RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: CCT-T07

# Ransomware in the Middle East

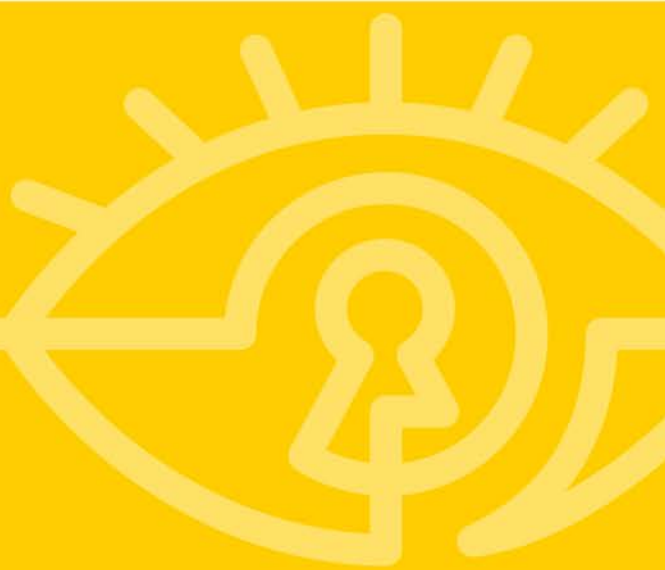
**Kenneth Geers**

Senior Research Scientist

Comodo

@KennethGeers

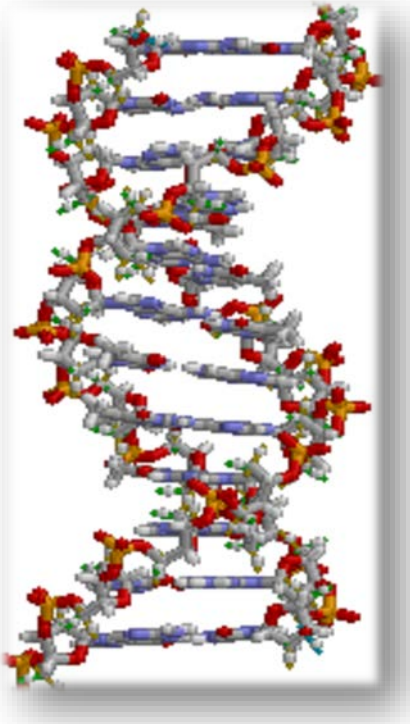
#RSAC



# What is Ransomware?

# Concept

- Cryptovirus
- Extortion: denial of access
- Hostage: data, software, hardware
- Target: organizations, individuals
  - Criminals find “sweet spot”
- Goal: crime, coercion
- Future: IoT

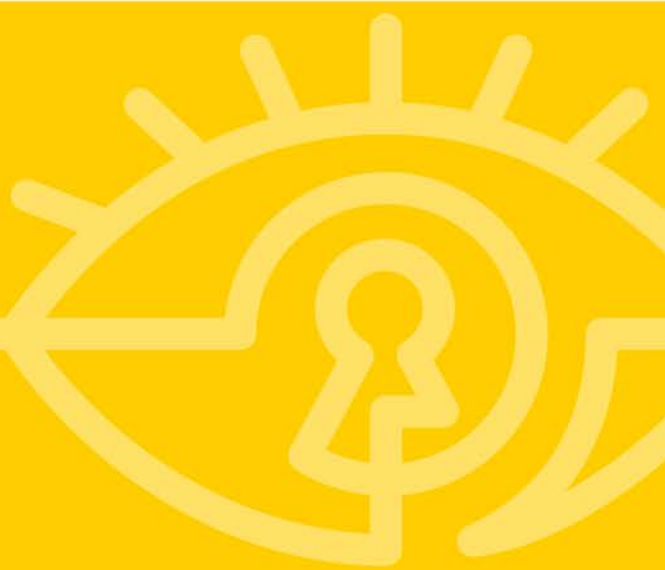


# Details

- Scareware: fake warning messages, OS or app blocking
- Ransomware: professional encryption
- Propagation: apps, botnet, drive-by website, email, entertainment, exploit kit, files, links, macros, P2P, spam, “updates”, USB
- Social engineering: carrots & sticks
- Payment : bitcoin, e-cash, Tor, dark web service (millions paid)
- Command and Control: manual, automated, $ laundering

