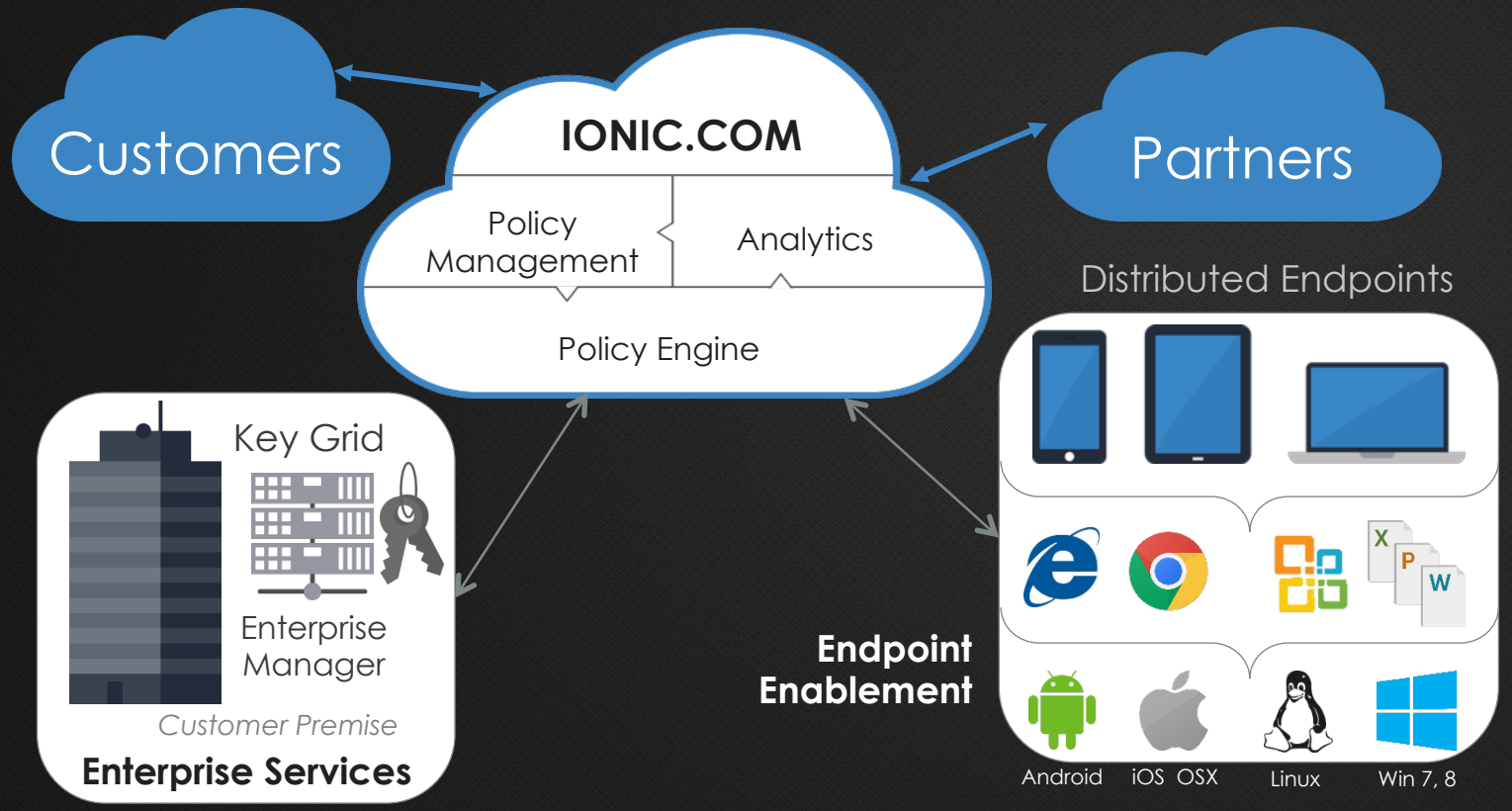
Discussion of Intrusion Software Controls for Bureau of Industry and Security's (BIS) Information Systems Technical Advisory Committee (ISTAC)

Technology Case Studies

Example Affected Products

Ionic Security Overview

- Information must be protected from the point of creation to point of consumption
- Businesses must maintain control over critical data… no matter where it resides.



Ionic Security Value

Protection:

- Scalable encryption & key management
- Enforce policy at the moment of data consumption
- Dynamically revoke access to data

Visibility:

- Coverage of all devices & data types
- Unified platform & single viewpoint
- User profiling & behavioral analysis

Control:

- Apply rights management to apps & data
- Centralized dynamic policy enforcement

Swept Into Definition

Proposed Intrusion Software Language (ECCN 4A005)

- ‘‘Systems,’’ ‘‘equipment,’’ or ‘‘components’’ therefor, ‘‘specially designed’’ or modified for the generation, operation or delivery of, or communication with, ‘‘intrusion software’’

- Intrusion software: (Cat 4) “Software” “specially designed” or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’, of a computer or network-capable device, and performing any of the following:
  a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
  b) The modification of the standard execution path of a program or process in order to allow the executions of externally provided instructions

