Started from the Bottom: Exploiting Data Sources to Uncover ATT&CK Behaviors

• 2 likes • 893 views AI-enhanced description

The document discusses enhancing ATT&CK data sources by developing data models. It proposes opportunities like addressing lack of context, redundancy, and broad scope Read more

JamieWilliams130

More Related Content

Started from the Bottom: Exploiting Data Sources to Uncover ATT&CK Behaviors

1. **Started From the** Bottom: Exploiting Data Sources to Uncover ® Behaviors Jose Rodriguez @Cyb3rPandaH Jamie Williams @jamieantisocial MITRE ATT&CK @MITREattack

2. **Agenda ● Data sources? ●** Are ATT&CK data sources sufficient for security operations? ● Any opportunities for ATT&CK data sources improvement? ● How can we enhance current data sources? ● How do these concepts apply to ATT&CK? ● Data-driven hunt experiment

3. **Data sources?**

4. **When you hear** about a new threat…. As defenders, what can we do?

5. **Threat modeling Exploit** Public- Facing Application
6. **Threat modeling Exploit** Public- Facing Application Rundll32 Service Execution Regsvr32 Windows Command Shell
7. **Threat modeling Exploit** Public- Facing Application Rundll32 Service Execution Regsvr32 Windows Command Shell Match Legitimate Name or Location Scheduled Task COR_PROFILER Windows Service Modify Registry …
8. **Exploit Public- Facing Application Rundll32 Service** Execution Regsvr32 Windows Command Shell Match Legitimate Name or Location Scheduled Task COR_PROFILER Windows Service Modify Registry Threat modeling++ …
9. **Threat modeling++ Exploit Public- Facing Application Rundll32 Regsvr32 Service Execution Windows Command Shell Match** Legitimate Name or Location Scheduled Task COR_PROFILER Windows Service Modify Registry Initial Access ImpactC2Exfil.Collection Lateral Movement Discovery Cred. Access Defense Evasion Priv. Esc.PersistenceExecution
10. **Threat modeling++ Exploit Public- Facing Application Rundll32 Regsvr32 Service Execution Windows Command Shell Match** Legitimate Name or Location Scheduled Task COR_PROFILER Windows Service Modify Registry Initial Access ImpactC2Exfil.Collection Lateral Movement Discovery Cred. Access Defense Evasion Priv. Esc.PersistenceExecution
11. **Initial Access ImpactC2Exfil.Collection Lateral Movement Discovery Cred. Access Defense Evasion Priv. Esc.PersistenceExecution ATT&CK**
12. **Initial Access ImpactC2Exfil.Collection Lateral Movement Discovery Cred. Access Defense Evasion Priv. Esc.PersistenceExecution ATT&CK**
13. **Initial Access ImpactC2Exfil.Collection Lateral Movement Discovery Cred. Access Defense Evasion Priv. Esc.PersistenceExecution ATT&CK**
14. **Data source Source of** information collected by a sensor or logging system that may be used to collect information relevant to identifying the action being performed, sequence of actions, or the results of those actions by an adversary. DLL monitoring Process monitoring Netflow Windows event logs File monitoring …
15. **Are ATT&CK data sources sufficient** for security operations?
16. **How data sources** support this process? Adversary Behavior Telemetry Data Sources Modeling Threat Actor Identifying Relevant Data
17. **Data Sources Command ProcessProcess Port Ip Process dll Connected to Connected** to Created Created Executed Loaded Sysmon 3 Network Connection Sysmon 7 Image Loaded PowerShell 4104 Script Block Logging Threat Actor Model – Data Perspective Relevant Data What data are we generating? What data are we collecting? Effective Detection Strategy Process command-line parameters Process monitoring Netflow Windows event logs File monitoring Security 4624 Successful Logon Zeek Conn Log TCP/UDP/ICMP Osquery Process_events How data sources support this process?
18. **ATT&CK data sources** mapped to sub-techniques
19. **Any opportunities for ATT&CK data** sources improvement? https://screenrant.com/lord-rings-movies-gandalf-staffs-grey-white-explained/
20. **Some opportunities for** improvement are: • Lack of context • Redundancy and overlapping • Too broad scope https://www.pinterest.com/pin/535013630705243890/
21. **Opportunity: Lack of** context More context will help to map ATT&CK data sources to event logs Sysmon 1 Process Creation Sysmon 3 Network Connection Sysmon 5 Process Terminated Sysmon 8 Create Remote Thread Sysmon 10 Process Access Process Monitoring? ?
22. **Opportunity: Redundancy and** overlapping Standardize names & account for intersections
23. **Opportunity: Too broad** scope Breaking down data sources with a broad scope
24. **How can we enhance** current ATT&CK data sources? https://lotr.fandom.com/wiki/Gandalf
25. **Enter data modeling!! A** data model is a collection of concepts for organizing data elements and standardizing how they relate to one another.

