

DNS-based Detection of Scanning Worms in an Enterprise Network

By David Whyte, Evangelos Kranakis, P.C. van Oorschot

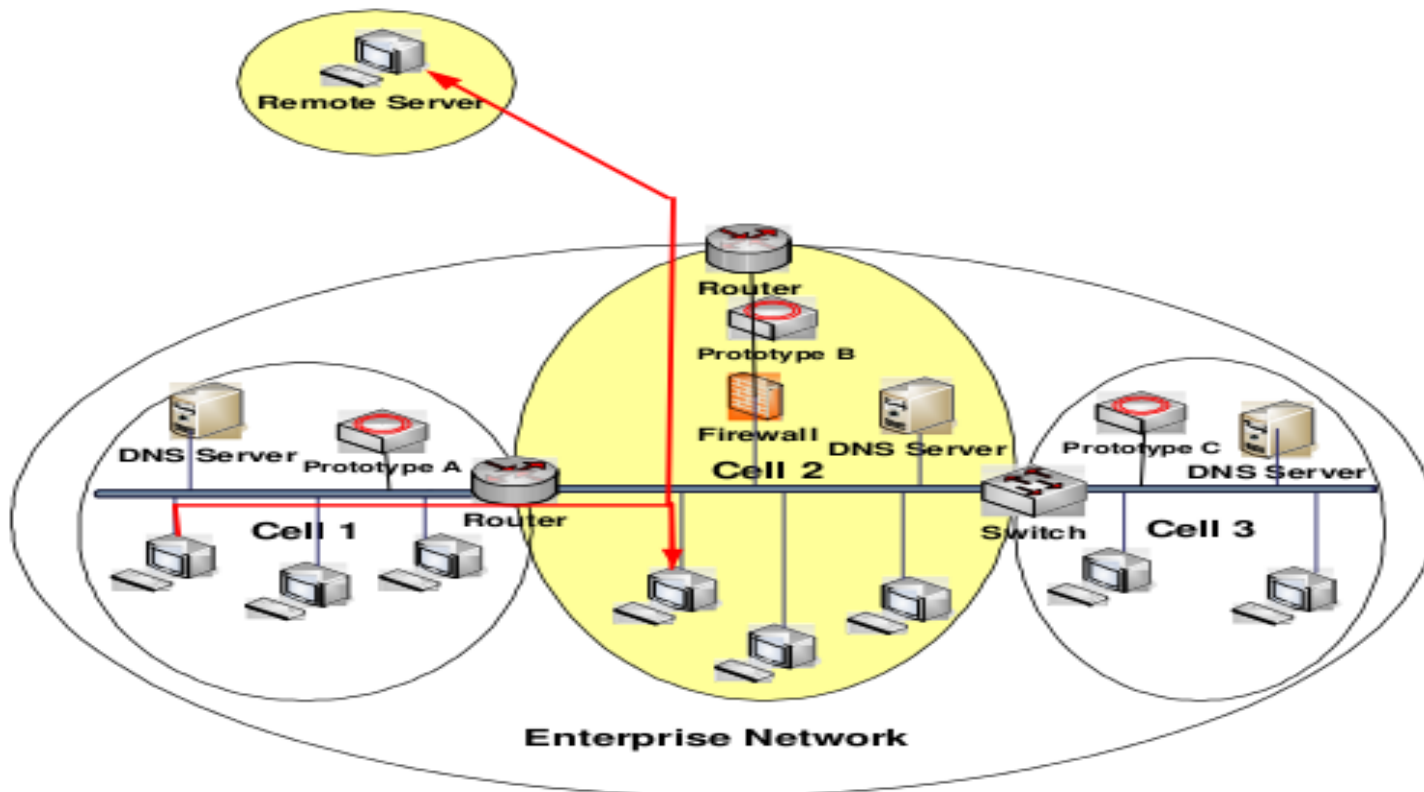
By
Albert Kim

Basic Idea

- Behavior of worm:
 - Pick a random IP address
- Most connections today:
 - Name servers
- No DNS request = worm!

