TLP: GREEN

Issue Date: 2015.10.28

Risk Factor- Medium

Threat Advisory: NetBIOS name server, RPC portmap and Sentinel reflection DDoS

1.0 / OVERVIEW / In the third quarter of 2015, Akamai mitigated and analyzed three new reflection DDoS attack vectors – NetBIOS name server reflection DDoS, RPC portmap reflection DDoS and Sentinel reflection DDoS, which reflects off of licensing servers.

For malicious actors looking to bring a website or web service offline, distributed reflection denial of service (DrDoS) attacks have been a popular weapon for years. Reflection DDoS attacks work because some Internet protocol services provide amplification – the response sent back is larger than the query sent by the malicious actor. Attackers spoof the source of the attack, so the responses are directed at the attacker's target. Reflection attack vectors allow attackers to consume far less of their own bandwidth while consuming far more of their targets' bandwidth – leading to a denial of service outage.

UDP services are especially popular for reflection DDoS attacks. Unlike TCP, UPD is connectionless – there is no mechanism to verify that a particular transmission was received. It looks like no UDP service is safe from use by DDoS attackers, though some UDP services have disadvantages such as only a limited number of hosts running the service.

The three new reflection DDoS attacks and the payloads observed by Akamai are analyzed in this threat advisory, including the risk they each pose.

2.0 / REFLECTION DDOS METHODOLOGY / The Network Basic Input/Output System (NetBIOS) attack, the remote procedure call (RPC) portmap DDoS attack, and the Sentinel reflection DDoS attack are all new reflection attack vectors that abuse UDP.

In a reflection DDoS attack, a malicious actor begins by sending a query to a victim IP address. The victim is an unwitting accomplice in the attack. The victim could be any device on the Internet that exposes a reflectable UDP service. The attacker's query is spoofed to appear to originate from the attacker's target. The attacker uses an automated attack tool to send malicious queries at high rates to a large list of victims, who will in turn respond to the target. Figure 1 shows the malicious queries generated in a lab environment by each of three attack tools designed to generate one of these new reflection attacks.

```
NetBIOS spoofed query using source port 80

15:35:37.764702 IP (tos 0x0, ttl 255, id 55883, offset 0, flags [none], proto UDP (17),
length 78)
    192.168.0.1.80 > 10.1.1.10.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST

RPC portmap spoofed query using source port 80
23:11:05.216035 IP (tos 0x0, ttl 255, id 32197, offset 0, flags [none], proto UDP (17),
length 68)
    192.168.0.1.80 > 10.1.1.10.111: UDP, length 40

Sentinel spoofed query using source port 80
15:31:15.281467 IP (tos 0x0, ttl 255, id 40053, offset 0, flags [none], proto UDP (17),
length 34)
    192.168.0.1.80 > 10.1.1.10.5093: UDP, length 6
```

Figure 1: Sample spoofed queries sent to victim hosts listening for NetBIOS, RPC, and Sentinel

Each of these queries abuses a different reflected UDP service and generates a response from the host at IP address 10.1.1.10 to the host at IP address 192.168.0.1. In a real DDoS attack, the 192.168.0.1 IP address would be replaced with the IP address of a target website or other target service the malicious actor wants to bring down.

The responses would originate from the victim IP address – in this case 10.1.1.10. Each would come from the port that offers that service, and was targeted by a query: NetBIOS from port 137, RPC from port 111, and Sentinel from port 5093. The responses would be sent to the target's UDP port 80. Although the target may not be listening on UDP port 80, nonetheless a flood of responses arriving from all over the world would likely exceed the network capacity available at the target site if not protected by a cloud-based DDoS mitigation service.

2.1 / ATTACK TIMELINE: 10 ATTACK CAMPAIGNS / Akamai has mitigated each of the three new reflection attack methods multiple times while protecting our customers. An attack timeline from March to September 2015 shows the 10 attack campaigns that use of these three DDoS attack vectors (Figure 2). One of the 10 reflection attack campaigns was especially large. The RPC reflection attack vector was used in a mega attack that generated more than 100 Gbps (gigabits per second).