# Steps

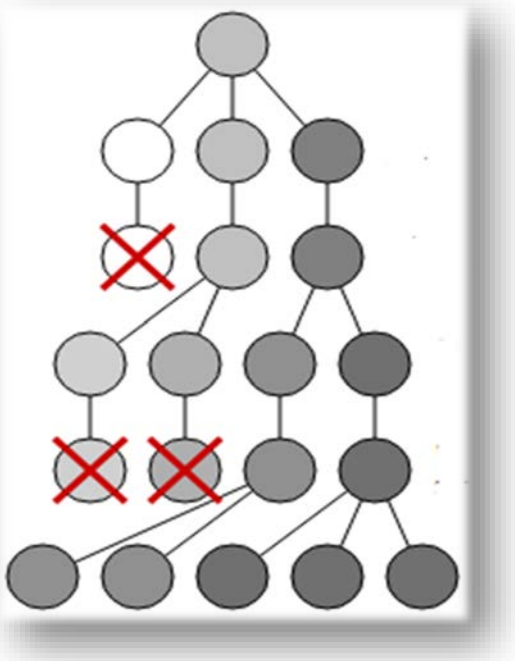
1. Infection: phishing, malware installation
2. C2: downloads, persistence
3. Management: 2 keys, backup deletion, isolation
4. Encryption: selected file extensions + backup
5. Extortion: threat is $ or X, malware removal



# Ransomware History

# Birth

- 1989: “AIDS”
- 1996: IEEE paper
- 2006: RSA encryption
- 2010: WinLock
- 2011: Windows Activation notice
- 2012: Reveton “Police Trojan”



# Evolution

- 2013: CryptoLocker (targeted U.S.)
- 2013: Bitcoin, OS X
- 2014: Op Tovar, Bogachev, Scatter
- 2014: CryptoWall, malvertising
- 2015: Web hacking
- 2016: Locky, healthcare

# Volatility



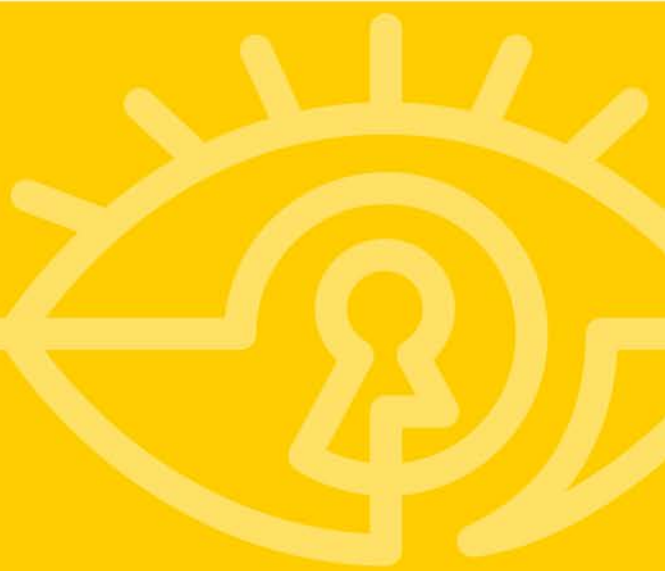
| Location | 1H15 Ransomware ER | Location | 2H15 Ransomware ER |
|---|---|---|---|
| United Arab Emirates | 2.98 % | Canada | 1.54 % |
| Portugal | 1.48 % | United States | 1.24 % |
| Italy | 1.35 % | Turkey | 1.03 % |
| Qatar | 1.22 % | Portugal | 1.01 % |
| Senegal | 0.99 % | Romania | 0.92 % |
| Hungary | 0.95 % | Saudi Arabia | 0.91 % |
| Belgium | 0.82 % | United Kingdom | 0.88 % |
| Mexico | 0.77 % | Italy | 0.84 % |
| Switzerland | 0.75 % | Pakistan | 0.83 % |
| Latvia | 0.71 % | Cambodia | 0.82 % |

