NEXUSGUARD®

A New Threat to CSP Networks

The impending “Black Storm”

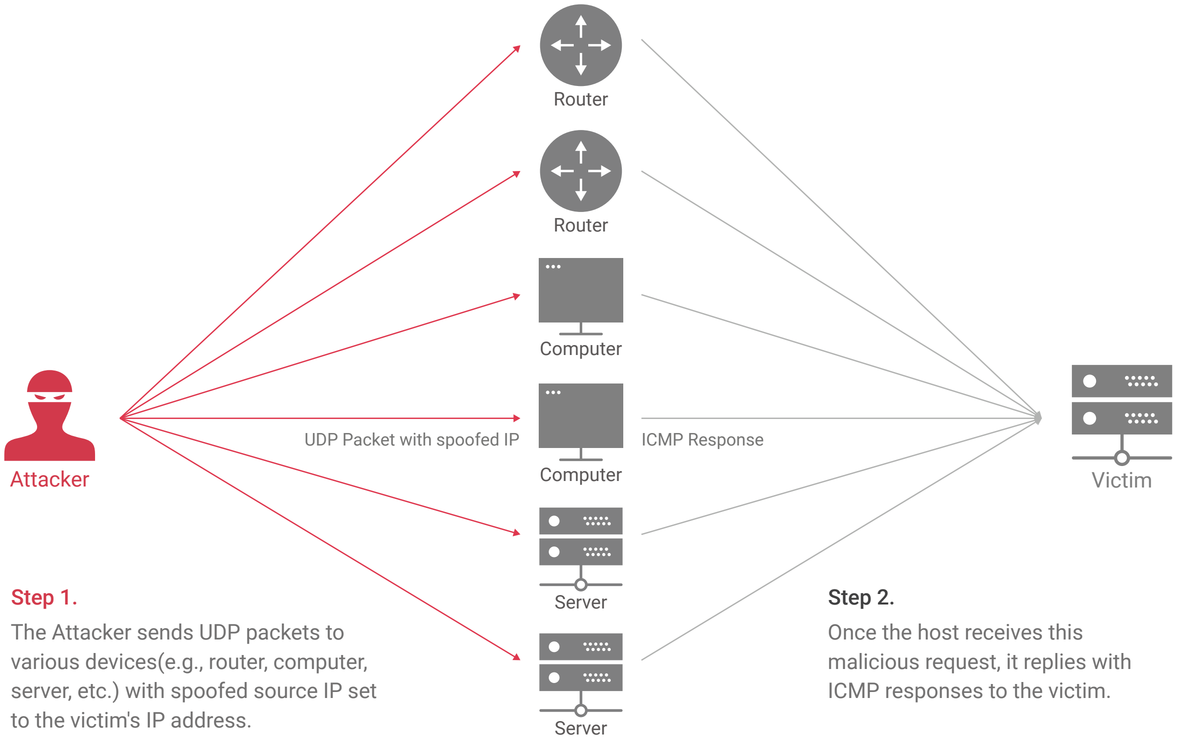
WHITE PAPER

Introduction

Nexusguard Research Team recently theorized that a cyber threat, coined the “Black Storm” attack, could potentially be used by attackers to wreak havoc on CSP (Communications Service Provider) networks. It first began when we saw evidence of a BlackNurse attack being employed in a reflective manner, thereby creating a new type of attack which we shall henceforth name Reflected BlackNurse or “rBlackNurse” for short.

A BlackNurse attack, in a nutshell, is based on ICMP Type 3 (Destination Unreachable) Code 3 (Port Unreachable) requests. These are packet replies typically returned to ping sources indicating the destination port is unreachable.

A rBlackNurse attack, however, involves an attacker generating spoofed UDP requests to CSP devices’ UDP ports that are closed. When this happens, the devices respond with an ICMP Type 3/Code 3 destination port unreachable response to the spoofed IP source. As more and more devices continue to respond to the spoofed IP source, the targeted CSP network is completely overwhelmed by the accumulated volume of these responses, generating an ICMP storm effect, which then manifests into a Black Storm attack.