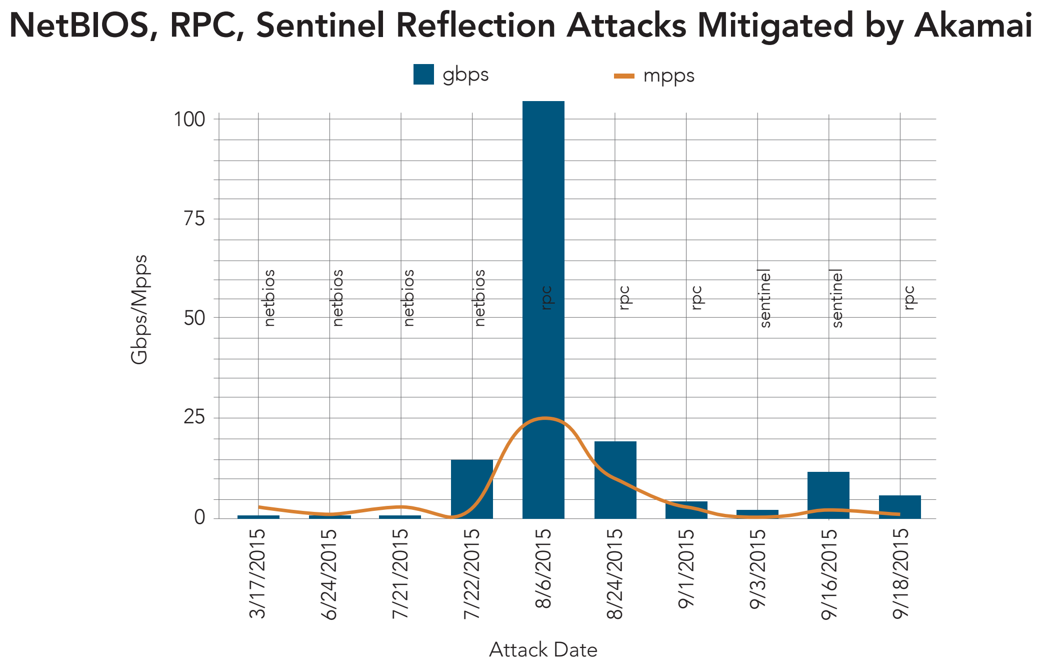

Figure 2: A timeline of NetBIOS, RPC portmap, and Sentinel reflection attacks.
RPC portmap reflection generated the most traffic

3.0 / NetBIOS NAME SERVER REFLECTION PAYLOAD AND AMPLIFICATION / The NetBIOS reflection DDoS attack – specifically NetBIOS Name Service (NBNS) reflection – was observed by Akamai as occurring sporadically from March to July 2015. Although legitimate and malicious NBNS queries to UDP port 137 are a common occurrence, a response flood was first detected in March 2015 during a DDoS attack mitigated for an Akamai customer. A sample of the NetBIOS response traffic captured during the attack is shown in Figure 3.

```
NetBIOS response flood traffic
12:56:33.677742 IP (tos 0x0, ttl 115, id 16677, offset 0, flags [none], proto UDP (17),
length 293)
    X.X.X.X.137 > X.X.X.X.80: NBT UDP PACKET(137): QUERY; POSITIVE; RESPONSE; UNICAST

12:56:33.397793 IP (tos 0x0, ttl 116, id 28481, offset 0, flags [none], proto UDP (17),
length 239)
    X.X.X.X.137 > X.X.X.X.80: NBT UDP PACKET(137): QUERY; POSITIVE; RESPONSE; UNICAST

Expanded view of the previous packet contains computer name(information redacted)
12:56:33.677742 IP (tos 0x0, ttl 115, id 16677, offset 0, flags [none], proto UDP (17),
length 293)
    X.X.X.X.137 > X.X.X.X.80: NBT UDP PACKET(137): QUERY; POSITIVE; RESPONSE; UNICAST
<snip>.................... CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!.........<redacted>
...WORKGROUP      ...<redacted>    ..WORKGROUP      ...WORKGROUP      .....__MSBROWSE
__......>.*m..............................................................................
.................*m.......................................................................
........................
```

Figure 3: Attack signature of a NetBIOS name service (NBNS) reflection attack

The size of the response packets, including headers, was typically 200-300 bytes, which can be compared to the 78-byte attack request to identify an amplification factor of 2.56 to 3.85. Akamai observed four NetBIOS name server reflection attacks, with the largest recorded at 15.7 Gbps.

