

Cybersecurity – Trends and Perspectives

ICT4FUTURE: Segurança e Open ICT

Pedro Queirós, Cybersecurity Engineer

September 15th, 2016

A photograph of two rock climbers on a steep, light-colored rock face. One climber in a yellow shirt is higher up, and another in a blue shirt is lower down, both secured by ropes. The background shows a clear blue sky and distant mountains.

multicert

Engineering for digital security

Summary

1. Cybersecurity Threats
2. Why worry?
3. Cybersecurity Responses
4. Perspectives

1. Cybersecurity Threats

- Rise of ransomware and spearphishing¹

1. SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing
2. Microsoft Quick Guide to the Most Important Insights in Security

1. Cybersecurity Threats

- Rise of ransomware and spearphishing ¹
- More vulnerabilities found and exploited on the IoT and mobile platforms ¹

1. SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing
2. Microsoft Quick Guide to the Most Important Insights in Security

1. Cybersecurity Threats

- Rise of ransomware and spearphishing ¹
- More vulnerabilities found and exploited on the IoT and mobile platforms ¹
- Trojans + social engineering increased 57% ²

1. SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing

2. Microsoft Quick Guide to the Most Important Insights in Security

1. Cybersecurity Threats

- Rise of ransomware and spearphishing ¹
- More vulnerabilities found and exploited on the IoT and mobile platforms ¹
- Trojans + social engineering increased 57% ²
- Java exploits are not as hot ²

1. SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing

2. Microsoft Quick Guide to the Most Important Insights in Security

1. Cybersecurity Threats

- Rise of ransomware and spearphishing ¹
- More vulnerabilities found and exploited on the IoT and mobile platforms ¹
- Trojans + social engineering increased 57% ²
- Java exploits are not as hot ²
- Vulnerability disclosures - 41.8% rated as highly severe ²

1. SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing

2. Microsoft Quick Guide to the Most Important Insights in Security

1. Cybersecurity Threats

- Rise of ransomware and spearphishing ¹
- More vulnerabilities found and exploited on the IoT and mobile platforms ¹
- Trojans + social engineering increased 57% ²
- Java exploits are not as hot ²
- Vulnerability disclosures - 41.8% rated as highly severe ²
- A shortage in specialized talent

1. SANS State of Cyber Threat Intelligence Survey: CTI Important and Maturing

2. Microsoft Quick Guide to the Most Important Insights in Security

1. Cybersecurity Threats

| Category | Worldwide | USA | Brazil | China | Russia | France | Germany | UK | Italy | Canada | Japan |
|--------------------------------------|-----------|------|--------|-------|--------|--------|---------|-------|-------|--------|-------|
| Browser Modifiers | 7.6% | 9.1% | 11.8% | 0.6% | 7.0% | 14.3% | 8.7% | 10.9% | 15.3% | 11.3% | 4.2% |
| Trojans | 7.1% | 4.2% | 12.7% | 10.2% | 20.8% | 5.7% | 4.3% | 4.4% | 7.0% | 5.1% | 1.5% |
| Worms | 3.3% | 0.6% | 8.9% | 5.6% | 4.6% | 1.9% | 1.1% | 0.8% | 3.9% | 0.6% | 0.7% |
| Software Bundlers | 3.1% | 1.7% | 1.5% | 0.2% | 0.5% | 2.2% | 0.9% | 2.3% | 2.5% | 2.5% | 0.5% |
| Downloaders & Droppers | 2.2% | 2.3% | 6.5% | 3.2% | 6.6% | 2.8% | 1.5% | 3.2% | 3.1% | 3.3% | 0.4% |
| Obfuscators & Injectors | 1.7% | 1.0% | 5.3% | 5.2% | 7.3% | 1.9% | 1.6% | 1.7% | 2.8% | 1.6% | 0.6% |
| Adware | 1.6% | 4.5% | 7.1% | 0.2% | 5.2% | 7.8% | 4.1% | 4.7% | 7.2% | 5.3% | 2.0% |
| Exploits | 1.4% | 3.4% | 2.4% | 1.7% | 1.3% | 2.5% | 3.2% | 4.4% | 4.3% | 5.7% | 3.2% |
| Viruses | 1.1% | 0.4% | 2.2% | 7.4% | 1.5% | 0.4% | 0.3% | 0.3% | 0.8% | 0.4% | 0.2% |
| Other | 0.6% | 0.9% | 0.3% | 1.2% | 0.3% | 0.5% | 0.5% | 0.6% | 0.7% | 1.5% | 0.2% |
| Backdoors | 0.5% | 0.7% | 1.4% | 1.8% | 2.0% | 0.9% | 0.6% | 0.9% | 1.0% | 0.7% | 0.3% |
| Ransomware | 0.3% | 0.6% | 0.5% | 0.0% | 0.6% | 0.7% | 0.6% | 0.4% | 1.4% | 0.7% | 0.4% |
| Password Stealers & Monitoring Tools | 0.2% | 0.4% | 1.0% | 0.5% | 0.8% | 0.3% | 0.4% | 0.4% | 0.6% | 0.6% | 0.3% |