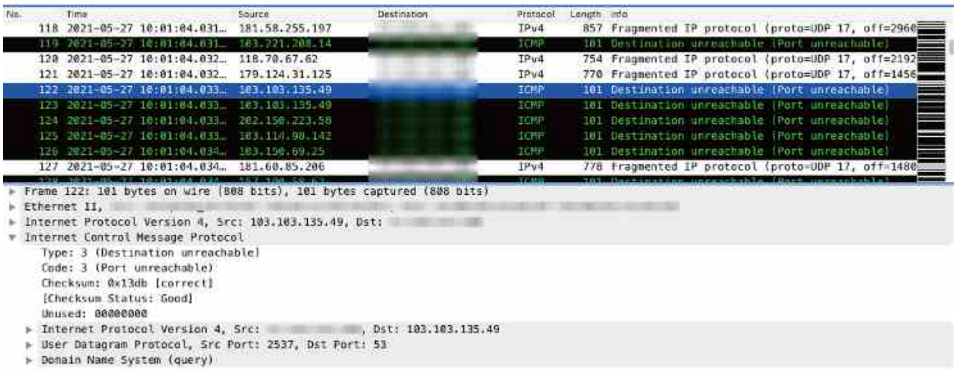
Step 1.
The Attacker sends UDP packets to various devices(e.g., router, computer, server, etc.) with spoofed source IP set to the victim's IP address.

Step 2.
Once the host receives this malicious request, it replies with ICMP responses to the victim.

Figure 1 - rBlackNurse Attack

Black Storm attacks are far easier to generate than the more prominent amplification attacks

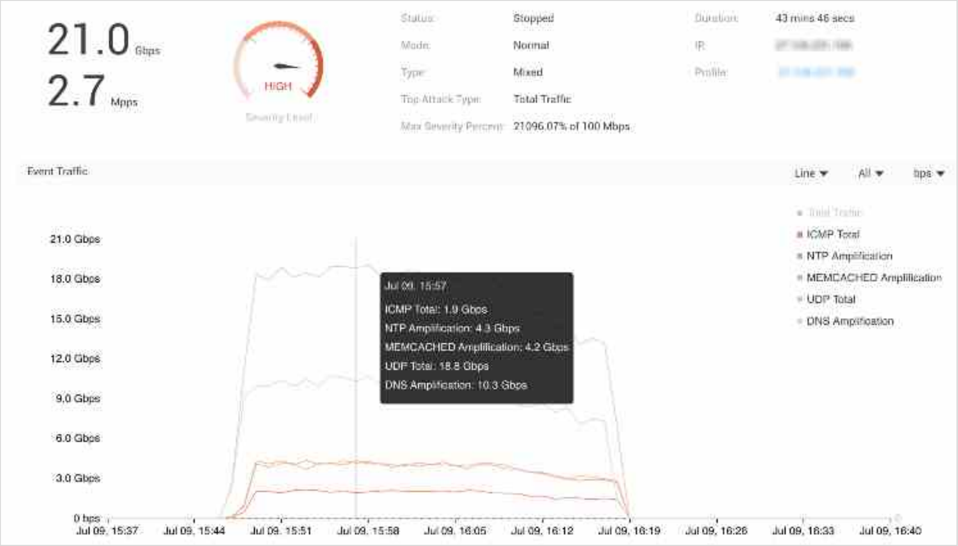
On the evidence of what we’ve seen, a rBlackNurse attack leverages ICMP with Type 3/Code 3 packets embedded in a UDP request (DNS, NTP, etc.) to generate Black Storm attacks against CSP networks, as illustrated in the code shown in Figure 2.



```
No.     Time                     Source            Destination  Protocol  Length  Info
    118 2021-05-27 10:01:04.031… 181.58.255.197    [redacted]   IPv4        857  Fragmented IP protocol (proto=UDP 17, off=2960
    119 2021-05-27 10:01:04.031… 103.221.208.14                 ICMP        101  Destination unreachable (Port unreachable)
    120 2021-05-27 10:01:04.032… 118.70.67.62                   IPv4        754  Fragmented IP protocol (proto=UDP 17, off=2192
    121 2021-05-27 10:01:04.032… 179.124.31.125                 IPv4        770  Fragmented IP protocol (proto=UDP 17, off=1456
    122 2021-05-27 10:01:04.033… 103.103.135.49                 ICMP        101  Destination unreachable (Port unreachable)
    123 2021-05-27 10:01:04.033… 103.103.135.49                 ICMP        101  Destination unreachable (Port unreachable)
    124 2021-05-27 10:01:04.033… 202.150.223.58                 ICMP        101  Destination unreachable (Port unreachable)
    125 2021-05-27 10:01:04.033… 103.114.98.142                 ICMP        101  Destination unreachable (Port unreachable)
    126 2021-05-27 10:01:04.034… 103.150.69.25                  ICMP        101  Destination unreachable (Port unreachable)
    127 2021-05-27 10:01:04.034… 181.60.85.206                  IPv4        778  Fragmented IP protocol (proto=UDP 17, off=1480
▸ Frame 122: 101 bytes on wire (808 bits), 101 bytes captured (808 bits)
▸ Ethernet II, [redacted]
▸ Internet Protocol Version 4, Src: 103.103.135.49, Dst: [redacted]
▾ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 3 (Port unreachable)
    Checksum: 0x13db [correct]
    [Checksum Status: Good]
    Unused: 00000000
  ▸ Internet Protocol Version 4, Src: [redacted], Dst: 103.103.135.49
  ▸ User Datagram Protocol, Src Port: 2537, Dst Port: 53
  ▸ Domain Name System (query)
```