3.1 / ABOUT NetBIOS NAME SERVICE / The primary purpose of NetBIOS is to allow applications on separate computers to communicate and establish sessions to access shared resources and to find each other over a local area network. For example, if computers running the Windows operating system are connected in the same network and are not part of a domain but are part of a workgroup, a NetBIOS name can be used to communicate with each computer. NetBIOS name queries are one of the methods attempted for name resolution. A broadcast query from a local computer can be sent to UDP port 137 to discover the names of other computers in the network. This service eliminates the need to recall the IP address of each computer since the computer name would appear in the list of local computers.

3.2 / NetBIOS REFLECTION CAMPAIGN ATTRIBUTES / Of the four attacks, NetBIOS name server reflection was used primarily against gaming customers, but the largest campaign was launched against a hosting customer. Some stats from the largest attack are as follows:

- Peak bandwidth: 15.7 Gbps
- Peak packets per second: 1.8 Mpps
- Source port: 137
- Destination port: UDP 80

3.3 / NetBIOS ATTACK POTENTIAL AND DISTRIBUTION / Project Sonar scans show that slightly more than 2 million unique sources are listening on UDP port 137. Most organizations would not expose such a vulnerable service to the Internet, so the majority of these sources are likely to be home users and cybersecurity defense honeypots and other monitoring services. As a result, it seems likely that this attack will remain more of a nuisance than a significant threat. The pie chart in Figure 4 shows the source country distribution of hosts listening on UDP port 137.

