SHADOW Indications Technical Analysis
Coordinated Attacks and Probes
Sep 04 1998 Updated DEC 14 1998

Naval Surface Warfare Center
Dahlgren Division, Code XDC3

Special Note: This document has largely been overtaken by new advances in hacker technology. Before you report a coordinated attack to your CIRT (and please always report to your CIRT) you may want to look at the following common attack and scan tools: Nmap 2.08's decoy option, ICMP by slayer, Hping. The traces in this paper all predate these capabilities, but it can be challenging to sort things with the look and feel of a coordinated attack from the real thing. Please see the coordinated attack paper presented at the Usenix Intrusion Detection and Network Monitoring conference for a more complete discussion of this network behavior.

Shadow - FEB 24, 1999

Timeframe: Analysis performed on detects from Sep 1998
Caveat: None of the names or IP Addresses in this document are correct, any resemblance to a real domain name is purely coincidental.

Executive Summary:
This document details attacks and probes that have been recently observed in which multiple attackers are clearly working together toward a common goal from different IP addresses. Often these IP addresses are also physically separated, in different countries or even different continents.

There are three obvious purposes for this type of activity:

- Stealth. By working from multiple IP addresses the attackers achieve a smaller per-IP signature and are more difficult to detect with conventional means. In addition, stealth is enhanced by the development of new hard-to-detect probing techniques.

- Firepower. By coordinating multiple attacking IP addresses, the attackers will be able to deliver more exploits on target in a smaller time window. Target in this case can be one or more sites. Further, the defense technique of blocking an attacker IP or subnet (shunning) will be less effective. We believe that the use of coordinated scans and probes from

differing sites represents a new and continuing capability that merits further analysis and tracking. Some of these coordinated probes and scans we are seeing today may be practice runs for future larger scale attacks.

- More data. By working from different IP addresses, often entirely different subnets, against the same target it is possib to obtain data that is difficult from a single source IP scan or probe. This data may include shortest route data (i.e. packe from source A arrive faster than from source B), or even potenti backdoors (i.e. packets from source A can gain access to hosts t source B can't see). This type of data can be used to optimise future scans, probes, or attacks.

Analysis:
Multiple different attacks and probes are documented here. The commonality is that the attacker is able to launch the attack from multiple unrelated (or partially related) addresses in a coordinated fashion. Special thanks to Vicki Irwin, and Pedro Vazquez for their help in deciphering this puzzle.

==========
EXAMPLE 1: Coordinated traceroutes
These have been reported previously, but they make an excellent example of the general approach.

Five different sources all hit the target (a firewall) within minutes of each other. The signature of each hit is nearly identical. Note the use of two entirely different domains within seconds of each other. This will allow them to have timing data for multiple paths.

```
12:29:30.012086 5.net.39964 > target.33500: udp 12 [ttl 1]
12:29:30.132086 5.net.39964 > target.33501: udp 12 [ttl 1]
12:29:30.252086 5.net.39964 > target.33502: udp 12 [ttl 1]
12:29:30.352086 5.net.39964 > target.33503: udp 12 [ttl 1]
12:29:30.482086 5.net.39964 > target.33504: udp 12 [ttl 1]

12:27:37.712086 4.I.net.46164 > target.33485: udp 12 [ttl 1]
12:27:55.122086 4.I.net.46164 > target.33487: udp 12 [ttl 1]
12:27:55.162086 4.I.net.46164 > target.33488: udp 12 [ttl 1]
12:27:55.182086 4.I.net.46164 > target.33489: udp 12 [ttl 1]

12:29:26.132086 4.v.net.43327 > target.33491: udp 12 [ttl 1]
12:29:26.242086 4.v.net.43327 > target.33492: udp 12 [ttl 1]
12:29:26.372086 4.v.net.43327 > target.33493: udp 12 [ttl 1]
```

```
12:29:26.482086 4.v.net.43327 > target.33494: udp 12 [ttl 1]

12:27:32.962086 3.net.55528 > target.33485: udp 12 [ttl 1]
12:27:33.072086 3.net.55528 > target.33486: udp 12 [ttl 1]
12:27:33.172086 3.net.55528 > target.33487: udp 12 [ttl 1]
12:27:33.292086 3.net.55528 > target.33488: udp 12 [ttl 1]
12:27:33.422086 3.net.55528 > target.33489: udp 12 [ttl 1]

12:27:30.552086 com.35251 > target.33475: udp 12 [ttl 1]
12:27:30.562086 com.35251 > target.33476: udp 12 [ttl 1]
12:27:30.582086 com.35251 > target.33477: udp 12 [ttl 1]
12:27:30.592086 com.35251 > target.33478: udp 12 [ttl 1]
12:27:30.612086 com.35251 > target.33479: udp 12 [ttl 1]
```