Figure 2 - Attack Code

Based on our findings, a rBlackNurse attack aimed at a single CSP network, illustrated in Figure 3 had been reflected by multiple routers around the world. The size of each attack can vary between 100Mbps and 1Gbps, though the attack itself can become even more potent when mixed with other types of amplification attacks.



21.0 Gbps
2.7 Mpps

Status: Stopped
Mode: Normal
Type: Mixed
Top Attack Type: Total Traffic
Max Severity Percent: 21096.07% of 100 Mbps
Duration: 43 mins 46 secs
IP: [redacted]
Profile: [redacted]

Jul 09, 15:57
ICMP Total: 1.9 Gbps
NTP Amplification: 4.3 Gbps
MEMCACHED Amplification: 4.2 Gbps
UDP Total: 18.8 Gbps
DNS Amplification: 10.3 Gbps

Figure 3 - Attack Graph

With amplification attacks, attackers leverage the functionality of open services such as DNS servers in order to overwhelm a target server or network with an amplified amount of traffic, rendering the server and its surrounding infrastructure inaccessible. Because these services have fixed IP addresses, the origin of such attacks have to be traced before they can be stopped in their tracks by applying appropriate mitigation measures.

Black Storm attacks, however, are generated through rBlackNurse attacks which can be triggered simply by exploiting any type of device with closed ports on a CSP network that responds to an ICMP Destination Port Unreachable request, and then used as reflectors within the CSP network. In view of these factors, we believe that Black Storm attacks can be more easily achieved than amplification attacks, and could potentially take the cyberworld by storm.

"While amplification attacks rely on open services such as DNS servers, a Black Storm attack can leverage any device connected to the Internet"

The potential devastation of Black Storm attacks on CSP networks

To give an idea of the potency of a Black Storm attack - if the target is a medium to large-sized enterprise, the attack volume generated from the attack would be enough to terminate the target in a clean sweep. However, if the target were a large-scale CSP network and a rBlackNurse attack is used in conjunction with other amplification attacks to create a Black Storm attack, the overall effect would have an astronomical impact on the network, leaving it severely crippled, while for small and medium-sized CSP networks, the entire networks would be completely saturated.

