GLOBAL IMPACT REPORT

NOMINET CYBER

PUBLISHED JULY 2022

Foreword

DAVID CARROLL
MD NOMINET CYBER

Building resilience: how to protect an entire nation?

Cyber insecurity is not new, and for more than a decade most industrialised nations have been responding to its challenges via well-funded national strategies, delivered by newly established agencies working in partnership with regulators, law enforcement, industry, and citizens. Despite good progress, economic losses are mounting: supply chain attacks have compromised entire nations, and ransomware now poses a significant threat to national security, potentially threatening lives as well as economies.

The policy maker's challenge is multi-faceted. Cyber criminals operate from remote safe havens, often with tacit support from their host nations. Their crime-as-a-service business model holds broad appeal and is enabled by new technologies and widespread vulnerability. We are potentially approaching a tipping point whereby centralised cybersecurity regulation may be deemed preferable to the vertically integrated approach in existence today. Such a move would be controversial, as would banning ransom payments. Both measures have the potential for unintended consequences and more research is required, as is public debate.

"The pandemic has shown us that cybersecurity is now viewed as a public good, a bit like environmental protection... not just a domain of military operations, but also an environment of human activity."

CIARAN MARTIN
FORMER CEO, NCSC

NOMINET CYBER

In the meantime, diplomatic pressure to establish cyber norms will help, as will making it harder for criminals to move money, as was done to disrupt terrorist networks post 9/11. Wherever possible, disrupting the digital infrastructures of cyber criminals also offers grounds for hope. However, these options are all difficult to implement, and require a balanced, globally co-ordinated approach.

One immediate step that most people can agree on, is the requirement to build national resilience. Bold collaborative measures to reduce harm at scale, should be at the heart of any nation's cyber defences. In capitalist societies we tend to allow free markets to address new challenges; but, even with increased regulation, the market alone is unlikely to take care of the problem of cyber insecurity. It is unreasonable and inefficient to expect operators of critical national infrastructure and providers of essential public services to collectively address national security risk. Hospitals should be focused on keeping people alive and healthy, not combatting international ransomware gangs.

This report illustrates the capabilities of Nominet's delivery of Protective DNS solutions for the National Cyber Security Centre (NCSC) and Australian Cyber Security Centre (ACSC). These deliveries operate at national scale, protecting millions of users across public sectors, in thousands of organisations across the world. The purpose of our work echoes the aims of the UK NCSC's Active Cyber Defence programme: "to protect the majority of people from the majority of the harm caused by the majority of the cyber-attacks the majority of the time."

SUMMARY

- *Cyber security came a long way in 2021; we helped to protect the UK's health service during a pandemic and the economy from a sophisticated supply chain attack when SolarWinds was compromised*
- *Whilst 2021 was a record year for cyber threats encountered and defended against, 2022 is on course to surpass, with economic losses mounting*
- *Now, cyber defences are heightened more than ever as warfare takes between sovereign nations, whilst governments and industry must continue to collaborate, it has never been more pertinent for allied nations to work together to meet the threat head-on*

NOMINET CYBER

Introduction

DNS is often referred to as the address book of the internet. The Recursive DNS servers ask the question 'What is the IP address for www.example.com?' and the Authoritative DNS servers hold the answer.

DNS can be used to distribute and operate malware, phishing attacks and botnet control by resolving the address of malicious content or as an exfiltration channel.

Nominet Cyber's Protective DNS has a recursive resolver at its heart, built to answer DNS queries. Critically, it does not resolve the query – connect the user to the IP address – if the domain is known to be malicious.

Nominet Cyber delivers Protective DNS services to the UK Government on behalf of the National Cyber Security Centre (NCSC). It also delivers services to the Australian Government, on behalf of the Australian Cyber Security Centre (ACSC).

NOMINET CYBER

Capable of millions of blocks that may have otherwise damaged an essential part of the country's infrastructure and services

Case in point: Protection of Australia's digital census

Nominet has worked closely with the Australian government since 2019. First delivering the AUPDNS pilot and more recently launching the full service.

The AUPDNS capability seeks to prevent access to domains identified as malicious by blocking access to sites that host malware, ransomware, phishing attacks and other malicious content. The capability also provides situational awareness on system vulnerabilities within Commonwealth entities.

"The AUPDNS has already analysed over 10 billion queries and blocked over 1 million connections to malicious domains, and this technology formed part of the defensive suite that helped to protect this year's digital census."

"Throughout the census, AUPDNS processed around 200 million queries a day and blocked more than 10,000 connections to known malicious domains, any one of which could have resulted in a phishing or ransomware attack."