Source: Microsoft

# Middle East: ransomware cases



- **bh:** Motorsport
- **cy:** “Police Emergency Response Unit”
- **eg:** Trend Micro “Top Target”
- **ir:** Sec Works: CryptoLocker “Top Ten”
- **iq:** Locky
- **il:** Israel Electric Authority
- **jo:** “Hashemite Kingdom of Jordan”
- **kw:** Kaspersky: Locky #3
- **lb:** “Lebanon Police”
- **om:** VPN, proxies
- **ps:** “Palestinian Civil Police Force”
- **qa:** “State of Qatar Ministry of Interior”
- **sa:** “Ministry of Interior”
- **sd:** Locky
- **sy:** Syrian Electronic Army
- **tr:** Cerber
- **ye:** Yemen Cyber Army



# Ransomware in Action

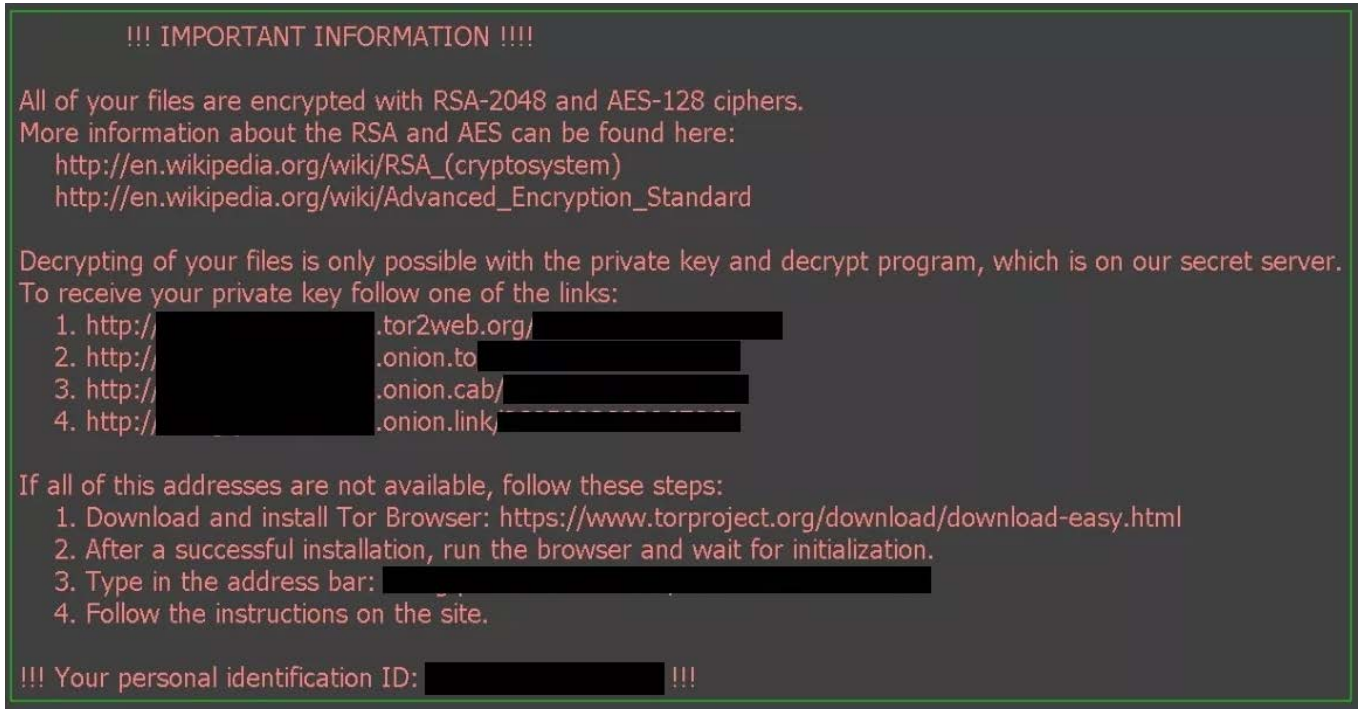
# Encryption

- Increasing sophistication
- “Lockers” to real encryption
- Public-key cryptography
- May encrypt HD, shares, backup
- May overwrite MBR
- May encrypt physical sectors on disk