Microsoft Quick Guide to the Most Important Insights in Security

1. Cybersecurity Threats

| Category | Worldwide | USA | Brazil | China | Russia | France | Germany | UK | Italy | Canada | Japan |
|--------------------------------------|-----------|------|--------|-------|--------|--------|---------|-------|-------|--------|-------|
| Browser Modifiers | 7.6% | 9.1% | 11.8% | 0.6% | 7.0% | 14.3% | 8.7% | 10.9% | 15.3% | 11.3% | 4.2% |
| Trojans | 7.1% | 4.2% | 12.7% | 10.2% | 20.8% | 5.7% | 4.3% | 4.4% | 7.0% | 5.1% | 1.5% |
| Worms | 3.3% | 0.6% | 8.9% | 5.6% | 4.6% | 1.9% | 1.1% | 0.8% | 3.9% | 0.6% | 0.7% |
| Software Bundlers | 3.1% | 1.7% | 1.5% | 0.2% | 0.5% | 2.2% | 0.9% | 2.3% | 2.5% | 2.5% | 0.5% |
| Downloaders & Droppers | 2.2% | 2.3% | 6.5% | 3.2% | 6.6% | 2.8% | 1.5% | 3.2% | 3.1% | 3.3% | 0.4% |
| Obfuscators & Injectors | 1.7% | 1.0% | 5.3% | 5.2% | 7.3% | 1.9% | 1.6% | 1.7% | 2.8% | 1.6% | 0.6% |
| Adware | 1.6% | 4.5% | 7.1% | 0.2% | 5.2% | 7.8% | 4.1% | 4.7% | 7.2% | 5.3% | 2.0% |
| Exploits | 1.4% | 3.4% | 2.4% | 1.7% | 1.3% | 2.5% | 3.2% | 4.4% | 4.3% | 5.7% | 3.2% |
| Viruses | 1.1% | 0.4% | 2.2% | 7.4% | 1.5% | 0.4% | 0.3% | 0.3% | 0.8% | 0.4% | 0.2% |
| Other | 0.6% | 0.9% | 0.3% | 1.2% | 0.3% | 0.5% | 0.5% | 0.6% | 0.7% | 1.5% | 0.2% |
| Backdoors | 0.5% | 0.7% | 1.4% | 1.8% | 2.0% | 0.9% | 0.6% | 0.9% | 1.0% | 0.7% | 0.3% |
| Ransomware | 0.3% | 0.6% | 0.5% | 0.0% | 0.6% | 0.7% | 0.6% | 0.4% | 1.4% | 0.7% | 0.4% |
| Password Stealers & Monitoring Tools | 0.2% | 0.4% | 1.0% | 0.5% | 0.8% | 0.3% | 0.4% | 0.4% | 0.6% | 0.6% | 0.3% |