Taken from ACSC launches new cyber guard for government data

NOMINET CYBER

Gives Government Cyber response information to react with incident response

Case in point: PDNS dataset as primary source of analysis and response in SolarWinds

Nominet proudly delivers Protective DNS (PDNS) on behalf of the National Cyber Security Centre (NCSC) to protect the UK public sector.

It has been mandated for use by central government services and is available to all public sector organisations in the UK.

The delivery of Protective DNS forms a vital part of the UK's Active Cyber Defence (ACD) programme, designed to tackle cyber attacks to improve national resilience.

In 2020 a malicious, unauthorised modification to SolarWinds Orion was identified. It compromised SolarWinds, which is in the supply chain of many other organisations. The impact of the attack was felt globally.

"PDNS's broad view of DNS activity across the UK public sector enabled NCSC analysts to rapidly measure how many public bodies were affected. As details of the incident became clearer, historic PDNS data revealed the extent of compromise in each affected organisation. This information helped the NCSC prioritise its support to organisations with the more concerning indicators of malicious activity and, just as importantly, to provide assurance to many core parts of government that were not affected."

Taken from NCSC's Active Cyber Defence – The Fourth Year report

NOMINET CYBER

Provides protection from financial losses

Case in point: Independent research commissioned to quantify the value of protection offered by Protective DNS

Commissioned by Nominet, Cyentia's report provides an analysis of the DNS queries blocked by Protective DNS, finds commonalities among the end users that are protected, and uses a financial model to estimate the value of the threat prevention provided by Protective DNS to the UK economy.

In 2020, Protective DNS successfully resolved 237 billion queries, blocking nearly 105 million queries for 160,000 distinct domains suspected to be malicious.

The report found that:

PREVENTS LOSSES OF
£48M – £223M

Threats and attacks vary, but almost always (9 out of 10 years) Protective DNS prevents losses of £48m – £223m

SAFEGUARDS AGAINST A
LOSS OF OVER £223M

For rarer, but potentially catastrophic major events, Protective DNS safeguards the UK public sector against a 1-in-20 year loss of over £223m

Taken from 'Quantifying the financial savings Protective DNS (PDNS) brings to the UK public sector' report

NOMINET CYBER

Helps Governments to have visibility of the security posture of their entire public sector

Case in point: Research and analysis with PDNS data

PDNS dataset is a rich source of public sector domain names and IP addresses. Governments can combine this information with other data, such as commercial and open-source data.

"PDNS data is a rich source of information for the NCSC's cyber security research projects. In 2019, the NCSC's data scientists developed a network model of government organisations using this data. The work involved identifying pairs of public bodies that request each other's domain names frequently. This simple metric is a powerful way to build up a picture of the working relationships between public bodies."

"This research helps the NCSC spot new government digital estate as soon as it starts to be used, and gives us a better understanding of how public bodies interact in cyberspace. This helps us provide cyber security support to the organisations and infrastructure that will have the greatest effect on the overall cyber resilience of government."

Taken from the NCSC's Active Cyber Defence – The Third Year report

NOMINET CYBER

Dedicated team behind the scenes proactively analysing data

Case in point: Analysis of Newly Observed Domain (NODs) detection

Whilst Protective DNS solutions are built to identify, act, and inform on a diverse range of threats, further value can be derived through human analysis of the outputted data.

The Nominet research team analysed NODs seen in PDNS with the aim of defining procedures, methods and algorithms that could lead to automatic malicious NOD detection.

"Using a combination of PDNS data, security feed data, WHOIS data, zone file crawling, certificate transparency logs and reverse DNS lookup data, the team created several heuristic models and assessed their performance over a period of one month. All models were built with the human-in-the-loop approach."

"At the end of the first month, 79.8% of domains analysed by a human after filtering algorithms were applied were found to be malicious (and subsequently blocked)."

"The above work confirmed the benefits of human-in-the-loop heuristic models for augmenting human analysis."

Taken from the NCSC's Active Cyber Defence – The Fifth Year report

NOMINET CYBER

NOMINET

PUBLIC BENEFIT COMPANY

CONNECTED | INCLUSIVE | SECURE

Operating in the public interest underpins all our activities

TRUSTED .UK REGISTRY

Relied on by millions of businesses

Resolving disputes and tackling online crime

CRITICAL NATIONAL INFRASTRUCTURE OPERATOR

Safe, secure, resilient infrastructure

Underpins .UK Registry and Government services

PROTECTING PUBLIC SERVICES

Securing public services

Millions of end users protected across healthcare organisations, local and central government