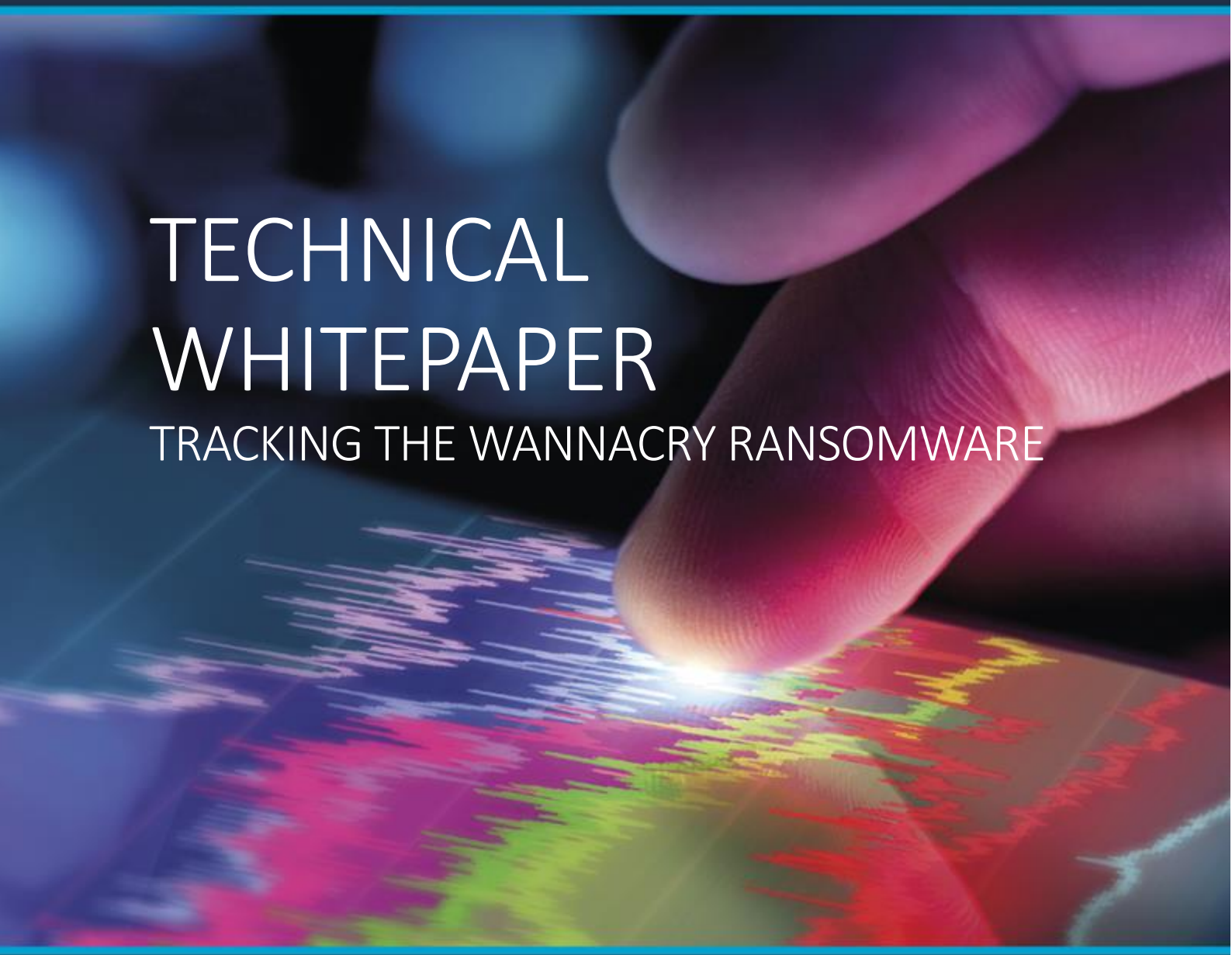


TECHNICAL WHITEPAPER

TRACKING THE WANNACRY RANSOMWARE

NOMINET

Commercial statement – copyright

Contact us

Contact us to arrange a 30-day free trial of our DNS Cyber Security Services

turing.net

turing@nominet.uk

UK: +44 (0) 1865 332255

USA: +1 267.908.3004

Customer service office hours are 8:00am to 6:00pm (GMT), Monday to Friday.