# Infection


Source:
Cotswold
IT Guy

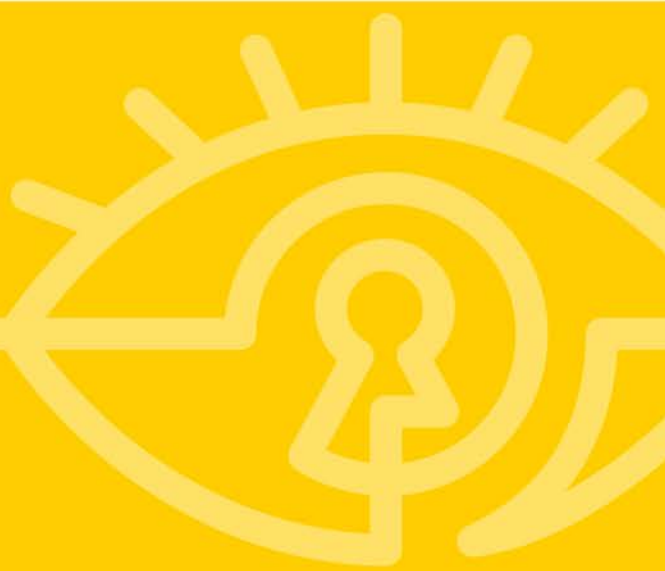
# Infection




Source: MS

# Decryption

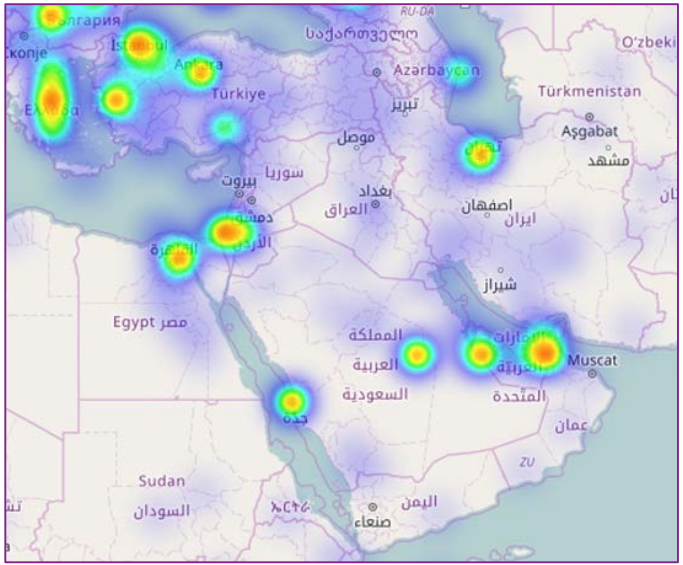
- Attacker retains decryption key until $ paid
- Payment activation screen
- Validation: malware -> C2 to verify payment
- Processing: minutes to weeks
- Attacker may decrypt files, uninstall malware
- Recovery tools (e.g. Crilock: FireEye/Fox-IT)



# Data Analysis

# Comodo Data (Aug-Oct 2016)

- 187 million malware events
  - 234 country code top-level domains
  - 203,202 trojan events
- 128,797 ransomware events
  - 139 ccTLDs
  - 100+ infections: 55 ccTLDs
- Middle East analysis
  - 17 countries