Special note: Recently we began screening for large ICMP packets. Many of the ICMP scans we categorized as Smurf attacks were in excess of 1k. Such packets can be used for maximum transmission unit of a path discovery. Please see page 152 in Stevens' TCP/IP Illustrated for further information.[1] Also note the DF flag will be set.[2]

==========

EXAMPLE 2 Simultaneous Reset Scans

During the week of 13 SEP Reset Scans were observed from 14 different internet addresses, primarily ISPs. They are working together and are mapping multiple target sites. This appears to be a long term effort, some of the attackers scan rate is as low as 2 packets/day/target site, well below commonly set thresholds for scan detectors.

Until recently these types of scans were easy to detect due to common "signature acknowledgement numbers" (i.e. the IP packet ACK field was always a fixed number, usually 674719802 or 674711610). The more recent probes have random acknowledgement numbers.

The primary signature here is RESET packets with no other activity from that source (such as an active open (SYN) from the source or the target)

```
17:40:45.870769 hook.24408 > target1.1457: R 0:0(0) ack 674719802 win 0
17:40:53.025203 hook.33174 > target2.1457: R 0:0(0) ack 674719802 win 0
17:41:12.115554 hook.36250 > target3.1979: R 0:0(0) ack 674719802 win 0
17:43:37.605127 router > hook: icmp: time exceeded in-transit
17:43:43.139158 hook.44922 > target4.1496: R 0:0(0) ack 674719802 win 0

17:42:30.400665 grin.3532 > target1a.1167: R 0:0(0) ack 674719802 win 0
17:42:40.582531 grin.33233 > target2a.1797: R 0:0(0) ack 674719802 win 0
17:44:28.836701 grin.52504 > target3a.1634: R 0:0(0) ack 674719802 win 0
17:47:52.578558 grin.46657 > target4a.2121: R 0:0(0) ack 674719802 win 0
```

```
17:47:52.698378 router > grin: icmp: time exceeded in-transit
```

NOTE: When the target site's router replies back to the attacker, they know that host or net does not exist. By locating the places that do not exist, they can take the inverse of the map to target future exploit efforts, scans, probes, or attacks.

NOTE: Certain hosts, primarily IRC servers are under a denial of service attack using spoofed addresses which can cause false positive resets.

NOTE: If the resets center around a particular destination address this could be an indication of IP Spoofing to use RESETS to disrupt a connection. In this case the sequence numbers should show a discernable pattern.

==========

EXAMPLE 3 Coordinated Exploits

To date the coordinated exploits have neither been large scale nor effectual. The scale at least is certain to change as shown by the recent escalation of reset scans.

Some examples of coordinated exploits are shown to illustrate this technique. In addition to the patterns shown below, we have seen UDP 137 (NBTSTAT) scans with similar signatures.

Example 3A Searching for Back Orifice

This had been seen previously but rarely. In a short time frame three attackers were detected at multiple target locations using the same signature. Two (A and B) are shown here:

```
04:10:34.355832 dax.no.1534 > TARGETBa.31337: udp 19
04:51:15.261462 cpu.com.1534 > TARGETBb.31337: udp 19
04:54:19.101595 dax.no.1534 > TARGETBc.31337: udp 19
06:51:39.392441 dax.no.1534 > TARGETAa.31337: udp 19
06:52:32.700418 cpu.com.1534 > TARGETAb.31337: udp 19
06:06:52.320331 eb.net.1534 > TARGETAc.31337: udp 19
```