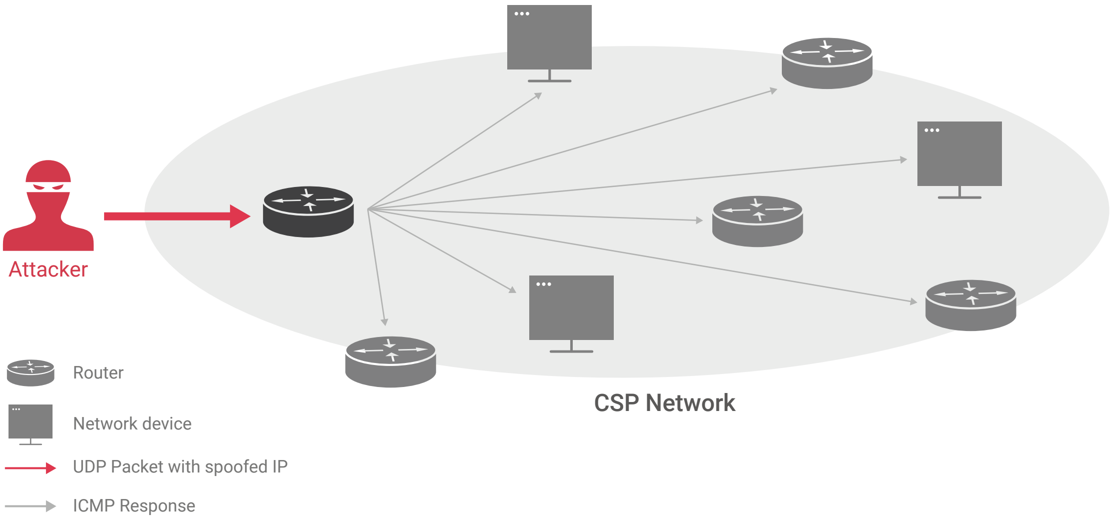
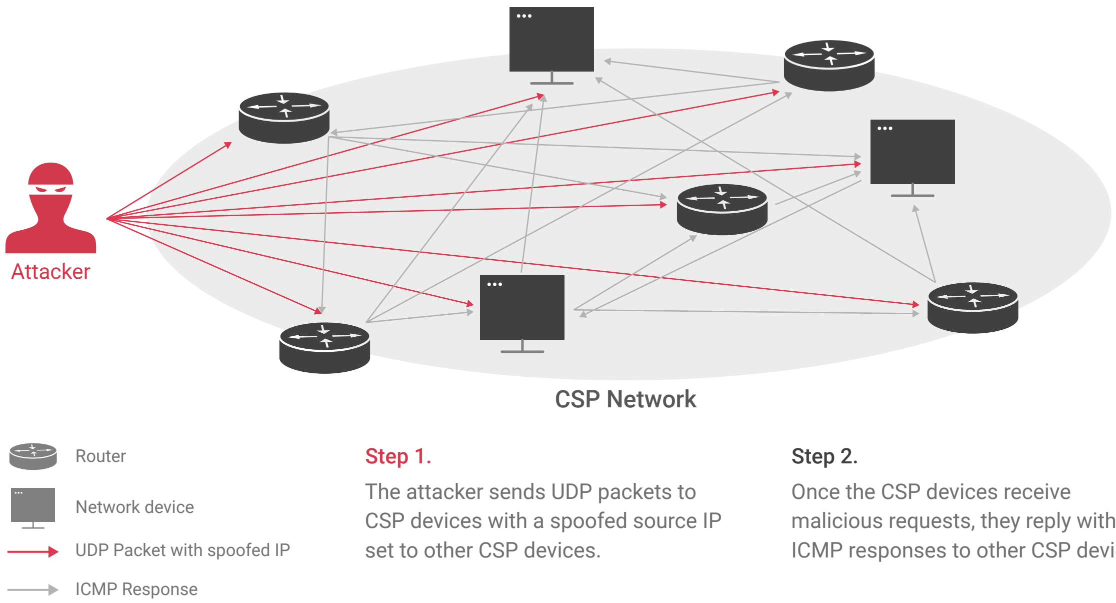