26. **How to identify** data elements and relationships? A data dictionary describes a single event log and its corresponding event field names.

27. **Documenting event logs** via data dictionaries Module dllProcess Loaded Sysmon 7 Image Loaded Field Type Description Sample Value Process Guid String Process Guid of the process that loaded the image {A98268C1-A12A-5ACD- 0000-0010E4C8B300} Process Id Integer Process ID used by the os to identify the process that loaded the image 3532 Image String File path of the process that loaded the image C:WindowsSystem32 cmd.exe Image Loaded String Full path of the image loaded C:WindowsSystem32 msvcrt.dll Description String Description of the image loaded Windows NT CRT DLL

28. **Documenting data sources** via data dictionaries Module dllProcess Loaded Process IpProcess Connected to PortProcess Connected to IpUser Connected to PortUser Connected to Sysmon 7 Image Loaded Sysmon 3 Network Connection Data fields - ProcessGuid - ProcessId - Image - ImageLoaded - Product - Description - Signed - Signature - SignatureStatus Data fields - ProcessGuid - ProcessId - Image - User - Protocol - SourceIp - SourcePort - DestinationIp - DestinationPort Sysmon 8 Create Remote Thread Data fields - SourceProcessGuid - SourceProcessId - SourceImage - TargetProcessGuid - TargetProcessId - TargetImage - StartModule - StartFunction ProcessProcess Wrote to Sysmon 11 File Create File FileProcess Created Data fields - ProcessGuid - ProcessId - Image - TargetFileName - CreationUtcTime

29. **How do these concepts** apply to ATT&CK?

30. **Adding metadata to** ATT&CK data sources Process Sysmon 1 Process Creation Sysmon 3 Network Connection Sysmon 8 Create Remote Thread Sysmon 10 Process Access Security 4688 Process Created Security 5156 Connection Permitted ProcessProcess Created ProcessUser Created IpProcess Connected To IpUser Connected To ProcessProcess Wrote To ProcessProcess Opened Process Network Connection Process Creation Process Modification Process Access Data Sources Components Relationships Event Logs

31. **Identifying relevant data** via data sources objects Sysmon 7 Image Loaded Sysmon 3 Network Connection Data fields - ProcessGuid - ProcessId - Image - ImageLoaded - Product - Description - Signed - Signature - SignatureStatus Data fields - ProcessGuid - ProcessId - Image - User - Protocol - SourceIp - SourcePort - DestinationIp - DestinationPort Sysmon 8 Create Remote Thread Data fields - SourceProcessGuid - SourceProcessId - SourceImage - TargetProcessGuid - TargetProcessId - TargetImage - StartModule - StartFunction Sysmon 11 File Create Data fields - ProcessGuid - ProcessId - Image - TargetFileName - CreationUtcTime API Auth. logs Process Module Netflow File Windows event logs

32. **Identifying relevant data** via data sources objects Sysmon 7 Image Loaded Sysmon 3 Network Connection Data fields - ProcessGuid - ProcessId - Image - ImageLoaded - Product - Description - Signed - Signature - SignatureStatus Data fields - ProcessGuid - ProcessId - Image - User - Protocol - SourceIp - SourcePort - DestinationIp - DestinationPort Sysmon 8 Create Remote Thread Data fields - SourceProcessGuid - SourceProcessId - SourceImage - TargetProcessGuid - TargetProcessId - TargetImage - StartModule - StartFunction Sysmon 11 File Create Data fields - ProcessGuid - ProcessId - Image - TargetFileName - CreationUtcTime Identify coverage and gaps ? ? API Auth. logs Process Module Netflow File Windows event logs Windows event logs

33. **T1574.012 Hijack Execution Flow:** COR_PROFILER PERSISTENCE Data-driven hunt experiment

34. **A basic detection** research process 1. Research goal definition 2. Initial detection modeling 3. Adversary simulation 4. Detection model definition 5. Detection model validation 6. Documentation & communication

35. **1. Research goal:** COR_PROFILER

36. **1. Research goal:** COR_PROFILER Creation of malicious dll Use of wmic.exe Modification of the registry to set environment variable Load of dll through .NET processes Where will we find this, and more, data?

