Unusual File Modification by dns.exe

Identifies an unexpected file being modified by dns.exe, the process responsible for Windows DNS Server services, which may indicate activity related to remote code execution or other forms of exploitation.

Rule type: eql

Rule indices:

- winlogbeat-*
- logs-endpoint.events.file-*
- logs-windows.sysmon_operational-*
- endgame-*

Severity: high

Risk score: 73

Runs every: 5m

Searches indices from: now-9m (Date Math format, see also `Additional look-back time`)

Maximum alerts per execution: 100

References:

- https://research.checkpoint.com/2020/resolving-your-way-into-domain-admin-exploiting-a-17-year-old-bug-in-windows-dns-servers/
- https://msrc-blog.microsoft.com/2020/07/14/july-2020-security-update-cve-2020-1350-vulnerability-in-windows-domain-name-system-dns-server/
- https://www.elastic.co/security-labs/detection-rules-for-sigred-vulnerability

Tags:

- Domain: Endpoint
- OS: Windows
- Use Case: Threat Detection
- Tactic: Lateral Movement
- Data Source: Elastic Endgame
- Use Case: Vulnerability
- Data Source: Elastic Defend
- Data Source: Sysmon

Version: 211

Rule authors:

Detection alerts from this rule indicate potential unusual/abnormal file writes from the DNS Server service process (`dns.exe`) after exploitation from CVE-2020-1350 (SigRed) has occurred. Here are some possible avenues of investigation: - Post-exploitation, adversaries may write additional files or payloads to the system as additional discovery/exploitation/persistence mechanisms. - Any suspicious or abnormal files written from `dns.exe` should be reviewed and investigated with care.

Rule query

edit

```
file where host.os.type == "windows" and process.name : "dns.ex
  not file.name : "dns.log" and not
  (file.extension : ("old", "temp", "bak", "dns", "arpa") and f

  /* DNS logs with custom names, header converts to "DNS Server
  not ?file.Ext.header_bytes : "444e5320536572766572206c6f67*"
```

Framework: MITRE ATT&CK™

- Tactic:
  - Name: Lateral Movement
  - ID: TA0008
  - Reference URL: https://attack.mitre.org/tactics/TA0008/
- Technique:
  - Name: Exploitation of Remote Services
  - ID: T1210
  - Reference URL: https://attack.mitre.org/techniques/T1210/

« Unusual File Creation - Alternate Data Stream

Unusual High Confidence Misconduct Blocks Detected »

Notice

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the cookie policy.
Use the “Accept” button to consent. Use the “Reject” button to continue without accepting.

Follow us

Blog

Newsroom

Join us

Careers

Career portal

Investor relations

Investor resources

Governance

Financials

Stock

EXCELLENCE AWARDS

Previous winners

ElasticON Tour

Become a sponsor

All events

Become a partner

Trust & Security

Trust center

EthicsPoint portal

ECCN report

Ethics email

Trademarks Terms of Use Privacy Sitemap