Microsoft Quick Guide to the Most Important Insights in Security

1. Cybersecurity Threats

| Category | Worldwide | USA | Brazil | China | Russia | France | Germany | UK | Italy | Canada | Japan |
|--------------------------------------|-----------|------|--------|-------|--------|--------|---------|-------|-------|--------|-------|
| Browser Modifiers | 7.6% | 9.1% | 11.8% | 0.6% | 7.0% | 14.3% | 8.7% | 10.9% | 15.3% | 11.3% | 4.2% |
| Trojans | 7.1% | 4.2% | 12.7% | 10.2% | 20.8% | 5.7% | 4.3% | 4.4% | 7.0% | 5.1% | 1.5% |
| Worms | 3.3% | 0.6% | 8.9% | 5.6% | 4.6% | 1.9% | 1.1% | 0.8% | 3.9% | 0.6% | 0.7% |
| Software Bundlers | 3.1% | 1.7% | 1.5% | 0.2% | 0.5% | 2.2% | 0.9% | 2.3% | 2.5% | 2.5% | 0.5% |
| Downloaders & Droppers | 2.2% | 2.3% | 6.5% | 3.2% | 6.6% | 2.8% | 1.5% | 3.2% | 3.1% | 3.3% | 0.4% |
| Obfuscators & Injectors | 1.7% | 1.0% | 5.3% | 5.2% | 7.3% | 1.9% | 1.6% | 1.7% | 2.8% | 1.6% | 0.6% |
| Adware | 1.6% | 4.5% | 7.1% | 0.2% | 5.2% | 7.8% | 4.1% | 4.7% | 7.2% | 5.3% | 2.0% |
| Exploits | 1.4% | 3.4% | 2.4% | 1.7% | 1.3% | 2.5% | 3.2% | 4.4% | 4.3% | 5.7% | 3.2% |
| Viruses | 1.1% | 0.4% | 2.2% | 7.4% | 1.5% | 0.4% | 0.3% | 0.3% | 0.8% | 0.4% | 0.2% |
| Other | 0.6% | 0.9% | 0.3% | 1.2% | 0.3% | 0.5% | 0.5% | 0.6% | 0.7% | 1.5% | 0.2% |
| Backdoors | 0.5% | 0.7% | 1.4% | 1.8% | 2.0% | 0.9% | 0.6% | 0.9% | 1.0% | 0.7% | 0.3% |
| Ransomware | 0.3% | 0.6% | 0.5% | 0.0% | 0.6% | 0.7% | 0.6% | 0.4% | 1.4% | 0.7% | 0.4% |
| Password Stealers & Monitoring Tools | 0.2% | 0.4% | 1.0% | 0.5% | 0.8% | 0.3% | 0.4% | 0.4% | 0.6% | 0.6% | 0.3% |

