DNS: from Frenemy to Hero

Using DNS to Protect against Online Threats

Kier Prior-Williams

Who Am I ?

- Working with DNS since 2000 - and DHCP, IPAM!
- Trusted Advisor for Architecture, Migrations, Training
- Experienced with commercial DDI products
- Also MS DNS, BIND, DNS Hosting
- Typically found on a bike somewhere
- Or, annoyin' my kids by blocking Fortnite

The Trouble with DNS

Is DNS Facilitating Crime ?

My Brief History of DNS Security

- In 2000 - DNS Security challenges:
  - Securing ACLs: allow-update, allow-transfer, allow-query, etc.

- These days, challenges may include (direct & indirect):
  - Malware
  - Phishing
  - Tunneling
  - Filtering
  - Data Exfiltration
  - **Reconnaissance*
  - DDoS / Amplification / Floods
  - Cache Poisoning
  - Server/Protocol exploits
  - Domain Hijacking
  - **Bitsquatting*
  - Cryptojacking
  - And more …

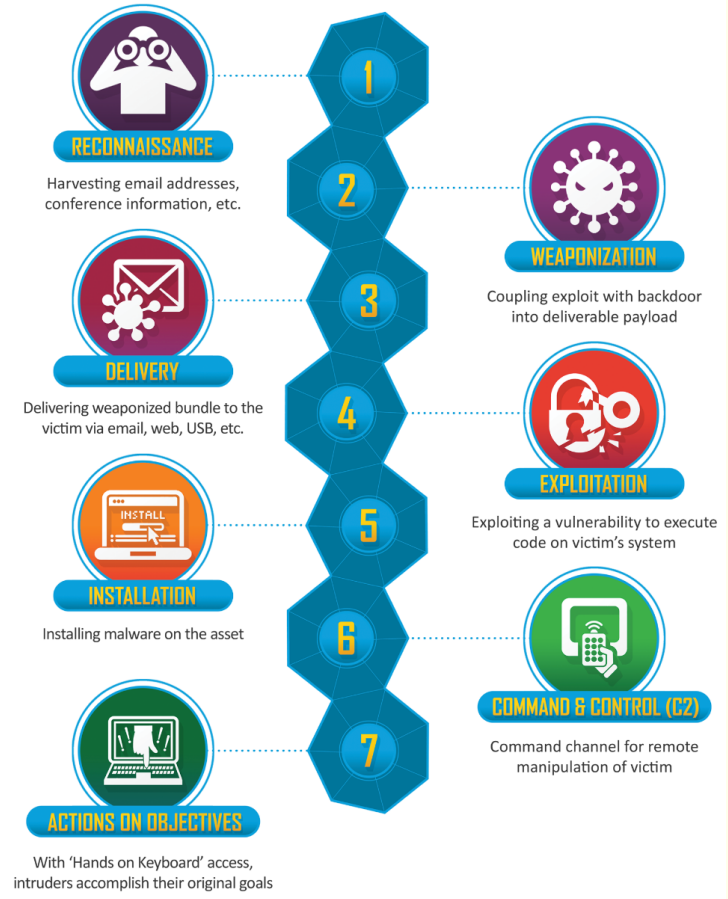
Bad Intentions

- DNS is used for Good and Bad intent
- Lockheed Martin:
  "Cyber Kill Chain® framework"

  The defender has seven opportunities to break the chain

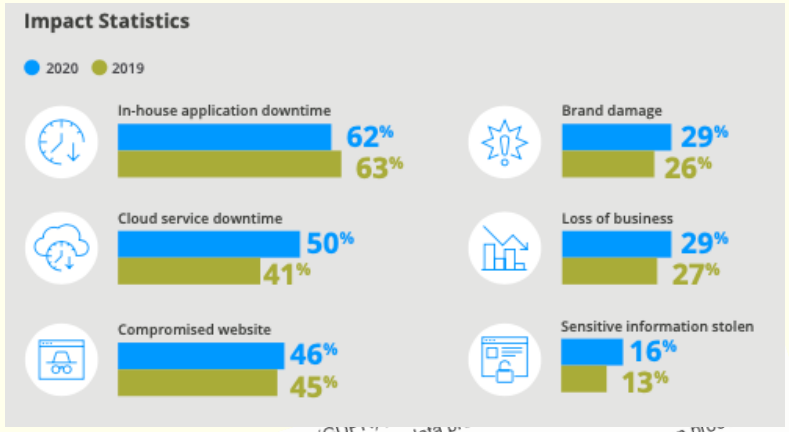
  JUST ONE MITIGATION
  BREAKS THE CHAIN