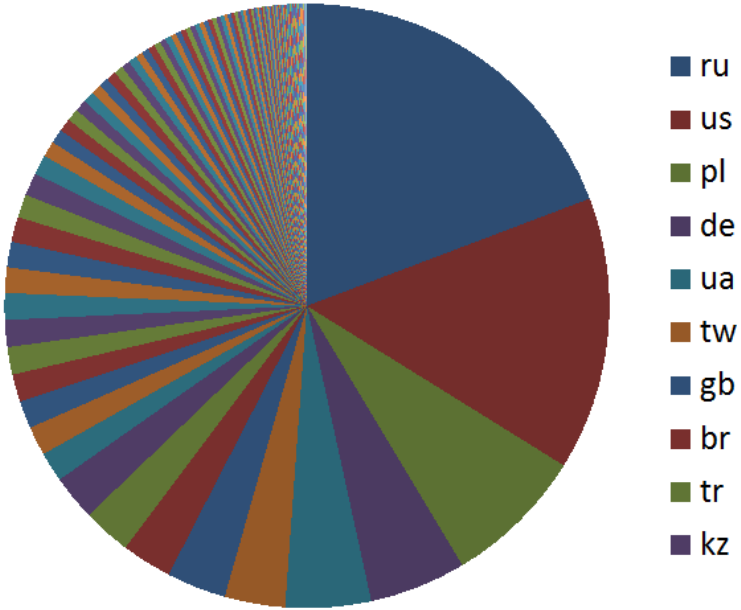



COMODO
Creating Trust Online®

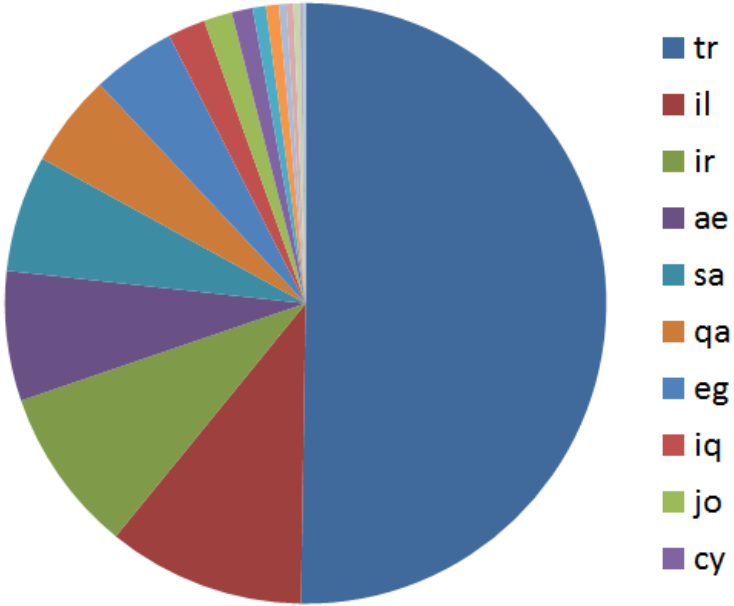
# All Malware



World: 234 Countries




Middle East: 17 Countries



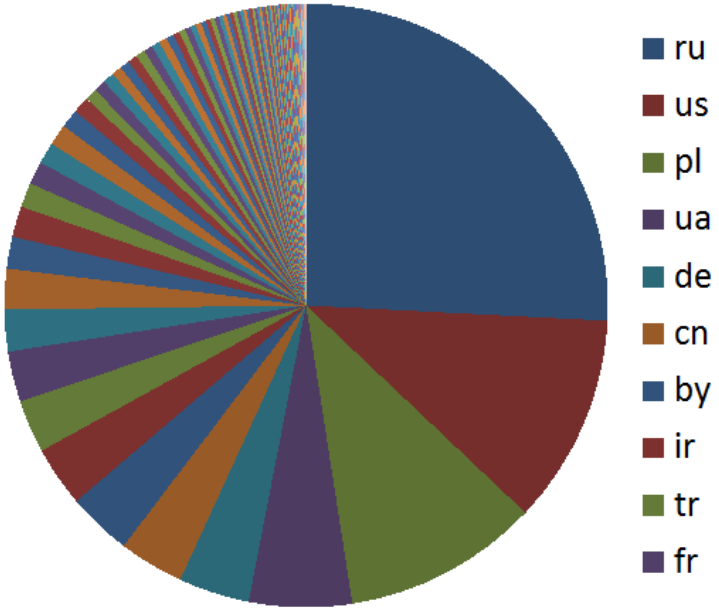

Source: Comodo

COMODO
Creating Trust Online®

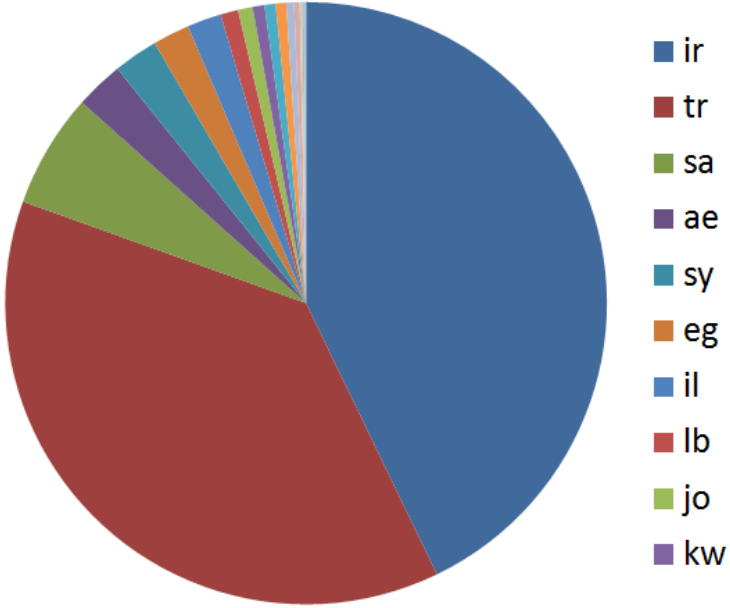
# Trojans



World: 167 Countries




Middle East: 17 Countries



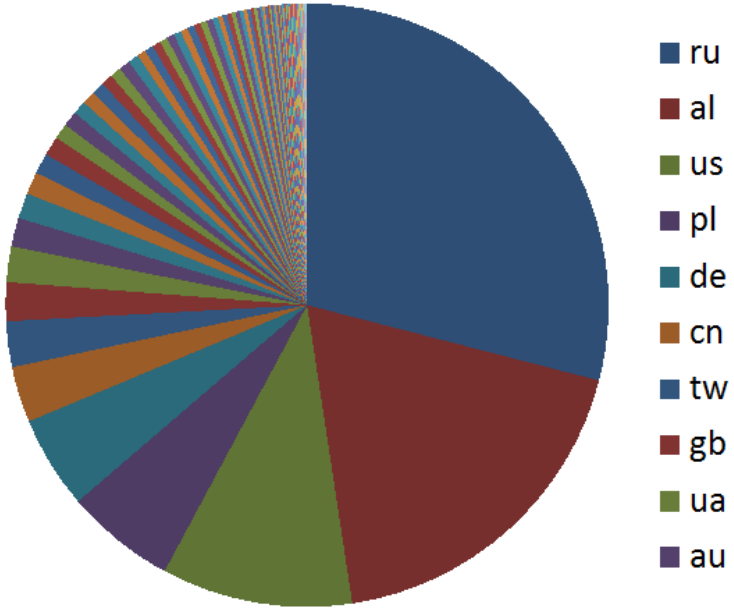

Source: Comodo

COMODO
Creating Trust Online®

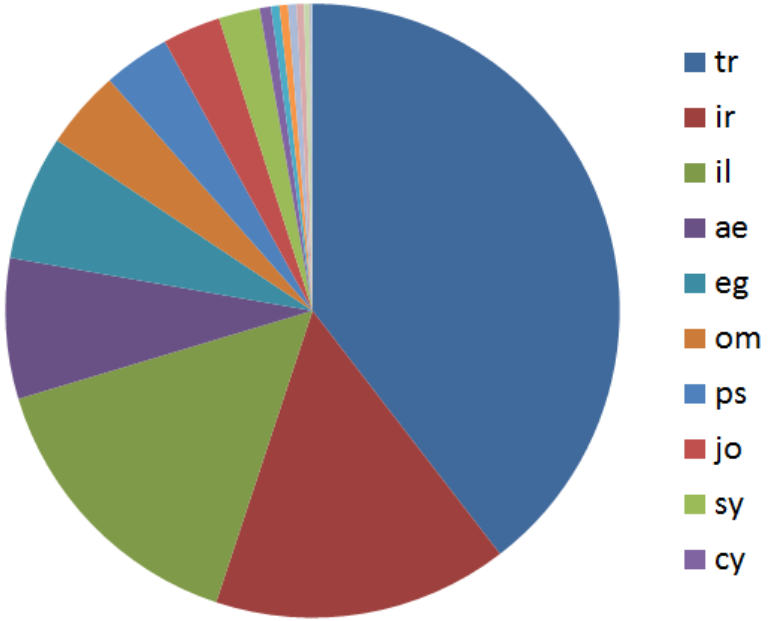
# Ransomware



World: 139 Countries




Middle East: 17 Countries




Source: Comodo

COMODO
Creating Trust Online®

# Ransomware / Malware Ratio



## Highest Ratio

1. Albania
2. South Korea
3. Finland
4. China
5. Denmark
6. Russia
7. Australia
8. Japan
9. Malaysia
10. Sweden

## Lowest Ratio

46. UAE
47. Canada