Example 3B DNS ZONE

Here we see an interesting pattern occurring within the same day. SourceA connects first, there is no RESET from the DNS server. SourceB then connects from an entirely different IP subnet to the same DNS server and generates a RESET.

```
07:15:17.563185 SourceA.56141 > TARGETA.domain: S 5335035:53 35035(0) ac
07:15:17.565758 SourceB.domain > TARGETA.domain: S 4601818:46 01818(0) a
07:15:17.570577 TARGETA.domain > SourceB.domain: R 4601817:46 01817(0) w
```

```
22:11:13.044850 SourceA.18052 > TARGETB.domain: S 5624156:56241 56(0) ac
22:11:13.479834 SourceB.domain > TARGETB.domain: S 4849093:48490 93(0) a
22:11:13.480759 TARGETB.domain > SourceB.domain: R 4849092:48490 92(0) w
```

==========

EXAMPLE 4 Probes against a firewall

One site with SHADOW Intrusion Detection systems has a very low attack rate. With that in mind, consider the following report which is way out of the norm for this site.

This attack starts out with secure shell and NNTP probes and then packets with odd TCP flags are detected from multiple locations.

```
07:36:55.734342 ad.com.14363 > target.22: S 14974665:14974177(12) win 65
07:37:21.804342 media.com.58521 > target.22: S 2215978:2216514(536) win
07:37:53.634342 media.com.24463 > target.22: S 8514393:8514929(536) win
07:38:00.614342 media.com.28349 > target.119: S 956785:957321(536) win 6
```

Malformed packet, note SYN/RESET/FIN all set as is urgent:

```
10:47:36.614342 media.com.2048 > target.48579: SFR 2842082:2842590(508)
11:23:42.974342 media.com.2048 > target.47720: SFP 4820865:4821409(544)
13:49:44.334342 gm.com.49608 > target.49606: SFP 7051:7607(556) ack 2147
13:49:44.724342 gm.com.22450 > target.1591: SFRP 2038:2074(36) ack 11606
```

Here is some related activity not from original attacking site but is within the same general timeframe:

```
12:18:46.254342 im.com.5500 > target.1137: SFP 3241821:3242365(544) win
13:37:30.334342 im.com.22555 > target.22555: SF 8440982:8441538(556) win

14:52:57.454342 demon.net.30975 > target.16940: SFRP 2029994540:20299950
14:53:01.634342 demon.net.30975 > target.556: SFRP 2029978156:2029978684
```

NOTE: For further information about fun with codebits see: http://www.apostols.org/projectz/queso or nmap.