37. **2. Initial detection** modeling: COR_PROFILER Creation of malicious dll Use of wmic.exe Modification of the registry to set environment variable Load of dll through .NET processes Process Process creation User Process created Process Process created Sysmon 1 Process Creation File Windows Registry Module Data Sources module load Data Components Windows registry key modification File creation Process File created Relationships Environment Activity Event Logs Sysmon 11 File Creation Process Registry Key Value modified Sysmon 13 Registry Value Set Process dll loaded Sysmon 7 Image Loaded

38. **3. Adversary simulation:** COR_PROFILER
39. **4. Detection model:** Persistence & COR_PROFILER User Process Process File Process Registry Key Value modifies Process dll loads Before reboot After reboot Data Model creates creates creates Creation of malicious dll Use of wmic.exe Modification of the registry to set environment variable Load of dll through .NET processes Environment Activity
40. **4. Detection model:** COR_PROFILER Sysmon 13 Registry Value Set Sysmon 1 Process Creation Creation of malicious dll Use of wmic.exe Modification of the registry to set environment variable Load of dll through .NET processes Environment Activity
41. **4. Detection model:** COR_PROFILER Sysmon 13 Registry Value Set Sysmon 1 Process Creation Creation of malicious dll Use of wmic.exe Modification of the registry to set environment variable Load of dll through .NET processes Environment Activity
42. **4. Detection model:** CMD.EXE ParentProcess cmd.exe also has more child processes
43. **4. Detection model:** COR_PROFILER (Before Rebooting) cmd.exe wmic.exe wmiprvse.exe modifies modifies reg.exe creates modifies Registry Entry e0b3489da74f.dll Inprocserver32 CLSID {11111111-1111-1111-1111- 1111deadbeef} Environment Variable COR_ENABLING_PROFILING Environment Variable COR_PROFILER CLSID {11111111-1111-1111- 1111-1111deadbeef} Data Model Simulation Data creates Registry Entry e0b3489da74f.dll Inprocserver32 CLSID {11111111-1111-1111-1111- 1111deadbeef} Environment Variable COR_ENABLING_PROFILING Creation of malicious dll Use of wmic.exe Modification of the registry to set environment variable Load of dll through .NET processes Environment Activity Environment Variable COR_PROFILER CLSID {11111111-1111-1111- 1111-1111deadbeef} Registry Entry e0b3489da74f.dll Inprocserver32 CLSID {11111111-1111-1111-1111-1111deadbeef} Environment Variable COR_PROFILER CLSID {11111111-1111-1111- 1111-1111deadbeef}
44. **4. Detection model:** COR_PROFILER (Before Rebooting) process process process modifies modifies process creates modifies Registry Entry e0b3489da74f.dll Inprocserver32 CLSID {11111111-1111-1111-1111- 1111deadbeef} Environment Variable COR_ENABLING_PROFILING Environment Variable COR_PROFILER CLSID {11111111-1111-1111-1111- 1111deadbeef} Data Model Adversary Behavior creates registry key value Inprocserver32 CLSID {XXX-XXX-XXX-XXX-XXX} registry key value COR_ENABLING_PROFILING Creation of malicious dll Use of wmic.exe Modification of the registry to set environment variable Load of dll through .NET processes Environment Activity registry key value COR_PROFILER CLSID {XXX-XXX-XXX-XXX-XXX}
45. **4. Detection model:** COR_PROFILER (Before Rebooting) Data Analytic
46. **4. Detection model:** COR_PROFILER (Before Rebooting) Data Analytic dll registered using inprocserver and CLSID COR_PROFILER environment variable configured with same CLSID
47. **4. Detection model:** COR_PROFILER (Before Rebooting) Data Analytic Results
48. **After a nice** weekend... https://wifflegif.com/tags/67564-bombur-gifs
49. **4. Detection model:** e0b3489da74f.DLL load Sysmon 7 Image Loaded Creation of malicious dll Use of wmic.exe Modification of the registry to set environment variable Load of dll through .NET processes Environment Activity
50. **4. Detection model:** e0b3489da74f.DLL load Sysmon 7 Image Loaded Creation of malicious dll Use of wmic.exe Modification of the registry to set environment variable Load of dll through .NET processes Environment Activity
51. **4. Detection model:** Persistence & COR_PROFILER Data Model Adversary Behavior Before Reboot After Reboot process process process modifies modifies process creates modifies creates registry key value Inprocserver32 CLSID {XXX-XXX-XXX-XXX-XXX} dll registry key value COR_ENABLING_PROFILING registry key value COR_PROFILER CLSID {XXX-XXX-XXX-XXX-XXX} process loads dll
52. **4. Detection model** : COR_PROFILER (After Reboot) Data Analytic
53. **4. Detection model** : COR_PROFILER (After Reboot) Data Analytic dll registered using inprocserver and CLSID COR_PROFILER environment variable configured with same CLSID dll loaded after reboot
54. **4. Detection model** : COR_PROFILER (After Rebooting) Data Analytic Results
55. **4. Detection model** : COR_PROFILER (After Rebooting) Data Analytic Results
56. **Is that all? https://gifer.com/en/gifs/saruman**
57. **4. Detection model:** Visual Studio 2019 (victim) What else does the victim process do?