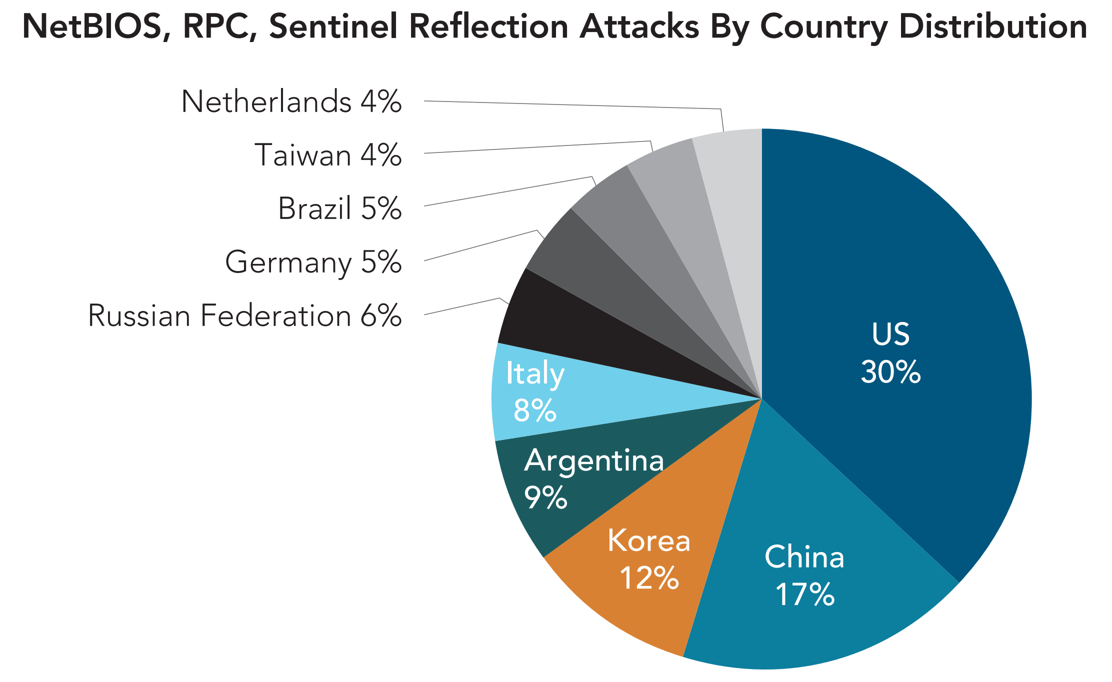

Figure 4: Source IP country distribution based on project sonar list

4.0 / RPC PORTMAP REFLECTION ATTACK / The first RPC portmap reflection DDoS attack observed and mitigated by Akamai occurred in August 2015 in a multi-vector attack campaign against a financial firm. The attack generated more than 105 Gbps of traffic to the target. This vector has been discussed on the Internet such as this blog post by Level 3. The tool attackers are using for the RPC reflection attack produces request with characteristics that can be used for DDoS detection and DDoS mitigation by victims. The targets will likely need a cloud-based DDoS mitigation solution.

4.1 / RPC PORTMAP CAMPAIGN ATTRIBUTES / Of the four RPC reflection attack campaigns mitigated by Akamai, one exceeded 100 Gbps, making it an extremely powerful attack. Akamai expects this attack to continue to be used in the coming quarters. Some stats from the largest attack are as follows:

- Peak bandwidth: 105.96 Gbps
- Peak packets per second: 24.10 Mpps
- Attack vector: RPC reflection and amplification
- Source port: 111
- Destination port: 46694

4.2 / RPC PORTMAP REFLECTION ATTACK METHOD / An RPC reflection DDoS attack begins with malicious queries to the `portmap` program protocol of RPC. The attack tool makes requests similar to the `rpcinfo` tool available on many operating systems. The `rpcinfo` tool by default will make a TCP request on port 111 with a random transaction identifier (XID). Although the attack tool makes the request on UDP port 111, it always uses the same XID. Figure 5 shows a sample query using rpcinfo and an attack script as seen over the packet capture utility `tshark`. The `rpcinfo` tool is set to generate a UDP request with the `-T` option.

```
Command
rpcinfo -T udp -p victim_reflector_ip

Command as seen in tshark (40 byte request payload portion only)
Remote Procedure Call, Type:Call XID:0x3f64c630
    XID: 0x3f64c630 (1063568944)  << different xid generated by client each time
    Message Type: Call (0)
    RPC Version: 2
    Program: Portmap (100000)
    Program Version: 2
    Procedure: DUMP (4)  << request is a port mapper dump
    Credentials
        Flavor: AUTH_NULL (0)
        Length: 0
    Verifier
        Flavor: AUTH_NULL (0)
        Length: 0
Portmap
    [Program Version: 2]
    [V2 Procedure: DUMP (4)]

Attack tool request as seen in tshark(40 byte request payload portion only)
Remote Procedure Call, Type:Call XID:0x65720a37
    XID: 0x65720a37 (1701972535) << hardcoded XID never changes in attack tool
    Message Type: Call (0)
    RPC Version: 2
    Program: Portmap (100000)
    Program Version: 2
    Procedure: DUMP (4)
    Credentials
        Flavor: AUTH_NULL (0)
        Length: 0
    Verifier
        Flavor: AUTH_NULL (0)
        Length: 0
Portmap
    [Program Version: 2]
    [V2 Procedure: DUMP (4)]
```

Figure 5: `rpcinfo` command-line tool query compared to `portmap` attack tool

4.3 / RPC PORTMAP REFLECTION PAYLOAD AND AMPLIFICATION / Figure 6 shows payloads observed during RPC portmap reflection campaigns mitigated by Akamai. The most common payload length observed during the attacks was 628 bytes; the largest was 3,360 bytes.

```
Two sample response packets
17:04:16.178164 IP (tos 0x0, ttl 59, id 0, offset 0, flags [DF], proto UDP (17), length
756)
    x.x.x.x.111 > x.x.x.x.46694: UDP, length 728

17:04:16.185464 IP (tos 0x0, ttl 52, id 0, offset 0, flags [DF], proto UDP (17), length
656)
    x.x.x.x.111 > x.x.x.x.46694: UDP, length 628  << most common payload length observed
during attacks

Largest observed response full packet 1
15:31:33.911707 IP (tos 0x0, ttl 54, id 5741, offset 0, flags [+], proto UDP (17), length
1500)
    x.x.x.x.111 > x.x.x.x.32228: UDP, length 3368

fragment 1
15:31:33.912752 IP (tos 0x0, ttl 54, id 5741, offset 1480, flags [+], proto UDP (17),
length 1500)
    x.x.x.x > x.x.x.x: ip-proto-17

fragment 2
15:31:33.912753 IP (tos 0x0, ttl 54, id 5741, offset 2960, flags [none], proto UDP (17),
length 436)
    x.x.x.x > x.x.x.x: ip-proto-17
```

