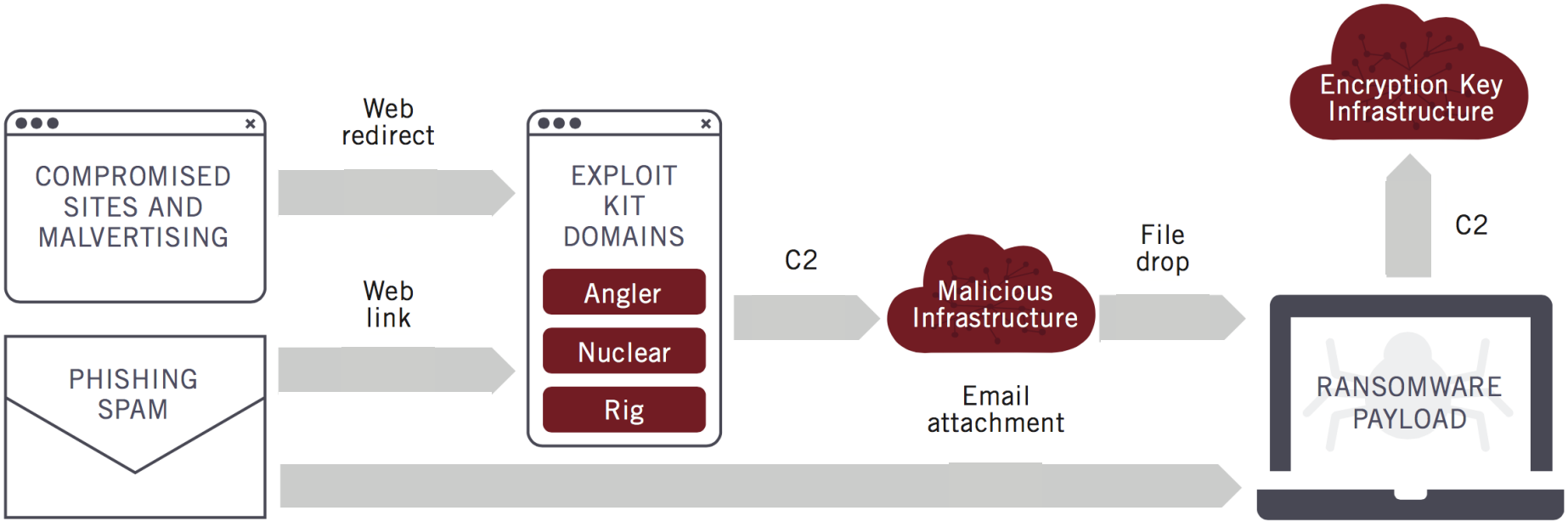
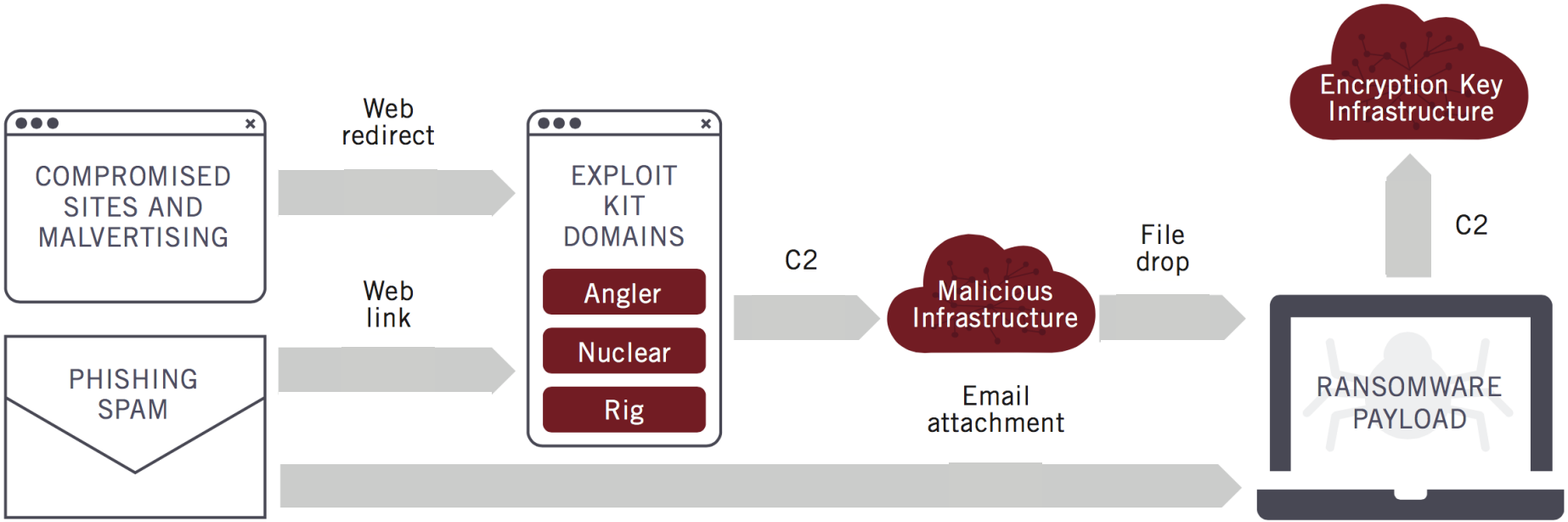
Defending Against Ransomware

