to be originated or destined to malicious IP addresses.

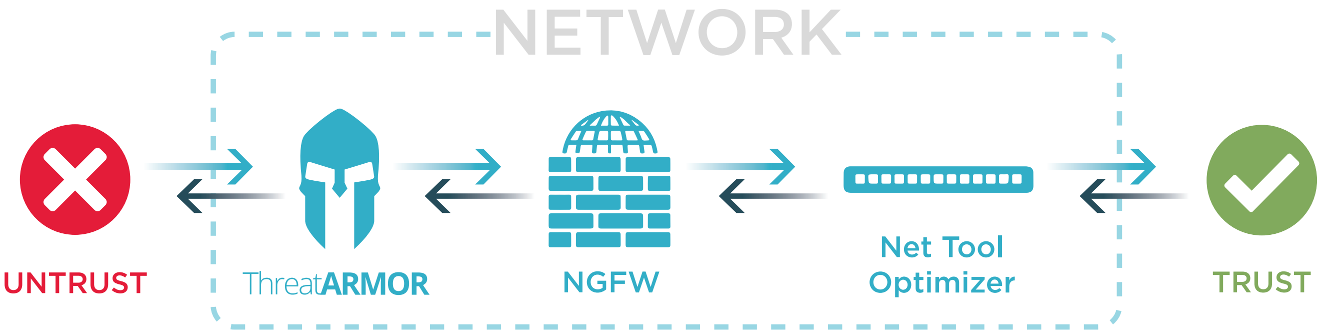

Figure 2: ThreatARMOR and NGFW

adjustment was made, we saw roughly 60,000 connections blocked in a single week, where the security events originated from all over the globe. The top blocked regions were Hong Kong, the United States, China, the Netherlands, and Indonesia.

One noteworthy event that was seen in the Rap Sheet was a machine inside of the customer's trusted site attempting to make contact with an IP address in Ukraine that was a known host of malware. Based off the research done by our ATI team, we had a highly revealing screenshot of the webpage the compromised machine was attempting to view. The content of the page was wild graphics and Ukrainian text; the customer immediately stated that there was no logical reason why an employee of their US-based Financial firm would ever venture to such a dark corner of the Internet during work hours on their company-issued machine.

Conclusion

The value shown during the first few weeks of deployment was immediate and tangible. The security team easily justified the cost of purchasing two ThreatARMOR systems for their production network. ThreatARMOR currently runs in their production network, inline, in blocking mode, adding a necessary and highly valuable layer to this institution's network security posture.

ABOUT IXIA

Ixia provides testing, visibility and security solutions, strengthening applications across physical and virtual networks for enterprises, governments, service providers, and network equipment manufacturers.

IXIA WORLDWIDE HEADQUARTERS
26601 AGOURA RD.
CALABASAS, CA 91302
(TOLL FREE NORTH AMERICA)
1.877.367.4942
(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 1.818.871.1805
www.ixiacom.com

IXIA EUROPEAN HEADQUARTERS
IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM
SALES +44.1628.408750
(FAX) +44.1628.639916

IXIA ASIA PACIFIC HEADQUARTERS
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591
SALES +65.6332.0125
(FAX) +65.6332.0127