Cisco Ransomware Defense

Quick Prevention against Ransomware

Marilena Kallenou

Nikos Theodosiou

10/4/2019

Ransomware

Malicious
Software

Encrypts
Critical Data

Demands
Payment

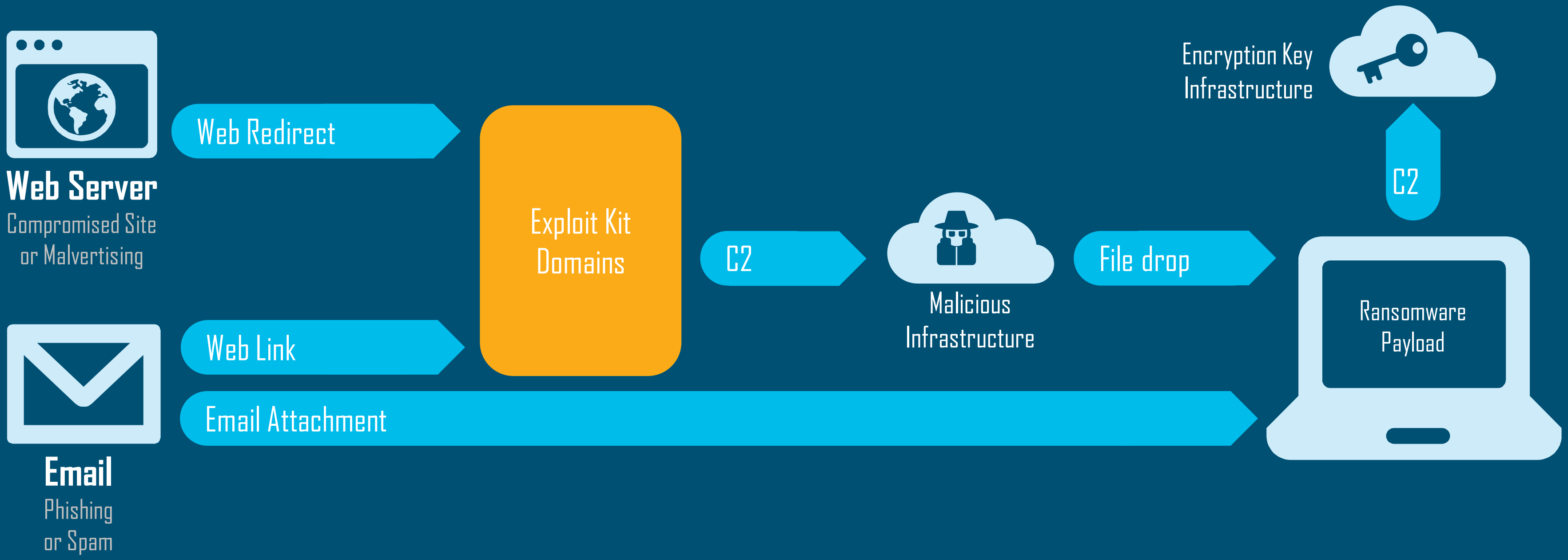
Did You Know?

Over 99%

of malware is sent by either web server or email

logicom Solutions

Ransomware Email and Web Delivery



logicom Solutions

Did You Know?

Over 90%

of known-bad malware use DNS to

- gain command and control
- exfiltrate data
- redirect traffic

Ransomware and DNS

	Encryption Key				Payment MSG
NAME*	DNS	IP	NO C2	TOR	PAYMENT
Locky	●	●			DNS
SamSam			●		DNS (TOR)
TeslaCrypt	●				DNS
CryptoWall	●				DNS
TorrentLocker	●				DNS
PadCrypt	●				DNS (TOR)
CTB-Locker	●			●	DNS
FAKBEN	●				DNS (TOR)
PayCrypt	●				DNS
KeyRanger	●			●	DNS

Cisco
Ransomware Defense

Quick Prevention

Cisco
Umbrella

Cisco Cloud Email Security with
Advanced
Malware Protection

Cisco Advanced Malware Protection
for Endpoints

logicom
Solutions

Defend Across All Attack Vectors

- Blocks users from connecting to malicious web sites
- Stops hackers from controlling and spreading ransomware

Cisco Umbrella

- Blocks users from receiving phishing attack emails and the harmful attachments that cause ransomware