Figure 6: Payload sample of an RPC reflection attack

The payloads are the responses from victim hosts with the port mapper service exposed on UDP port 111. The largest response of 3,360 bytes (3,436 with headers) was observed from two IP addresses in the attack sample. A single 40-byte request (68 bytes with headers) produced response so large that it was broken into three packets: two IP fragments and one full packet with UDP and IP header. The data payload size of packet fragments would vary depending on the target infrastructure maximum transmission unit (MTU) size and any additional headers. The largest responses had an amplification factor of 50.53. A more common amplification factor was 9.65.

4.4 / RPC PORTMAP ATTACK POTENTIAL AND DISTRIBUTION /

A total of 40,726 unique sources were collected as a subset of attack traffic during RPC portmap reflection campaigns mitigated by Akamai. The distribution of source countries is shown in Figure 7.

Based on the distribution and number of hosts involved, this vector may remain a serious threat. Akamai observed active malicious reflection requests almost daily against various targets in September 2015.

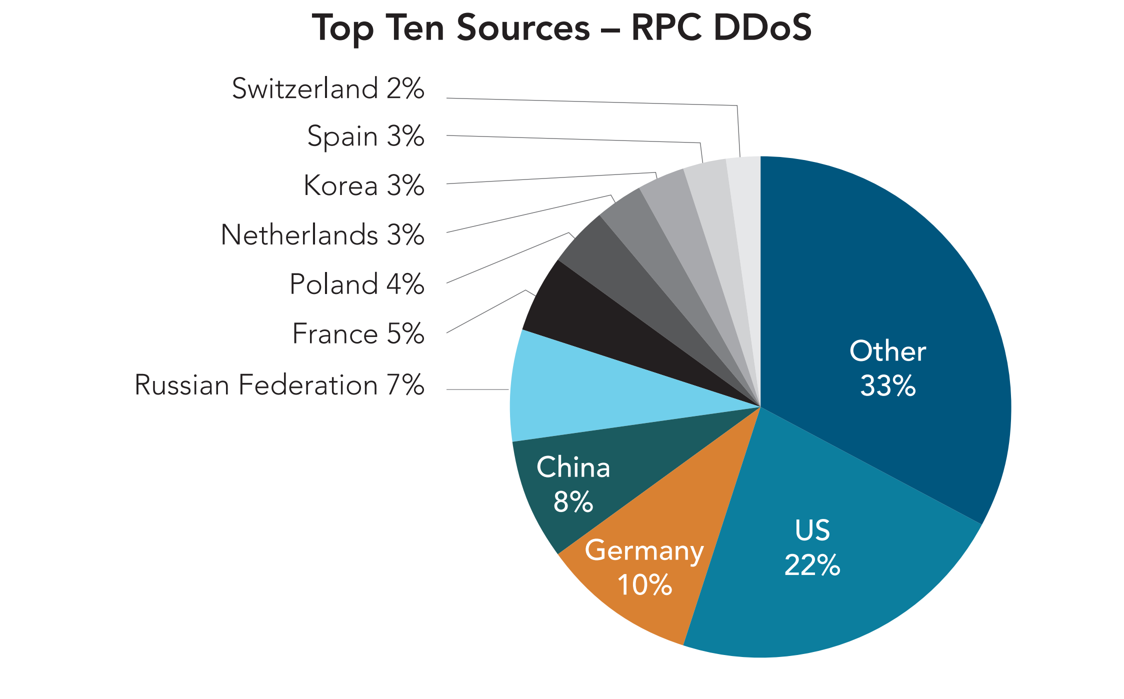

Figure 7: The top ten source countries for RPC reflection DDoS attacks

5.0 / SENTINEL REFLECTION DDOS ATTACK / The first Sentinel reflection DDoS attack was observed in June 2015 at Stockholm University and identified as a vulnerability in the license server for SPSS, a statistical software package from IBM. The university's license servers were apparently leveraged in reflection DDoS attacks. This threat was also discussed in an advisory by Nexusguard. Akamai mitigated two Sentinel reflection DDoS campaigns in September 2015. One attack targeted a financial company and the other targeted a gaming company. Although the attack sources were less numerous than the RPC and NetBIOS attacks, they included more powerful servers with high bandwidth availability, such as university servers. This service is not something that is expected to be found on home user networks.

5.1 / SENTINEL REFLECTION CAMPAIGN ATTRIBUTES / Statistics are provided for one of the two Sentinel reflection DDoS campaigns observed by Akamai in September 2015. Even with the extra bandwidth afforded by servers in well-connected networks, the number of reflectors available limited this attack.

- Peak bandwidth: 11.7 Gbps
- Peak packets per second: 2.5 Mpps
- Attack Vector: Sentinel reflection and amplification