EXECUTIVE SUMMARY

On May 12th 2017, the WannaCry ransomware story broke across the globe, the malware exploiting a known vulnerability in Microsoft Windows: Server Message Block (SMB). By scanning networks for computers that had not yet patched this vulnerability, the ransomware spread rapidly, with infections recorded across 150 countries globally. Organizations hit by the ransomware included:

- National Health Service (NHS)
- Telefonica
- Renault
- Deutsche Bahn

Microsoft had patched this flaw on March 14th 2017 meaning that there was a period of almost two months when System Administrators could have protected themselves from this threat. If there is one big take away from this story, it is the importance of a regular patching cycle when running IT infrastructure.

Nominet monitors DNS infrastructures globally on behalf of clients through our DNS Threat Intelligence platform, *turing*. We can filter billions of DNS packets to identify DNS queries, WannaCry issues and assist network operators in remediation.

INTRODUCTION

turing allows us to filter billions of DNS queries down to key packets that match a given signature. This is an incredibly powerful capability analysts can leverage when hunting malware.

DNS queries are a great place to hunt for malware infections. We know (thanks to well documented security research) that early versions of the WannaCry ransomware make queries for two non-existent domains.

1. www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
2. www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

See the following for more details:
https://www.ncsc.gov.uk/guidance/ransomware-wannacry-guidance-enterprise-administrators-1

When WannaCry receives a response that indicates that these domains have been registered (in DNS terms, a non-NX response), it shuts down. This is what is known as a kill switch.

This behavior is significant as the kill switch mechanism can effectively disarm WannaCry. It is a logical deduction to theorize that this mechanism was added to protect WannaCry from antivirus researchers but this feature appears to have backfired. This mechanism is one that other malware families have used to avoid being run in a “sandbox” environment that antivirus researchers use to observe their operation. By hindering this analysis, the malware author hopes to extend the period of time before effective countermeasures can be created and rolled out to customers.

Antivirus researchers often run malware samples in restricted environments that simulate internet connections. Of course, all network traffic from these environments, including any DNS lookups, is logged. The creators of this malware may not have thought that anyone would register these domains. This assumption was incorrect because a researcher did exactly that:
https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

By leveraging this knowledge, we can monitor for potential infections and make timely interventions when required.

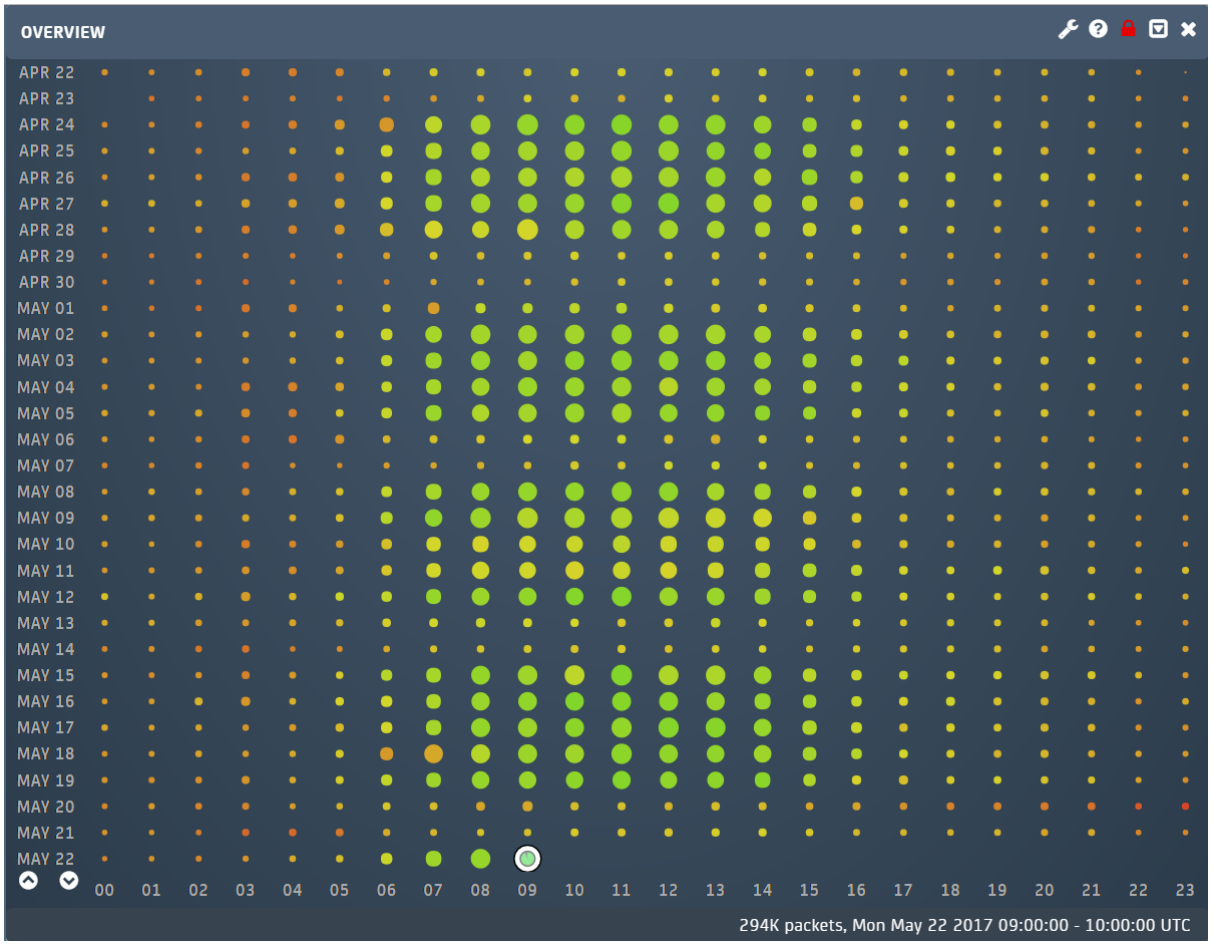
ALL QUIET ON THE RANGE?