Detecting DNS Requests

- Divide network into cells (subnets)
- Types of connections: L2L, L2R, R2L, intra-cel



Whitelist

- HTTP
- P2P
- Remote administration

Architecture

- Packet Processing Engine (PPE):
 - New connections (TCP, UDP)
 - HTTP
 - DNS
- DNS Correlation Engine (DCE):
 - Validation

Evaluation

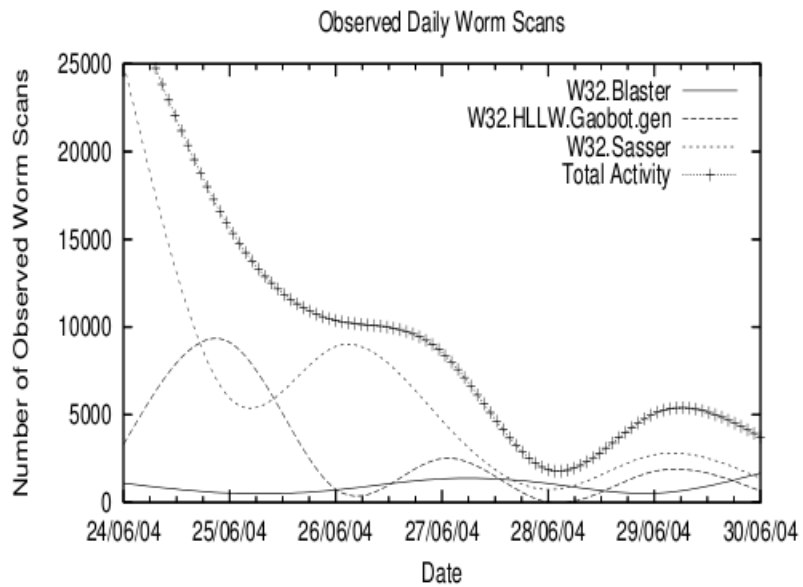


Figure 4. IDN Worm Activity

Table 3. IDN Worm Activity

| Alerts | | | |
|------------|--------|---------|--------|
| Date | Sasser | Blaster | Gaobot |
| 06-24-2004 | 25,052 | 1,104 | 3,299 |
| 06-25-2004 | 5,946 | 539 | 9,137 |
| 06-26-2004 | 8,894 | 721 | 761 |
| 06-27-2004 | 4,680 | 1,353 | 2,516 |
| 06-28-2004 | 739 | 1,085 | 21 |
| 06-29-2004 | 2,731 | 532 | 1,778 |
| 06-30-2004 | 1,383 | 1,680 | 659 |
| Total | 49,425 | 7,014 | 18,171 |

| Infected Hosts | | | |
|----------------|--------|---------|--------|
| Worm | Sasser | Blaster | Gaobot |
| Total | 101 | 38 | 56 |

False Positives

- Authorized Network Connections
- Config Errors
- Scanning
- True FP

Table 4. Additional IDN Alerts

| Alerts | Activity |
|-------------------|--|
| 125 | Optix Pro Trojan Horse scanning: port 3410 TCP |
| 5 | Random scanning: port 60510-60518 TCP |
| 12 | Ident/auth service: 113 TCP |
| 49 | Common Unix Printing System (CUPS): 631 TCP |
| Total Alerts: 191 | |

Table 5. Lab Alerts

| Date | # of Alerts | Known False Positives | True False Positives |
|------------|-------------|-----------------------------------|----------------------|
| 06-24-2004 | 18 | 6 Internal Lab, 3 Streaming Audio | 9 HTTP |
| 06-25-2004 | 20 | 4 Streaming Audio | 16 HTTP |
| 06-26-2004 | 1 | | 1 HTTP |
| 06-27-2004 | 6 | | 6 HTTP |
| 06-28-2004 | 1 | | 1 HTTP |
| 06-29-2004 | 4 | 2 Port 90 TCP | 2 HTTP |
| 06-30-2004 | 2 | 1 Port 90 TCP | 1 HTTP |
| Total | 52 | 16 | 36 |

False Negatives

$$\beta = r \frac{N}{2^{32}}.$$

Table 7. Probability of False Negatives due to Remote DNS Monitoring

| DNS Records | 10 Infected Systems | 100 Infected Systems | 200 Infected Systems | 500 Infected Systems |
|-------------|-------------------------|------------------------|-------------------------|------------------------|
| 500 | 1.1641×10^{-6} | 5.821×10^{-6} | 1.1641×10^{-5} | 2.328×10^{-5} |
| 1000 | 2.328×10^{-6} | 1.164×10^{-5} | 2.328×10^{-5} | 4.656×10^{-5} |
| 2000 | 4.656×10^{-6} | 2.328×10^{-5} | 4.657×10^{-5} | 9.313×10^{-5} |
| 5000 | 1.1641×10^{-5} | 5.821×10^{-5} | 1.1641×10^{-4} | 2.328×10^{-4} |
| 10000 | 2.328×10^{-5} | 1.164×10^{-4} | 2.328×10^{-4} | 4.656×10^{-4} |

Circumvention and Limitations

- Require worm writers to perform DNS requests
- R2L
- Open network
- Covert channels
- Mail

References

- *DNS-based Detection of Scanning Worms in a Enterprise Network* by David Whyte, Evangelos Kranakis, P.C. van Oorschot