- Source port : 5093
- Destination port: Random

5.2 / SENTINEL REFLECTION PAYLOAD AND AMPLIFICATION / The Sentinel reflection attack begins by sending a simple 6-byte query to a sentinel license server. The query contains only the letter z and 5 nulls (z.....). Payloads from an attack campaign are shown in Figure 8.

```
16:01:14.572122 IP (tos 0x0, ttl 123, id 24986, offset 0, flags [none], proto UDP (17),
length 1460)
    x.x.x.x.5093 > x.x.x.x.1351: UDP, length 1432

16:01:14.576212 IP (tos 0x0, ttl 123, id 24988, offset 0, flags [none], proto UDP (17),
length 1460)
    x.x.x.x.5093 > x.x.x.x.1351: UDP, length 1432
```

Figure 8: Sentinel reflection attack signature

The response payloads captured during each of the two Sentinel reflection attacks mitigated by Akamai were always 1,432 bytes (1,460 bytes with headers). The attack tool generates a 6-byte request payload(34 bytes with headers). This puts the amplification factor at a consistent 42.94.

5.3 / SENTINEL ATTACK POTENTIAL AND DISTRIBUTION / Only 745 unique sources of this attack traffic have been identified. Each was noted more than 2,000 times in trace captures. In comparison, the sources of the RPC reflection attack were more distributed and each appeared fewer than 100 times. It seems there are few hosts with license manager servers listening on UDP port 5093, which constrains attacker resources.

6.0 / THE ATTACK TOOLS / The attack tools for each of these new reflection attacks are related – they are all modifications of the same C code. Each attack vector requires the same basic recipe for success – a script that sends a spoofed request to a list of victim reflectors. The command-line options are similar across all the tools, as shown in Figure 9. The RPC script is lacking the source port parameter; it generates the source port randomly.

```
NetBIOS NS attack script
./nbt <target IP> <target port> <reflection file> <threads> <pps limiter, -1 for no limit>
<time>

RPC portmap attack script
./rpc [IP] [file] [threads] [limiter] [time]

Sentinel attack script
./sentinel <target IP> <target port> <reflection file> <threads> <pps limiter, -1 for no
limit> <time>
```

Figure 9: Command-line parameters available on various DDoS reflection attack scripts

6.1 / ATTACK TOOL TESTS /Using a virtual lab, Akamai tested each of the three attack tools. Each usually comes with a companion scanner tool used to scan the Internet for the specific UDP service to build a list of reflectors.