At the time the WannaCry story broke, Nominet began monitoring for WannaCry on behalf of customers.

Here we see a month's data which represents billions of DNS queries made across national, distributed corporate infrastructure. There is a mixture of human and machine generated traffic as well as corporate and consumer-related queries.

Unless you have a large IT team and, more importantly, time and specialist expertise, it can be difficult to make sense of all this data. This is where *turing* comes in.

Each dot represents an hour's traffic. The color of the dot represents the health of the traffic in each hour, calculated by response code, i.e. was the answer to the question asked good or bad. The size of each dot is proportional to the volume of DNS requests seen.

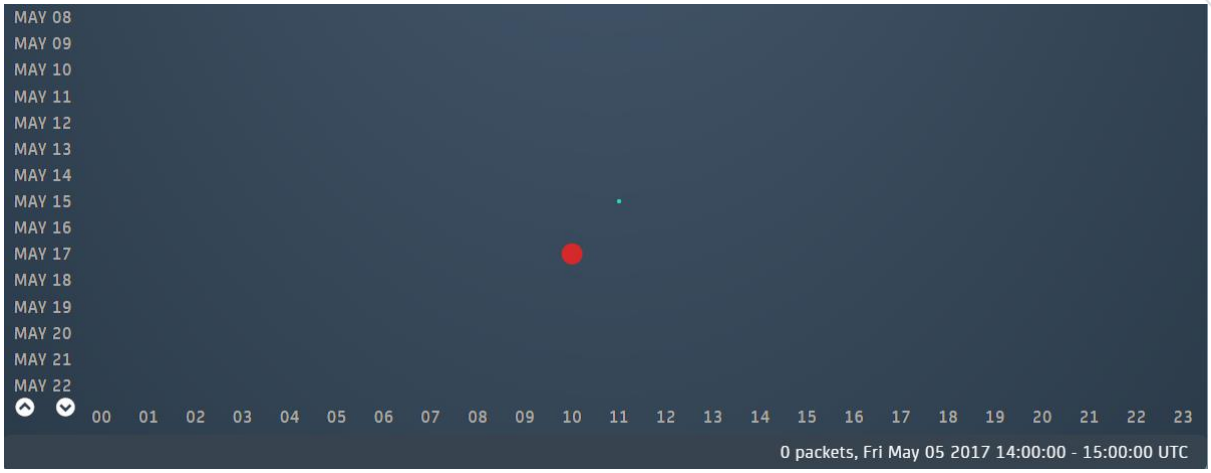


Monitoring for requests for a given domain name in *turing* is easy. *turing* supports a lot of different filters which allows Nominet Analysts to quickly filter for the queries we're looking for, in this case any queries for the following two domains.

