**Abstract**

This paper attempts to profile the port scanning entities based on the data from internet. It also tries to identify the cause of port scans. Additionally, it tries to understand the mechanism taken by organization in the light of such scans and how it differentiates between a malign and benign scan. It ends with providing recommendations to organizations who wishes to perform scan based on the recent advancements in the field.

While port scanning is pervasive, the introduction of ZMap and Masscan in 2013 shifted the scanning landscape by reducing the time taken to scan the ipv4 space from months to minutes. The paper also attempts to profile the scanners and the type of scans performed. The bullet-proof hosting providers facilitated an increase in the scanning practices since the past 5-10 years.

The paper highlights that researchers are using the scanners to cull DDos attacks and measure distributed systems and attackers are using them to find vulnerable hosts with 24hours of the discovery of the vulnerability. The paper further adds that majority of the network operators do not regards scanning as a thread thus painting a dismal picture of the current security.

The paper shows that 80% of the internet probe traffic arise from horizontal scanning and that though many scans are conducted by academic researchers, attackers stills hold a large percent of the space and utilize is to find and attack vulnerability.

The paper studied 5.5M addresses, or 0.145% of the ipv4 traffic. An activity was defined as a scan if a source address contacted atleast 100 unique addresses on the same port and protocol at scan rate of 10 packets per second.

Scan dynamics: while there is a relatively small number of large scans (0.28%), nearly 80% of scan traffic is generated by these scans.

10.8M scans from 1.76M hosts out of which 4.5M are target <1% of the IpAS and are likely Conficker traffic. Excluding Conficker, the scans are 56.4% TCP-SYN packets, 35 UDP and 8.6 ICMP. Only 17,918 scans (0.28%) targeted more than 1% of the address space, 2,699 (0.04%) targeted more than 10%, and 614 (0.01%) targeted more than 50% (see Figure 5). However, after excluding Conficker traffic, we note that 78% of probe traffic is generated by scans targeting >1% of the IPv4 address space, 62% by scans targeting 10%, and 30% by scans targeting 50% (see Figure 4)..

Targeted sevices: Close to half of all scan traffic ~49% targets NetBIOS. Of these, 95.1% emerge from small scans- scans targeting <10% of the ipv4 space-are conficker. Small scan and large scan show different characterisitcs. In both large and small scans, there appear to be a mix of protocols frequently associated with vulnerability scanning (e.g. Microsoft RDP, telnet, Microsoft SQL server, and VNC) as well protocols frequently studied by academic researchers (e.g. HTTP, HTTPS, SSH). particularly China, which performs regular scans against SSH, SQL Server, and Microsoft RDP. For example, while Microsoft Remote Desktop Protocol (RDP) is the fourth most scanned protocol, 77% of scans and 76% of probe packets originate from China

Regularly Scheduled Scans

We investigate the 25 most aggressive scanners and find several examples of both academic research scans and likely malicious groups performing repeated scans. In many of the cases where scans were performed from an academic network, researchers provided information on the purpose of their scanning. However, most scans take place from bullet-proof hosting providers or from China and provide no identifying information. The academic and non-profit scans primarily focus on protocols used for DDoS amplification and studying cryptographic ecosystems (e.g. HTTPS and SSH). All of the groups we identified explained the purpose of their scanning and allow operators to request exclusion. Similarly, several security companies also completed scans. The Shodan Search Engine [34] was the only security group that we were able to detect that did not provide information over the web on scan addresses.

ZMap and Masscan Usage: The majority of scans targeting >10% of the IPv4 address space used either ZMap or Masscan. However, as scan coverage increases, the probability that a scanner uses ZMap steeply increases.

4.1 Linksys Backdoor: In late December 2013, Eloi Vanderbeken disclosed a backdoor in common Cisco, Linksys, and Netgear home and small business routers [44]. The backdoor allowed full, unauthenticated, remote access to routers over an undocumented ephemeral port, TCP/32764. While there was previously only negligible traffic to the port, traffic spiked on January 2, 2014 when news sources began to cover the story [1,11,21]. There remained an average, sustained 1.98 billion estimated probe packets and 99.55 GB of traffic per day through the end of January (Figure 9). After the disclosure, 22 hosts completed 43 scans targeting port 32764 on 1% of the IPv4 address space. scan traffic was not from a large number of distributed botnets hosts, but rather a small number of high-speed scanners.

Heartbleed Vulnerability:

In the week following the disclosure, we detected 53 scans from 27 hosts targeting HTTPS. In comparison, in the week prior to the disclosure, there were 29 scans from 16 hosts. Unlike the Linksys vulnerability, there was not a sustained increase in scanning behavior. However, scan traffic was temporarily more than doubled for several days following the public disclosure. While we do not know whether the scanners intended to exploit the vulnerability, we can detect which hosts began scanning for the first time following the disclosure. Of the 29 HTTPS scans seen prior to the disclosure, seven were daily scans from the University of Michigan, one was executed as part of Rapid7’s SSL Sonar Project, and one belonged to the Shodan Project. A Chinese host (218.77.79.34) also performed daily scans.

NTP DDos Attack

The scanning behavior surrounding NTP is similar to what we observed for the Linksys backdoor and the Heartbleed vulnerability. Specifically, 97.3% of probe traffic destined for NTP was part of large scans (targeting >1%), rather than from distributed botnet scanning. In January 2014, 29 scans from 19 hosts targeted NTP (UDP/123); 8 of the hosts used ZMap; 1 used Masscan. Three groups completed regular scans: Ruhr-Universitaet Bochum completed weekly scans, Shodan performed daily scans, and Errata Security completed one scan. Three hosts in China completed full scans.

Defense Measures

This section talks about the response to the above mentioned attacks at length. The networks are not scanning proactively but are stumbling upon the attacks after years of consistent scanning. The paper shows using data that only a small amount of firms are detecting and blocking scan traffic. The removal of a small number organizations that blocked traffic resulted in large changes in the aggregate inaccessible address space. The ratio of organization aware of the scanning vs the no of organizations requesting exclusion shows that many are cognizant of the activity and do not have an issue with it. 40% organizations blacklisted the subnet used resulting in the exclusion of 18.7% of the address space. We suspect that the organizations that request exclusion or begin blocking traffic years later are not proactively noticing scan traffic, but rather happening upon log entries during other maintenance and troubleshooting.

The scan detection methods of the organization appears to be simply relying on the server and the firewall logs.

The papers provides recommendation to the current and the future researchers by stating the importance of publishing the details of the research scan and providing necessary contact points.