APTLD75 Dubai

Internet Routing Security

DNS Threat Landscape

Maher Yamout
Global Research and Analysis Team,
Kaspersky Lab

KASPERSKY

Why DNS is so important?

Connects the whole world together… considered as a critical component in IT infrastructure connectivity

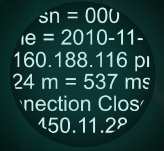
Inherited flaws by design allowing abuse in many ways

Used and abused across the entire cyber kill chain... by everyone

DNS Threat Landscape
Throughout most of the intrusion kill chain

Reconnaissance
- Zone transfers
- Service queries

Exploitation
- DNS hijacking / poisoning
- DNS spoofing
- Domain admin panel hijacking
- Registrar panel hijacking



Weaponization
- Protocol stack exploits
- Web exploits against panels

Actions on Objectives
- DNS tunneling for data exfil
- DNS FastFlux
- Reflective DDoS
- Traffic interception

FOCUS: KC-EXPLOITATION

- What's common in DNS spoofing and hijacking / poisoning attacks?
- Both are exploited due to protocol weaknesses... No authentication on who does what. It just trust everyone
- What's common in domain admin panel hijacking and registrar panel hijacking attacks?
- Both are exploited due to weak credentials or authentication framework weaknesses
- Exploited by cyber criminals and the APTs alike

KASPERSKY lab

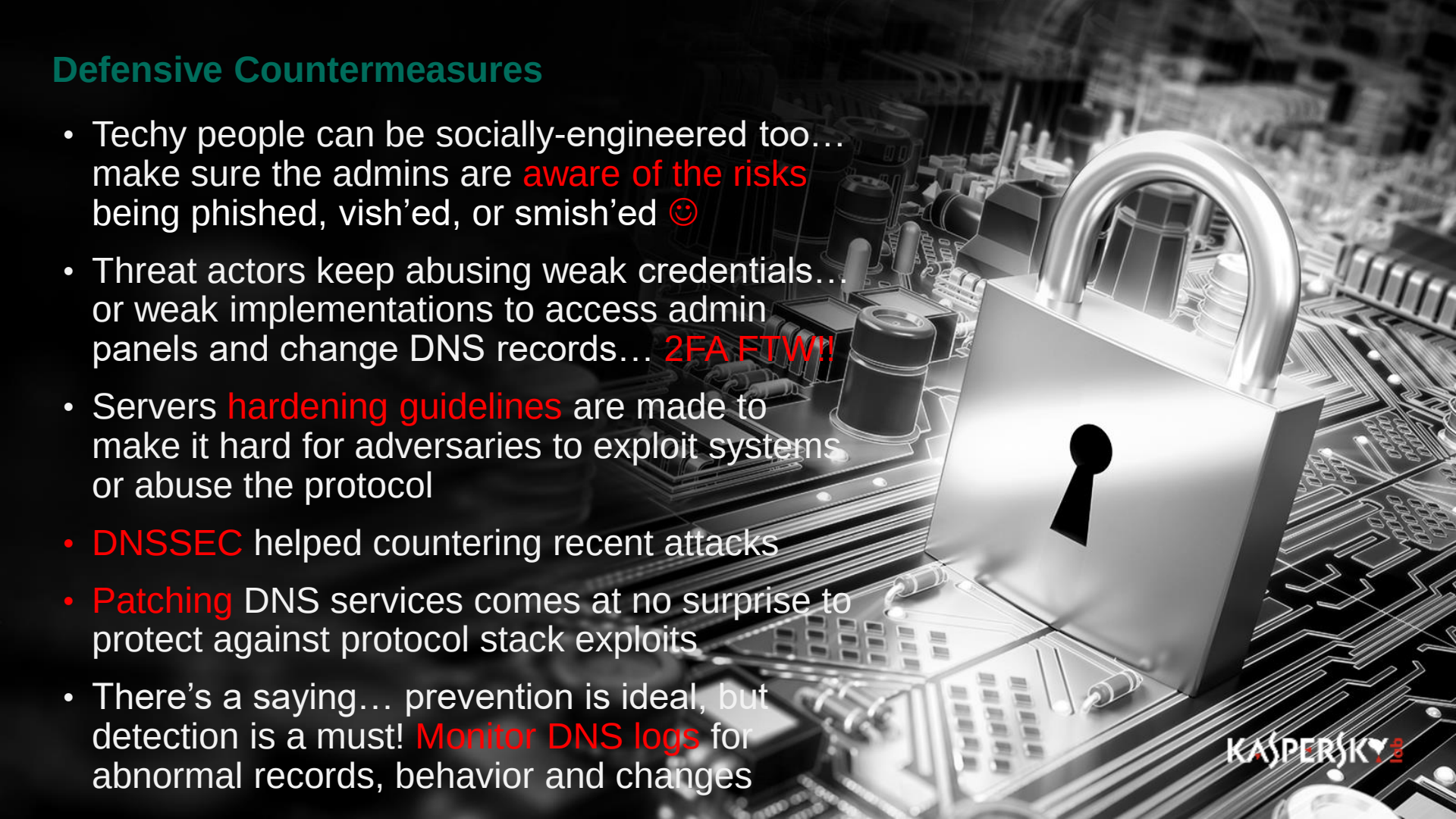
FOCUS: KC-ACTIONS ON OBJECTIVES

- DNS does not validate the source / destination… hence the Reflective DDoS attack (a.k.a. DNS amplification) – common with most UDP protocols like SNMP, NTP, etc… **mostly used with Hacktivists**

- What if a threat actor was able to alter a target domain's A record to a host he control? Or able to modify the NS records of the target? Traffic interception for the mass! Used recently by an APT to capture user credentials at a wide scale

Defensive Countermeasures

- Techy people can be socially-engineered too… make sure the admins are aware of the risks being phished, vish'ed, or smish'ed ☺
- Threat actors keep abusing weak credentials… or weak implementations to access admin panels and change DNS records… 2FA FTW!!
- Servers hardening guidelines are made to make it hard for adversaries to exploit systems or abuse the protocol
- DNSSEC helped countering recent attacks
- Patching DNS services comes at no surprise to protect against protocol stack exploits
- There's a saying… prevention is ideal, but detection is a must! Monitor DNS logs for abnormal records, behavior and changes



LET'S TALK?

Maher.Yamout@kaspersky.com

Global Research and Analysis Team (GReAT)

www.Kaspersky.com
www.securelist.com

KASPERSKY lab