Meg Diaz
OpenDNS Products
July 21,2016



	Encryption C&C				Payment MSG
NAME	**DNS**	**IP**	**NO C&C**	**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

3



Blocked by OpenDNS Umbrella

Blocked by Cisco AMP for Endpoints

Blocking Ransomware: Real World Example with a Locky Domain

glslindia[.]com (detection Date: 15/03/2016)

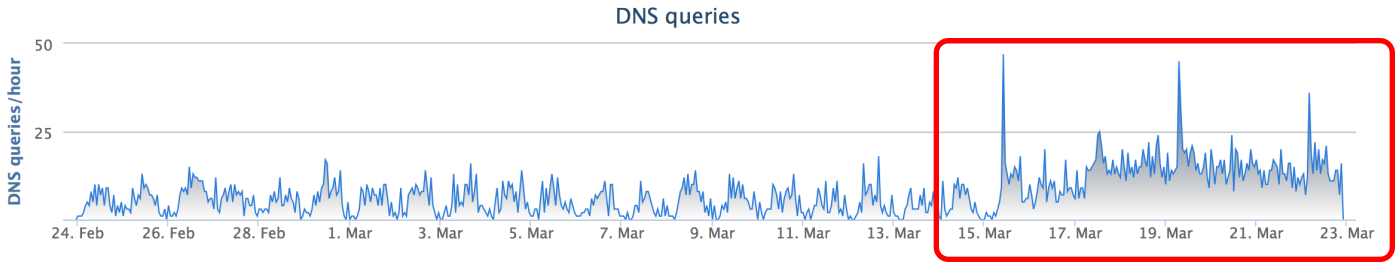