6.1A / NetBIOS REFLECTION TOOL / During our NetBIOS attack test, a virtual machine (VM) running Microsoft Windows XP was set as the victim, and the target was a Linux host. The attack script was run from a separate Linux VM. All three machines had different IP addresses. The attack host sent a query (pretending to be the target Linux host) to the Windows XP machine, as shown in Figure 10.

```
Spoofed query to victim VM using source port 8475 and NBNS UDP port 137
15:35:37.765276 IP (tos 0x0, ttl 255, id 1575, offset 0, flags [none], proto UDP (17),
length 78)
    192.168.0.1.8475 > 10.1.1.10.137: NBT UDP PACKET(137): QUERY; REQUEST; UNICAST
```

Figure 10: Spoofed NetBIOS name server request

By design, the victim machine receives the request and responds to the source IP address. Since the query was spoofed, the victim host replied with unsolicited traffic to the target VM at 192.168.0.1, as the attack intended. The payload received by the target is shown in Figure 11.

```
15:37:28.529947 IP (tos 0x0, ttl 127, id 4654, offset 0, flags [none], proto UDP (17),
length 221)
    10.1.1.10.137 > 192.168.0.1.8475: NBT UDP PACKET(137): QUERY; POSITIVE; RESPONSE;
UNICAST
............ CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA..!.......w.WVICTIM1       ...WORKGROUP
...WVICTIM1         ..WORKGROUP      .....'..h............................................
...............
```

Figure 11: Attack tool variant payloads observed including scan option

Notice that in the example above only two IP addresses are visible. The attacker IP is never seen, since the requests all pretend to come from a different source.

6.1B / RPC PORTMAP REFLECTION TOOL / The RPC portmap attack script variant we tested was missing the port option. This could be easily modified using the other scripts as examples. Attack campaigns mitigated by Akamai to date contain evidence of modified variants with custom ports, such as the popular destination port 80. This option is unnecessary, because the targeted services usually don't match the attack vector protocol anyway, so the attack's final destination is the firewall or router protecting the web server. Unfortunately once the malicious traffic has reached the target network, the damage is done. The bandwidth generated by these attacks is enough to saturate a network and achieve a denial of service outage.

The payload queries used by the RPC portmap attack tool are shown in Figure 12, which only shows the requests observed to date in the wild that match the attack tool payloads. Two attack payload query variants and one Internet scanner tool payload variant are shown.

```
Attack Payload Query Variant 1(40 Bytes)
Remote Procedure Call, Type:Call XID:0x65720a37
    XID: 0x65720a37 (1701972535)
    Message Type: Call (0)
    RPC Version: 2
    Program: Portmap (100000)
   Program Version: 2
    Procedure: DUMP (4)
    Credentials
        Flavor: AUTH_NULL (0)
        Length: 0
    Verifier
        Flavor: AUTH_NULL (0)
        Length: 0
Portmap
    [Program Version: 2]
    [V2 Procedure: DUMP (4)]

Attack Payload Query Variant 2(50 Bytes)
Remote Procedure Call, Type:Call XID:0x65720a37
    XID: 0x65720a37 (1701972535)
    Message Type: Call (0)
    RPC Version: 2
    Program: Portmap (100000)
    Program Version: 2
    Procedure: DUMP (4)
    Credentials
        Flavor: AUTH_NULL (0)
        Length: 0
    Verifier
        Flavor: AUTH_NULL (0)
        Length: 0
Portmap
    [Program Version: 2]
    [V2 Procedure: DUMP (4)]
    Data (10 bytes)

0000  00 65 72 72 6f 72 2e 20 67 6f                     .error. go
        Data: 006572726f722e20676f
        [Length: 10]

Internet Scanner tool Payload Query(41 Bytes)
Remote Procedure Call, Type:Call XID:0x65720a37
    XID: 0x65720a37 (1701972535)
    Message Type: Call (0)
    RPC Version: 2
    Program: Portmap (100000)
    Program Version: 2
    Procedure: DUMP (4)
    Credentials
        Flavor: AUTH_NULL (0)
        Length: 0
    Verifier
        Flavor: AUTH_NULL (0)
        Length: 0
Portmap
    [Program Version: 2]
    [V2 Procedure: DUMP (4)]
    Data (1 byte)

0000  00                                                .
        Data: 00
        [Length: 1]
```

Figure 12: Attack tool variant payloads observed, including a scan script payload

Both of the RPC portmap attack tool variants are observed by Akamai to be sending requests almost daily – already this attack seems to be monetized into a DDoS-for-hire framework.

