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

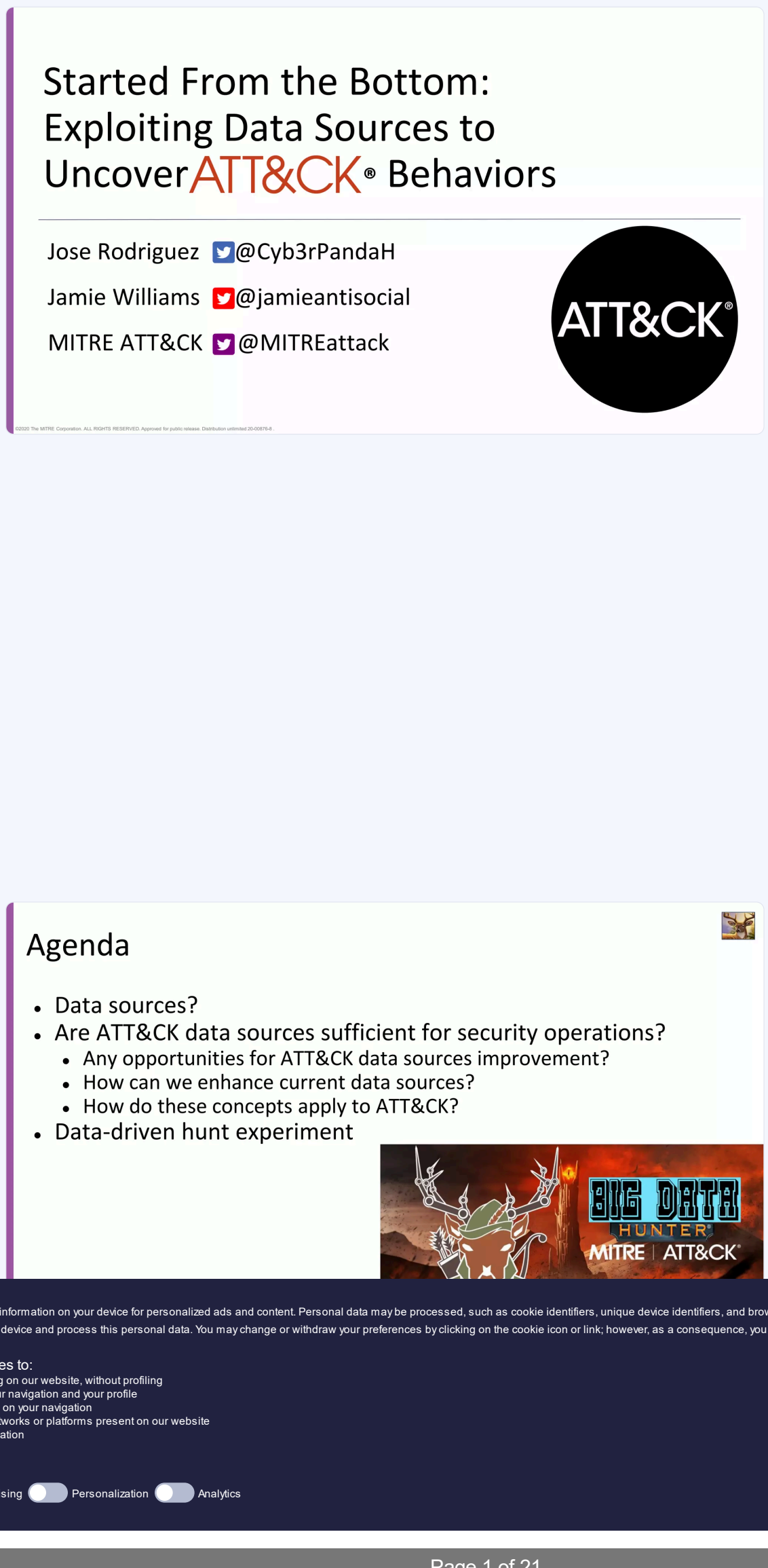
Sep 11, 2020 • 2 likes • 893 views

AI-enhanced description

JamieWilliams130 Follow

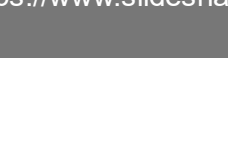
The document discusses enhancing ATT&CK data sources by developing data models. It proposes opportunities like addressing lack of context, redundancy, and broad scope in ATT&CK data sources. It then describes a process to model adversary behavior li…