DETAILS FOR GLSLINDIA.COM

Search in Google

Search in VirusTotal

This domain is currently in the OpenDNS Security Labs block list

This domain is associated with the following type of threat: Dropper

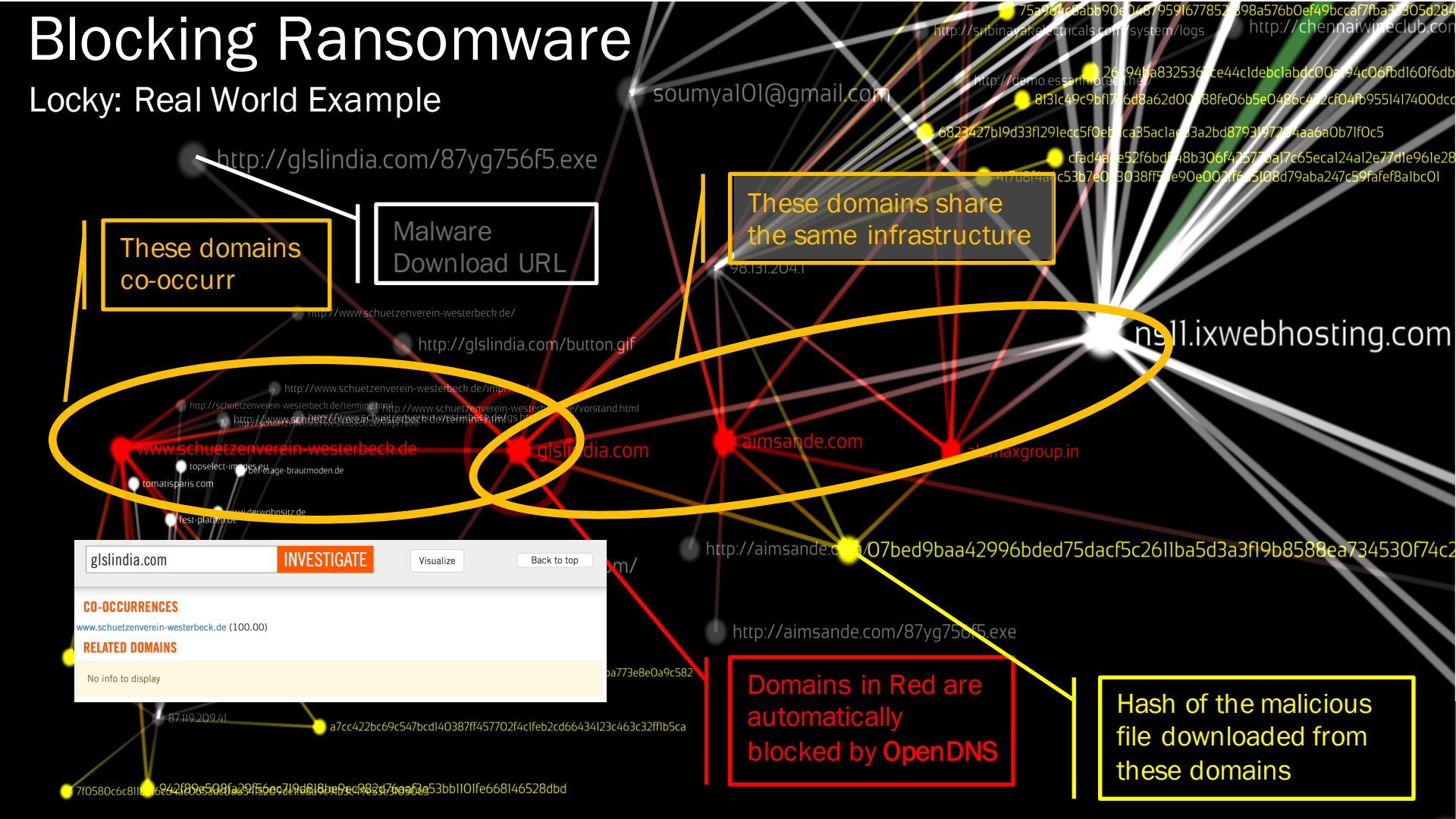


DOMAIN TAGGING

Period	Category	URL
Mar 18, 2016 - Current	Malware	http://glslindia.com/87yg756f5.exe
Mar 15, 2016 - Current	Malware	