58. **4. Detection model:** Persistence & COR_PROFILER Data Model Adversary Behavior Before Reboot After Reboot process process process modifies modifies process creates modifies creates registry key value Inprocserver32 CLSID {XXX-XXX-XXX-XXX-XXX} dll registry key value COR_ENABLING_PROFILING registry key value COR_PROFILER CLSID {XXX-XXX-XXX-XXX- XXX} process loads process ip Connects to process dll creates creates

59. **4. Detection model** : COR_PROFILER (After Reboot) Data Analytic

60. **4. Detection model** : COR_PROFILER (After Reboot) Data Analytic dll registered using inprocserver and CLSID COR_PROFILER environment variable configured with same CLSID dll loaded after reboot Child process of process that loaded dll Child process making a network connection

61. **5. Detection model:** Persistence & COR_PROFILER

62. **5. Detection model:** Persistence & COR_PROFILER regsvr32.exe connected to 151.101.208.133 after being spawned by a powershell.exe that loaded e0b3489da74f.dll due to COR_PROFILER environment variables set by wmiprvse.exe and reg.exe

63. **6. Documentation and** communication Before Reboot After Reboot process process process modifies modifies process creates modifies creates registry key value Inprocserver32 CLSID {XXX-XXX-XXX-XXX-XXX} dll registry key value COR_ENABLING_PROFILING registry key value COR_PROFILER CLSID {XXX-XXX-XXX-XXX- XXX} process loads process ip Connects to process dll creates creates

64. **6. Documentation and** communication Before Reboot After Reboot process process process modifies modifies process creates modifies creates registry key value Inprocserver32 CLSID {XXX-XXX-XXX-XXX-XXX} dll registry key value COR_ENABLING_PROFILING registry key value COR_PROFILER CLSID {XXX-XXX-XXX-XXX- XXX} process loads process ip Connects to process dll creates creates Behavior Context

65. **Conclusion •Modeling data sources** can provide more context •We can use this enhanced understanding of data sources and their relationships to more effectively uncover ATT&CK behaviors

66. **Contact info and** relevant links • attack.mitre.org • redcanary.com/blog/ blue-mockingbird-cryptominer/ • redcanary.com/blog/ cor_profiler-for-persistence/ • 3gstudent.github.io/ 3gstudent.github.io/ Use-CLR-to-maintain-persistence/ Jose Rodriguez @Cyb3rPandaH Jamie Williams @jamieantisocial MITRE ATT&CK @MITREattack • github.com/redcanaryco/atomic-red-team • github.com/Cyb3rWard0g/HELK • github.com/OTRF/OSSEM • github.com/OTRF/Mordor • mitre.org/sites/default/files/publications/ pr-19-3892-ttp-based-hunting.pdf

Download now