HOST BASED IOC VALIDATION
An approach for large networks without an enterprise solution in place

26.01.2016 - Christoph Giese
Deutsche Telekom CDC/CERT
AGENDA

1. Use Case
2. Requirements: (Agentless) Host Based IoC Validation
3. Development
4. Rollout (e.g. using McAfee ePO) & Data analysis
5. Further steps
6. Summary
USE CASE
USE CASE
IOC-CHECKS IN DTAG

SPAM E-MAILS  BINARY DATA  TEXT DATA  SHARING

ANALYSIS

RESULTS: INDICATORS OF COMPROMISE
IPs, FQDNs, Substrings, MD5s, Filenames, Pathinformation,
Registry-Values, Handles, Mutexes, Hooks, (Hidden-) Processes
→ Combinations

IOC-DATABASE

DNS-SERVER  PROXY-SERVER  ID/PS
FIREWALL  FIREEye  AV

WORKSTATIONS 150K+
SERVER 60K

–Public–  Christoph Giese / Host Based IoC Validation
REQUIREMENTS
AGENTLESS HOST BASED IOC VALIDATION
REQUIREMENTS
NECESSARY FUNCTIONALITY & OPTIONAL FEATURES

## LIVE IOC-SCANNING, REMOTE FORENSICS

- IoC-Types (Strings, Hashes, Parsing binary data, IPs, FQDN, Registry-Values ...)
- Import interfaces (OpenIOC, STIX/CyBox, YARA...)
- Scheduling (Scanning in predefined timeframes, periodically saving files for diffs)
- Status of Collection (System reachable, not reachable, continuously not reachable)

## LIVE DATA-ACQUISITION, REMOTE FORENSICS

- General system information (Hostname, HDD, Memory, processes, patches, SW)
- Forensic-Triage
- Full/Selected dump of files, registry hives, RAM
- “Rule based” data acquisition

## PORTABLE USAGE

- Fast IoC checks in different networks
- No external dependencies needed
- No installation required
- Multiple operating systems (Windows first)

## (OTHER THINGS WITH NO SPECIAL TITLE)

- Privacy / Workers council (approval process, pseudonymization, four-eyes principle)
- Allows execution of self-developed scripts on target system
- Interfaces to existing products (SIEM, FireEye-NX)
DEVELOPMENT
**DEVELOPMENT**

**SELF-DEVELOPED IOC-CHECKERS / DATA COLLECTORS**

**SELF-DEVELOPED IOC-SCANNER / DATA COLLECTOR**

- **Input:** Indicators of Compromise
- **Implementation of checks**
  - PyWin32
  - PylInstaller
  - Include TSK tools
- **Output:** One-Click-Executable
  - No ext. dependencies

- **Input:** Baselining data
- **Implementation of data acquisition**
  - istat.exe
  - icat.exe...

**Tools:**
- Registry
- Hash
- Files
- Tasks
ROLLOUT / DATA ANALYSIS
ROLLOUT
EXAMPLE USING MCAFEE EPO

Host Based IoC Validator
- Modul usage
- Modul development

Analysis
1. Follow up alerts on IoCs
2. Analysis of baseling data

TEST & DEPLOYMENT
McAfee EPO

RESULT COLLECTION
Dropzone (SMB, SFTP, ...)

OFFICE NETWORK
DATA ANALYSIS
USING POSTGRESQL

DROPING ZONE (SMB/SFTP)

RESULTS HOST A

RESULTS HOST B

DATABASE

IMPORT

Alert on IoC-Match

Least existing
Registry-Run-Keys

Least existing
Scheduled Tasks

...
FURTHER STEPS
FURTHER STEPS

IDENTIFY NEW VEHICLES (ROLLOUT)

- NatCos (European partners)
- Server scans (Auditserver)
- Other (sub-) networks in DTAG / T-Systems

STANDARDIZED INPUT/OUTPUT FORMAT

DATA ANALYSIS

- Development of further use cases

FEATURE DEVELOPMENT

- Removed pictures
- Process
- Mutex
- Dump
- Custom
- Yara-Rule
THANK YOU! QUESTIONS?
Host Based IoC Validation <cert@telekom.de>

26.01.2016 Christoph Giese <C.Giese@telekom.de>
Deutsche Telekom CDC/CERT