Cisco Cloud Email Security with Advanced Malware Protection

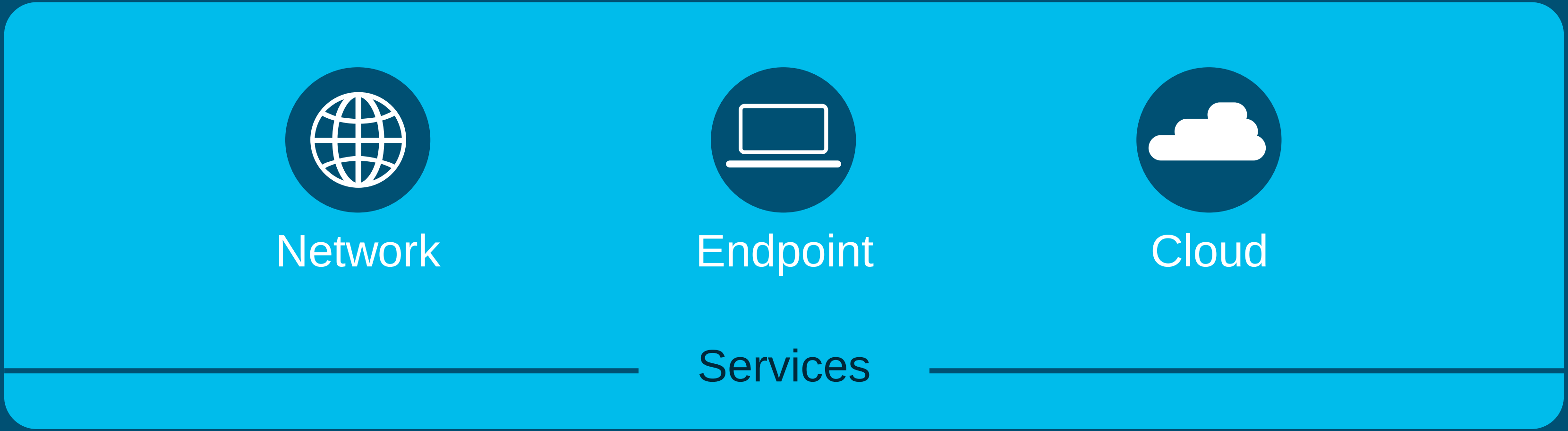
- Quarantines malicious files on endpoints to prevent infection
- Prevents the lateral movement of ransomware across your network

Cisco Advanced Malware Protection for Endpoints

logicom Solutions

Security that works together
Cisco Security Architecture

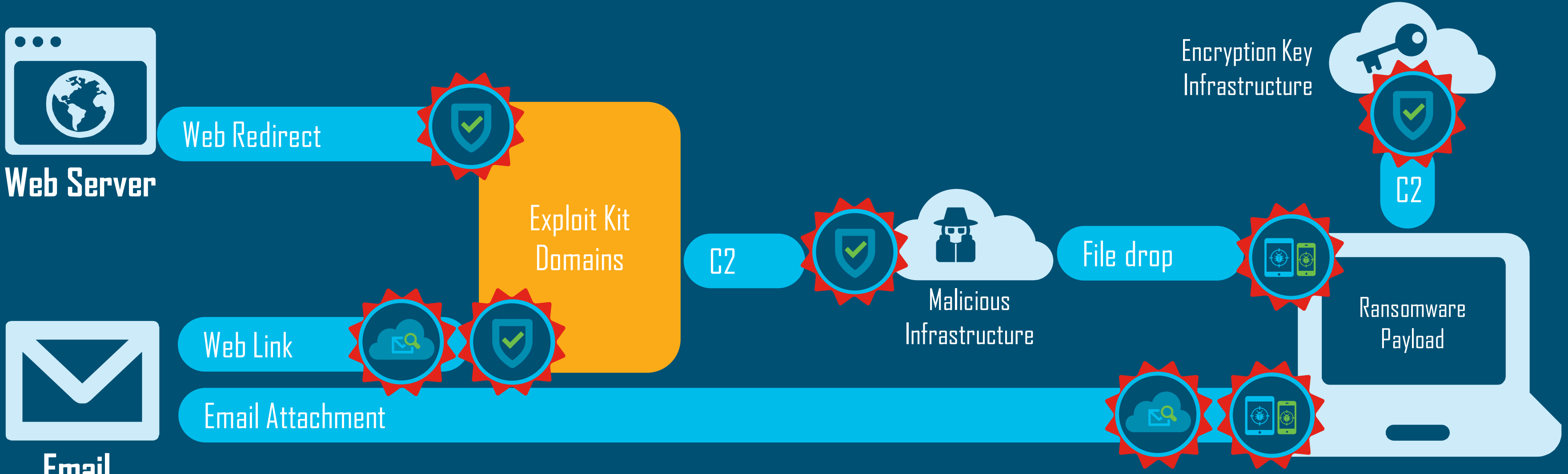
Threat intelligence – TALOS



Layers of Defense

logicom
Solutions

Break the Ransomware Chain



Cisco Ransomware Defense

✓ Stopped by Cisco Umbrella

Stopped by Cisco Cloud Email Security with AMP

Stopped by Cisco AMP for Endpoints

logicom Solutions

cisco

Logicom
Solutions