1. www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
2. www[.]ifferfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com

BINGO

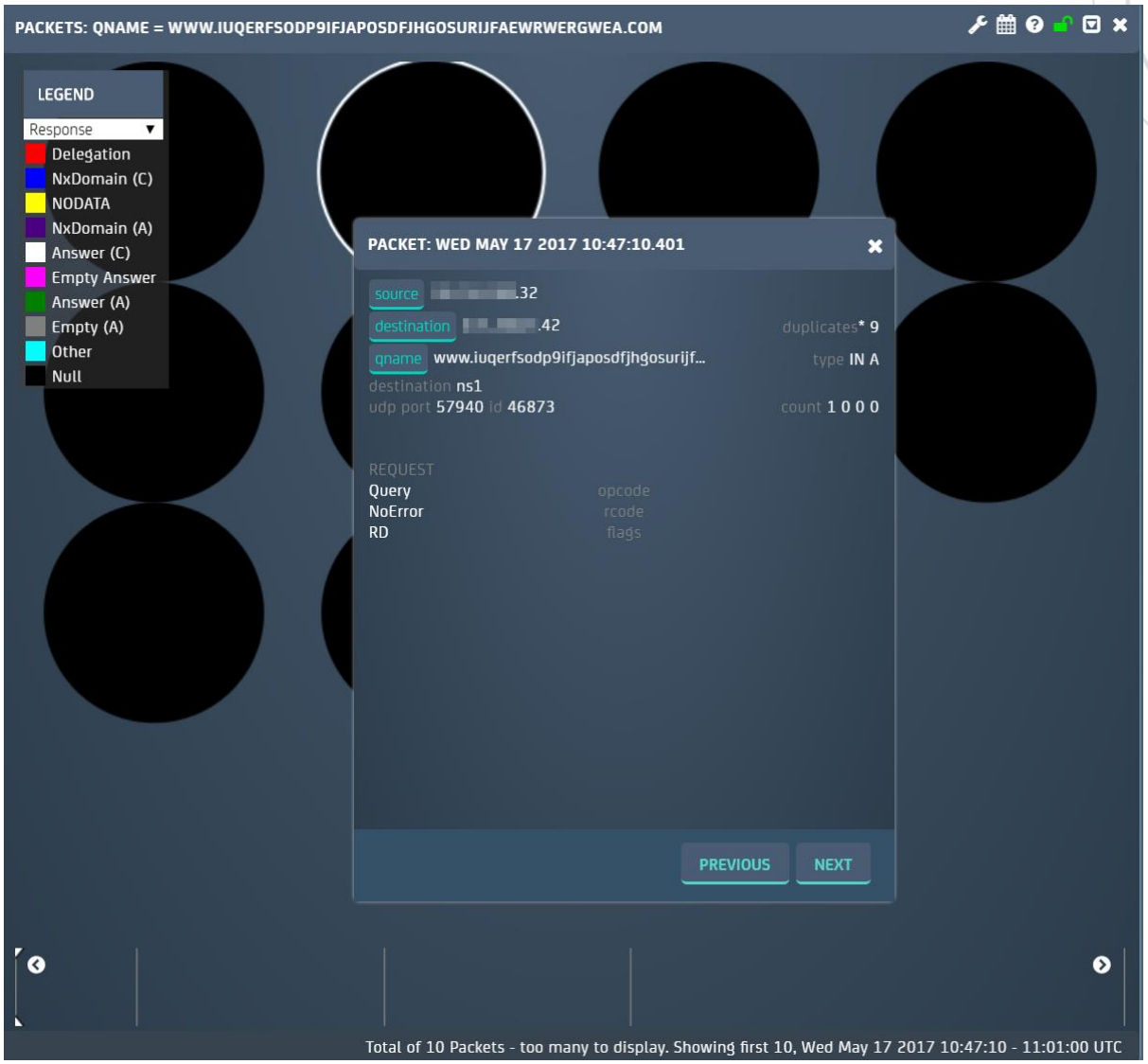
When we filter down the data we can see that there were a couple of hits.



The first small blue dot on May 15th at 11:00am is interesting; although despite initial appearances, this was not a WannaCry infection. Certain browsers like Chrome automatically issue queries for anything on a web page that looks like a domain name every time a new page is displayed. The rationale here is that having already looked up the next potential page via DNS, the user does not have to wait for this step when they click on a link; it is known as “pre-caching”.

This shaves a few milliseconds off the time it takes to fetch the next web page but is worth doing so when performance is your underlying goal, performance in Chrome is something Google takes very seriously.

