PROTECTING YOUR NETWORK

Vitor Ventura - @_vventura
Threat Researcher

Industry-leading threat intelligence. The largest threat detection network in the world.
Agenda
Agenda

• The threat landscape
• How TALOS address the threats
• How local targeting attacks go behind borders
• Closing thoughts
Threat landscape
THREAT LANDSCAPE
THREAT LANDSCAPE

Jurassic Park

The Godfather
THREAT LANDSCAPE

- Network Accessible
- Low Complexity
- No Authorization

Low Hanging Fruit on Decline

19.4%
What does this mean?

The Matrix
**THREAT INTEL**

- **1.5 MILLION** Daily Malware Samples
- **600 BILLION** Daily Email Messages
- **16 BILLION** Daily Web Requests
- **20 BILLION** Threats Blocked
- Internet-Wide Scanning
- Product Telemetry
- Vulnerability Discovery (Internal)
- Open Source Communities
- Honeypots

**INTEL SHARING**

- Customer Data Sharing Programs
- Provider Coordination Program
- Industry Sharing Partnerships (ISACs)
- Open Source Intel Sharing
- 3rd Party Programs (MAPP)
- 500+ Participants

**250+** Full Time Threat Intel Researchers

**MILLIONS** Of Telemetry Agents

**4** Global Data Centers

**100+** Threat Intelligence Partners

**1100+** Threat Traps
THREATS DON’T GO AWAY, HOW DO WE ADDRESS IT?
### Multi-Tiered Defense

**Cloud to Core Coverage**
- **WEB**: Reputation, URL Filtering, AVC
- **END POINT**: AMP, ClamAV
- **CLOUD**: FireAMP & ClamAV detection content
- **EMAIL**: Reputation, AntiSpam, Outbreak Filters
- **NETWORK**: Snort Subscription Rule Set, VDB – FireSIGHT Updates & Content, SEU/SRU Product Detection & Prevention Content
  - Global Threat Intelligence Updates
Industry Leading Expertise

- Threat Intelligence
- Engine Development
- Detection Research
- Vulnerability R&D / Operations
- Open Source & Community
- Outreach
European countries with a Talos representative
Forcing the Bad Guys to Innovate

- Spreading security news, updates, and other information to the public

  - ThreatSource Newsletter: cs.co/TalosUpdate
  - Social Media Posts:
    - Facebook: TalosGroupatCisco
    - Twitter: @talossecurity
  - White papers, articles, & other information: talosintelligence.com
  - Talos Blog: blog.talosintelligence.com
  - Instructional Videos: cs.co/talostube
Local attacks with global impacts
Mass email campaigns would target as many individuals as possible.

The effect on organizations would be mainly:

- shared drive encryption
- Business operations disruption due to workstation encryption
Some of these campaigns were limited due to:
- Language
- Geography

Big impact on organizations would require a lot of effort and a bit of luck.
What changed?
Local targeting becomes global

- The introduction of non-exploit based worm-like behavior
- The internal networks becomes the initial attack vector
- The companies threat model needs to expand
TALOS : Closing thoughts
Closing thoughts

collateral damage

casualties or damage

military action: to minimize precision in bombing

/Untrusted
Mitigations

- Be ready, have a plan, prepare your organization to react and recover
- Isolate vendors as much as possible, specially if they require high privileges.
- Segregate your networks, be ready to perform emergency segment isolation
- Deploy EDR like solutions, traditional AV aren’t enough anymore
- Ensure that you have a proper patch management program
Feedback and review

Please Rate and Review Feedback?

vitventu@cisco.com

@_vventura