Figure 4 - Proliferation of rBlackNurse traffic within a CSP Network

CSPs are primarily equipped with standard DDoS mitigation solutions designed to detect and mitigate incoming traffic but not so much internal traffic. When attackers send UDP packets with spoofed source IPs to network devices, the rBlackNurse traffic rapidly starts to proliferate internally within the CSP network, as illustrated in Figure 4.

The attack power from a rBlackNurse attack coupled with reflected internal attack traffic (depicted by grey lines in Figure 5), to generate a Black Storm attack, has the potency to completely obliterate the entire CSP network. To make matters worse, attackers could also generate other types of DDoS attacks at the same time to maximize the impact even further. This seriously calls into question whether a CSP's general DDoS Mitigation solutions can operate effectively without compromising stability when dealing with attacks of this nature, capable of paralyzing entire networks.



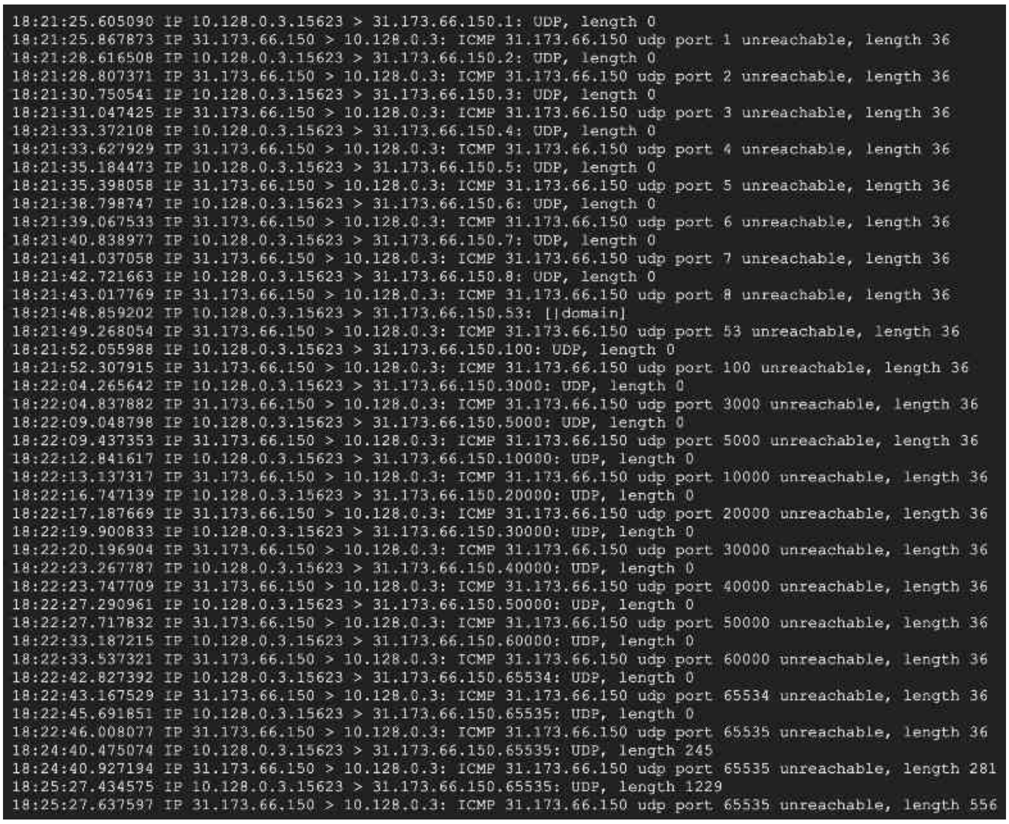
Step 1.
The attacker sends UDP packets to CSP devices with a spoofed source IP set to other CSP devices.