The next, red dot on May 17th at 10:00am could not be explained so easily. When we looked at the packets issued by the machine making the query, we quickly concluded that this was a genuine infection.

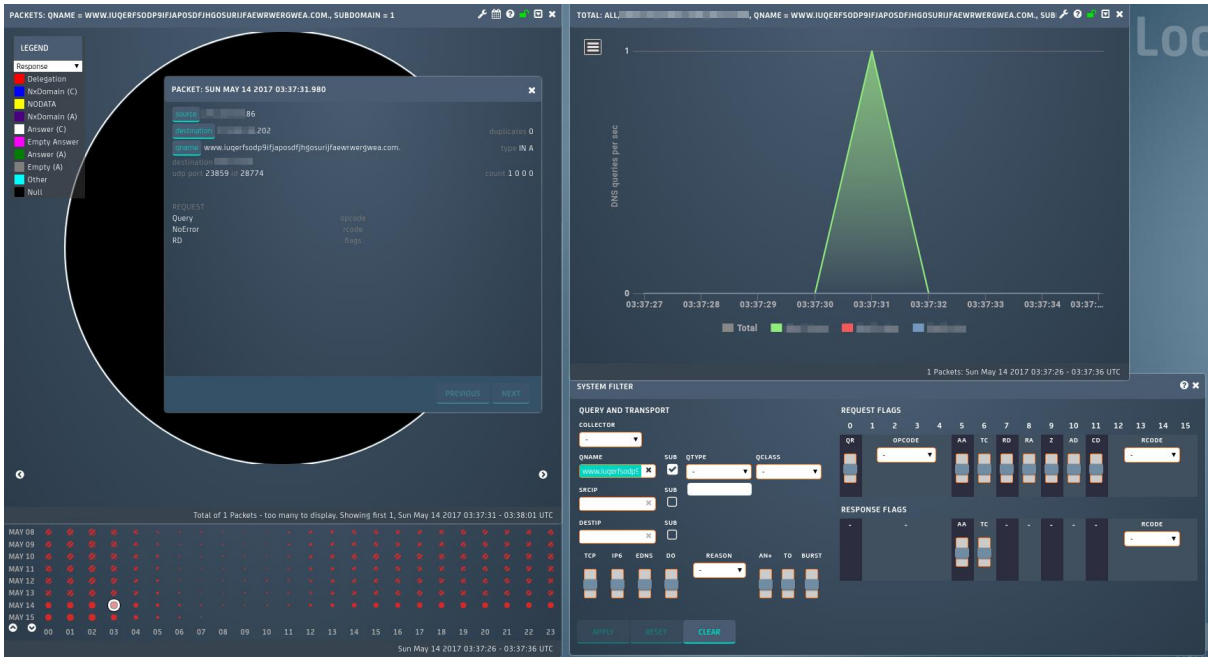


Luckily, because we had the source IP of the infection, we could quickly identify the source of these queries which we escalated to our customer.

THE THREAT EVOLVES

The cyber security landscape is constantly evolving, clearly demonstrated by what happened in the aftermath of the discovery of the WannaCry kill switch. As soon as this news hit the internet, we began to see new variants of the malware appearing. Some would only operate if the kill switch domains were registered and some would operate if they weren't: a difficult scenario for virus researchers and potential victims alike.

Using *turing* we continued to visualize infections to help our clients identify and remediate potential infections. *turing* is deployed on networks globally, here is a good example of the WannaCry ransomware impacting a network in South America.



CONCLUSION

The one lesson we can all take away from WannaCry is the importance of a regular patching cycle when running any kind of infrastructure. This is especially important when you are running legacy technologies such as Windows XP. This simple step neutralizes attack surfaces and can quickly close off attack vectors.

As the world becomes more connected, and these sorts of attacks are a fact of life. Back up your data and upgrade your operating system. A simple step, but critically important.

turing allows you to quickly delete and mitigate this type of attack on large distributed infrastructures. Nominet offers a range of DNS cyber security services which blend the capabilities of turing with in-house expertise to harden customer networks.

ABOUT NOMINET

We protect, promote and support the online presence of more than 10 million domain names and handle around 3 billion DNS requests each day.

With over 20 years' experience in running one of the busiest and most successful internet registries in the world, Nominet remains a leading authority on DNS analytics and cyber intelligence.

Nominet is one of the leading authorities on DNS. We work closely with Internet Corporation of Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF) and law enforcement.