7.0 / DDOS MITIGATION AND SYSTEM HARDENING /For all three attack types, upstream filtering can be used for mitigation where possible. Otherwise a cloud-based DDoS mitigation service provider will be needed. Figure 13 shows a Snort mitigation rule for RPC reflection malicious query to a victim. The rule can be used or modified as needed to detect the specific signature of the malicious queries generated by the RPC portmap attack tool. Similar rules can be made to detect the Sentinel service.

```
alert udp $EXTERNAL_NET any -> $HOME_NET 111 \
(msg: “RPC portmapper reflection request”; \
flow: to_server; \
content: “|65 72 0a 37 00 00 00 00 00 00 00 02 00 01 86 a0 00 00 00 02 00 00 00 04 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00|”; dsize:40<>50; \
classtype:Reflection-Abuse; \
sid: 201500010; rev:1;)
```

Figure 13: snort mitigation rule for RPC Reflection malicious query to victim

For all three services, we should ask if the service needs to be exposed to everyone on the Internet. For NetBIOS, the answer is probably no. For the other two the answer may be yes, and the issue becomes how to protect them. RPC and Sentinel traffic can be monitored with an intrusion detection system (IDS). The Snort IDS has rules built in to detect any RPC portmap query with a message of `RPC portmap listing UDP 111`.

8.0 / SUMMARY /Reflection attacks are not new among DDoS attacks. As more services are probed Akamai expects that more services will be leveraged for DDoS reflection. Many booter and stresser sites feature these attacks as part of their suite of DDoS-for-hire attack vectors. Malicious actors find these attacks easy to use because infection is unnecessary to maintain a reflector army.

DDoS prevention in this case is the responsibility of the victims of these attacks, most of whom are unaware of what is happening or do not have the resources or knowledge to mitigate the abuse. Not every UDP service will make a suitable reflector source, and some that start off strong will be minimized as administrators become aware of the threat.

Like NTP reflection, which is no longer as powerful as it was during the first months of use, NetBIOS reflection is expected to be short-lived. NetBIOS reflection attacks so far have been less effective than other reflection methods, and so may end up only being used occasionally.

Given our samples to date, RPC portmap reflection appears to be a serious threat. It had a fairly quick start, and Akamai has continued to observe to observe RPC queries daily. It’s a likely candidate for continued use.

Although the Sentinel threat has a high amplification factor, the service lacks the widespread availability of RPC. In addition, Sentinel reflection depends on leveraging a service that is in the hands of networking professionals with the knowledge to mitigate its abuse. Sentinel reflection will probably end as license servers are patched or server operators take steps to further limit its effectiveness.

About Akamai Security Intelligence Response Team (SIRT) Focuses on mitigating malicious global cyber threats and vulnerabilities, the Akamai Security Intelligence Response Team (SIRT) conducts and shares digital forensics and post-event analysis with the security community to proactively protect against threats and attacks. As part of its mission, the Akamai SIRT maintains close contact with peer organizations around the world and trains Akamai's Professional Services and Customer Care teams to both recognize and counter attacks from a wide range of adversaries. The research performed by the Akamai SIRT is intended to help ensure Akamai's cloud security products are best of breed and can protect against any of the latest threats impacting the industry.

About Akamai® As the global leader in Content Delivery Network (CDN) services, Akamai makes the Internet fast, reliable and secure for its customers. The company's advanced web performance, mobile performance, cloud security and media delivery solutions are revolutionizing how businesses optimize consumer, enterprise and entertainment experiences for any device, anywhere. To learn how Akamai solutions and its team of Internet experts are helping businesses move faster forward, please visit www.akamai.com or blogs.akamai.com, and follow @Akamai on Twitter.

Akamai is headquartered in Cambridge, Massachusetts in the United States with operations in more than 57 offices around the world. Our services and renowned customer care are designed to enable businesses to provide an unparalleled Internet experience for their customers worldwide. Addresses, phone numbers and contact information for all locations are listed on www.akamai.com/locations.