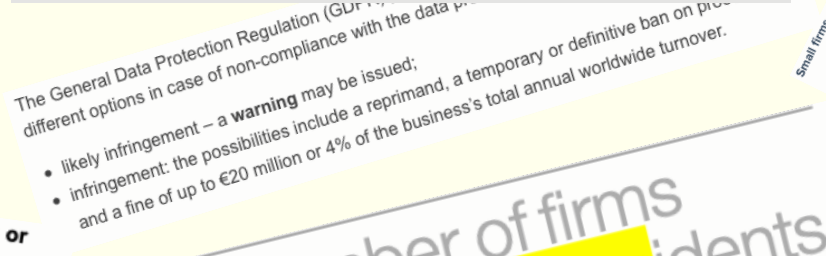
iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

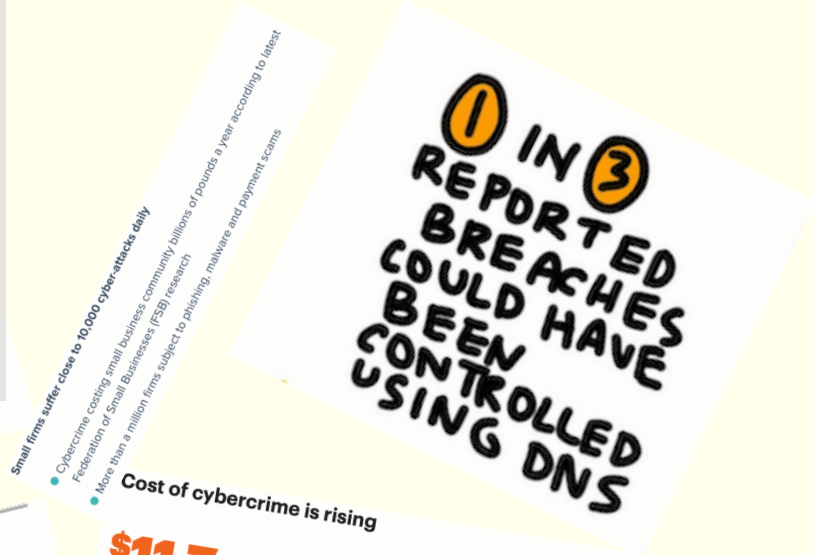


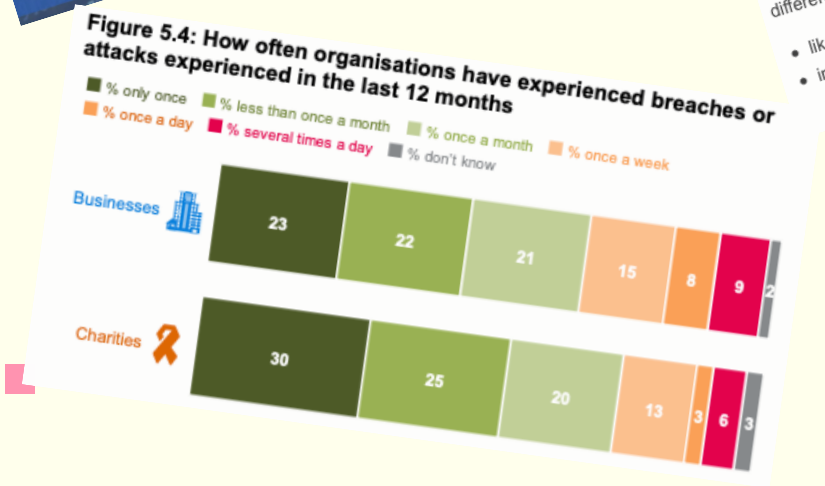
Source: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

“It’s not that bad, is it?”









Sources: [1]BlueCat, [2]NS1, [3]Hiscox, [4]Accenture Security, [5]UK DCMS, [6]European Commission, [7] UK FSB, [8] IDC/efficient iP

The Consequences

Hackers go after anything - and becoming a victim can have a major impact…

- Data loss - customer and company data
- Brand reputation damage
- Downturn in customer trust and sales
- Loss of Intellectual Property and competitive edge
- Company money stolen
- Legal consequences
- Staff time investigating how a breach occurred
- Cost of fixing the issue

DNS as a Protector

Use DNS to Stop Bad Stuff

DNS as a Security Layer

- DNS is one layer of security
- Important as DNS can indicate intent and give signals
- Identify malicious activity and take an action
- Several opportunities to use DNS to stop the Malware Lifecycle:

1. User directed to a malicious site (link, malvertising, typo)
2. Website delivers initial exploit (dropper)
3. Exploit contacts C2 (millions of domains/DGAs, only 1needs to work)
4. Malicious payload deployed
5. Malicious action (data exfiltration, etc.)