Read more



Recommended

Lateral Movement wi…
kieranjacobsen



Android malware …
Jason Ross

Outlook and Exchange for …
Nick Landers

Hunting for Credentials …
Teymur Kheirkhabarov

A Case Study in Attacking …
Will Schroeder

BriMor Labs Live Respons…
BriMorLabs

Android malware …
Sandeep Joshi

File security system
ÁŠHÍŸÂ ŹÂBÊÊÑ

FireEye Use Cases — …
Valery Yelanin

Windows Ağlarda Saldır…
Sparta Bilişim

ATT&CK Data sources? 🤔

Tactics: Persistence, Privilege Escalation, Defense Evasion

Platforms: Windows

Permissions Required: Administrator, User

Data Sources: File monitoring, Process command-line parameters, Process monitoring, Windows Registry

Contributors: Jesse Brown, Red Canary

Version: 1.0

Created: 24 June 2020

Last Modified: 26 June 2020

When you hear about a new threat....

Introducing Blue Mockingbird

Red Canary Intel is monitoring a potentially novel threat that is deploying Monero cryptocurrency-mining payloads on Windows machines at multiple organizations.

As defenders, what can we do?

Threat modeling

Gaining entry

Exploit Public-Facing Application

In at least two incident response (IR) engagements, Blue Mockingbird has exploited public-facing web applications (T1190: Exploit Public-Facing Application) that implemented Telerik UI for ASP.NET AJAX. This suite of user interface components accelerates the web development process, but some versions are susceptible to a deserialization vulnerability, CVE-2019-18935. The exploitation of this CVE is not unique to Blue Mockingbird, but it has been a common point of entry.

In exploiting this vulnerability, two DLLs are uploaded to a web application running on a Windows IIS web server. In telemetry, investigators will notice `w3wp.exe` writing the DLLs to disk and then immediately loading them into memory afterward. In some cases, this will cause `w3wp.exe` to temporarily freeze and fail to successfully serve HTTP responses.

For a diagnostic to determine whether you are potentially affected by the Telerik CVE, you can search the IIS access logs for the string `POST Telerik.Web.UI.WebResource.axd`. In victim environments, our IR partners found entries similar to these:

```
2020-04-29 02:01:24 10.0.0.1 POST /Telerik.Web.UI.WebResource.axd type=rau 80 -  Mozilla/5.0+
(Windows+NT+10.0;+Win64;+x64;+rv:54.0)+Gecko/20100101+Firefox/54.0 - 200 0 0 625

2020-04-29 02:01:27 10.0.0.1 POST /Telerik.Web.UI.WebResource.axd type=rau 80 -  Mozilla/5.0+
(Windows+NT+10.0;+Win64;+x64;+rv:54.0)+Gecko/20100101+Firefox/54.0 - 500 0 0 46
```


Threat modeling

Exploit Public-

```
(Windows+NT+10.0;+Win64;+x64;+rv:54.0)+Gecko/20100101+Firefox/54.0 - 200 0 0 625

2020-04-29 02:01:27 10.0.0.1 POST /Telerik.Web.UI.WebResource.axd type=rau 80 -  Mozilla/5.0+
(Windows+NT+10.0;+Win64;+x64;+rv:54.0)+Gecko/20100101+Firefox/54.0 - 500 0 0 46
```


Threat modeling

```
cmd.exe /c sc config wercplsupport start= auto && sc start wercplsupport && copy
c:\windows\System32\dllhost.dll c:\windows\System32\wercplsupporte.dll /y && schtasks /create /tn "Windows
Problems Collection" /tr "regsvr32.exe /s c:\windows\System32\wercplsupporte.dll" /sc DAILY /st 09:02 /F /RU
System && start "" regsvr32.exe /s c:\windows\System32\dllogex.dll
```

