# WANNACRY TWO YEARS LATER:
## HOW DID WE GET THE DATA?

# WANNACRY TWO YEARS LATER:

## How Did We Get the Data?

**DNS Cache Probing WannaCry's Kill Switch Domain**

The DNS cache probing technique was first introduced in a 2004 paper titled "Snooping the Cache for Fun and Profit." The technique is used to identify domain names in use by users of a specific ISP by identifying poorly configured DNS servers and probing their domain cache.

By sending specific queries to these DNS servers, it is possible to ascertain if a specific domain name was previously queried by one (or more) of the ISP's clients. This results in that domain becoming registered on the DNS server's domain cache for a limited amount of time, depending on the TTL of the domain.

In a recent study, the Citizen Lab group used this technique to identify ISPs in which NSO's Pegasus spyware was in use. For.our research, we adapted this technique to track ISPs that have WannaCry's main kill switch domains in their DNS servers' cache.

The technical implementation details of this technique were largely detailed in previous works, but these are the steps we conducted:

1. We set up four servers, in different parts of the world and conducted a full IPv4 scan to create a current database of all the DNS servers worldwide. This resulted in approximately 5 million DNS servers.

2. From this initial list, we needed to identify the servers which supported cache snooping, but in a trustworthy way which would enable us to query their cache for the kill switch domain, and verify whether it is present in the cache.

   This left us with about 10,000 DNS servers spanning across more than 120 countries. This subset of all DNS servers worldwide is a sufficient sample to determine the locations around the world where WannaCry is still attempting to contact its kill switch domain.

   Also, since the kill switch domain has a TTL of 300 seconds, by querying these servers every few minutes we can identify each time the domain is re-entered into the cache of a specific DNS server. Every time this occurs, we can determine that a DNS query to the kill-switch domain was sent. This is an under-estimate of that rate, since the domain may be queried while the domain is already in the cache, without a measurable effect.

3. Probing the list of 10,000 DNS servers that were found prone to probing, from four different servers, every few minutes, during the course of one week, allowed us to identify 2,648 DNS servers owned by 423 distinct ASNs from 61 countries that had the WannaCry killswitch domain in their cache. The ISPs holding these DNS servers account for 22% of the entire IPv4 address space.

4. In total, we observed approximately 600,000 DNS queries to the WannaCry kill switch domain over one week. That translates to about 3,500 queries per hour. This means that by taking into account only 22% of all ISPs, we can determine that WannaCry attacks are performed almost **once a second**, around the world. It is safe to assume that the number of attacks unobservable through DNS Cache probing are at least 3-4 times that rate.

### A WannaCry honeypot

To better determine the number of affected devices - both by the original WannaCry ransomware and by the WannaCry variants that have popped up since we set up a WannaCry honeypot. We used the Dionaea honeypot which is simply an Internet server that simulates a vulnerable Windows device with an SMB port (445) open to the Internet. We've set up five of these servers; two in Europe, two in North America, and one in Asia.

Over the course of almost a week, we observed more than 1,500 **successful** attacks on these five honeypots from unique IP addresses using almost 1,000 unique hashes representing different variants of the WannaCry ransomware. In summary, we observed an average of 2.56 attacks per hour.

WannaCry has a built-in propagation mechanism that tries to attack devices using the EternalBlue vulnerability in SMB. It creates one thread that scans hosts on the local subnet and additional 32 (*actually 128 but 96 of those are unusable due to what seems like an internal bug*) threads that scan the Internet for vulnerable hosts. Each of the Internet-scanning threads will chose a **random** IPv4 address and attempt to connect to it over SMB and spread the attack.

On average, each attempt, whether successful or not, takes approximately 1.5 seconds. And since the attacked IP address is chosen randomly, we can track the rate of attacks on our Internet-exposed honeypots, and estimate the number of affected devices around the world.

Two years ago, a similar honeypot infrastructure peaked at 3,500 attacks **a day**. At that time, it was estimated that about 240,000 devices were where compromised by WannaCry. Using the same technique with a few modifications (counting only the infections that dropped a payload) we found the current tally of infections is around 145,000 devices affected worldwide.

To calculate the number of infected devices, we investigated the original WannaCry variant. We found out that only 32 threads are actually used for random IP generation. To find the number of infected devices we used these calculations:

$$N_{average\ infection/hour} = N_{infected\ devices}\ x\ P_{hitting\ honeypot/hour}$$

$$P_{hitting\ honeypot/hour} = 1\ -\ P_{not\ hitting\ honeypot\ ip/hour}$$

$$P_{not\ hitting\ honeypot\ ip/hour} = (P_{\ not\ hitting\ honeypot\ in\ one\ attack})^{N_{IP\ checks/hour}}$$

$$N_{IP\ checks/hour} = \frac{N_{seconds\ in\ hour}}{N_{seconds/check}} x\ N_{scanning\ threads}$$

$$P_{\ not\ hitting\ honeypot\ in\ one\ attack} = \frac{N_{IPv4\ addresses} - 1}{N_{IPv4\ addresses}}$$

## About Armis

Armis is the first agentless, enterprise-class security platform to address the new threat landscape of unmanaged and IoT devices. Fortune 1000 companies trust our unique out-of-band sensing technology to discover and analyze all managed, unmanaged, and IoT devices—from traditional devices like laptops and smartphones to new unmanaged smart devices like smart TVs, webcams, printers, HVAC systems, industrial robots, medical devices and more. Armis discovers devices on and off the network, continuously analyzes endpoint behavior to identify risks and attacks, and protects critical information and systems by identifying suspicious or malicious devices and quarantining them. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

20190528-1