Step 2.
Once the CSP devices receive malicious requests, they reply with ICMP responses to other CSP devices.

Figure 5 - Black Storm attack within a CSP Network

Determining Vulnerability

To study the behaviour of reflection requests, we conducted an experiment on a CSP router. Using ports 1-65535 as our testing range, we generated a number of UDP requests to various closed UDP ports. We recorded that for each and every request sent, the router replied with an ICMP "Destination Port Unreachable" response, as illustrated in Figure 6 below.



```
18:21:25.605090 IP 10.128.0.3.15623 > 31.173.66.150.1: UDP, length 0
18:21:25.867873 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 1 unreachable, length 36
18:21:28.616508 IP 10.128.0.3.15623 > 31.173.66.150.2: UDP, length 0
18:21:28.807371 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 2 unreachable, length 36
18:21:30.750541 IP 10.128.0.3.15623 > 31.173.66.150.3: UDP, length 0
18:21:31.047425 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 3 unreachable, length 36
18:21:33.372108 IP 10.128.0.3.15623 > 31.173.66.150.4: UDP, length 0
18:21:33.627929 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 4 unreachable, length 36
18:21:35.184473 IP 10.128.0.3.15623 > 31.173.66.150.5: UDP, length 0
18:21:35.398058 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 5 unreachable, length 36
18:21:38.798747 IP 10.128.0.3.15623 > 31.173.66.150.6: UDP, length 0
18:21:39.067533 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 6 unreachable, length 36
18:21:40.838977 IP 10.128.0.3.15623 > 31.173.66.150.7: UDP, length 0
18:21:41.037058 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 7 unreachable, length 36
18:21:42.721663 IP 10.128.0.3.15623 > 31.173.66.150.8: UDP, length 0
18:21:43.017769 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 8 unreachable, length 36
18:21:48.859202 IP 10.128.0.3.15623 > 31.173.66.150.53: [|domain]
18:21:49.268054 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 53 unreachable, length 36
18:21:52.055988 IP 10.128.0.3.15623 > 31.173.66.150.100: UDP, length 0
18:21:52.307915 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 100 unreachable, length 36
18:22:04.265642 IP 10.128.0.3.15623 > 31.173.66.150.3000: UDP, length 0
18:22:04.837882 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 3000 unreachable, length 36
18:22:09.048798 IP 10.128.0.3.15623 > 31.173.66.150.5000: UDP, length 0
18:22:09.437353 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 5000 unreachable, length 36
18:22:12.841617 IP 10.128.0.3.15623 > 31.173.66.150.10000: UDP, length 0
18:22:13.137317 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 10000 unreachable, length 36
18:22:16.747139 IP 10.128.0.3.15623 > 31.173.66.150.20000: UDP, length 0
18:22:17.187669 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 20000 unreachable, length 36
18:22:19.900833 IP 10.128.0.3.15623 > 31.173.66.150.30000: UDP, length 0
18:22:20.196904 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 30000 unreachable, length 36
18:22:23.267787 IP 10.128.0.3.15623 > 31.173.66.150.40000: UDP, length 0
18:22:23.747709 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 40000 unreachable, length 36
18:22:27.290961 IP 10.128.0.3.15623 > 31.173.66.150.50000: UDP, length 0
18:22:27.717832 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 50000 unreachable, length 36
18:22:33.187215 IP 10.128.0.3.15623 > 31.173.66.150.60000: UDP, length 0
18:22:33.537321 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 60000 unreachable, length 36
18:22:42.827392 IP 10.128.0.3.15623 > 31.173.66.150.65534: UDP, length 0
18:22:43.167529 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 65534 unreachable, length 36
18:22:45.691851 IP 10.128.0.3.15623 > 31.173.66.150.65535: UDP, length 0
18:22:46.008077 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 65535 unreachable, length 36
18:24:40.475074 IP 10.128.0.3.15623 > 31.173.66.150.65535: UDP, length 245
18:24:40.927194 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 65535 unreachable, length 281
18:25:27.434575 IP 10.128.0.3.15623 > 31.173.66.150.65535: UDP, length 1229
18:25:27.637597 IP 31.173.66.150 > 10.128.0.3: ICMP 31.173.66.150 udp port 65535 unreachable, length 556
```