Since `COR_PROFILER` was configured, any process that loaded the Microsoft .NET Common Language Runtime would execute the command above, re-establishing persistence. The command configured the Windows Problem Reports and Solutions Control Panel Support service to execute automatically at boot (T1543.003: Windows Service). In a separate command, the actor modified the existing `wercplsupport` service to use the miner DLL instead of the legitimate one:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\wercplsupport\Parameters" /f /v ServiceDll /t
REG_EXPAND_SZ /d "c:\windows\System32\wercplsupporte.dll"
```

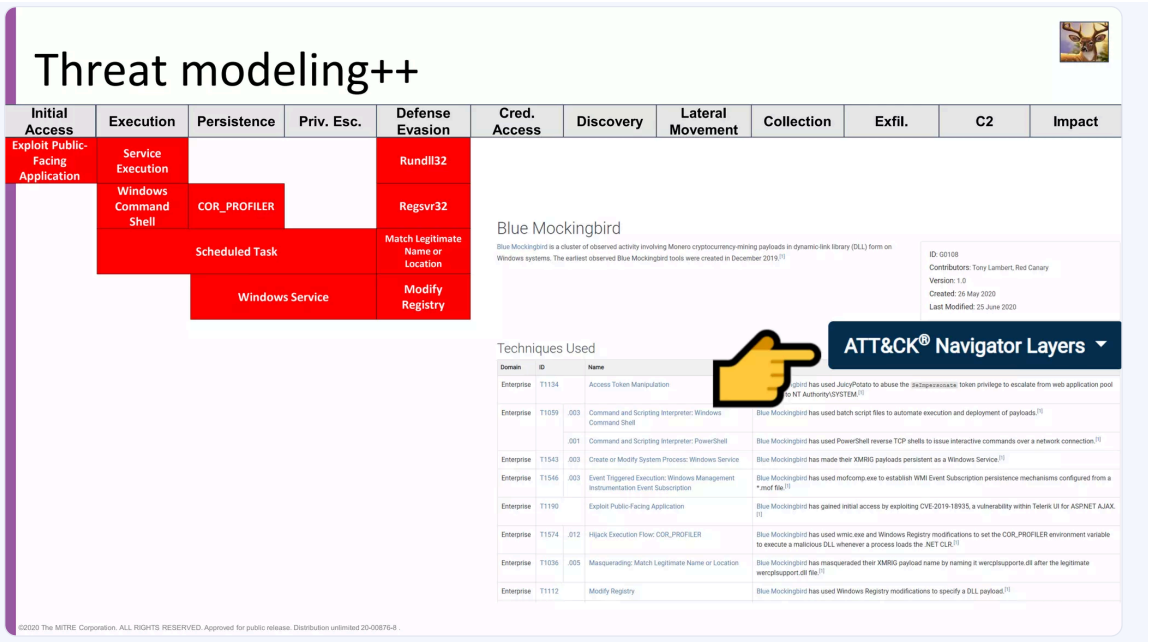
- Exploit Public-Facing Application
- Rundll32
- Regsvr32
- Service Execution
- Windows Command Shell
- Match Legitimate Name or Location
- Scheduled Task
- COR_PROFILER
- Windows Service
- Modify Registry
- •••

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
- •••

Threat modeling++

Initial Access	Execution	Persistence	Priv. Esc.	Defense Evasion	Cred. Access	Discovery	Lateral Movement	Collection	Exfil.	C2	Impact
Exploit Public-Facing Application	Service Execution			Rundll32							
	Windows Command Shell	COR_PROFILER		Regsvr32							
	Scheduled Task			Match Legitimate Name or Location							
		Windows Service		Modify Registry							



More Related Content

What's hot (20)

- FireEye Use Cases — FireEye Solution …
- Windows Ağlarda Saldırı Tespiti
- Windows Forensic 101
- Transparent Data Encryption in PostgreSQL …
- The Travelling Pentester: Diaries of the Shortest Pat…
- Android security

Similar to Started from the Bottom: Exploiting Data Sources to Uncover ATT&CK Behaviors (20)

- The Enterprise Guide to Building a Data Mesh - …
- Redis Streams plus Spark Structured Streaming
- fundamentalsofeventdriven microservices1172848973…
- DBMS PPT(CRIME DATABASE).pptx Database s
- “Lights Out”Configuration using Tivoli Netcool …
- Presentation.pdf

Recently uploaded (20)

SQL Database Design For Developers - Cascadia PHP…

Return-Conveyor-loopteq-o-400-english-pdf

Energy Modelling and Data Analytics for Net-Zero …

Unlocking AI-Powered Automation with UiPath …

Using ScyllaDB for Extreme Scale Workloads

Session 8 AI Assoc Series: Fundamen

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