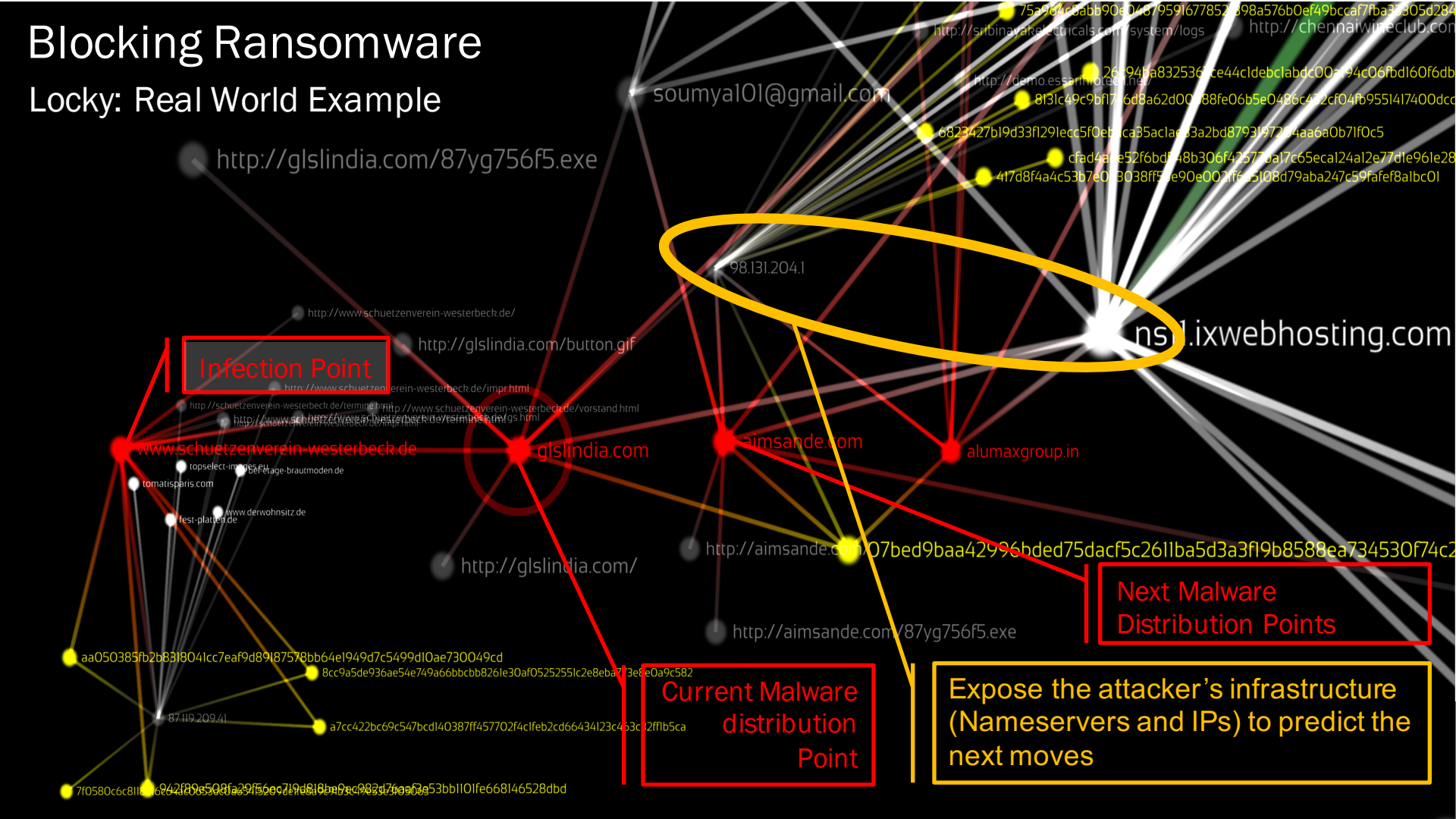
Blocking Ransomware

Locky: Real World Example



Blocking Ransomware

Locky: Real World Example



Discover the Threats Before They Happen (1)

VT Link:
https://virustotal.com/en/file/07bed9baa42996bded75dacf5c2611ba5d3a3f19b8588ea734530f74c2586087/analysis/
(first **VT** submission: **2016-03-18** 16:51:45 **three days** OpenDNS)

File information

Identification | Details | Content | Analyses | Submissions | ITW | Behaviour | Comments