Microsoft Quick Guide to the Most Important Insights in Security

1. Cybersecurity Threats

| Category | Worldwide | USA | Brazil | China | Russia | France | Germany | UK | Italy | Canada | Japan |
|--------------------------------------|-----------|------|--------|-------|--------|--------|---------|-------|-------|--------|-------|
| Browser Modifiers | 7.6% | 9.1% | 11.8% | 0.6% | 7.0% | 14.3% | 8.7% | 10.9% | 15.3% | 11.3% | 4.2% |
| Trojans | 7.1% | 4.2% | 12.7% | 10.2% | 20.8% | 5.7% | 4.3% | 4.4% | 7.0% | 5.1% | 1.5% |
| Worms | 3.3% | 0.6% | 8.9% | 5.6% | 4.6% | 1.9% | 1.1% | 0.8% | 3.9% | 0.6% | 0.7% |
| Software Bundlers | 3.1% | 1.7% | 1.5% | 0.2% | 0.5% | 2.2% | 0.9% | 2.3% | 2.5% | 2.5% | 0.5% |
| Downloaders & Droppers | 2.2% | 2.3% | 6.5% | 3.2% | 6.6% | 2.8% | 1.5% | 3.2% | 3.1% | 3.3% | 0.4% |
| Obfuscators & Injectors | 1.7% | 1.0% | 5.3% | 5.2% | 7.3% | 1.9% | 1.6% | 1.7% | 2.8% | 1.6% | 0.6% |
| Adware | 1.6% | 4.5% | 7.1% | 0.2% | 5.2% | 7.8% | 4.1% | 4.7% | 7.2% | 5.3% | 2.0% |
| Exploits | 1.4% | 3.4% | 2.4% | 1.7% | 1.3% | 2.5% | 3.2% | 4.4% | 4.3% | 5.7% | 3.2% |
| Viruses | 1.1% | 0.4% | 2.2% | 7.4% | 1.5% | 0.4% | 0.3% | 0.3% | 0.8% | 0.4% | 0.2% |
| Other | 0.6% | 0.9% | 0.3% | 1.2% | 0.3% | 0.5% | 0.5% | 0.6% | 0.7% | 1.5% | 0.2% |
| Backdoors | 0.5% | 0.7% | 1.4% | 1.8% | 2.0% | 0.9% | 0.6% | 0.9% | 1.0% | 0.7% | 0.3% |
| Ransomware | 0.3% | 0.6% | 0.5% | 0.0% | 0.6% | 0.7% | 0.6% | 0.4% | 1.4% | 0.7% | 0.4% |
| Password Stealers & Monitoring Tools | 0.2% | 0.4% | 1.0% | 0.5% | 0.8% | 0.3% | 0.4% | 0.4% | 0.6% | 0.6% | 0.3% |

Microsoft Quick Guide to the Most Important Insights in Security

1. Cybersecurity Threats

| Category | Worldwide | USA | Brazil | China | Russia | France | Germany | UK | Italy | Canada | Japan |
|--------------------------------------|-----------|------|--------|-------|--------|--------|---------|-------|-------|--------|-------|
| Browser Modifiers | 7.6% | 9.1% | 11.8% | 0.6% | 7.0% | 14.3% | 8.7% | 10.9% | 15.3% | 11.3% | 4.2% |
| Trojans | 7.1% | 4.2% | 12.7% | 10.2% | 20.8% | 5.7% | 4.3% | 4.4% | 7.0% | 5.1% | 1.5% |
| Worms | 3.3% | 0.6% | 8.9% | 5.6% | 4.6% | 1.9% | 1.1% | 0.8% | 3.9% | 0.6% | 0.7% |
| Software Bundlers | 3.1% | 1.7% | 1.5% | 0.2% | 0.5% | 2.2% | 0.9% | 2.3% | 2.5% | 2.5% | 0.5% |
| Downloaders & Droppers | 2.2% | 2.3% | 6.5% | 3.2% | 6.6% | 2.8% | 1.5% | 3.2% | 3.1% | 3.3% | 0.4% |
| Obfuscators & Injectors | 1.7% | 1.0% | 5.3% | 5.2% | 7.3% | 1.9% | 1.6% | 1.7% | 2.8% | 1.6% | 0.6% |
| Adware | 1.6% | 4.5% | 7.1% | 0.2% | 5.2% | 7.8% | 4.1% | 4.7% | 7.2% | 5.3% | 2.0% |
| Exploits | 1.4% | 3.4% | 2.4% | 1.7% | 1.3% | 2.5% | 3.2% | 4.4% | 4.3% | 5.7% | 3.2% |
| Viruses | 1.1% | 0.4% | 2.2% | 7.4% | 1.5% | 0.4% | 0.3% | 0.3% | 0.8% | 0.4% | 0.2% |
| Other | 0.6% | 0.9% | 0.3% | 1.2% | 0.3% | 0.5% | 0.5% | 0.6% | 0.7% | 1.5% | 0.2% |
| Backdoors | 0.5% | 0.7% | 1.4% | 1.8% | 2.0% | 0.9% | 0.6% | 0.9% | 1.0% | 0.7% | 0.3% |
| Ransomware | 0.3% | 0.6% | 0.5% | 0.0% | 0.6% | 0.7% | 0.6% | 0.4% | 1.4% | 0.7% | 0.4% |
| Password Stealers & Monitoring Tools | 0.2% | 0.4% | 1.0% | 0.5% | 0.8% | 0.3% | 0.4% | 0.4% | 0.6% | 0.6% | 0.3% |