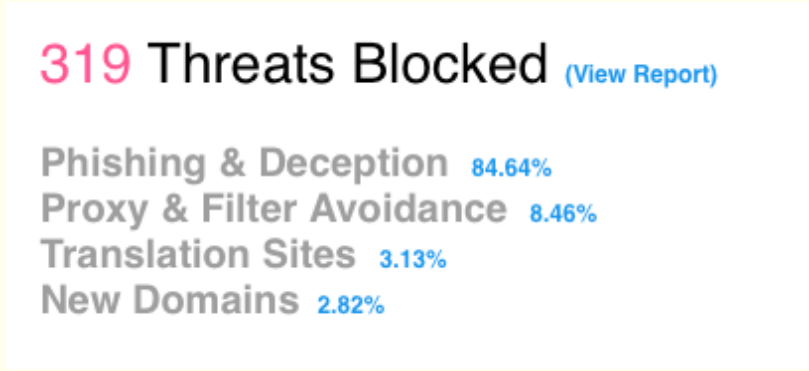
➢That domain on slide 5? The WannaCry "kill switch"

Filtering DNS

- DNS sinkhole: maintains a list of "bad" domains
  - Block or Redirect queries to a designated address (=information!)
- RPZ (Response Policy Zones)
  - The "DNS Firewall" rules in a DNS zone
  - Triggers: domain name, IP addresses, NS data
  - Actions: DROP, NXDOMAIN, PASSTHRU, Alternate RR (redirect)…
- Feeds are "important" – internal or external subscriber
  - How many new domains are created a day?
    - >100,000 new domains registered every day
- Filter on the DNS packet data, not just the domain name

DNS Products

- Open Source: BIND, Unbound, PowerDNS (RPZ ready)
  - Pi-hole, Technitium DNS Server, no doubt others !
- Community Firewalls: pfBlockerNg, unbound-plus
- Commercial vendors:
  - On-Prem DNS Firewall add-on (RPZ)
  - Feeds: Local or Subscribed
  - Cloud-based filtering resolvers



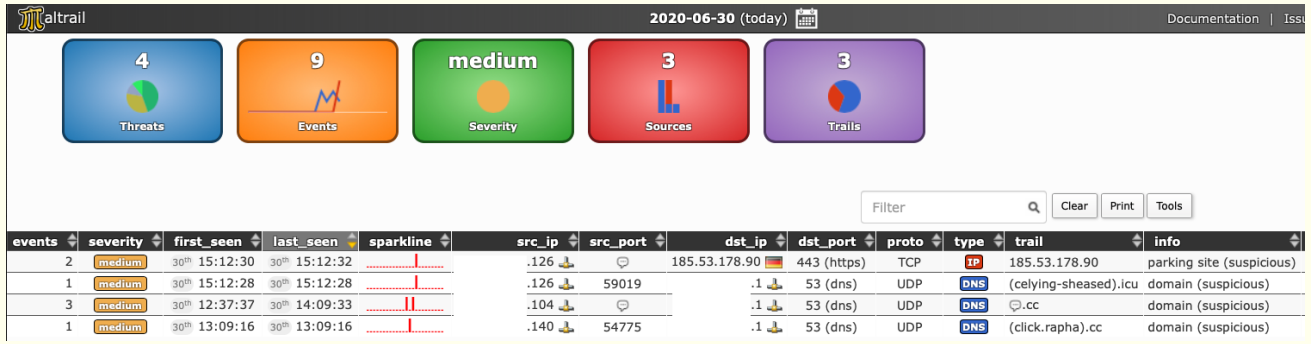
- dnstap: a more efficient way of collecting DNS queries and responses

Source: DNSFilter

Useful Data

- Data = Information = Knowledge = Action
- Investigation Context: Who, What, When ?
  - Grab the Client IP where possible (subject to PII rules)
- Send data to Syslog, SIEM, somewhere…

```
01-Jul-2020 10:05:22.930 rpz: info: client @0x7f7180586960 212.159.153.153#33123 (7th-club.com): rpz
QNAME NXDOMAIN rewrite 7th-club.com via 7th-club.com.urlhaus.zone
```



Source: [5] Maltrail

Challenges

- Know your Feed ! Thank you Tom Lawrence ☺

"… The remaining feeds don't make a valuable service at this point. The idea of the "Suspicious Domain" list was to aggregate different lists, but with essentially only 1 or 2 lists left, that doesn't make sense and I decided to no longer maintain the feed until we find new inputs." Johannes B. Ullrich, Ph.D. , Dean of Research, SANS Technology Institute

- Choose your Feed Subscription wisely:
  - As well as blocking bad stuff, what else are they filtering/supressing?
- How is your data being stored and used by vendors?
- Remote Workers, Split Tunnel VPN, No VPN !
  - Apply the same policies to users on or off the network
- DoT, DoH …

Source: [1] ISC SANS

Final Thoughts

- Get Visibility, the Knowledge to take Action
- Implement some kind of DNS Filtering
  - Start small, test, perhaps monitor but not block, observe
  - Roll out
  - Protect off-prem clients as well as on-prem
- Check the logs !
- Use layers of Protection, with different feeds
  - Using same feed for NGFW/IDS/IPS/DNS probably isn't ideal
- Oh, and check those ACLs are still good to go 😉

Source: [1] ISC SANS

Danke

@kierpw

www.linkedin.com/in/kierpw/