48. Belarus
49. Portugal
50. South Africa
51. Mexico
52. Serbia
53. Moldova
54. Turkey
55. Kazakhstan

Based on 100+ Ransomware Infections

Source: Comodo

COMODO
Creating Trust Online®

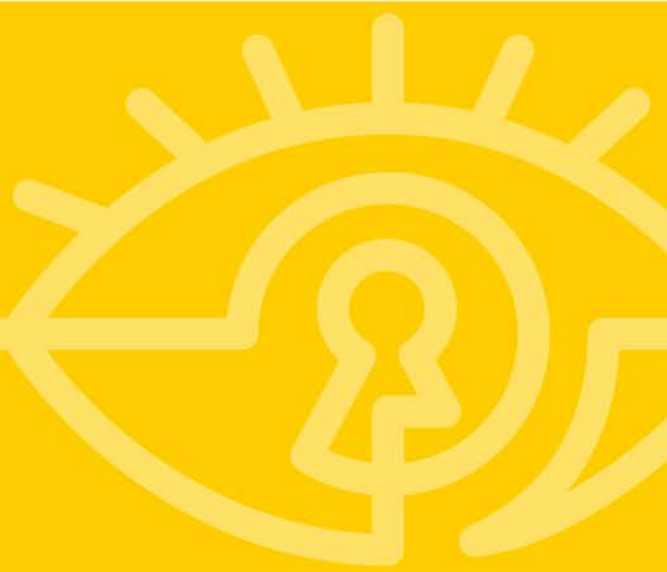
# Middle East: Ransomware Ratio



1. Palestine
2. Oman
3. Syria
4. Jordan
5. Iran
6. Egypt
7. Israel
8. Kuwait
9. UAE
10. Yemen
11. Turkey
12. Cyprus
13. Lebanon
14. Bahrain
15. Iraq
16. Qatar
17. Saudi Arabia

Source: Comodo

COMODO
Creating Trust Online®



# Ransomware Mitigation

# Apply: Today

- Designate personnel
  - Contingency plans, business continuity
  - Know tech, bank, law enforcement contacts
- Awareness campaign, testing
  - Realize recovery may be impossible
- *Offline* backup: not net shares
  - MS OneDrive, File History

# Apply: 3 Months



- Best practices
  - AV, patch, “least privilege”, whitelist, known indicators
  - Macros, links, embedded code, pop-ups, attachments, .exe
  - Social engineering: don’t trust, evaluate
- Response tactics
  - Catch before C2 established, encryption begins
  - SafeMode, rescue disk, restore point, anti-malware, decrypt tools
  - MS: Task Manager, Safety Scanner, Windows Defender

# Ethics of Payment



- Law enforcement discourage– but 1%+ may pay
- Some enterprises (e.g. hospitals) feel no choice
- Some save bitcoin for payment
- Payment does not guarantee anything
- Hackers may leave backdoor
- Payment may mean harassment & future target

RSAConference2016

Abu Dhabi | 15–16 November | Emirates Palace

Connect to Protect

SESSION ID: CCT-T07

# Ransomware in the Middle East

**Kenneth Geers**

Senior Research Scientist

Comodo

@KennethGeers

#RSAC