Product Capabilities

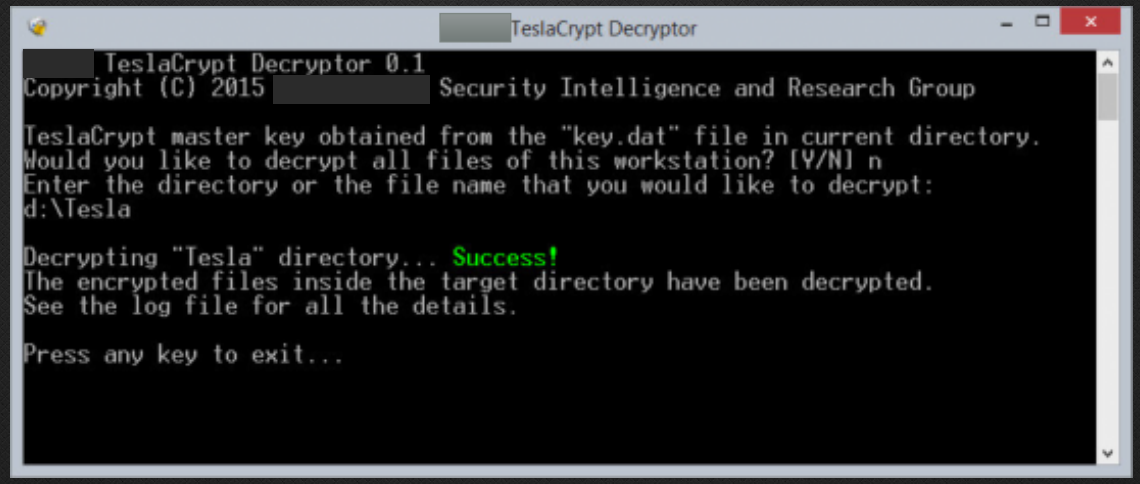
DETAILS OMITTED

Recovery Tools Overview

- An example class of malware are "crypto-lockers" or "ransomware"
  - Encrypts all the user's valuable files
  - Asks the user to pay a "ransom" to get the decryption keys back
  - An example piece of malware is called "Teslacrypt"
- Corresponding recovery tool example:
  - Easy-to-use tool that results in the user recovering their files and removing the Teslacrypt malware.

Value

- Assist a user in regaining control of their system.
- Remove malware from system.
- Recover data/files if applicable.
  - i.e. in cases of ransomware
- Stop the spread of malware laterally to other systems.



Screenshots from http://blogs.cisco.com/security/talos/teslacrypt

Swept Into Definition

Proposed Intrusion Software Language (ECCN 4A005)

- ‘‘Systems,’’ ‘‘equipment,’’ or ‘‘components’’ therefor, ‘‘specially designed’’ or modified for the generation, operation or delivery of, or communication with, ‘‘intrusion software’’
- Intrusion software: (Cat 4) “Software” “specially designed” or modified to avoid detection by ‘monitoring tools’, or to defeat ‘protective countermeasures’, of a computer or network-capable device, and performing any of the following:
  a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or
  b) The modification of the standard execution path of a program or process in order to allow the executions of externally provided instructions

Product Capabilities

- Defeats the system and malware’s protective countermeasures, potentially including:
  - Mitigations such as DEP/ASLR
  - Any Process/Session Isolation
  - Malware’s integrity checking
- Modifies the execution path of the malware.
- Extracts data from the malware to obtain the encryption keys.
- Extracts and modifies data from the system to recover the encrypted files.
- Is delivered in an package from the providing company’s servers to users so they can run it.

Examples of Definitions Used

Rootkit

- Is described as presumptively offensive, but is a crucial capability for anti-virus programs to be able to intercept/ inspect/modify system actions at a low level to stop malicious software.

"Avoid detection" or "defeat"

- FAQ #8 states auto-updaters are not controlled because they "may need to interact" with monitoring tools/etc but don't "defeat" or "subvert" the system. Interaction in these cases, however, is to keep the monitoring tool from detecting the update as malicious and interrupting it.

"Monitoring tool"

- FAQ #8 says anti-virus is excluded as it is a monitoring tool. Nothing says that all monitoring tools are excluded. Software like keyloggers can be monitoring tools for legitimate or illegitimate purposes.

Exploits/Malware for Defensive vs. Offensive Purposes

Defensive

- Need to design defenses that can stop not just a single sample, but current/future variants of it.
- Need technology, not just samples, to understand the root cause of the vulnerability.
  - Patching the root cause means a better defense.
  - Patching without understanding root cause has a long history of being ineffective.
- If attacker has a mass-distribution method (botnet C&C, mutation generator, etc) then need this as well to discover how to stop it.
  - Analyze communication methods to malware to write network signatures.
  - Analyze mutation generators to make signatures to catch variants.

Offensive

- Only need to succeed once.
- A single sample of malware is enough to compromise a target.
- No need for user to understand the root cause of the vulnerability, just need to 'throw' the malware/exploit against a vulnerable target.
- Can be delivered with general purpose tools, for example:
  - Email attachment (spear-phishing)
  - Seeding of webpages
  - Exploit delivered by netcat or other simple socket communications to a vulnerable system.

Contact Information

Ryan Speers
Director of Applied Research
ryan@ionic.com