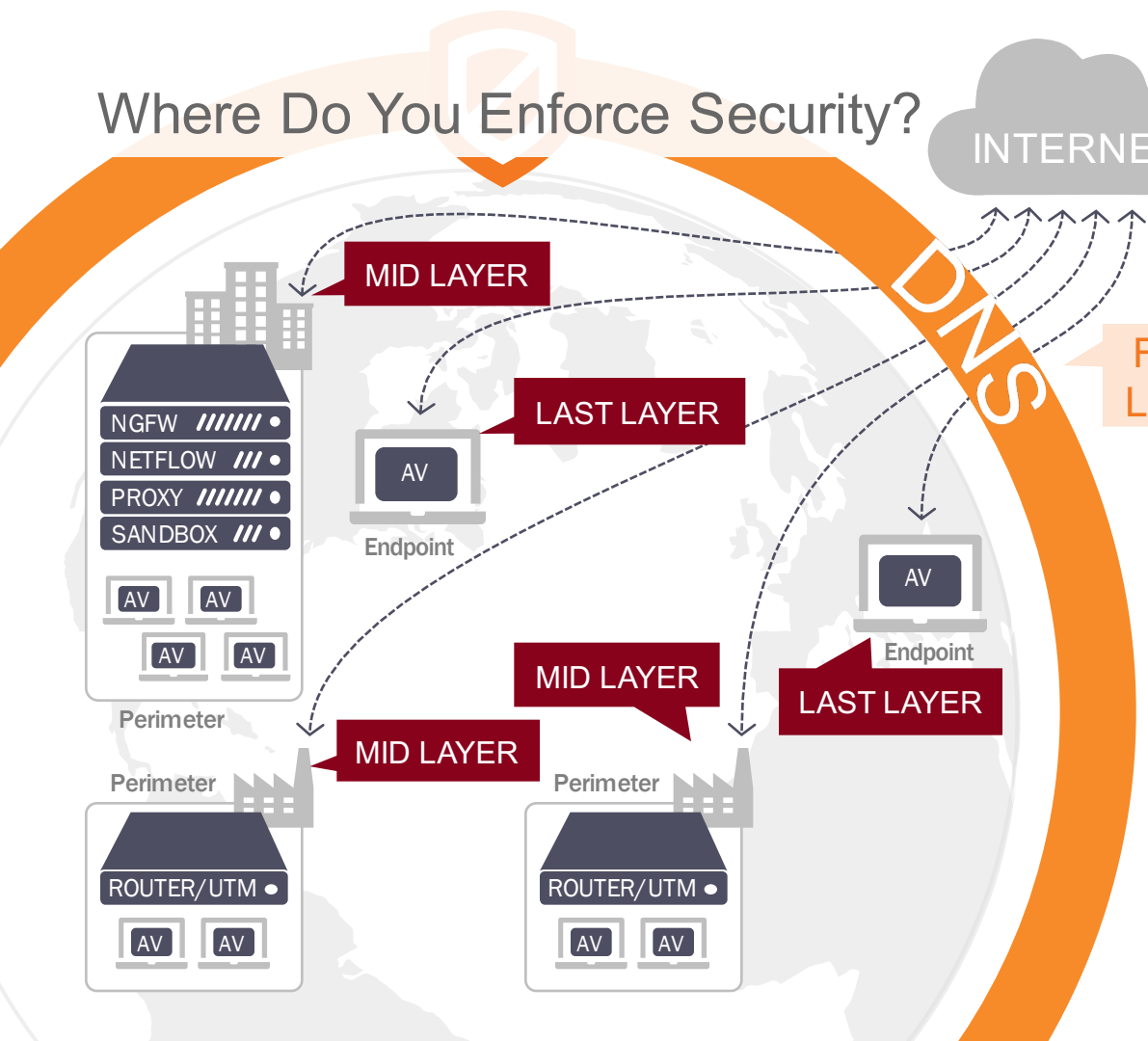
Date	File name	Source	Country
2016-04-06 14:09:36	69b933a694710f8ceb314dc897a94cbe.exe	00625b5b (email)	FR
2016-03-29 23:07:06	69b933a694710f8ceb314dc897a94cbe.exe	00625b5b (email)	FR
2016-03-24 15:42:12	Malware_MSEXE_07bed9baa42996bded75dac...	92c8a5a8 (web)	BR
2016-03-22 21:54:19	69b933a694710f8ceb314dc897a94cbe.exe	00625b5b (email)	FR
2016-03-19 05:07:44	vti-rescan	77377302 (community)	PH
2016-03-19 01:50:42	69b933a694710f8ceb314dc897a94cbe	880cc5f3 (api)	KR
2016-03-18 22:51:12	69b933a694710f8ceb314dc897a94cbe	40787d1a (api)	KR
2016-03-18 21:18:56	69b933a694710f8ceb314dc897a94cbe	8ecc9426 (web)	EC
2016-03-18 19:51:40	69b933a694710f8ceb314dc897a94cbe	892a7459 (api)	KR
2016-03-18 16:51:45	69b933a694710f8ceb314dc897a94cbe	a1ac7217 (api)	KR

Download file | Re-scan file | Close

Best Practice Recommendations

- Solid patch management
- Non-native document rendering PDF + Office
- Users run as non-privileged users (no admin)
- Disable RDP
- Firewall enabled on endpoints
- Segmented and secured backups (tested)
- Encryption of backups and local documents
- Look into adding Endpoint Threat Detection & Response and DNS-layer security

Where Do You Enforce Security?



BENEFITS

Alerts Reduced 2-10x; Improves Your SIEM

Traffic & Payloads Never Reach Target

Provision Globally in UNDER 30 MINUTES

Thank you.