==========

EXAMPLE 5 Simultaneous DNS scans

Here is an excellent example of the stealth of these type of scans. In this case the goal appears to be to locate DNS servers within various target subnets. We see two sources running identical scans (probably the same tool) from vastly different IP addresses (the IP addresses appear to be on two different continents) but running them against the same target networks at the same time.

```
06:12:33.282195 SourceA.10053 > TargetNetA.34.1.domain: S 992750649:9927
06:34:18.663344 SourceA.10053 > TargetNetA.35.1.domain: S 3455530061:345
06:56:04.045981 SourceA.10053 > TargetNetA.36.1.domain: S 1895963699:189
07:17:49.443476 SourceA.10053 > TargetNetA.37.1.domain: S 2485794595:248
07:39:34.811723 SourceA.10053 > TargetNetA.38.1.domain: S 3785701160:378
08:01:20.227869 SourceA.10053 > TargetNetA.39.1.domain: S 1471781129:147
08:23:05.643730 SourceA.10053 > TargetNetA.40.1.domain: S 4110489384:411
08:44:50.962887 SourceA.10053 > TargetNetA.41.1.domain: S 1486592867:148

06:10:56.527024 SourceA.10053 > TargetNetB.34.1.domain: S 1935318310:193
06:32:42.146384 SourceA.10053 > TargetNetB.35.1.domain: S 552822870:5528
06:54:27.317188 SourceA.10053 > TargetNetB.36.1.domain: S 944974642:9449
07:16:12.731522 SourceA.10053 > TargetNetB.37.1.domain: S 3045099303:304
07:37:58.160387 SourceA.10053 > TargetNetB.38.1.domain: S 323776127:3237
07:59:43.537424 SourceA.10053 > TargetNetB.39.1.domain: S 1212319841:121
08:21:28.992543 SourceA.10053 > TargetNetB.40.1.domain: S 87682610:87682
08:43:14.379838 SourceA.10053 > TargetNetB.41.1.domain: S 1460815479:146

06:21:38.677266 SourceA.10053 > TargetNetC.35.1.domain: S 771480424:7714
06:43:24.079835 SourceA.10053 > TargetNetC.36.1.domain: S 1357786460:135
08:10:25.907162 SourceA.10053 > TargetNetC.40.1.domain: S 292016656:2920
08:32:11.129991 SourceA.10053 > TargetNetC.41.1.domain: S 2826350638:282

06:00:06.556853 SourceB.10053 > TargetNetA.16.1.domain: S 1738779185:173
06:00:11.681430 SourceB.10053 > TargetNetA.17.1.domain: S 2597129298:259
06:00:16.796096 SourceB.10053 > TargetNetA.18.1.domain: S 3216686157:321
06:00:21.918547 SourceB.10053 > TargetNetA.19.1.domain: S 4121612834:412
06:00:27.038290 SourceB.10053 > TargetNetA.20.1.domain: S 1501341045:150
06:00:32.158748 SourceB.10053 > TargetNetA.21.1.domain: S 134807152:1348
06:00:37.291499 SourceB.10053 > TargetNetA.22.1.domain: S 2224429686:222
06:00:42.395105 SourceB.10053 > TargetNetA.23.1.domain: S 1480631621:148
06:00:47.542147 SourceB.10053 > TargetNetA.24.1.domain: S 4111668847:411
06:00:52.634943 SourceB.10053 > TargetNetA.25.1.domain: S 2034911826:203
06:00:57.761173 SourceB.10053 > TargetNetA.26.1.domain: S 2622853216:262
06:01:02.876331 SourceB.10053 > TargetNetA.27.1.domain: S 3504466453:350
06:01:07.992931 SourceB.10053 > TargetNetA.28.1.domain: S 3453873749:345
06:01:13.126171 SourceB.10053 > TargetNetA.29.1.domain: S 3984740181:398
06:01:18.237385 SourceB.10053 > TargetNetA.30.1.domain: S 1101968762:110
06:01:23.354751 SourceB.10053 > TargetNetA.31.1.domain: S 3145478250:314
06:01:28.481710 SourceB.10053 > TargetNetA.32.1.domain: S 3742923526:374
06:01:33.601717 SourceB.10053 > TargetNetA.33.1.domain: S 685017136:6850
06:01:38.711348 SourceB.10053 > TargetNetA.34.1.domain: S 357520157:3575
06:01:43.831041 SourceB.10053 > TargetNetA.35.1.domain: S 3114347597:311
06:01:48.950822 SourceB.10053 > TargetNetA.36.1.domain: S 3989749054:398
06:01:54.071207 SourceB.10053 > TargetNetA.37.1.domain: S 104626974:1046
06:01:59.190766 SourceB.10053 > TargetNetA.38.1.domain: S 3121137008:312
```

```
06:49:55.793053 SourceB.10053 > TargetNetB.0.1.domain: S 3172885021:3172
06:50:00.433858 SourceB.10053 > TargetNetB.1.1.domain: S 4008039718:4008
06:50:05.578539 SourceB.10053 > TargetNetB.2.1.domain: S 3133502723:3133

06:06:19.492397 SourceB.10053 > TargetNetC.158.1.domain: S 3057098328:30
06:15:35.877587 SourceB.10053 > TargetNetC.160.1.domain: S 3057098328:30
06:24:56.256924 SourceB.10053 > TargetNetC.162.1.domain: S 3057098328:30
06:34:20.474591 SourceB.10053 > TargetNetC.164.1.domain: S 3057098328:30
06:39:00.552359 SourceB.10053 > TargetNetC.165.1.domain: S 3057098328:30
```

NOTE: This particular scan continued for two or three days at a very low hourly rate (except for the unusually high rate SourceB used against TargetNetA early on, although this could have been an attempt to mask SourceA's scan, or just a misconfiguration). Only a fraction of the data is shown here to give a feel for the type of coordinated signature we are detecting. Both SourceA and SourceB started the scans within minutes of each other, and ended their scans within hours of each other.

==========

CONCLUSION:

The examples shown above represent a change in the kinds of attacks and probes we track. Previously it has been common for a single attacker to target multiple sites. Now we see indications of multiple attackers working together to target either single sites or multiple sites. We assert that these techniques are starting to be widely used and that the attacker community is likely to continue using these new techniques for the forseeable future. It is imperative that intrusion detection tools, techniques, and tracking databases be developed or modified to detect and respond to this new threat.

[1] Irwin
[2] Vazquez