Figure 6 - ICMP Destination Port Unreachable responses

Vulnerability Checks against rBlackNurse Attacks

To test if your device is vulnerable to rBlackNurse attacks, send a UDP packet to your network using the following commands:

```
Hping3 -2 <target ip> -p <closed port> -c 1
```

Your device is susceptible to rBlackNurse attacks if an ICMP Destination Port Unreachable response is received while the test is running.

Recommendations to CSPs

REC. 1
deep learning-based detection

It is beyond the capabilities of CSPs with standard DDoS mitigation systems to discern and drop internal UDP traffic (with or without spoofed IPs) generated from DNS/NTP requests or from random port UDP packets with no payloads within a CSP network. Moreover, applying access control to CSP devices is easier said than done due to the complexities and intricacies behind a CSP's network. It is therefore recommended that deep learning-based detection methods are employed to learn and analyze network traffic patterns, so that Black Storm attacks are detected well before they can be exploited. The added bonus is that deep learning-based detection is extremely proficient in analyzing huge amounts of data quickly and accurately, overcoming the inefficiencies inherent in threshold and signature-based detection methods.

REC. 2
access control

Although ICMP packets like Destination Port Unreachable are necessary to allow networks to work properly, the recommended best practice is to apply some form of access control to routers, similar to a black/white list, such that access to UDP and TCP ports is limited to only allow trusted source IPs.

REC. 3
vulnerability scanning regularly

Lastly, performing vulnerability scanning regularly (e.g. every quarter) to ensure that there are no network vulnerabilities is always strongly recommended, particularly for devices that reply to ICMP Type 3 Code 3 packets.

To defend against Black Storm attacks, it is essential to have a rapid response system that can automatically detect and mitigate malicious UDP traffic as soon as possible.

Research & Methodology

As a global leader in Distributed Denial of Service (DDoS) attack mitigation, Nexusguard observes and collects real-time data on threats facing enterprise and service-provider networks worldwide. Threat intelligence is gathered via attack data, research, publicly available information, Honeypots, ISPs, and logs recording traffic between attackers and their targets. The contents of this paper are based on analyses and experimental verification of actual attack cases to assist in evaluating the potential impacts on CSPs. The analysis conducted by our research team identifies vulnerabilities and measures attack trends worldwide to provide a comprehensive view of DDoS threats.

Attacks and hacking activities have a major impact on cybersecurity. Because of the comprehensive, global nature of our data sets and observations, Nexusguard is able to evaluate DDoS events in a manner that is not biased by any single set of customers or industries. Many zero-day threats are first seen on our global research network. These threats, among others, are summarized in this paper produced by Nexusguard's research team:

- Tony Miu, Editor, Research Direction, Threat Analysis and Content Development
- Ricky Yeung, Research Engineer, Data Mining & Data Analysis

About Nexusguard

Founded in 2008, Nexusguard is a leading cloud-based distributed denial of service (DDoS) security solution provider fighting malicious internet attacks. Nexusguard ensures uninterrupted internet service, visibility, optimization and performance. Nexusguard is focused on developing and providing the best cybersecurity solution for every client across a range of industries with specific business and technical requirements. Nexusguard also enables communications service providers to deliver DDoS protection solution as a service. Nexusguard delivers on its promise to provide you with peace of mind by countering threats and ensuring maximum uptime.

NEXUSGUARD®

www.nexusguard.com