Protective DNS in Action

The National Cyber Security Centre's (NCSC) Active Cyber Defence (ACD) programme aims to 'Protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber attacks the majority of the time.' Its third year report (covering the 2019 calendar year) provides transparency into these efforts and evidences of their effectiveness.

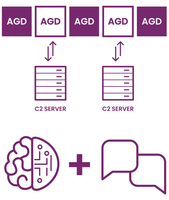
A part of the ACD programme is Protective DNS (PDNS), which is delivered by Nominet on behalf of the NCSC. PDNS prevents users from accessing domains or IPs that are known to contain malicious content and stops malware already on a network from calling home.

PDNS
Protective DNS

ACTIVE CYBER DEFENCE - THE THIRD YEAR

2019 saw significant progress behind the scenes in how the NCSC share and use PDNS data internally, meaning that this data can be exploited in new ways to make observations at scale to provide enhanced security across the public sector.

Machine learning AGD detection



SITUATION:

Role of Algorithmically Generated Domains (AGDs) in malware distribution

AGDs are used as rendezvous points with their C2 servers. Not all AGD domains will connect to the servers, but the high volume presents a challenge for identification and removal.

RESPONSE:

PDNS data analysed with new techniques

a) Machine learning

b) Natural language processing techniques

OUTCOME:

Threat mitigation

- Word-based AGD exposed novel malware strains
- New types of AGDs were accurately identified, ready for removal

Incident response

SITUATION:

Security incident occurs

Examples - Citrix & Cisco vulnerabilities

RESPONSE:

Historical PDNS data analysis by NCSC

a) Research technical indicators of compromise

b) Find fingerprints in PDNS organisation data

c) Monitor incident to track remediation

d) Evaluate different mitigations effectiveness

OUTCOME:

Intelligence gained

- Extent of incident known
- Full ACD data analysis complete
- Incident management, cyber operations and engagement teams prepped for response

Phishing campaigns

SITUATION:

Unusual spikes in domain query traffic

NCSC identified spikes in queries for subdomains of a foreign internet service provider (ISP) originating from various PDNS customers.

RESPONSE:

Analysis of domains through PDNS

a) Scrutinise naming convention of domains to identify purpose

b) Identify if any domain names were associated with spam campaigns

c) Investigate where the spam campaigns are originating from

OUTCOME:

Remediation triggered

- Situation communicated to affected parties to enact remediation

Infected virtual machines

SITUATION:

Spike in queries for domain names known to be associated with malware

Low number of unique domains blocked proved that domain names were all related to same malware family.

RESPONSE:

Investigation into blocked queries

a) Provide PDNS logs of blocked queries

b) Identify device behind the attempted malicious connections

c) Analyse potential for infected virtual machine (VM)

OUTCOME:

Threat mitigated & resilience increased

- Infected VM deleted, eliminating connected spam campaign
- Other VMs investigated for evidence of malware
- Increased monitoring and further security provisions put in place

"PDNS is maturing, and as our active users grow, our visibility across the public sector is allowing us to make observations, provide more meaningful metrics and feedback, and identify the areas most needing attention."

Active Cyber Defence
The Third Year | NCSC

"The sheer extent of queries and responses demonstrates that PDNS is a genuine force multiplier in cyber defence and the data produced has proved instrumental in identifying and quickly remediating incidents. Once aware of an incident affecting a particular type of infrastructure of service, PDNS data informs analysis to identify affected organisations and to begin the next steps of remediation.

Suffice to say, Active Cyber Defence is pioneering and we look forward to playing our part as it treads new ground in years to come."

David Carroll
Managing Director | Nominet Cyber

National Cyber Security Centre | NOMINET