Microsoft Quick Guide to the Most Important Insights in Security

2. Why worry?

2016 Ponemon Cost of Data Breach Study

- Total \$4 million; up 29% since 2013
- Cost per record: \$158
- Incident response helps save \$16 per record
- Time to identify: 229 days
- Time to contain: 82 days

Likelihood of breach happening over the next 24 months is 26%

3. Cybersecurity Responses

- The evolving involvement of top executives ¹

1. PWC The Global State of Information Security® Survey 2016
2. Cybernetic Cyber Security Trends 2016
3. Gartner Six Trends in Cybersecurity

3. Cybersecurity Responses

- The evolving involvement of top executives ¹
- More budget for cybersecurity ²

1. PWC The Global State of Information Security® Survey 2016
2. Cybernetic Cyber Security Trends 2016
3. Gartner Six Trends in Cybersecurity

3. Cybersecurity Responses

- The evolving involvement of top executives ¹
- More budget for cybersecurity ²
- Spend less time on prevention and invest in detection and response ³

1. PWC The Global State of Information Security® Survey 2016

2. Cybernetic Cyber Security Trends 2016

3. Gartner Six Trends in Cybersecurity

3. Cybersecurity Responses

- The evolving involvement of top executives ¹
- More budget for cybersecurity ²
- Spend less time on prevention and invest in detection and response ³
- Moving Target Defense

1. PWC The Global State of Information Security® Survey 2016

2. Cybernetic Cyber Security Trends 2016

3. Gartner Six Trends in Cybersecurity

3. Cybersecurity Responses

- The evolving involvement of top executives ¹
- More budget for cybersecurity ²
- Spend less time on prevention and invest in detection and response ³
- Moving Target Defense
- Collaboration ¹

1. PWC The Global State of Information Security® Survey 2016

2. Cybernetic Cyber Security Trends 2016

3. Gartner Six Trends in Cybersecurity

3. Cybersecurity Responses

- The evolving involvement of top executives ¹
- More budget for cybersecurity ²
- Spend less time on prevention and invest in detection and response ³
- Moving Target Defense
- Collaboration ¹
- Legislation ²

1. PWC The Global State of Information Security® Survey 2016

2. Cybernetic Cyber Security Trends 2016

3. Gartner Six Trends in Cybersecurity

3. Cybersecurity Responses

- The evolving involvement of top executives ¹
- More budget for cybersecurity ²
- Spend less time on prevention and invest in detection and response ³
- Moving Target Defense
- Collaboration ¹
- Legislation ²
- Education ²

1. PWC The Global State of Information Security® Survey 2016

2. Cybernetic Cyber Security Trends 2016

3. Gartner Six Trends in Cybersecurity

4. Perspectives

- Stop ticking the pentest box

4. Perspectives

- Stop ticking the pentest box
- Evaluate your collaborators security awareness level

4. Perspectives

- Stop ticking the pentest box
- Evaluate your collaborators security awareness level
- Security by design

4. Perspectives

- Stop ticking the pentest box
- Evaluate your collaborators security awareness level
- Security by design
- Collaborate

Thank you!

Questions?

Pedro Queirós
pedro.queiros@multicert.com

multicert

Engineering for digital security

Lagoas Park, Edifício 3, Piso 3
2740-266 Porto Salvo
Oeiras – Portugal
Tel.: +351 217 123 010
Fax: +351 217 123 011

Avenida Sidónio Pais, 379
Edifício Hoechst A, Piso 3, Direito
4100-468 Porto – Portugal
Tel.: +351 223 391 810
Fax: +351 223 391 811

www.multicert.com